

# Установка сертификатов и списка отозванных сертификатов

15.02.2012

НП НУЦ

Гудилина Н.С., Бойков Л.В.

## Оглавление

1.	Установка корневых сертификатов НУЦ.....	3
2.	Установка списка отозванных сертификатов (CRL).....	6
3.	Установка личных сертификатов.....	8

## 1. Установка корневых сертификатов НУЦ

Сертификаты и списки отозванных сертификатов публикуются на сайте Удостоверяющего центра по адресу <http://www.nucrf.ru> в разделе «Информация о сертификатах» (См. Рис. 1.1):

**ВНИМАНИЕ!** Для работы с электронной подписью необходимо установить на компьютер сертификат владельца, корневые сертификаты удостоверяющего центра и списки отозванных сертификатов (в зависимости от даты выпуска сертификата владельца). Порядок установки изложен в "[Инструкции](#)".

Дата выпуска сертификата владельца	Корневые сертификаты УЦ и списки отозванных сертификатов
с 11.02.2012	Корневые сертификаты: <a href="#">ta03.cer</a> <a href="#">ta23.cer</a> Списки отозванных сертификатов: <a href="#">ta03.crl</a> <a href="#">ta23.crl</a>
с 03.09.2011 по 10.02.2012	Корневые сертификаты: <a href="#">ta02.cer</a> <a href="#">ta22.cer</a> Списки отозванных сертификатов: <a href="#">ta02.crl</a> <a href="#">ta22.crl</a>
с 10.09.2009 по 02.09.2011	Корневые сертификаты: <a href="#">ta0.cer</a> <a href="#">ta2.cer</a> Списки отозванных сертификатов: <a href="#">ta0.crl</a> <a href="#">ta2.crl</a>

Рис. 1.1. Страница сайта с информацией о сертификатах

Для начала работы необходимо скачать корневые сертификаты Удостоверяющего Центра. Если сертификат владельца выпущен в период с 10.09.2009 по 02.09.2011, то необходимо скачать сертификаты **ta0.cer** и **ta2.cer**. Если сертификат владельца выпущен в период с 03.09.2011 по 10.02.2012, то необходимо скачать сертификаты **ta02.cer** и **ta22.cer**. Если сертификат владельца выпущен после 10.02.2012, то необходимо скачать сертификаты **ta03.cer** и **ta23.cer**.

**ВНИМАНИЕ! Запомните место, куда Вы сохранили файлы!**

Для установки сертификата Удостоверяющего центра **ta0.cer**, **ta02.cer** или **ta03.cer** необходимо открыть в Проводнике папку, куда был сохранен файл **ta0.cer**, **ta02.cer** или **ta03.cer**, и по нажатию правой кнопки мыши на файле **ta0.cer**, **ta02.cer** или **ta03.cer** в контекстном меню выбрать пункт «Установить сертификат».

В результате выполненных действий откроется страница приветствия «Мастера импорта сертификатов». В этом окне необходимо нажать кнопку «Далее» (См. Рис. 1.2):

