

# **Руководство пользователя**

## Установка сертификатов

## ОГЛАВЛЕНИЕ

|   |   |
|---|---|
| НЕОБХОДИМЫЕ КОМПОНЕНТЫ .....              | 2 |
| ПОРЯДОК УСТАНОВКИ.....                    | 3 |
| Установка сертификата ключа подписи ..... | 3 |
| Установка корневого сертификата.....      | 8 |

## НЕОБХОДИМЫЕ КОМПОНЕНТЫ

Для корректной работы системы необходимо, чтобы на рабочей станции было установлено следующее программное обеспечение:

1. Лицензионная операционная система (с последними пакетами обновлений):
  - Windows Vista SP2 и выше;
  - Windows Server 2003 и выше;
  - Windows Server 2008 и выше;
  - Windows 7;
  - Windows 8;
  - Windows 8.1;
  - Windows Server 2012 и выше;
  - Windows 10.
2. .NET Framework 3.5 Service Pack 1.
3. Интернет браузер Internet Explorer 9.0 и выше.
4. СКЗИ КриптоПро CSP версии 3.6 и выше.
5. Компонент СФЕРА.
6. Драйвер для защищенного носителя ЭП (если таковой используется).

Также необходимо наличие USB-порта и доступа в Интернет.

Компоненты 1-3 должны быть установлены на компьютер самостоятельно; в настоящем руководстве рассматривается только установка компонентов 4-6 и настройка компонента 3.

Все необходимые для установки дистрибутивы можно скачать по указанным в инструкции ссылкам либо с [сайта](#) в разделе «Установка программного обеспечения и настройка сервиса».

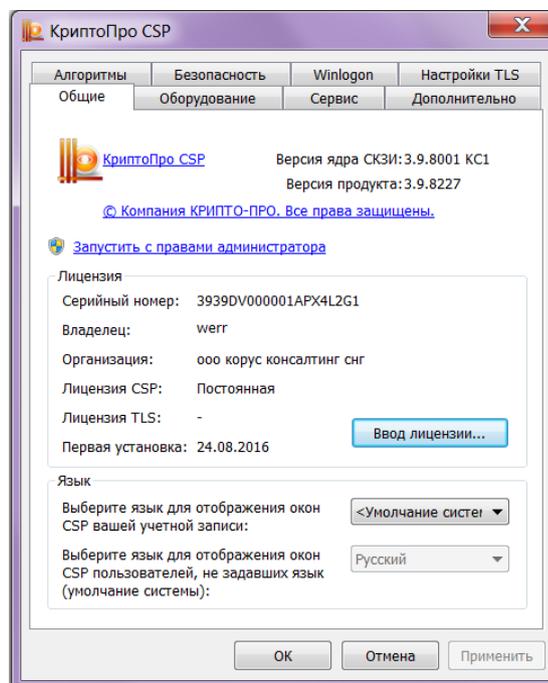
# ПОРЯДОК УСТАНОВКИ

## УСТАНОВКА СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

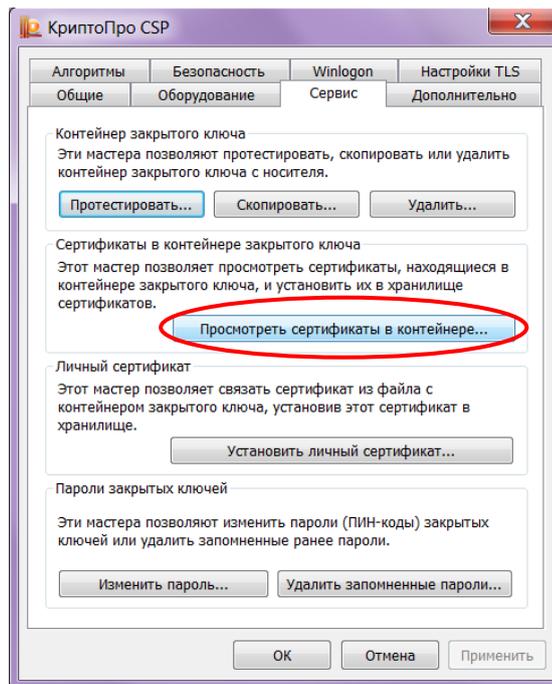
**Внимание!** Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель в USB-порт компьютера.

