Федеральная государственная информационная система ценообразования в строительстве
(ФГИС ЦС)

Инструкция пользователя для подключения к ФГИС ЦС с использованием сертификатов по ГОСТ Р 34.10-2012

Москва 2024

Содержание

Список терминов и сокращений 3
Аннотация 4
1. Общие положения 5
2. Порядок получения СКЗИ 5
3. Требования к АРМ пользователя 5
4. Подготовка АРМ пользователя к установке СКЗИ 6
5. Установка сертификатов в локальное хранилище АРМ 7
6. Установка СКЗИ при помощи «Единого инсталлятора» 11
7. Регистрация ПО «Континент TLS-клиент» версия 2 13
8. Настройка ПО «Континент TLS-клиент» версия 2 15
9. Установка сертификата пользователя 21
10. Установка Jinn Sign Extension для браузеров Chrome, Mozilla 24
11. Подключение к личному кабинету ФГИС ЦС 28
12. Использование Крипто Про CSP 30
13. Установка Крипто Про ЭЦП Browser plug-in 31

Список терминов и сокращений

Термин/ сокращение	Определение
CRL	Certificate Revocation List – список аннулированных сертификатов
RDP	Remote Desktop Protocol – протокол удаленного рабочего стола, использующийся для обеспечения удалённой работы пользователя с сервером терминалов
АРМ	Автоматизированное рабочее место
Портал Госуслуг	Портал государственных услуг Российской Федерации
ЕСИА	Единая система идентификации и аутентификации
ОС	Операционная система
ПО	Программное обеспечение
ПО «Jinn-Client»	Сертифицированное средство криптографической защиты информации для создания электронной подписи и доверенной визуализации документов
СКЗИ	Средство криптографической защиты информации
СКЗИ «Континент TLS-клиент»	Средство криптографической защиты информации, система обеспечения защищенного удаленного доступа к web-приложениям с использованием алгоритмов шифрования ГОСТ
УКЭП	Усиленная квалифицированная электронная подпись
УЦ	Удостоверяющий центр
ФГИС ЦС	Федеральная государственная информационная система ценообразования в строительстве

Аннотация

Данная инструкция предназначена для пользователей ФГИС ЦС, использующих в работе с системой СКЗИ Сертификат Удостоверяющего Центра (по ГОСТ Р 34.10-2012), и описывает порядок действий по установке и настройке программного обеспечения на АРМ пользователя ФГИС ЦС для работы с квалифицированными сертификатами электронной подписи, выпущенными по ГОСТ Р 34.10-2012, для получения доступа к личному кабинету ФГИС ЦС.

1. Общие положения

1.1 Для входа в личный кабинет ФГИС ЦС, необходимо сначала пройти авторизацию на Портале государственных услуг Российской Федерации https://www.gosuslugi.ru/ и получить усиленную квалифицированную электронную подпись (УКЭП), которая понадобится для обеспечения юридической значимости передаваемых в ФГИС ЦС данных.

1.2 Для регистрации организации зарегистрируйте физическое лицо (руководителя организации либо представителя организации, имеющего право действовать от имени организации без доверенности). Для этого:

- авторизуйтесь на Портале Госуслуг под учетной записью физического лица и нажмите кнопку «Показать все личные данные» на вкладке «Персональная информация». Следует учитывать, что для создания учетной записи организации необходимо предварительное наличие средства УКЭП юридического лица.
- получите средства УКЭП, обратившись в один из аккредитованных Минцифра России УЦ, перечень которых размещен по ссылкам https://e-trust.gosuslugi.ru/#/portal/accreditation/accreditedcalist или https://digital.gov.ru/ru/activity/govservices/certification_authority.

2. Порядок получения СКЗИ

2.1 Текущим пользователям ФГИС ЦС, которые ранее уже приобрели СКЗИ «Jinn Client» и «Континент TLS-клиент» 1.2, необходимо обратиться по адресу электронной почты производителя СКЗИ order@securitycode.ru для получения лицензионного ключа опционального ПО «eXtended Container». В теме письма обязательно указать «ГГЭ 2012», в теле письма должен быть указан номер лицензии купленного СКЗИ «Jinn Client», а во вложении – скан этой лицензии.

2.2 Информация для новых пользователей о способах приобретения и получения СКЗИ размещена на сайте производителя:
https://www.securitycode.ru/where_to_buy/price-list/?login=yes.
Данную информацию также можно получить написав электронное письмо по адресу buy@securitycode.ru.

2.3 Рекомендуется пройти регистрацию на сайте поставщика СКЗИ, расположенному по адресу https://skzi.infosec.ru/, заполнив все регистрационные данные. По результатам регистрации для пользователя создается «Личный кабинет», в котором доступна возможность просмотра уведомлений о текущем статусе заявки.

3. Требования к АРМ пользователя

3.1 Минимальные системные требования к АРМ пользователя ФГИС ЦС указаны в Таблице 1.

Таблица 1 – Минимальные системные требования к АРМ

Параметр	Значение
Операционная система **Внимание!** Должны быть установлены все обновления системы	Windows 10 (кроме выпуска Home Edition); Windows 8.1; Windows 7 SP1 (кроме выпусков Starter и Home Edition)
Процессор, Оперативная память	В соответствии с требованиями ОС, установленной на компьютер
Жесткий диск (свободное место)	500 МБ

Оптический привод	Привод DVD/CD-ROM
Дополнительное ПО	Веб-браузер: • Яндекс.Браузер 22.3 и выше (для Windows 7, 8.1,10); • Google Chrome 48 или выше (для Windows 7, 8.1,10); • Mozilla Firefox 46 или выше (для Windows 7, 8.1,10)

3.2 Поддерживается как 32-битная, так и 64-битная архитектуры ОС.

3.3 Допускается применение любого официального пакета обновлений ОС.

3.4 Поддерживаются следующие носители ключевой информации сертификата пользователя:

- USB-флэш-накопители;
- USB-ключи – Рутокен S (версия 2.0 и 3.0), Рутокен 0, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java);
- смарт-карты – JaCarta ГОСТ, eToken PRO (Java).

4. Подготовка АРМ пользователя к установке СКЗИ

4.1 В случае если пользователю необходимо использовать СКЗИ «КриптоПро CSP» для работы с другими информационными системами, то оно должно быть установлено на АРМ пользователя первоочередно. Для корректного взаимодействия СКЗИ «КриптоПро CSP» и ПО, требуемого для подключения к ФГИС ЦС, рекомендуется использовать «КриптоПро CSP» версии 4.0.9969. Подробнее о входе в личный кабинет ФГИС ЦС с использованием ПО «КриптоПро CSP» описано в пункте 12 и 13 данного руководства.

4.2 Перед настройкой АРМ пользователя для подключения к личному кабинету ФГИС ЦС требуется выполнить следующие проверки:

4.2.1 Проверьте, что на АРМ пользователя **НЕ** установлено следующее ПО:

- Jinn-Client;
- eXtended Container (или XC);
- Континент TLS клиент 1.2 (в исполнении КС1);
- Код Безопасности CSP;
- Jinn Sign Extension Provider.

Для просмотра перечня ПО установленного на АРМ, перейдите в меню «Пуск», откройте «Панель управления» и откройте панель «Программы и компоненты». Убедитесь, что в появившемся списке отсутствует указанное выше ПО. В случае если на АРМ пользователя установлено какое-либо из перечисленного выше ПО, то в панели «Программы и компоненты» выберите его нажатием левой кнопкой мыши и нажмите «Удалить». Далее следуйте указаниям мастера по удалению ПО. По требованию ОС перезапускайте АРМ.

4.2.2 Проверьте наличие на АРМ директории C:\Program Files\Security Code\CSP. Если она существует, запустите находящийся в ней деинсталлятор криптопровайдера «Код Безопасности CSP» – файл csp_uninst.exe. Следуйте указаниям мастера удаления ПО. По требованию перезапустите АРМ.

4.2.3 Запустите редактор реестра командой «regedit» от имени Администратора и удалите подразделы «Security Code» в ветках реестра: *Компьютер\HKEY_CURRENT_USER\SOFTWARE\Security Code*
Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Security Code.

4.2.4 Далее скачайте архив утилит и запустите файл Step5.cmd с правами администратора (правой кнопкой мыши по файлу – запустить от имени администратора (Рис. 1).

Примечание *– архив утилит размещается в личном кабинете пользователя на сайте поставщика СКЗИ по адресу https://skzi.infosec.ru/ в разделе «Техническая поддержка».*

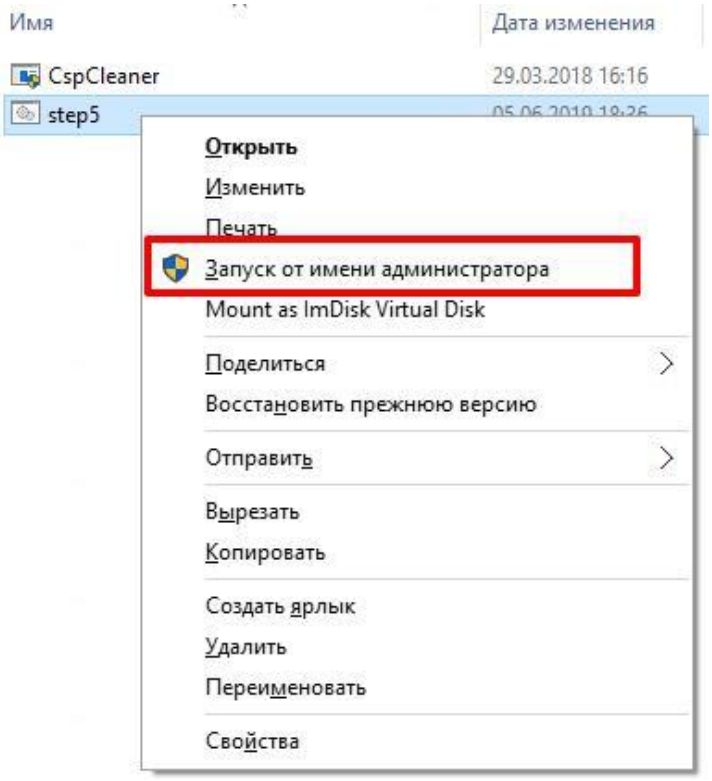


Рис. 1 – Запуск утилиты от имени администратора

4.2.5 Разрешите перезапуск АРМ после выполнения скрипта – нажмите Y, затем любую клавишу для завершения выполнения (Рис. 2).

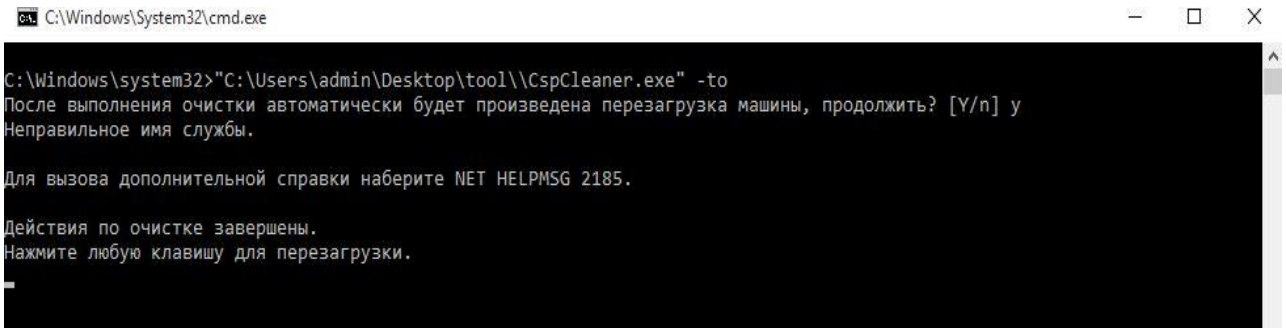


Рис. 2 – Завершение выполнения файла Step5.cmd

4.2.6 Проверьте, создана ли на АРМ директория C:\Program Files\Security Code. Если создана, то удалите ее.

4.2.7 После выполнения вышеперечисленных действий, перейдите к следующему разделу.

5. Установка сертификатов в локальное хранилище АРМ

5.1 Скачайте сертификат сервера «Континент TLS-Сервер», корневой сертификат УЦ Казначейства России и корневой сертификат Минцифры России. Для этого перейдите в раздел База знаний/Обучающие материалы в открытой части портала ФГИС ЦС и скачайте сертификаты:

- Сертификат сервера «Континент TLS-Сервер» (по ГОСТ Р 34.10-2012)» (прямая ссылка https://fgiscs.minstroyrf.ru/api/values/GetFileContent/76ae341b-59aa-4572-b7a6-d58403b44ccc);

- Сертификат Удостоверяющего Центра Казначейства России (по ГОСТ Р 34.10-2012) (прямая ссылка https://fgiscs.minstroyrf.ru/api/values/GetFileContent/25c6787e-931c-420c-a6cd-381498f6a4ce);
- Сертификат Минцифра России (прямая ссылка https://roskazna.gov.ru/upload/iblock/f5e/Kornevoy-sertifikat-GUTS-2022.CER).

5.2 Откройте сертификат Минцифра России. Нажмите кнопку «Установить сертификат» (Рис. 3).

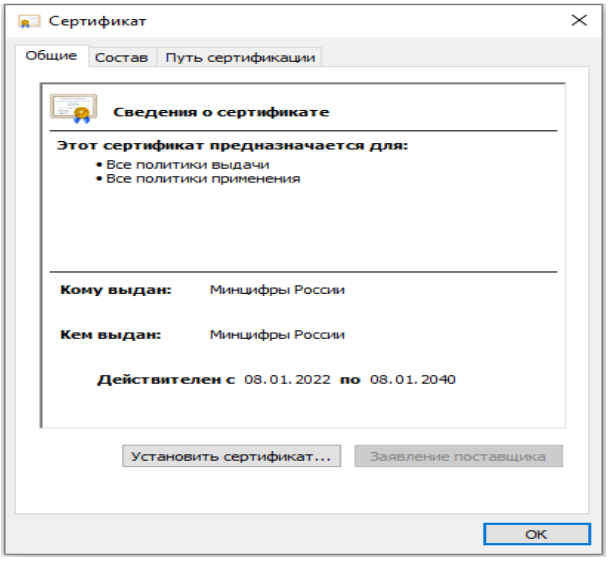


Рис. 3 – Сертификат Минцифра России

5.3 В открывшемся окне «Мастер импорта сертификатов» выберите хранилище «Локальный компьютер», нажмите кнопку «Далее» (Рис. 4).

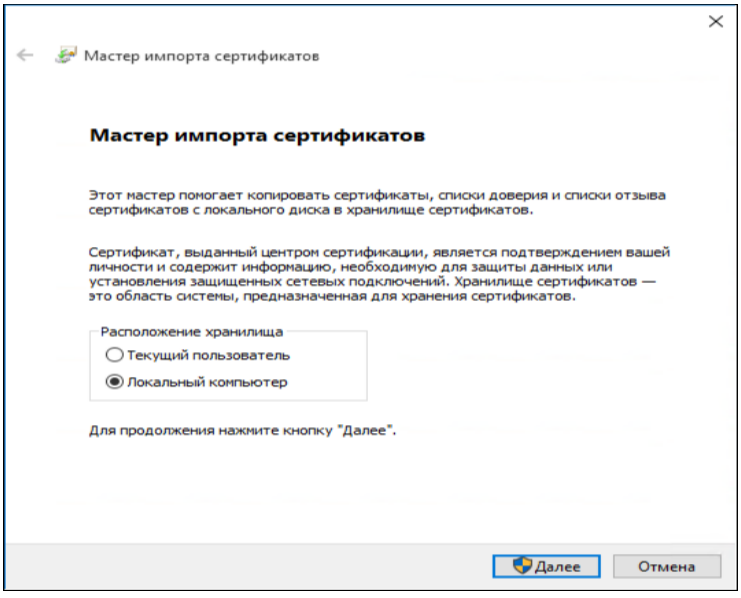


Рис. 4 – Мастер импорта сертификатов

5.4 Выберите параметр «Поместить все сертификаты в следующее хранилище», нажмите «Обзор» (Рис.5). Выберите в качестве хранилища сертификатов «Доверенные корневые центры сертификации». Нажмите «ОК».

