Установка компонентов, необходимых для работы с сертификатом электронной подписи ООО «КОРУС Консалтинг СНГ» записанным на Единую карту петербуржца (ЕКП)

Оглавление

Все программы и компоненты можно скачать по ссылке:
http://www.esphere.ru/support/download/uc/

Установка карт-ридера Gemalto IDBridge CT30

Данный считыватель поддерживает стандарт CCID, его особенность состоит в том, что он не требует установки дополнительных драйверов.

1. Вставляете карт-ридер в usb-порт, без вставленной в него карты.
2. Начнётся автоматическая настройка карт-ридера (в зависимости от операционной системы процесс настройки отображается по-разному). В данный момент карт-ридер должен начать мигать зелёным цветом.
3. По итогу успешной установки в «Диспетчер устройств» (расположен в «Панель управления») должен отобразиться раздел «Устройства чтения смарт-карт», где будет отображаться устройство чтения смарт-карт. В случае положительного результата установки пройдите к разделу «Установка СКЗИ КриптоПро CSP».

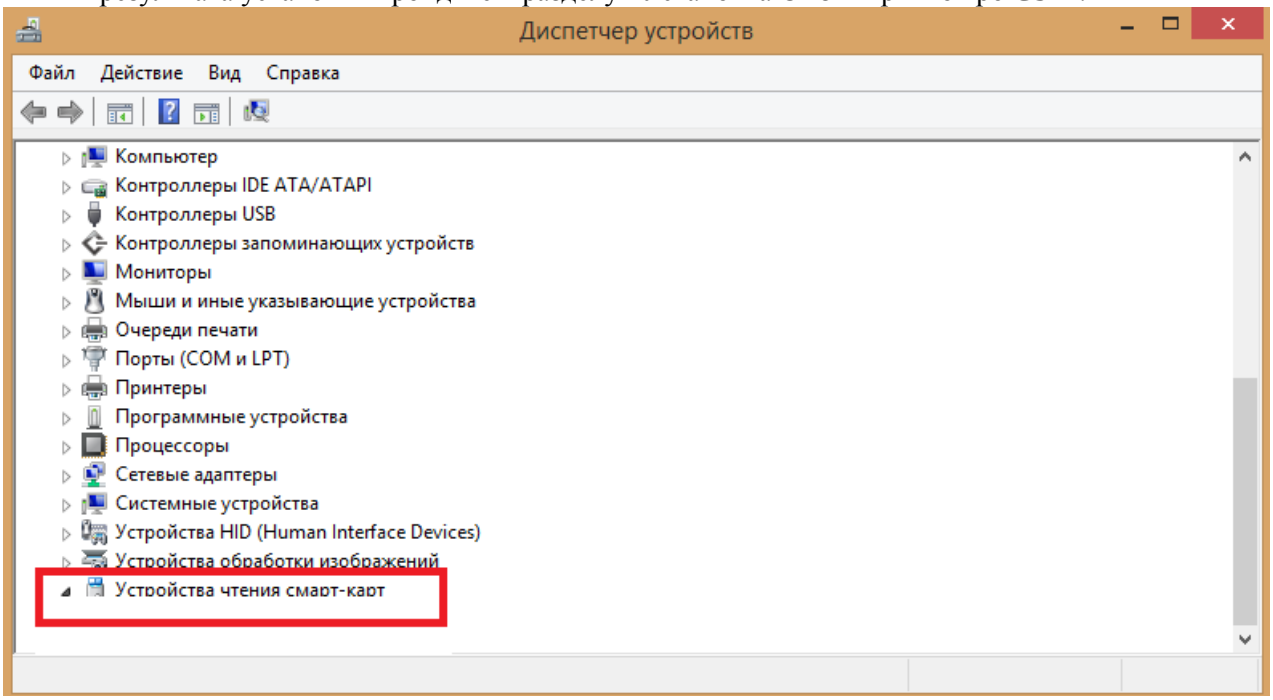

Рисунок 1. Диспетчер устройств. Проверка установки считывателя смарт-карт.

4. Если по п.3 отсутствует блок «Устройства чтения смарт-карт», вытащите карт-ридер и повторите п. 1-3.
5. Если п.4 не помог, необходимо установить драйвера для карт-ридера, скачать их можно на сайте производителя IDBridge CT30, компании Gemalto, где выбираете драйвер для скачивания, совместимый с Вашей операционной системой.