Если у вас имеется несколько сертификатов ключей подписи, указанные действия необходимо произвести для каждого сертификата.

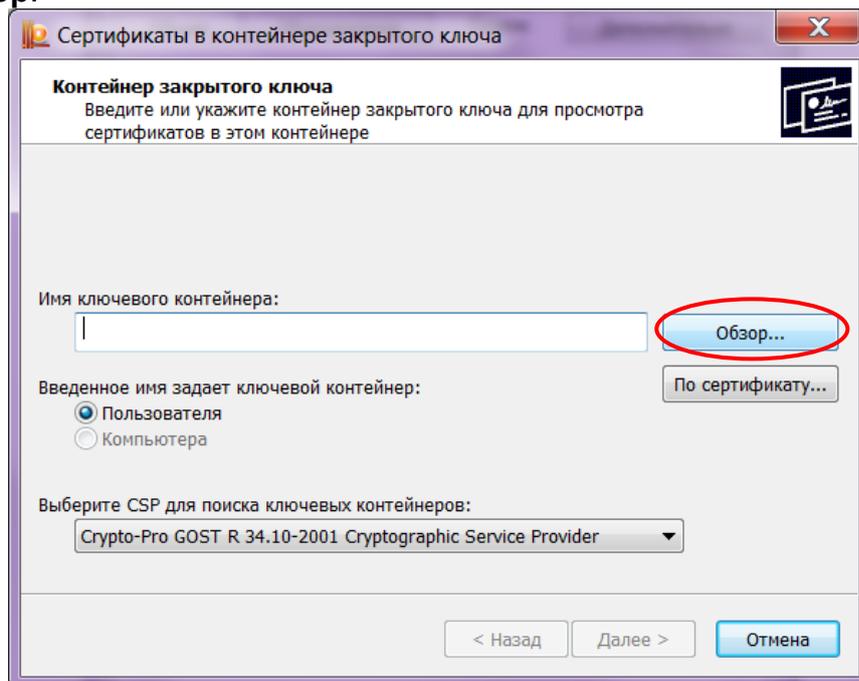
1. Запустите **КриптоПро CSP** (Пуск -> Панель Управления -> КриптоПро CSP).



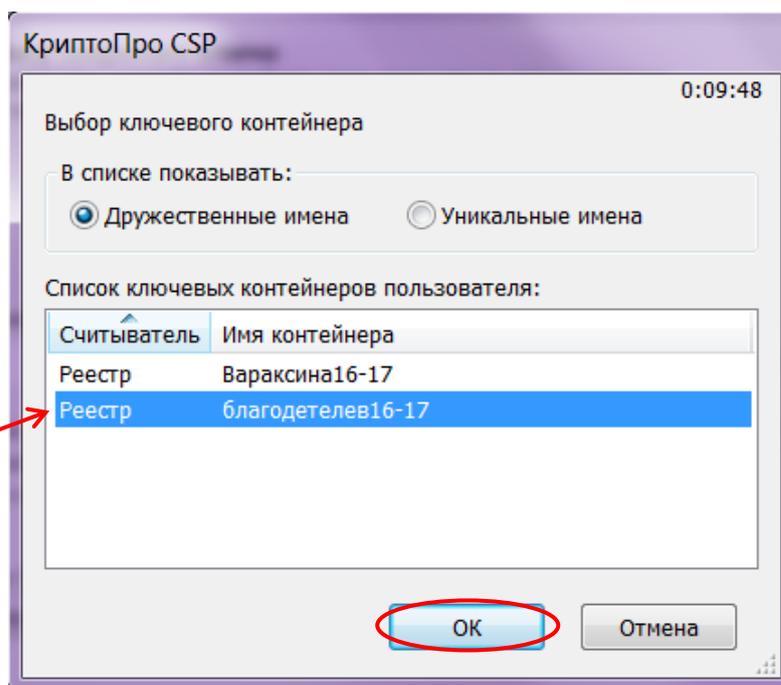
2. Выберите вкладку «Сервис» и нажмите кнопку **Просмотреть файлы в контейнере**.



