

Генерация ключа на Рутокен ЭЦП 2.0 для работы с ЕГАИС

СОДЕРЖАНИЕ

I. ПОДГОТОВИТЕЛЬНЫЕ МЕРОПРИЯТИЯ	2
II. ГЕНЕРАЦИЯ КЛЮЧА И УСТАНОВКА СЕРТИФИКАТА ГОСТ НА РУТОКЕН ЭЦП 2.0...6	6
III. ПОЛУЧЕНИЕ RSA-КЛЮЧА.....9	9
IV. УДАЛЕНИЕ ЛИШНЕЙ КЛЮЧЕВОЙ ПАРЫ	10

I. ПОДГОТОВИТЕЛЬНЫЕ МЕРОПРИЯТИЯ

Важно!

- На компьютере должны быть установлены драйвера Рутокен, которые поддерживают Рутокен ЭЦП 2.0 (желательно последней версии).
- Рутокен ЭЦП 2.0 должен быть настроен для работы в ЕГАИС.
- Для перевыпуска сертификата необходимо отформатировать ключевой носитель. Для этого в «Панели управления Рутокен» на вкладке «Администрирование» необходимо ввести PIN-код администратора и нажать кнопку «Форматировать». **Все сертификаты и ключи на Рутокен ЭЦП 2.0 будут уничтожены!**

1. Установка драйверов Rutoken

На время установки драйверов Рутокен **не должен** быть подключен к компьютеру.

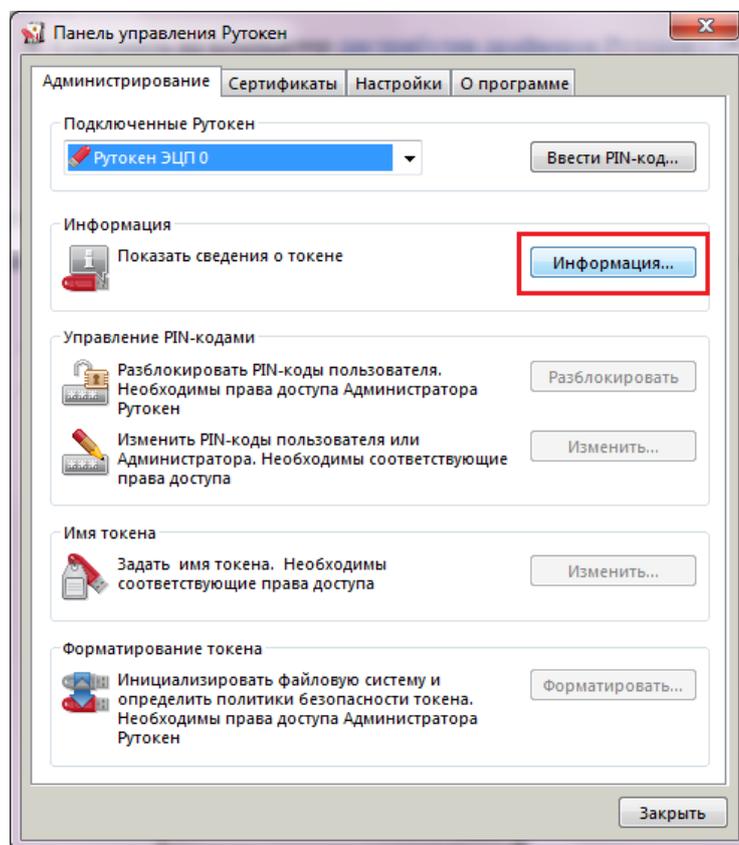
Для установки драйверов Рутокен ЭЦП 2.0 выполняются следующие действия:

- 1.1 Загрузить дистрибутив с официального сайта производителя www.rutoken.ru (раздел «Центр загрузки» - «Драйверы для ЕГАИС»).
- 1.2 Запустить сохраненный файл (обычно это **rtDrivers.exe**).
- 1.3 Может открыться окно предупреждения системы безопасности, в нем необходимо «Запустить».
- 1.4 Следовать инструкциям Мастера установки, в конце нажать «Заккрыть»

