Установка корневого сертификата удостоверяющего центра и неквалифицированного сертификата пользователя.

Установка корневого сертификата

1. Установка Корневого сертификата удостоверяющего центра ООО «КОРУС Консалтинг СНГ»

2. Скачайте и откройте файл, в появившемся окне сертификата нажмите кнопку **«Установить сертификат»**.

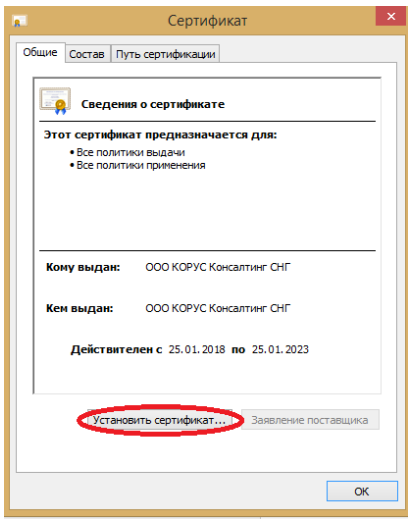

Рисунок 1. Установка корневого сертификата УЦ ООО «КОРУС Консалтинг СНГ»

3. После этого запустится **«Мастер импорта сертификатов»**. Для продолжения установки выберите расположение хранилища: **Локальный компьютер**. Нажать **«Далее»**.

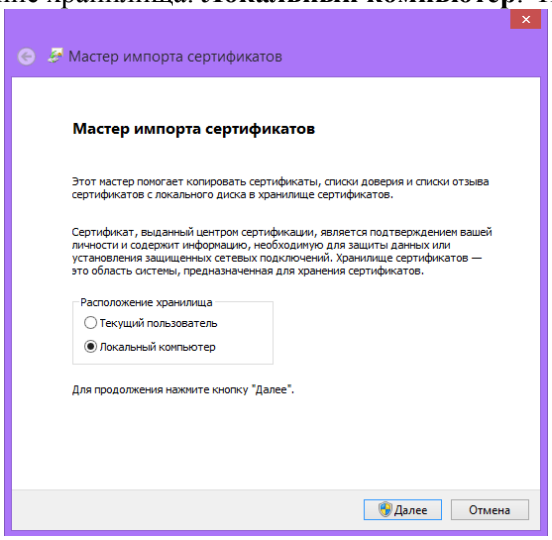

Рисунок 2. Мастер импорта сертификатов

4. В появившемся окне, поставьте галочку **«Поместить все сертификаты в следующее хранилище»** и нажмите кнопку **«Обзор»**.

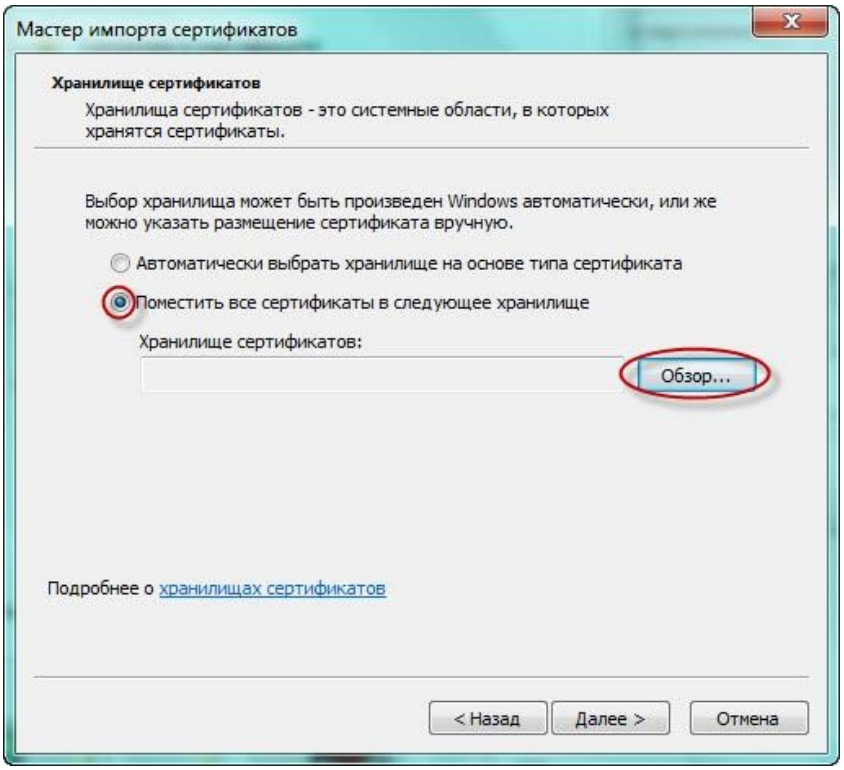

Рисунок 3. Установка корневого сертификата УЦ ООО «КОРУС Консалтинг СНГ»