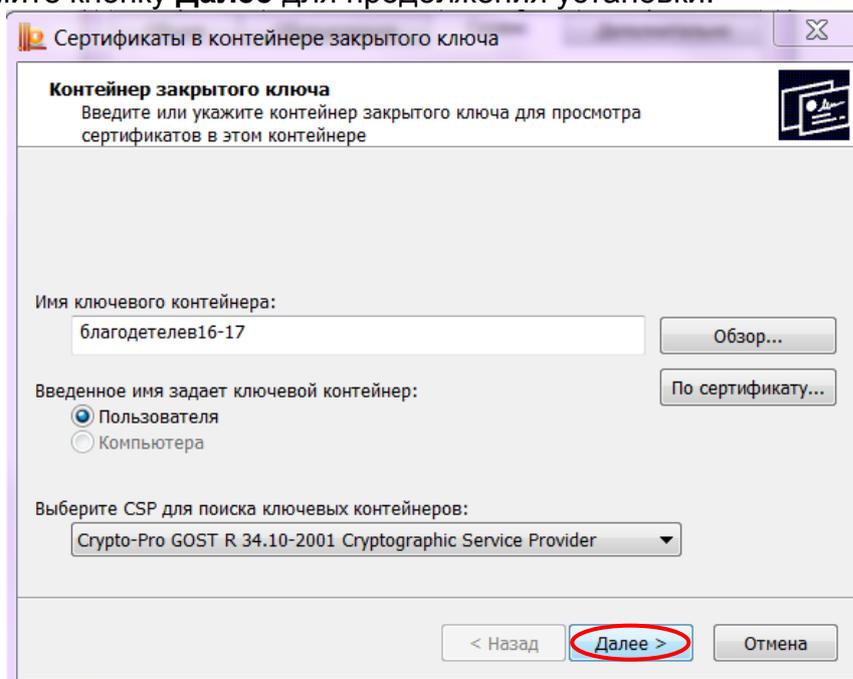
3. В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку **Обзор**.



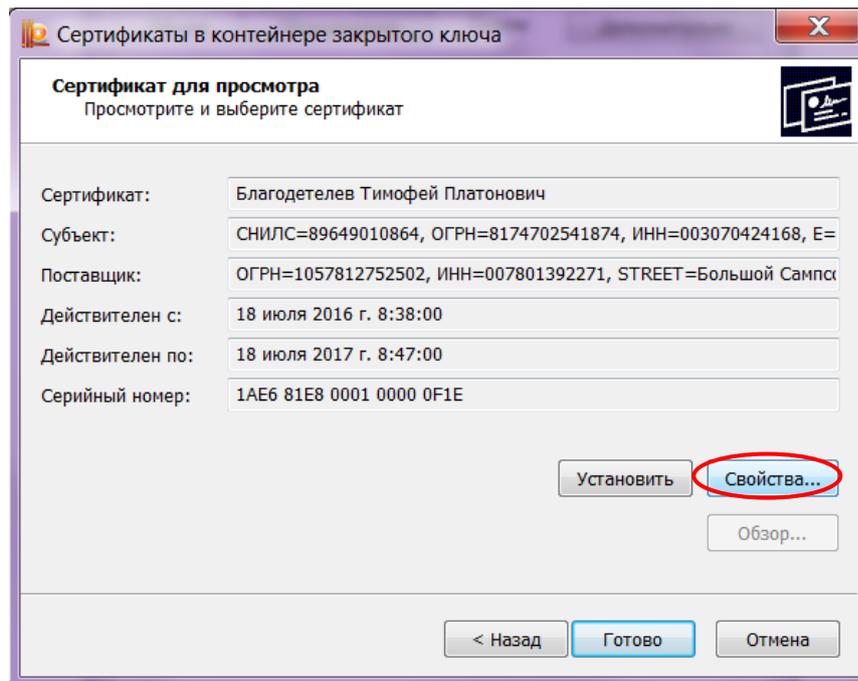
4. В списке ключевых носителей выберите нужный личный сертификат и нажмите кнопку **Ок**.



