ИНСТРУКЦИЯ

по подключению организаций
к сервису распространения дистрибутивов
информационной системы
«Автоматизация органов криптографической защиты»

СОДЕРЖАНИЕ

Основные термины, сокращения и определения 3

Расшифровка графических элементов веб-интерфейса ИС АОКЗ 4

1. Общие положения 5

2. Подготовка к работе 5

2.1. Требования к АРМ пользователя 5

2.2. Установка и настройка криптопровайдера КриптоПро CSP 5

2.3. Установка плагина «КриптоПро ЭЦП browser plug-in» 9

2.4. Добавление доверенных узлов в КриптоПро ЭЦП browser plug-in 14

2.5. Установка сертификатов 15

2.5.1. Установка корневого сертификата головного удостоверяющего центра 16

2.5.2. Установка личного сертификата (при необходимости) 19

2.6. Настройка браузера 23

3. Регистрация в ИС АОКЗ 26

4. Порядок работы в ИС АОКЗ 29

4.1. Раздел «Экземпляры СКЗИ» 29

4.2. Управление экземплярами СКЗИ 32

5. Раздел «Лицензии» 33

6. Выход из системы 33

ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

Термин или сокращение	Пояснение
АРМ	Автоматизированное рабочее место.
ГРО	Главный регистратор организации.
ГУЦ	Головной удостоверяющий центр Минцифры России
ЕСИА	Единая система идентификации и аутентификации.
Инструкция № 152	Инструкция об организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденная приказом ФАПСИ от 13.06.2001 № 152.
ИС	Информационная система.
ИС АОКЗ	Информационная система «Автоматизация органа криптографической защиты».
Обладатель конфиденциальной информации (ОКИ)	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
Орган криптографической защиты информации (ОКЗИ)	Организация или структурное подразделение, функцией которого является разработка и осуществление мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации. Органом криптографической защиты информации может быть организация, структурное подразделение организации, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены на физическое лицо.
Организация	Организация, обслуживаемая в ТОФК
ПО	Программное обеспечение.
ПОИБ СОБИ ФК	Подсистема обеспечения информационной безопасности Системы обеспечения безопасности информации Федерального казначейства.
Регистратор	Сотрудник организации, которому назначена роль «Регистратор» в ПОИБ СОБИ ФК, выполняющий администрирование ученых записей пользователей
СКЗИ	Средство криптографической защиты информации.
Сотрудник ОКИ	Физическое лицо, непосредственно наделенное функциональной ролью обладателя конфиденциальной информации, необходимой для работы в ПО АОКЗ.
ТОФК	Территориальный орган Федерального казначейства
УЦ ФК	Удостоверяющий центр Федерального казначейства.
УЗ	Учетная запись
ФК	Федеральное казначейство.
Электронная подпись (ЭП)	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

РАСШИФРОВКА ГРАФИЧЕСКИХ ЭЛЕМЕНТОВ ВЕБ-ИНТЕРФЕЙСА ИС АОКЗ

№	Изображение элемента	Пояснение
1.		Просмотр комплекта поставки.
2.		Удаление экземпляра СКЗИ/СКЗИ/Ключевого документа/Лицевого счета пользователя СКЗИ и т.д.
3.		Выгрузка в xls.
4.		Просмотр скрытого текста.
5.		Просмотр реквизитов электронной подписи мероприятия.
6.		Подтверждение получения экземпляра СКЗИ от ОКЗИ.
7.		Сообщить, что указанный экземпляр СКЗИ был введён в действие.
8.		Сообщить, что указанный экземпляр СКЗИ был выведен из действия.
9.		Вернуть экземпляр СКЗИ в ОКЗИ.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция предназначена для описания процесса передачи СКЗИ, эксплуатационной и технической документации, лицензионных ключей к ним между ТОФК и Организацией.

Осуществление передачи СКЗИ, эксплуатационной и технической документации, лицензионных ключей к ним происходит в рамках выполнения требований Инструкции № 152.

2. ПОДГОТОВКА К РАБОТЕ

Для полноценной работы с ИС АОКЗ пользователю необходимо выполнить обязательные настройки, описанные ниже.

2.1 Требования к АРМ пользователя

На АРМ пользователя должно быть установлено следующее ПО:

Браузер с поддержкой шифрования защищенных соединений по ГОСТ (ГОСТ 34.10-2012, ГОСТ 34.12-2018 и ГОСТ 34.13-2018): Яндекс.Браузер версии 20.2.1 или выше или Chromium-GOST версии 84 или выше;

Криптопровайдер КриптоПро CSP не ниже версии 4.0 и КриптоПро ЭЦП Browser plug-in не ниже версии 2.0.

Разрешение экрана АРМ пользователя должно быть не менее 1920x1080.

2.2 Установка и настройка криптопровайдера КриптоПро CSP

1. Запустите файл установки КриптоПро CSP. Откроется стартовое окно мастера установки КриптоПро CSP.

Примечание:

Первоначальное получение КриптоПро CSP осуществляется в ТОФК по месту нахождения (обслуживания) Организации на физическом носителе (CD, DVD-диски).

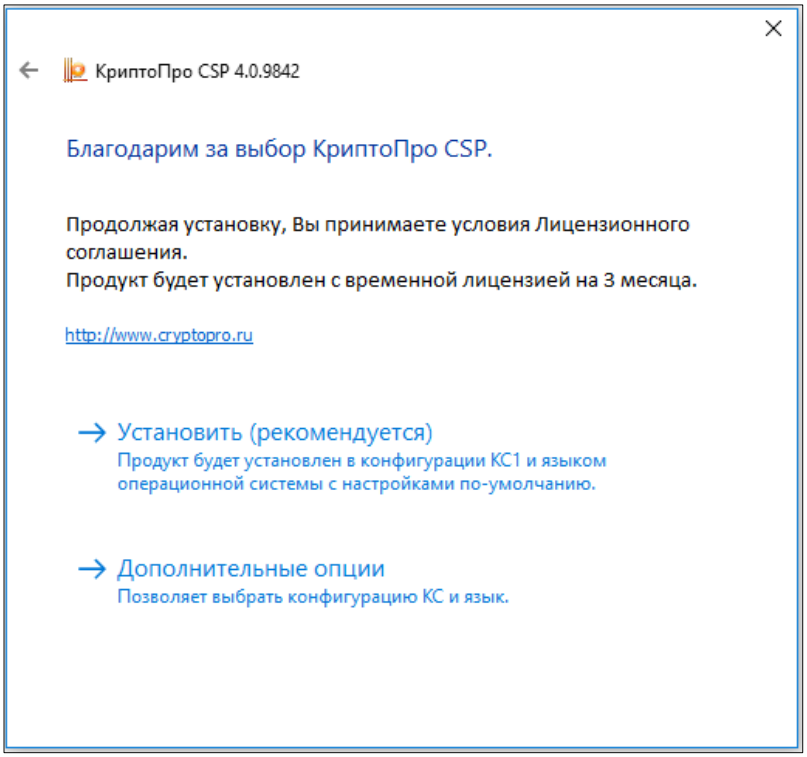


Рисунок 1 – Стартовое окно мастера установки КриптоПро CSP

2. Нажмите на кнопку «Установить (рекомендуется)».

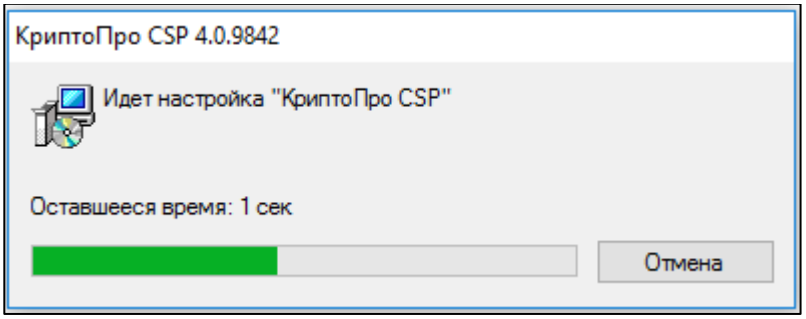


Рисунок 2 – Процесс установки КриптоПро CSP

3. Отображается окно процесса установки КриптоПро CSP.

После успешной установки криптопровайдера отобразится диалог «КриптоПро CSP успешно установлен».

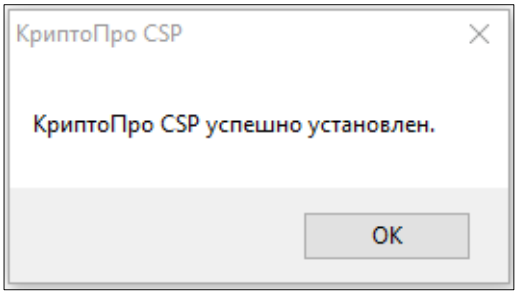


Рисунок 3 – Успешная установка КриптоПро CSP

4. Нажмите на кнопку «ОК»;

5. Запустите КриптоПро CSP.

6. На вкладке «Общие» нажмите на кнопку «Ввод лицензии» и введите лицензионный ключ;

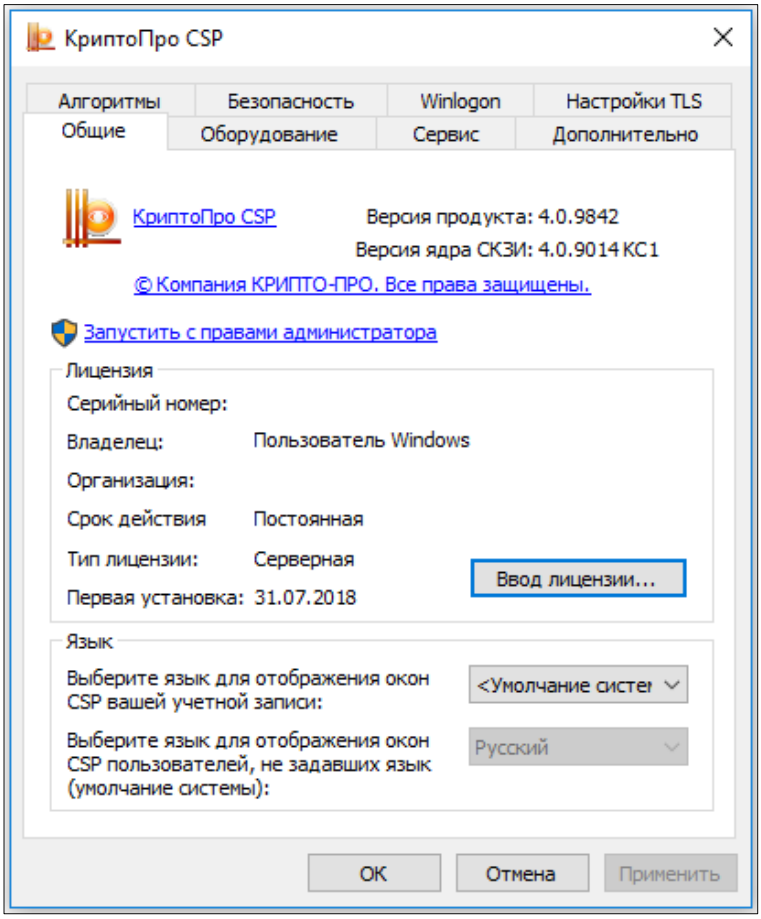


Рисунок 4 – Вкладка «Общие». КриптоПро CSP

Для настройки криптопровайдера необходимо выполнить следующие действия:

1. Запустите КриптоПро CSP от имени Администратора;

2. Перейдите на вкладку «Настройки TLS»;

3. Включите в разделе «Клиент» следующие чекбоксы:

Не проверять сертификат сервера на отзыв;

Не проверять назначение собственного сертификата.