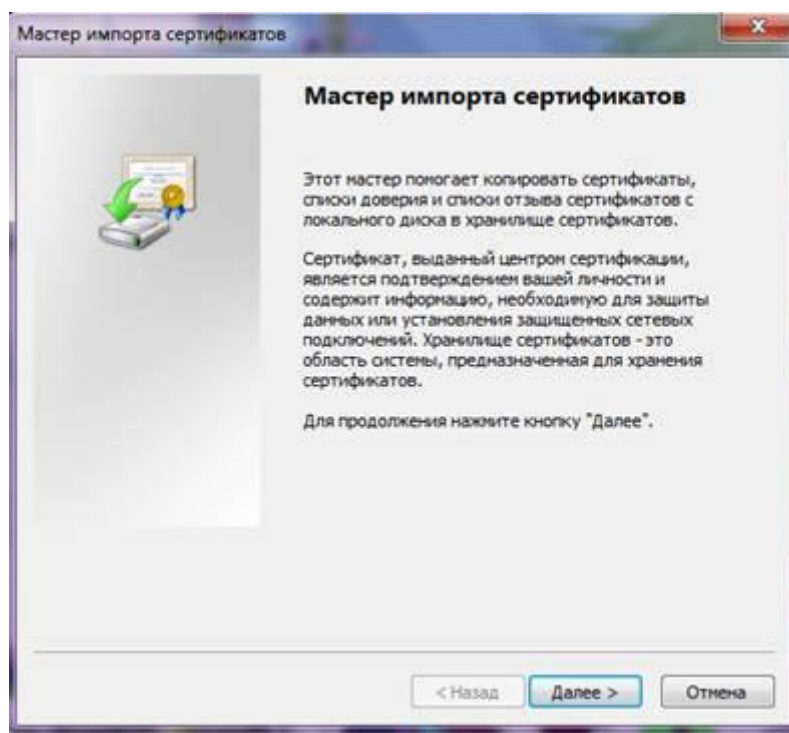


Рис. 1.2. Окно приветствия мастера импорта сертификатов

Откроется страница «**Хранилище сертификатов**». На этой странице необходимо установить переключатель в позицию «**Поместить все сертификаты в следующее хранилище**» и затем нажать кнопку «**Обзор**» (См. Рис. 1.3):

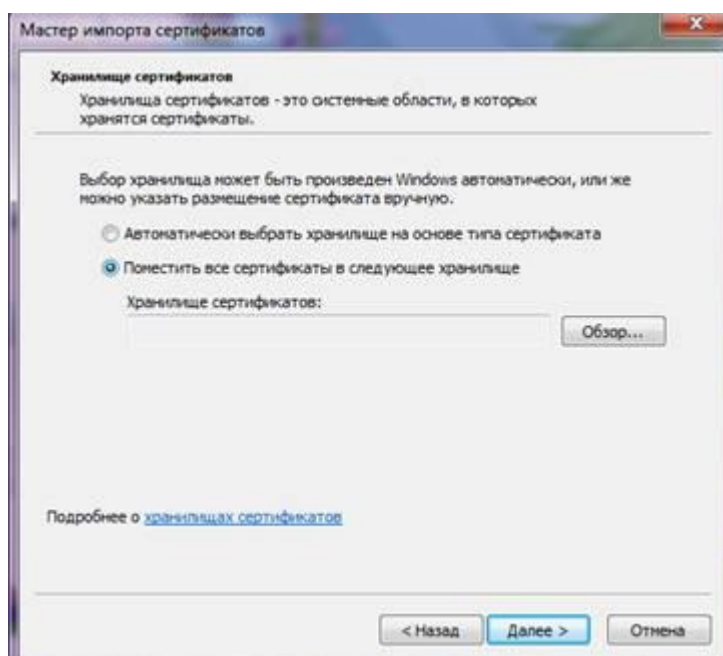


Рис. 1.3. Хранилище сертификатов

Откроется окно «**Выбор хранилища сертификата**». В этом окне необходимо выбрать хранилище «**Доверенные корневые центры сертификации**» и нажать кнопку «**ОК**» (См. Рис. 1.4):