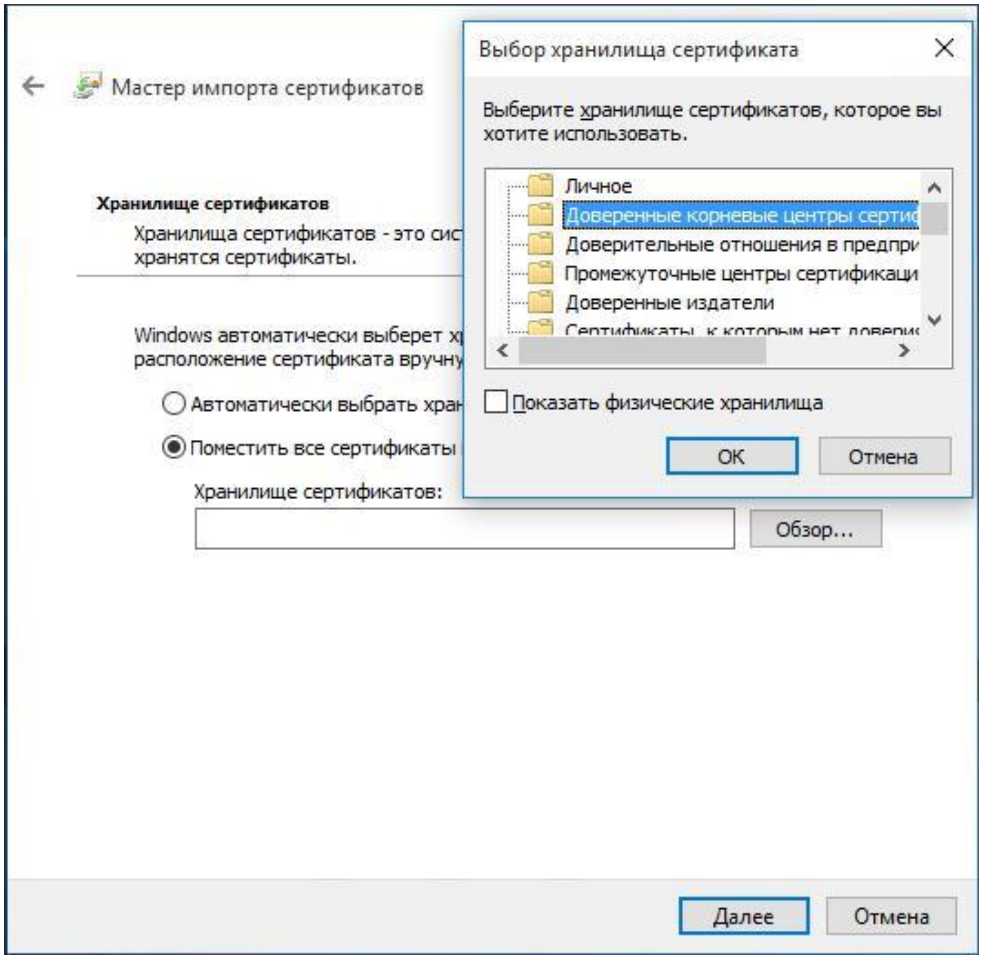


Рис. 5 – Выбор хранилища сертификата Минцифра России

5.5 В окне мастера импорта сертификатов нажмите «Далее». На последнем шаге установки сертификата нажмите «Готово». При появлении предупреждения системы безопасности нажмите «ДА». По окончанию установки сертификата появится информационное сообщение «Импорт сертификата успешно выполнен». Нажмите «ОК» (Рис. 6).

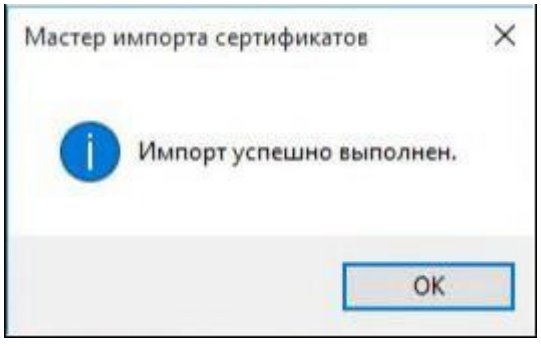


Рис. 6 – Завершение установки сертификата

5.6 Таким же образом необходимо установить сертификат Удостоверяющего центра Казначейства России в «Промежуточные центры сертификации».

Для этого необходимо открыть сертификат УЦ Казначейства России, нажать кнопку «Установить сертификат». В открывшемся окне «Мастер импорта сертификатов» выберите хранилище «Локальный компьютер», нажмите кнопку «Далее». Выберите параметр «Поместить все сертификаты в следующее хранилище», нажмите «Обзор». Выберите в качестве хранилища сертификатов «Промежуточные центры сертификации». Нажмите «ОК» (Рис. 7).

В окне мастера импорта сертификатов нажмите «Далее». На последнем шаге установки сертификата нажмите «Готово». При появлении предупреждения системы безопасности нажмите «ДА». По окончанию установки сертификата появится информационное сообщение «Импорт сертификата успешно выполнен». Нажмите «ОК».

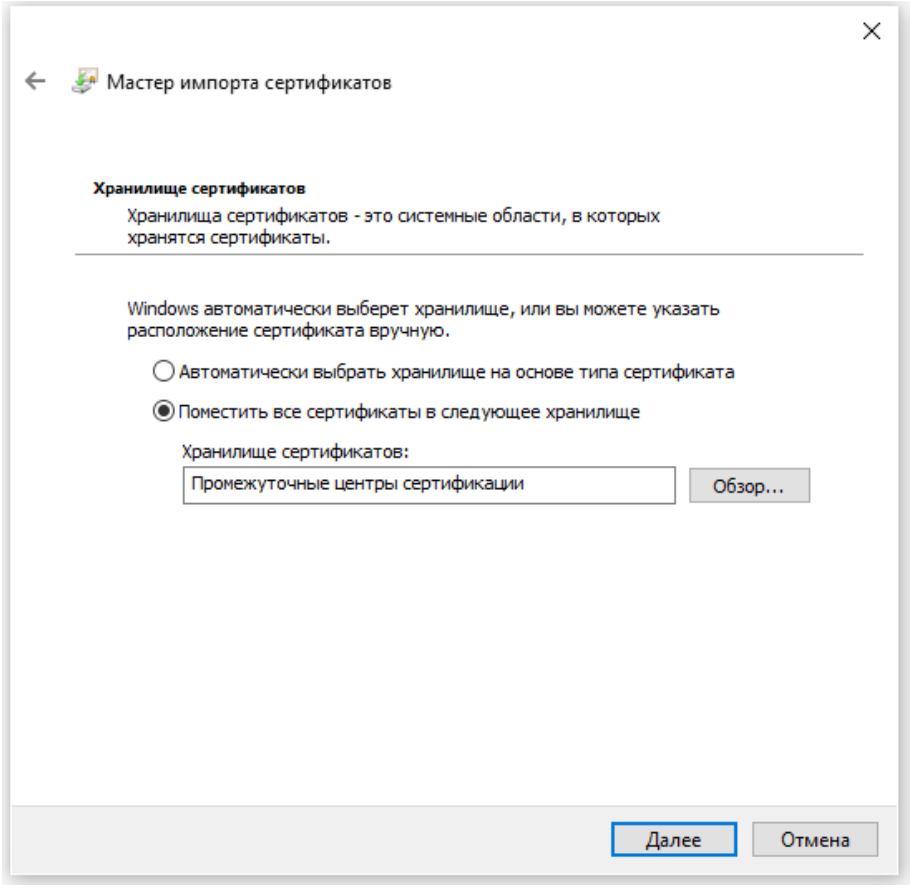


Рис. 7 – Выбор хранилища сертификата УЦ Казначейства России

6. Установка СКЗИ при помощи «Единого инсталлятора»

6.1 Единый инсталлятор выполняет установку следующего ПО:

- Jinn-Client;
- eXtended Container (XC);
- СКЗИ «Континент TLS-клиент». Версия 2;
- Код Безопасности CSP;
- Единый клиент JaCarta, eToken PKI Client 5.1 SP1, драйверы Рутокен, JC Sigh Plugins Bundle.

Примечание *– дистрибутив «Единого инсталлятора» размещается в личном кабинете пользователя на сайте поставщика СКЗИ по адресу* https://skzi.infosec.ru/ *в разделе «Техническая поддержка».*

6.2 Для установки ПО выполните следующие действия:

6.2.1 Перейдите в директорию, в которой расположен исполняемый файл «Единого инсталлятора» и запустите «Единый инсталлятор.exe» от имени администратора (Рис. 8).

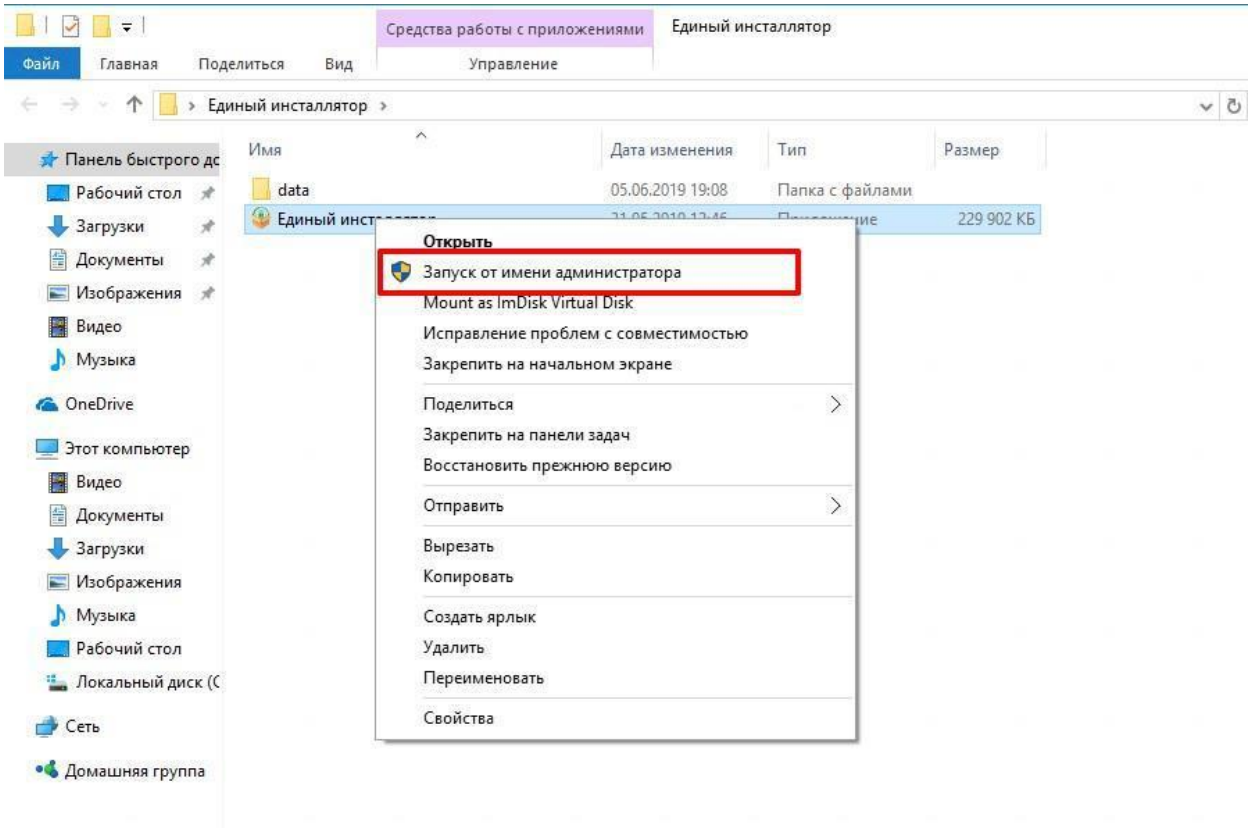


Рис. 8 – Запуск «Единого инсталлятора»

6.2.2 В открывшемся окне введите лицензионный ключ для «Jinn-Client» в верхней строке и лицензионный ключ для расширенной поддержки ключевых контейнеров (eXtended Container) в нижней строке (Рис. 9).

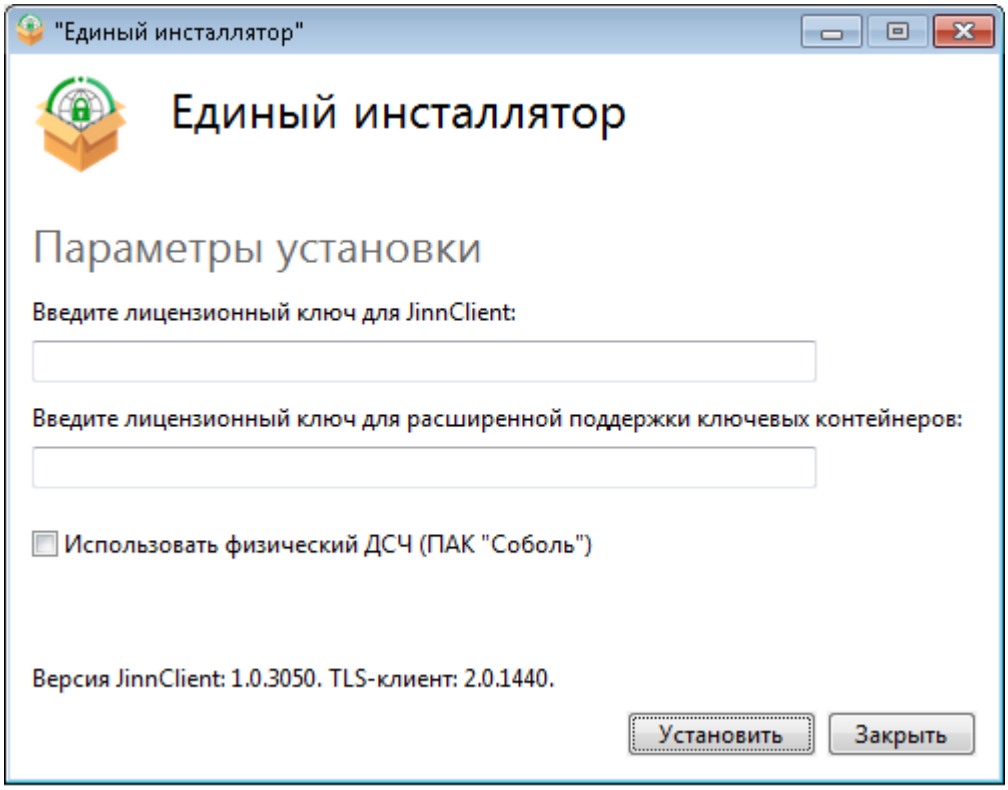


Рис. 9 – Окно установки

6.2.3 Нажмите кнопку «Установить».

6.2.4 Дождитесь окончания установки ПО «Единого инсталлятора».

6.2.5 После завершения установки нажмите кнопку «Перезагрузить» и выполните перезагрузку компьютера.

7. Регистрация ПО «Континент TLS-клиент» версия 2

7.1 Запустите ПО «Континент TLS-клиент», нажав на соответствующий ярлык на рабочем столе: 

.

7.2 Во время первого запуска ПО «Континент TLS-клиент» криптопровайдер «Код Безопасности CSP» потребует набрать вектор энтропии. Нажимайте в центр всплывающих «мишеней» пока процесс не завершится (Рис. 10). Обратите внимание, что набор вектора энтропии невозможен при подключении к АРМ пользователя по протоколу RDP.

