

Руководство по настройке рабочего места пользователя ФГИС СОУТ

Оглавление

1. Получение ключа электронной подписи	1
2. Настройка входа в систему	2
Проверка установки КриптоПро CSP.....	2
Запуск КриптоПро CSP.....	3
Настройка КриптоПро CSP. Установка личного сертификата	4
Настройка КриптоПро CSP. Установка корневого сертификата	9
Настройка КриптоПро CSP. Установка прочих сертификатов	12
Установка списка отзыва сертификатов.....	12
3. Подача заявки на создание пользователя	15
4. Технические требования для использования системы ФГИС СОУТ	16

1. Получение ключа электронной подписи

Получить ключ электронной цифровой подписи можно, обратившись в аккредитованный удостоверяющий центр. Реестр аккредитованных удостоверяющих центров ведется на сайте [Минкомсвязи РФ](#). Удостоверяющий центр записывает сертификат на физический токен. Обычно удостоверяющий центр предоставляет токен, также его можно приобрести самостоятельно. Рекомендуется использовать токен, поддерживающий контейнеры КриптоПРО (Рутокен, EToken, JaCarta и др.). Сертификат, содержащий цифровую подпись, должен удовлетворять следующим требованиям:

1. Для получения государственных услуг, подписания заявлений, документов при электронном обращении в государственный орган путем подачи документа, подписанного сертификатом электронной подписи с возможностью проверки подлинности клиента, в состав сертификата должны быть включены расширения:
 - 1.1. Поле «Улучшенный ключ» должно содержать значение «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)».
 - 1.2. Поле «Использование ключа» должно содержать значение «Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)».
 - 1.3. Поле «Точки распространения списков отзыва CRL» должно содержать адреса точек распространения списков отзывов отозванных сертификатов, например:

[1]Точка распределения списка отзыва (CRL)
Имя точки распространения:

Полное имя:

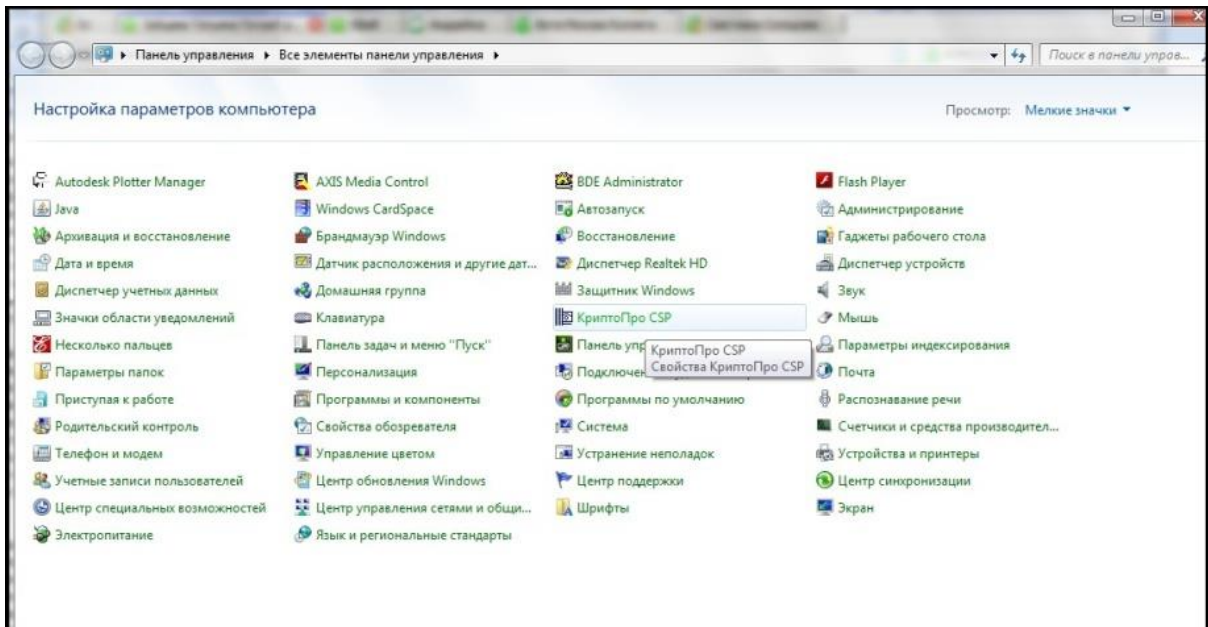
URL=http://taxor.ru/teor-2019_cp/l/tenca-2019_cp.crl

2. В состав сертификата электронной подписи для юридических и физических лиц, госучреждений при использовании для ФГИС СОУТ входят обязательные поля и компоненты:
 - 2.1. Поле «Версия» (version) должно иметь значение не ниже 3.
 - 2.2. Поле «Серийный номер» (serialNumber) должно содержать серийный номер сертификата, уникальный в пределах серийных номеров всех сертификатов, выданных удостоверяющим центром, издателем сертификата.
 - 2.3. Поле «Алгоритм подписи» должно содержать Алгоритм шифрования по ГОСТ Р 34.11-2012/34.10-2012, например 1.2.643.7.1.1.2.2, 1.2.643.7.1.1.3.2.
 - 2.4. Поле «Издатель сертификата» (issuer) должно содержать данные удостоверяющего центра, выдавшего сертификат.
 - 2.5. Поля «Действителен с» «Действителен по» должны содержать дату начала и дату истечения срока действия сертификата в формате UTC;
 - 2.6. Поле «Владелец сертификата» (Subject) содержит данные владельца подписи.
3. Усиленная квалифицированная электронная подпись (согласно Федеральному закону №63-ФЗ «Об электронной подписи» для создания и проверки ЭП должны использоваться средства криптозащиты, которые сертифицированы ФСБ РФ. Сертификаты квалифицированной ЭП выдаются аккредитованными удостоверяющими центрами [Перечень аккредитованных УЦ](#)).

2. Настройка входа в систему

Проверка установки КриптоПро CSP

Для того чтобы настроить доступ по ключу, на компьютере необходимо наличие установленного «КриптоПро CSP» версии не ниже 4.0. Проверить наличие «КриптоПро CSP» можно в «Панели управления» компьютера, там должен быть ярлык «КриптоПро CSP» как на рисунке:



