

I.00.000.133-004

**Электронная подпись**  
**Настройка системы**  
**Инструкция администратора**

2017

**Электронная подпись. Настройка системы**  
Инструкция администратора  
Версия документа I.00.000.133-004



**В зависимости от версии работа Системы может отличаться от приведенного описания. За более актуальной информацией обратитесь к справочной системе**

## Содержание

1	Настройка Системы для работы с ЭП.....	4
1.1.	Переустановка сертификатов пользователя.....	4
1.2.	Установка ПО для использования электронной подписи для работы в операционной системе Windows .....	11
1.3.	Установка ПО для использования электронной подписи для работы в операционной системе Linux .....	12
1.4.	Загрузка сертификатов пользователей.....	13

# 1 Настройка Системы для работы с ЭП

**Внимание!** Последние версии браузеров прекратили поддержку Java, в связи с этим необходимо переустановить компоненты для использования электронной подписи.

Для использования электронной подписи:

1. Установите последнюю версию FireFox (не ESR, не CryptoFox, не portable-версию).
2. Загрузите с сайта КриптоПро и установите последнюю версию плагина <https://www.cryptopro.ru/products/cades/plugin> (версия 2.0 для пользователей).
3. Установите расширение для браузера FireFox с сайта КриптоПро [https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox\\_cryptopro\\_extension\\_latest.xpi](https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi).
4. Для каждой учетной записи пользователя Системы, который использует электронную подпись, установите сертификат: Сервис – Пользователи - в свойствах пользователя «Сертификаты» – кнопка «Добавить»;
5. Перезапустите Firefox, заново авторизуйтесь в Системе под учетной записью пользователя.

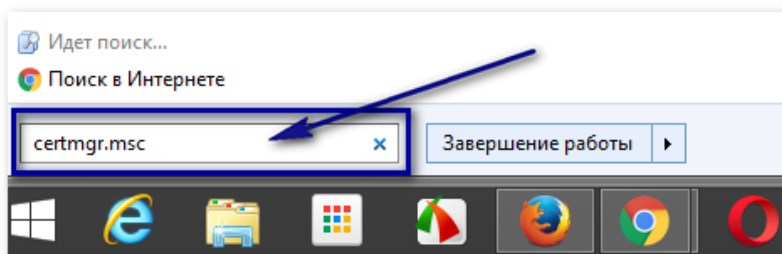
**Важно!** Если ранее были установлены сертификаты в хранилище на ПК, необходимо их сохранить, и повторно добавить для учетной записи пользователя. Подробное описание см. п. 1.1.

## 1.1. Переустановка сертификатов пользователя

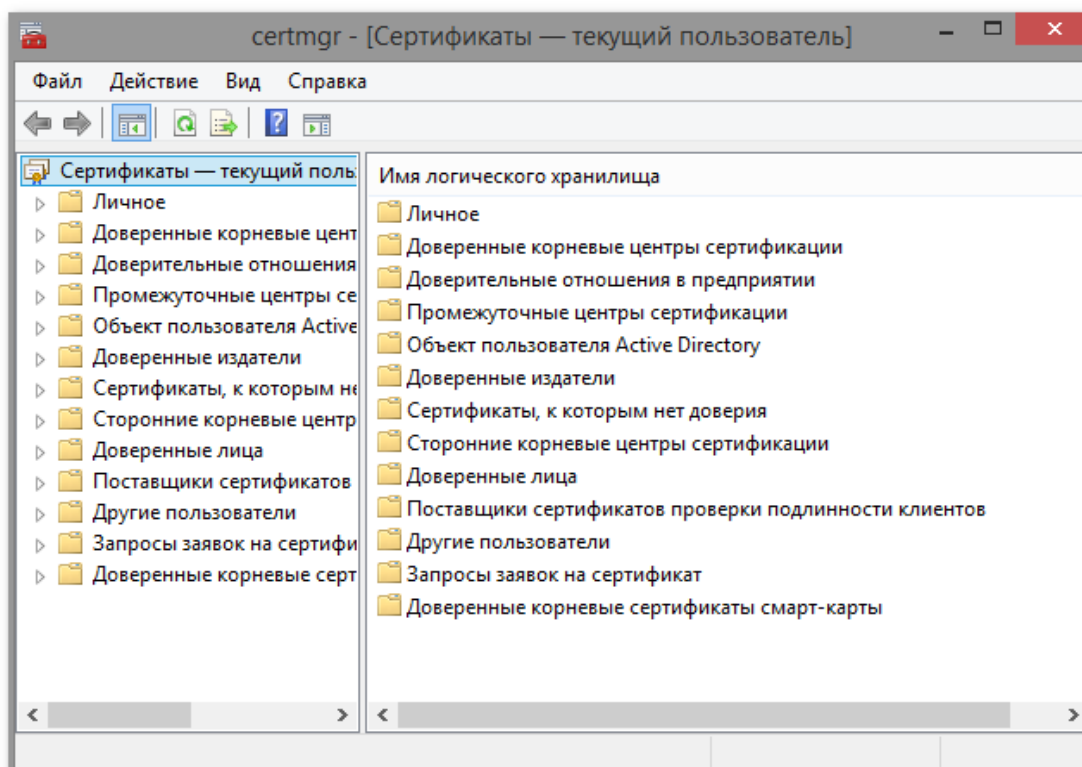
Если ранее на системе были установлены сертификаты в хранилище ОС, необходимо их экспортировать и установить для учетной записи пользователя Системы.