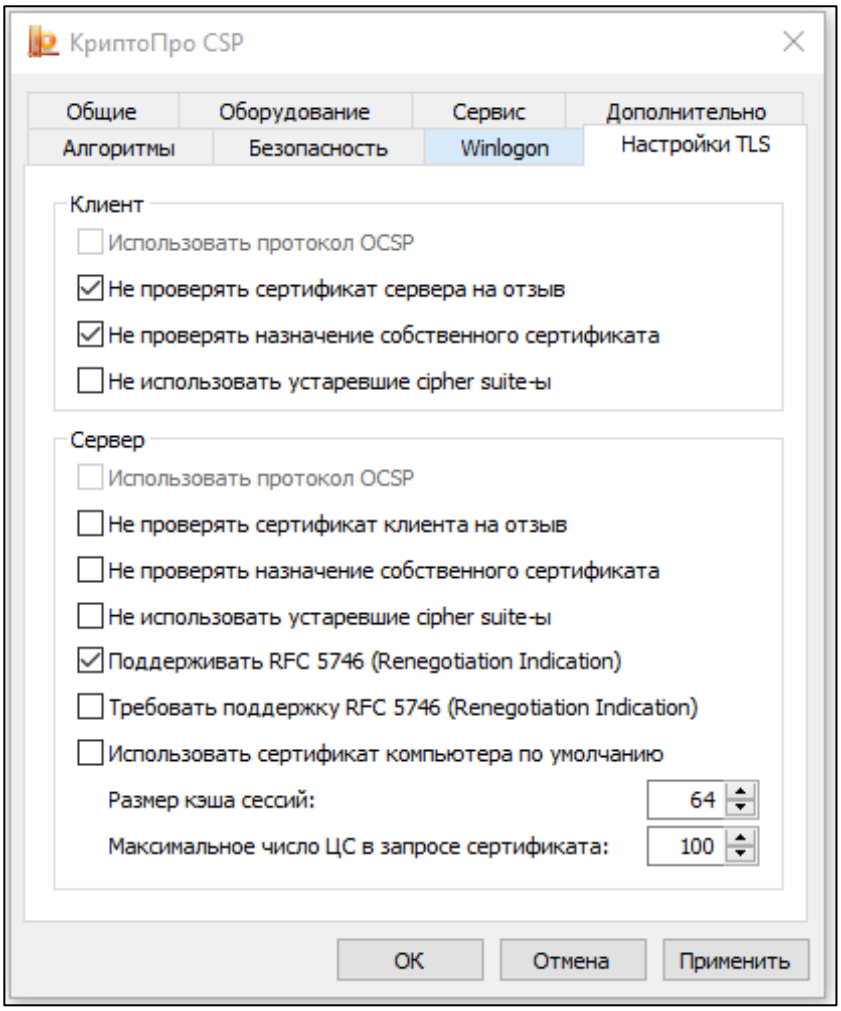


Рисунок 5 – Вкладка «Настройки TLS». КриптоПро CSP

4. Нажмите на кнопку «Применить». Появится запрос на перезагрузку АРМ;

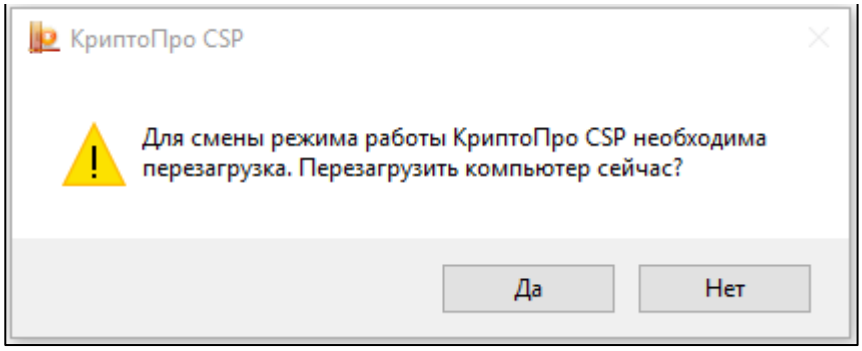


Рисунок 6 – Запрос на перезагрузку после смены режима работы

5. Нажмите на кнопку «Да»;

6. АРМ перезагрузится.

2.3 Установка плагина «КриптоПро ЭЦП browser plug-in»

Плагин «КриптоПро ЭЦП Browser plug-in» предназначен для создания и проверки электронной подписи на веб-страницах с использованием СКЗИ «КриптоПро CSP».

Файл установки доступен по адресу:

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

Последовательность шагов для установки плагина:

1. Запустите файл установки;



Рисунок 7 – Скаченный файл установки

2. Нажмите «Да» в окне подтверждения установки плагина;

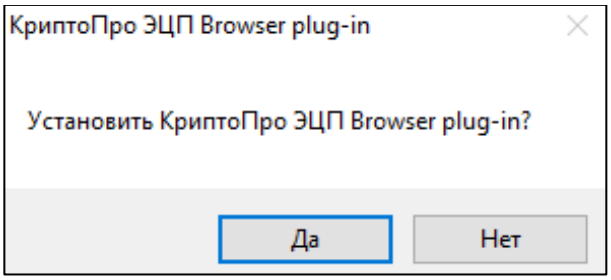


Рисунок 8 – Подтверждение установки

3. При необходимости разрешите выполнение программы;

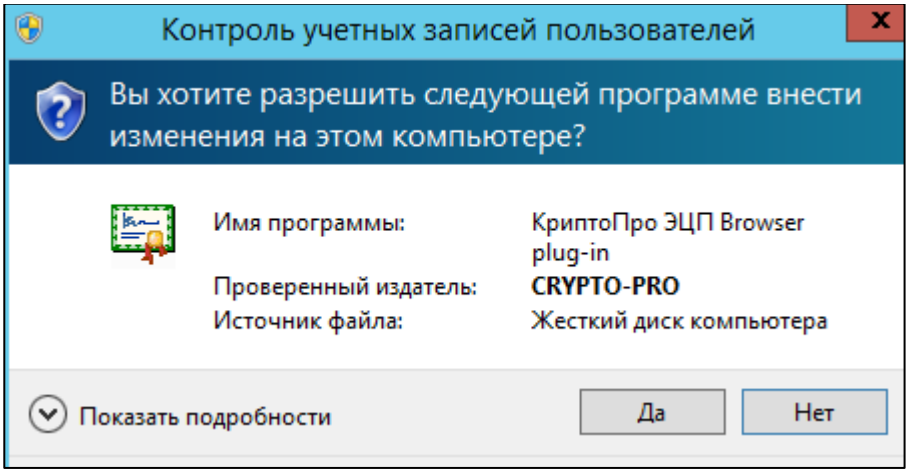


Рисунок 9 – Разрешение на установку плагина

4. Выполняется процесс установки;

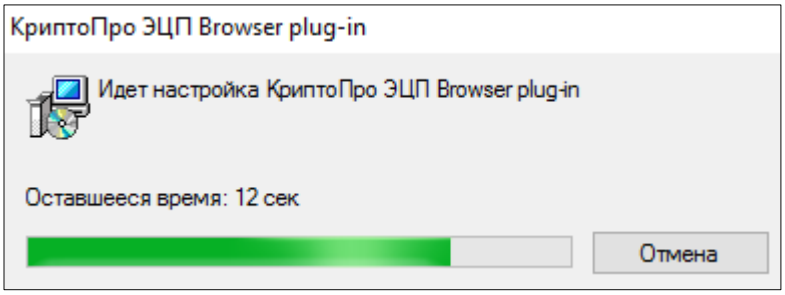


Рисунок 10 – Процесс установки плагина

4. Отображается уведомление об успешной установке плагина;

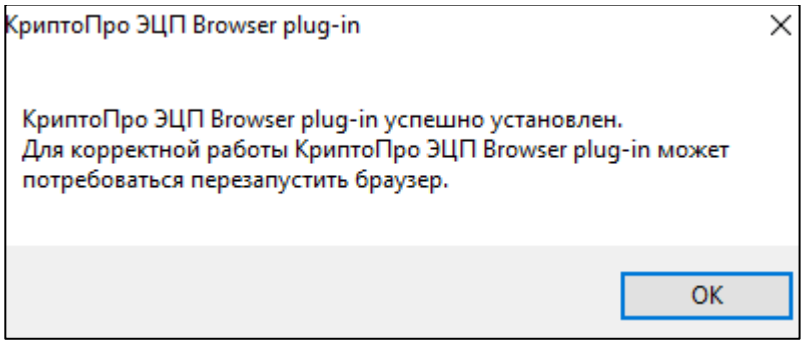


Рисунок 11 – Успешно выполнена установка плагина

5. Нажмите кнопку «ОК»;

6. Затем включите расширение КриптоПро ЭЦП в используемом для работы с ИС АОКЗ браузере (см. ниже рисунки по шагам 1-3):

6.1. Запустите браузер;

6.2. Выберите в настройках браузера пункт «Дополнения»;

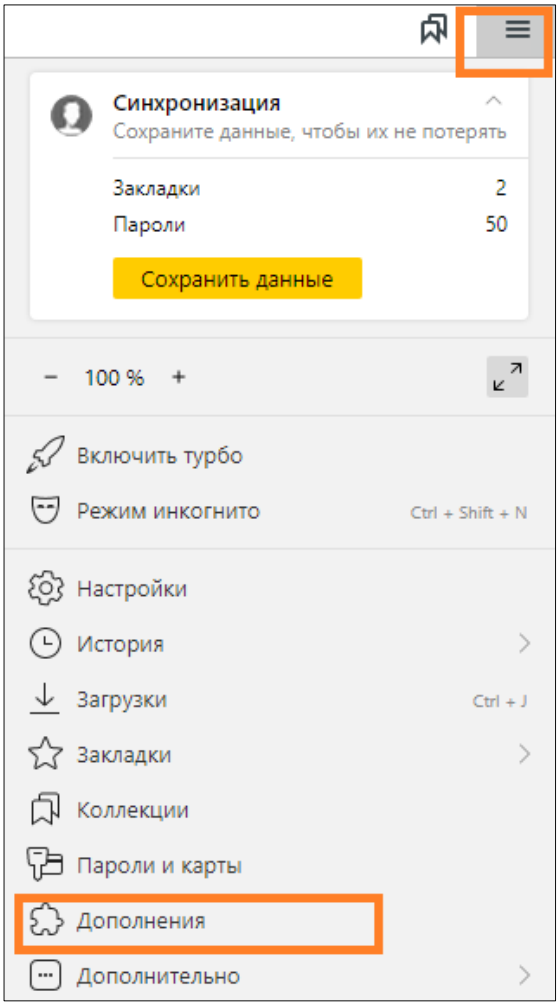


Рисунок 12 – Включение плагина в браузере. Шаг-1

6.3. Отображается список расширений, доступных для включения;

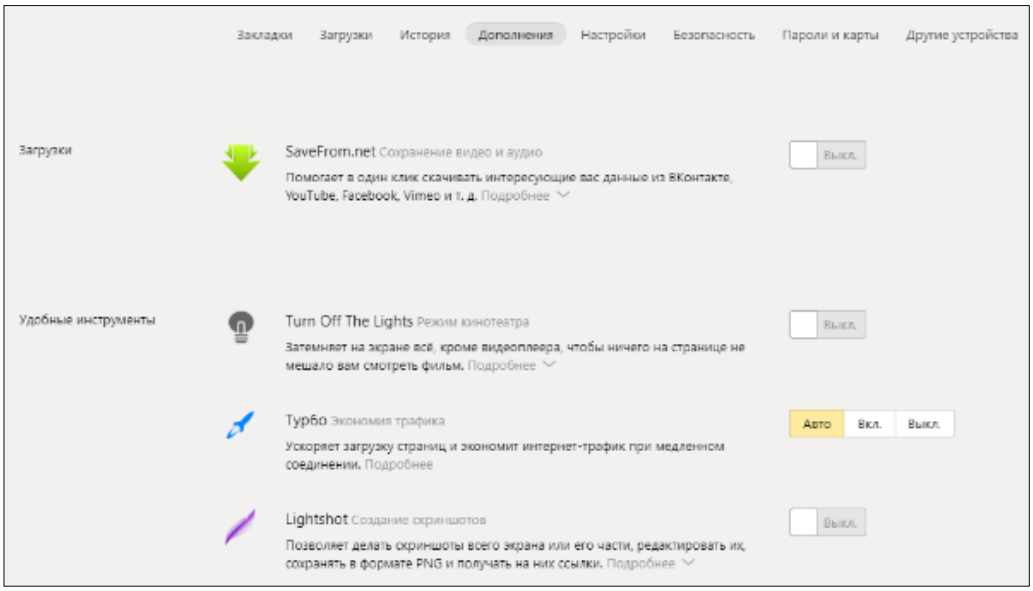


Рисунок 13 – Включение плагина в браузере. Шаг-2

6.4. Найдите в списке и включите расширение КриптоПро ЭЦП;

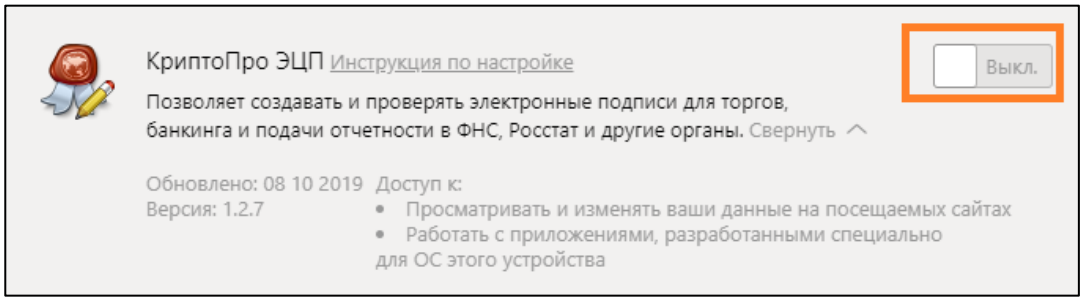


Рисунок 14 – Включение плагина в браузере. Шаг-3

6.5 В браузере в верхнем правом углу отобразится уведомление об успешной установке плагина;

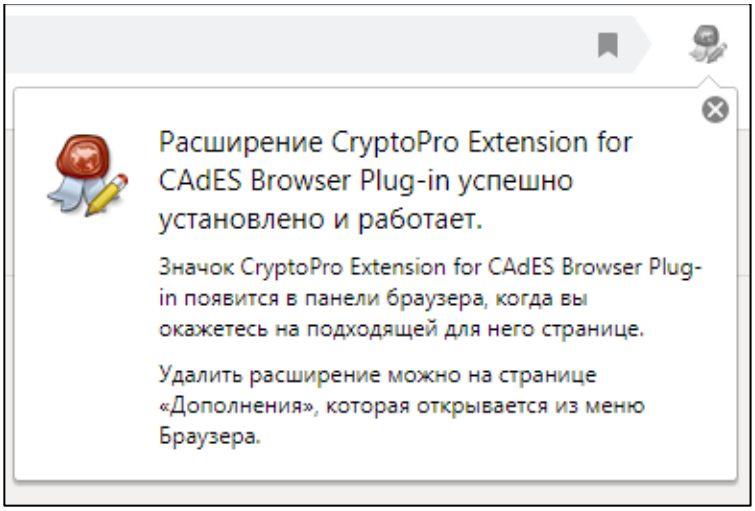


Рисунок 15 – Уведомление об успешной установке плагина в браузере

7. Плагин успешно установлен.