5. В списке хранилищ выберите хранилище **«Доверенные корневые центры сертификации»**, нажмите **«ОК»** и **«Далее»**.

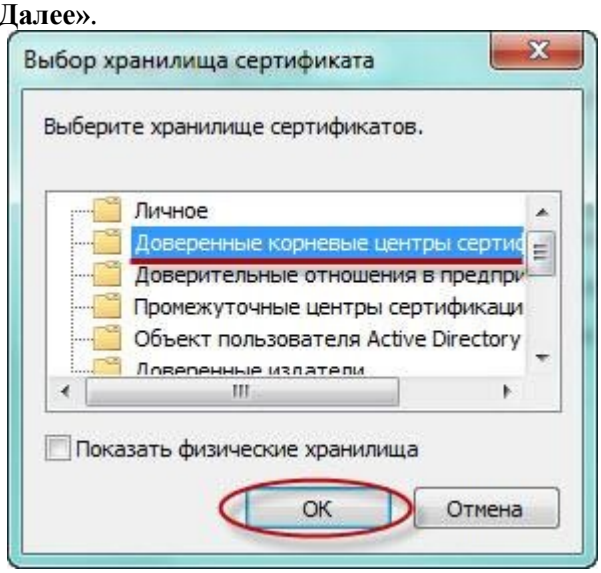

Рисунок 4. Выбор хранилища сертификата

6. Для завершения установки сертификата нажмите кнопку **«Готово»**.

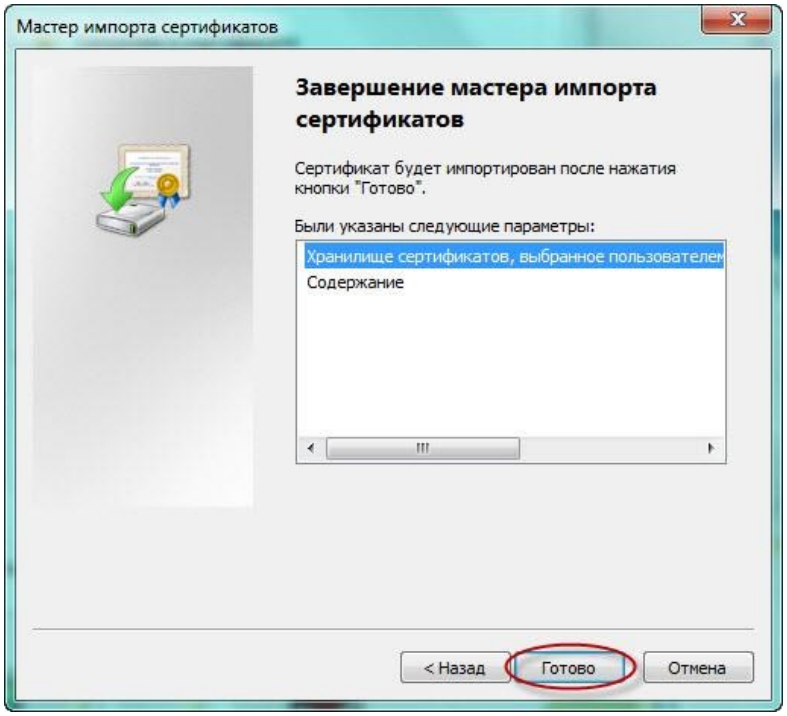

Рисунок 5. Завершение мастера импорта сертификатов

7. При запросе системы подтвердить доверие данному издателю сертификата, необходимо нажать «Да».