Для этого:

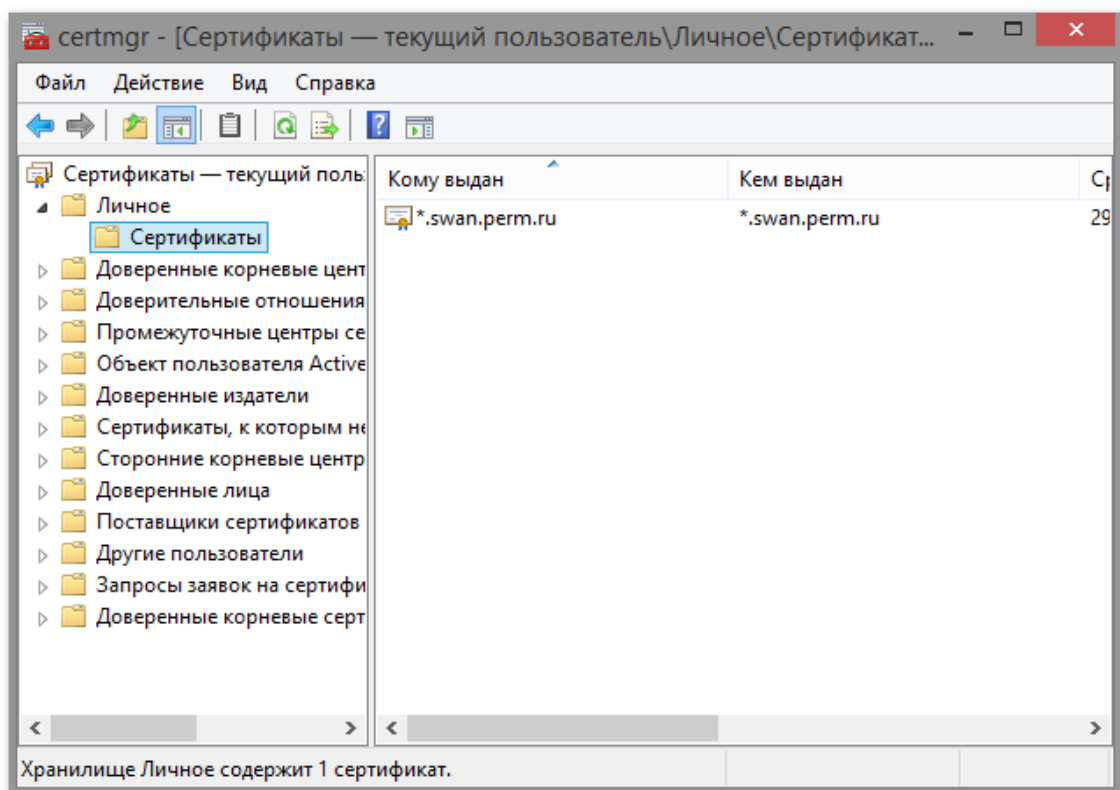
1. Нажмите кнопку **Пуск**.
2. Введите в строке **certmgr.msc** и нажмите кнопку **Enter**.



