Руководство
по настройке рабочего места пользователя Сервиса электронной подачи заявки на ТЗ, НМПТ/ПНМПТ

2018

Оглавление

Введение

Настоящий документ содержит описание действий по настройке рабочего места Сервиса электронной подачи заявки на товарный знак, заявки на регистрацию заявляемого обозначения в качестве наименования места происхождения товара и/или предоставление исключительного права на ранее зарегистрированное наименование места происхождения товара (далее - Сервис), включающих в себя установку и настройку необходимого программного обеспечения.

Для выполнения установки и настройки ПО в соответствии с настоящим руководством пользователь должен обладать навыками по работе с компьютером.

Для выполнения установки и настройки ПО пользователь должен иметь права локального администратора на своем компьютере.

1 Программно-аппаратные требования

Программно-аппаратные требования для работы в Сервисе:

- клавиатура, мышь или совместимое указывающее устройство;
- разрешение экрана не менее чем 1024x768 точек;
- доступ к веб-серверу через Интернет по адресу https://kpsrtz.fips.ru ;
- операционная система Windows 7, Windows 8.1, Windows 10;
- браузеры Internet Explorer 11 или Google Chrome (версия 49.0 и выше);
- ПО "КриптоПро ЭЦП Browser plug-in" версия 2.0;
- ключевой носитель (например, Рутокен S);
- драйвер ключевого носителя (необходимо, например, для Рутокен S);
- квалифицированный сертификат (с ключом электронной подписи под «КриптоПро CSP»);
- средство ЭП (криптопровайдер «КриптоПро CSP» версии 3.9, 4.0), сертифицированное ФСБ России;
- текстовый редактор Microsoft Office Word 2003-2016 или другие средства, обеспечивающие корректный просмотр документов формата DOC/DOCX;
- средство просмотра pdf-документов (Adobe Reader).

2 Порядок настройки рабочего места пользователя

Для работы в Сервисе необходимо приобрести квалицированный сертификат ЭП для работы на интернет порталах в одном из аккредитованных удостоверяющих центров (далее – УЦ). Перечень всех аккредитованных УЦ опубликован на портале уполномоченного федерального органа в области использования электронной подписи (http://e-trust.gosuslugi.ru/CA).

Настройку компьютера для работы с электронной подписью выполните по инструкциям УЦ, в котором был приобретён сертификат. Эта настройка осуществляется в следующем порядке:

- Установка средства электронной подписи (криптопровайдер), предназначенного для работы с вашим ключом ЭП;
- Установка драйвера ключевого носителя (например, Рутокен S), при необходимости;
- Установка личного сертификата;
- Установка цепочки сертификатов для личного сертификата.

  Цепочку личного сертификата следует построить через сертификаты Минкомсвязи РФ. Для автоматической установки цепочки личного сертификата можно использовать программу «Автоконфигуратор» (см. Приложение 1).

- Настройка браузера для электронной подписи (см. раздел 3 настоящего Руководства).

3 Настройка браузера для электронной подписи

Для входа в Сервис и подписания подготовленных документов электронной подписью необходимо установить и включить ПО "КриптоПро ЭЦП Browser plug-in". Для этого выполните следующие действия.

1. По ссылке http://www.cryptopro.ru/products/cades/plugin/get_2_0 скачайте установочный файл "КриптоПро ЭЦП Browser plug-in", запустите его, дождитесь завершения установки.

2. Включение "КриптоПро ЭЦП Browser plug-in" в браузере.

   2а. для браузера Google Chrome

Откройте меню браузера -> «Дополнительные настройки» -> «Расширения», включите расширение "CryptoPro Extension for CAdES Browser Plug-in" (см. Рис. 1).