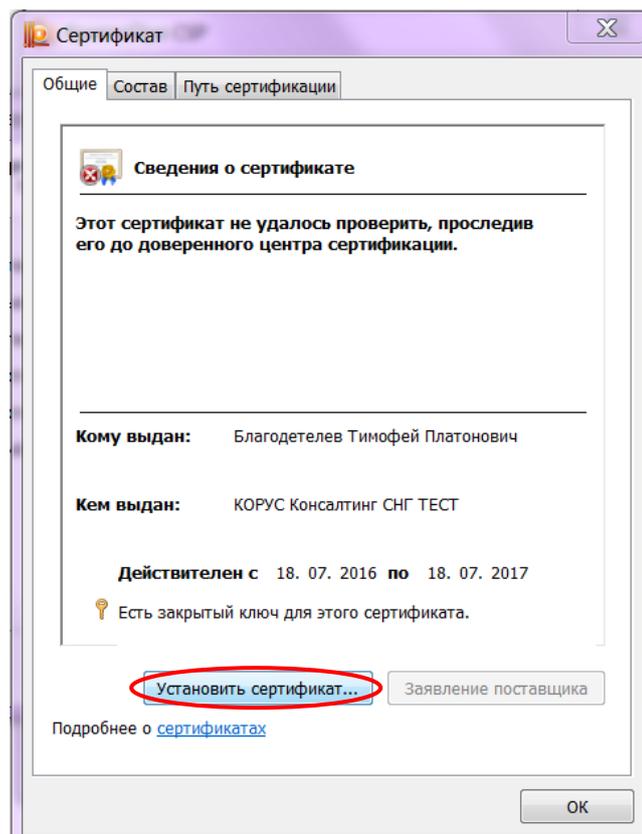
5. Нажмите кнопку **Далее** для продолжения установки.



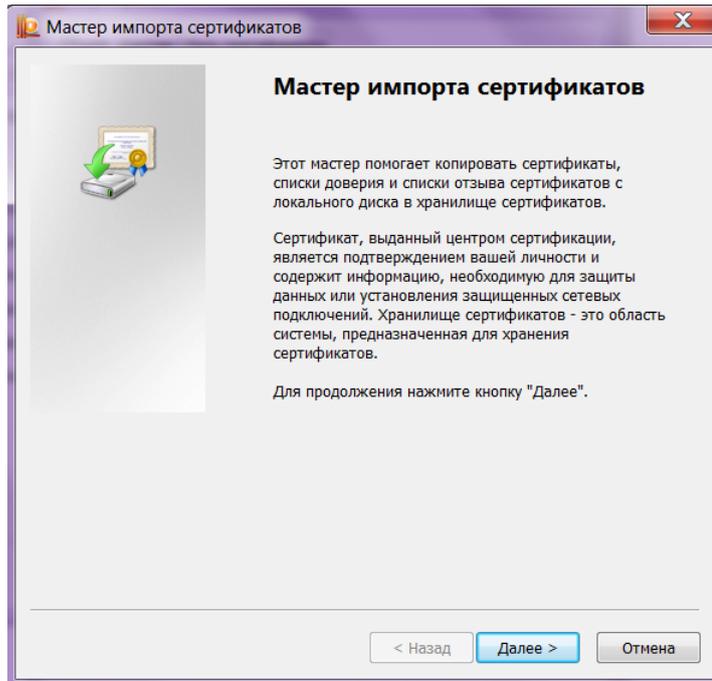
6. В окне информации о выбранном сертификате нажмите кнопку **Свойства**.



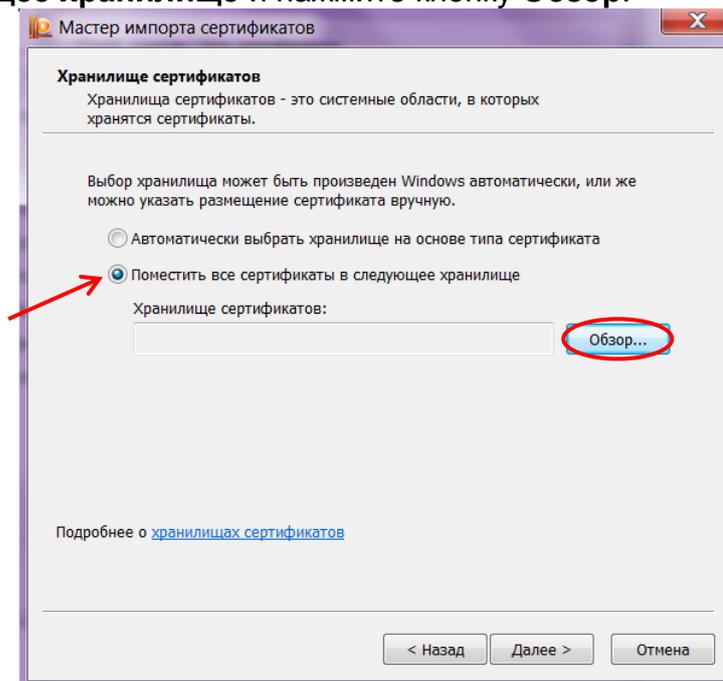
7. В открывшемся окне сертификата нажмите кнопку **Установить сертификат**.