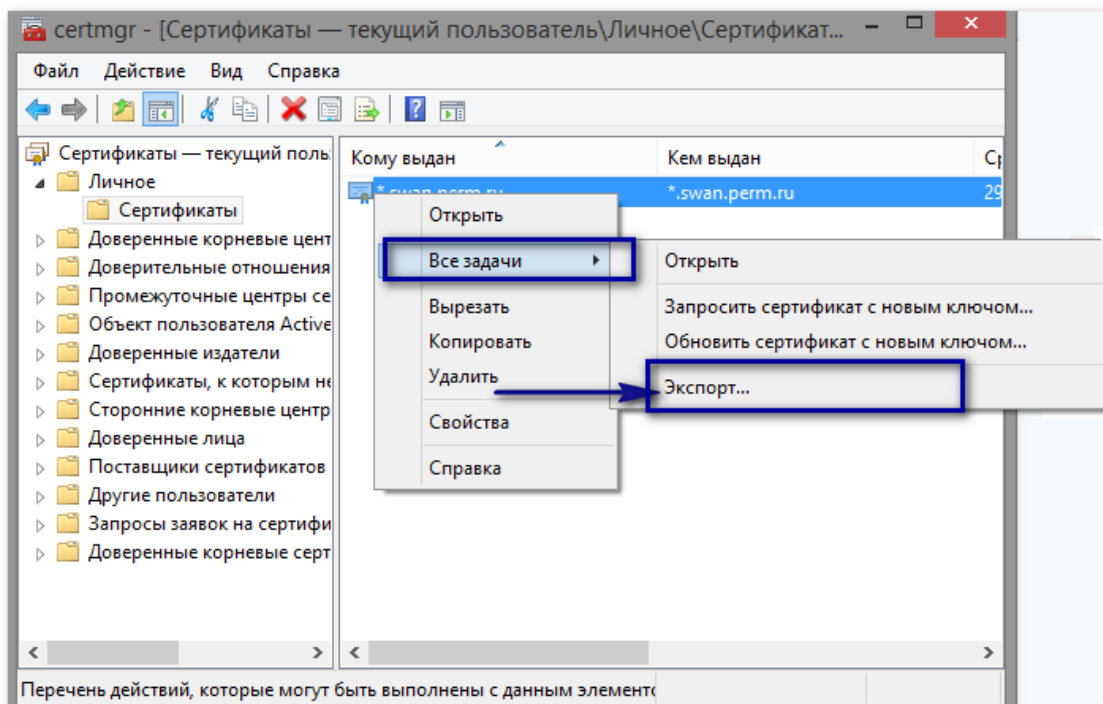
Отобразится форма работа с сертификатами.



3. Раскройте папку **Личное, Сертификаты**. В области справа отобразится перечень сертификатов пользователей данного ПК.