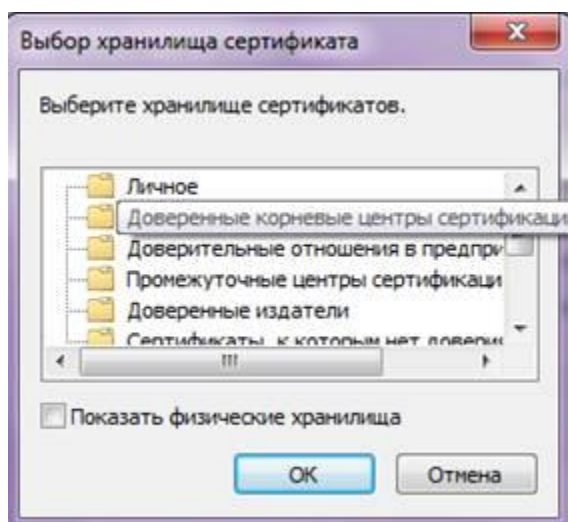


Рис. 1.4. Выбор хранилища сертификата

Окно **«Выбор хранилища сертификата»** закроется. Мастер установки сертификатов вернется на страницу **«Хранилище сертификатов»**. Необходимо нажать кнопку **«Далее»**. Мастер установки сертификатов перейдет на страницу **«Завершение мастера импорта сертификатов»**. Необходимо нажать кнопку **«Готово»** (См. Рис. 1.5):

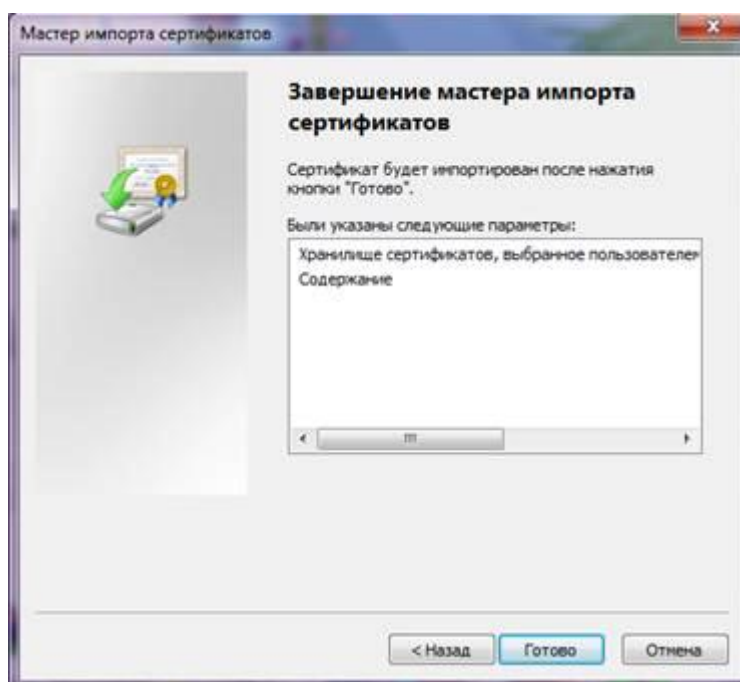


Рис. 1.5. Завершение мастера импорта сертификатов

В некоторых случаях может появиться предупреждение системы безопасности о том, что готовится сертификата от центра сертификации НП НУЦ. На вопрос о том, следует ли установить сертификат необходимо ответить утвердительно, нажав кнопку **«Да»** (См. Рис. 1.6):

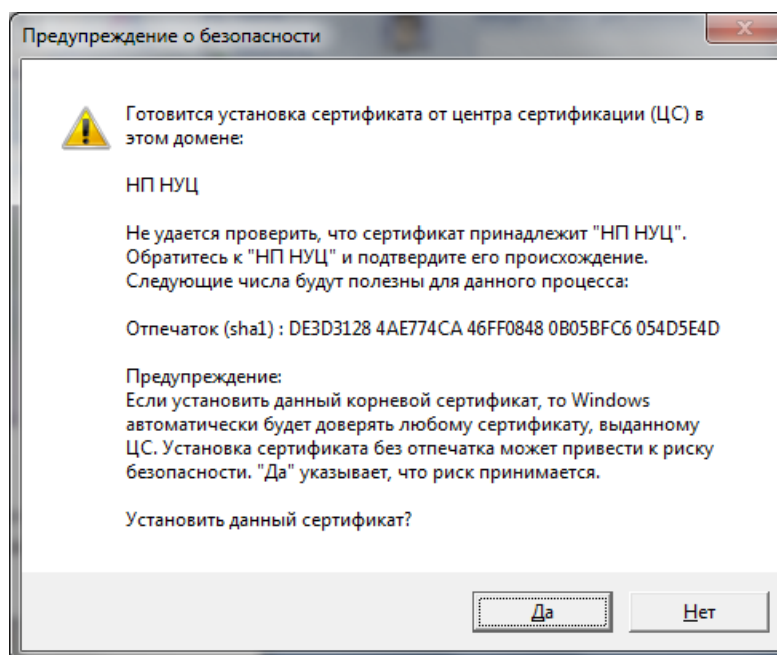


Рис. 1.6. Предупреждение о безопасности

Установка сертификата Удостоверяющего центра **ta0.cer**, **ta02.cer** или **ta03.cer** завершена.