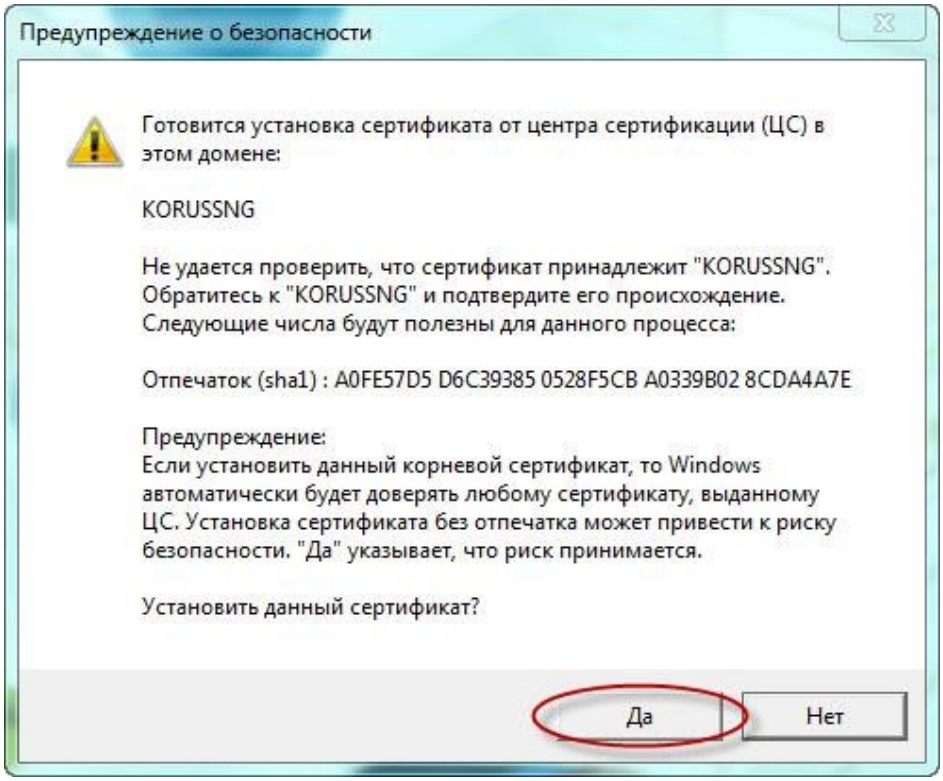

Рисунок 6. Предупреждение о безопасности

8. Об успешном импорте сертификата в хранилище будет выдано сообщение «Импорт успешно выполнен».

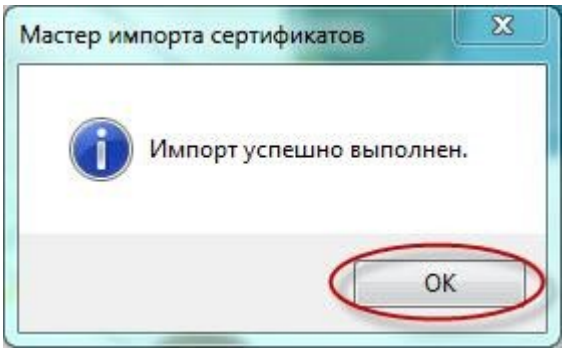

Рисунок 7. Успешное завершение импорта

Установка личного сертификата пользователя

Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель Рутокен/ESMART в USB-порт компьютера (предварительно произведя установку необходимых драйверов и ПО).