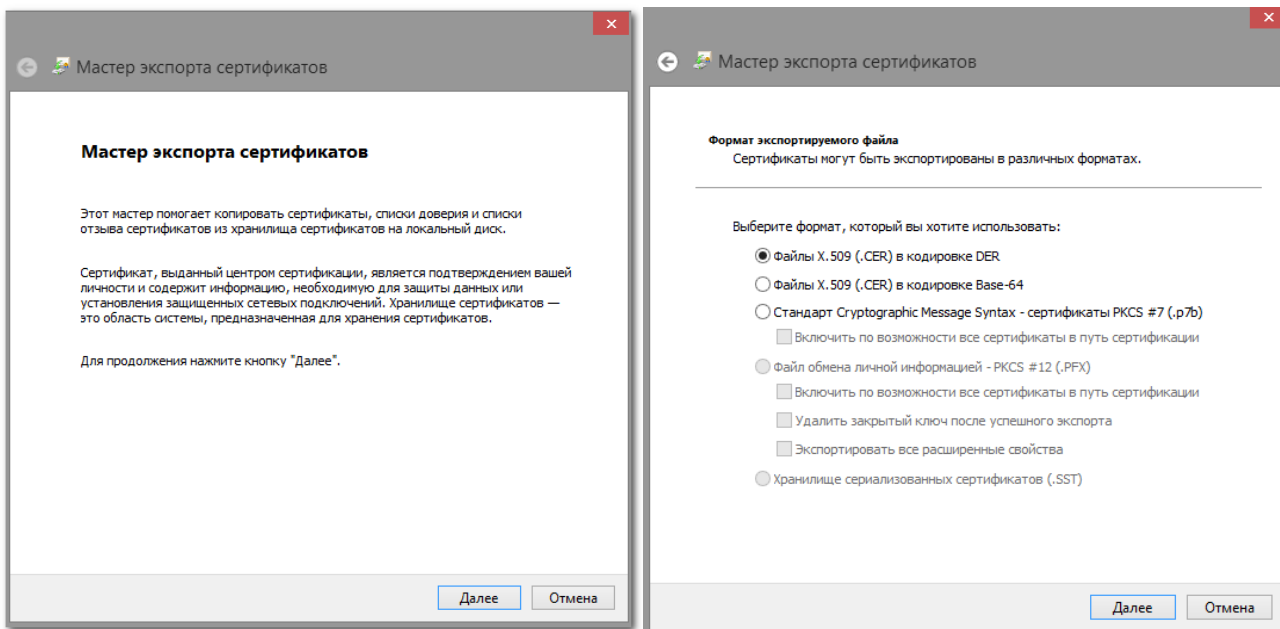
4. Нажмите правой кнопкой мыши на записи с сертификатом, который надо экспортировать. Отобразится контекстное меню.



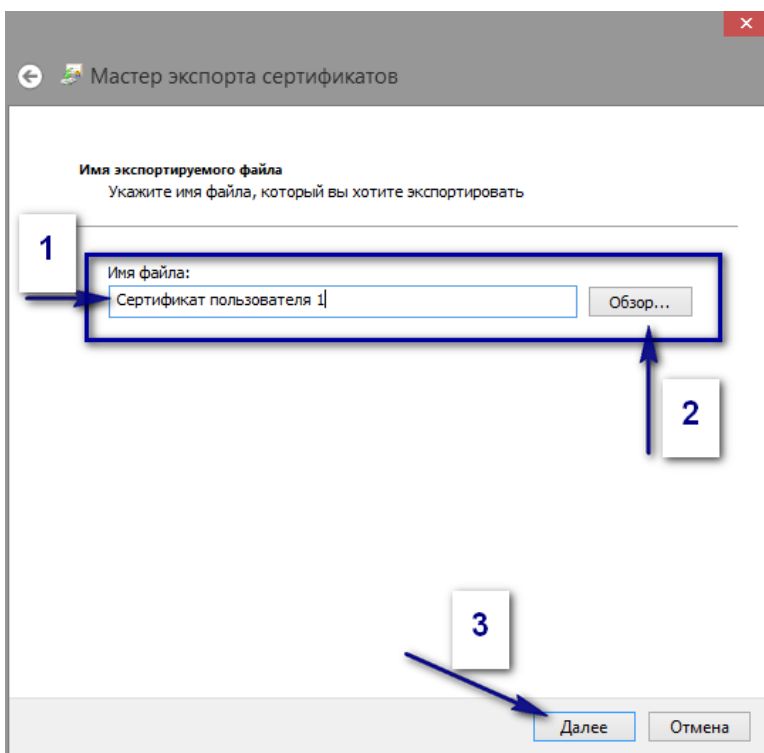
5. Выберите пункт **Все задачи – Экспорт**. Запустится **Мастер экспорта сертификатов**.

Примечание – Содержимое меню может отличаться в зависимости от типа операционной системы на ПК пользователя.