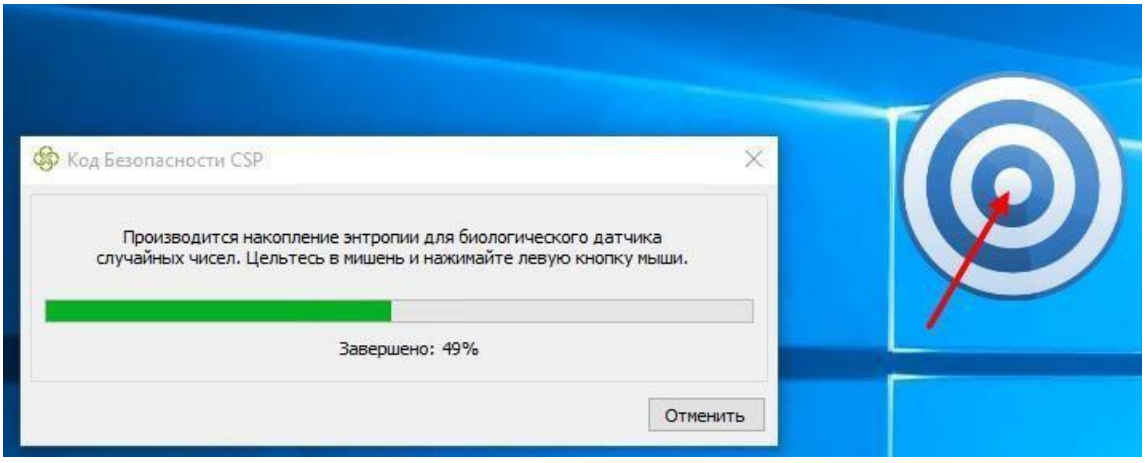


Рис. 10 – Накопление энтропии

7.3 После создания вектора энтропии появится диалоговое окно ПО «Континент TLS-клиент» с надписью: «Вы используете незарегистрированную версию программы». При нажатии на кнопку «Продолжить без регистрации» пользователю будет предоставлен демонстрационный период эксплуатации ПО продолжительностью 14 рабочих дней. По истечении данного срока работа ПО «Континент TLS-клиент» будет приостановлена. Для прохождения регистрации в диалоговом окне нажмите кнопку «Зарегистрировать» (Рис. 11).

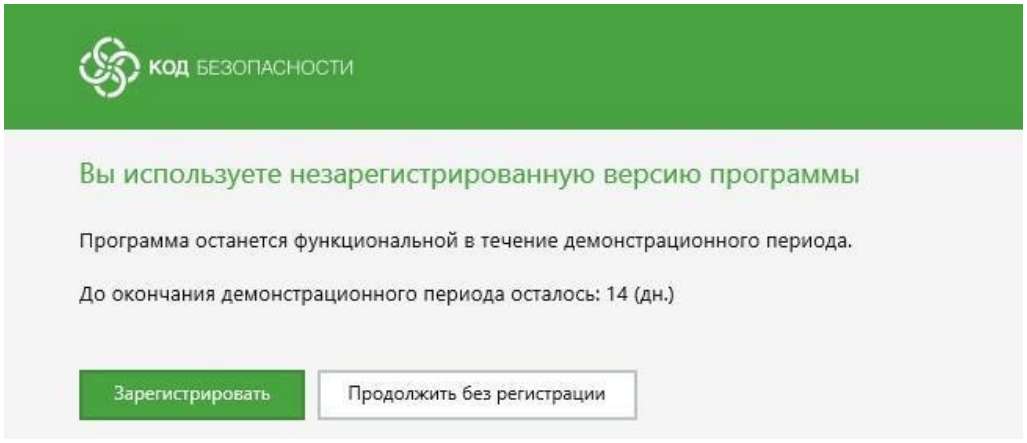


Рис. 11 – Запрос регистрации ПО «Континент TLS-клиент»

7.4 Заполните обязательные поля для регистрации (Рис. 12):

- Фамилия;
- Имя;
- Электронная почта;
- Адрес сервера регистрации оставьте по умолчанию: **registration.securitycode.ru**
- В поле класс защиты выберите значение «**КС1**».

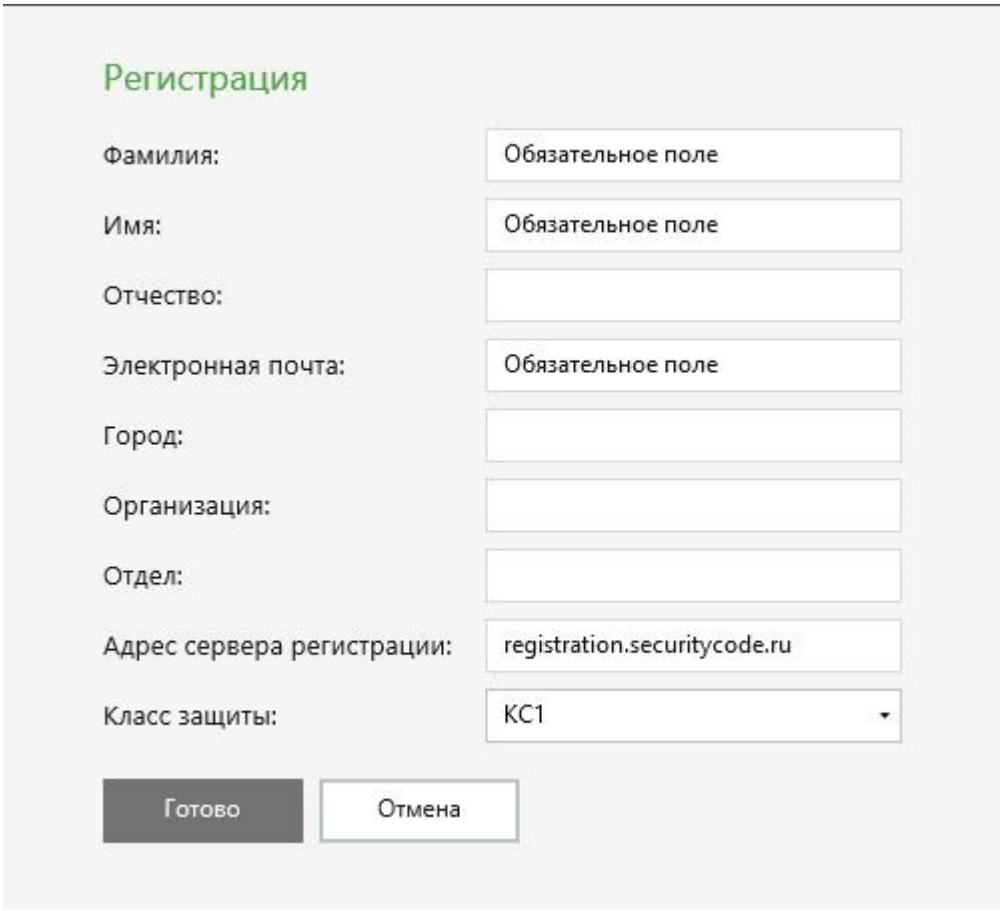


Рис. 12 – Поля для регистрации ПО «Континент TLS-клиент»

7.5 После заполнения обязательных полей нажмите «Готово». В правом нижнем углу рабочего стола появится окно, сообщающее об успешной регистрации (Рис. 13). На адрес электронной почты, которую Вы указали, придет письмо об успешной регистрации.

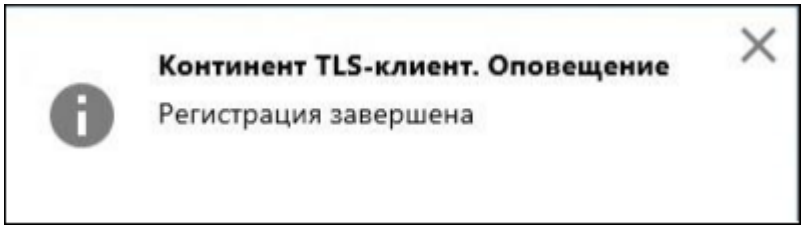


Рис. 13 – Оповещение об успешной регистрации ПО «Континент TLS-клиент»

8. Настройка ПО «Континент TLS-клиент» версия 2

8.1 Сохраните в любую удобную директорию файл конфигурации «Континент-клиент: fgiscs_conf.JSON.

Примечание *– файл конфигурации ПО «Континент TLS-клиент» размещается в личном кабинете пользователя на сайте поставщика СКЗИ по адресу https://skzi.infosec.ru/ в разделе «Техническая поддержка».*

8.2 Откройте меню настроек ПО «Континент TLS-клиент» (Рис. 14).

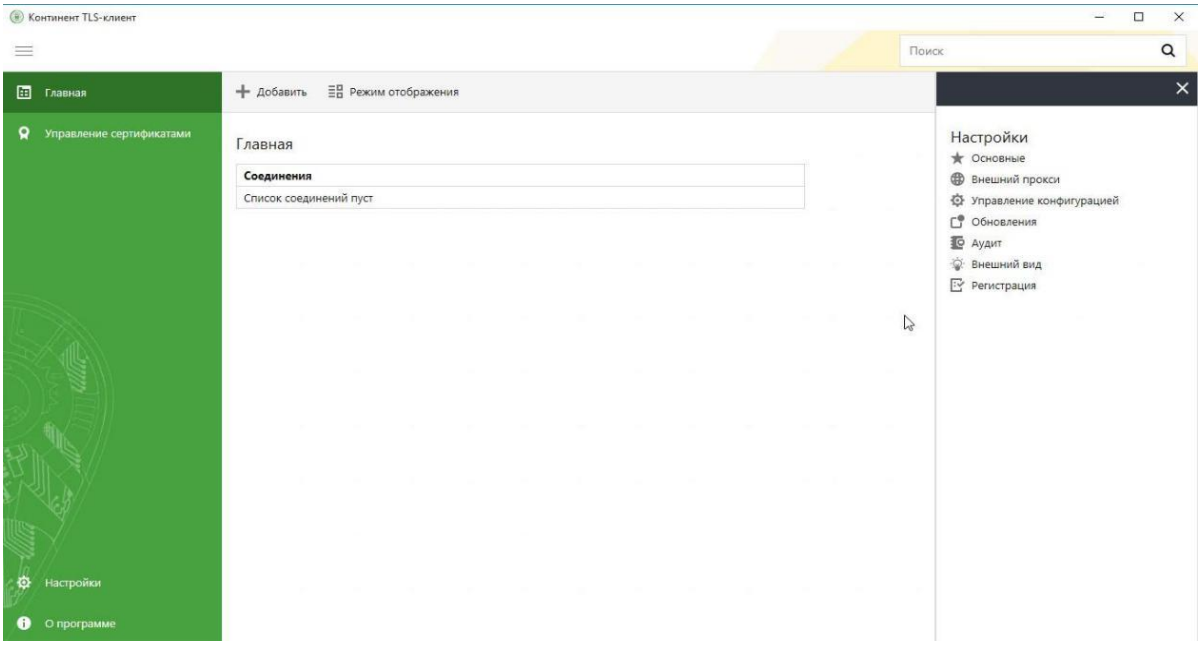


Рис. 14 – Меню ПО «Континент TLS-клиент»

8.3 Перейдите в раздел «Управление конфигурацией», затем нажмите «Импортировать конфигурацию» и выберите конфигурационный файл, сохраненный ранее (Рис. 15). Нажмите «Открыть».

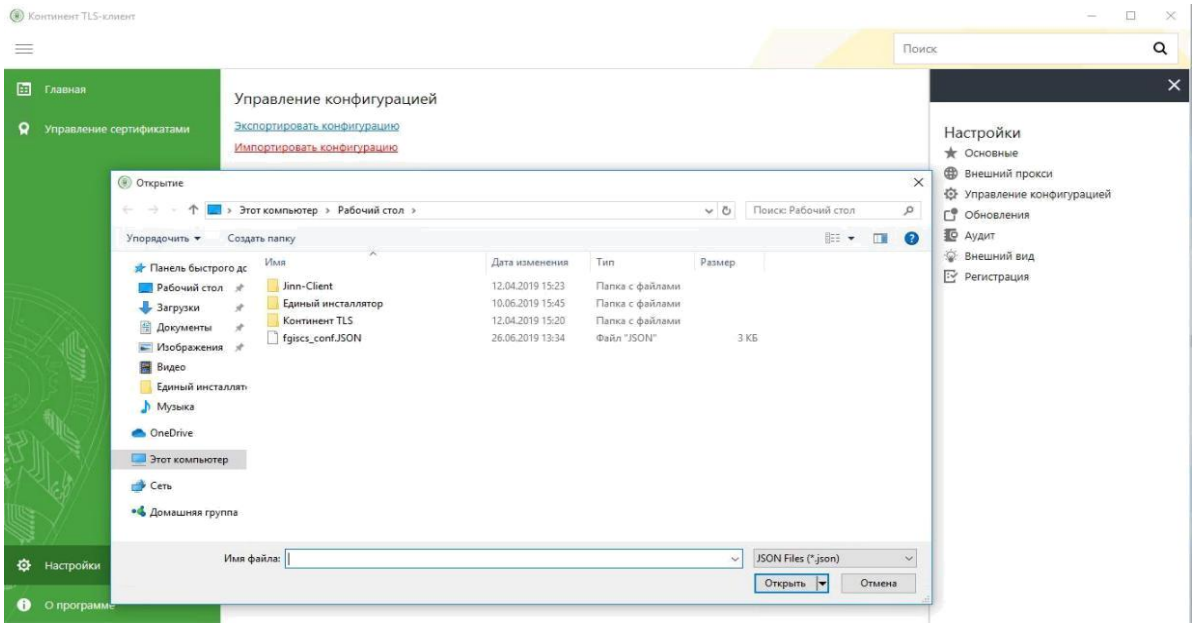


Рис. 15 – Импорт конфигурационного файла

8.4 При успешном импорте появится информационное сообщение «Импорт конфигурации завершен». Нажмите «ОК» (Рис. 16).

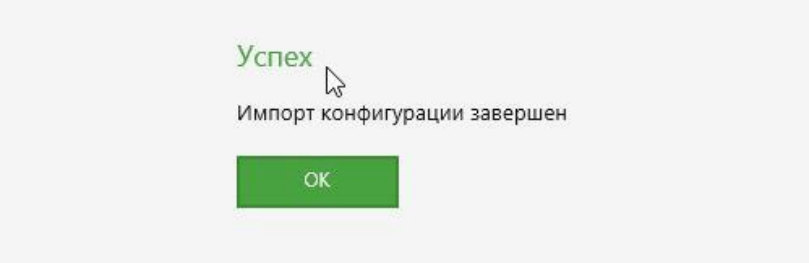


Рис. 16 – Результат импорта конфигурационного файла

8.5 Перейдите в раздел настроек «Внешний прокси». Отметьте чекбокс «Настраивать автоматически».

8.6 В случае если в организации используется прокси-сервер, после сохранения настроек его параметры определятся автоматически.

8.7 Если прокси-сервер не используется, после сохранения окно параметров останется пустым.

8.8 Окно настроек внешнего прокси-сервера выглядит следующим образом (Рис. 17).