Установка СКЗИ КриптоПро CSP

Скачайте дистрибутив СКЗИ КриптоПро CSP 4.0 R4

1. Запустите установочный файл, который скачали;
2. В появившимся окне программы установки **«КриптоПРО CSP (в зависимости от версии окно выглядит по-разному)»** нажмите кнопку **«Далее»**;

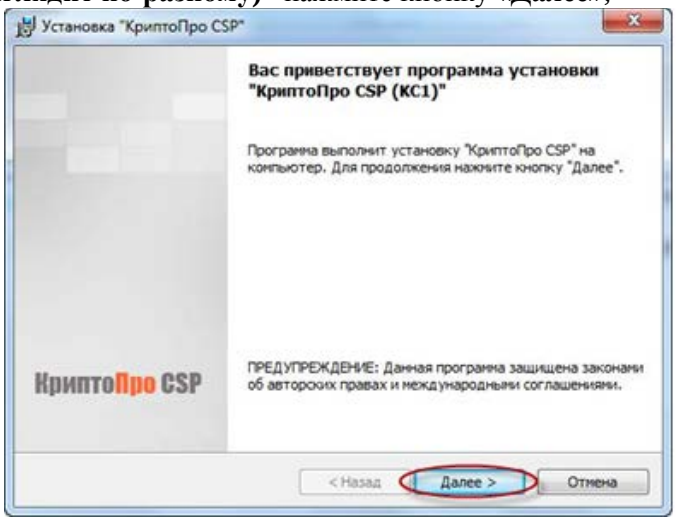

Рисунок 2. КриптоПро CSP. Приветствие

3. Ознакомьтесь с текстом лицензионного соглашения, поставьте галочку **«Я принимаю условия лицензионного соглашения»** и нажмите кнопку **«Далее»**;

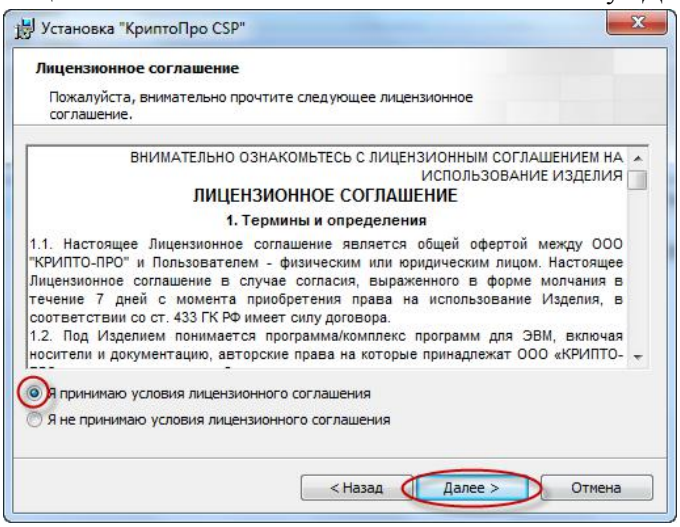

Рисунок 3. КриптоПро CSP. Лицензионное соглашение

4. В окне **«Сведения о пользователе»** введите Ваше ФИО, **и** нажмите кнопку **«Далее» (Ваш сертификат содержит встроенную лицензию, вводить номер не нужно)**;

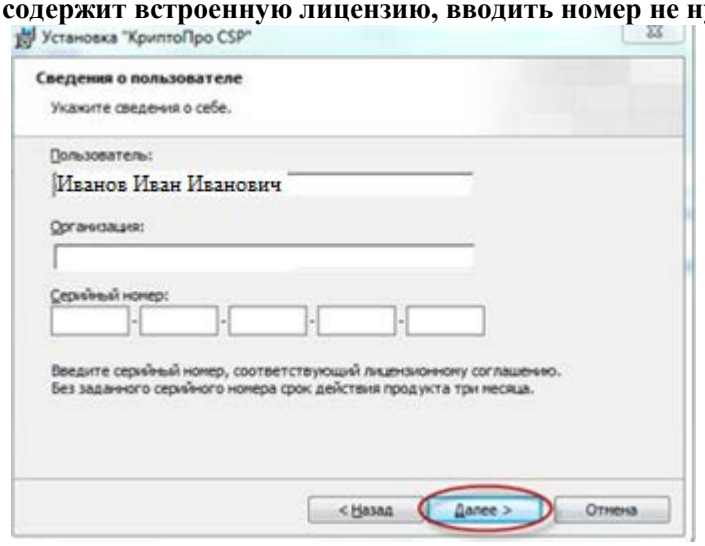

Рисунок 4. КриптоПро CSP. Сведения о пользователе

5. В следующем окне выберите обычный вид установки и нажмите кнопку **«Далее»**.

