****

**Государственная информационная система
«Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»**

**ИНСТРУКЦИЯ**

**по использованию электронной подписи в ГИС ТОР КНД**

Москва

2021 г.

## **Список понятий и сокращений**

|  |  |  |
| --- | --- | --- |
| **№** | **Понятия и сокращения**  | **Расшифровка/определение**  |
| **1** | **ГИС ТОР КНД**  | **Государственной информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»** |
| **2** | **ЭП** | **Электронная подпись** |
| **3** | **Криптопровайдер**  | **Дополнительное программное обеспечение, которое позволяет инициировать работу сертификатов ЭП и осуществлять криптографические операции в операционных системах, устанавливаемое на локальный компьютер** |
| **4** | **Корневой сертификат** | **Корневой сертификат (контейнер закрытого ключа) — часть ключа, которым центры сертификации подписывают выпущенные SSL-сертификаты.**  |
| **5** | **Сертификат ЭП** | **Документ, который подтверждает, что данная подпись принадлежит его владельцу. Выдается только удостоверяющими центрами (центрами сертификации).** |
| **6** | **Удостоверяющий центр**  | **Удостоверяющий центр (УЦ) – доверенная организация, которая имеет право выпускать сертификаты электронной подписи юридическим и физическим лицам.** |
| **7** | **КНО** | **Контрольный (надзорный) орган** |
| **8** | **Усиленная квалифицированная ЭП (УКЭП)** | **ЭП, для создания и проверки которой используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным законом "Об электронной подписи" от 06.04.2011 N 63-ФЗ** |
| **9** | **Отсоединенная ЭП**  | **ЭП, которая формируется в отдельном от подписываемого документа файла. Файл подписи называется так же, как подписанный документ и имеет расширение. sig. Для проверки действительности подписи нужно оба файла.** |

## **Общие сведения**

В ГИС ТОР КНД реализована функция использования ЭП для работы инспекторов и руководителей КНО, расширяющая возможности работы с документами
с использованием криптографических мер безопасности и передачи данных о подписи Для работы с цифровой подписью в системе ГИС ТОР КНД необходимо иметь предустановленный на автоматизированном рабочем месте оператора **криптопровайдер.** ГИС ТОР КНД предоставляет возможность работы в системе с любым сертифицированным в РФ криптопровайдером.

Для функционирования ЭП в браузере необходим **дополнительный плагин** - C**AdES Browser plugin** от компании CryptoPro. Помимо этого, для работы необходим **контейнер закрытого ключа (корневой сертификат)**, а также **сертификат электронной цифровой подписи**.

## **Требования к ЭП**

Для использования ЭП в системе ГИС ТОР КНД должностному лицу контрольного (надзорного) органа необходимо иметь в наличии **усиленную квалифицированную электронную подпись,** выданную удостоверяющим центром, аккредитованным Министерством цифрового развития связи и массовых коммуникаций Российской Федерации, в соответствии с законом 63-ФЗ.

Электронная подпись должна содержать информацию о КНО (юридическом лице) и её владельце.

Запись "CN" сертификата электронной подписи должна содержать наименование организации.

Запись "T" сертификата электронной подписи должна содержать должность владельца сертификата.

**Настройка браузера для работы с ЭП**

### **Предварительная настройка**

Для того, чтобы иметь возможность работать с ЭП в ГИС ТОР КНД, на локальном компьютере пользователя должен быть установлен криптопровайдер, контейнер закрытого ключа (корневой сертификат). В контейнере закрытого ключа должен находиться сертификат ЭП. Сотрудникам КНО необходимы действующие сертификаты УКЭП, используемые ими в трудовой деятельности и выданные сертифицированными **удостоверяющими центрами.**

**Шаг 1.** Необходимо удостовериться, что в интерфейсе локального криптопровайдера пользователя отображается информация о выданной электронной цифровой подписи (Рисунок 1. **Внимание: в качестве примера на рисунке приведен тестовый сертификат ЭП. Для работы должностных лиц в ГИС ТОР КНД необходим сертификат УКЭП, требования к которому описаны в разделе «**[**Требования к ЭП**](#_Требования_к_ЭП)**»**).

В качестве примера демонстрируется криптопровайдер CryptoPro SCP. Данный криптопровайдер сертифицирован ФСБ России как средство криптографической защиты информации. Возможно использование любого другого криптопровайдера, лицензированного для работы на территории РФ



*Рисунок 1 –* *информация о сертификате в интерфейсе криптопровайдера «КриптоПро CSP»*

### **Установка CAdES Browser plugin**

Данный плагин представляет из себя расширение, позволяющее осуществлять работу с ЭП непосредственно через браузер. Предполагается, что перед установкой плагина в системе уже установлен локальный криптопровайдер, корневой сертификат и сертификат ЭП. Данный плагин взаимодействует с криптопровайдером и получает от него информацию об ЭП. Создание ЭП для документа (вычисление хэша в соответствии с ГОСТ Р 34.11-2012 и шифрование на закрытом ключе пользователя в соответствии с ГОСТ Р 34.10-2012) происходит на локальном компьютере пользователя и с помощью данного плагина предается в веб-среду.