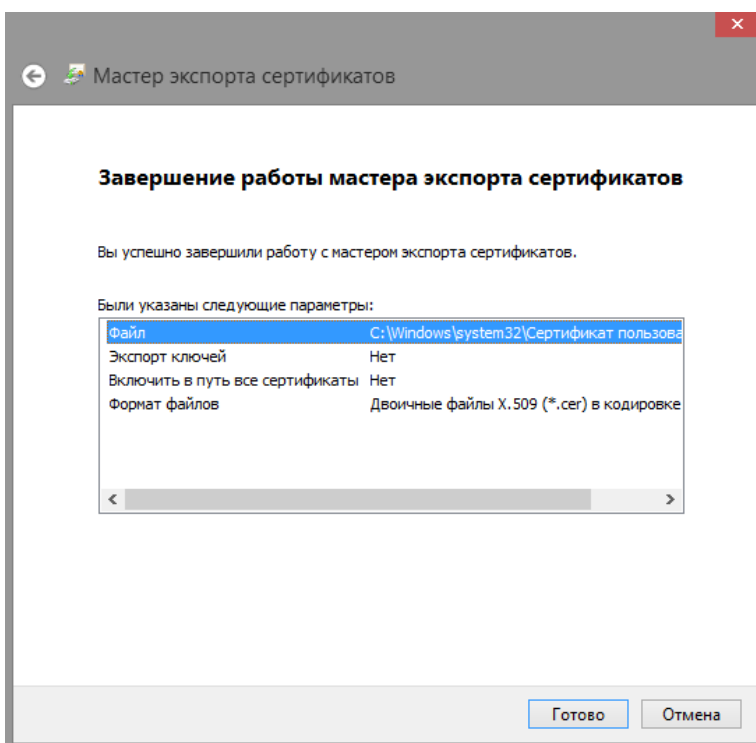
6. Следуйте указаниям Мастера, выгрузите сертификат. Для перехода между шагами Мастера используйте кнопку **Далее**. Значения параметров оставьте по умолчанию.



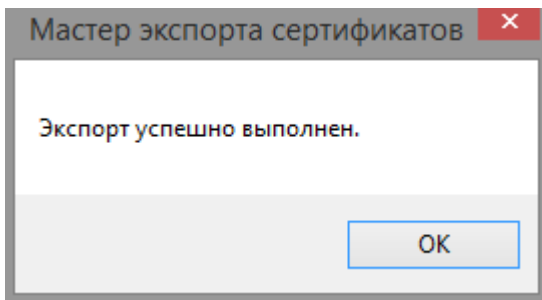
7. Укажите наименование для файла-сертификата в поле **Имя файла**, нажмите кнопку **Обзор** чтобы задать место для сохранения файла на ПК, например, «Рабочий стол», нажмите кнопку **Далее**.



8. Завершите работу мастера с помощью кнопки **Готово**.



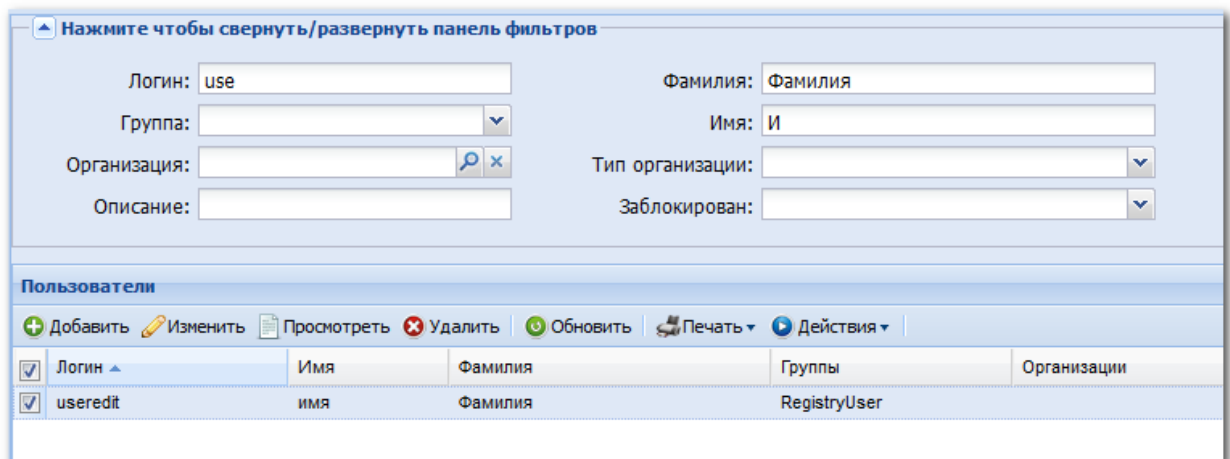
Информация о результате экспорта отобразится на экране.