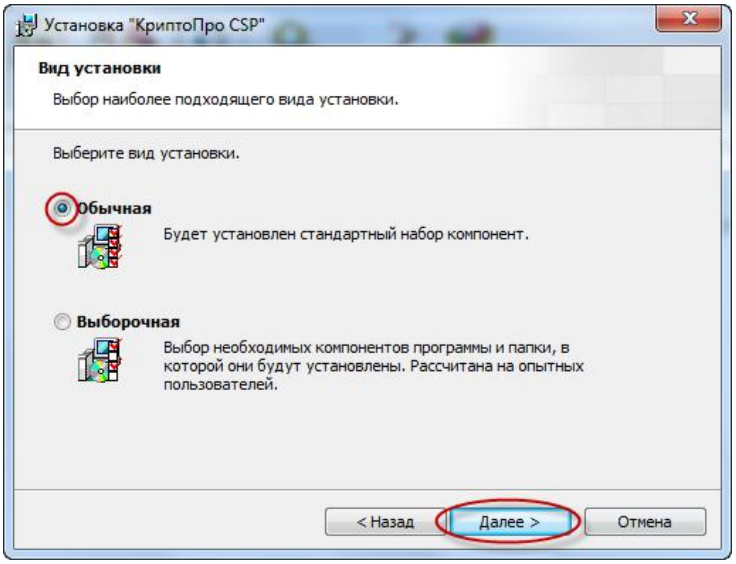

Рисунок 5. КриптоПро CSP. Вид установки

6. Укажите виды считывателей, которые необходимо зарегистрировать в **«КриптоПро CSP»**. По умолчанию **«Зарегистрировать считыватель смарт-карт»** и **«Зарегистрировать считыватель съемных носителей»**. Нажмите кнопку **«Установить»**;

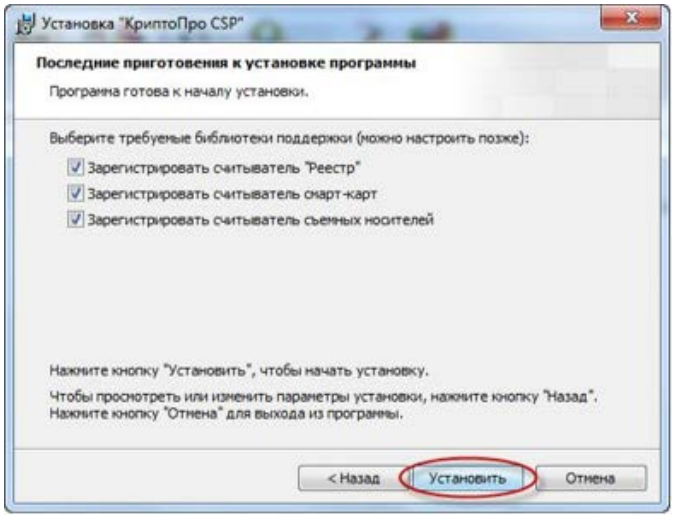

Рисунок 6. КриптоПро CSP. Последние приготовления к установке программы

7. По окончании установки нажмите кнопку **«Готово»**.

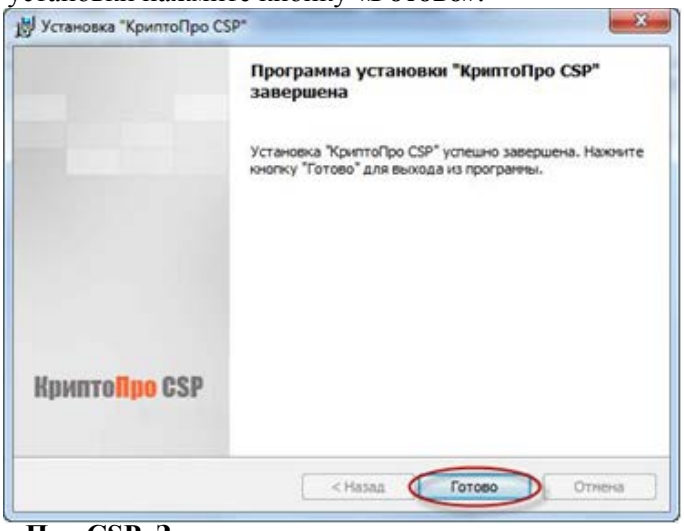

Рисунок 7. КриптоПро CSP. Завершение установки

8. Для завершения процесса установки программы необходимо перезагрузить компьютер. При появлении окна **«Сведения о программе установки КриптоПро CSP»** с предложением перезагрузки, следует нажать кнопку **«Да»**:

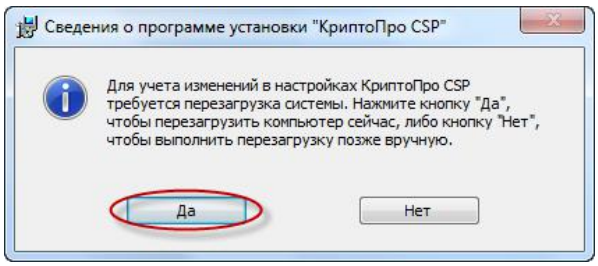

Рисунок 8. КриптоПро CSP. Перезагрузка системы

Установка личного сертификата ключа подписи

Перед установкой сертификата ключа подписи необходимо вставить ключевой носитель – ЕКП в устройство чтения смарт-карт.