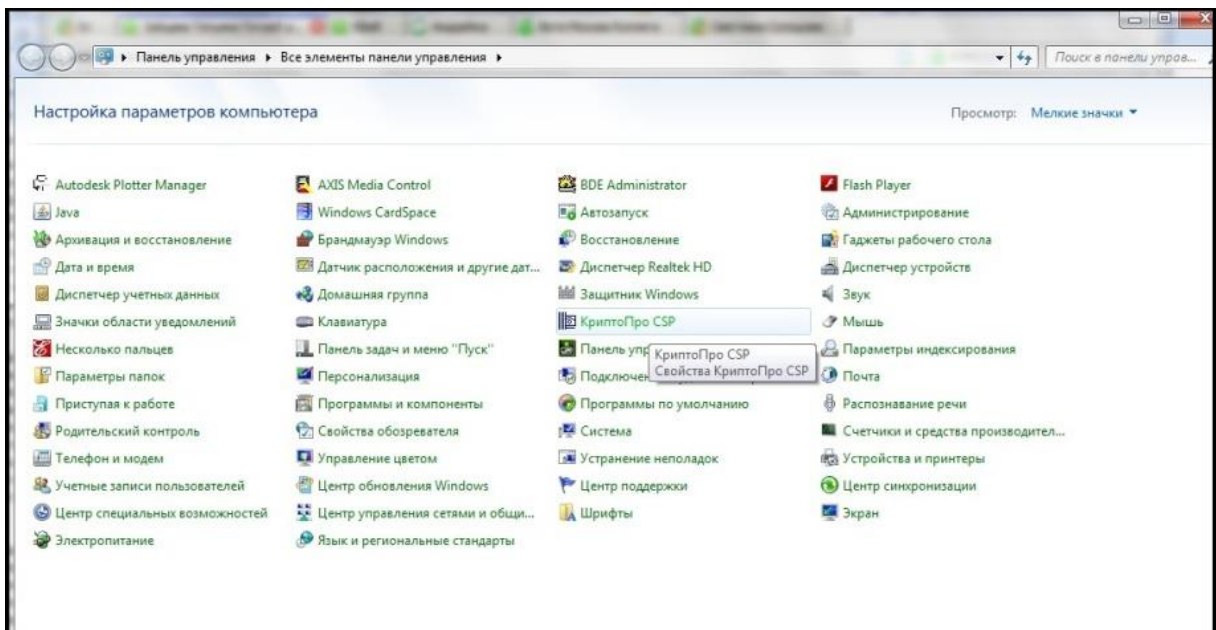
Если вы не обнаружили ярлык «КриптоПро CSP», то скачать программу можно отсюда - <https://www.cryptopro.ru/products/csp/downloads>

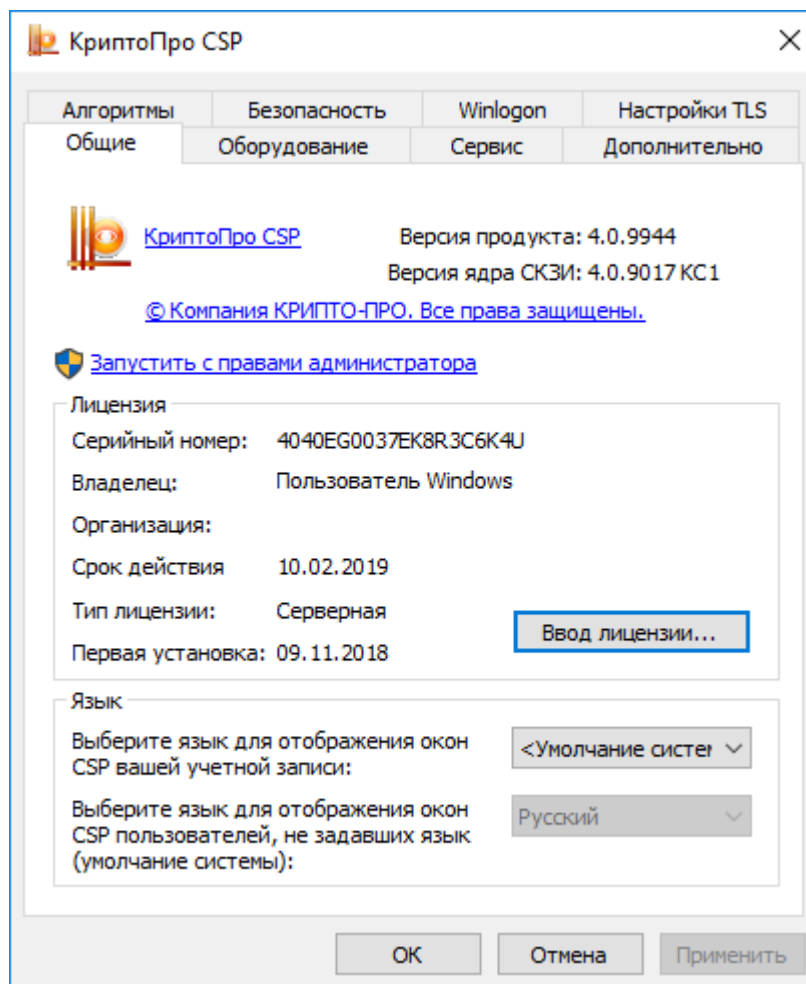
Если у вас ключ от производителя «Рутокен» (на нем написано «РУТОКЕН»), то помимо «КриптоПро CSP» необходимо установить «Драйверы Рутокен» и «Модуль поддержки КриптоПро CSP» для вашей операционной системы. Страница загрузки Драйвера Рутокен - <http://www.rutoken.ru/support/download/drivers-for-windows>

Страница загрузки Модуля поддержки КриптоПро CSP - <http://www.rutoken.ru/support/download/rutoken-for-cp>

Запуск КриптоПро CSP

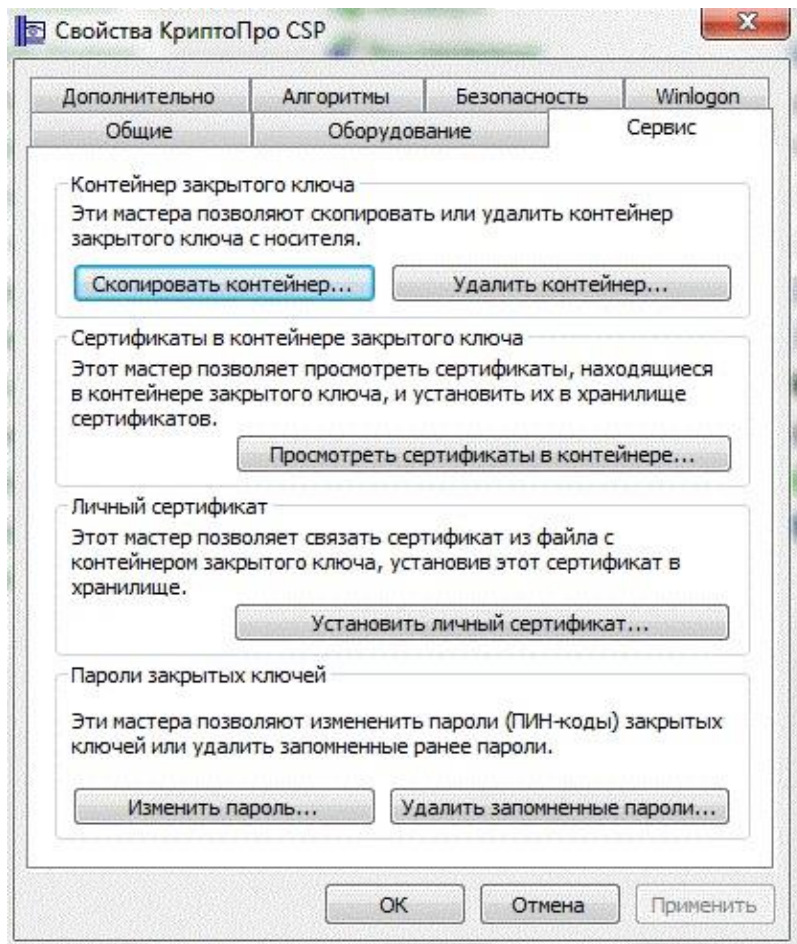
Нужно открыть «Панель управления» компьютера, где выбрать из списка программ КриптоПро CSP 4.0 и запустить ее. Сделать это можно двойным кликом левой кнопкой мыши на иконке программы.