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

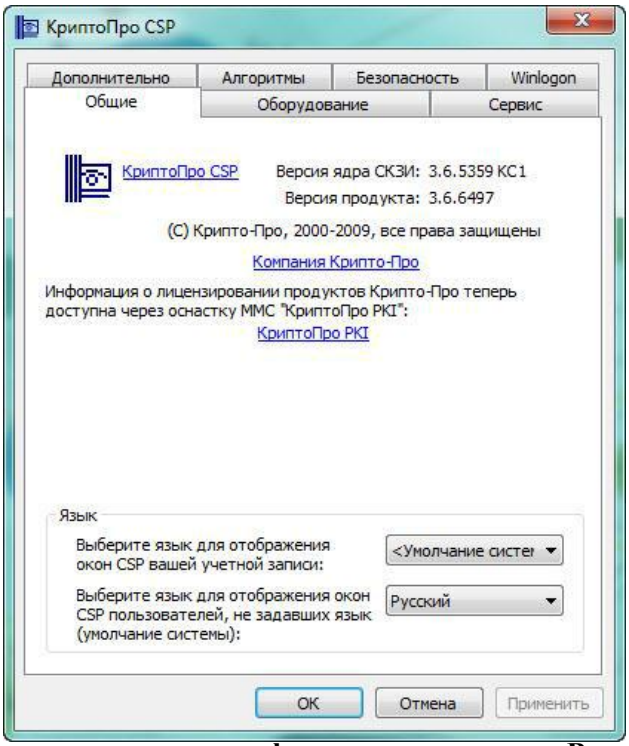

Рисунок 8. Установка открытого ключа сертификата пользователя. Вкладка «Общие»

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

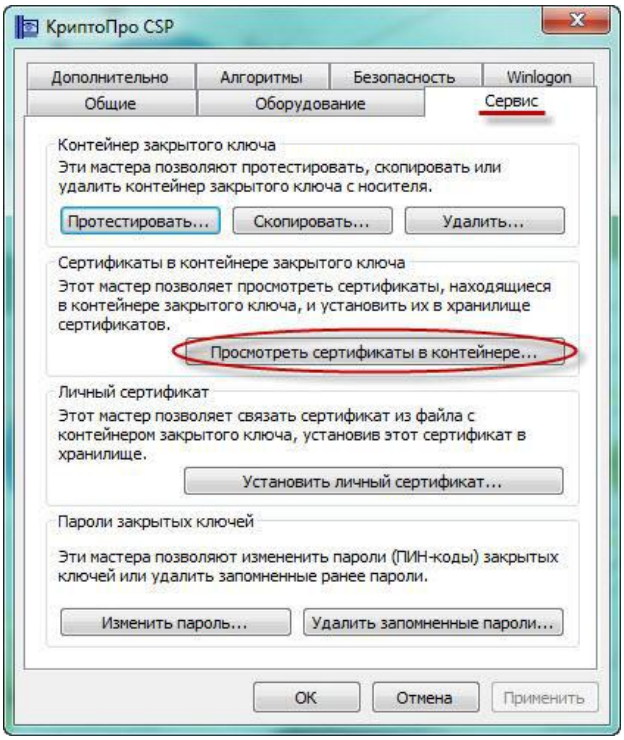

Рисунок 9. Установка ключа сертификата пользователя. Вкладка «Сервис»

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

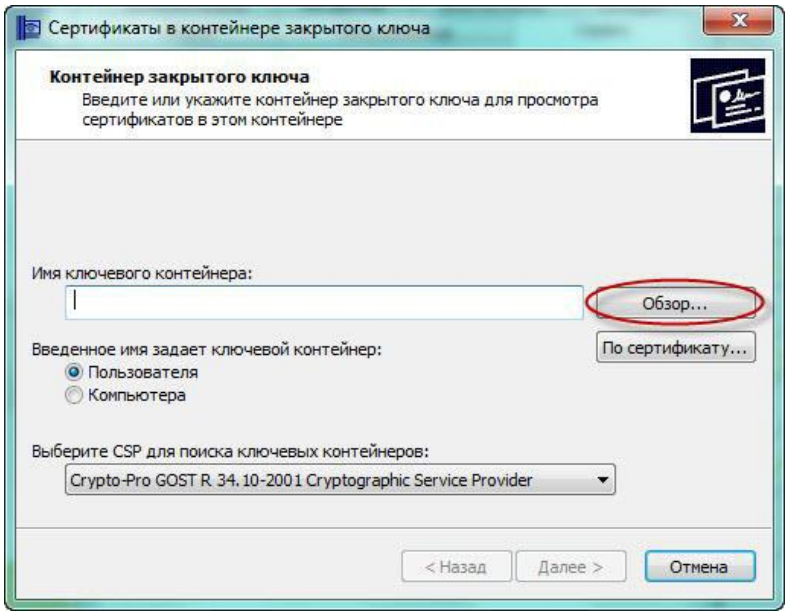

Рисунок 10. Установка открытого ключа сертификата пользователя. Сертификаты в контейнере закрытого ключа

4. В списке ключевых носителей выберите нужный личный сертификат и нажмите **«ОК»**;

