**Утверждаю**

Директор Департамента

информационной безопасности

АО «Национальные информационные

технологии»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Надирханов Г.М.

« » \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2019 года

**Инструкция по работе с сервисом подписи и проверки электронных документов**

****

г. Астана, 2019 г.

**Содержание**

[1. Назначение документа 2](#_Toc497900698)

[2. Минимальные требования к компьютеру пользователя 2](#_Toc497900699)

[3. Подключенние модуля ezSigner в NCALayer 2](#_Toc497900700)

[4. Вход в систему EzSigner 4](#_Toc497900701)

[5. Раздел 1. Подпись документа электронной цифровой подписью 4](#_Toc497900702)

[5. Раздел 2. Проверка электронной цифровой подписи документа 7](#_Toc497900703)

[5.1 «Проверить документ» 7](#_Toc497900704)

[5.2 «Извлечь исходный документ» 8](#_Toc497900705)

# **Назначение документа**

Настоящая инструкция разработана с целью описания возможностей работы с сервисом подписи и проверки электронных документов «ezSigner». Перед началом использованием сервиса «ezSigner» необходимо ознакомиться с настоящей инструкцией пользователя.

Сервис «ezSigner» предназначен для формирования и проверки электронной цифровой подписи (далее – ЭЦП) под электронным документом. При работе с сервисом «ezSigner» используются регистрационные свидетельства, выданные Национальным удостоверяющим центром Республики Казахстан. Сервис «ezSigner» поддерживает следующие виды носители ключевой информации: eToken, KAZTOKEN, JaCarta, aKey, удостоверение личности и файловая система. Работа в сервисе осуществляется анонимно, авторизация при проверке и подписи электронного документа не требуется. Файлы сохранятся на рабочей станции пользователя.

Порядок формирования и проверки подлинности ЭЦП осуществляется в соответствии с приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года №1187 «Об утверждении Правил проверки подлинности электронной цифровой подписи».

# **Минимальные требования к компьютеру пользователя**

* Операционная система: Windows XP/7/8/10, Linux, OS X 10;
* Браузер: Internet Explorer 10+, Firefox 4+, Opera 10+, Google Chrome 4+, Safari 5+;
* NCALayer (с подключенным модулем ezSigner).

# **Подключение модуля ezSigner в NCALayer**

**Шаг 1.** Для подключения модуля ezSigner в NCALayer необходимо запустить NCALayer и в панели уведомлений найти значок NCALayer (Рис. 1).