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

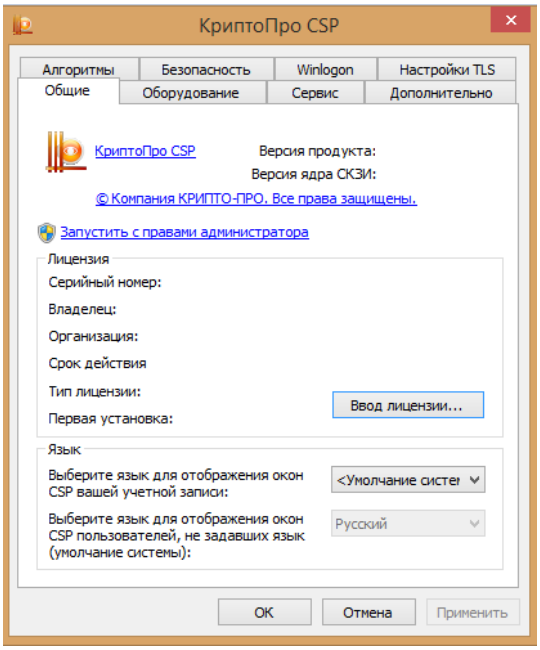

Рисунок 9. Установка открытого ключа сертификата пользователя. Вкладка «Общие»

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

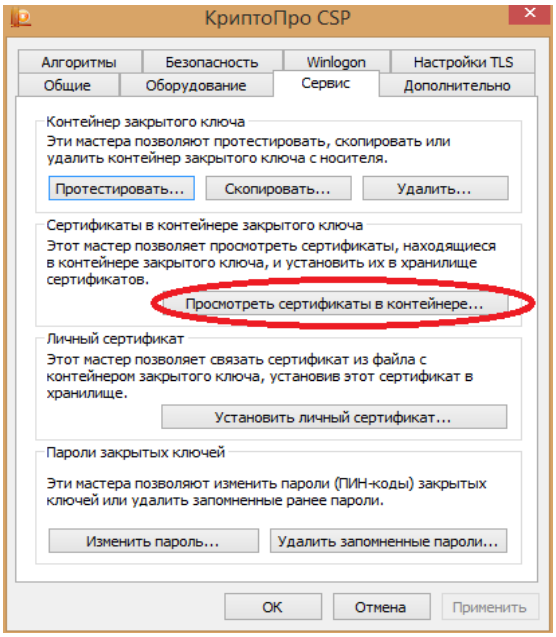

Рисунок 10. Установка ключа сертификата пользователя. Вкладка «Сервис»

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

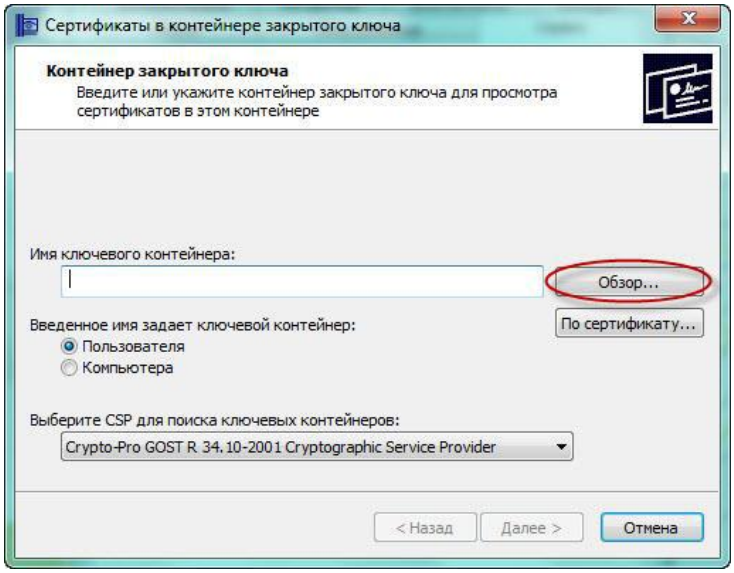

Рисунок 11. Установка открытого ключа сертификата пользователя. Сертификаты в контейнере закрытого ключа

4. В списке ключевых носителей выберите нужный личный сертификат (наименование считывателя и имя контейнера у Вас будут отличаться от приведенного на рисунке 13) и нажмите **«ОК»**;

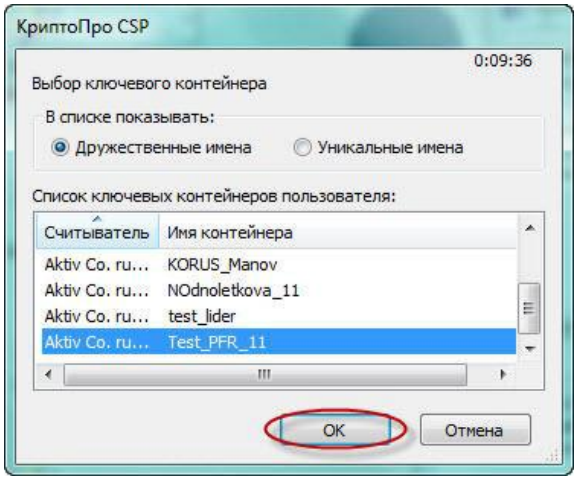

Рисунок 12. Установка открытого ключа сертификата пользователя. Список ключевых контейнеров пользователя