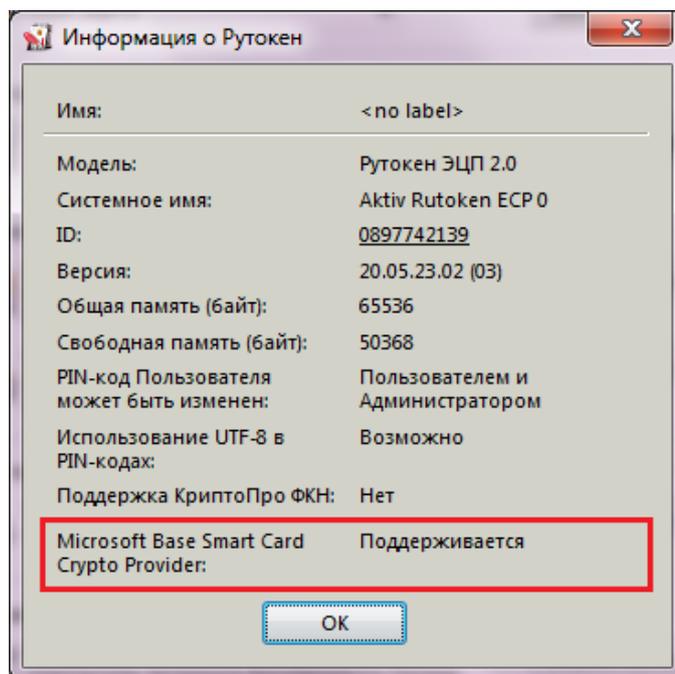
2. Настройка Рутокен ЭЦП 2.0 для работы в ЕГАИС

Настройка для работы в ЕГАИС выполняется следующим образом:

1. Вставить ключевой носитель Рутокен ЭЦП 2.0.
2. Запустить Панель управления Рутокен.
3. На вкладке «Администрирование» нажать кнопку «Информация».



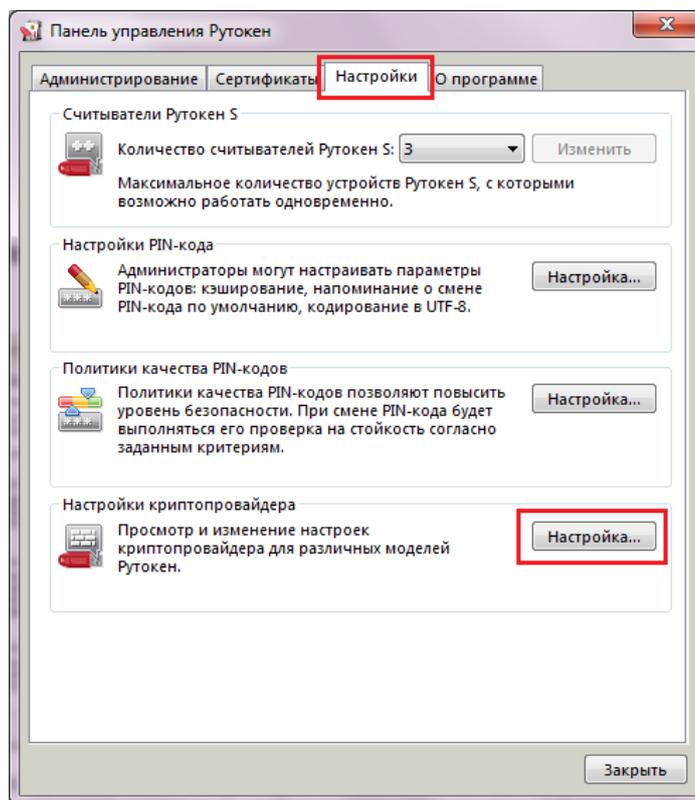
4. Откроется окно с информацией о носителе. Необходимо проверить статус «**Microsoft Base Smart Card Crypto Provider**».