8. В заключение следует проверить корректность установки плагина:

8.1. Открыть страницу проверки работы плагина: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html

8.2. Отобразится окно для подтверждения доступа;

Примечание:

Чтобы данное окно для подтверждения доступа не отображалось в будущем при подписании документов электронной подписью в ИС АОКЗ, следует добавить доверенные узлы в плагин. О том, как это сделать, см. следующий раздел настоящей инструкции.

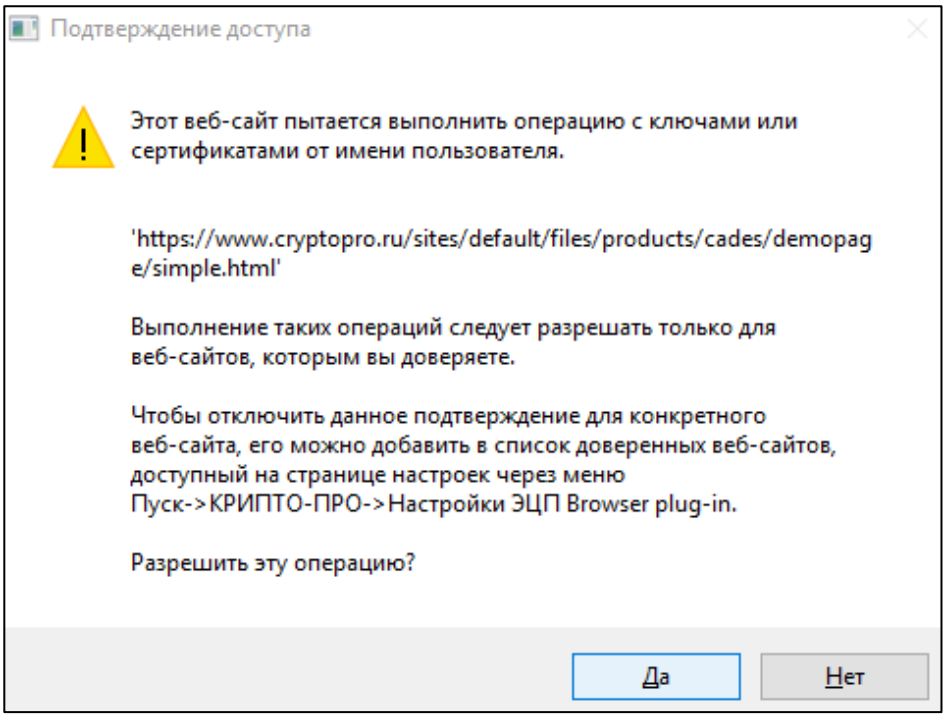


Рисунок 16 – Запрос подтверждения доступа

8.3. Нажмите кнопку «Да»;

8.4. Отображается страница проверки плагина. При успешной установке плагина на данной странице отображается надпись «Плагин загружен» с зеленой точкой (см. ниже рисунок).

Примечание:

При отсутствии корневого сертификата удостоверяющего центра и личного сертификата безопасности, установленных на АРМ пользователя, отобразится уведомление об ошибке на странице проверки плагина. Как установить данные сертификаты, см. в разделе «Установка сертификатов безопасности».

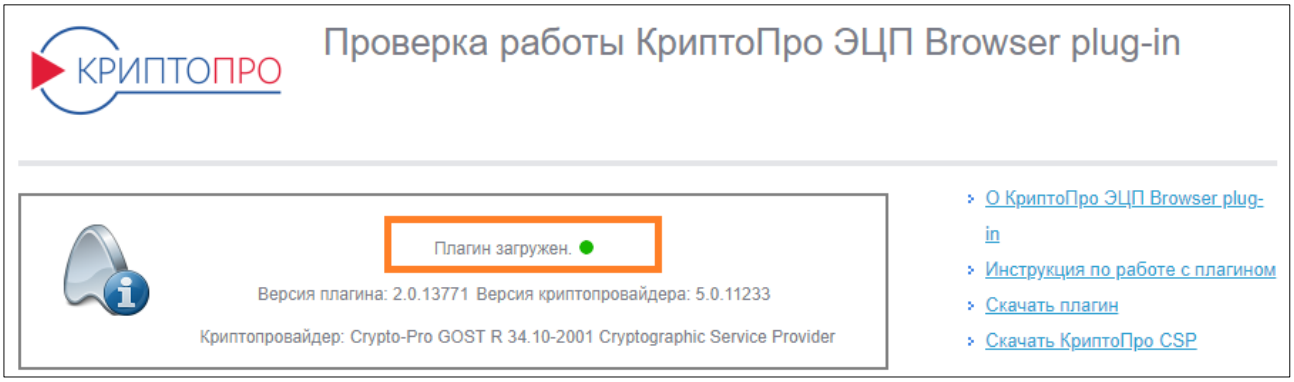


Рисунок 17 – Страница для проверки плагина

2.4 Добавление доверенных узлов в КриптоПро ЭЦП browser plug-in

Выберите ПУСК → КРИПТО-ПРО → Настройки ЭЦП Browser Plug-in.

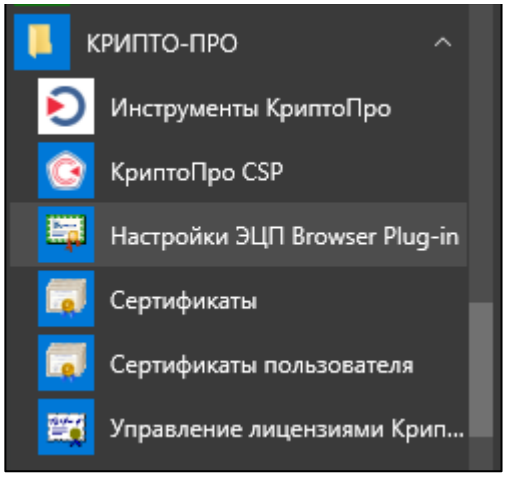


Рисунок 18 – Открытие настроек плагина

В браузере откроется страница с настройками плагина.

Нажмите правой кнопкой мыши на пункте «Настройки ЭЦП Browser Plug-in» и в меню выберите «Дополнительно > Открыть папку с файлом». Затем в открывшейся папке нажмите правой кнопкой мыши на файле «Настройки ЭЦП Browser Plug-in» и в меню выберите «Открыть с помощью > [Yandex/ChromiumGOST]» (см. рисунки ниже).

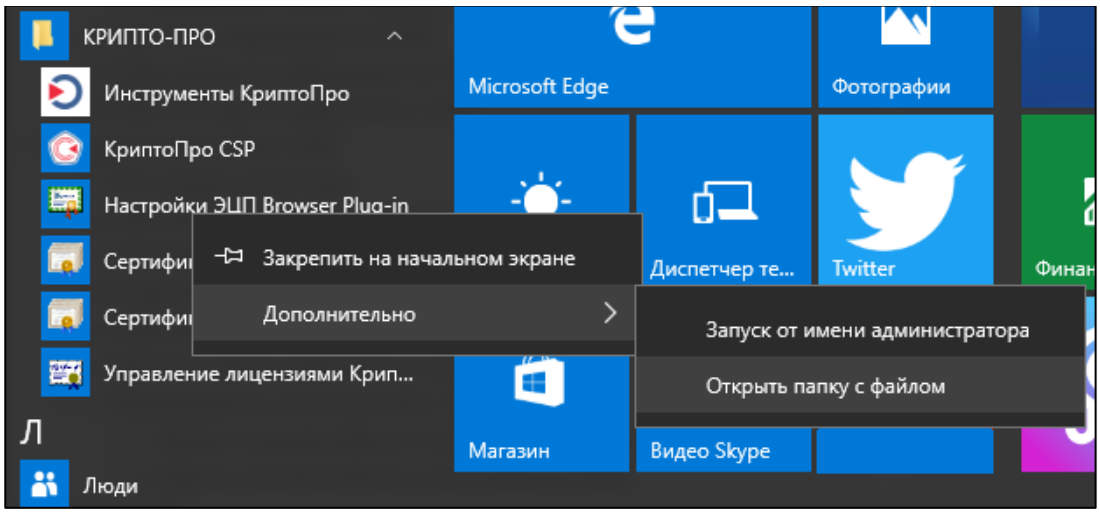


Рисунок 19 – Открытие настроек плагина в браузере.

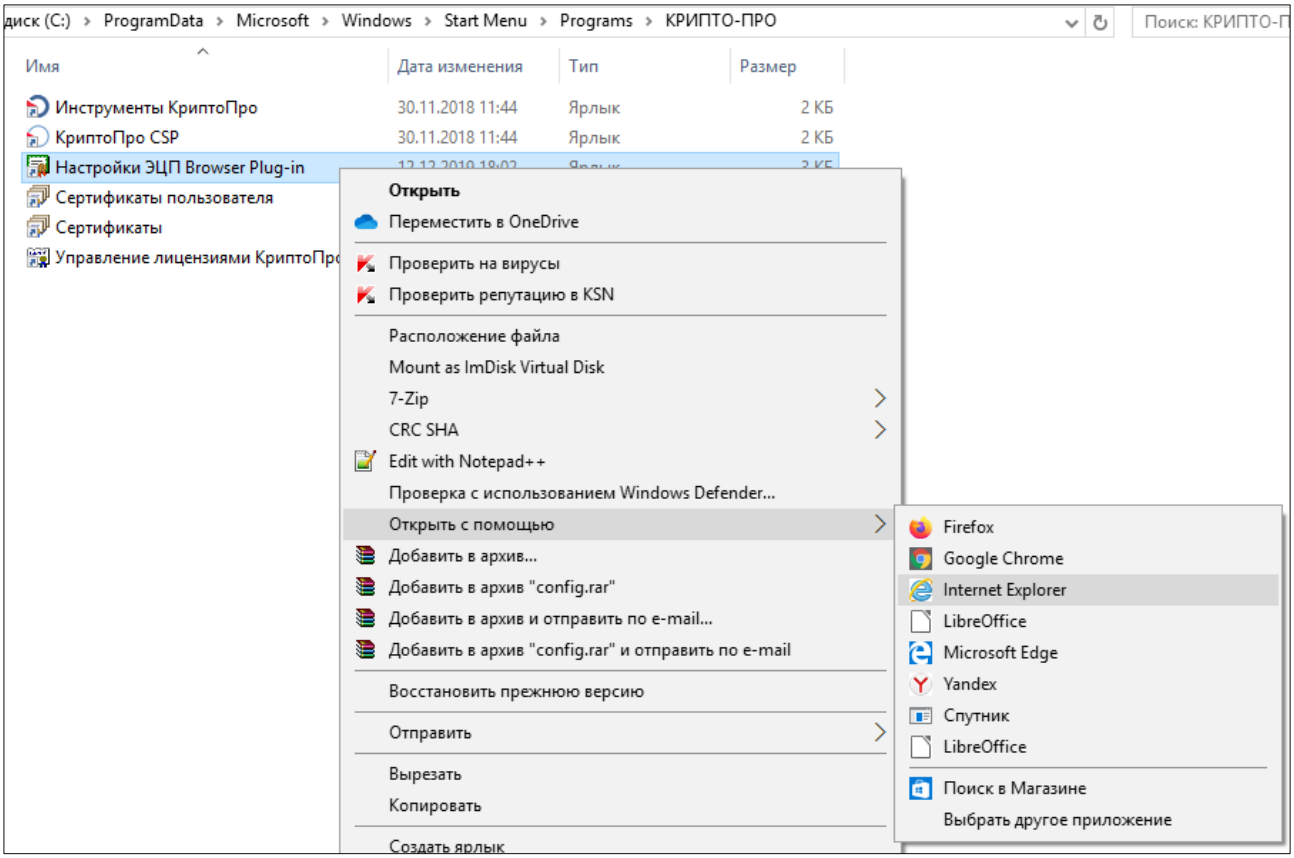


Рисунок 20 – Открытие настроек плагина в браузере.

Система отображает настройки плагина в браузере.

Добавьте доверенные узлы в окне настроек плагина.

В качестве доверенного узла можно указать адрес https://*.roskazna.ru.

Нажмите кнопку «Сохранить», чтобы записать введенные доверенные узлы.

2.5 Установка сертификатов

Для выполнения функций в ИС АОКЗ на АРМ пользователя должны быть установлены сертификаты:

корневой сертификат головного удостоверяющего центра (см. раздел «Установка корневого сертификата головного удостоверяющего центра");

личный сертификат пользователя (см. раздел «Установка личного сертификата безопасности»).

Если для формирования цепочки сертификатов требуется установка подчинённого сертификата, то она производится аналогично установке корневого сертификата с единственным отличием: на шаге 4.3 нужно выбрать хранилище сертификатов «Промежуточные центры сертификации».

Примечание:

Сертификат безопасности выдается аккредитованным удостоверяющим центром, который уполномочен создавать такие сертификаты.