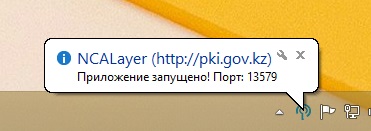


Рис.1

**Шаг 2.** Правой кнопкой мыши нажать на «Управление модулями» (Рис. 2).

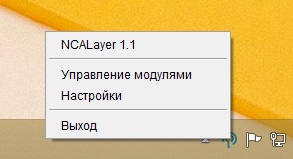


Рис. 2

**Шаг 3.** В открывшемся окне из списка модуля выбрать «модуль ezSigner» и нажать «Установить модуль» (Рис 3.).

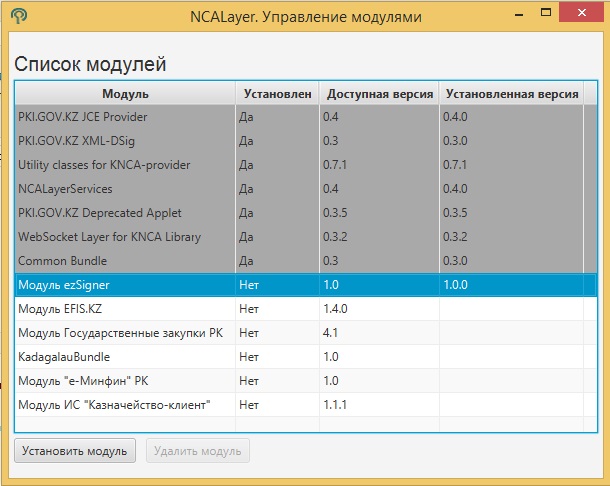


Рис. 3

**Шаг 4.** Для установки модуля программа запросит перезагрузку NCALayer, нажмите кнопку «Перезапустить» (Рис. 4)

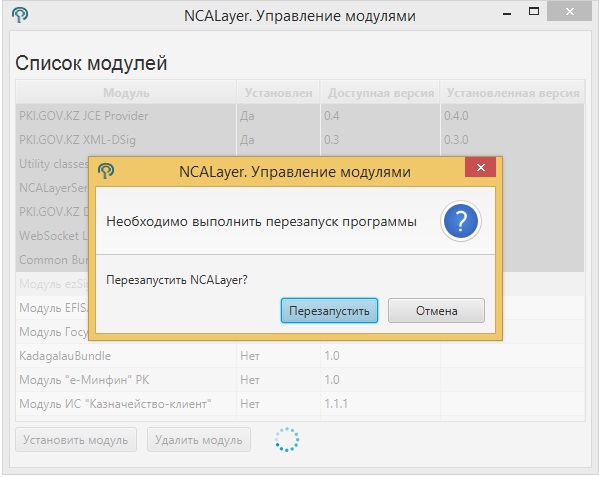


Рис. 4

*При успешной перезагрузке выйдет сообщение о запуске NCALayer (Рис. 1).*

***Процедура установки модуля ezSigner в NCALayer завершена!***

# **Открытие сервиса «EzSigner»**

Для того чтобы начать работу в Сервисе подписи и проверки электронных документов, необходимо использовать один из перечисленных браузеров: MS Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, ввести в адресную строку – <http://ezsigner.kz/> (Рис. 5).