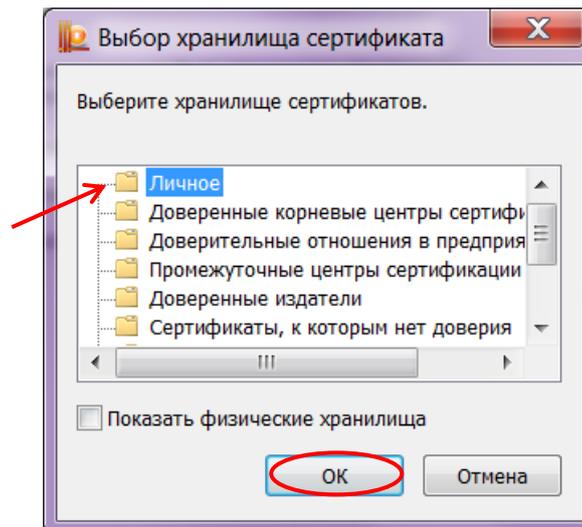
8. После этого будет запущен **Мастер импорта сертификатов**. Для продолжения установки нажмите кнопку **Далее**.



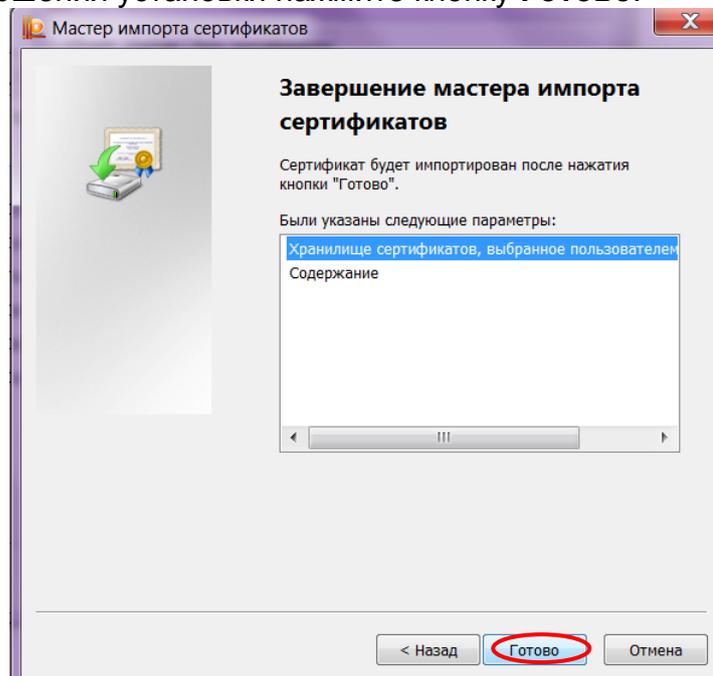
9. В появившемся окне поставьте отметку **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор**.



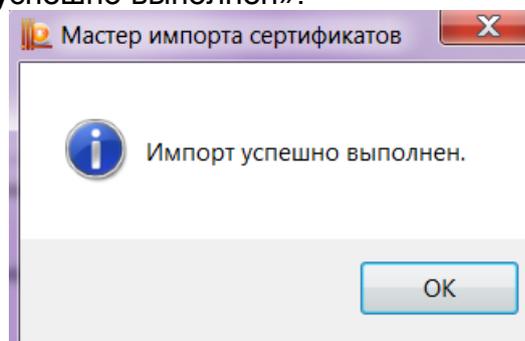
10. В списке хранилищ выберите хранилище «Личное», нажмите кнопку **Ок** и **Далее**.



11. Для завершения установки нажмите кнопку **Готово**.



В случае успешного импорта сертификата в хранилище будет выведено сообщение: «Импорт успешно выполнен».



## УСТАНОВКА КОРНЕВОГО СЕРТИФИКАТА

Для работы с электронной подписью необходимо установить корневой сертификат.