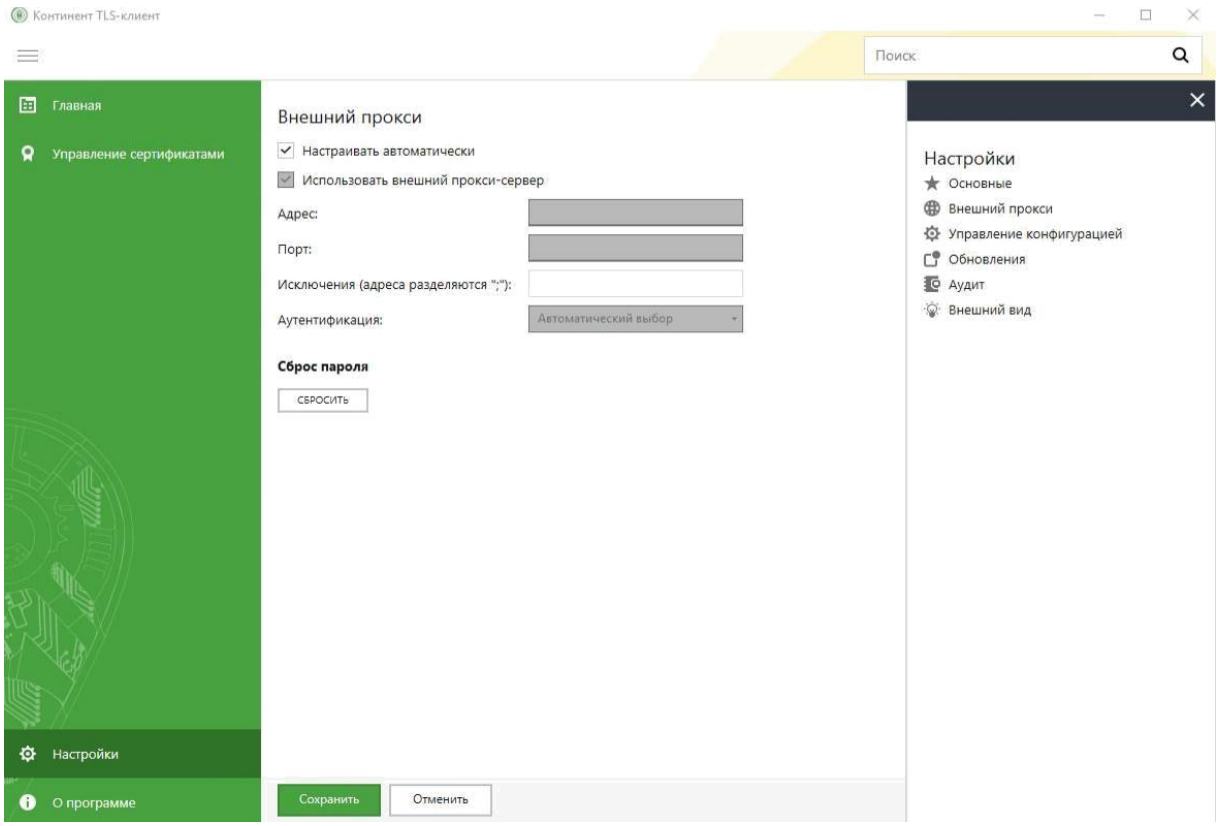


Рис. 17 – Окно настроек внешнего прокси-сервера

8.9 Перейдите в раздел «Управление сертификатами» на вкладку «Серверные сертификаты» и нажмите на кнопку «Импортировать». В открывшемся окне перейдите в директорию, в которую был скопирован серверный сертификат, и выберете его (Рис. 18).

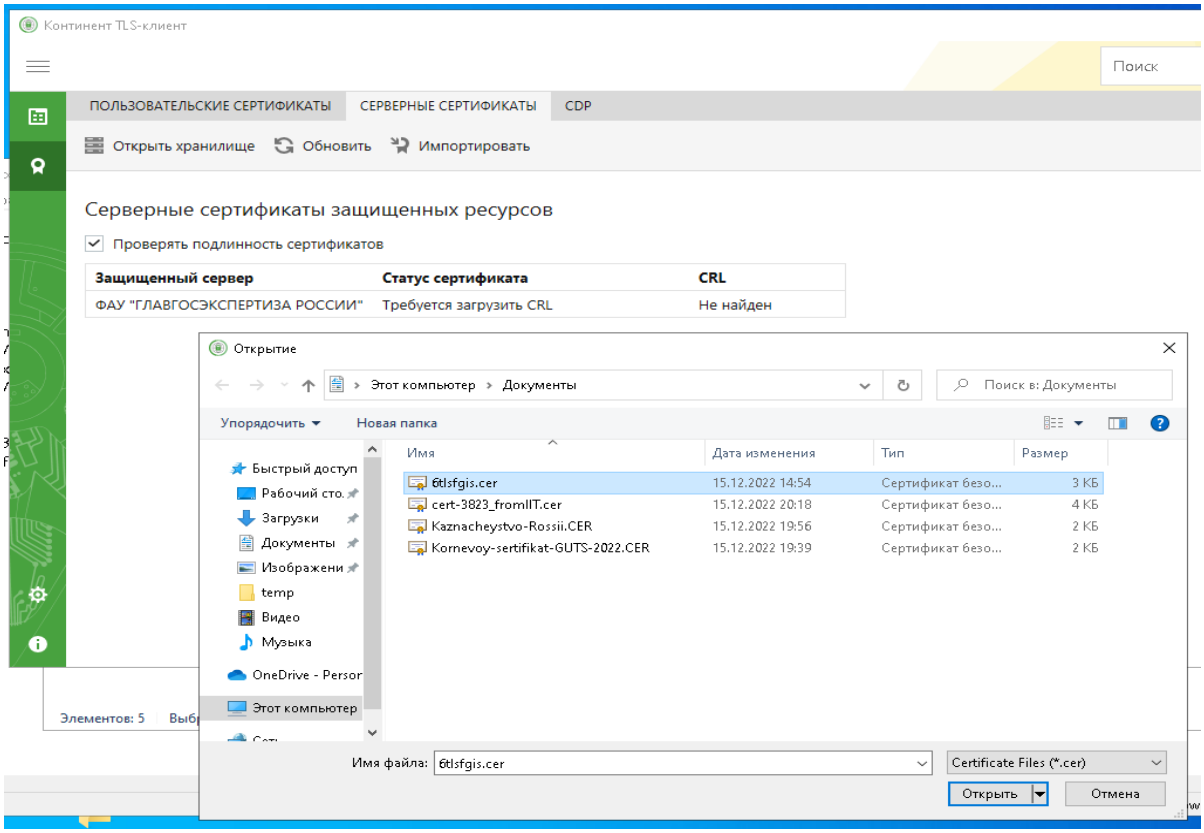


Рис. 18 – Выбор сертификата сервера

8.10 После выбора сертификата сервера вкладка настроек серверных сертификатов примет следующий вид (Рис. 19).

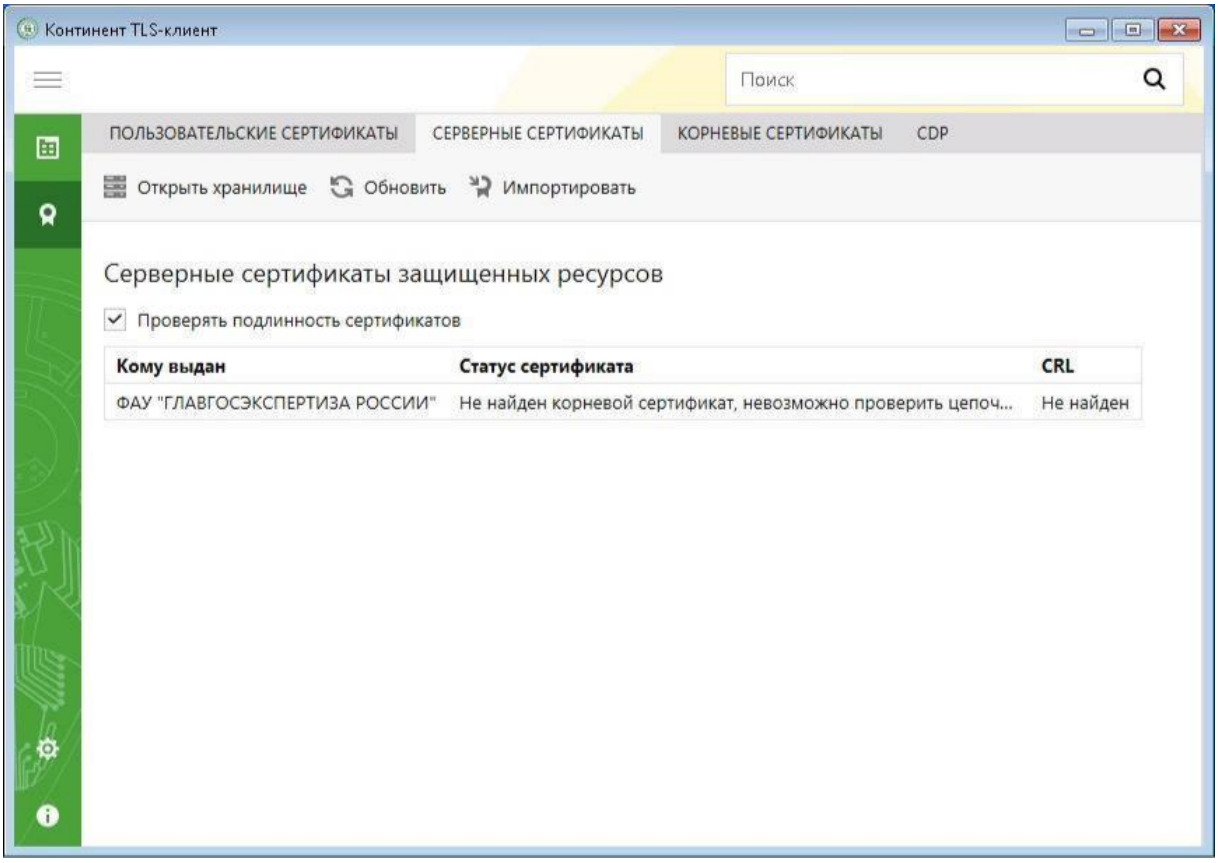


Рис. 19 – Вкладка настроек «серверные сертификаты»

8.11 Далее необходимо перейти на вкладку «Корневые сертификаты» и импортировать новые корневые сертификаты Минцифра России и УЦ Казначейства России. Для этого необходимо нажать кнопку «Импортировать», в открывшемся окне перейти в директорию, в которую были скопированы сертификаты на первом шаге данной инструкции, и выбрать новый корневой сертификат Минцифра России, а затем и УЦ Казначейства России.

В случае если вкладки «Корневые сертификаты» нет, то корневые сертификаты нужно загрузить вручную. Для этого произведите следующие действия:

Нажимаем правой кнопкой мыши на скачанный сертификат Минцифра России (Рис. 20).

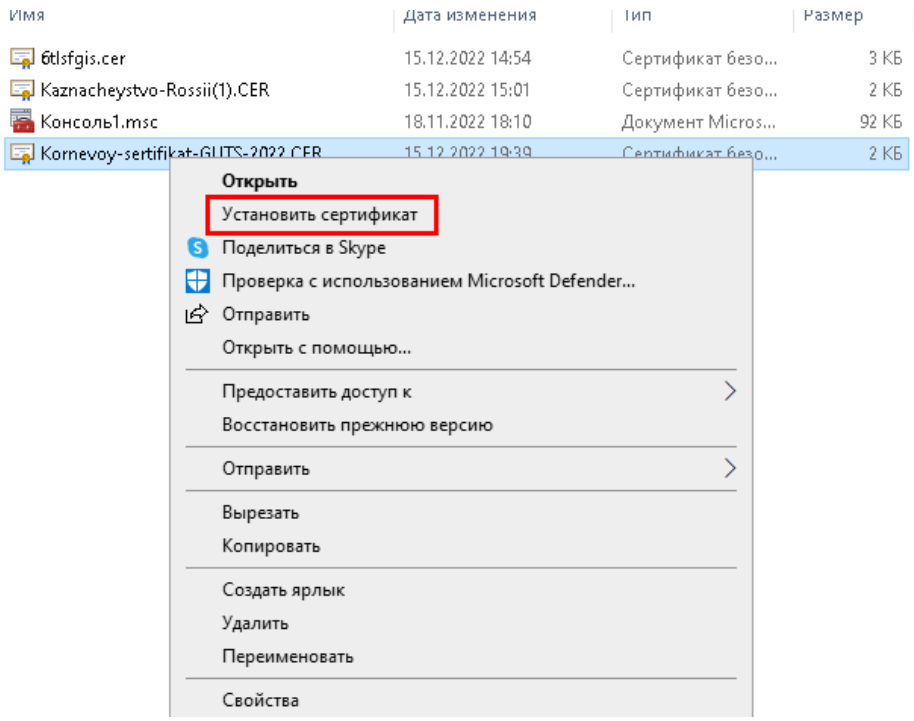


Рис. 20 – Установка корневого сертификата Минцифра России

Далее выбираем куда установить сертификат – Локальный компьютер (Рис. 21).

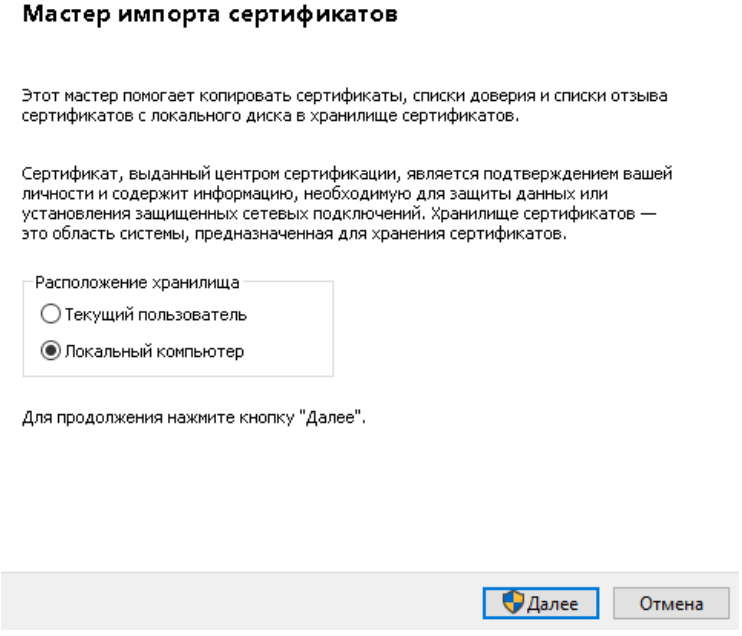


Рис. 21 – Выбор места установки корневого сертификата

Дальше в появившемся окне даем разрешение на внесение изменений нажатием на кнопку «Да» (*для этих действий пользователь должен обладать правами администратора на данном компьютере*).

В следующем окне выбираем хранилище для корневого сертификата: выбираем пункт «Поместить все сертификаты в следующее хранилище» и нажимаем кнопку «Обзор», выбираем строку «Доверенные корневые центры сертификации» и нажимаем ОК (Рис. 22).