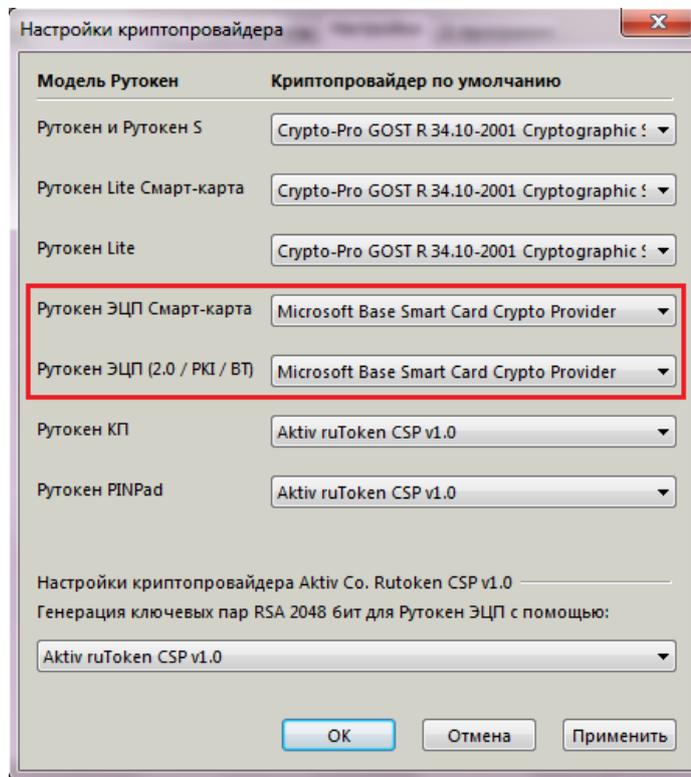
- Если статус «**Поддерживается**», то можно нажать «**ОК**» и перейти к следующему пункту данной инструкции.
- Если статус «**Активировать**», для начала необходимо активировать носитель.

– Статус «**Не поддерживается**» означает, что носитель не предназначен для работы с ЕГАИС.

5. На вкладке «**Настройки**» в разделе «**Настройки криптопровайдера**» необходимо нажать кнопку «**Настройка**».



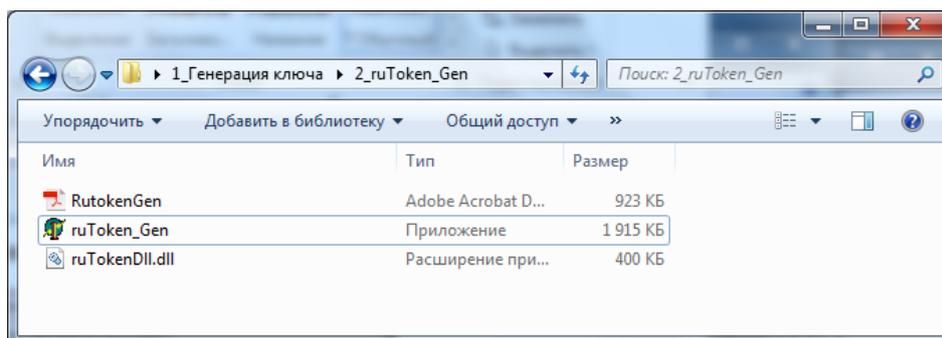
6. В полях «**Рутокен ЭЦП Смарт-карта**» и «**Рутокен ЭЦП (2.0)**» необходимо выбрать «**Microsoft Base Smart Card Crypto Provider**» и нажать «**ОК**»



7. Настройка Рутокен ЭЦП 2.0 для работы с ЕГАИС закончена.