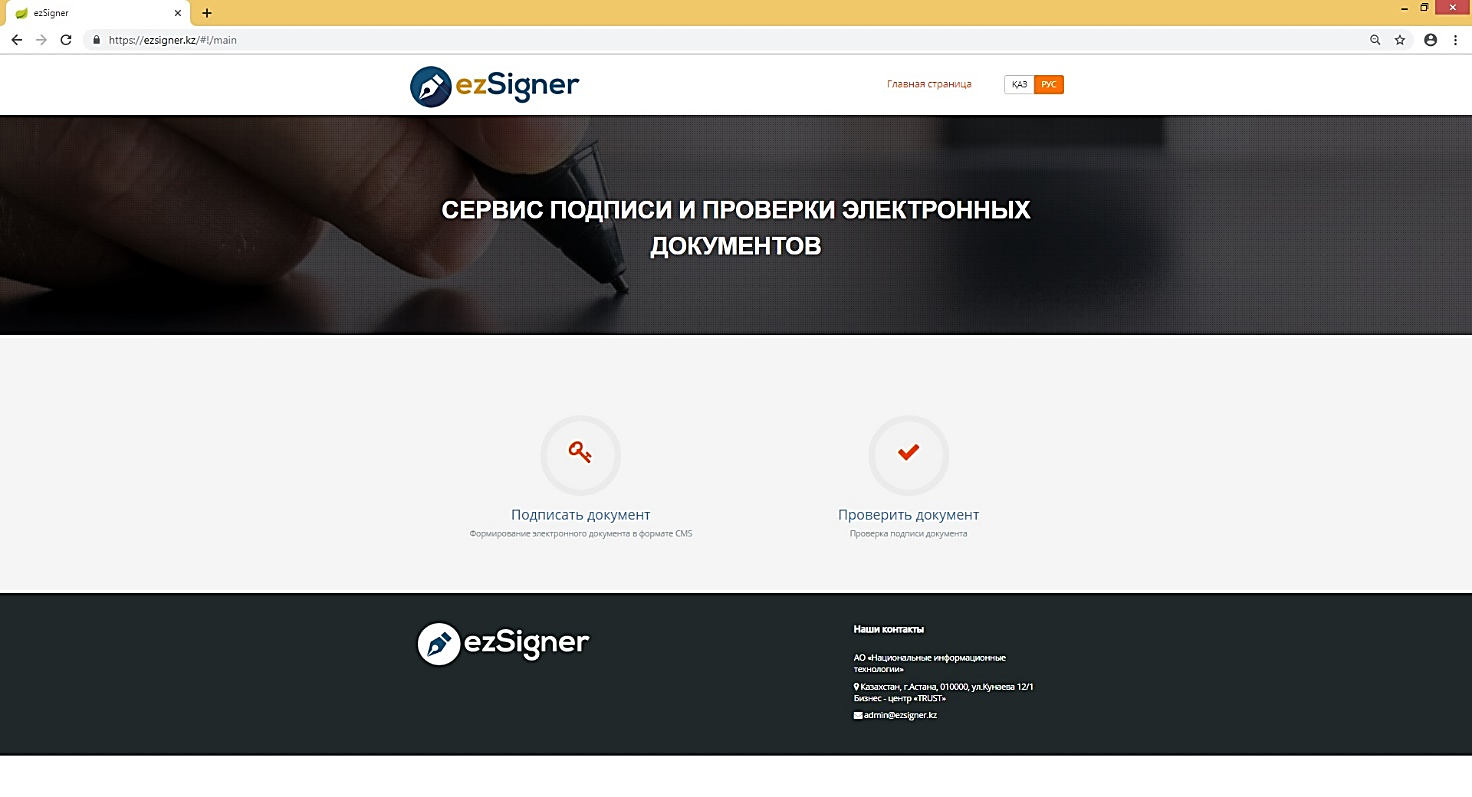


Рис.5

# **Раздел 1. Подпись документа электронной цифровой подписью**

**Шаг 1.** На странице входа необходимо нажать на кнопку «Подписать документ» (Рис. 5).

**Шаг 2.** В открывшемся окне в поле «Документ» (Рис. 6) Вам необходимо прикрепить документ**,** который Вы хотите подписать. Если документ находится на внешнем ресурсе выберите «Ссылка».

**Шаг 3.** Далее в поле «Сохранить подписанный документ» укажите место, где будет сохранен электронный документ, подписанный ключами ЭЦП.

***Внимание! После проставления ЭЦП формируется электронный документ в формате «cms***[[1]](#footnote-1)***».***

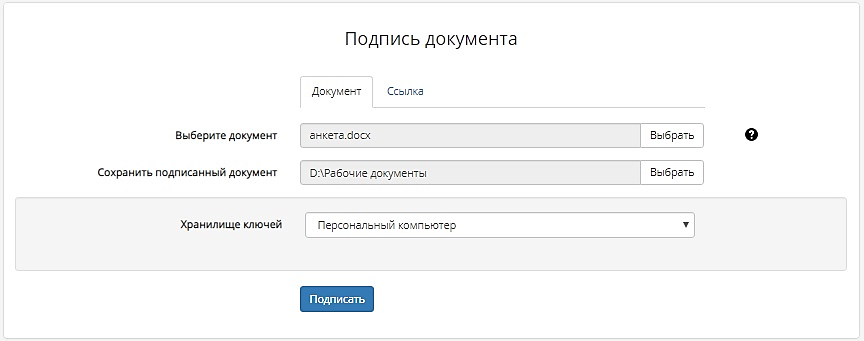


Рис. 6

**Шаг 4.** Вам необходимо выбрать тип «Хранилище ключей» из списка: Персональный компьютер, удостоверение личности, eToken PRO (Java, 72K), JaCarta, Kaztoken, Akey (Рис. 7) и нажать кнопку «Подписать».