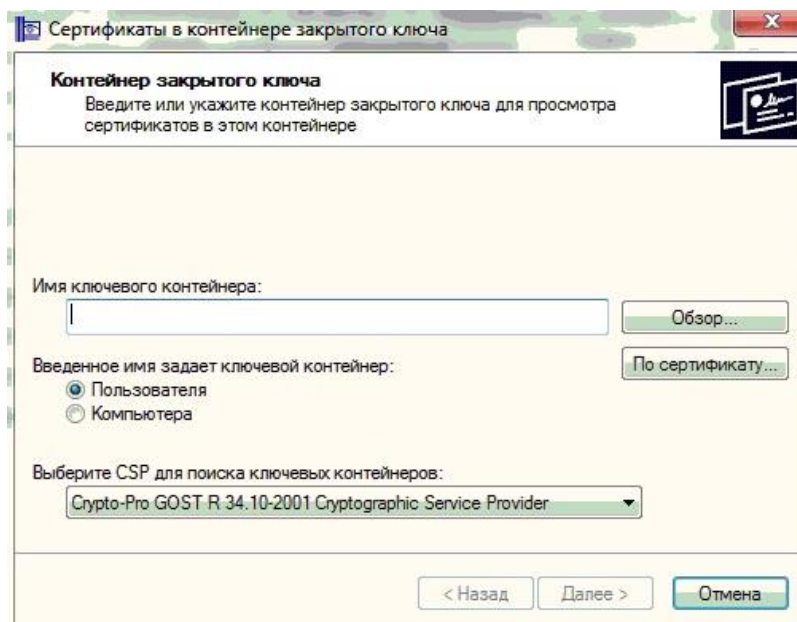


Настройка КриптоПро CSP. Установка личного сертификата

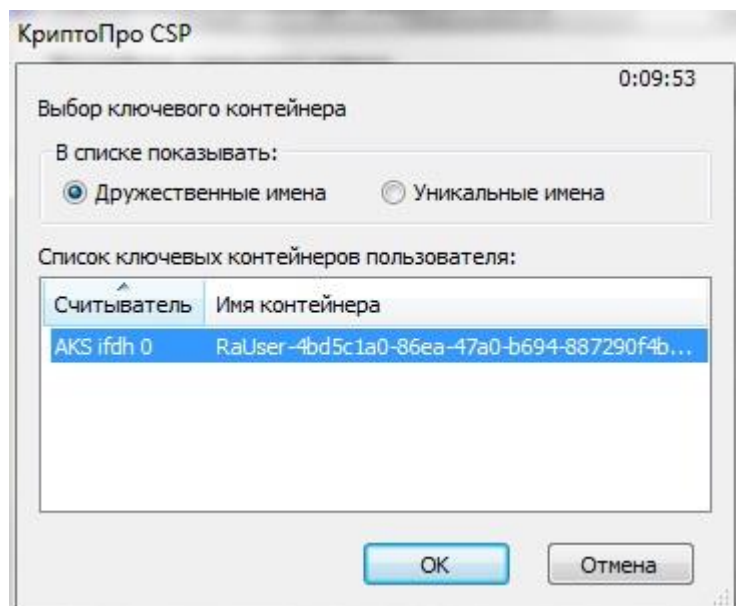
Запустив программу, мы видим окно с разными вкладками. Переходим на вкладку **«Сервис»**.



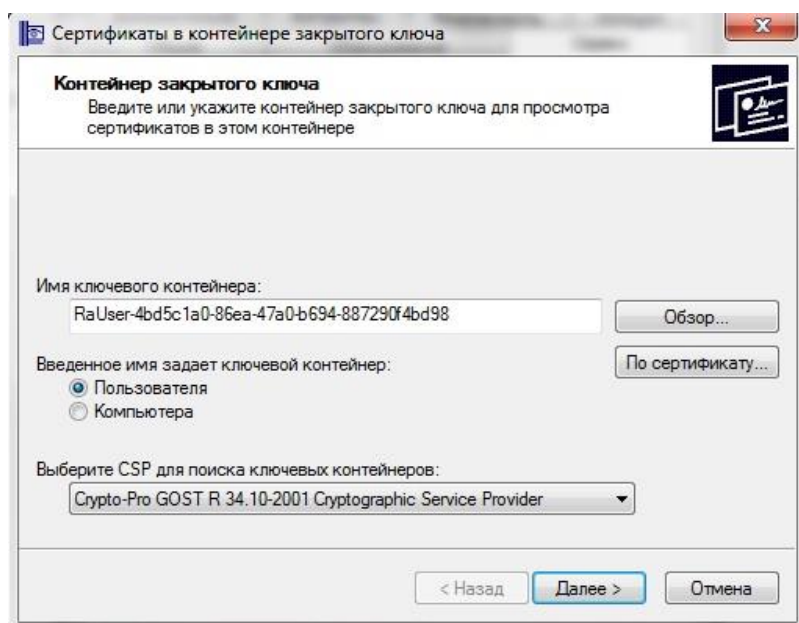
В открывшейся вкладке нужно выбрать пункт **«Просмотреть сертификаты в контейнере...»**.



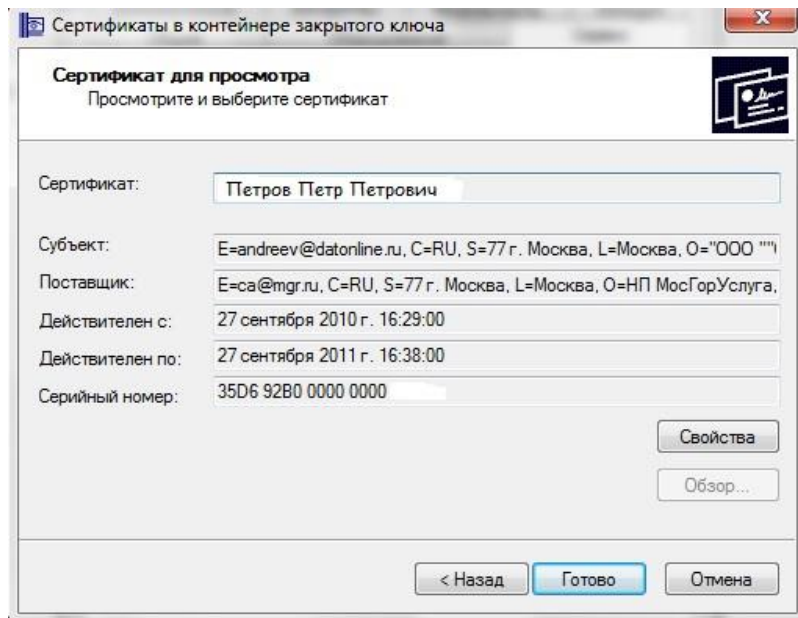
В окне пункта нажмите **«Обзор...»**, после чего появится еще одно окно демонстрирующее имя контейнера и доступный считыватель. Ознакомившись с полученной информацией, нажимаем кнопку **«ОК»**.