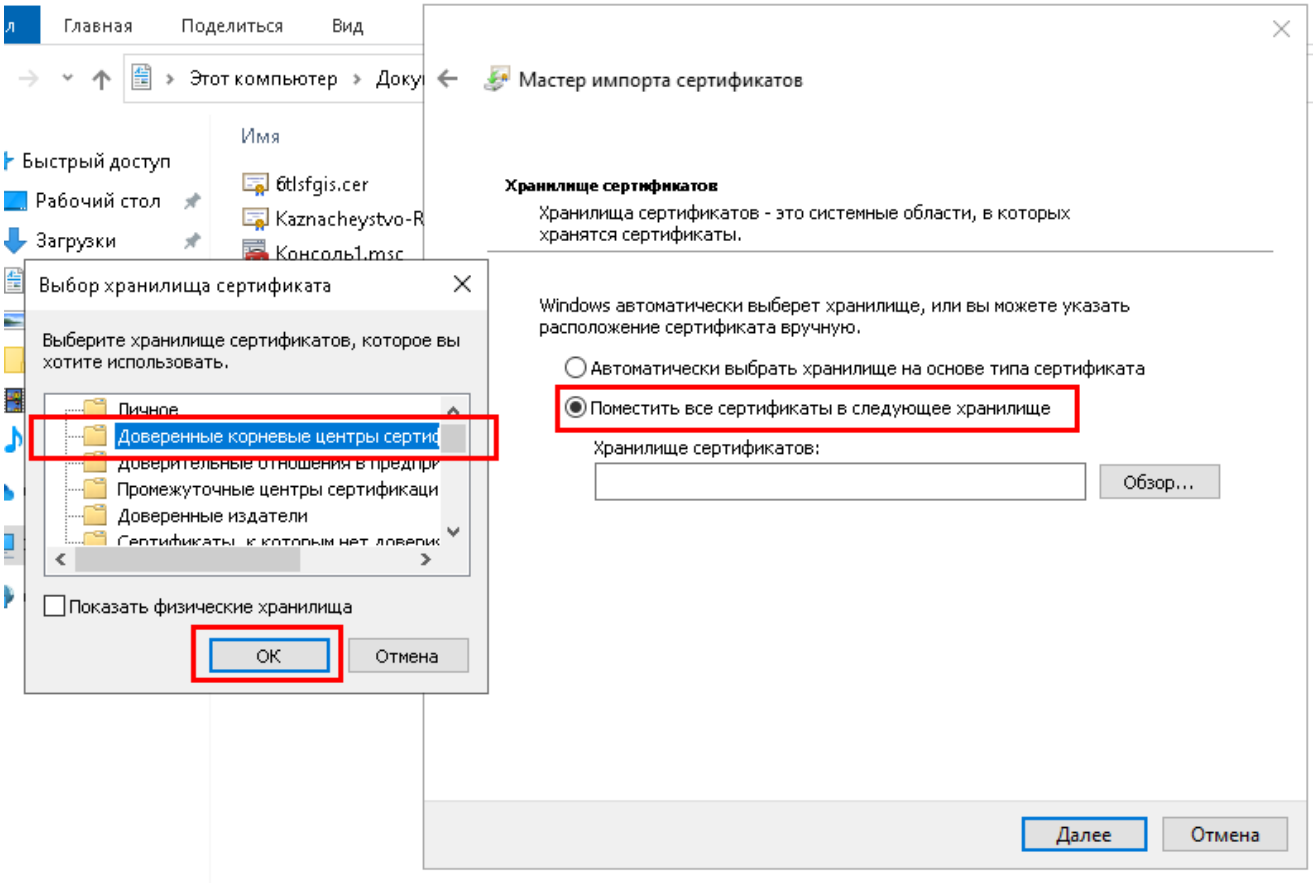


Рис. 22 – Выбор хранилища для корневого сертификата

Подтверждаем кнопкой «Далее» и «Готово». По успешному выполнению появится окно с сообщением «Импорт успешно выполнен».

8.12 Аналогичные действия делаем для установки предварительно скачанного промежуточного сертификата УЦ Казначейства России.

Нажимаем правой кнопкой мыши на сертификат Казначейства России, выбираем «Установить сертификат».

Выбираем «Локальный компьютер», нажимаем «Далее», подтверждаем разрешение на проводимые изменения нажатием кнопки «Да».

Выбираем «Поместить все сертификаты в следующее хранилище», нажимаем «Обзор», выбираем «Промежуточные центры сертификации», нажимаем «ОК». Это единственное отличие от предыдущих действий (Рис. 23).

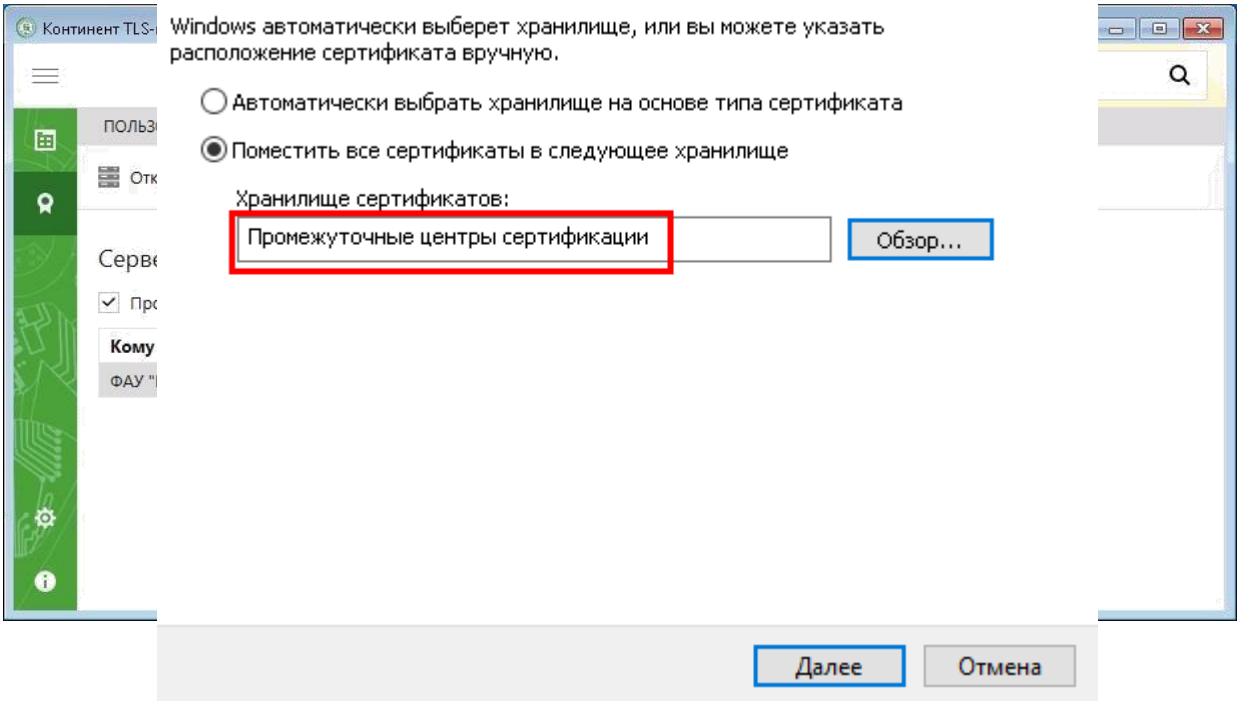


Рис. 23 – Выбор хранилища для промежуточного сертификата

Нажимаем «Далее» и «Готово». Ждем появления окна об успешном импорте.

8.13 После импорта сертификатов перейдите во вкладку «CDP» и нажмите кнопку «Скачать CRL» (Рис. 24). После скачивания статус CRL корневого сертификата изменится на «Действителен».

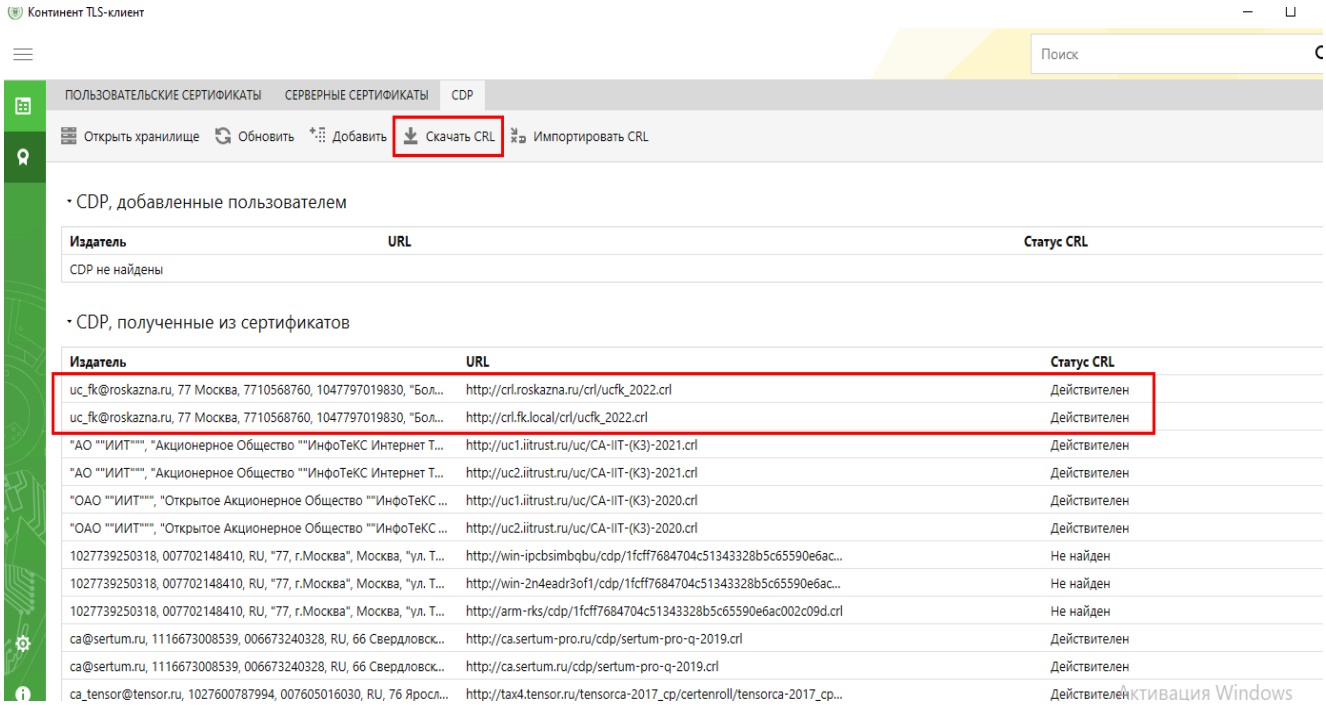


Рис. 24 – Вкладка «CDP»

После скачивания CRL вернитесь во вкладку «Серверные сертификаты». Статус CRL сертификата изменится на «Действителен».

9. Установка сертификата пользователя

9.1 Выполните установку сертификата пользователя при помощи «КриптоПро CSP» по инструкции:

9.2.1 Откройте «КриптоПро CSP» на вкладке «Сервис».

9.2.2 Перейдите в меню «Установить личный сертификат…».

9.2.3 В открывшемся мастере установки личного сертификата нажмите «Обзор» и выберите личный сертификат пользователя. Нажмите «Далее».

9.2.4 На втором шаге отобразятся параметры выбранного сертификата. Нажмите «Далее».

9.2.5 На третьем шаге установите чекбокс «Найти контейнер автоматически», либо нажмите «Обзор» и выберите контейнер закрытого ключа, находящегося на внешнем носителе, вручную. Нажмите «Далее».

9.2.6 На следующем шаге установите чекбокс «Установить сертификат (цепочку сертификатов) в контейнер». Нажмите «Далее».

9.2.7 На этапе завершения работы мастера установки сертификата нажмите «Готово». В случае, если на контейнер закрытого ключа сертификата пользователя установлен пароль, появится окно ввода пароля. Введите пароль, нажмите «ОК».

9.2.8 Перейдите к окну пользовательских сертификатов в «Континент TLS-клиент».

В разделе «Пользовательские сертификаты» нажмите «Обновить» - появится новый сертификат (Рис. 25).

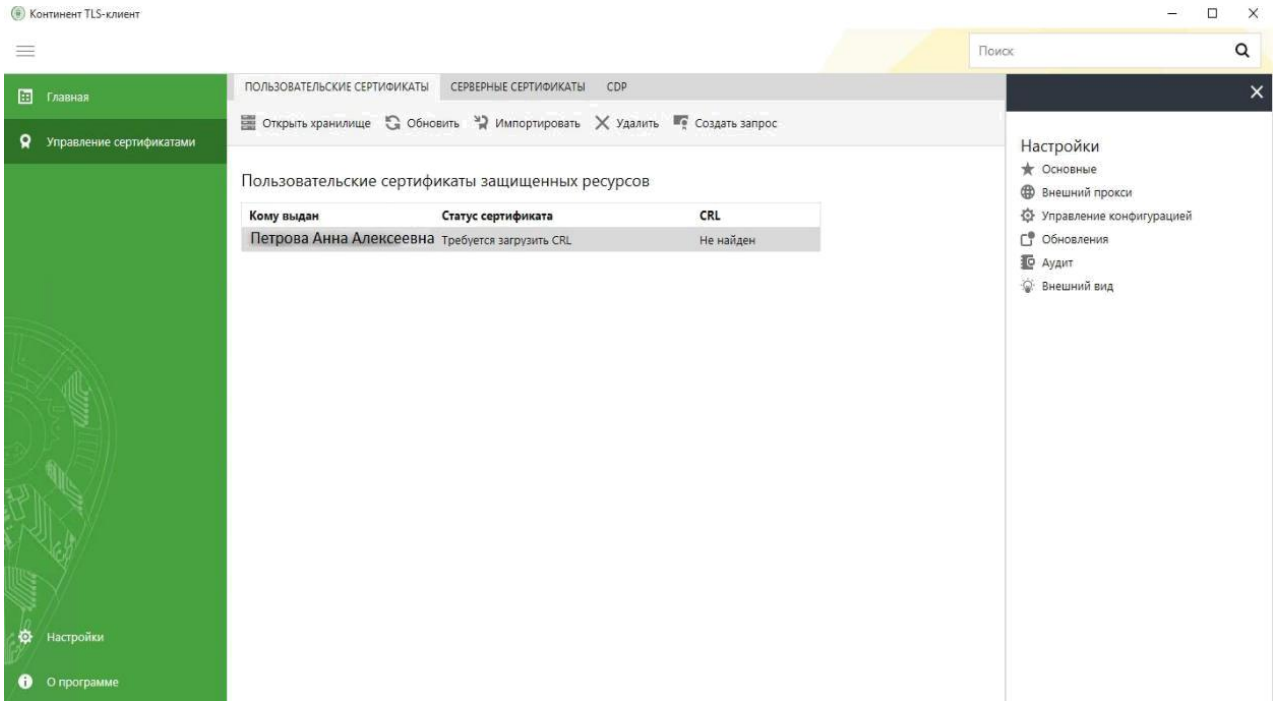


Рис. 25 – Окно пользовательских сертификатов в «Континент TLS-клиент»

9.2.9 Двойным кликом откройте добавленный сертификат пользователя в «Континент TLS-клиент». Перейдите во вкладку «Путь сертификации» и убедитесь, что все сертификаты действительны и установлены в хранилище (Рис. 26). Если цепочка сертификатов издателей сертификата пользователя установлена в хранилище АРМ, то в строке «Состояние сертификата» будет отображен статус «Этот сертификат действителен».

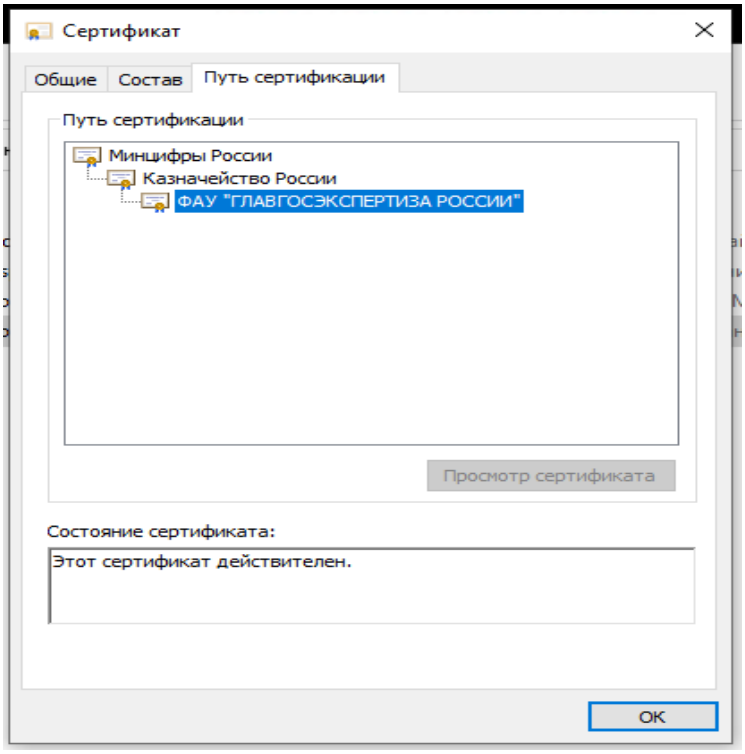


Рис. 26 – Путь сертификации

9.2.10 Если хотя бы один сертификат из цепочки издателей сертификата пользователя не установлен в хранилище АРМ, то в строке «Состояние сертификата» отобразится статус «Невозможно обнаружить поставщика этого сертификата.» или «Нет доверия к этому корневому сертификату центра сертификации, так как он не найден в хранилище доверенных корневых сертификатов центров сертификации.», а сам сертификат будет помечен красным крестиком (Рис. 27). Для корректной работы в личном кабинете ФГИС ЦС установите сертификаты издателей сертификата пользователя в хранилище АРМ.