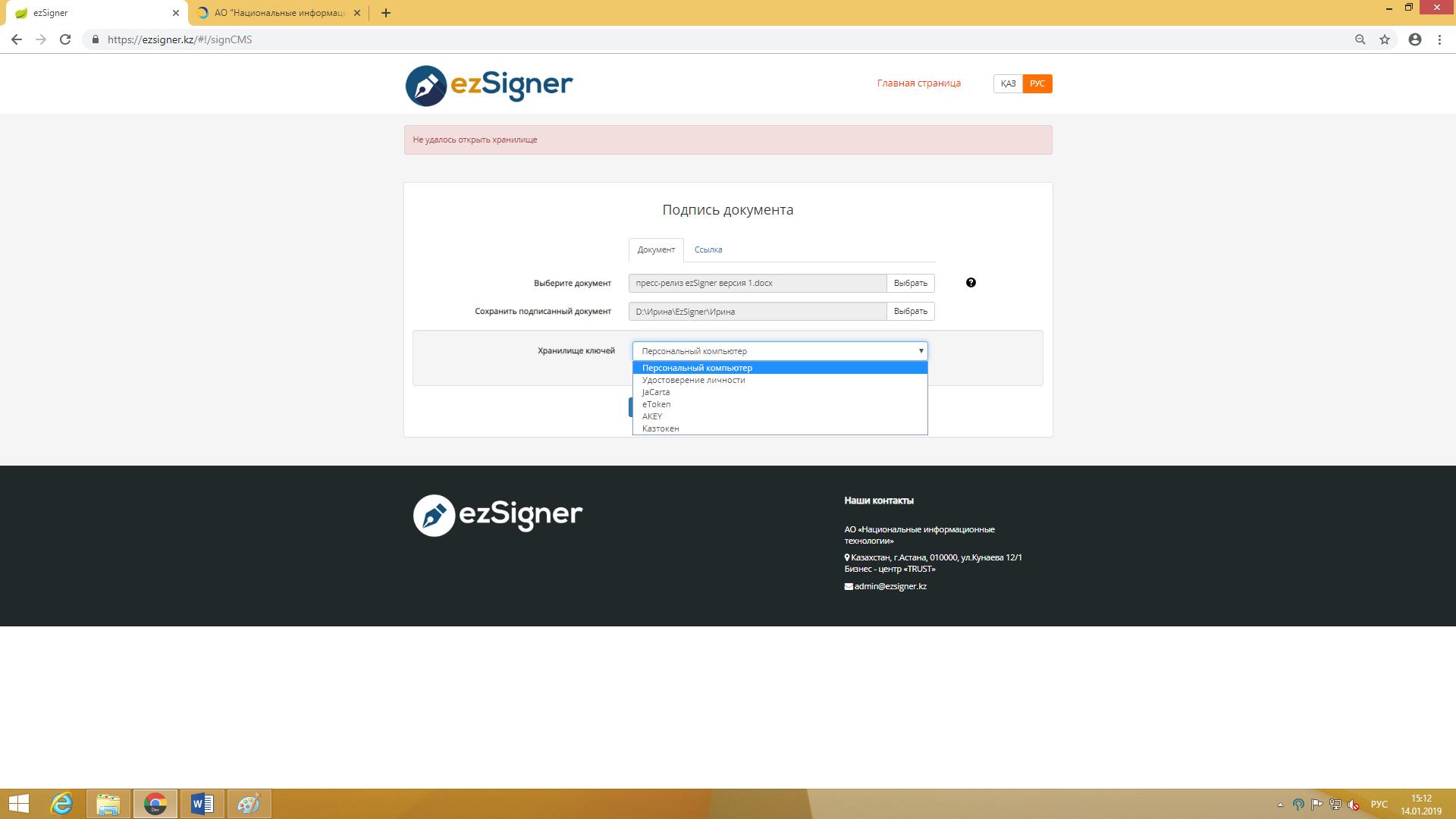


Рис.7

**Шаг 5.** В поле «Путь к хранилищу» необходимо указать путь, где расположены Ваши ключи ЭЦП. Выберите ключ подписи (Рис. 8) и введите Ваш пароль на хранилище ключей (Рис. 9). Нажмите кнопку «Открыть».