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

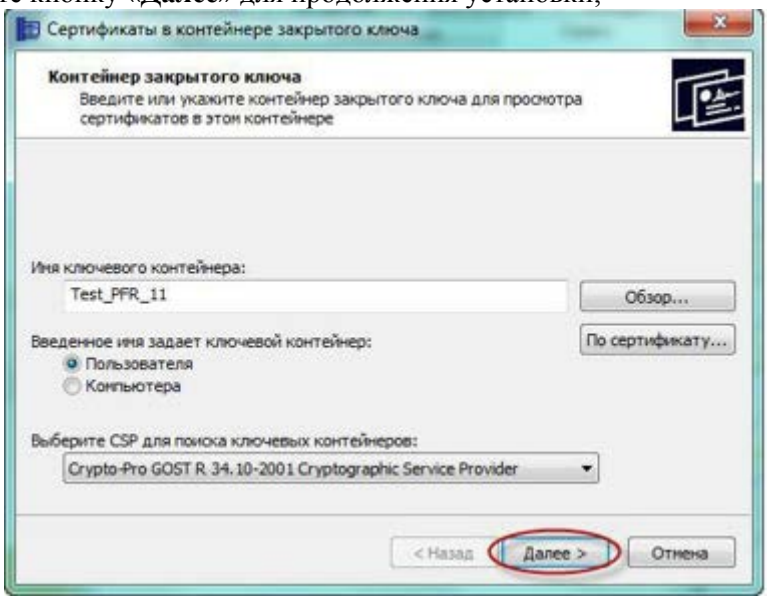

Рисунок 13. Установка открытого ключа сертификата пользователя. Имя ключевого контейнера

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

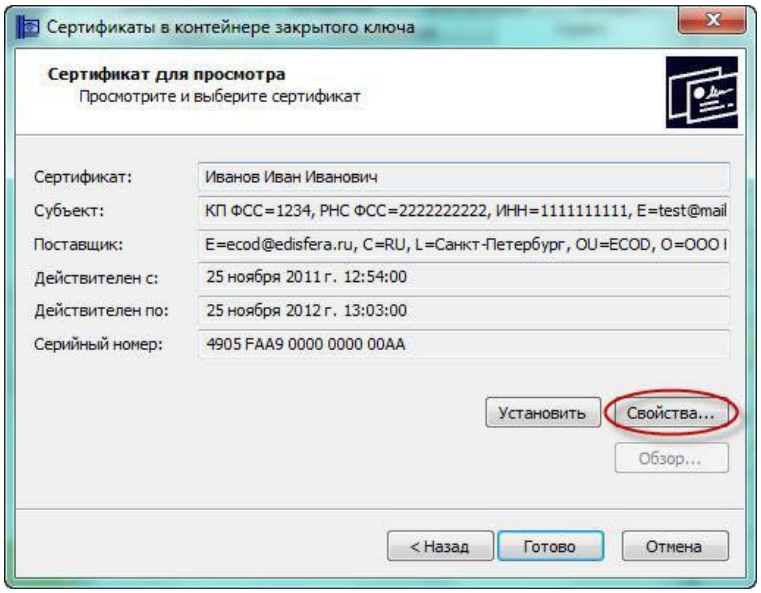

Рисунок 14. Установка открытого ключа сертификата пользователя. Сертификат для просмотра

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

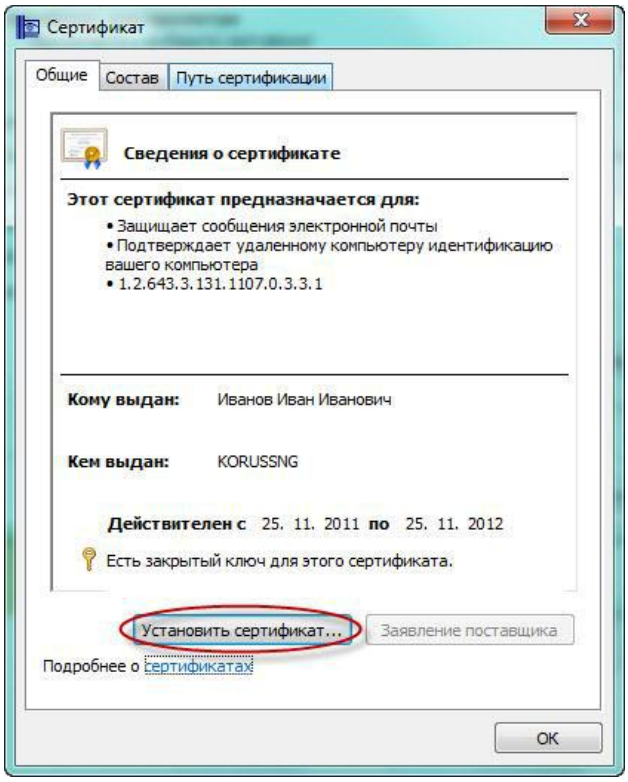

Рисунок 15. Установка открытого ключа сертификата пользователя. Сведения о сертификате