II. ГЕНЕРАЦИЯ КЛЮЧА И УСТАНОВКА СЕРТИФИКАТА ГОСТ НА РУТОКЕН ЭЦП 2.0

1. Запустите программу **ruToken_Gen**. Программа находится на диске, выдаваемом при приобретении сертификата. Актуальную версию также можно получить в АО «НТЦ СТЭК» или у его партнеров или скачать с сайта <http://www.stek-trust.ru>.



2. Заполните поля формы. Проверьте правильность и актуальность данных.

Генерация запроса на сертификат и установка готового сертификата на ruToken ЭЦП 2.0

1. Генерация ключа и запроса на сертификат | 2. Установка готового сертификата на ruToken

Заполните все обязательные поля (отмеченные красным подчеркиванием) вручную либо на основе сертификата или xml-шаблона и нажмите кнопку "Генерировать ключ ..."

Заполнить поля из сертификата
Заполнить поля из xml-шаблона

Тип владельца сертификата
 Юридическое лицо Индивидуальный предприниматель

Сведения о владельце сертификата

Фамилия: Тестовый СНИЛС: 0000000000
Имя: Тест E-mail: support@stek-trust.ru
Отчество: Тестович Должность: Директор

Юридический адрес организации

Область: 74 Челябинская область
Город: Челябинск Улица, дом: Энтузиастов 12Б

Сведения об организации

Наименование: Тест
Отдел / Обособ. подр.: Магазин на ул. Энтузиастов, 12Б для ЕГАИС необходимо ввести адрес точки продаж вручную (например, "магазин на ул. Энтузиастов, 12")

ОГРН (ИП): 000000000000000 ИНН: 009972957454 КПП: 781001001

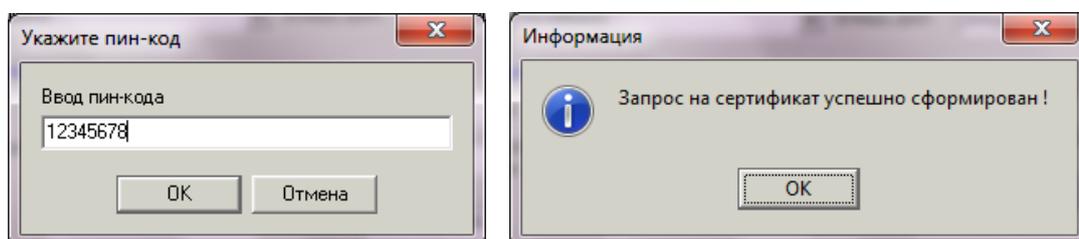
Срок действия запрашиваемого сертификата ключа ЭЦП: 12 месяцев (1 год) - от момента выпуска на УЦ

Генерировать ключ на ruToken и запрос на сертификат для передачи в УЦ Очистить все

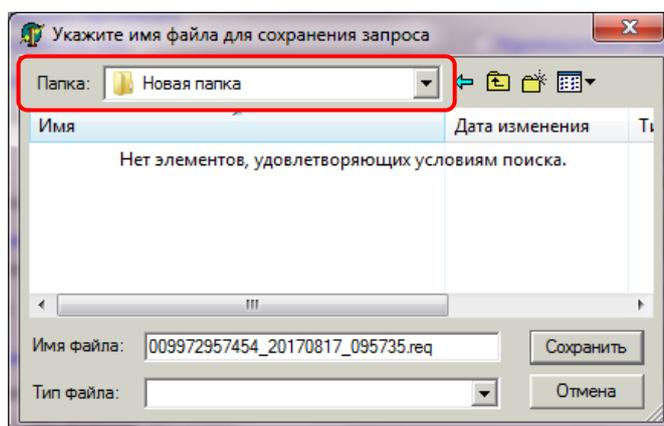
Помощь Закреть

В поле «Отдел / Обособ. подр.» необходимо внести фирменное название магазина или отличительный признак точки продаж. Эта информация будет отражена в сертификате для внутреннего использования и позволит отличить один сертификат от другого.