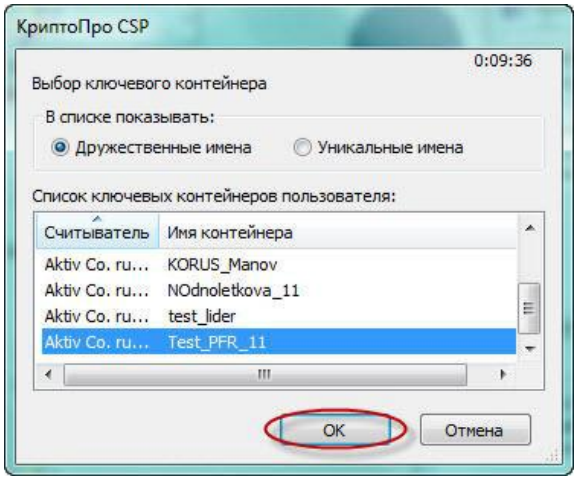

Рисунок 11. Установка открытого ключа сертификата пользователя. Список ключевых контейнеров пользователя

4. Нажмите кнопку **«Далее»** для продолжения установки;

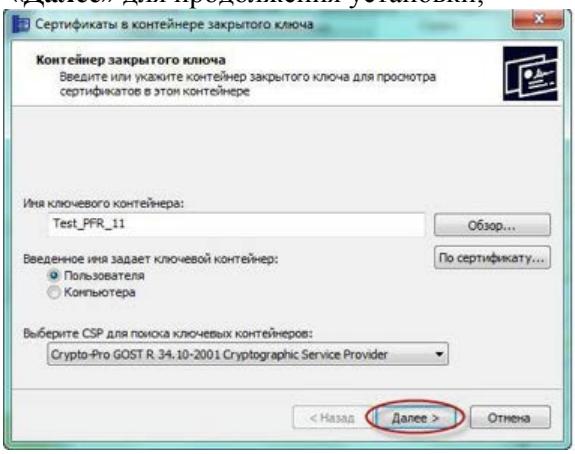

Рисунок 12. Установка открытого ключа сертификата пользователя. Имя ключевого контейнера

6. В информации о выбранном сертификате нажмите кнопку **«Свойства»**;

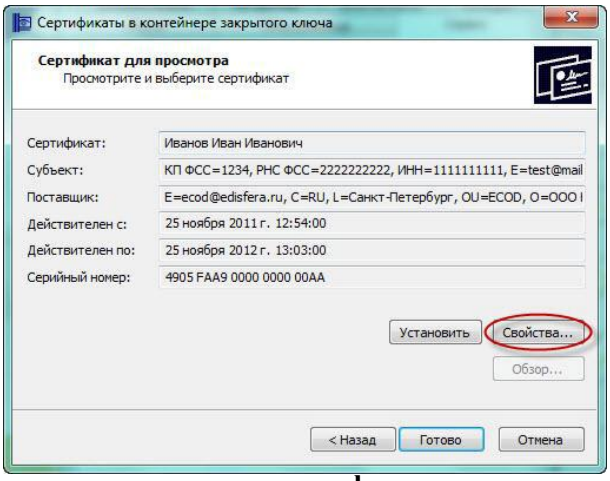

Рисунок 13. Установка открытого ключа сертификата пользователя. Сертификат для просмотра

7. Далее в появившемся окне сертификата нажмите кнопку **«Установить сертификат»**;