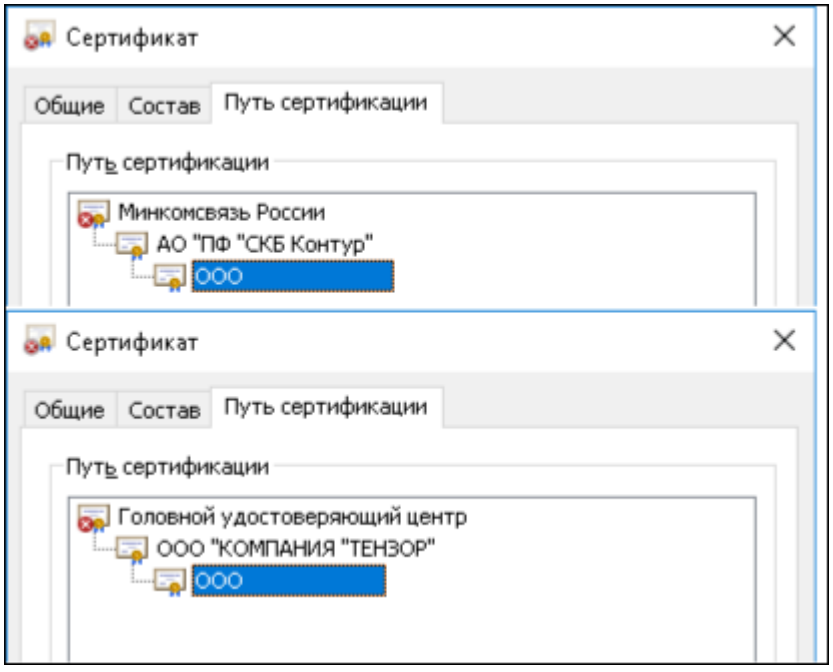


Рис. 27 – Путь сертификации сертификата пользователя

9.2.11 Сертификат издателя сертификата пользователя, как правило, публикуется на официальном сайте Удостоверяющего центра. Необходимо его скачать и установить по аналогии с сертификатом УЦ, выдавшим сертификат сервера ФГИС ЦС. Инструкция по установке сертификатов была описана в Разделе 5. Также, по этой же инструкции установите сертификаты Головного УЦ Минцифра России, которые можно скачать с сайта https://ca.gisca.ru/support/repository/ .

- [ГОСТ 34.10-2012] Корневой сертификат «Минцифры России» от 08.01.2022.

9.2.12 После завершения установки сертификатов УЦ, в настройках «Континент TLS-клиент» перейдите в раздел CDP и нажмите кнопку «Скачать CRL» (Рис. 28).

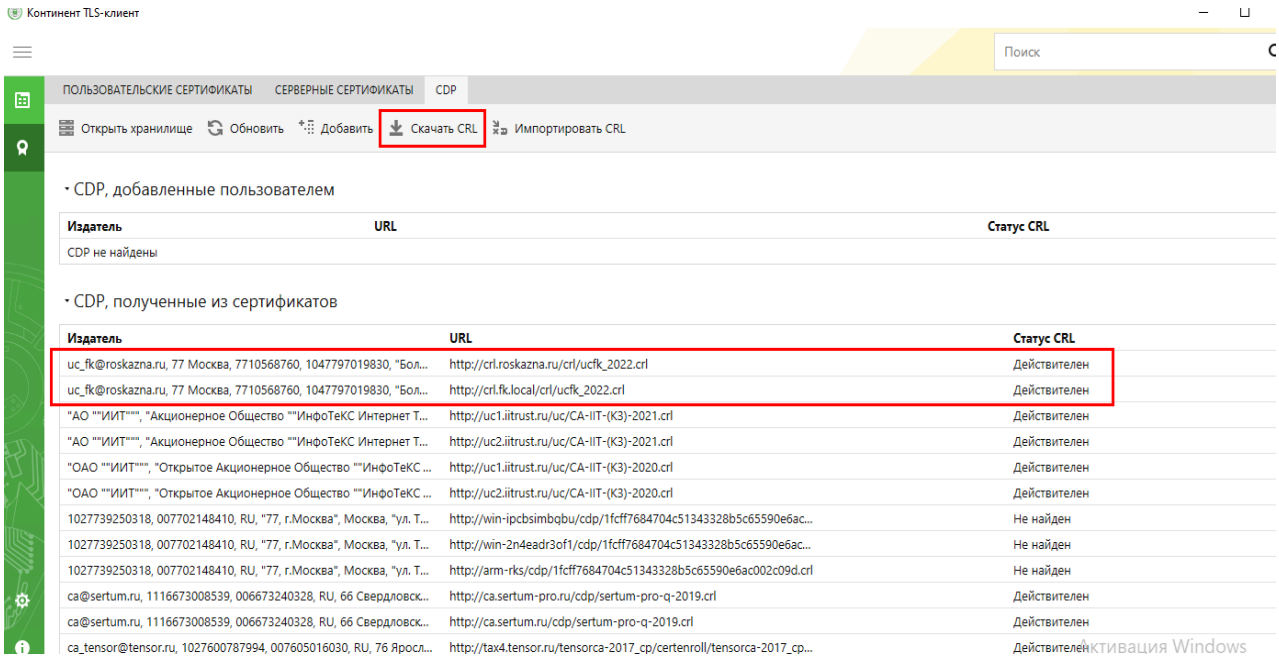


Рис. 28 – Вкладка «CDP»

После скачивания CRL вернитесь во вкладку «Пользовательские сертификаты». Статус CRL сертификата изменится на «Действителен» (Рис. 29).

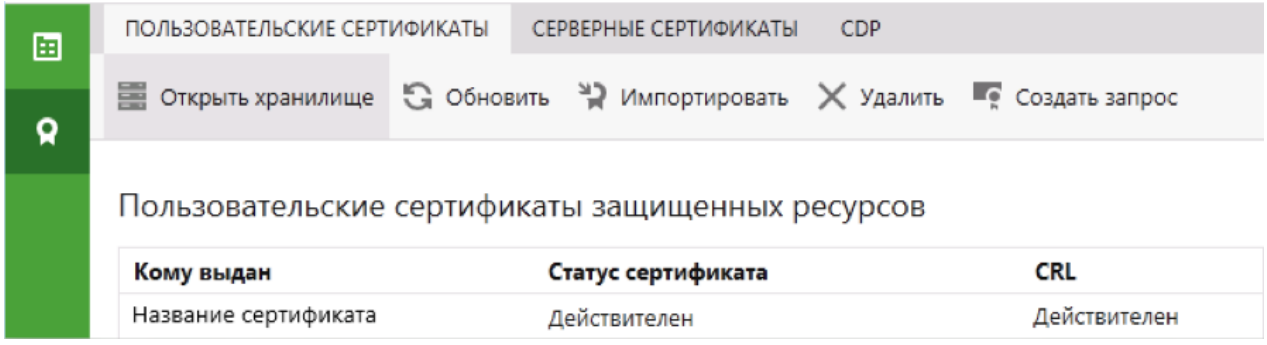


Рис. 29 – Вкладка настроек пользовательских сертификатов

9.2.13 На данном этапе настройка ПО «Континент TLS-клиент» завершена.

9.2.14 Для исключения блокировки ПО «Континент TLS-клиент» антивирусом необходимо добавить исполняемый файл клиента TlsClient.exe (C:\Program Files\Security Code\Continent TLS Client) и всю папку Security Code (C:\Program Files\Security Code) в доверенные программы.

10. Установка Jinn Sign Extension для браузеров Chrome, Mozilla

10.1 Процесс установки плагина Jinn Sign Extension зависит от используемого веб-обозревателя (браузера).

10.2 Если для подключения к личному кабинету ФГИС ЦС предполагается использовать браузер Internet Explorer, то установка плагина не требуется. Пропустите данный раздел и перейдите к Разделу 11.

10.3 Если для подключения к личному кабинету ФГИС ЦС предполагается использовать браузер Google Chrome, то выполните установку плагина по инструкции:

- Скачайте архив с расширением Jinn Sign Extension для браузера Google Chrome.

Примечание *– архив размещается в личном кабинете пользователя на сайте поставщика СКЗИ по адресу https://skzi.infosec.ru/ в разделе «Техническая поддержка».*

- Перейдите в раздел с расширениями Google Chrome - для этого в правом верхнем углу нажмите на значок ⋮, выберите «Дополнительные инструменты», в выпадающем списке выберите «Расширения». Включите режим разработчика соответствующим переключателем в правом верхнем углу окна и нажмите кнопку «Загрузить распакованное расширение» (Рис. 30).

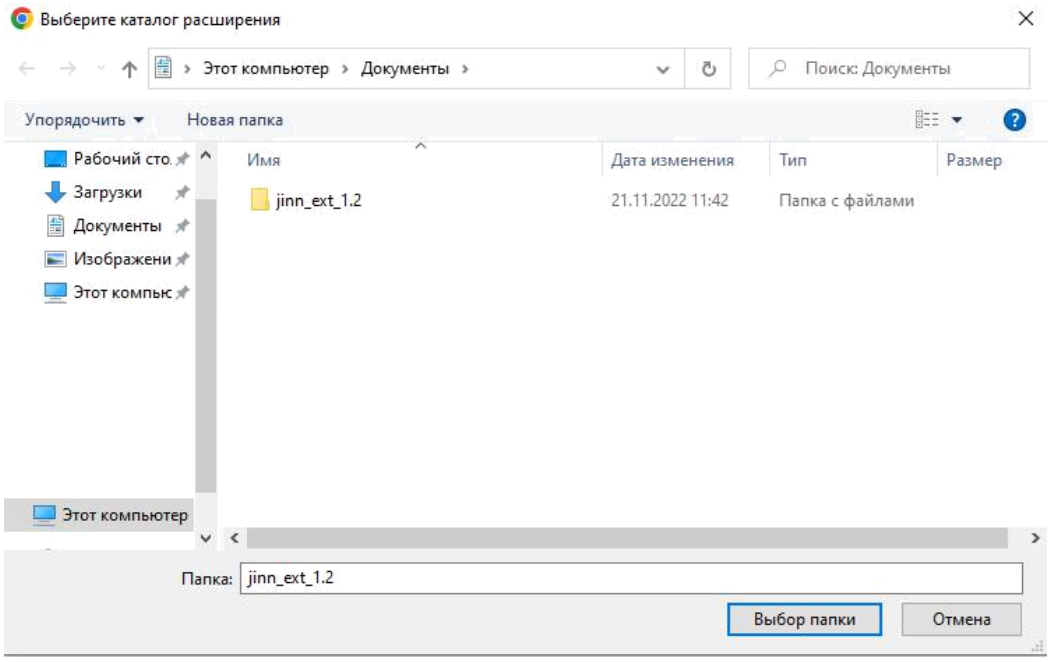


Рис. 30 – Включение режима разработчика

• В появившемся окне выберите папку с расширением для браузера и нажмите кнопку «Выбор папки» (Рис. 31).

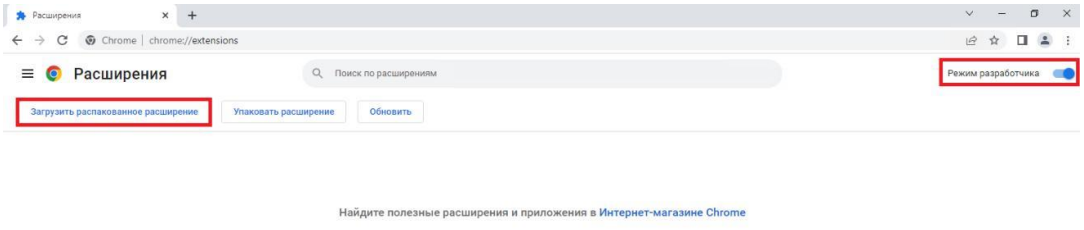


Рис. 31 – Выбор папки с расширением для браузера

10.4 Установка плагина завершается с появлением плагина в списке расширений браузера (Рис. 32).

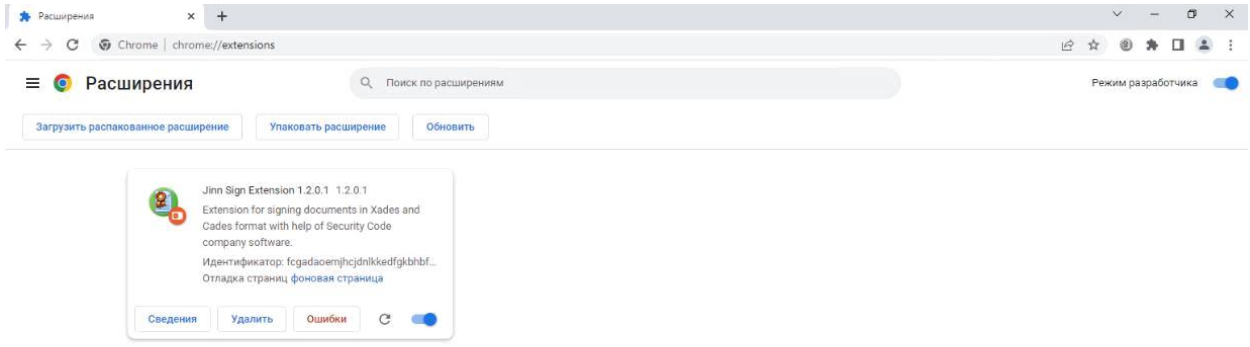


Рис. 32 – Завершение установки плагина «Jinn Sign Extension»

10.5 Убедитесь, что плагин «Jinn Sign Extension» включен. Для этого откройте список всех установленных расширений в браузере, в правом верхнем углу нажмите на значок ⋮, выберите «Дополнительные инструменты», в выпадающем списке выберите «Расширения». В открывшемся представлении найдите «Jinn Sign Extension» и убедитесь, что он включен (Рис. 33).



Рис. 33 – Включение плагина «Jinn Sign Extension»

10.6 Перезапустите браузер Google Chrome.

10.7 Если для подключения к личному кабинету ФГИС ЦС предполагается использовать браузер Mozilla Firefox, то выполните установку плагина по следующей инструкции:

- Откройте интернет-магазин Firefox по ссылке https://addons.mozilla.org/
- Выполните поиск по ключевым словам – Jinn Sign Extension. Среди результатов поиска выберите расширение «Jinn Sign Extension» (Рис. 34).