Для установки сертификата **ta2.cer**, **ta22.cer** или **ta23.cer** необходимо повторить указанные выше действия, за исключением того, что при выборе хранилища сертификатов необходимо выбрать хранилище «**Промежуточные центры сертификации**» (См. Рис. 1.3 и Рис. 1.4).

## 2. Установка списка отозванных сертификатов (CRL)

Для начала работы необходимо скачать списки отозванных сертификатов Удостоверяющего Центра. Если сертификат владельца выпущен в период с 10.09.2009 по 02.09.2011, то необходимо скачать сертификаты **ta0.crl** и **ta2.crl**. Если сертификат владельца выпущен в период с 03.09.2011 по 10.02.2012, то необходимо скачать сертификаты **ta02.crl** и **ta22.crl**. Если сертификат владельца выпущен после 10.02.2012, то необходимо скачать сертификаты **ta03.crl** и **ta23.crl**.

**ВНИМАНИЕ! Запомните место, куда Вы сохранили файлы!**

Для установки списков отозванных сертификатов Удостоверяющего центра **ta0.crl**, **ta02.crl** или **ta03.crl** необходимо открыть в Проводнике папку, куда был сохранен файл **ta0.crl**, **ta02.crl** или **ta03.crl** и по нажатию правой кнопки мыши на файле **ta0.crl**, **ta02.crl** или **ta03.crl** в контекстном меню выбрать пункт «**Установить список отзыва (CRL)**».

В результате выполненных действий откроется страница приветствия «**Мастера импорта сертификатов**». В этом окне необходимо нажать кнопку «**Далее**» (См. Рис. 1.2).

Откроется страница «**Хранилище сертификатов**». На этой странице необходимо установить переключатель в позицию «**Поместить все сертификаты в следующее хранилище**» и затем нажать кнопку «**Обзор**» (См. Рис. 1.3).

Откроется окно «**Выбор хранилища сертификата**». В этом окне необходимо выбрать хранилище «**Промежуточные центры сертификации**» и нажать кнопку «**ОК**» (См. Рис. 1.4).

Окно «**Выбор хранилища сертификата**» закроется. Мастер установки сертификатов вернется на страницу «**Хранилище сертификатов**». Необходимо нажать кнопку «**Далее**». Мастер установки

сертификатов перейдет на страницу «**Завершение мастера импорта сертификатов**». Необходимо нажать кнопку «**Готово**» (См. Рис. 1.5).

Установка списка отозванных сертификатов **ta0.crl**, **ta02.crl** или **ta03.crl** завершена.

Для установки списка отозванных сертификатов **ta2.crl**, **ta22.crl** или **ta23.crl** необходимо повторить указанные выше действия, также указав при выборе хранилища сертификатов хранилище «**Промежуточные центры сертификации**» (См. Рис. 1.3 и Рис. 1.4).

### 3. Установка личных сертификатов

На сайте Удостоверяющего центра в разделе **«Информация о сертификатах»** предоставляется возможность осуществлять поиск сертификатов пользователей Национального Удостоверяющего Центра.

Для поиска сертификата необходимо в поисковой форме указать **Фамилию** и/или **Имя** и/или **Отчество** и/или **«Наименование организации»**. Также можно ограничить либо расширить область поиска сертификатов по введенным параметрам с помощью раздела **«Только действующие»**, достаточно перенести переключатель в нужную позицию.