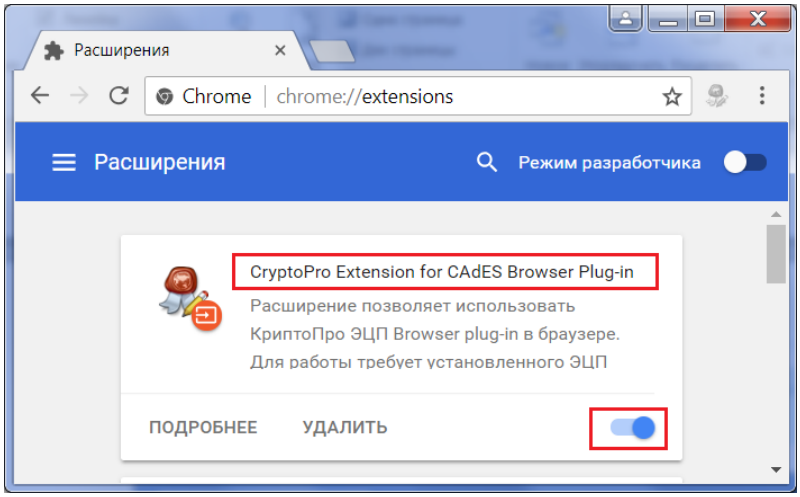

Рис. 1 Включение КриптоПро ЭЦП Browser plug-in для браузера Google Chrome.

Настройка для браузера Google Chrome завершена.

2б. для браузера Internet Explorer 11

Добавьте адрес https://kpsrtz.fips.ru в зону «Надёжные сайты», выполнив следующие действия:

Откройте браузер Internet Explorer, откройте меню «Сервис» -> «Свойства браузера» (см. Рис. 2)

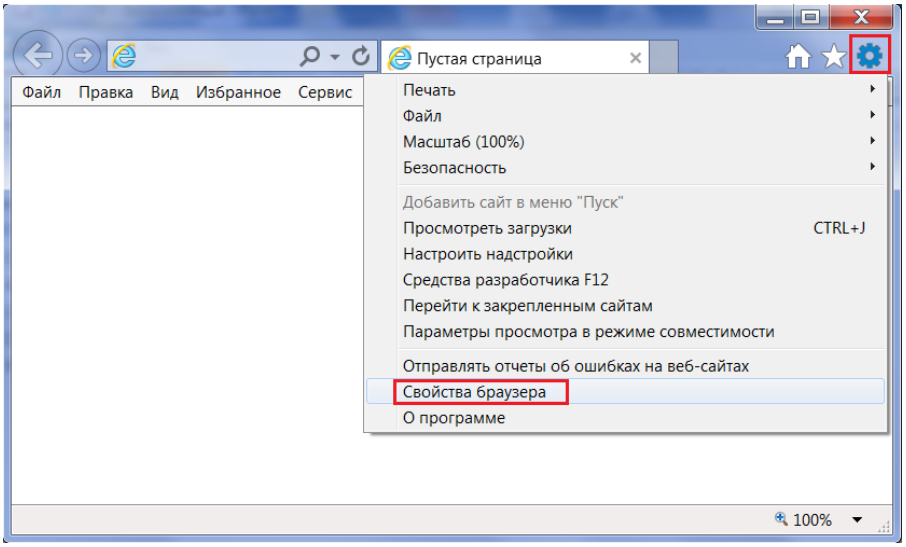

Рис. 2

В открывшемся окне перейдите на вкладку «Безопасность», выберите зону «Надежные сайты», нажмите кнопку «Сайты» (см. Рис. 3):

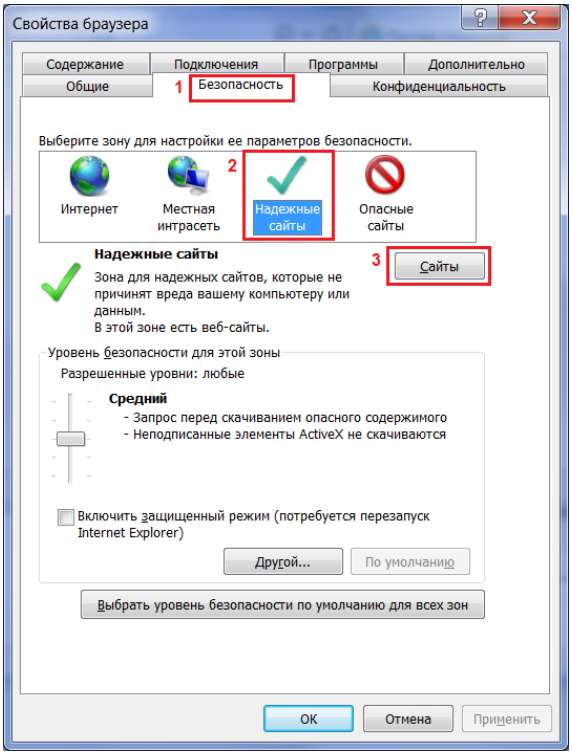

Рис. 3

Укажите адрес https://kpsrtz.fips.ru, нажмите кнопку «Добавить» (см. Рис. 4):