**Добавьте экспортируемый сертификат для учетной записи пользователя.**

Для этого:

1. Запустите Систему.
2. Выберите:
  - **Сервис – Пользователи** в главном меню Системы;
  - Кнопку **Пользователи** на боковой панели АРМ администратора ЦОД;
  - В АРМ администратора МО работа с пользователями выполняется на главной форме.
3. Найдите пользователя, используя поля фильтра.



4. Нажмите кнопку **Изменить**. Отобразится форма **Пользователь**.



Пользователь: Редактирование

1. Основное 2. Доступ к АРМ

Организация:

Наименование	Тип
Название не определено	

Логин:   Заблокирован Идент. МАРШа:

Временный пароль:

Токен:  До:

Сотрудник

Сотрудник:

Фамилия:  Полное имя:

Имя:  Эл. почта:

Отчество:  Описание:

Группы:

Группа	Описание
--------	----------

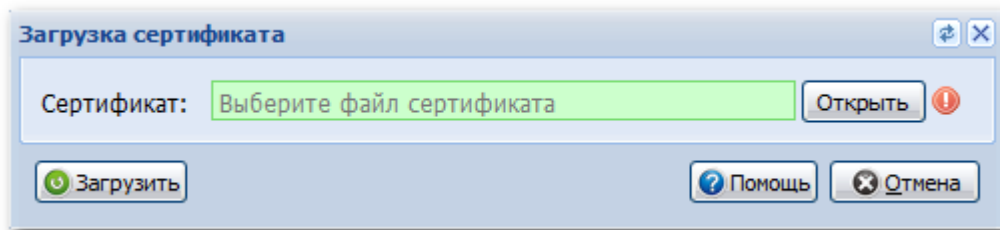
5. Нажмите кнопку **Сертификаты**. Отобразится форма для загрузки сертификатов.

Пользователь: Сертификаты

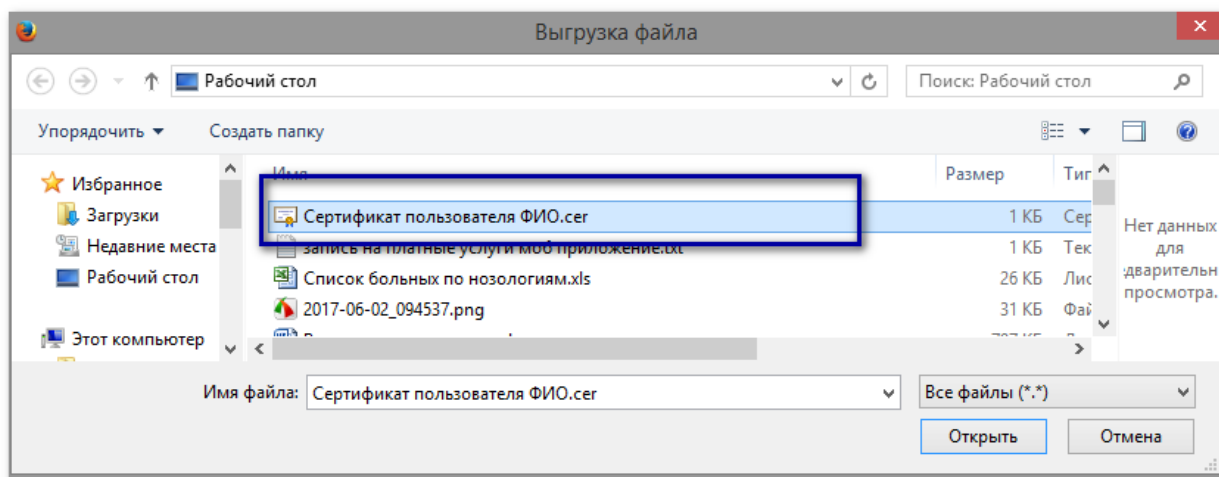
0 / 0

Название	SHA-1	Дата начала	Дата оконч...
----------	-------	-------------	---------------