2.5.1 Установка корневого сертификата головного удостоверяющего центра

1. Правой кнопкой мыши нажмите на файле корневого сертификата ГУЦ и выберите пункт «Установить сертификат»;

2. Отобразится мастер импорта сертификатов;

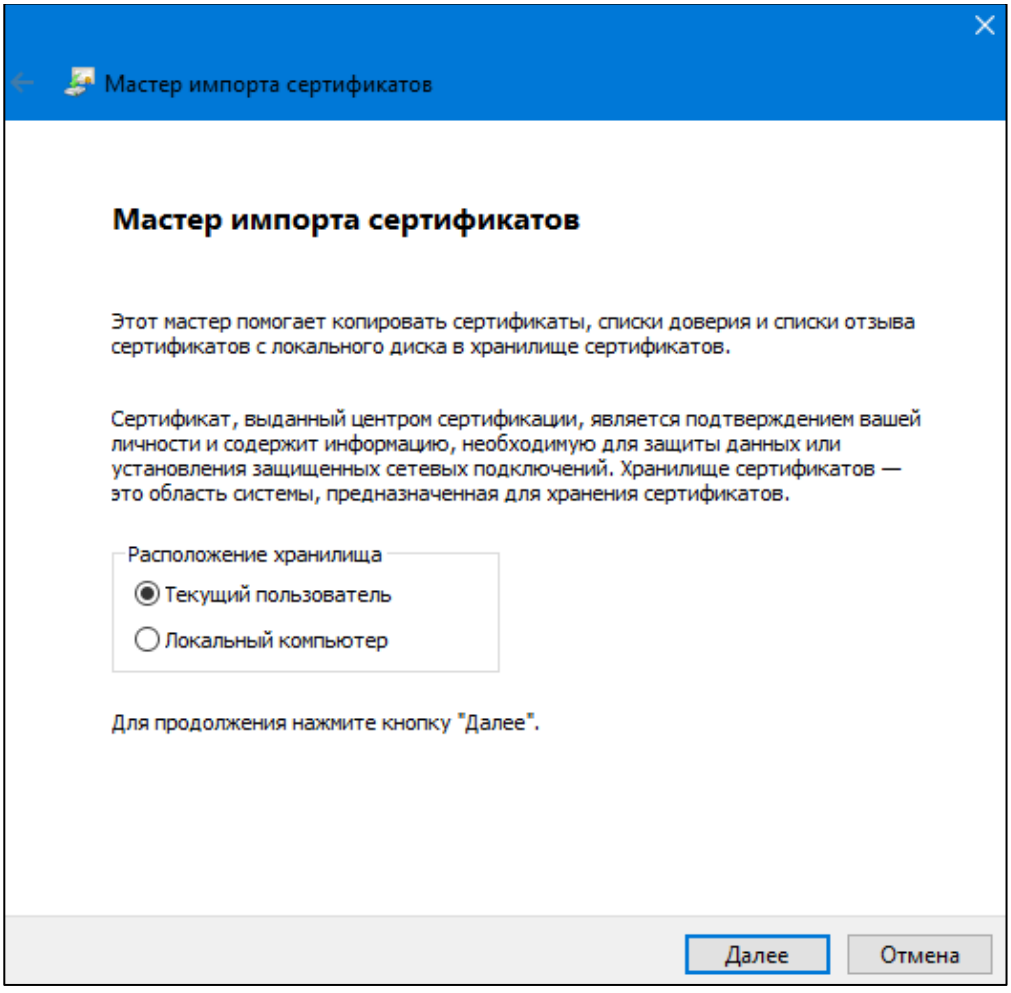


Рисунок 21 – Мастер импорта сертификатов

3. Выберите хранилище «Локальный компьютер» и нажмите на кнопку «Далее»;

Примечание:

Если отсутствует возможность выбора хранилища «Локальный компьютер», следует обратиться к системному администратору ЛВС для настройки прав локального администратора АРМ.

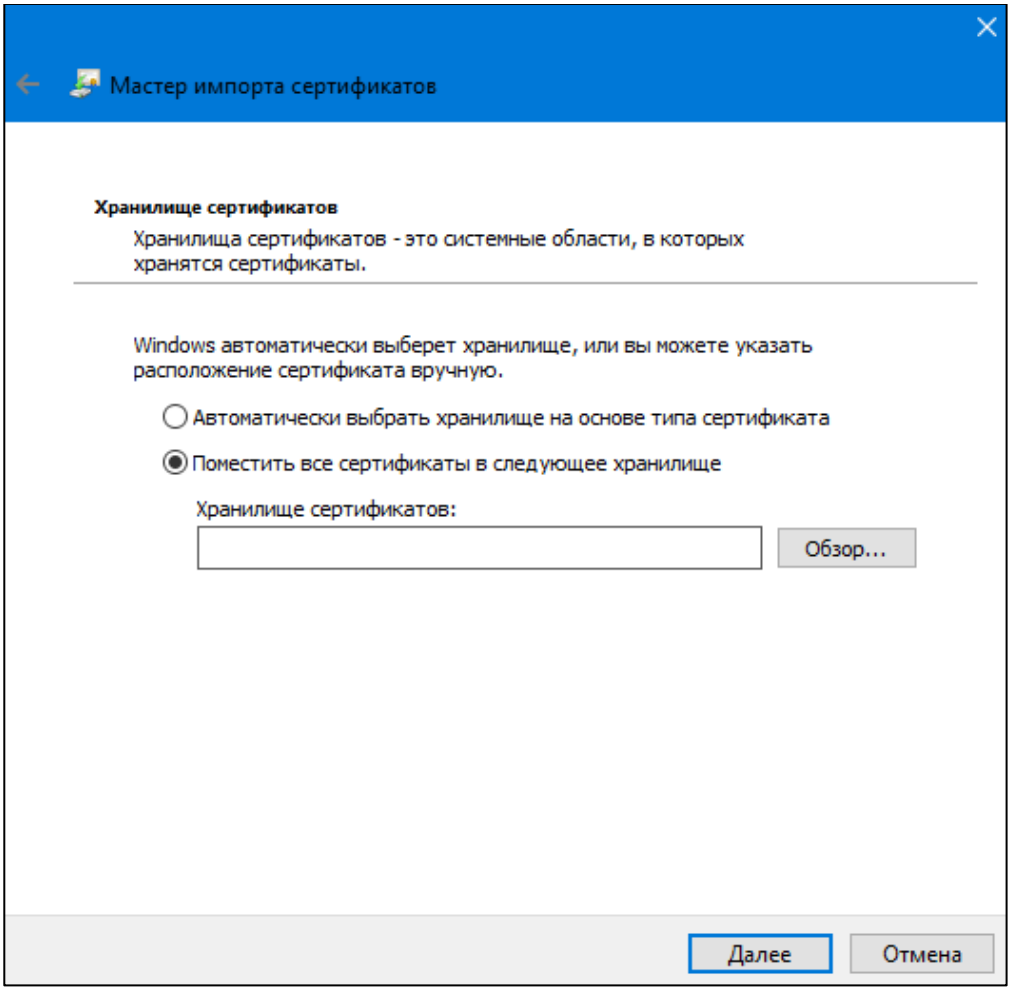


Рисунок 22 – Выбор хранилища сертификата

4. В окне «Хранилище сертификатов» активируйте переключатель «Поместить сертификаты в следующее хранилище» и укажите директорию размещения сертификата:

4.1. Нажмите на кнопку «Обзор…»;

4.2. Откроется окно «Выбор хранилища сертификата»;

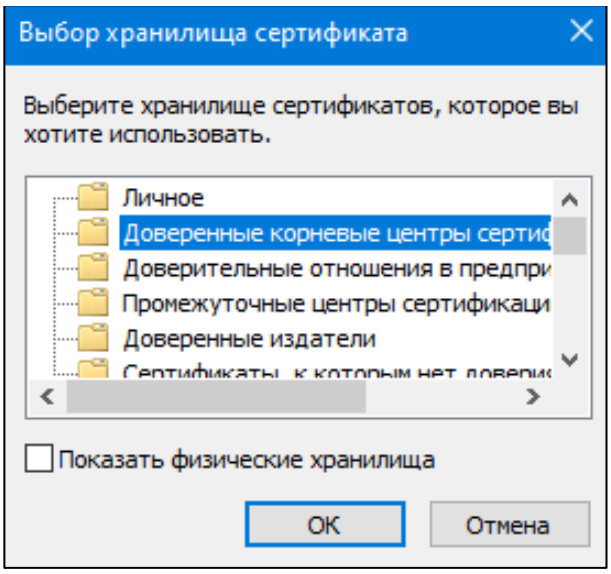


Рисунок 23 – Выбор хранилища сертификата

4.3. Выберите хранилище «Доверенные корневые центры сертификации»;

4.4. Нажмите на кнопку «ОК».

5. Откроется окно завершения работы мастера импорта сертификатов;

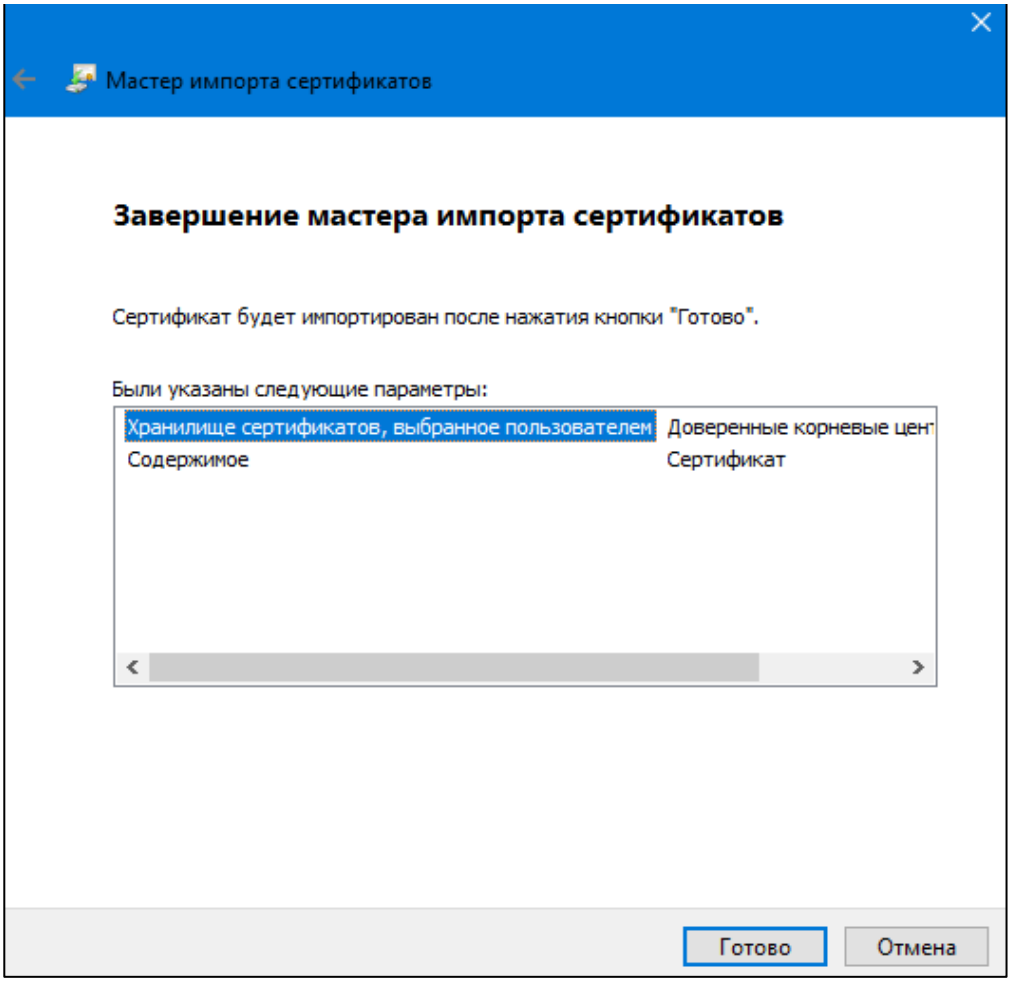


Рисунок 24 – Окно завершения работы мастера импорта сертификатов

6. Нажмите на кнопку «Готово»;

7. Появится сообщение, что импорт успешно выполнен;

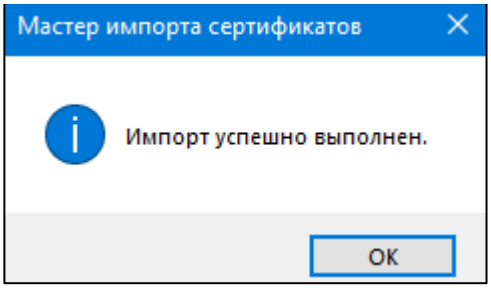


Рисунок 25 – Завершение установки

8. Нажмите на кнопку «ОК».

2.5.2 Установка личного сертификата (при необходимости)

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется в случае, если файл сертификата пользователя не является единым целым с закрытым ключом (в процессе получения в УЦ сертификат в формате «*.cer» был записан на отдельный носитель информации).

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в ИС АОКЗ.