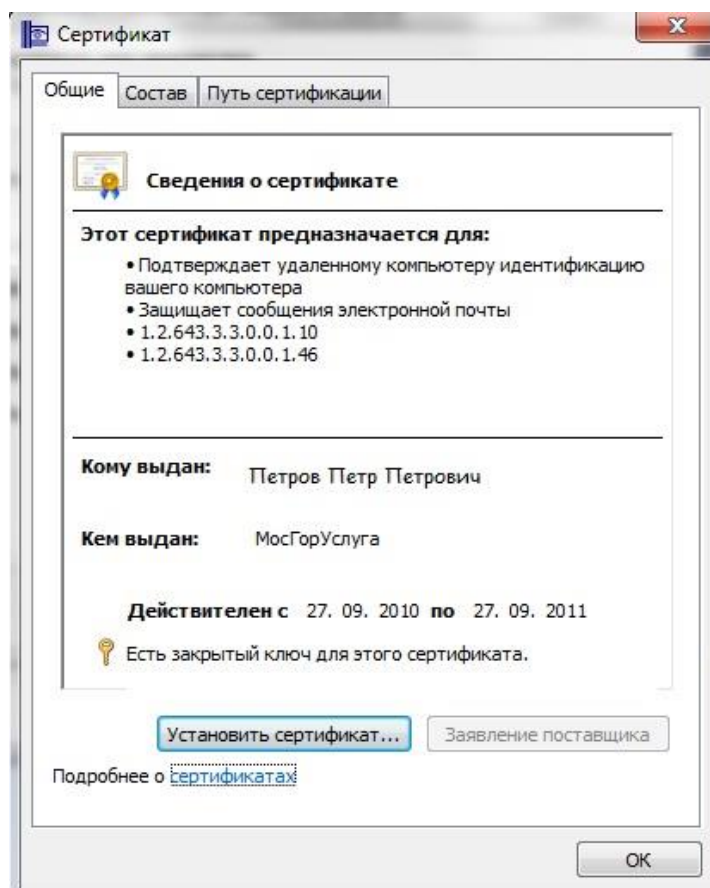
Появится окно **«Сертификаты в контейнере закрытого ключа»**, но никакие изменения в нем производить не нужно. Нажмите **«Далее»**.



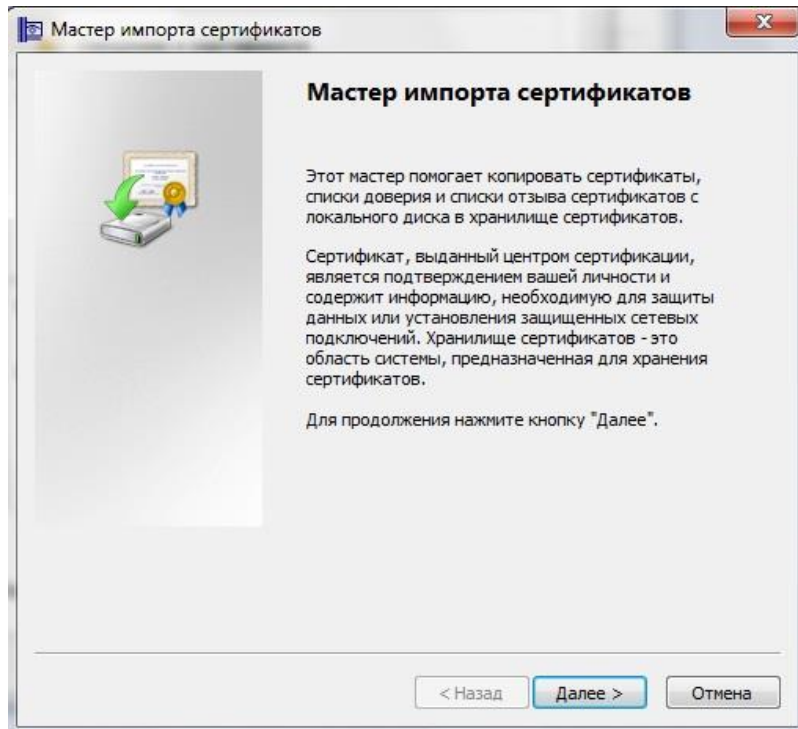
Перед вами окно, демонстрирующее информацию о пользователе, сроке действия электронной цифровой подписи, серийном номере. Нажмите **«Свойства»**.



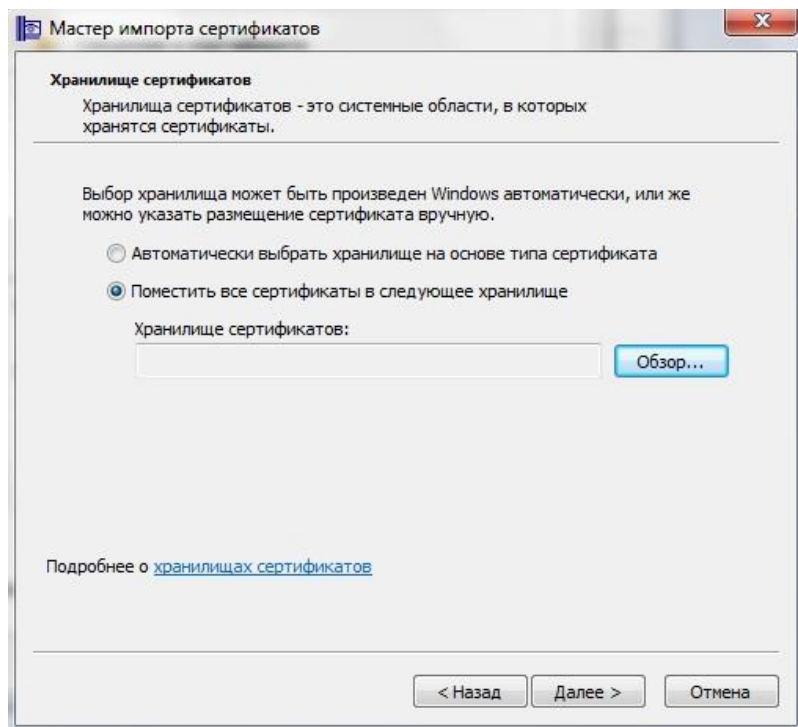
В открывшемся окне сертификата нужно установить новый с помощью кнопки **«Установить сертификат...»**.