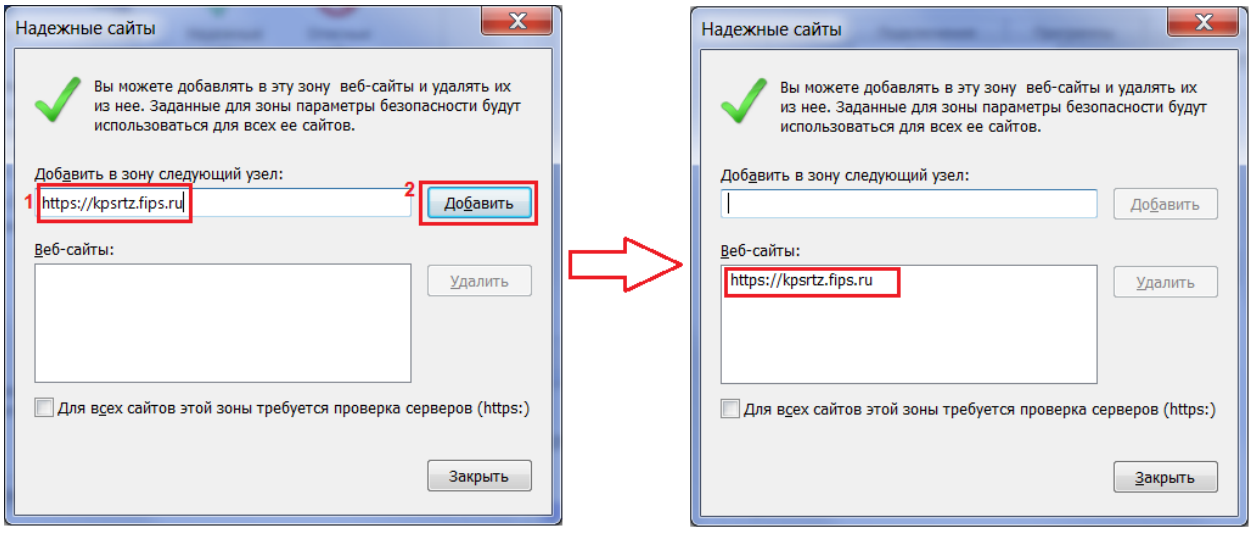

Рис. 4

Настройка для браузера Internet Explorer 11 завершена.

3. Проверка "КриптоПро ЭЦП Browser plug-in".

В случае возникновения проблем при входе в Сервис проверьте работу плагина на тестовой странице КриптоПро:

https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html
или
https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html

В случае успешного завершения проверки, после нажатия на кнопку «Подписать» появится электронная подпись в виде блока текстовых символов (см. Рис. 5).

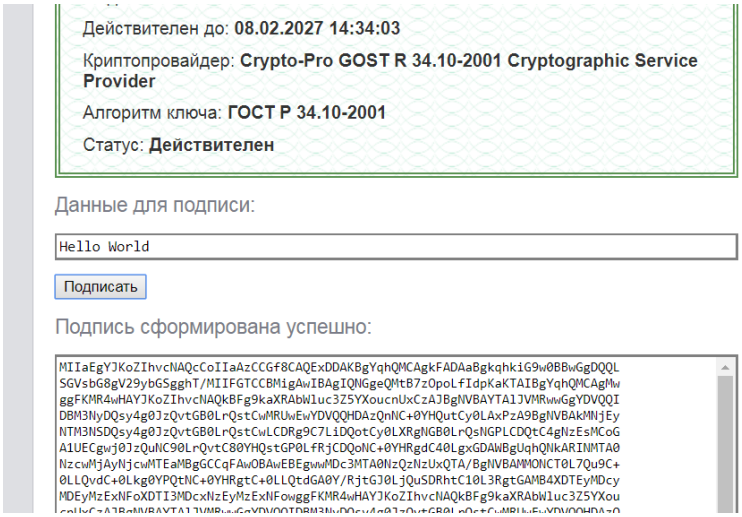

Рис. 5 Успешное завершение проверки на тестовой странице КриптоПро

Приложение 1. Инструкция по работе с программным приложением «Автоконфигуратор»