Для установки сертификата пользователя в хранилище личных сертификатов АРМ пользователя средствами СКЗИ «КриптоПро» необходимо:

1) Открыть приложение «КриптоПро CSP» и перейти на вкладку «Сервис»;

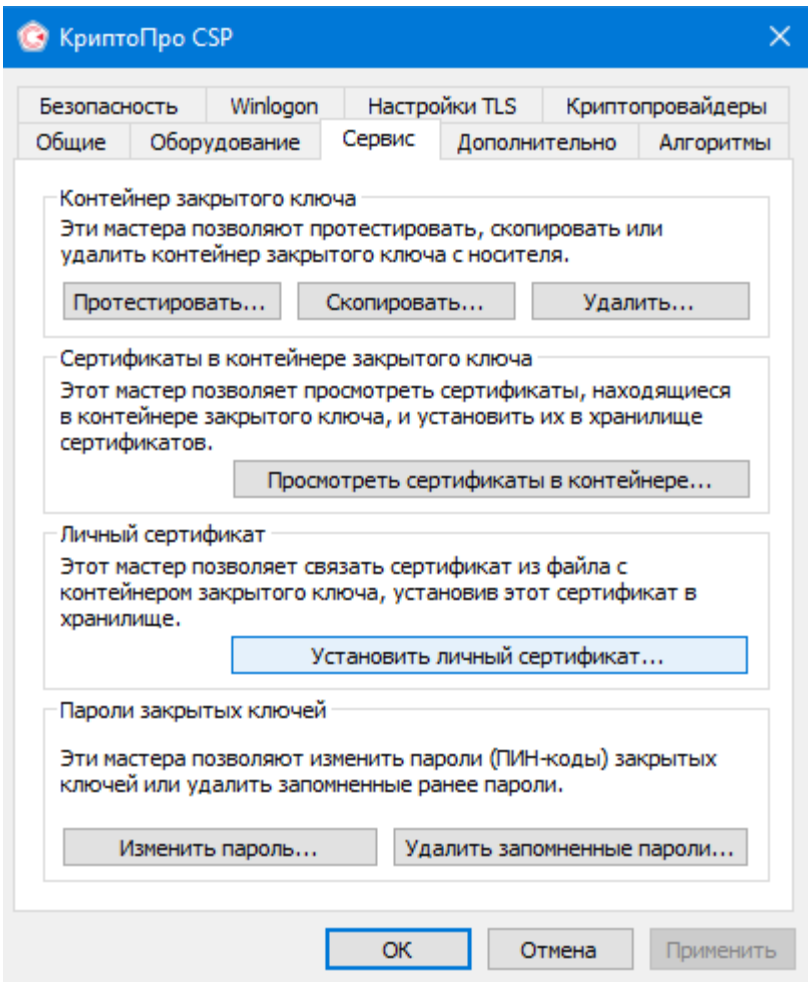


Рисунок 26 – Вкладка «Сервис»

2) Нажать кнопку «Установить личный сертификат»;
3) Выбрать личный сертификат, нажав на кнопку «Обзор»;

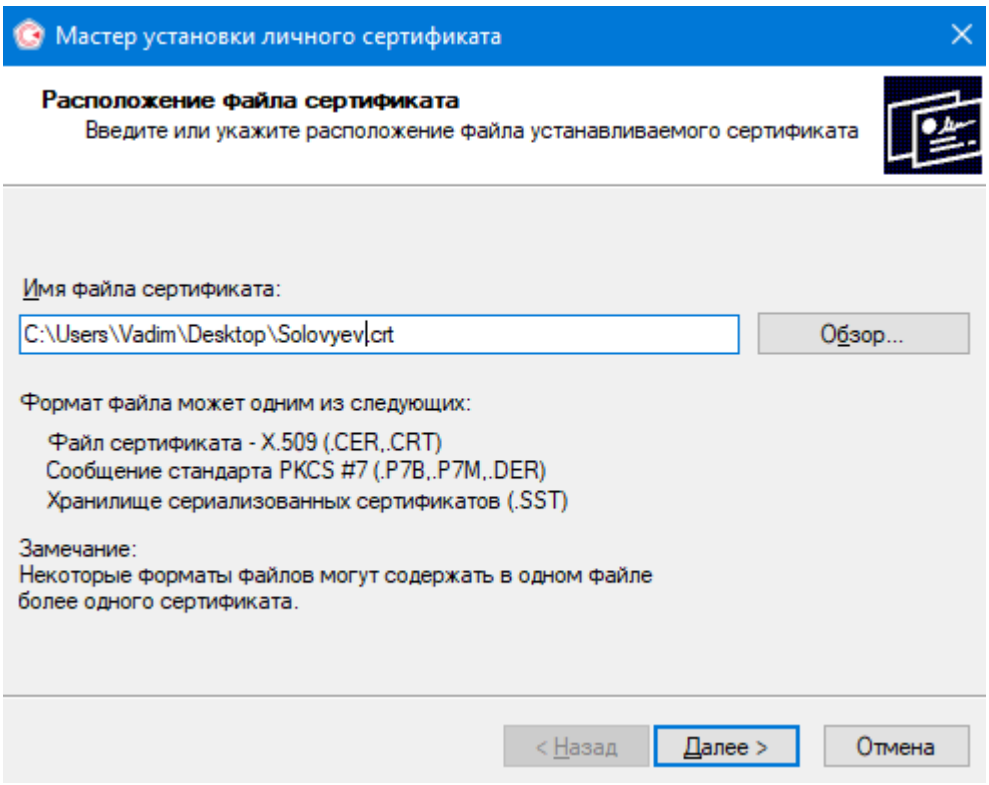


Рисунок 27 – Выбор сертификата

4) Нажать кнопку «Далее»;
5) Отобразится окно с данными о выбранном сертификате;
6) Нажать кнопку «Далее»;
7) Указать контейнер закрытого ключа;

Если контейнер располагается на присоединенном носителе, то следует установить признак «Найти контейнер автоматически».

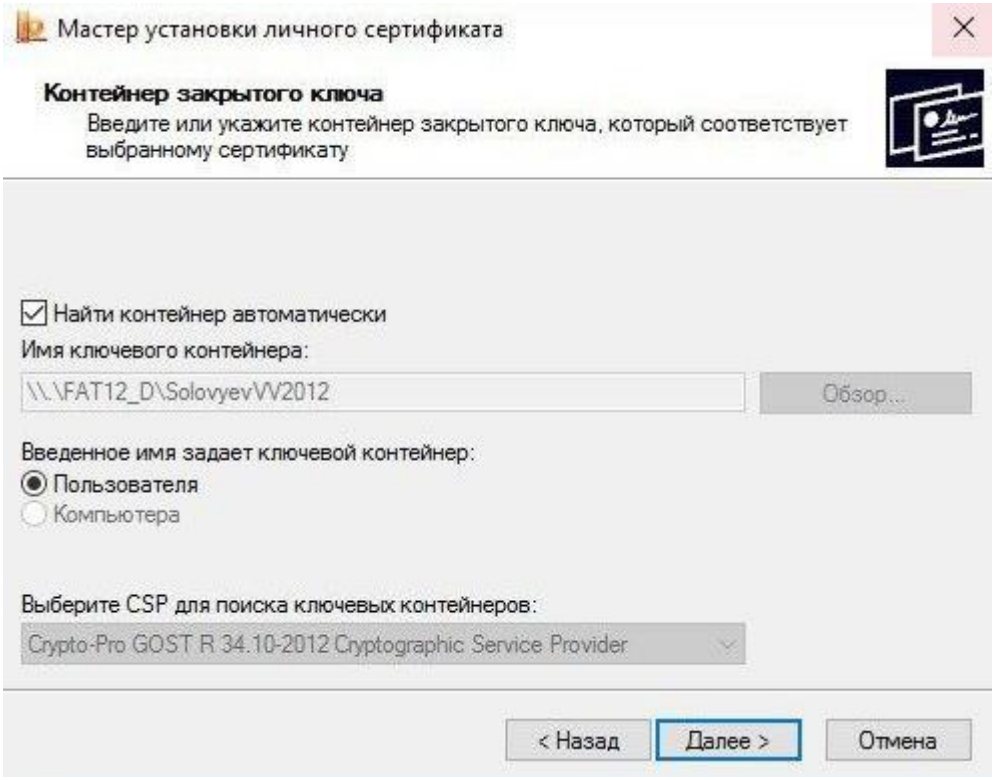


Рисунок 28 – Выбор контейнера закрытого ключа

8) Указать хранилище сертификата;

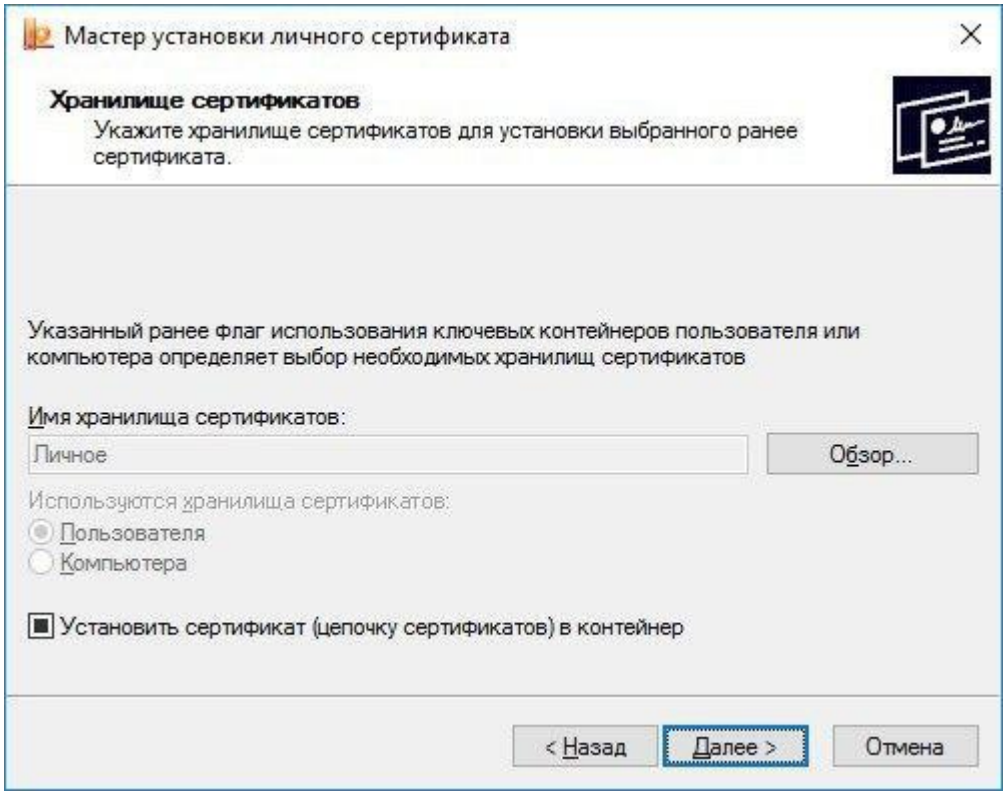


Рисунок 29 – Выбор хранилища сертификата

9) Нажать кнопку «Готово»;

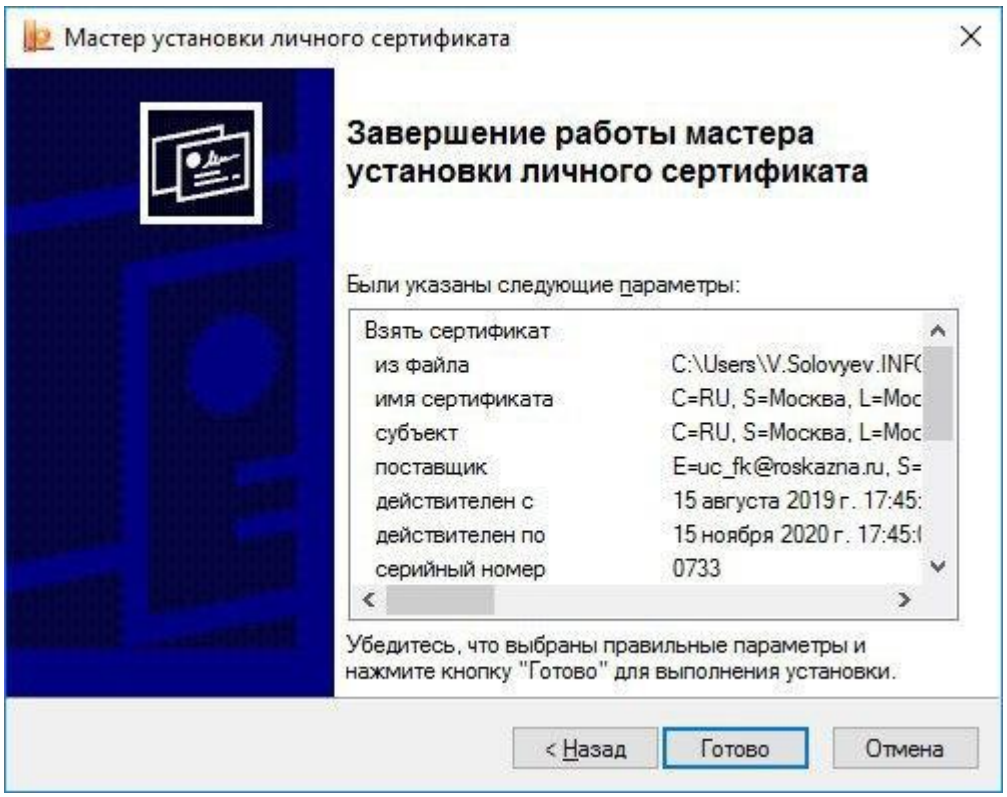


Рисунок 30 – Завершение настроек установки сертификата

10) Сертификат установлен в контейнер закрытого ключа и в хранилище «Личное» на АРМ пользователя.