Установка личного сертификата начинается с того момента как Вы сохранили файл своего сертификата на своем компьютере в удобном для Вас месте. Далее Вам необходимо выполнить следующие действия: последовательно выберите меню **Пуск**→**Настройка**→**Панель управления** (В случае, если на компьютере установлена ОС – Windows XP). В появившемся окне выберите **КриптоПро CSP** и запустите ее, дважды кликнув мышкой.

В появившемся окне **«КриптоПРО CSP»** необходимо перейти на вкладку **«Сервис»** (См. Рис. 3.1):

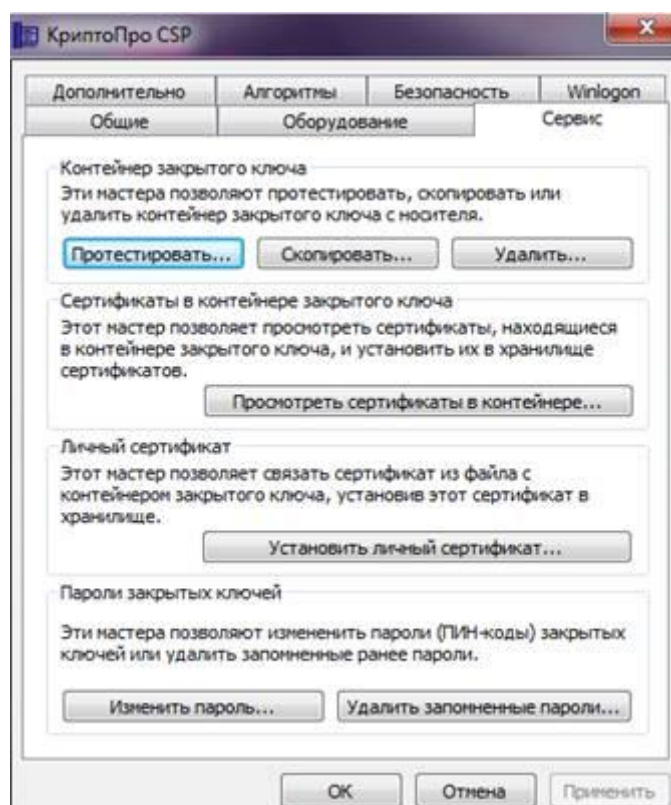


Рис. 3.1. КриптоПРО CSP. Вкладка «Сервис»

Далее, в разделе **«Личный сертификат»** необходимо нажать кнопку **«Установить личный сертификат»**. В открывшемся окне **«Мастера установки личного сертификата»** необходимо указать место расположения файла сертификата. Для этого необходимо нажать кнопку **«Обзор»** и указать местоположение файла сертификата. Необходимо нажать кнопку **«Далее»** (См. Рис. 3.2):

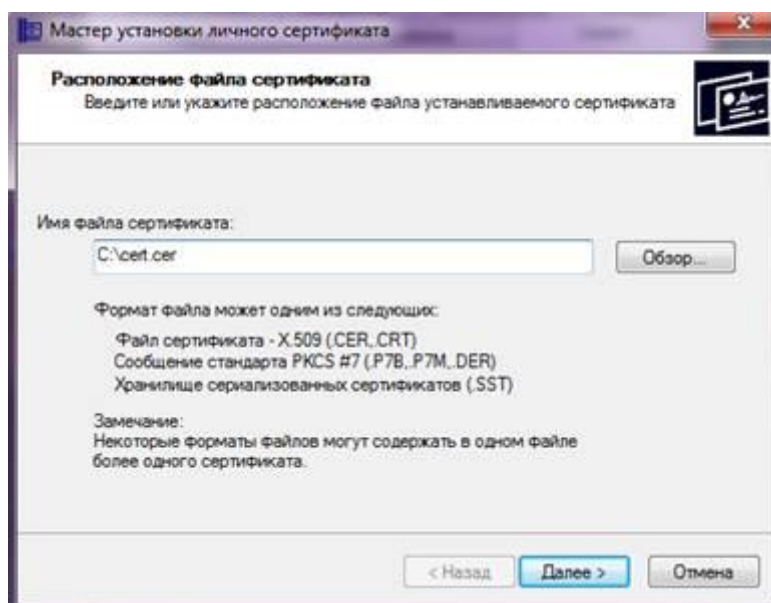


Рис. 3.2 Расположение файла сертификата

В следующем окне мастера с подзаголовком **«Сертификат для установки»** появится информация о выбранном сертификате. Необходимо нажать кнопку **«Далее»** (См. Рис. 3.3):