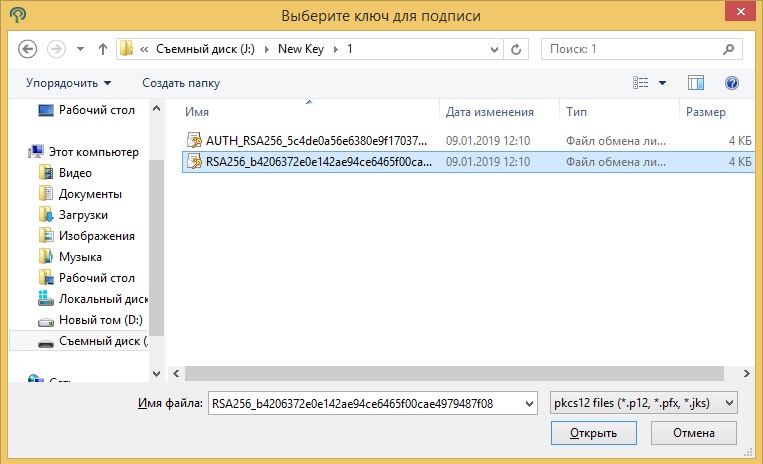


Рис.8

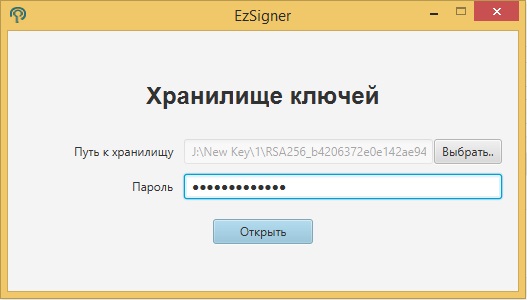


Рис. 9

**Шаг 6.** При корректном вводе пароля Ваш документ будет подписан.

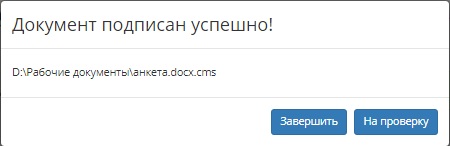


Рис. 10

***Процедура подписи документа завершена!***

*После успешного завершения (Рис. 10) Вы можете, при выборе кнопки «Завершить», снова перейти в раздел подписи документа, либо отправить данный документ на проверку.*

# **5. Раздел 2. Проверка электронной цифровой подписи документа**

# 

# **5.1 «Проверить документ»**

**Шаг 1.** На странице входа необходимо нажать на кнопку «Проверить документ» (Рис. 5).

**Шаг 2.** В открывшемся окне в поле «Электронный документ для проверки» (Рис. 11) Вам необходимо прикрепить подписанный документ, ЭЦП которой Вы хотите проверить.