2.6 Настройка браузера

Перед началом работы с ИС АОКЗ браузер должен быть настроен на работу по ГОСТу:

1. Откройте браузер;

2. Откройте настройки браузера;

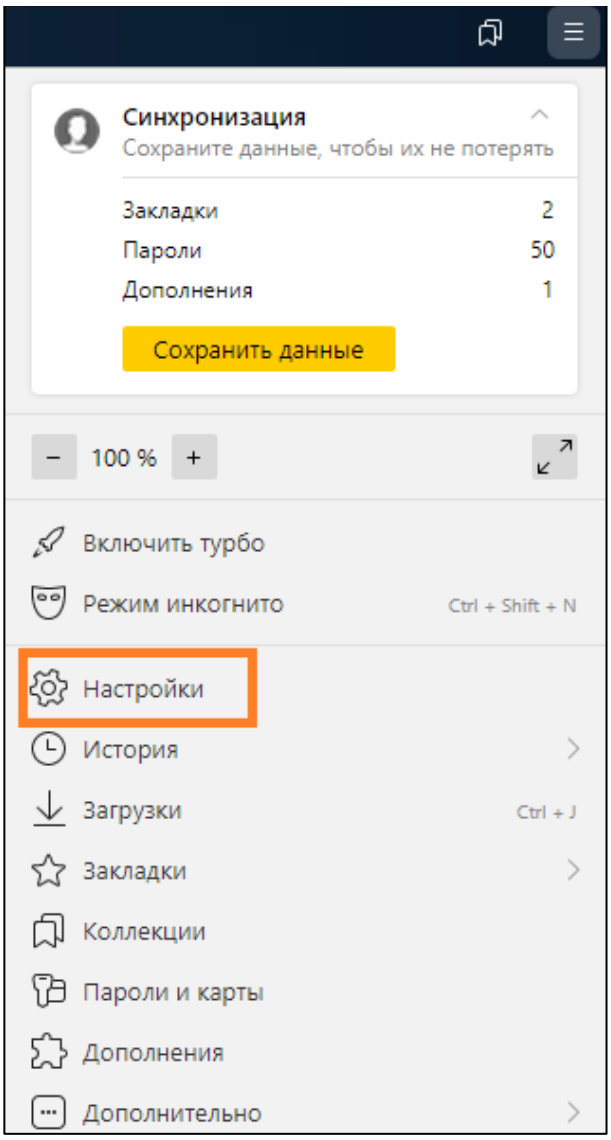


Рисунок 31 – Открытие настроек браузера

3. В панели навигации открыть раздел «Системные»;

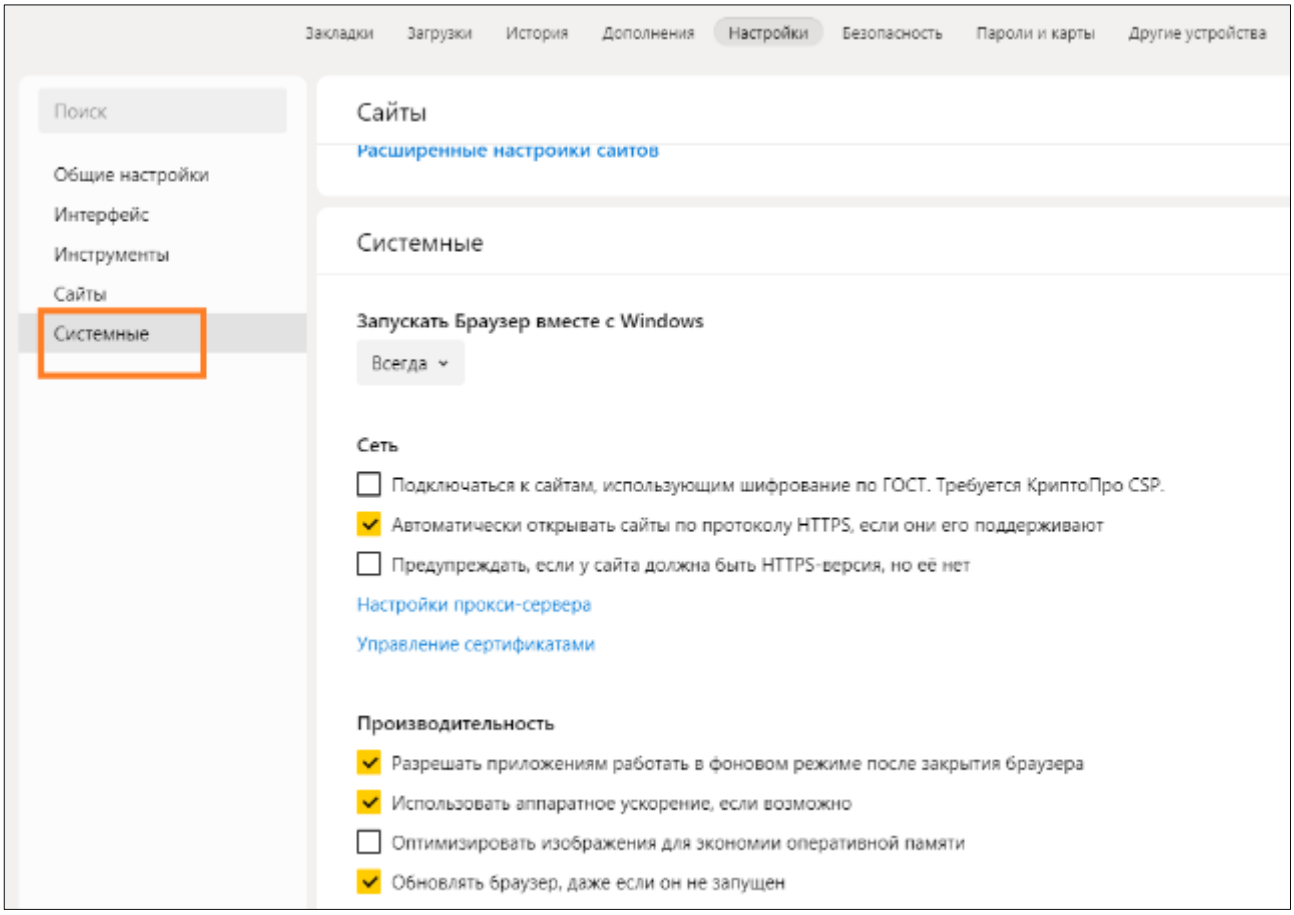


Рисунок 32 – Открытие системных настроек браузера

4. Включите чекбокс «Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется КриптоПро CSP».

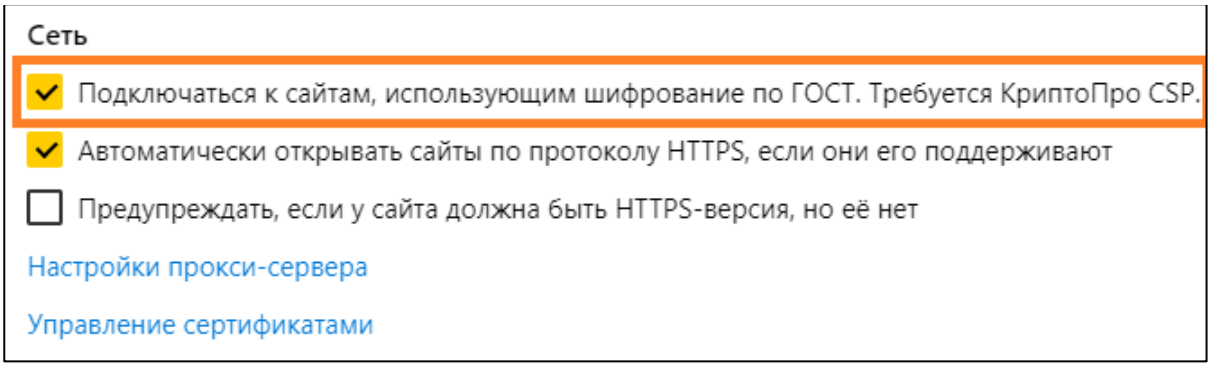


Рисунок 33 – Включение настройки браузера для подключения к сайтам, использующим шифрование по ГОСТ

3. РЕГИСТРАЦИЯ В ИС АОКЗ

В данной инструкции не рассматривается процедура регистрации в ПОИБ СОБИ ФК. При возникновении вопросов по работе в ПОИБ СОБИ ФК необходимо воспользоваться инструкциями, которые размещены на сайте Федерального казначейства https://roskazna.gov.ru в разделе «ГИС» – «Система обеспечения безопасности информации Федерального казначейства».

Для работы в ИС АОКЗ пользователю организации необходимо добавить роль «Сотрудник ОКИ» в ПОИБ СОБИ ФК.

Пользователю необходимо войти в ПОИБ СОБИ ФК по ссылке https://sobi.cert.roskazna.ru и выбрать свой сертификат для входа.

По умолчанию после входа открывается профиль пользователя.

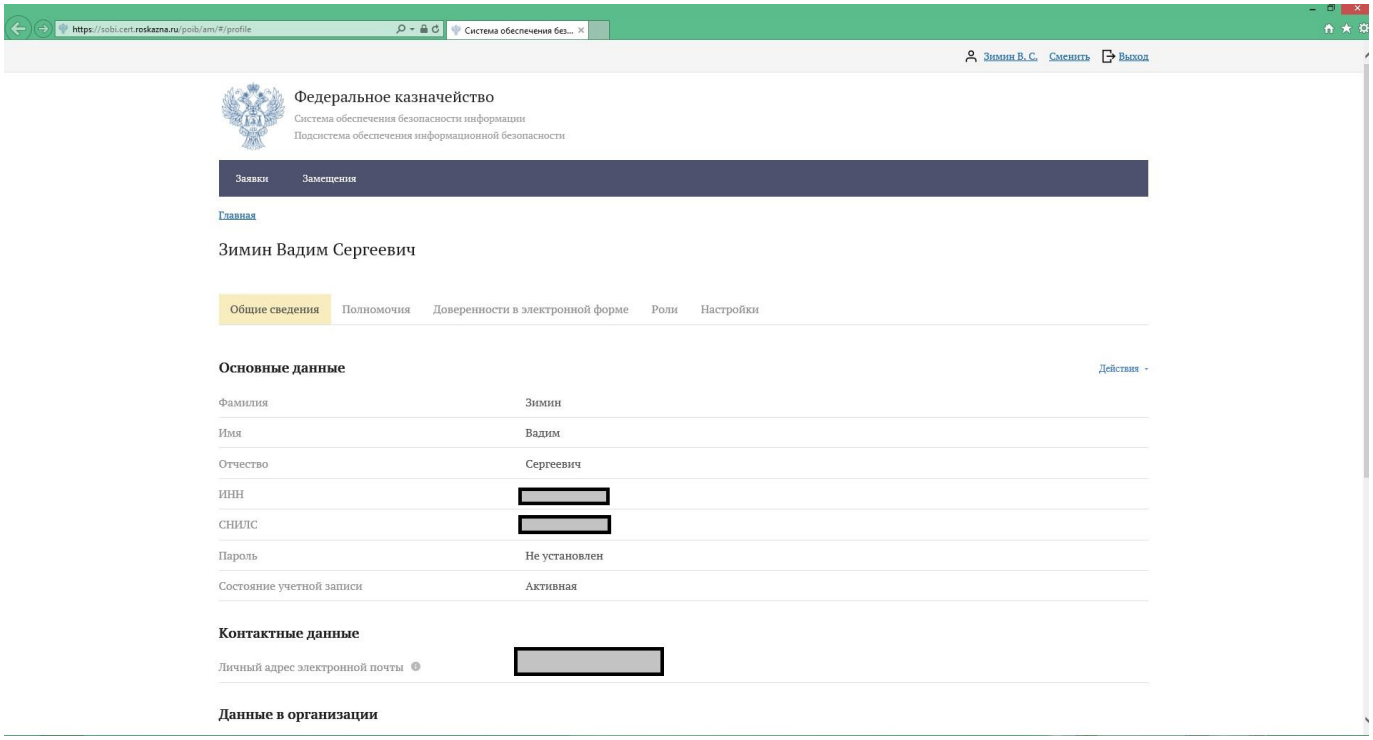


Рисунок 34 – Профиль пользователя в ПОИБ СОБИ ФК

Для изменения полномочий необходимо перейти на вкладку «Роли» и нажать кнопку «Изменить».

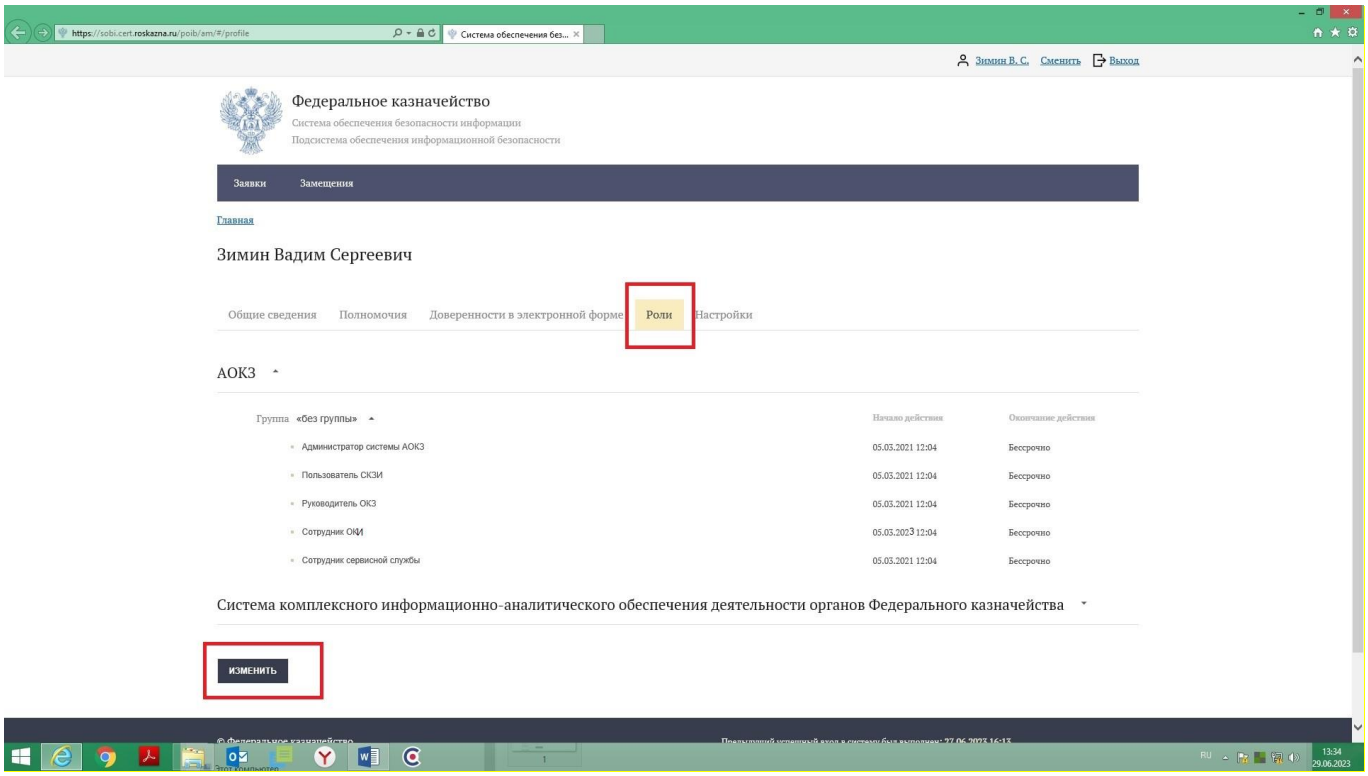


Рисунок 35 – Вкладка «Роли» в ПОИБ СОБИ ФК

В появившемся окне необходимо из выпадающего списка выбрать ИС АОКЗ, после чего отметить галочкой роль «Сотрудник ОКИ» и нажать кнопку «Продолжить».