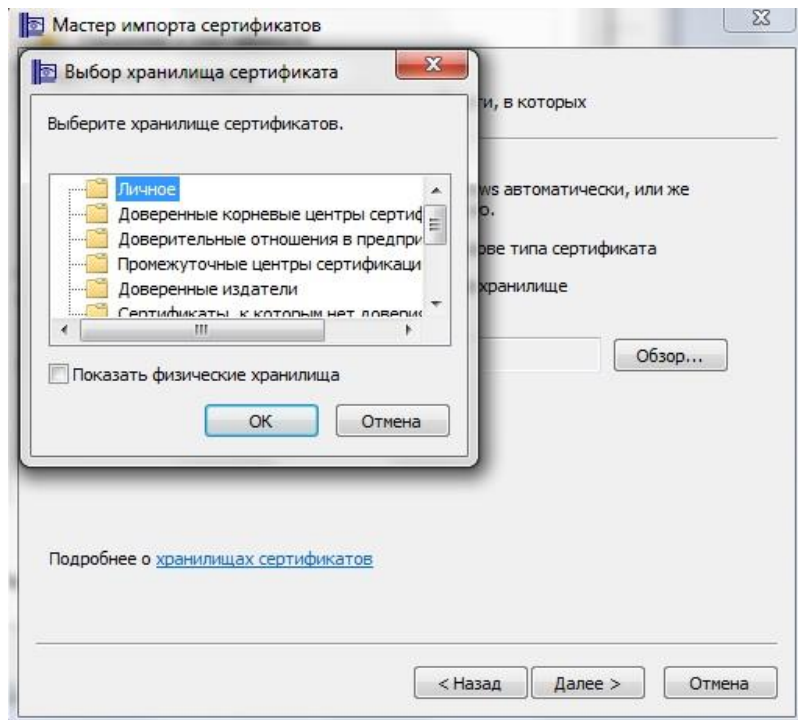
Откроется окно **«Мастер импорта сертификатов»**, ознакомившись с представленной информацией, нажимаем **«Далее»**.



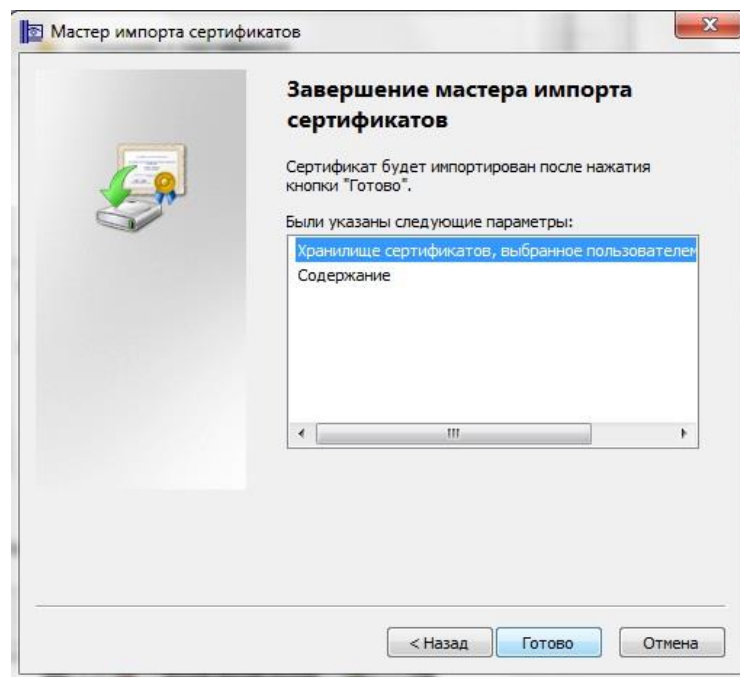
В открывшемся окне выберите пункт **«Поместить все сертификаты в следующее хранилище»** нажав **«Обзор...»**.



Выберите папку **«Личное»**, после чего нажмите **«ОК»**.



Сертификат установлен, нажмите кнопку **«Готово»**.

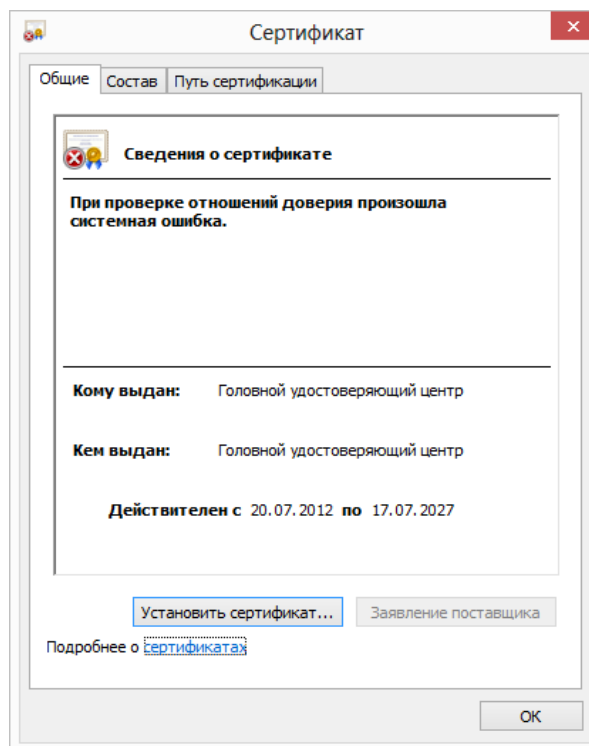


Настройка КриптоПро CSP. Установка корневого сертификата

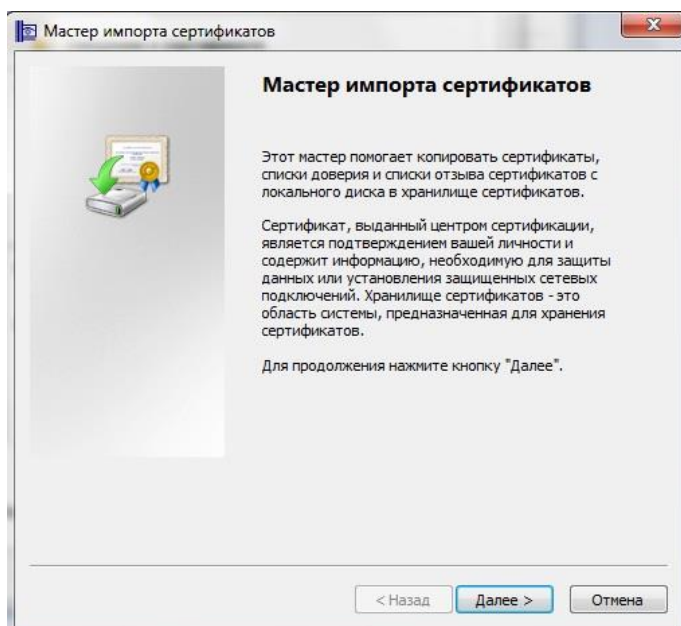
Скачайте корневые сертификаты с сайта Вашего удостоверяющего центра.