Для работы с электронной подписью, выданной Удостоверяющим центром ООО «КОРУС Консалтинг СНГ»:

- до 16.11.2016 - необходимо установить корневой сертификат Удостоверяющего центра ООО «КОРУС Консалтинг СНГ», который можно скачать в разделе «Корневой сертификат и реестр аннулированных сертификатов» на [сайте](#) или по ссылке:

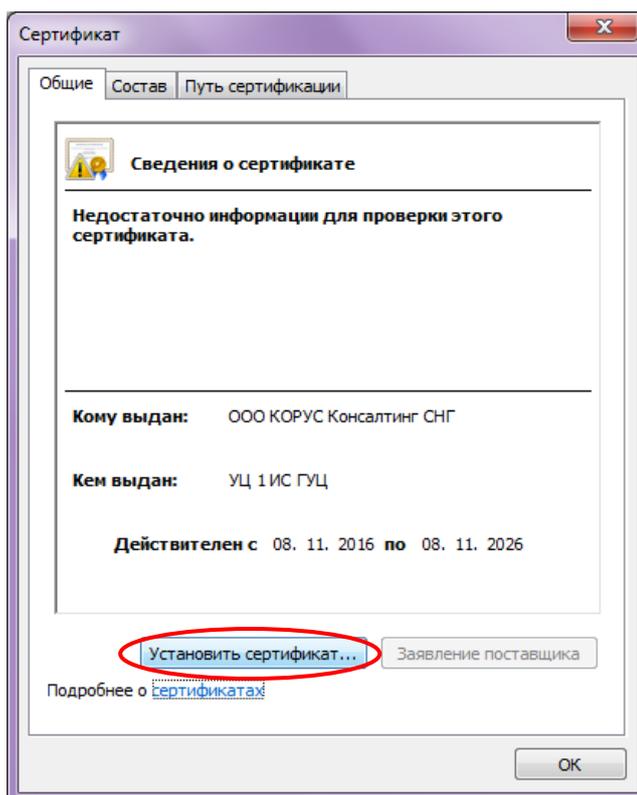
[Доверенный корневой сертификат Удостоверяющего центра ООО "КОРУС Консалтинг СНГ"](#);

- после 16.11.2016 - необходимо установить корневой сертификат Головного удостоверяющего центра Минкомсвязи, который можно скачать в разделе «Корневой сертификат и реестр аннулированных сертификатов» на [сайте](#) или по ссылке:

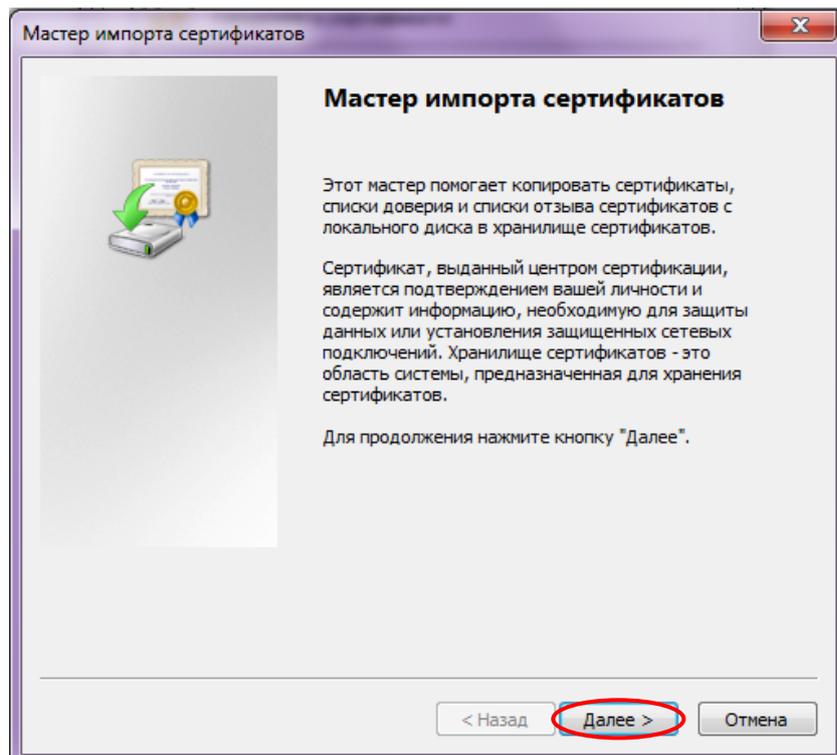
[Доверенный корневой сертификат Головного удостоверяющего центра Минкомсвязи.](#)