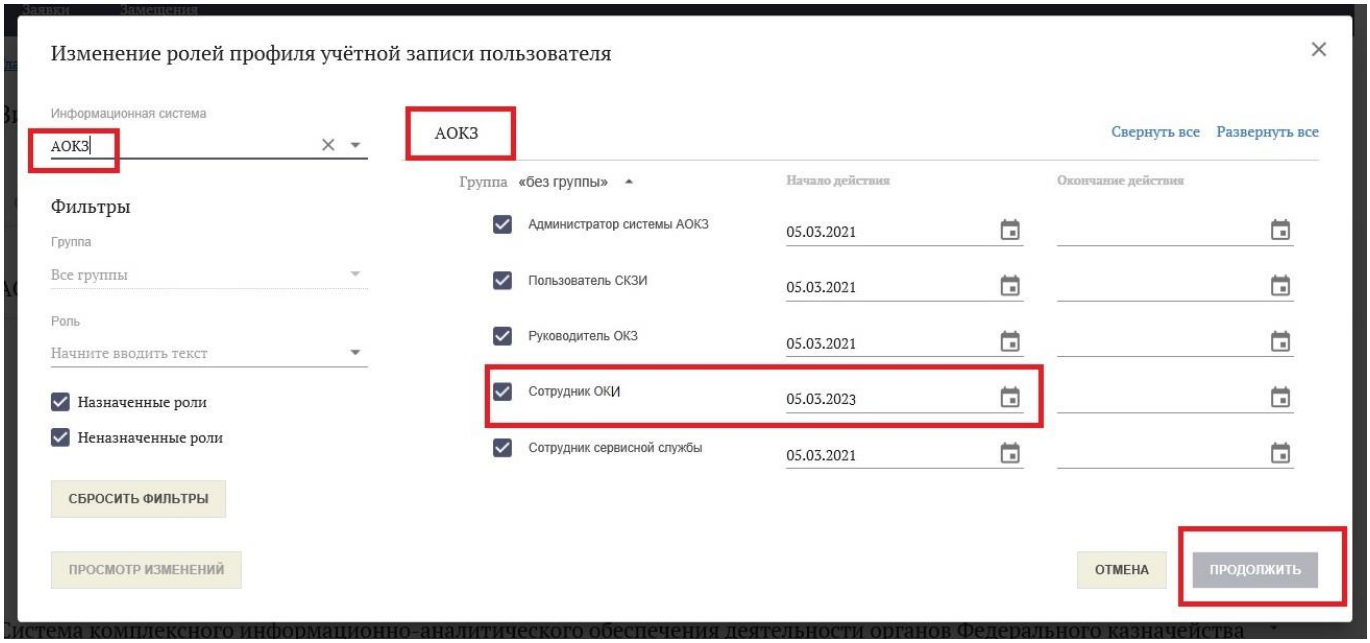


Рисунок 36 – Назначение роли «Сотрудник ОКИ» в ПОИБ СОБИ ФК

Далее необходимо выбрать свой сертификат (при наличии нескольких действующих сертификатов выбирается любой из них) и нажать кнопку «Подписать».

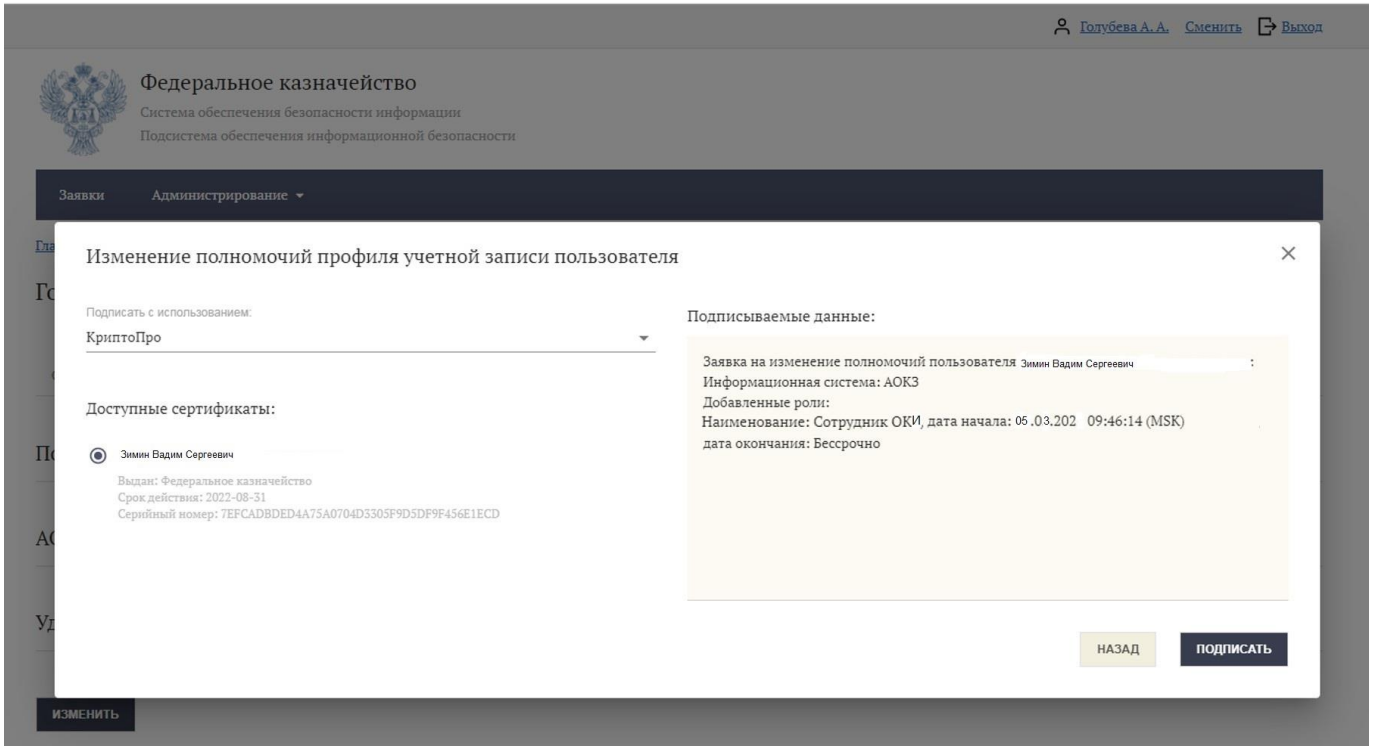


Рисунок 37 – Формирование заявки на изменение полномочий пользователя

После успешного подписания заявки система выдает сообщение, что заявка принята. После создания заявка поступает на утверждение Регистратору организации.

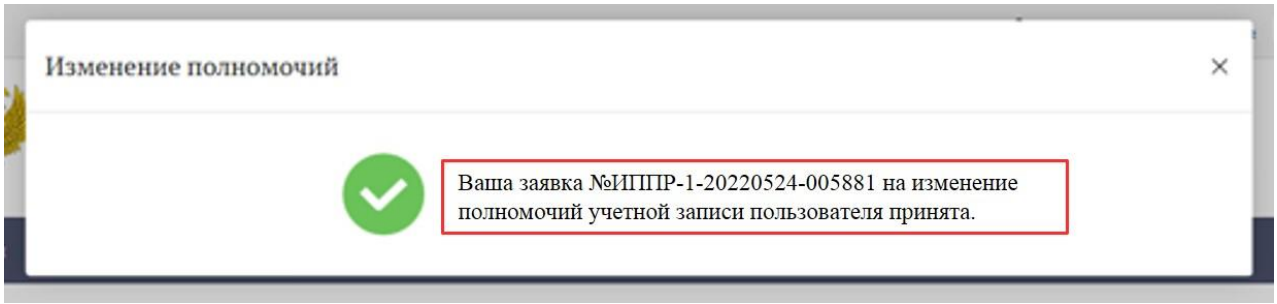


Рисунок 38 – Заявка на изменение полномочий пользователя

Перечень всех заявок можно просмотреть в разделе «Заявки» ПОИБ СОБИ ФК.

После утверждения заявки в ПОИБ СОБИ ФК Регистратором на адрес электронной почты пользователя, указанный при регистрации, придет сообщение об исполнении заявки.

4. ПОРЯДОК РАБОТЫ В ИС АОКЗ

Для работы в ИС АОКЗ необходимо перейти по одной из следующих ссылок:

– https://aokz.cert.roskazna.ru – вход по сертификату;

– https://aokz.login.roskazna.ru – вход по логину и паролю.

Интерфейс ИС АОКЗ содержит следующие разделы:

- Экземпляры СКЗИ
- Лицензии

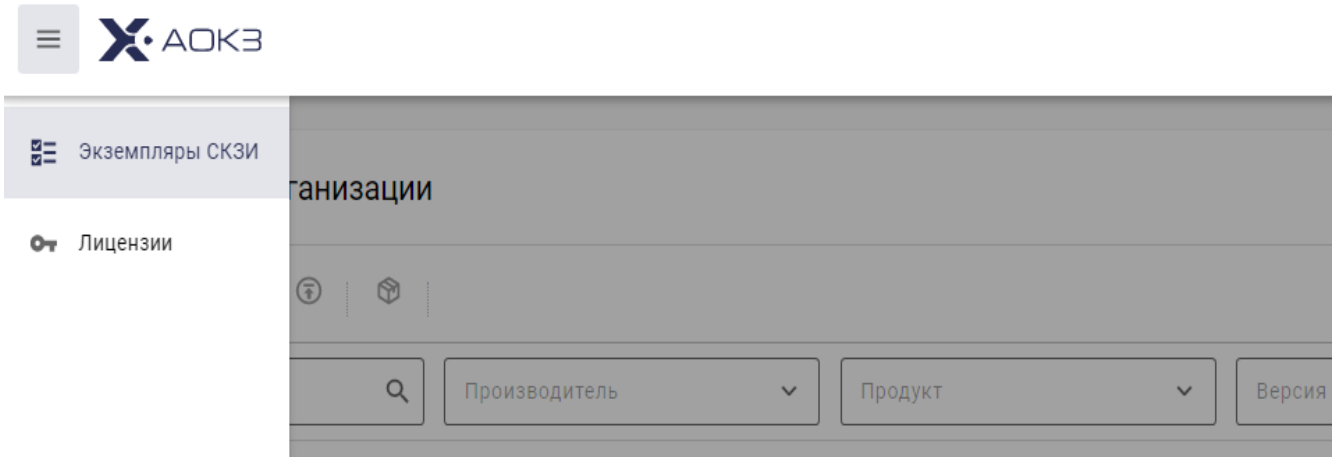


Рисунок 39 – Разделы ИС АОКЗ

4.1. Раздел «Экземпляры СКЗИ»

В разделе «Экземпляры СКЗИ» содержится полный список экземпляров СКЗИ, переданных в Организацию.

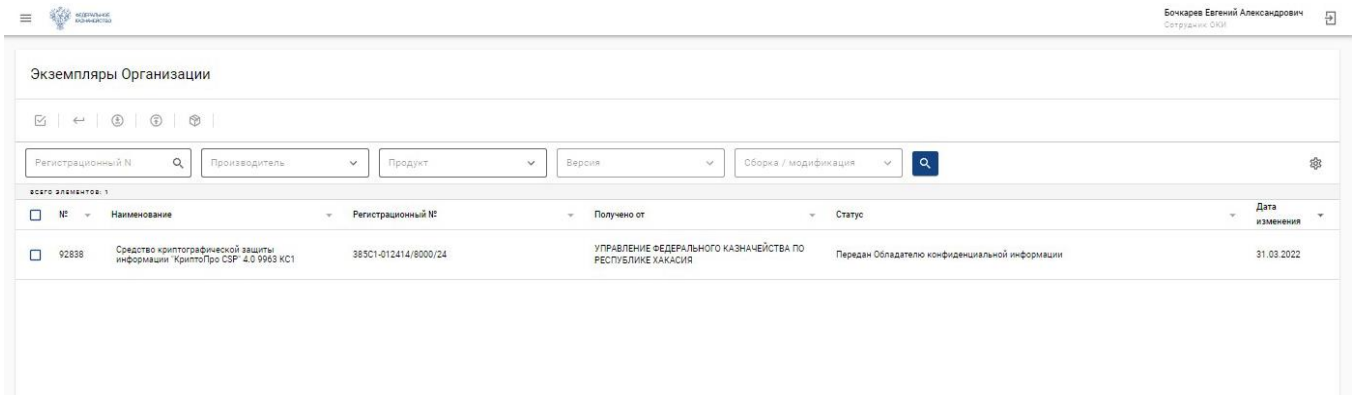


Рисунок 40 – Раздел «Экземпляры СКЗИ»

Для просмотра детальной информации об экземпляре СКЗИ, необходимо нажать на соответствующую строку в табличном представлении. В карточке экземпляра СКЗИ можно просмотреть общие данные об экземпляре СКЗИ, привязанные к экземпляру СКЗИ лицензии и информацию о мероприятиях, выполненных с данным экземпляром.