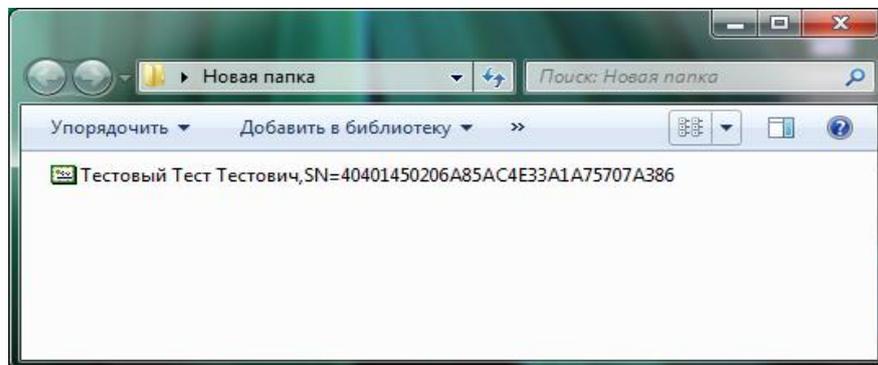
3. Нажмите кнопку «Генерировать ключ на ruToken и запрос на сертификат для передачи в УЦ». В окне «Укажите пин-код» введите PIN-код пользователя **12345678** (по умолчанию). Нажмите кнопку «ОК». Программа выдаст окно с информацией об успешном формировании запроса. Нажмите «ОК».



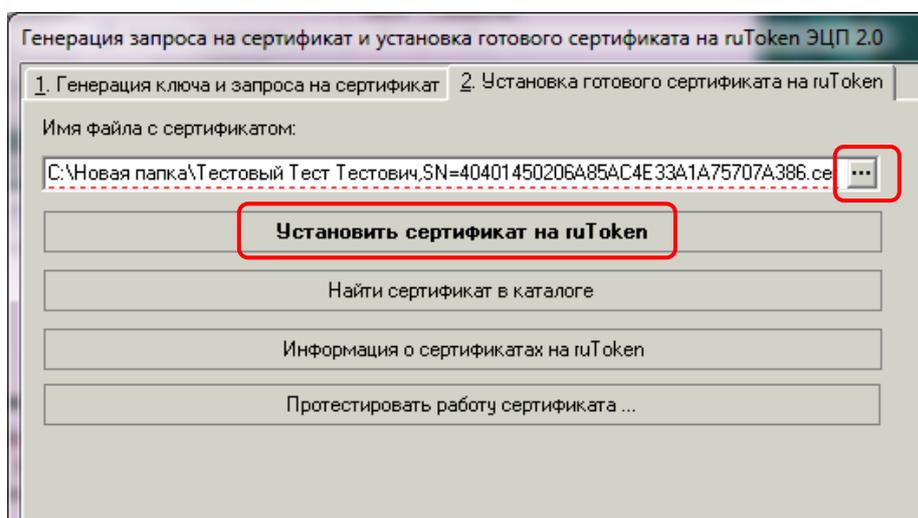
4. В окне «Укажите имя файла для сохранения запроса» необходимо указать папку, в которую будет сохранен файл с запросом на сертификат. Имя файла изменять не нужно. Нажмите «Сохранить».



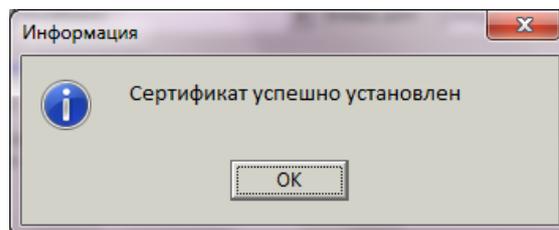
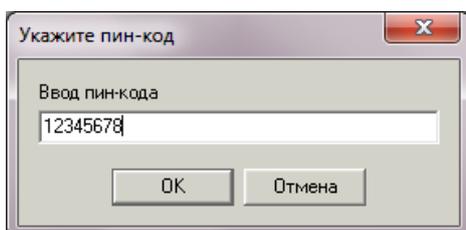
5. Для выпуска сертификата данный файл необходимо отправить в Удостоверяющий центр по электронной почте на адрес info@stek-trust.ru. После проверки документов специалисты Удостоверяющего центра обработают запрос и пригласят владельца сертификата для его получения. Сертификат следует сохранить на компьютер для последующей его установки.