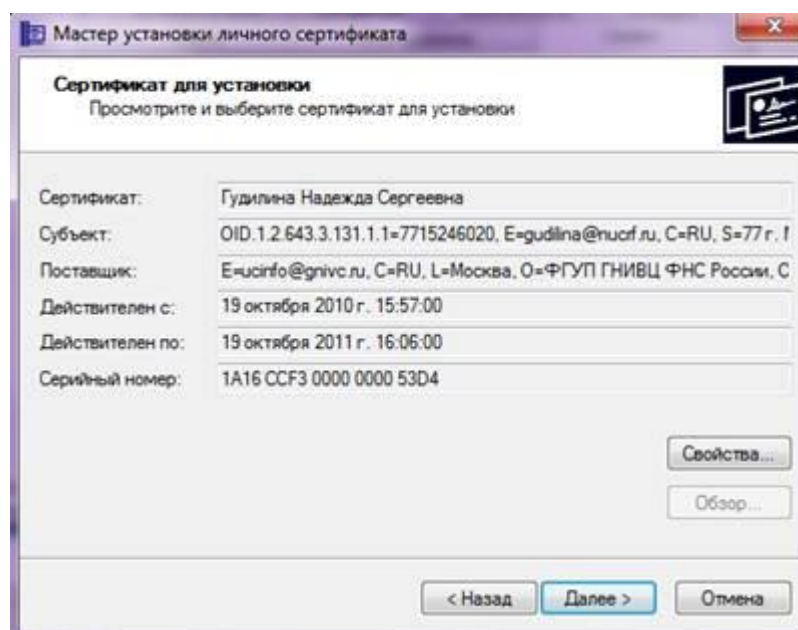


Рис. 3.3 Сертификат для установки

После выбора сертификата Мастер установки личного сертификата предложит указать имя ключевого контейнера, в котором размещен секретный ключ. Секретный ключ должен соответствовать открытому ключу, опубликованному в сертификате (осуществляется привязка ключа к сертификату). Чтобы найти и указать нужный ключевой контейнер необходимо выполнение следующих основных условий:

- к USB разъему подключен ключевой носитель, в котором содержится контейнер с вашим секретным ключом;

## Установка сертификатов и списка отозванных сертификатов

- в текущем окне, в разделе **«Выберете CSP для поиска ключевых контейнеров»** указан CSP, соответствующий формату криптоалгоритма, с помощью которого были сформированы электронные ключи (ключевая пара), в нашем случае это Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider, и эта настройка выбрана по умолчанию;

- в текущем окне в разделе **«Введенное имя задает ключевой контейнер»** переключатель должен стоять в позиции Пользователь.

После выполнения описанных выше условий необходимо нажать кнопку **«Обзор»** (См. Рис. 3.4):