Карточка экземпляра содержит следующие разделы:

- Информация;
- Мероприятия;
- Лицензии;
- История.

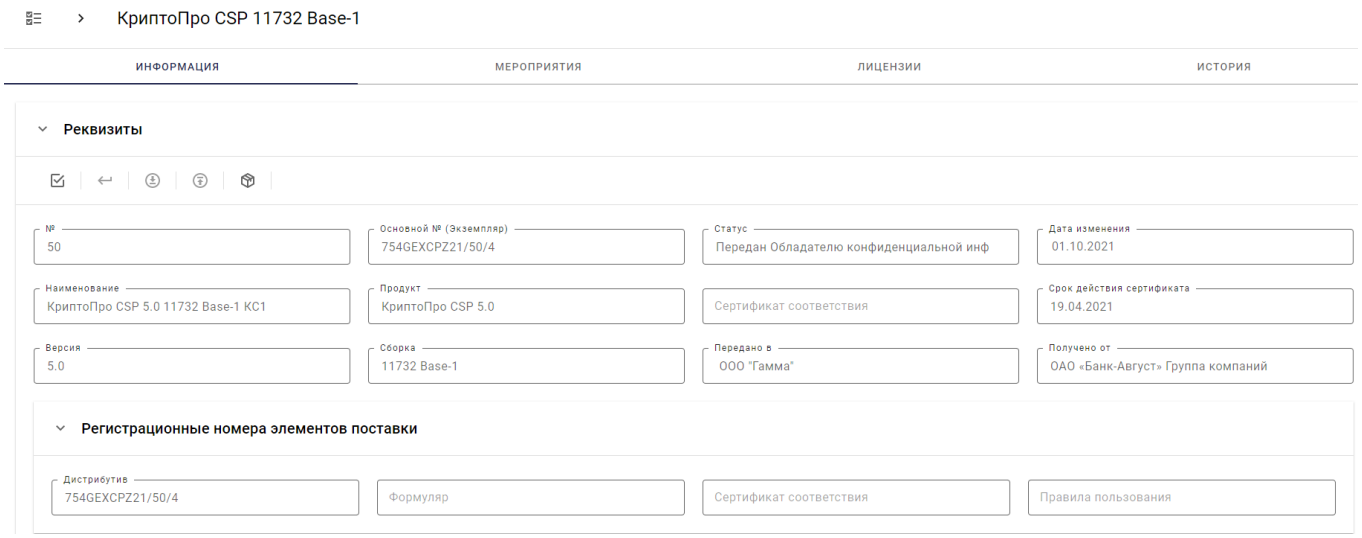


Рисунок 41 – Вкладка «Информация» карточки экземпляра СКЗИ

В разделе «Информация» представлены основные данные экземпляра СКЗИ. Для того, чтобы ознакомиться с комплектом поставки дистрибутива, необходимо нажать на кнопку . Для скачивания дистрибутива в открывшемся диалоговом окне выбрать файл или нажать на кнопку «Скачать все» для скачивания комплекта поставки СКЗИ целиком.

В разделе «Мероприятия» отображаются действия, выполненные с экземпляром СКЗИ с момента передачи экземпляра СКЗИ в Организацию.

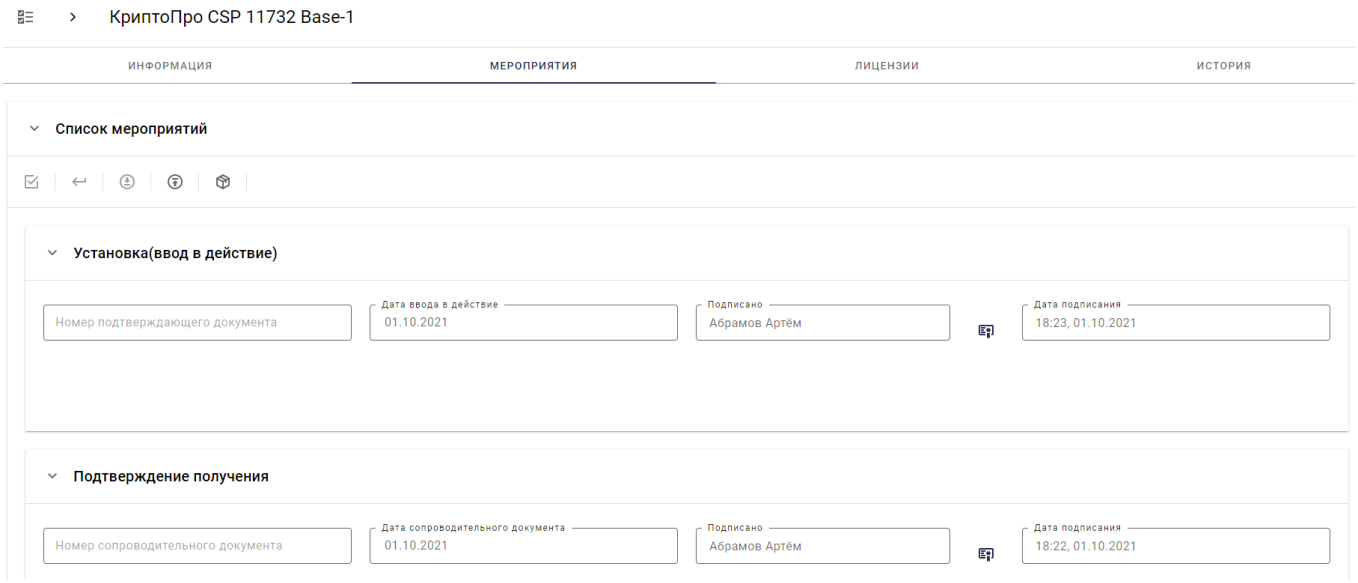


Рисунок 42 – Вкладка «Мероприятия» карточки экземпляра СКЗИ

В разделе «Лицензии» отображается список лицензий, переданных в Организацию совместно с указанным экземпляром СКЗИ или привязанных к нему вручную. Нажав на строку с лицензией, система переведет на страницу, где можно просмотреть лицензионный ключ, нажав на кнопку .

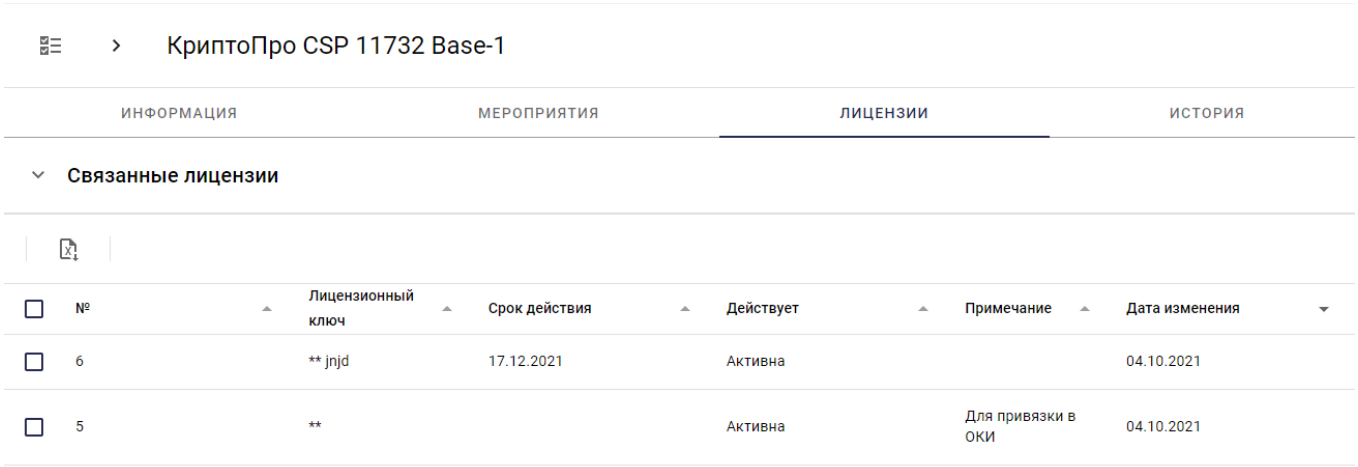


Рисунок 43 – Вкладка «Лицензии» карточки экземпляра СКЗИ

4.2. Управление экземплярами СКЗИ

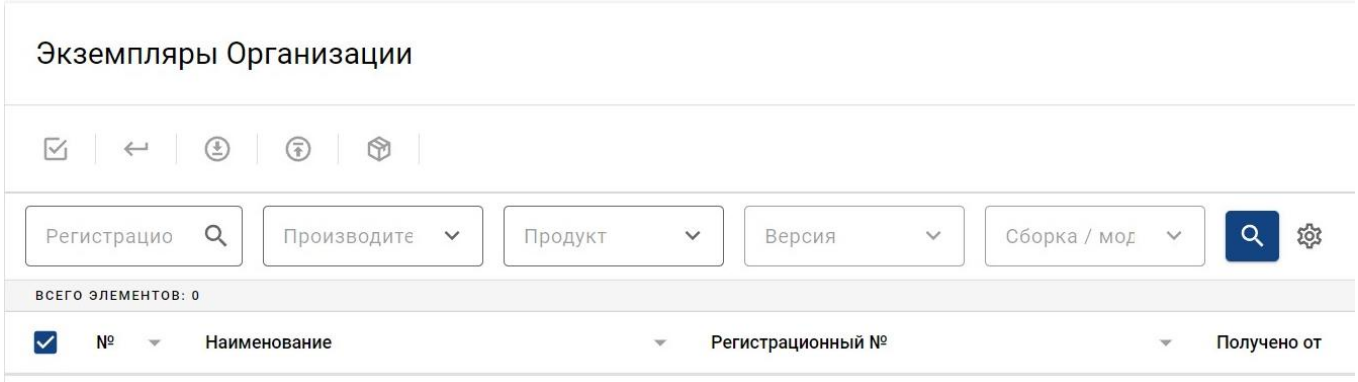


Рисунок 44 – Поля поиска экземпляров СКЗИ

Для перевода экземпляра СКЗИ в следующий статус по бизнес-процессу, необходимо в разделе «Экземпляры» выбрать экземпляр СКЗИ и нажать на необходимую кнопку перехода:

	Подтверждение получения экземпляра СКЗИ.
	Сообщить, что указанный экземпляр СКЗИ был введён в действие.
	Сообщить, что указанный экземпляр СКЗИ был выведен из действия.

↵	Вернуть экземпляр СКЗИ.

Также есть возможность выполнить данные мероприятия в карточке экземпляра СКЗИ. Для этого откройте карточку экземпляра СКЗИ, выбрав его в списке, и нажмите на кнопку перехода в соответствующий статус.

Ниже в таблице приведен перечень действий и уточняющие сведения, которые указываются при выполнении действий с экземплярами СКЗИ.

Действие	Уточняющие сведения
Подтверждение получения	Дата сопроводительного документа; Номер сопроводительного документа.
Установка (Ввод в действие)	Дата ввода в действие; Номер подтверждающего документа.
Изъятие (Вывод из действия)	Дата изъятия; Номер подтверждающего документа.
Возврат	Номер сопроводительного документа; Дата сопроводительного документа.

5. РАЗДЕЛ «ЛИЦЕНЗИИ»

В разделе «Лицензии» отображен список лицензий на экземпляры СКЗИ в виде таблицы.

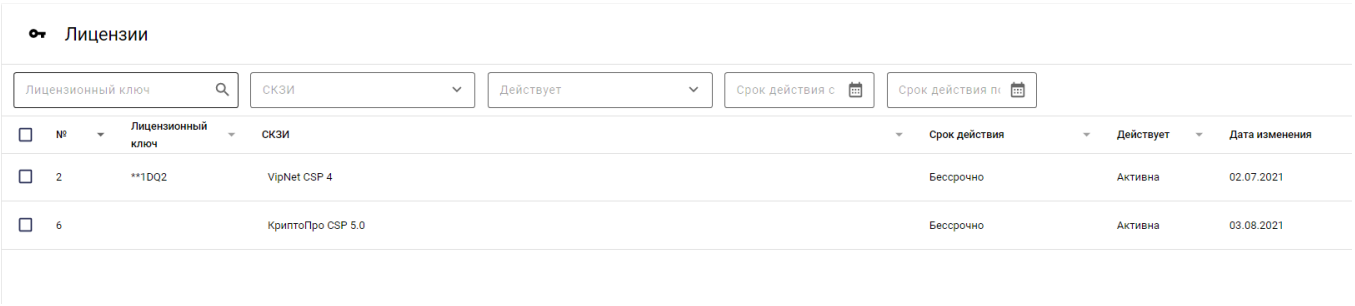


Рисунок 45 – Раздел «Лицензии» ИС АОКЗ

Наименования столбцов таблицы имеют следующие значения:

«№» — порядковый номер лицении в списке;

«Лицензионный ключ» — лицензионный ключ;

«СКЗИ» — наименование, версия и сборка экземпляра СКЗИ;

«Срок действия» — срок действия лицензии;

«Действует» — статус лицензии;

«Дата изменения» — дата изменения данных лицензии.

Предусмотрена возможность фильтрации списка лицензий согласно данным выбранного столбца.

В карточке лицензии можно просмотреть общие данные о лицензии, приложенные к лицензии файлы, а также привязанные к лицензии экземпляры СКЗИ.

6. ВЫХОД ИЗ СИСТЕМЫ

Для выхода из ИС АОКЗ необходимо нажать на кнопку «Выход из системы» и перезапустить браузер.