6. Запустите программу **ruToken_Gen**. Перейдите на вкладку «**2. Установка готового сертификата на ruToken**». Нажмите на кнопку , выберите полученный файл с сертификатом и нажмите кнопку «**Установить сертификат на ruToken**».



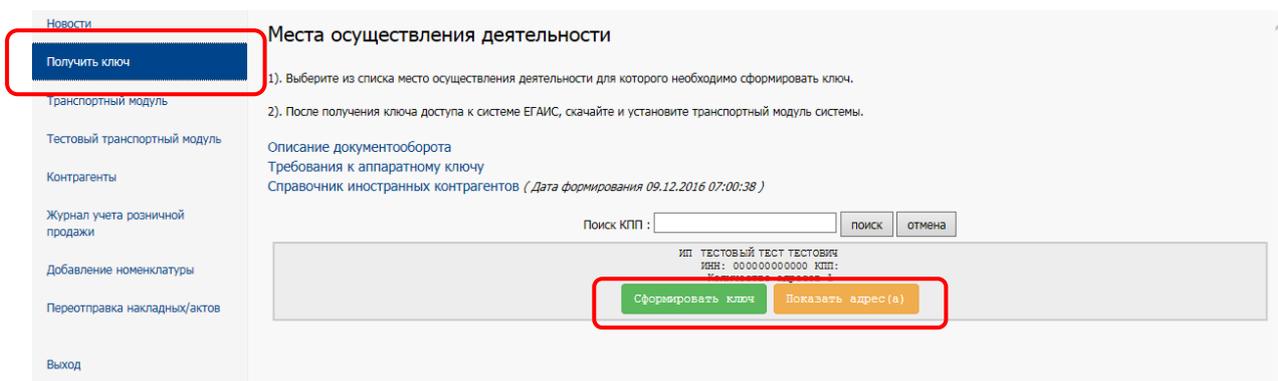
7. В окне «**Укажите пин-код**» введите PIN-код пользователя **12345678** (по умолчанию). Нажмите кнопку «**ОК**». Программа выдаст окно с информацией об успешной установке сертификата на Рутокен ЭЦП 2.0. Нажмите «**ОК**».



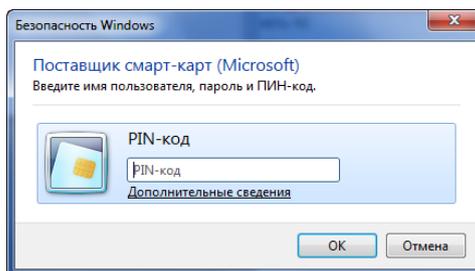
III. ПОЛУЧЕНИЕ RSA-КЛЮЧА

Для работы с ЕГАИС необходимо сгенерировать так называемый RSA-ключ. Выполняются следующие действия:

1. Необходимо войти в Личный кабинет ЕГАИС, перейти в раздел «**Получить ключ**». В правой части Личного кабинета будут представлены места осуществления деятельности. Необходимо выбрать требуемое место осуществления деятельности (по КПП или по кнопке «**Посмотреть адрес(а)**»), и нажать кнопку «**Сформировать ключ**»



2. В появившемся окне ввести пин-коды RSA и ГОСТ **12345678** (по умолчанию), подтвердить достоверность указанных сведений (поставить галочку). Затем нажать «**Сформировать ключ**».
3. Появится окно «**Безопасность Windows**», необходимо еще раз указать тот же пин-код пользователя: **12345678** (по умолчанию).