Кликните 2 раза на скачанном файле с расширением* .cer.

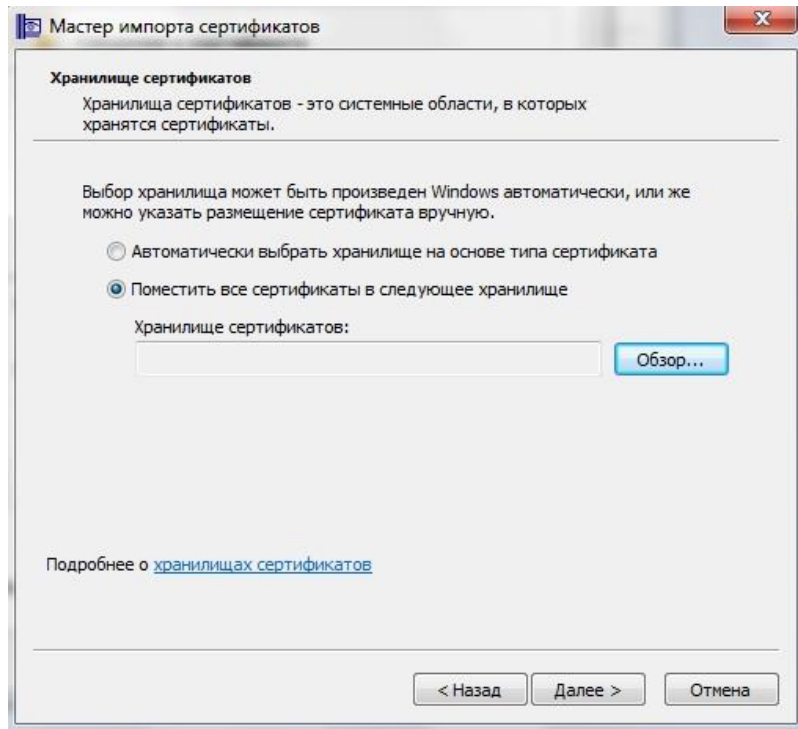
В открывшемся окне сертификата нужно установить новый с помощью кнопки **«Установить сертификат...»**.



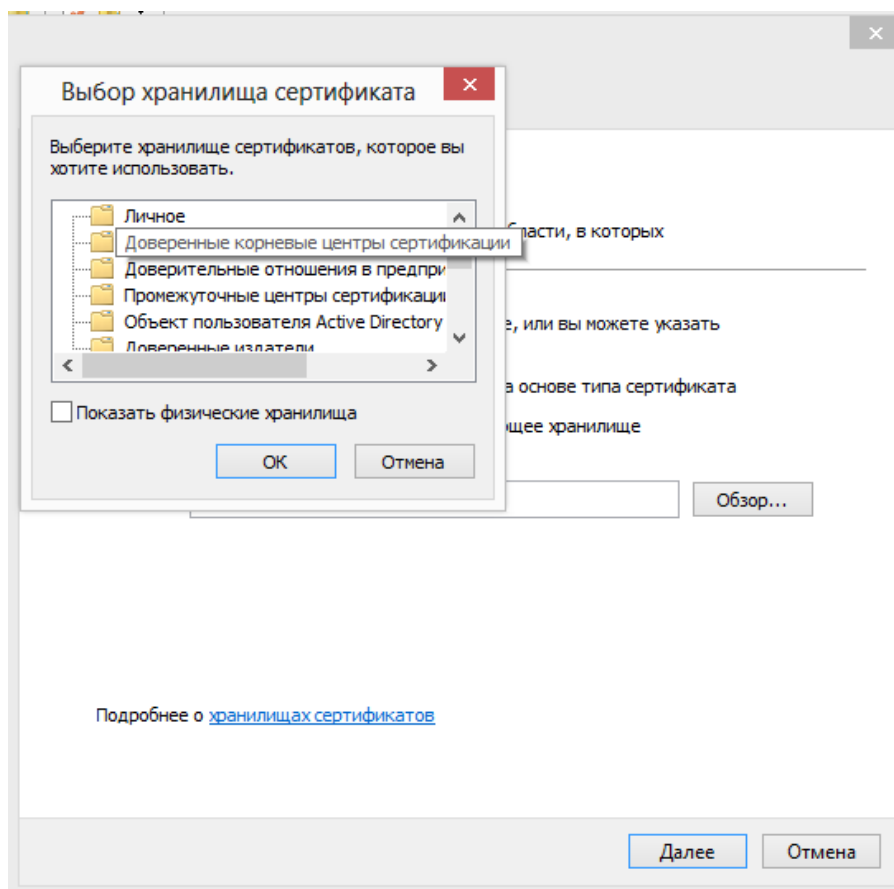
Откроется окно **«Мастер импорта сертификатов»**, ознакомившись с представленной информацией, нажимаем **«Далее»**.



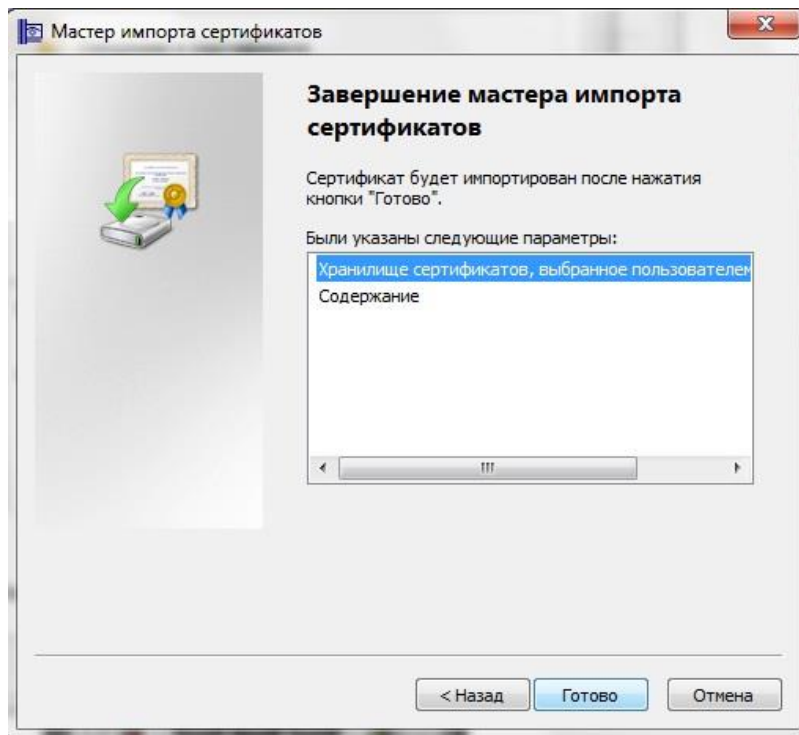
В открывшемся окне выберите пункт **«Поместить все сертификаты в следующее хранилище»** нажав **«Обзор...»**.