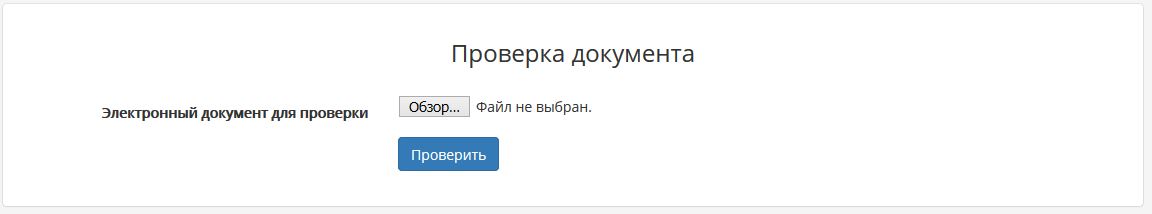


Рис. 11

**Шаг 3.** Нажмите кнопку «Проверить». Основная информация об ЭЦП будет отображена согласно Рис. 12.

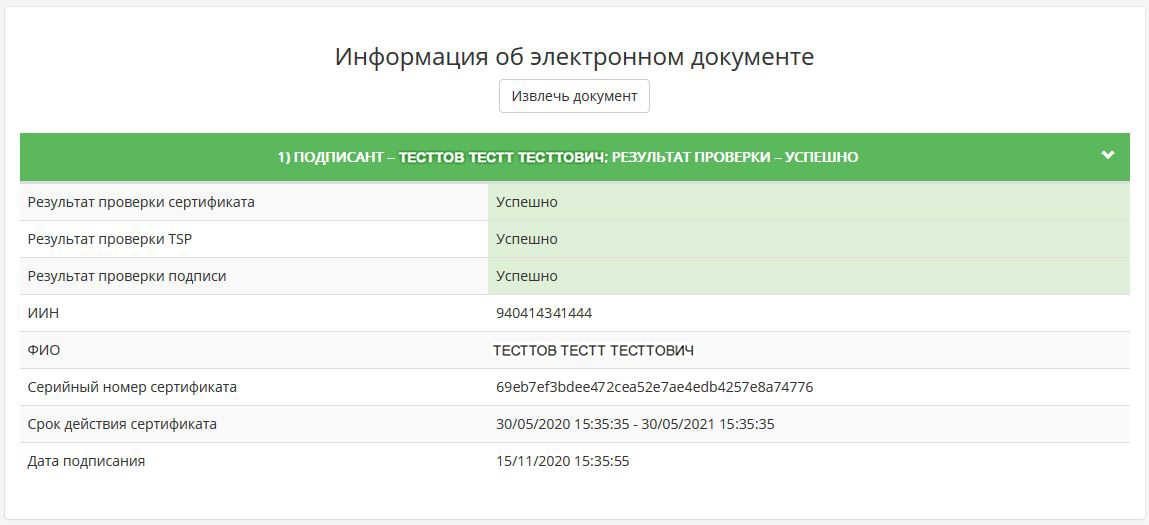


Рис. 12

***Процедура проверки ЭЦП документа завершена!***

# **5.2 «Извлечь исходный документ»**

После проверки подписи, описанной в секции «Проверить документ», необходимо нажать кнопку «Извлечь документ». После чего браузер даст Вам возможность либо открыть, либо сохранить исходный документ.

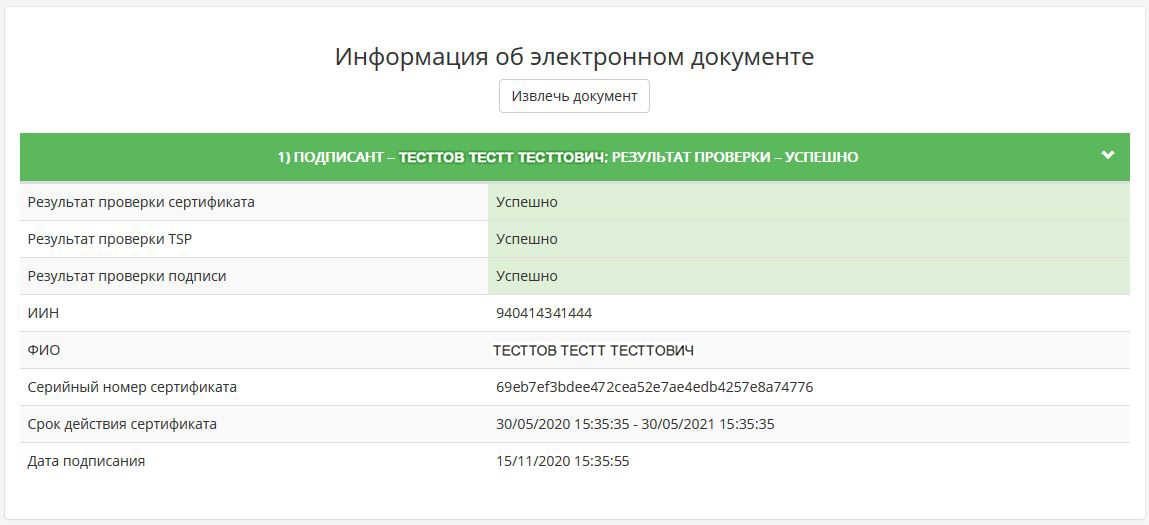


Рис. 13

***Процедура извлечения исходного документа из формата «cms» завершена!***

1. Стандарт СMS (Cryptographic Message Syntax) описывает структуру криптографических сообщений, включающих в себя защищенные данные вместе со сведениями, необходимыми для их корректного открытия или использования. [↑](#footnote-ref-1)