4. Если пин-код был указан верно, то RSA-ключ сформируется и запишется на носитель

ГЕНЕРАЦИЯ ЗАПРОСА НА СЕРТИФИКАТ: ✓
ЗАПРОС В УДОСТОВЕРЯЮЩИЙ ЦЕНТР: ✓
ЗАПИСЬ СЕРТИФИКАТА НА КЛЮЧ: ✓

СЕРТИФИКАТ УСПЕШНО ЗАПИСАН НА ТОКЕН

IV. УДАЛЕНИЕ ЛИШНЕЙ КЛЮЧЕВОЙ ПАРЫ

Важно!

ЕГАИС не работает с Rutoken, если в хранилище ГОСТ имеется несколько ключевых пар!

Если после установки сертификата и формирования ключа RSA при запуске УТМ появляется ошибка «ГОСТ хранилище не содержит подходящего сертификата», то как правило, это означает, что:

- на Rutoken была создана «лишняя» ключевая пара (открытый и закрытый ключ), например, несколько раз создавался запрос на сертификат.
- при генерации запроса на сертификат Rutoken предварительно не форматировался.

Для решения данной проблемы, как правило, помогают действия, описанные ниже.

1. Обновление драйверов Rutoken

На время обновления драйверов Рутокен **не должен** быть подключен к компьютеру.

Для обновления драйверов Рутокен ЭЦП 2.0 выполняются следующие действия:

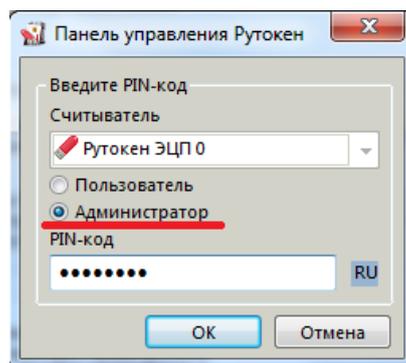
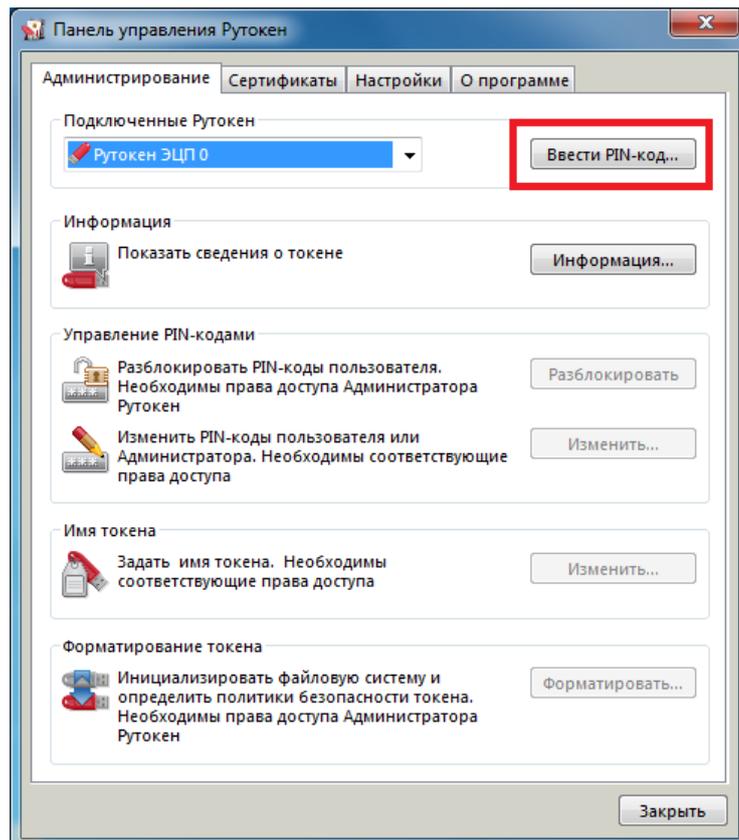
- 1.1 Загрузить дистрибутив с официального сайта производителя www.rutoken.ru (раздел «Центр загрузки» - «Драйверы для ЕГАИС»).
- 1.2 Запустить сохраненный файл (обычно это **rtDrivers.exe**).
- 1.3 Может открыться окно предупреждения системы безопасности, в нем необходимо нажать «**Запустить**».
- 1.4 Следовать инструкциям Мастера установки, в конце нажать «**Заккрыть**»