Выберите папку **«Доверенные корневые центры сертификации»**, после чего нажмите **«ОК»**.



Сертификат установлен, нажмите кнопку **«Готово»**.



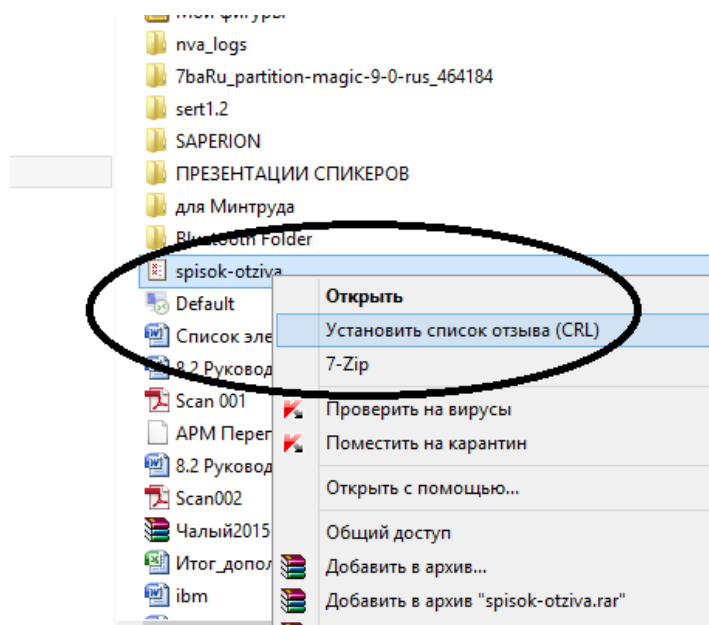
Настройка КриптоПро CSP. Установка прочих сертификатов

Аналогично следует произвести установку других корневых сертификатов, если их несколько.

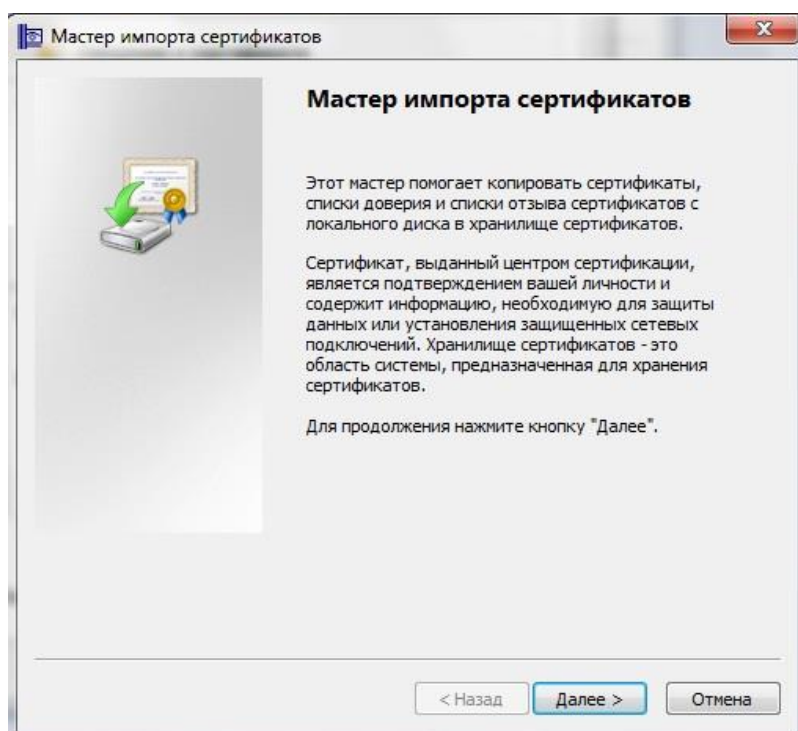
Установка списка отзыва сертификатов

Скачайте с сайта Вашего удостоверяющего центра список отзыва в формате *.crl (если таковой имеется). Если списка не имеется, пропустите этот пункт.

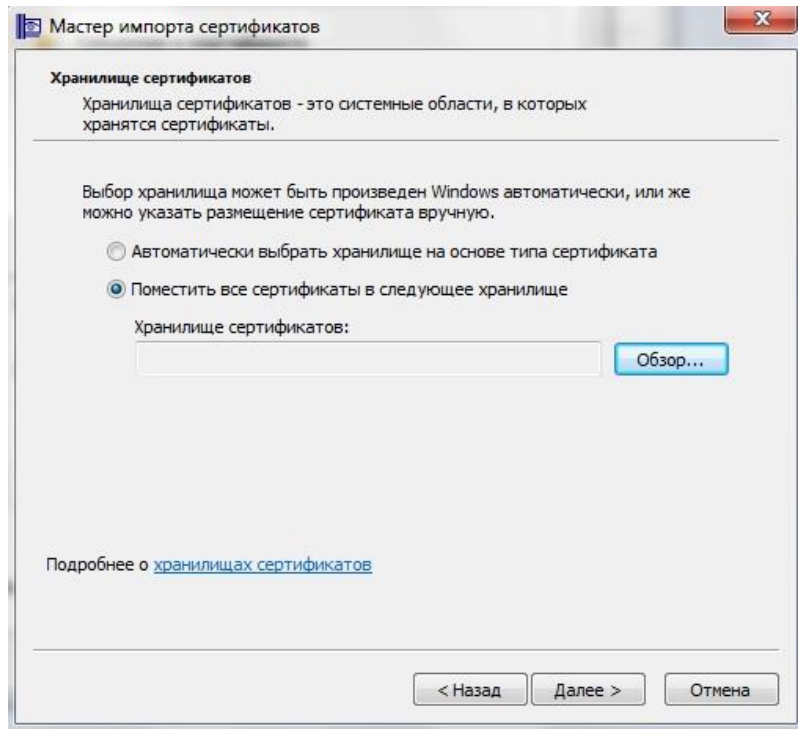
Правой кнопкой мыши нажмите на сохраненном файле и выберите пункт **"Установить список отзыва (crl)"**