До выполнения настройки с помощью Windows-приложения «Автоконфигуратор» (далее – Приложение), выполните установку средства электронной подписи, драйвера ключевого носителя и личного сертификата (см. раздел 2 настоящего Руководства).

Для запуска Приложения на компьютере должно быть установлено ПО Microsoft .NET Framework 4 (Windows 8 и более поздние версии Windows поставляются с установленной платформой .NET Framework 4, поэтому для этих ОС установка .NET Framework 4 не требуется).

Приложение автоматически выполняет следующие действия по настройке рабочего места пользователя Сервиса:

1. установка следующих сертификатов Минкомсвязи России:

- кросс-сертификат вашего удостоверяющего центра и соответствующий кросс-сертификат верхнего уровня («УЦ 1 ИС ГУЦ» или «УЦ 2 ИС ГУЦ»; если такой сертификат есть в цепочке) – в хранилище «Промежуточные центры сертификации»;
- сертификат «Головной удостоверяющий центр» - в хранилище «Доверенные корневые центры сертификации».

2. настройка браузера Internet Explorer 11:

- адрес веб-приложения https://kpsrtz.fips.ru будет добавлен в список надёжных сайтов;
- в дополнительных настройках IE11 будут включены протоколы "TLS 1.0" и "SSL 3.0".

Дополнительная настройка Google Chrome (версия 49.0 и выше) не требуется и не осуществляется «Автоконфигутором».

Скачайте архив с Приложением по ссылке «Автоконфигуратор», размещенной на сайте ФИПС в разделе «Подача заявки. Подача заявки на товарный знак, НМПТ/ПНМПТ» (http://new.fips.ru/podacha-zayavki/podacha-zayavki-na-tovarnyy-znak/ http://www1.fips.ru/wps/wcm/connect/content_ru/ru/el_zayav/tm_ap_new), распакуйте архив (в архиве содержится исполняемый файл - «IEConfigurator.exe»).

Последовательность действий при работе с Приложением:

1. Запустите файл IEConfigurator.exe на выполнение.

ОС Windows выдаст сообщение. Нажмите кнопку "Подробнее", затем "Выполнить в любом случае" (см. Рис. 6).