2. Удаление ключевых пар с Рутокен ЭЦП 2.0 для работы в ЕГАИС

Удаление лишних ключевых пар выполняется следующим образом:

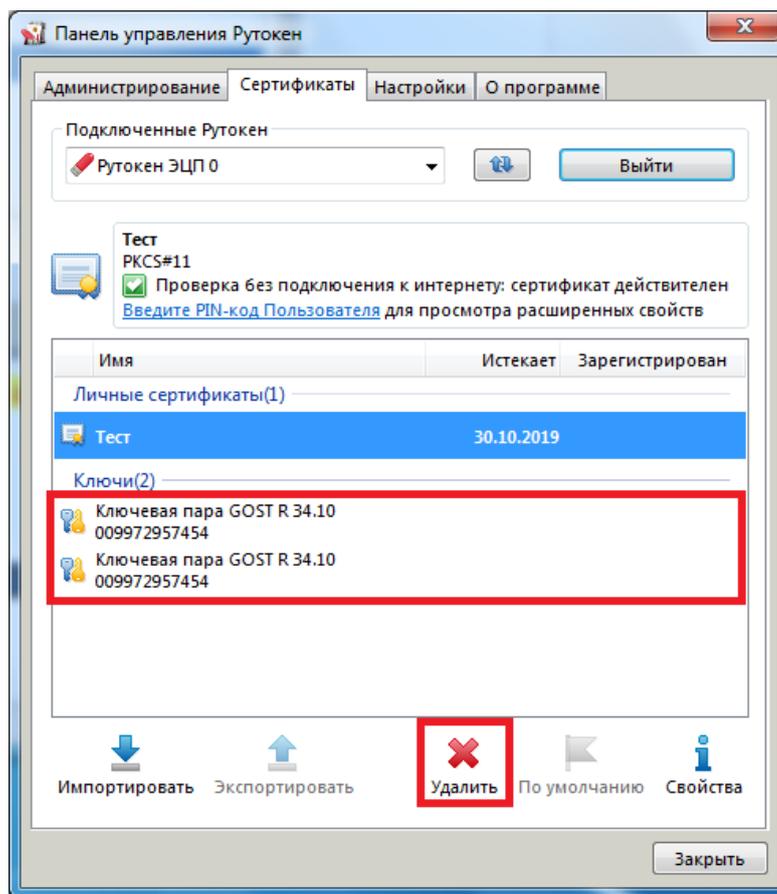
1. Вставить ключевой носитель Рутокен ЭЦП 2.0.
2. Запустить «Панель управления Рутокен».
3. На вкладке «Администрирование» нажать кнопку «Ввести PIN-код».

В появившемся окне ввести пин-код администратора **87654321** (по умолчанию).



4. На вкладке «Сертификаты» выбрать ключевую пару, которую нужно удалить, и нажать кнопку «Удалить». В появившемся окне ввести пин-код пользователя **12345678** (по умолчанию).

После установки сертификата на Рутокен ЭЦП 2.0 в панели управления могут быть видны «свободные» ключевые пары (выделены на рисунке ниже). Эти ключевые пары являются лишними и их необходимо удалить.



Важно!

- 1. Не удаляйте ключевые пары до загрузки сертификата!**
- 2. Внимательно выбирайте ключевую пару для удаления. Если удалить неверную ключевую пару, на которую выпущен сертификат, то повторный выпуск сертификата удостоверяющий центр может предложить оплатить дополнительно.**