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

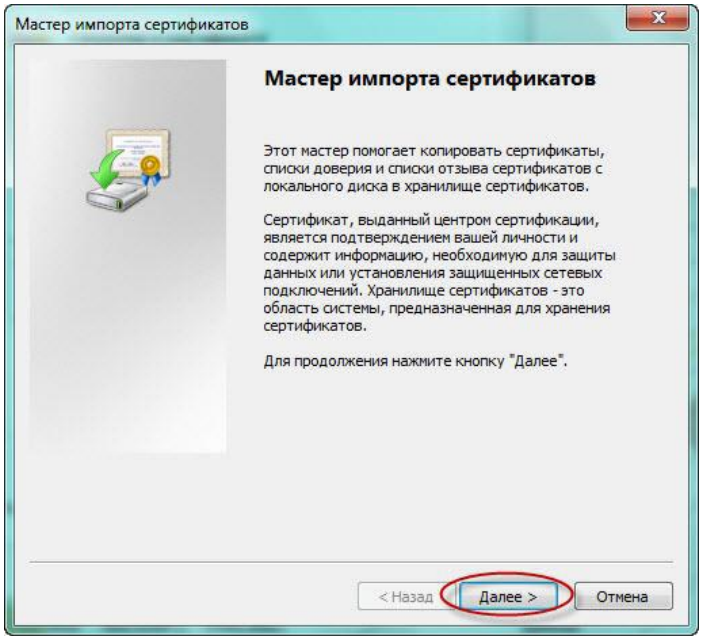

Рисунок 16. Установка открытого ключа сертификата пользователя. Мастер импорта сертификатов

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

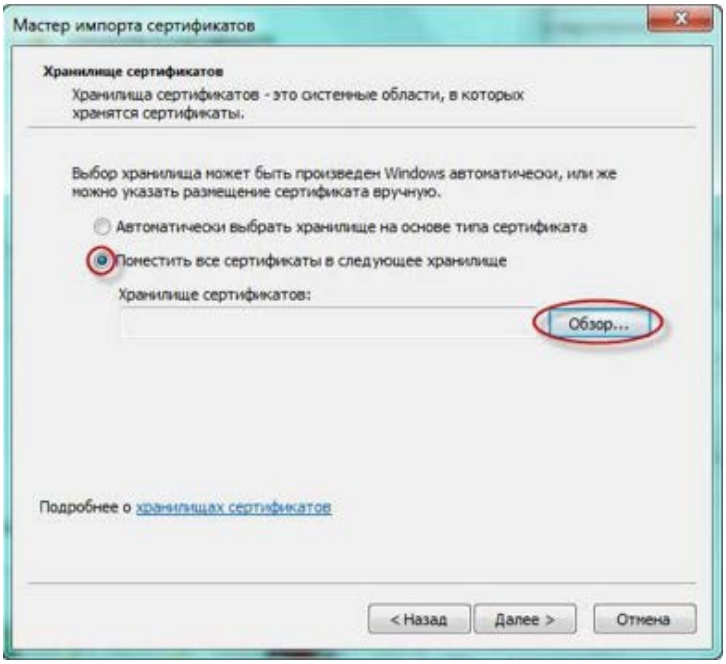

Рисунок 17. Установка открытого ключа сертификата пользователя. Выбор хранилища сертификатов

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

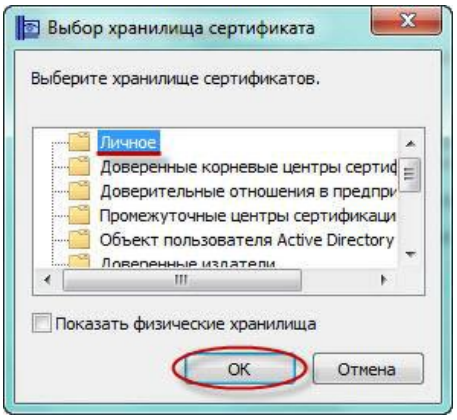

Рисунок 18. Установка открытого ключа сертификата пользователя. Хранилища сертификатов