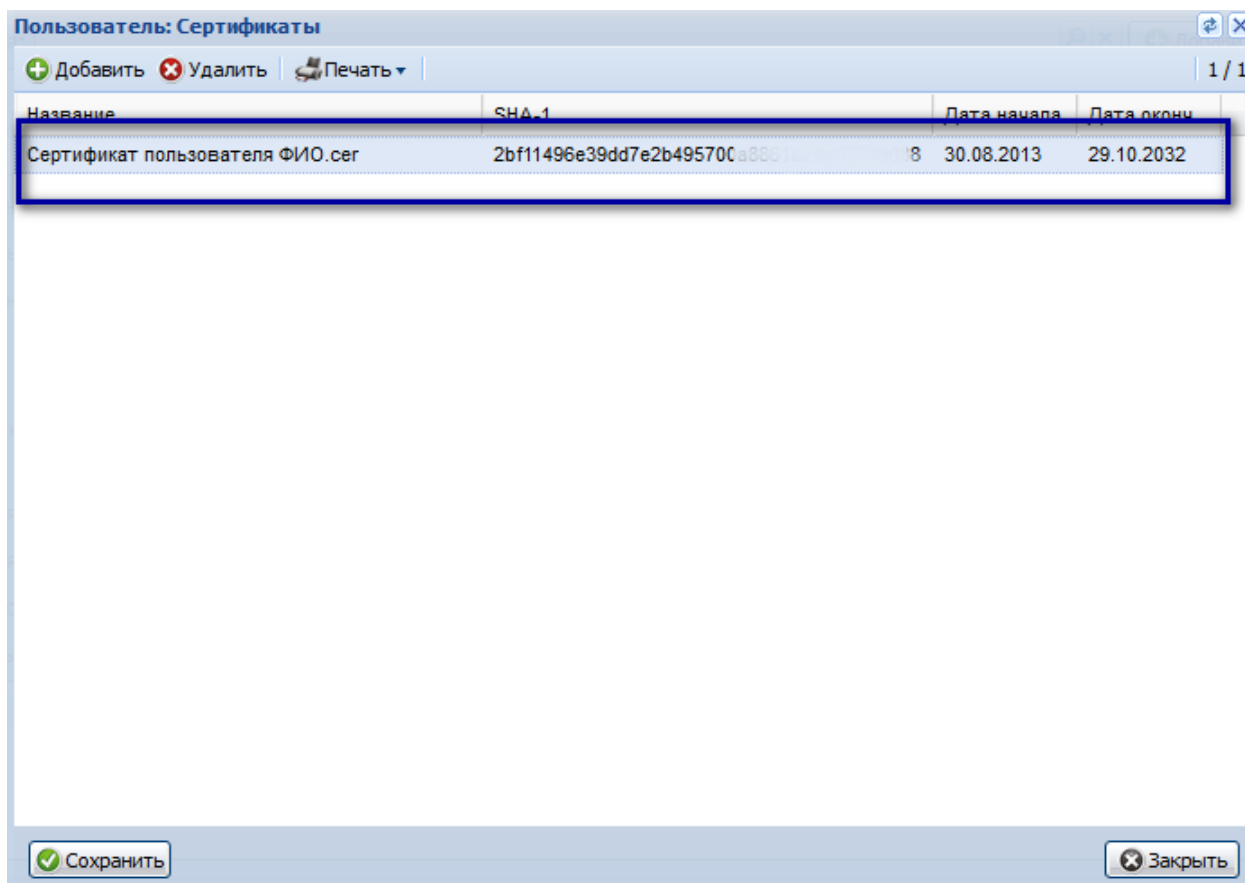
6. Нажмите кнопку **Добавить**. Отобразится форма **Загрузка сертификата**.



7. Укажите путь к файлу, который был экспортирован, с помощью кнопки **Открыть**.



8. Подтвердите загрузку с помощью кнопки **Загрузить**.  
Загруженный сертификат отобразится в списке.



9. Нажмите кнопку **Сохранить**. Сертификат будет добавлен для учетной записи пользователя.
10. Сохраните изменения для учетной записи пользователя.
11. Перезапустите браузер для работы в Системе, авторизуйтесь заново под учетной записью пользователя.