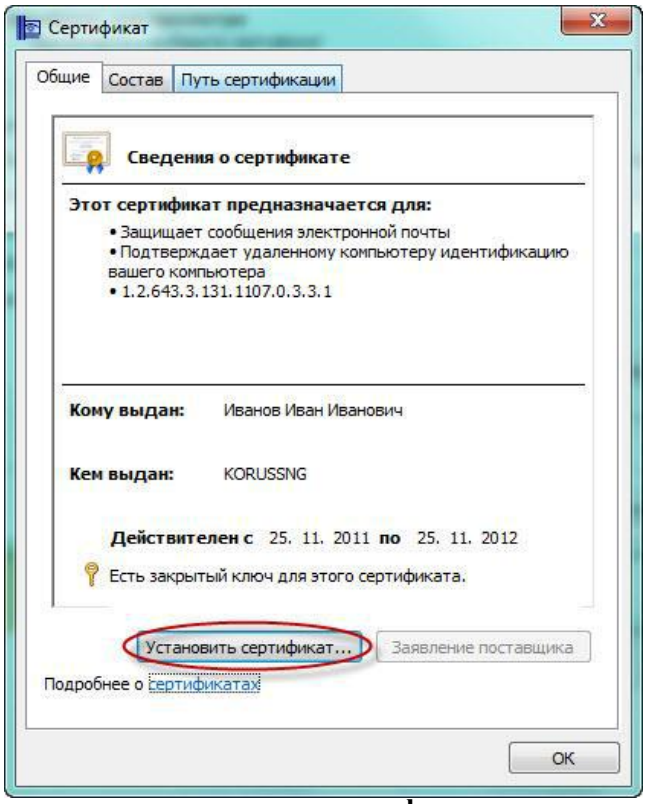

Рисунок 14. Установка открытого ключа сертификата пользователя. Сведения о сертификате

8. После этого запустится **«Мастер импорта сертификатов»**. Для продолжения установки нажмите **«Далее»**;

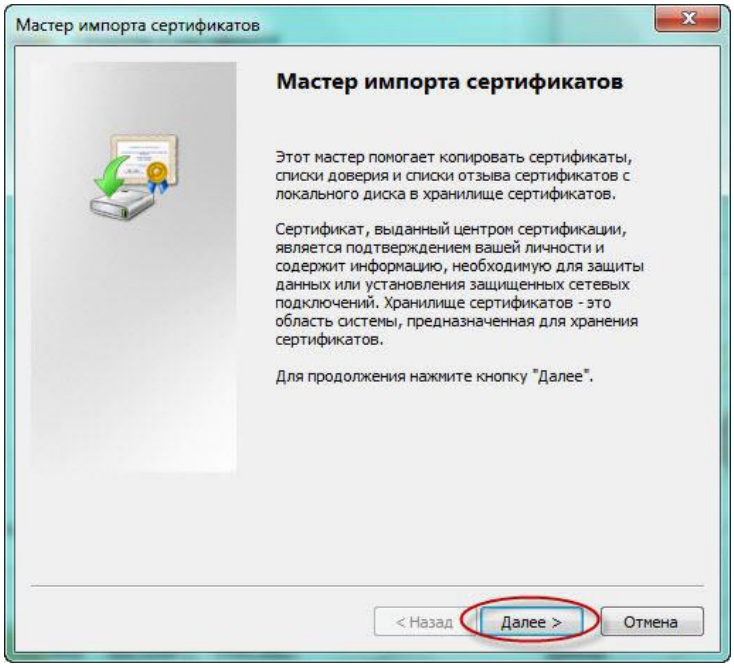

Рисунок 15. Установка открытого ключа сертификата пользователя. Мастер импорта сертификатов

9. В появившемся окне, поставьте галочку **«Поместить все сертификаты в следующее хранилище»** и нажмите кнопку **«Обзор»**;