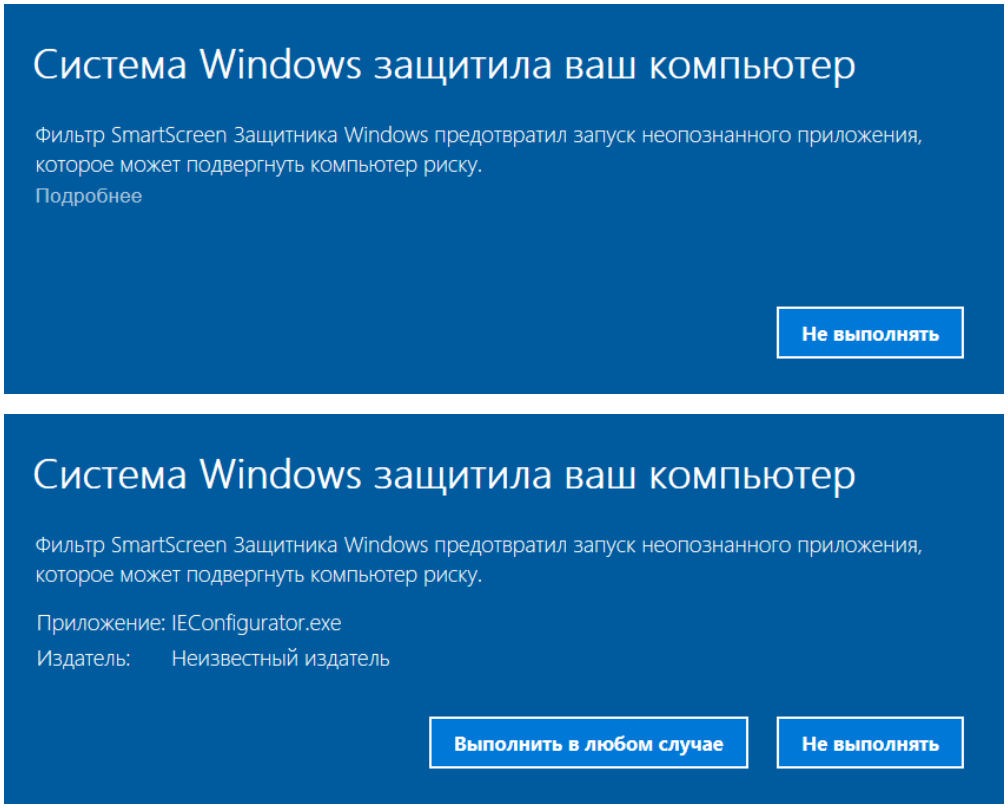

Рис. 6 Запуск приложения Автоконфигуратор

2. Откроется окно «Автоконфигуратор». Выберите опцию "Новый интерфейс сервиса подачи заявок на ТЗ (Chrome, IE11+) и нажмите кнопку "Выполнить настройку" (см. Рис. 7).

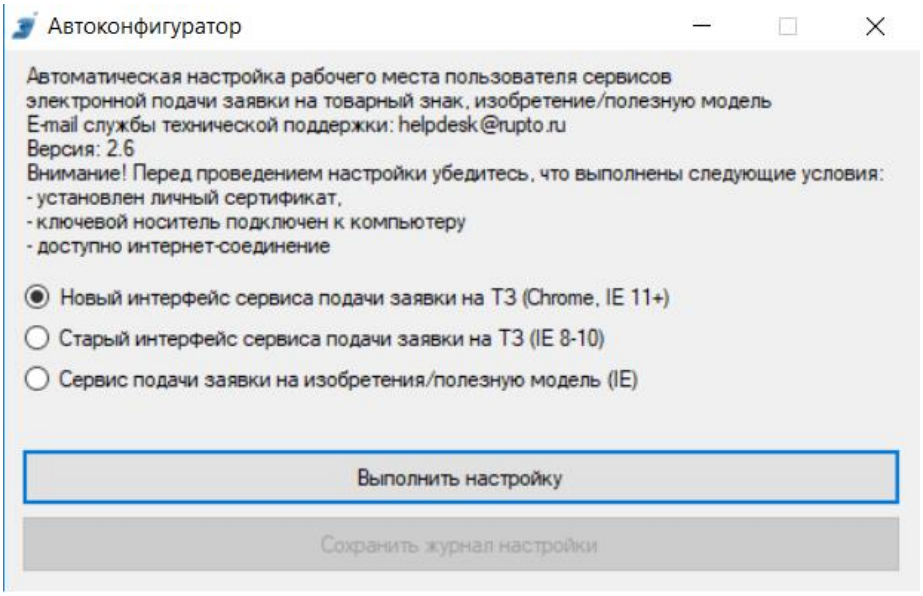

Рис. 7 Окно «Автоконфигуратор».

3. Приложение предложит выбрать личный сертификат, в случае, если на компьютере пользователя установлено более одного сертификата. Выберите нужный сертификат и нажмите

кнопку «ОК» (см. Рис. 8).