## 1.2. Установка ПО для использования электронной подписи для работы в операционной системе Windows

Если ранее не были установлены компоненты для применения ЭП, следует их установить:

1. Для работы плагина требуется установленный КриптоПро CSP версии 4.0 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке: <https://www.cryptopro.ru/products/csp/downloads>.
2. Плагин для установки доступен для загрузки с сайта производителя: [https://www.cryptopro.ru/sites/default/files/products/cades/current\\_release\\_2\\_0/cadesplugin.exe](https://www.cryptopro.ru/sites/default/files/products/cades/current_release_2_0/cadesplugin.exe)


3. Для браузера Chrome (Chromium) расширение для работы плагина устанавливается автоматически при перезапуске браузера. Для Firefox необходимо установить расширение по ссылке: [https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox\\_cryptopro\\_extension\\_latest.xpi](https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi).
4. Установите сертификат удостоверяющего центра.
5. Установите личный сертификат пользователя.
6. Загрузите сертификаты пользователя в Систему (описание см. ниже).

### 1.3. Установка ПО для использования электронной подписи для работы в операционной системе Linux

Если ранее не были установлены компоненты для применения ЭП, следует их установить:

1. Для работы плагина требуется установленный КриптоПро CSP версии 4.0 и выше. Дистрибутив и инструкцию по установке можно получить по ссылке: <https://www.cryptopro.ru/products/csp/downloads>. Для запуска установки распакуйте архив и запустите следующую команду в консоли:

```
sudo ./install.sh
```

 **Важно!** Для работы плагина должен быть установлен пакет **cprosp-rdr-gui-gtk**, при этом должен отсутствовать пакет **cprosp-rdr-gui**.

2. Плагин для установки доступен для загрузки с сайта производителя: <https://www.cryptopro.ru/products/cades/downloads> или по прямой ссылке: [https://www.cryptopro.ru/sites/default/files/products/cades/current\\_release\\_2\\_0/cades\\_linux\\_ia32.tar.gz](https://www.cryptopro.ru/sites/default/files/products/cades/current_release_2_0/cades_linux_ia32.tar.gz)
3. Для установки распакуйте архив и сконвертируйте все rpm-пакеты в deb-пакеты командой:

```
sudo alien -k название_пакета.rpm
```

При использовании некоторых 64 битных версий КриптоПро CSP 4.0 для rpm дистрибутивов потребуется указать флаг `--nodeps`.

4. Установите каждый deb-пакет.
5. Для браузера Chrome(Chromium) расширение для работы плагина устанавливается автоматически при перезапуске браузера. Для Firefox необходимо установить расширение по ссылке: [https://www.cryptopro.ru/products/cades/downloads\(https://www.cryptopro.ru/sites/default/files/products/cades/extensions/cryptopro\\_extension\\_for\\_cades\\_browser\\_plug\\_in-1.1.1-an+fx-windows.xpi\)](https://www.cryptopro.ru/products/cades/downloads(https://www.cryptopro.ru/sites/default/files/products/cades/extensions/cryptopro_extension_for_cades_browser_plug_in-1.1.1-an+fx-windows.xpi))
6. Установите сертификат удостоверяющего центра командой:

```
/opt/cproscsp/bin/ia32/certmgr -inst -store root -file <путь к файлу с сертификатом>
```



7. Установите личный сертификат с помощью команды:

```
/opt/cproscsp/bin/ia32/certmgr -inst -file <путь к файлу с сертификатом> -cont <имя контейнера>
```

8. Проверьте подпись на демо-странице: <https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html>

## 1.4. Загрузка сертификатов пользователей

Для учетной записи пользователя должен быть загружен сертификат в систему:

1. Откройте форму настройки параметров учетной записи пользователя **Сервис – Пользователи**.
2. Выберите в списке учетную запись, для которой следует загрузить сертификат ключа пользователя.
3. Откройте форму редактирования параметров учетной записи с помощью кнопки **Изменить**.  
 **Примечание** – Если учетная запись пользователя не создана, следует добавить ее в систему.
4. Нажмите кнопку **Сертификаты**. Отобразится форма загрузки сертификатов пользователя.  
 **Примечание** - Сертификат должен быть в формате PKCS7.
5. Для добавления сертификата пользователя нажмите кнопку **Добавить**.

6. Укажите путь к файлу-сертификату, нажмите кнопку **Загрузить**. Сертификат будет загружен. Файл сертификата предоставляется удостоверяющим центром, при выдаче электронного ключа.
7. Нажмите кнопку **Сохранить** для сохранения внесенных изменений.
8. Для применения настроек необходимо выйти из системы и авторизоваться под учетной записью пользователя, для которой были добавлены настройки.