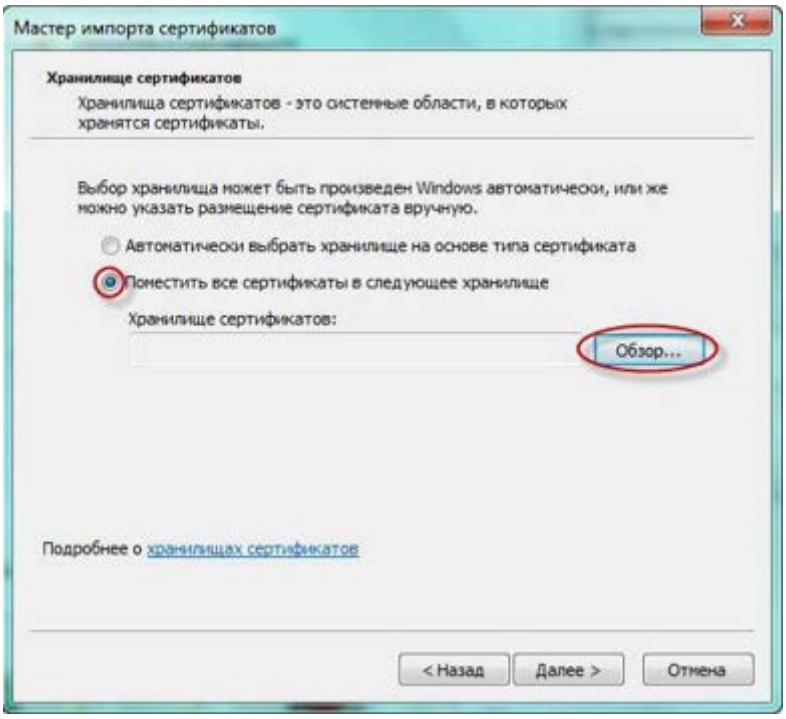

Рисунок 16. Установка открытого ключа сертификата пользователя. Выбор хранилища сертификатов

10. В списке хранилищ выберите хранилище **«Личное»**, нажмите **«ОК»** и **«Далее»**;

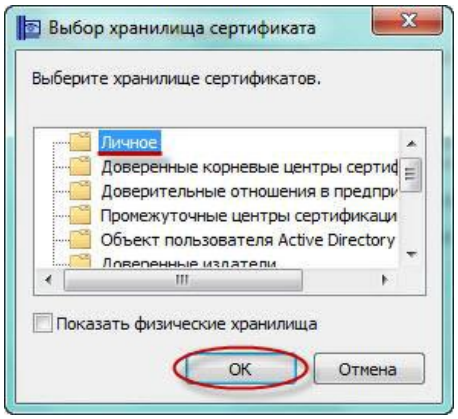

Рисунок 17. Установка открытого ключа сертификата пользователя. Хранилища сертификатов

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

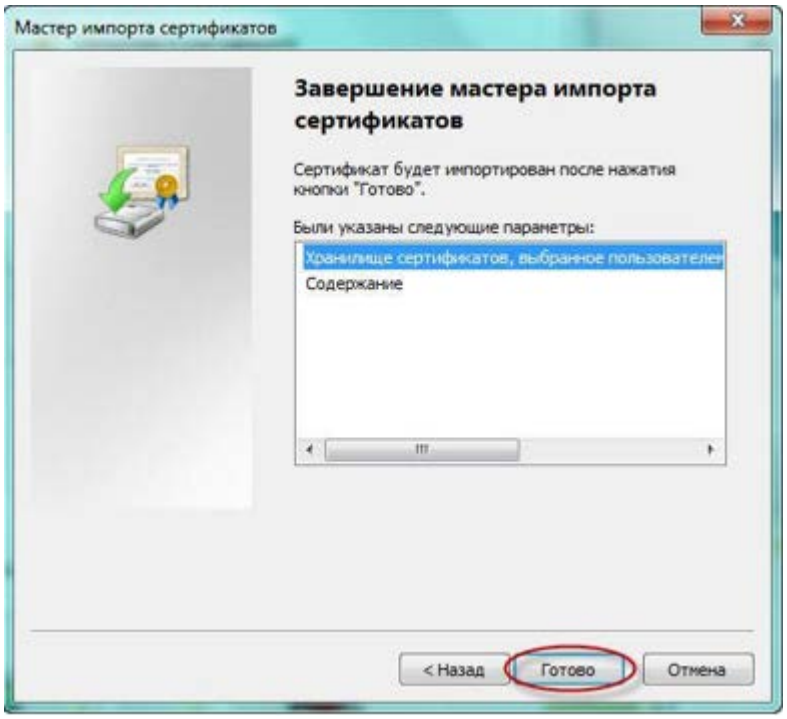

Рисунок 18. Установка открытого ключа сертификата пользователя. Завершение установки сертификата

12. Об успешном импорте сертификата в хранилище будет выдано сообщение **«Импорт успешно выполнен»**:

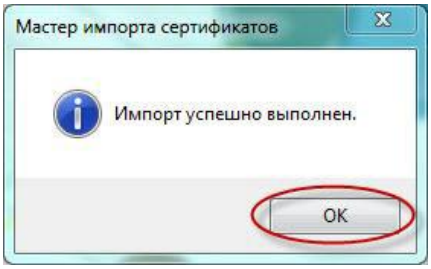

Рисунок 19. Установка открытого ключа сертификата пользователя. Подтверждение успешной установки