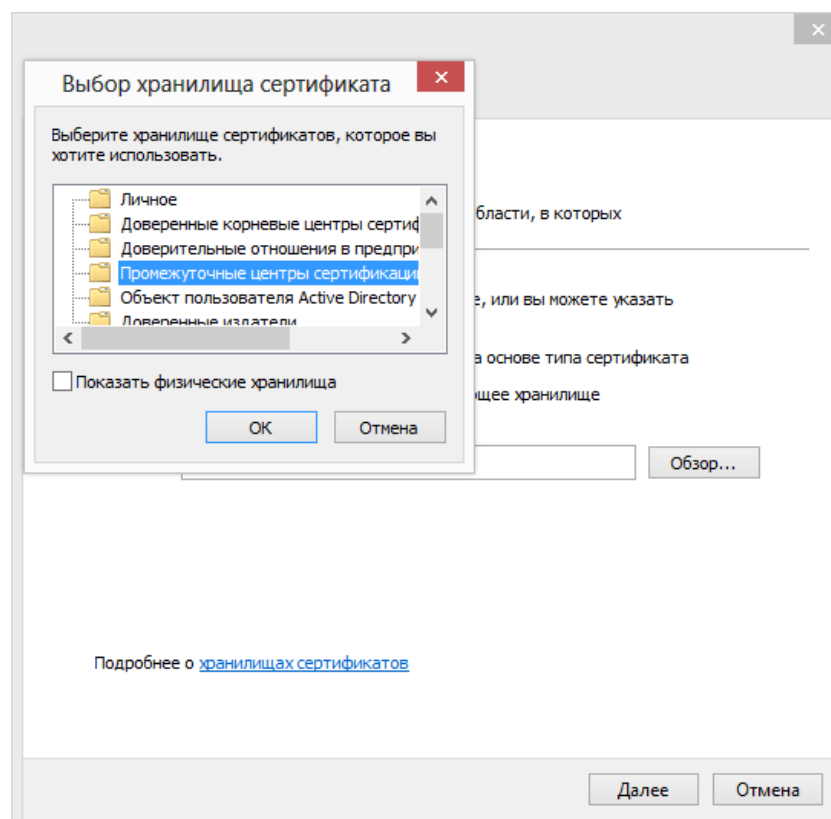
Откроется окно **«Мастер импорта сертификатов»**. Ознакомившись с представленной информацией, нажимаем **«Далее»**.



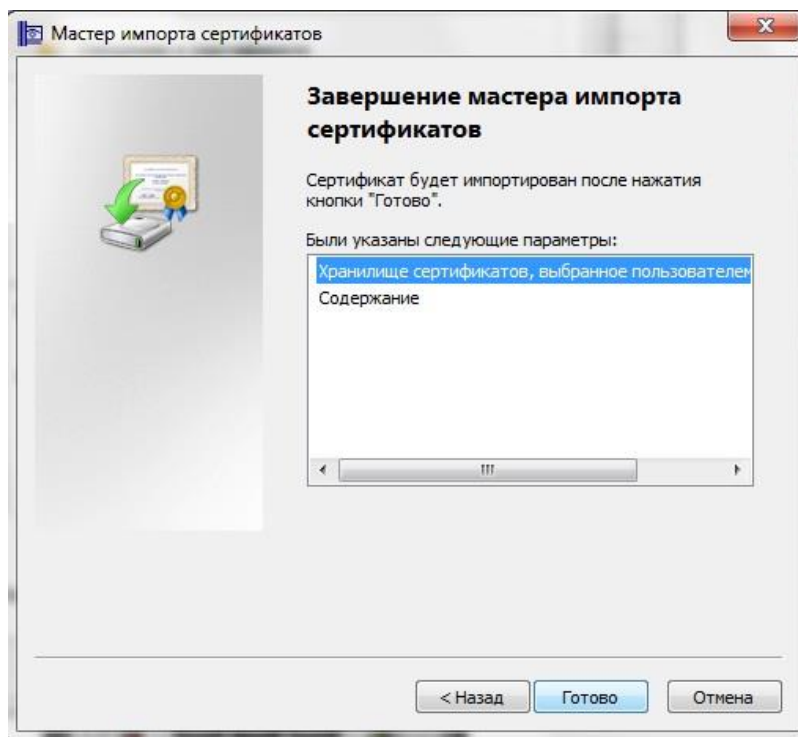
В открывшемся окне выберите пункт **«Поместить все сертификаты в следующее хранилище»** нажав **«Обзор...»**.



Выберете папку **«Промежуточные центры сертификации»**, после чего нажмите **«ОК»**.



Сертификат установлен, нажмите кнопку **«Готово»**.



3. Подача заявки на создание пользователя

Перейдите на сайт <http://akot.rosmintrud.ru/>

Выберите пункт «Заявка на создание пользователя». Откроется страница с формой заявки на создание пользователя ФГИС СОУТ:

Заявка на создание пользователей

[Руководство по настройке рабочего места пользователя ФГИС СОУТ](#)

Организация, проводящая СОУТ	<input type="text" value="не выбрано"/>
Открытая часть сертификата пользователя	<input type="text"/> Обзор...
Открытая часть корневого сертификата Удостоверяющего центра	<input type="text"/> Обзор...
Контактный Email	<input type="text"/>
Контактный телефон	<input type="text"/>
Примечание	<input type="text"/>

Если пользователь является сотрудников организации, проводящей СОУТ необходимо выбрать соответствующую организацию в выпадающем списке «Организация, проводящая СОУТ», затем необходимо приложить файлы сертификатов пользователя и удостоверяющего центра с расширением «cer», и заполнить поля «Контактный Email», «Контактный телефон», по которым в

случае необходимости сотрудники Минтруда России смогут связаться с заявителем. В поле «Примечание» можно оставить комментарии.

После заполнения всех обязательных полей необходимо нажать кнопку «Сохранить». Система отправит запрос на создание пользователя в ФГИС СОУТ, после чего отобразит страницу с присвоенным заявке уникальным номером, по которому можно будет уточнить статус обработки заявки в Минтруде России.

4. Технические требования для использования системы ФГИС СОУТ

- Токен поддерживающий контейнеры КриптоПРО
- Сертификат ключа проверки электронной подписи, выданный, одним из [аккредитованных удостоверяющих центров](#).
- Установить сертификаты доверенных корневых центров сертификации в папку [Доверенные корневые центры сертификации](#).
- Рекомендуемая версия [КриптоПРО](#) 4.0 и выше.
- Internet Explorer 9 и выше.
- В настройках браузера включена поддержка SSL, TLS.
- Адрес <https://sout.rosmintrud.ru> добавлен в надежные сайты.
- Установлен плагин КриптоПРО CADESCOM (версия 2) со страницы <http://www.cryptopro.ru/downloads>.
- Установлены все критические [обновления Windows](#).
- Операционная система Windows 7, 8, 8.1, 10 (x86 и x64)

Если на компьютере установлено антивирусное ПО, то рекомендуется его отключить или обратиться к системному администратору для его настройки.

Проверить доступ к защищенной части ФГИС СОУТ можно открыв эту ссылку – <https://sout.rosmintrud.ru> в браузере Internet Explorer версии не ниже 9.0.

Если все было настроено правильно, то после перехода по ссылке откроется окно выбора установленного сертификата пользователя, вы выбираете конкретного пользователя и нажимаете «ОК». Если в компьютер вставлен ключ выбранного пользователя, то откроется защищённая часть ФГИС СОУТ.