**Шаг 1***.* Чтобы скачать .exe данного файла, необходимо перейти по следующей ссылке в браузере:

<https://cryptopro.ru/products/cades/plugin/get_2_0>

**Шаг 2.** Необходимо произвести установку, запустив .exe файл. Плагин установится в браузер, заданный в системе по умолчанию. Необходимо будет перезагрузить браузер.

**Шаг 3***.* После перезагрузки браузера, необходимо перейти в управление расширениями (для примера используется браузер Chrome), для этого необходимо открыть список установленных в браузере расширений, кликнув на иконку «Пазл» в верхнем правом углу « » . Далее – «Управление расширениями»;

**Шаг 4***.* Убедиться, что расширение «CryptoPro Extension for CAdES Browser Plug-in» включено. Включить его при необходимости (Рисунок 2).



*Рисунок 2 – Расширение «CryptoPro Extension for CAdES Browser Plug-in в Chrome»*

**Шаг 5.** Убедиться, что расширение «CryptoPro Extension for CAdES Browser Plug-in» отображает информацию о сертификате локальной ЭП. Для этого необходимо открыть данное расширение в браузере, нажав на значок  (Рисунок 3), после чего раскрыть расширение и вызвать функцию «Проверить работу плагина» (Рисунок 4).



*Рисунок 3 – Информация о расширении в браузере*



*Рисунок 4 – «Проверить работу плагина»*

**Шаг 6.** Необходимо разрешить операцию работы с криптографическими протоколами в браузере (Рисунок 4).



*Рисунок 4 – «Предупреждение браузера»*

**Шаг 7.** Убедиться, что расширение «CryptoPro Extension for CAdES Browser Plug-in» отображает актуальную информацию об сертификате ЭП (Рисунок 5).



*Рисунок 5 – «Информация об сертификате ЭП в интерфейсе «CryptoPro Extension for CAdES Browser Plug-in»*

## **Использование ЭП в ГИС ТОР КНД**

**Шаг 1.** Для работы с ЭП в ГИС ТОР КНД необходимо открыть КНМ, с которой работает пользователь, и подписать документ, доступный пользователю-владельцу ЭП. Для этого необходимо в главном меню ГИС ТОР КНД открыть модуль «Кабинет руководителя» или «Кабинет инспектора» (Рисунок 9). В данных модулях происходит подписание документов.

*Следует отметить, что плагин «CryptoPro Extension for CAdES Browser Plug-in» должен быть включен в браузере, в котором производится работа с ГИС ТОР КНД.*



*Рисунок 9 – Модули ГИС ТОР КНД для работы с ЭП*

**Шаг 2.** После перехода в один из данных модулей необходимо выбрать вкладку «Процессы», в которых происходит работа с КНМ (Рисунок 10). Затем выбрать произвольную проверку, кликнув на нее мышью 2 раза.



*Рисунок 10 – Вкладка «Процессы», содержащая список проверок КНО.*

**Шаг 3.** На странице информации о проверке необходимо выбрать раздел «Документы». В появившемся списке документа найти нужный документ (Рисунок 11).



*Рисунок 11 – Раздел «Документы»*

**Шаг 4.**У выбранного документа необходимо кликнуть на цифру количества документов рядом с надписью «Файлы» , либо нажать на значок «Редактировать»  напротив нужного документа. После этого появится список всех выгруженных из ГИС ТОР КНД документов (Рисунок 12). Рядом с каждым будет кнопка «Подписать».



*Рисунок 12 – Список выгруженных файлов выбранного документа*.

**Шаг 5**. Следует нажать на кнопку «Подписать». Будет произведено подписание документа с помощью ЭП. Появится предупреждение браузера (Рисунок 13). Необходимо нажать «Да».



*Рисунок 4 – «Предупреждение браузера»*

**Шаг 6***.* После разрешения операции появится окно выбора сертификата электронной подписи (Рисунок 14). Необходимо выбрать сертификат и нажать на кнопку «Выбрать».



*Рисунок 14 – Выбор сертификата*

В результате произведенного действия выбранный экземпляр документа будет подписан ЭП. Данные об этом будут отображаться в системе (Рисунок 15).



*Рисунок 15 – Подписанный документ*

Помимо самого документа, в системе для выгрузки будет доступен файл с расширением «.sig» - . Данный файл будет являться **отсоединенной ЭП**. Он содержит информацию о сертификате ЭП данной версии документа и позволяет проверить его актуальность.

**Шаг 7.** Необходимо нажать на кнопку «Проверить». Появится результат
(Рисунок 16).



*Рисунок 16 – Результат проверки валидности подписи документа*

**Шаг 8***.* После подписания документа в системе ГИС ТОР КНД, необходимо нажать кнопки  и . Результатом данной операции будет сохранение подписанного документа и sig-файла его электронной цифровой подписи в среде системы.