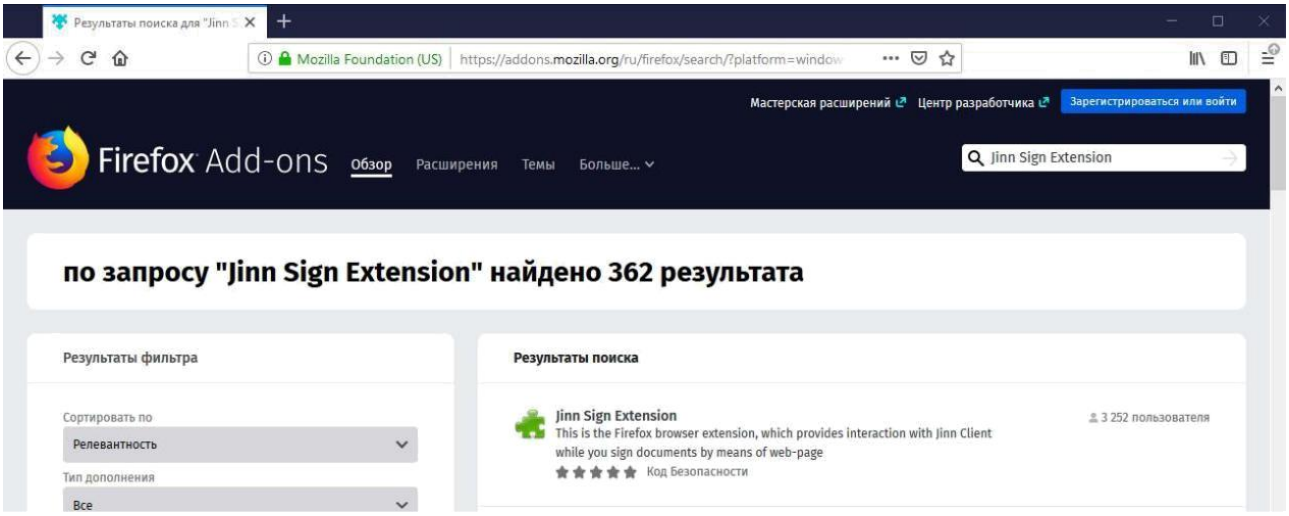


Рис. 34 - Результат поиска расширения Jinn Sign Extension

- Выберите расширение «Jinn Sign Extension» от Кода Безопасности и нажмите кнопку «+ Добавить в Firefox» (Рис. 35).

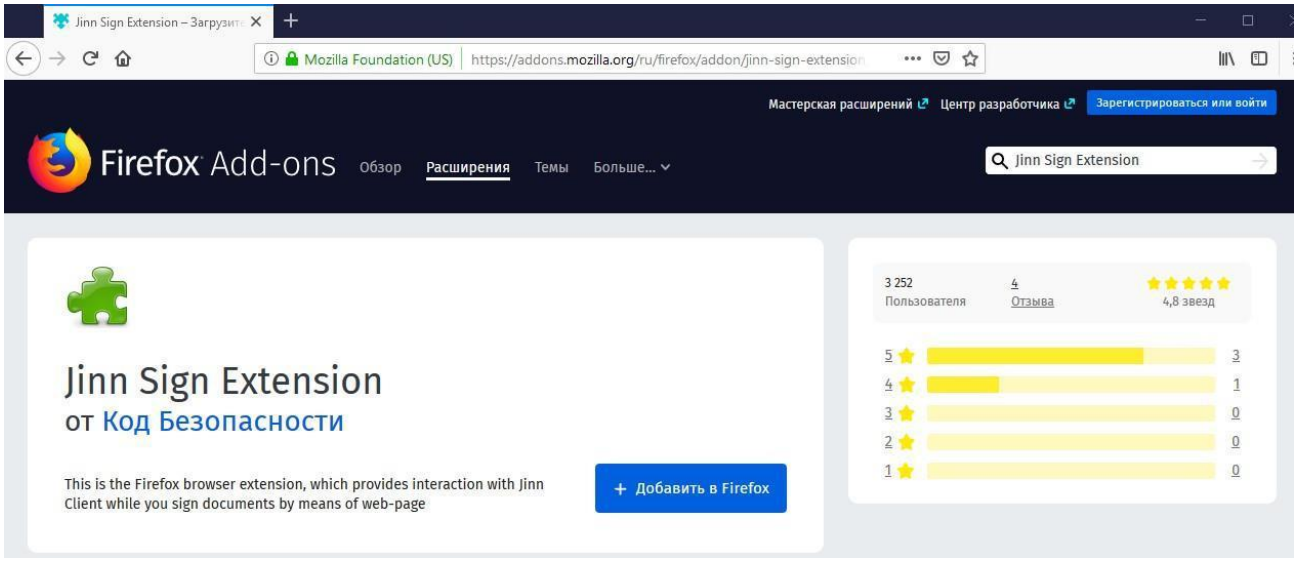


Рис. 35 – Расширение Jinn Sign Extension в браузере Firefox

- В появившемся запросе на установку расширения, нажмите «Добавить» (Рис. 36).



Рис. 36 – Запрос на добавление расширения «Jinn Sign Extension» в браузере Mozilla Firefox

- По завершению установки в правом верхнем углу браузера появится оповещение об установке расширения «Jinn Sign Extension» (Рис. 37). Нажмите «ОК».

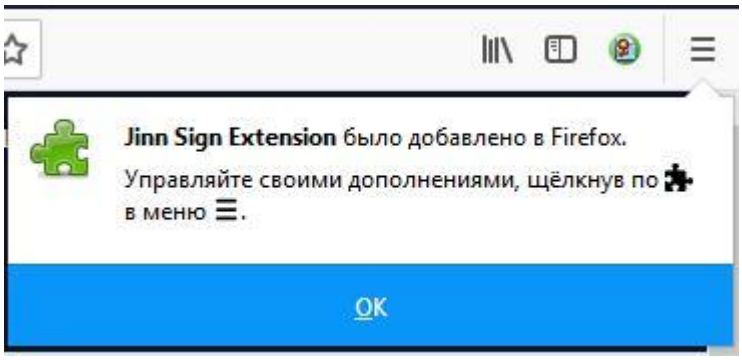


Рис. 37 - Сообщение об успешном завершении установки расширения «Jinn Sign Extension»

- Откройте список всех установленных расширений в браузере - для этого в правом верхнем углу нажмите на значок ☰, выберите «Дополнения». В левой части окна браузера выберите «Расширения». В открывшемся представлении найдите «Jinn Sign Extension» и убедитесь, что он включен (Рис. 38).

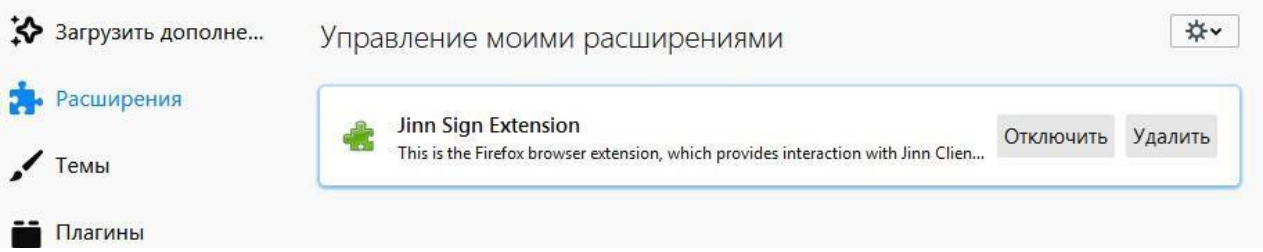


Рис. 38 – Расширение «Jinn Sign Extension» в Mozilla Firefox

11. Подключение к личному кабинету ФГИС ЦС

11.1 Запустите ПО «Континент TLS-клиент», для этого кликните два раза по его ярлыку на рабочем столе. В правом нижнем окне рабочего стола появится значок . В случае, если ПО «Континент TLS-клиент» фиксирует ошибку настроек, то значок будет отображаться с красным восклицательным знаком.

11.2 Нажмите на значок «Континент TLS-клиент» правой кнопкой мыши и выберете пункт «Сброс соединений» (Рис. 39).

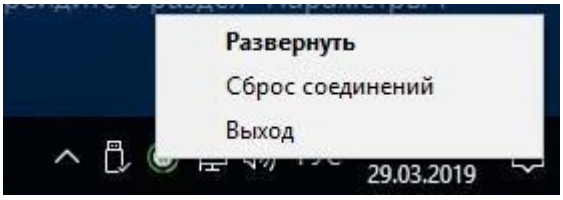


Рис. 39 – Сброс соединений

11.3 Далее в адресной строке браузера перейдите по ссылке: https://fgiscs-tls12.gge.ru:8444/.

11.4 При правильной настройке АРМ после перехода по вышеуказанной ссылке появится окно с выбором сертификата пользователя (Рис. 40).

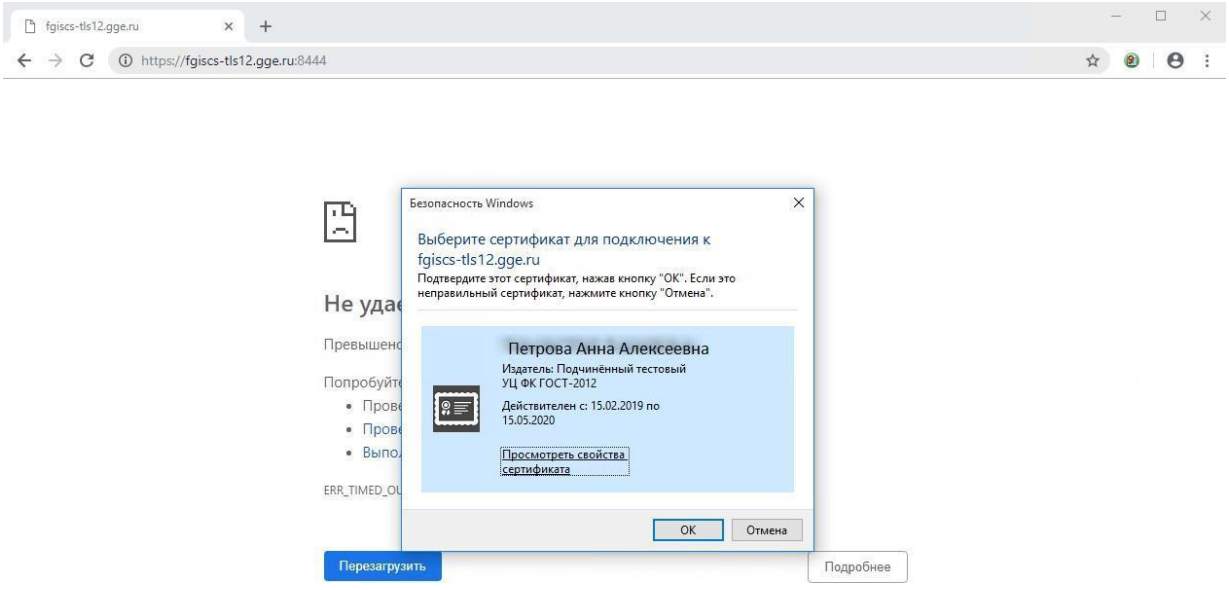


Рис. 40 – Выбор сертификата пользователя

11.5 Выберите сертификат пользователя и нажмите кнопку «ОК». В случае если на контейнер закрытого ключа или на внешний носитель закрытого ключа установлен пароль/пин-код, введите его. Нажмите «ОК».

11.6 На экране появится страница с сообщением «Ваше подключение не защищено»; нажмите «Дополнительные», затем нажмите на ссылку «Перейти на сайт fgiscs-tls12.gge.ru» (Рис. 41).

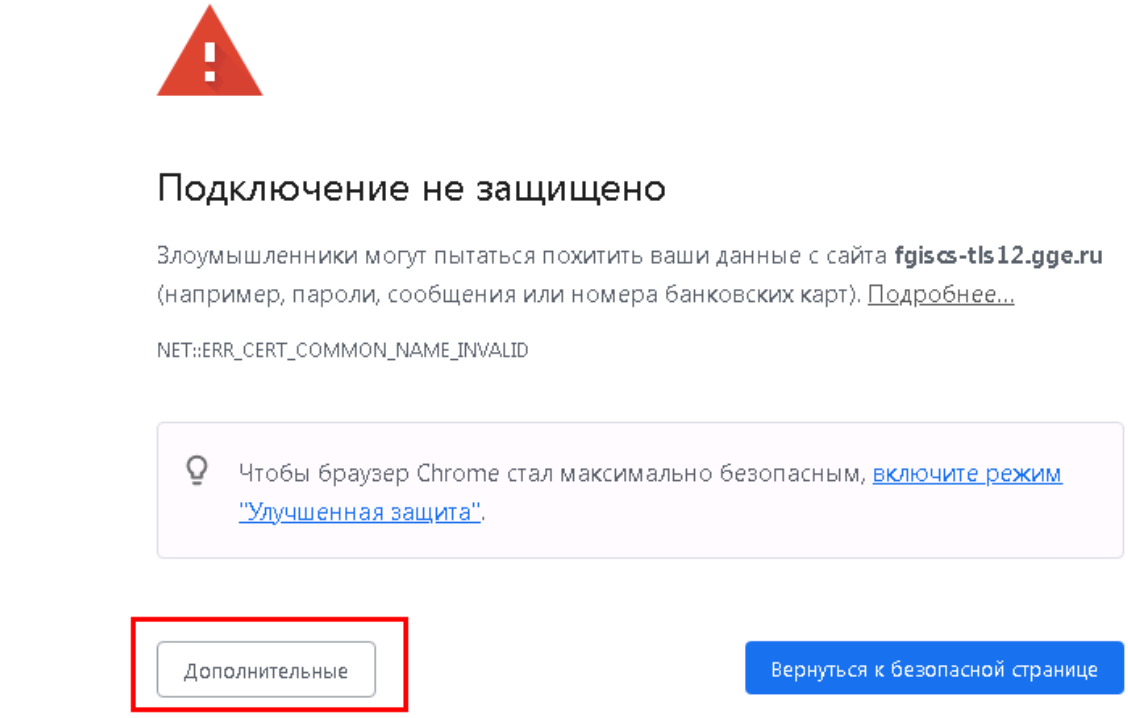


Рис. 41 – Кнопка «Дополнительные»

11.7 После загрузки страницы отобразится главная страница портала ФГИС ЦС (Рис. 42).

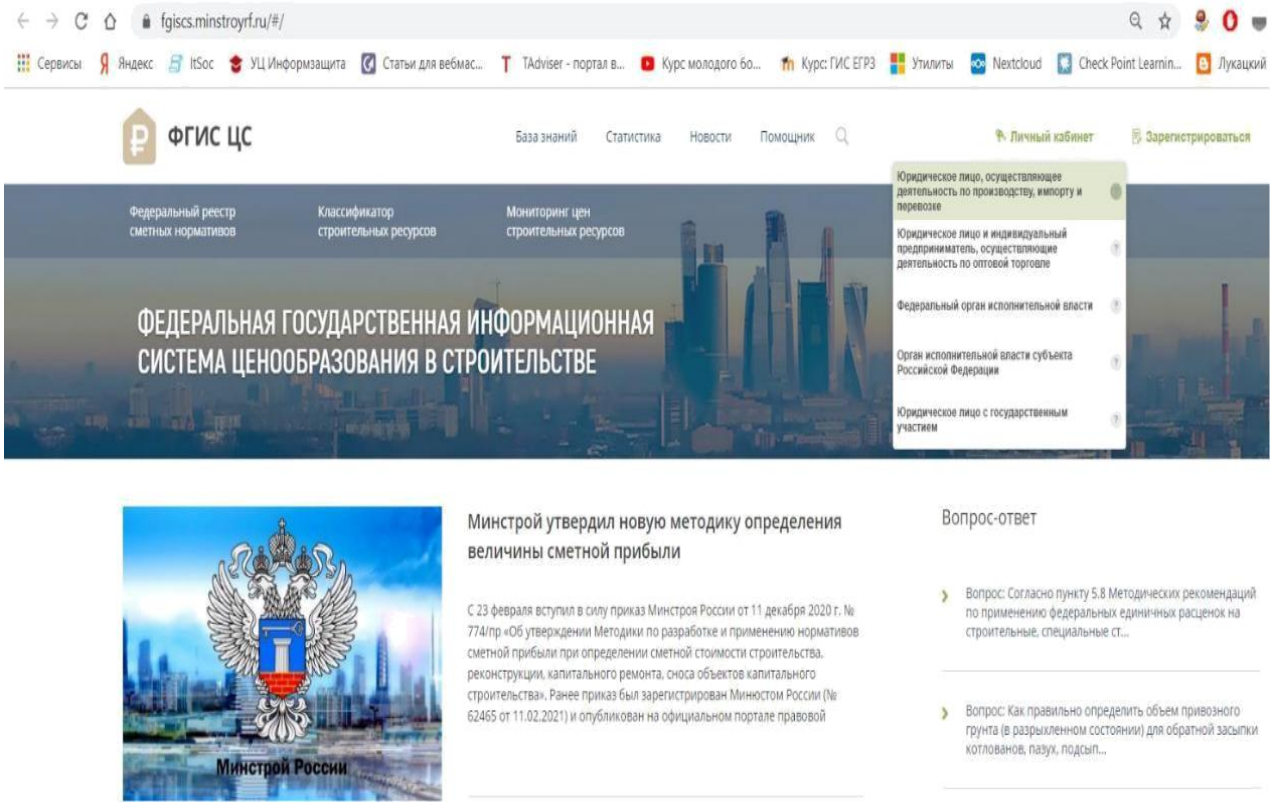


Рис. 42 – Главная страница портала ФГИС ЦС

11.8 Далее нажмите на ссылку «Личный кабинет» в правом верхнем углу портала, загрузится форма аутентификации в ЕСИА. Выполните аутентификацию и перейдите в личный кабинет ФГИС ЦС.