Для установки корневого сертификата выполните следующие шаги:

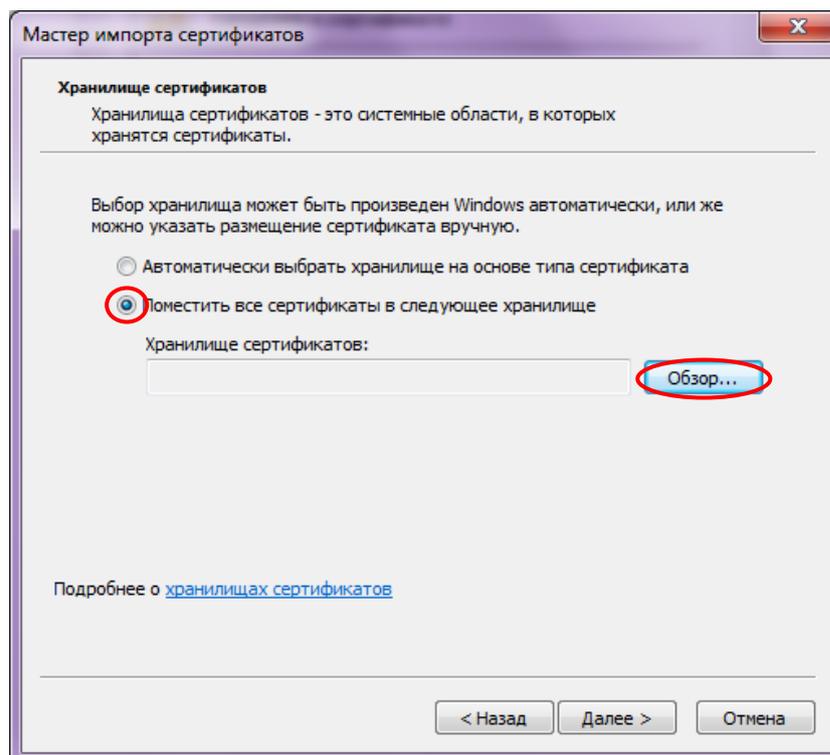
1. Откройте файл корневого сертификата.
2. Нажмите кнопку **Установить сертификат**.



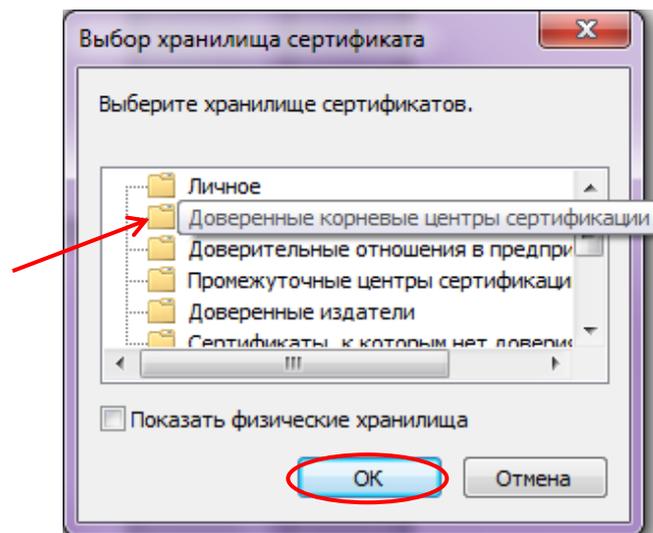
3. После этого запустится «Мастер импорта сертификатов». Для продолжения установки нажмите кнопку **Далее**.