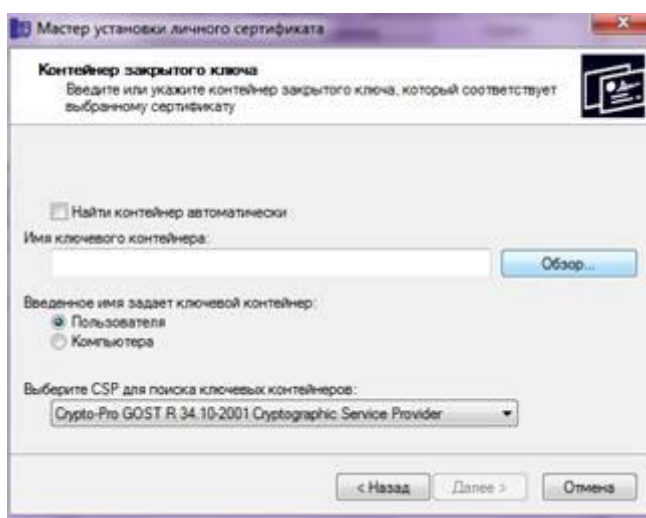


Рис. 3.4. Контейнер закрытого ключа

В результате описанных действий на экране появится окно **«Выбор ключевого контейнера»**. В этом окне необходимо выделить нужный ключевой контейнер и нажать кнопку **«ОК»**. Как правило, высвечивается один ключевой контейнер, который и надо выбрать (См. Рис. 3.5):

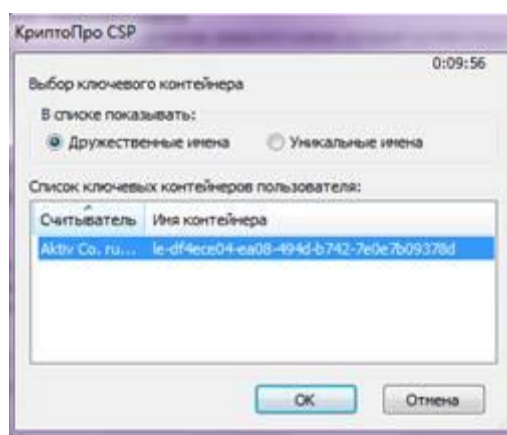


Рис. 3.5. Выбор ключевого контейнера

**Примечание:** в случае, если Вы забыли вставить ключевой носитель или система не нашла подходящий ключевой носитель или Вы неправильно ввели пароль, на экране появится окно уведомления, в котором будет отображено сообщение о несоответствии закрытого ключа

открытому ключу, опубликованному в сертификате. В этом случае необходимо подключить носитель с секретным ключом, соответствующим устанавливаемому сертификату (См. Рис. 3.6):

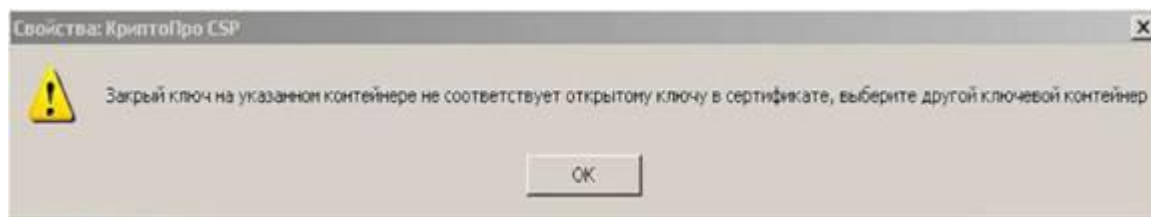


Рис. 3.6. Уведомление о несоответствии закрытого ключа открытому ключу

После того, как все поля Мастера установки личного сертификата заполнены, необходимо нажать кнопку **«Далее»**.

**«Мастер установки личного сертификата»** выполнит обращение к контейнеру с секретным ключом, в ответ на экране появится окно ввода пароля доступа к ключевому носителю:

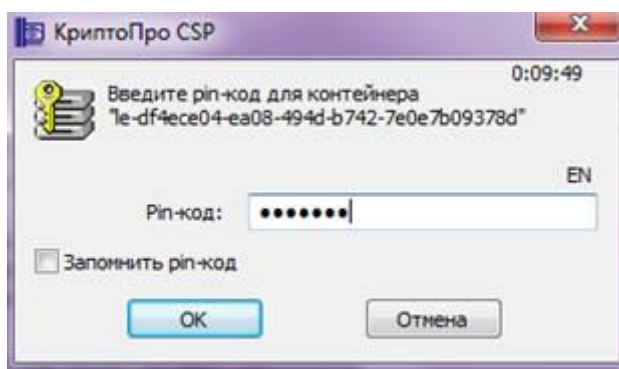


Рис. 3.7. Ввод PIN-кода

**Примечание:** при размещении ключевого контейнера на внешнем ключевом носителе пароль доступа к ключевому контейнеру будет совпадать с паролем доступа к ключевому носителю.