12. Использование Крипто Про CSP

12.1 Если у Вас установлено ПО Крипто Про CSP, Вы можете выполнить вход в личный кабинет с помощью данного ПО.

12.2 Для этого на странице https://fgiscs.minstroyrf.ru/#/ нажмите на кнопку "Личный кабинет", выберите необходимый пункт в выпадающем меню (Рис. 43).

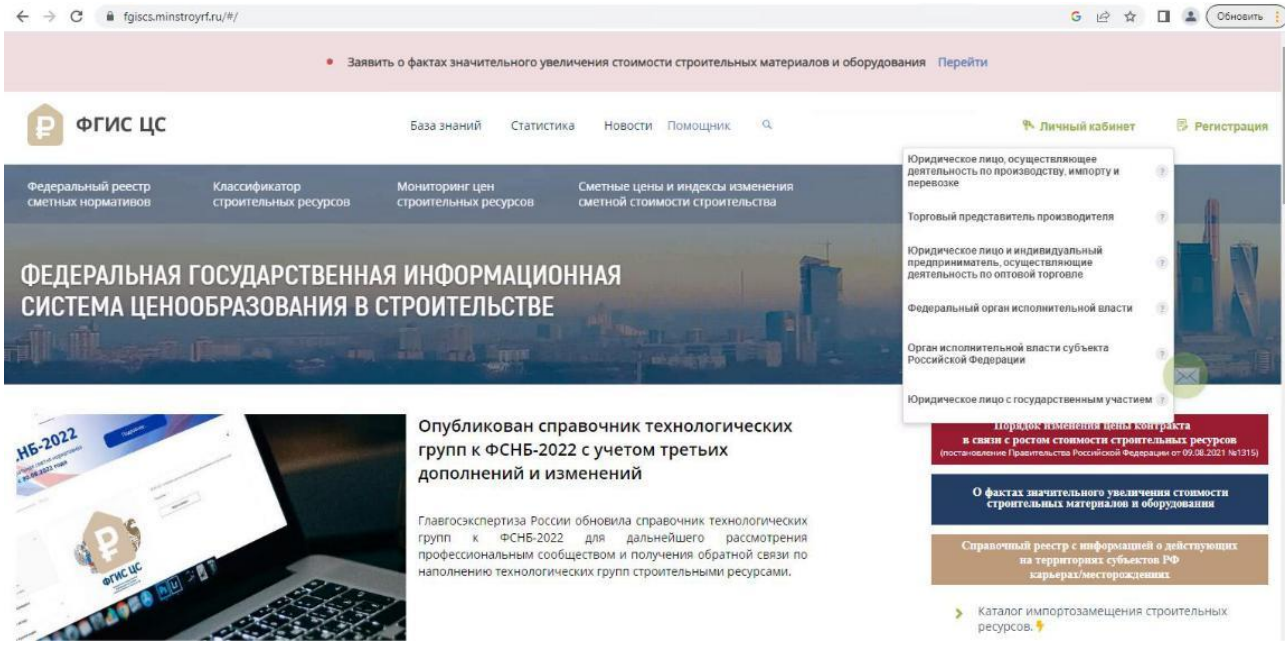


Рис. 43 – Вход в личный кабинет

12.3 Загрузится форма аутентификации в ЕСИА. Выполните аутентификацию и перейдите в личный кабинет ФГИС ЦС.

12.4 На странице выбора подключения через TLS или HTTPS, выберите вариант подключения через HTTPS. Установите соответствующую галочку в правом окне и нажмите кнопку «Войти».

13. Установка Крипто Про ЭЦП Browser plug-in

13.1 Если у Вас установлено ПО Крипто ПРО CSP, Вы можете выполнить подписание документов в личном кабинете с его помощью.

13.2 Установите на компьютере Крипто Про ЭЦП Browser plug-in. Скачайте программу установки Крипто Про ЭЦП Browser plug-in по ссылке:

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

13.3 Запустите исполняемый файл cadesplugin.exe (Рис.44).

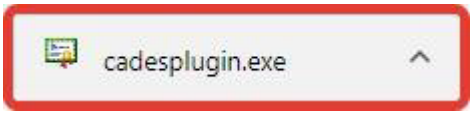


Рис. 44 – Запуск исполняемого файла

13. Подтвердите установку Крипто Про ЭЦП Browser plug-in (Рис.45)

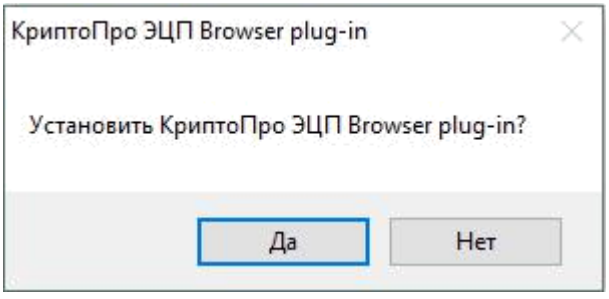


Рис. 45 – Подтверждение установки

a. Если потребуется, разрешите Крипто Про ЭЦП Browser plug-in внести изменения путем нажатия кнопки «Да» (Рис. 46)

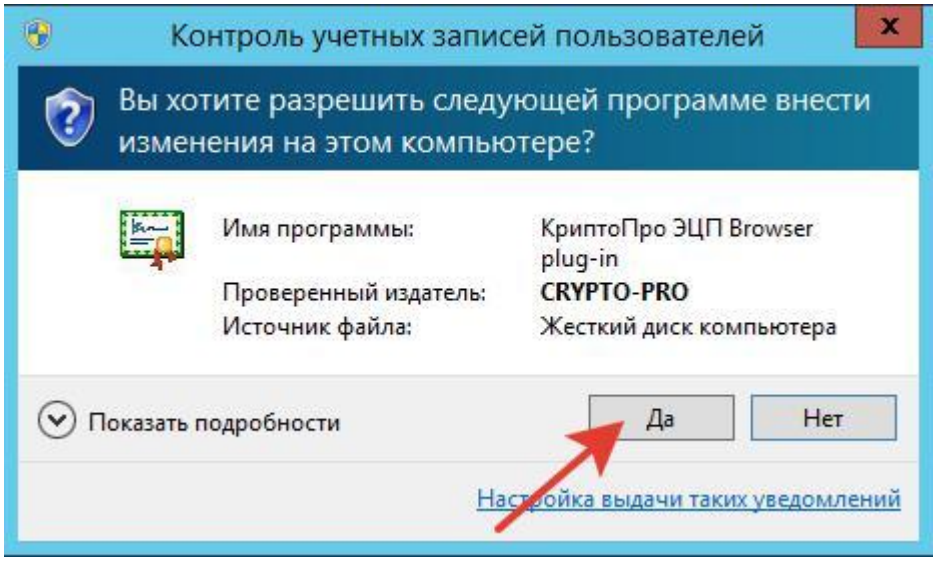


Рис. 46 – Подтверждение установки

Дождитесь окончания установки Крипто Про ЭЦП Browser plug-in. После окончания установки нажмите «ОК» (Рис. 47).

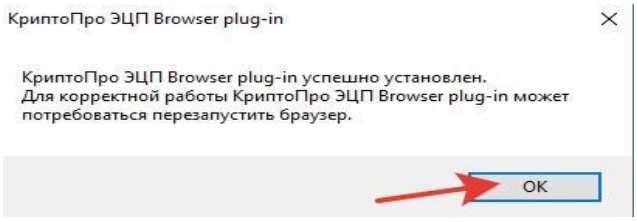


Рис. 47 – Нажатие кнопки «ОК»

b. Запустите браузер и дождитесь оповещения об установленном расширении «CryptoPro Extension for CAdES Browser Plug-in». Включите это расширение (Рис. 48).

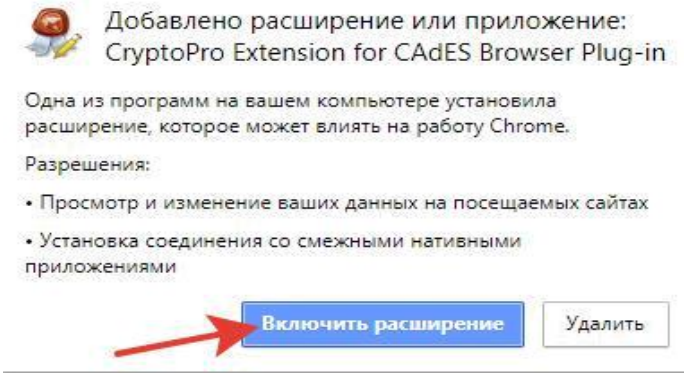


Рис. 48 – Кнопка «Включить расширение»

Если на Вашем компьютере ранее уже выполнялась установка расширения «CryptoPro Extension for CAdES Browser Plug-in», а потом оно был удалено, или вы используете Chromium Edge, то его потребуется установить отдельно. Для этого перейдите по https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnnmpdbibifmljnfjhpififfog и установите расширение из интернет-магазина Chrome. Убедитесь, что расширение включено на странице расширений (Рис. 49).

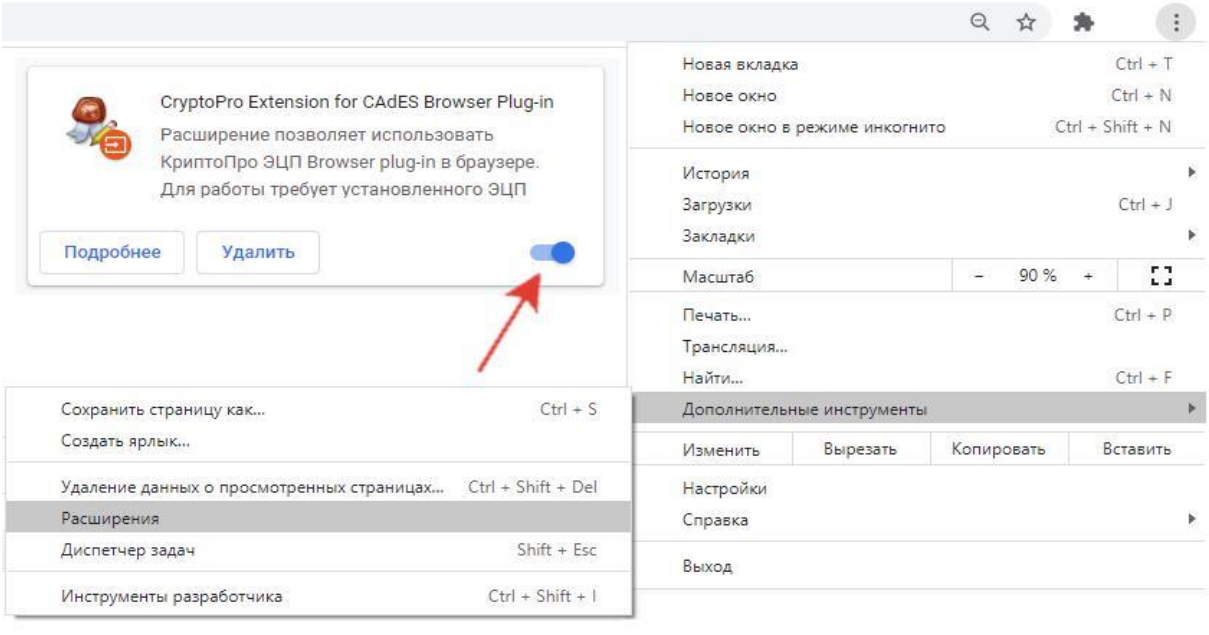


Рис. 49 – Включение расширения

13.5 Проверьте корректность установки на странице проверки плагина по ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html

13.6 Для этого в открывшемся окне подтвердите доступ путем нажатия кнопки "Да" (Рис. 50).

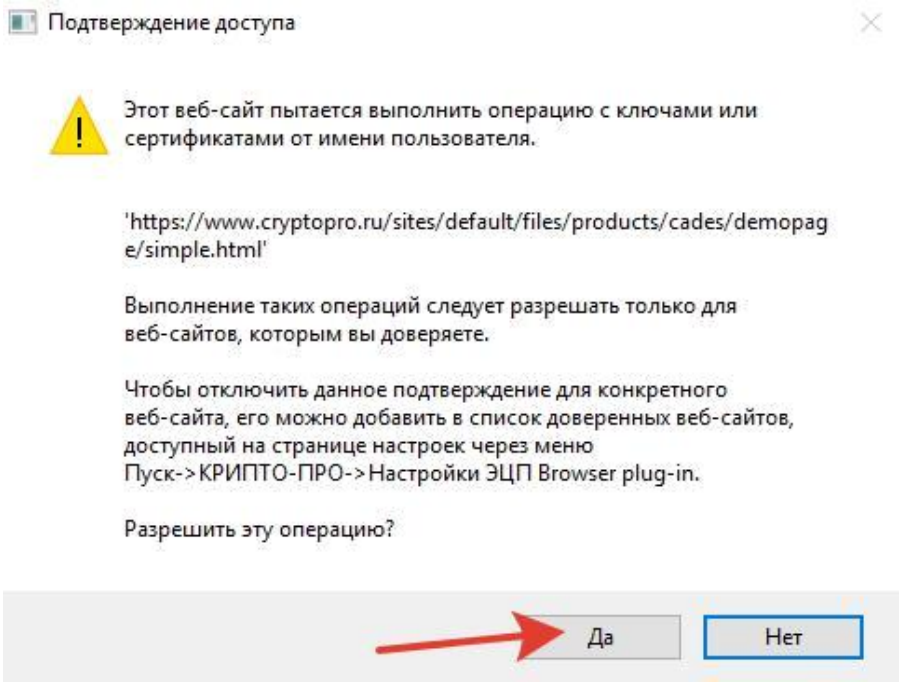


Рис. 50 – Подтверждение доступа

13.7 Если установка Крипто Про ЭЦП Browser plug-in прошла успешно, появится окно с надписью: "Плагин загружен", указанием его версии и используемой Вами версии Крипто Про CSP (Рис. 51).



Рис. 51 – Успешная загрузка плагина

Если в процессе установки у вас возникли вопросы для консультации обращайтесь в техническую поддержку по адресу https://skzi.infosec.ru/.