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

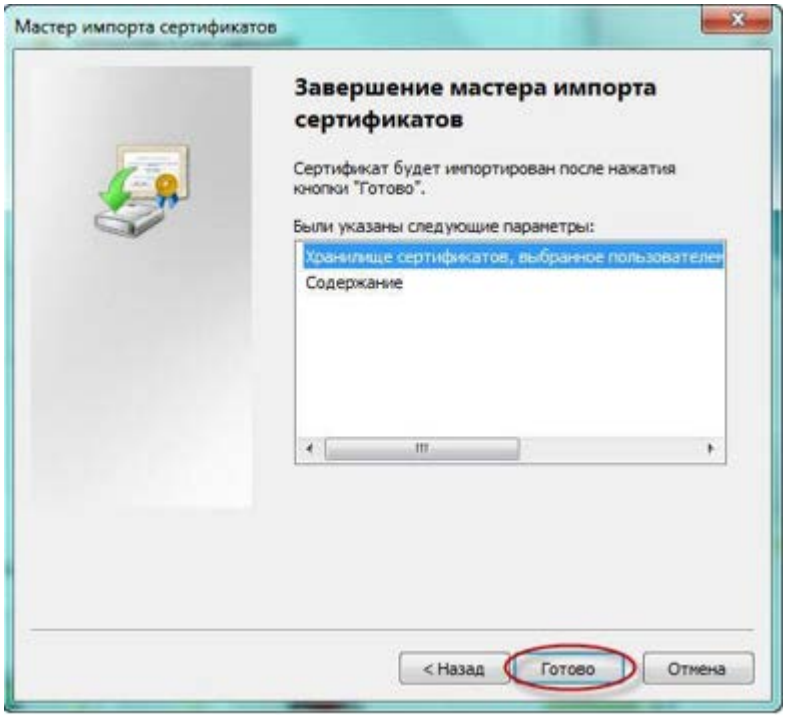

Рисунок 19. Установка открытого ключа сертификата пользователя. Завершение установки сертификата

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

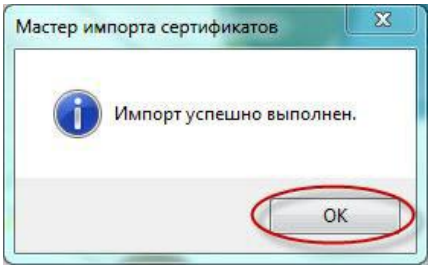

Рисунок 20. Установка открытого ключа сертификата пользователя. Подтверждение успешной установки

Установка корневого сертификата

1. Установка Корневого сертификата Головного удостоверяющего центра
2. Скачайте и откройте файл **Головной удостоверяющий центр**, в появившемся окне сертификата нажмите кнопку **«Установить сертификат»**.