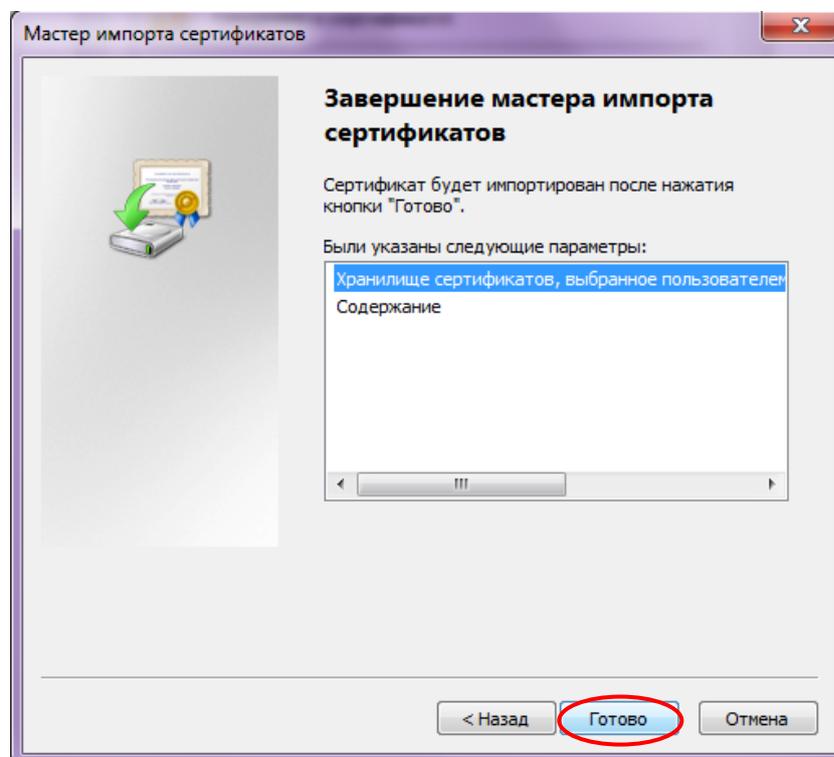
4. Установите отметку «Поместить все сертификаты в следующее хранилище» и нажмите кнопку **Обзор**.



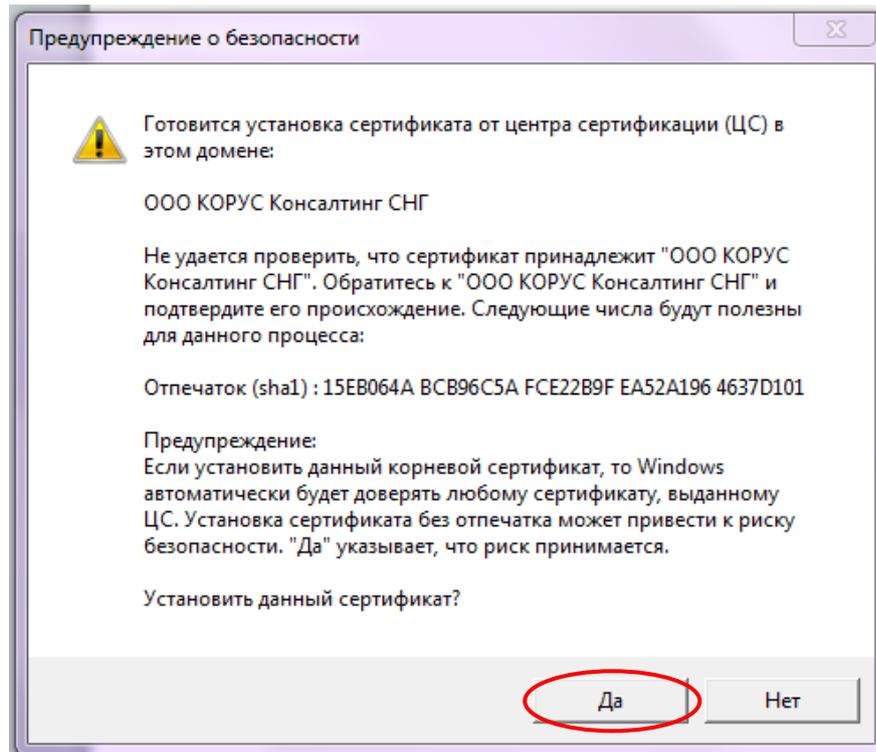
5. Выберите хранилище «Доверенные корневые центры сертификации», нажмите **ОК** и **Далее**.



6. Нажмите кнопку **Готово** для завершения установки сертификата.



7. При запросе системы нажмите кнопку **Да** для подтверждения доверия к данному издателю сертификата.



8. Нажмите кнопку **OK** в сообщении об успешном импорте сертификата в хранилище.