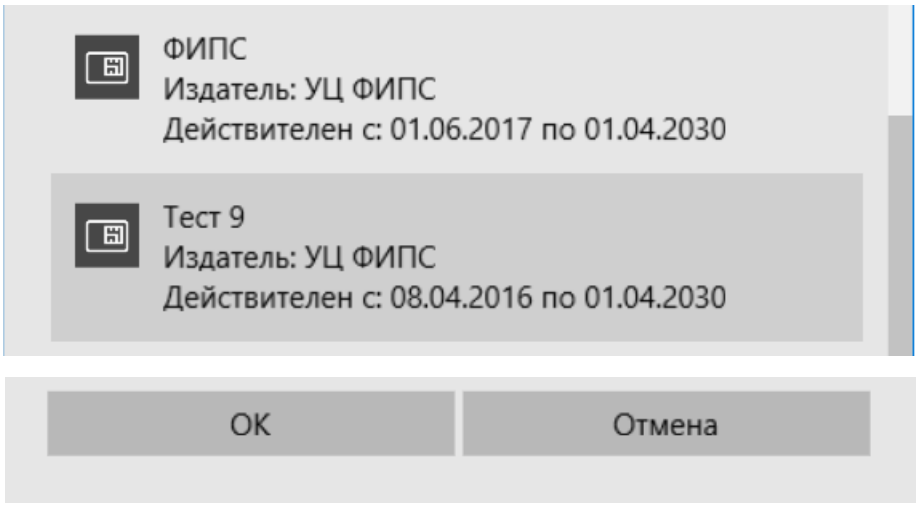

Рис. 8 Выбор сертификата

Если на компьютере пользователя установлен только один личный сертификат, то этот шаг будет пропущен.

4. В случае отсутствия сертификата Головного Удостоверяющего центра в хранилище "Доверенные корневые центры сертификации" будет выдано сообщение, нажмите кнопку "ДА" (см. Рис. 9).

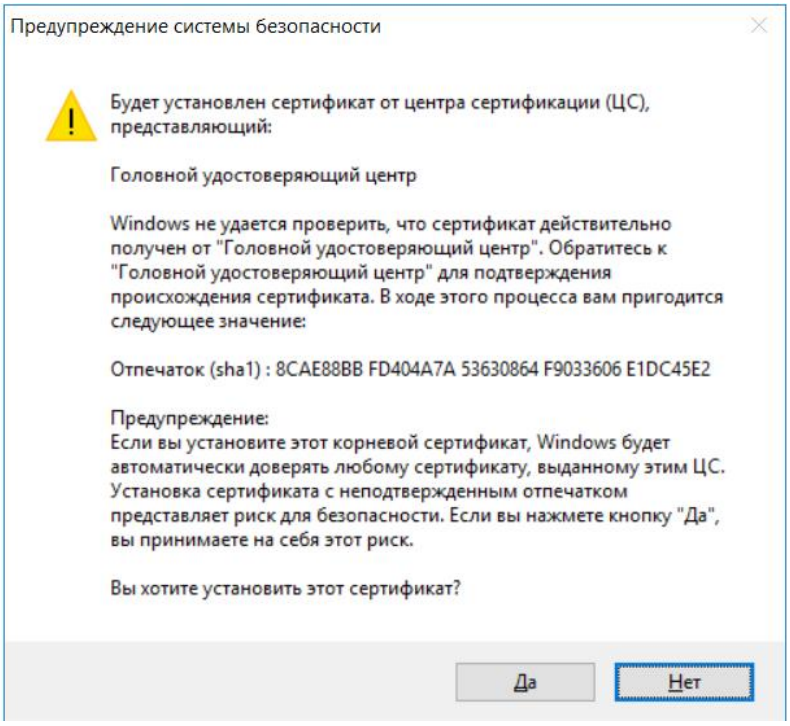

Рис. 9 Предупреждение системы безопасности

5. При успешном завершении автоматической настройки рабочего места пользователя, Приложение выдаст сообщение (см. Рис. 10) об успешном выполнении настройки.

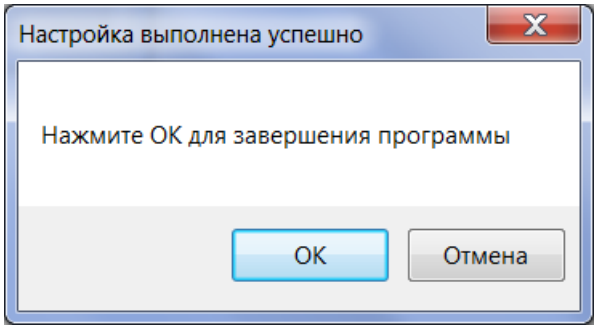

Рис. 10 Завершение настройки

Нажмите «ОК» для завершения работы Приложения.

6. Если во время выполнения автоматической настройки были открыты окна браузера, то для применения настроек необходимо браузер перезапустить.