Необходимо ввести pin-код для контейнера и нажать кнопку **«ОК»**. В случае правильного ввода пароля доступа к ключевому контейнеру(ключевому носителю) Мастер установки личного сертификата продолжит свою работу. Если пароль доступа введен неправильно, система предложит вам повторить попытку, после повторных неудачных попыток ввода пароля мастер выдаст сообщение, отображенное на Рис. 3.6.

**Внимание!** На внешних ключевых носителях, подключаемых к USB разъему, стоит ограничение на допустимое количество неудачных попыток ввода пароля. В результате достижения критического значения количества неудачных попыток ключевой носитель **блокируется**, и дальнейшая работа с ним будет невозможна без вмешательства специалиста Удостоверяющего центра.

После успешного ввода пароля доступа к ключевому носителю **«Мастер установки личного сертификата»** откроет окно с подзаголовком **«Хранилище сертификатов»** (Окно выбора хранилища сертификатов). Для выбора хранилища **«Личные»** необходимо нажать кнопку **«Обзор»** в текущем окне мастера (См. Рис. 3.8).

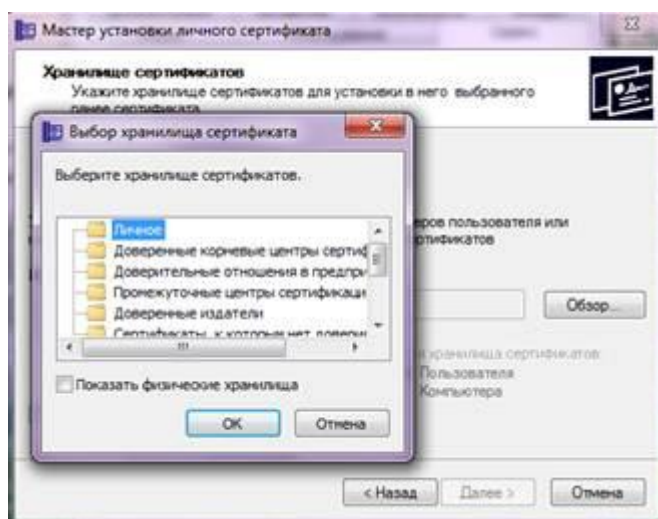


Рис. 3.8 Выбор хранилища сертификатов

После выбора хранилища сертификатов необходимо нажать кнопку **«Далее»**.

В результате **«Мастер установки личного сертификата»** перейдет к завершающей стадии установки личного сертификата - в окне мастера отобразится итоговая информация. Для завершения работы мастера необходимо нажать кнопку **«Готово»** (См. Рис. 3.9)

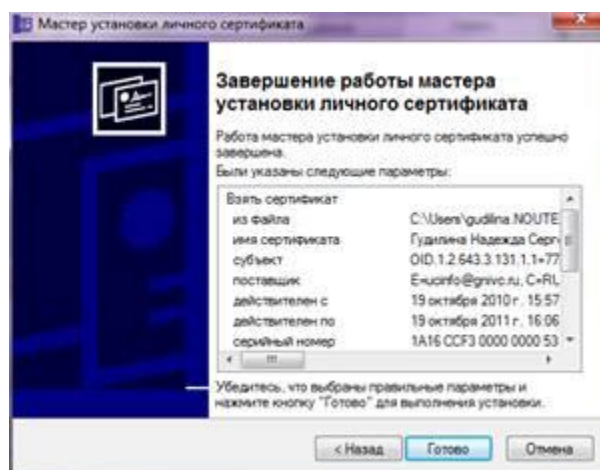


Рис. 3.9. Завершение работы мастера установки