После выполнения настройки с помощью Приложения, для работы с Сервисом дополнительно необходимо выполнить настройку, описанную в разделе 3 настоящего Руководства.

Если в процессе установки возникнут какие-либо проблемы, Приложение выдаст сообщение (см. Рис. 11). Следуя данному сообщению, направьте обращение в Службу технической поддержки ФИПС на адрес электронной почты helpdesk@rupto.ru, приложив файл журнала настройки.

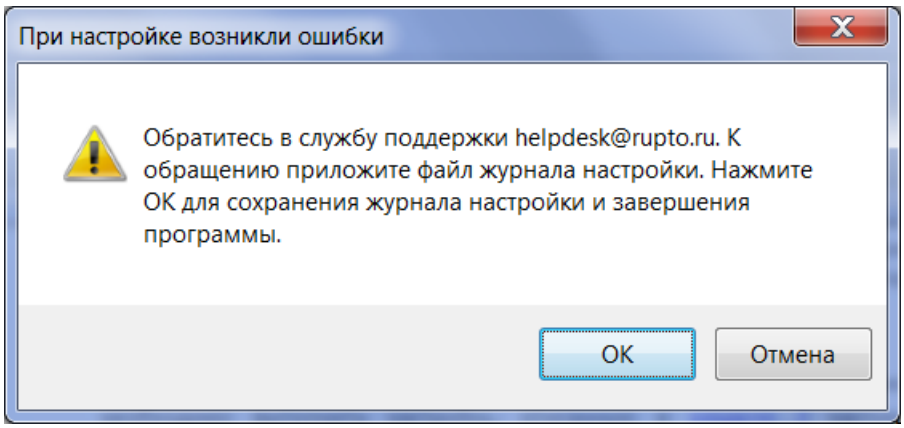

Рис. 11 Ошибка при настройке

Глоссарий

Сервис – сервис электронной подачи заявки на регистрацию ТЗ, НМПТ/ПНМПТ

ОС – операционная система

ПО – программное обеспечение

Заявка на ТЗ – Заявка на товарный знак

Заявка на НМПТ/ПНМПТ – Заявка на регистрацию заявляемого обозначения в качестве наименование места происхождения товара и/или предоставление исключительного права на ранее зарегистрированное наименование места происхождения товара

ФЗ-63 – Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011 (редакция от 23.06.2016 N 220-ФЗ).

ЭП (электронная подпись) – 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.

Квалифицированный сертификат – сертификат ключа проверки электронной подписи в электронном виде, выданный удостоверяющим центром, аккредитованным в Минкомсвязи РФ.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец сертификата ключа проверки электронной подписи (владелец ключа ЭП) – лицо, которому в установленном порядке (по ФЗ-63) выдан сертификат ключа проверки электронной подписи.

Удостоверяющий центр (УЦ) – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные ФЗ-63.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом в сфере использования электронной подписи соответствия удостоверяющего центра требованиям ФЗ-63.

Аутентификация – процедура проверки подлинности.

Средства электронной подписи (криптопровайдер) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и

ключа проверки электронной подписи.

Ключевой носитель – устройство, используемое для хранения ключа ЭП.

Закрытый ключ (private key, ключ ЭП) - закрытая (секретная) часть пары криптографических ключей. Служит для создания ЭП, которые потом можно проверять с помощью соответствующего открытого ключа, или для расшифровки сообщений, которые были зашифрованы соответствующим открытым ключом. Закрытый ключ конфиденциален (доступен только его владельцу), передача его кому-либо запрещена. Похищение закрытого ключа означает возможность получения злоумышленником любой информации, зашифрованной для владельца ключа ЭП, а также возможность подделки ЭП владельца ключа ЭП. Поэтому закрытый ключ должен сохраняться в тайне особо тщательно.

Открытый ключ (public key, ключ проверки ЭП) — открытая (несекретная) часть пары криптографических ключей. Служит для проверки электронных подписей, созданных с помощью соответствующего ему закрытого ключа, или для шифрования сообщений, которые будут потом расшифрованы соответствующим ему закрытым ключом. Удостоверяющий центр подтверждает принадлежность открытых ключей конкретным лицам по запросу любого обратившегося лица.