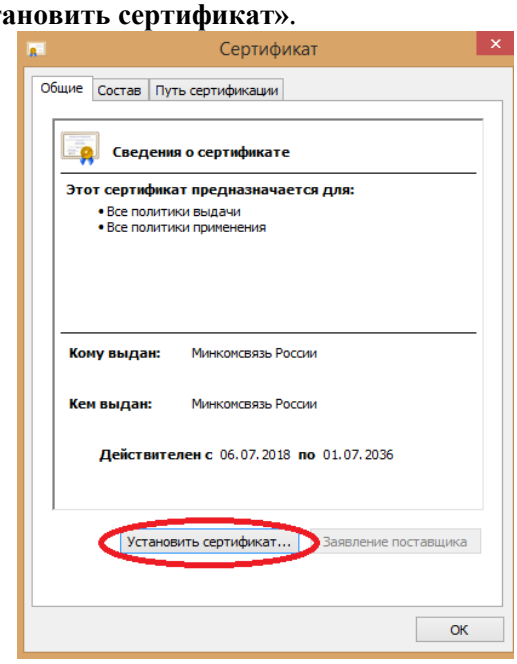

Рисунок 21. Установка корневого сертификата Головного удостоверяющего центра

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

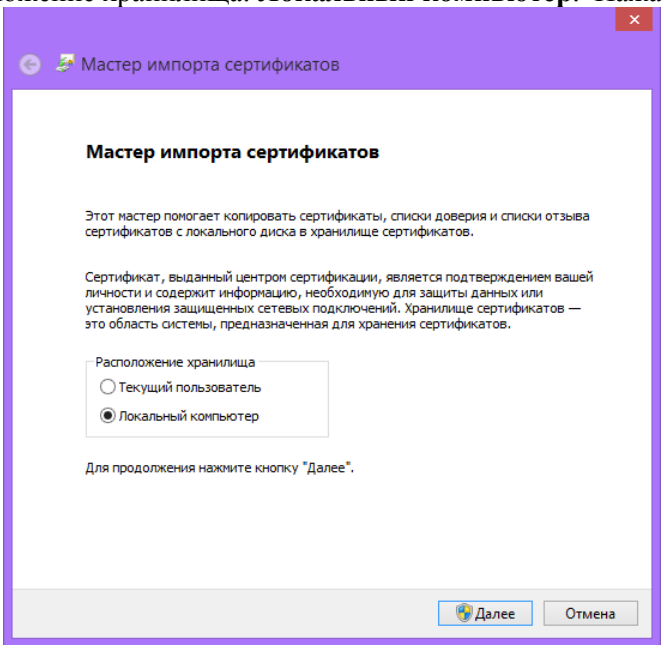

Рисунок 22. Мастер импорта сертификатов

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

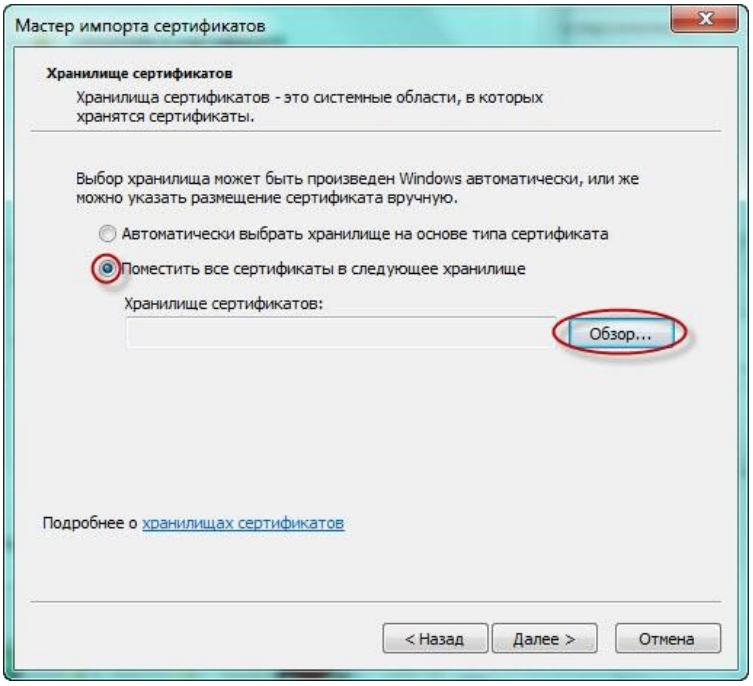

Рисунок 23. Установка корневого сертификата Головного удостоверяющего центра

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

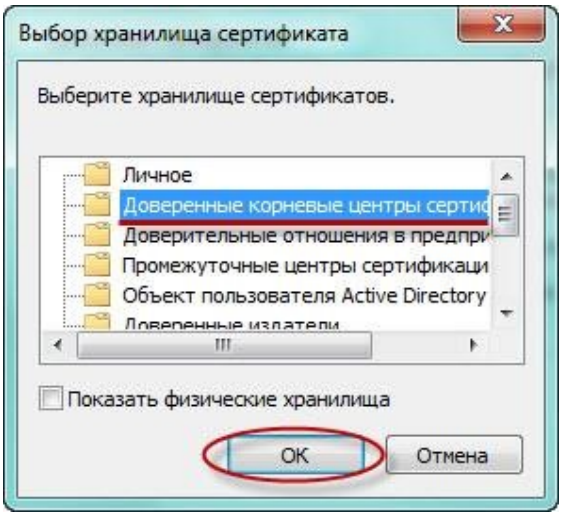

Рисунок 24. Выбор хранилища сертификата

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

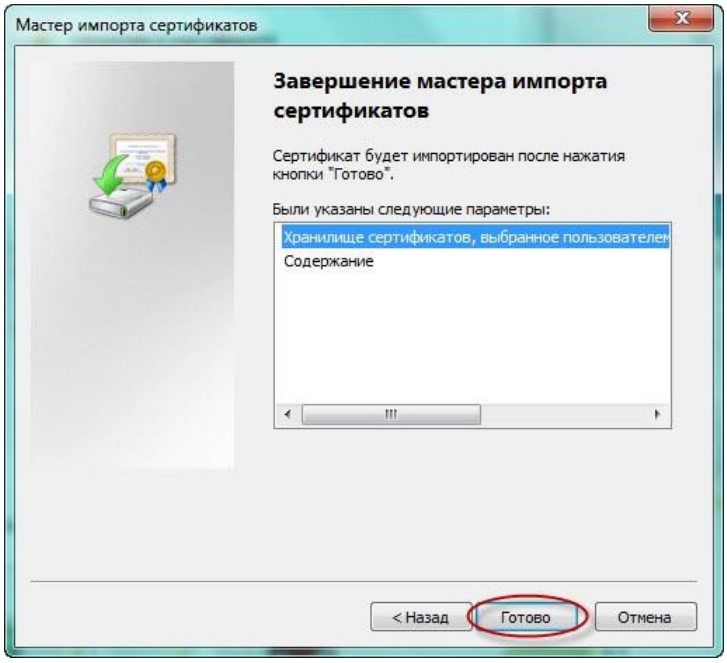

Рисунок 25. Завершение мастера импорта сертификатов

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

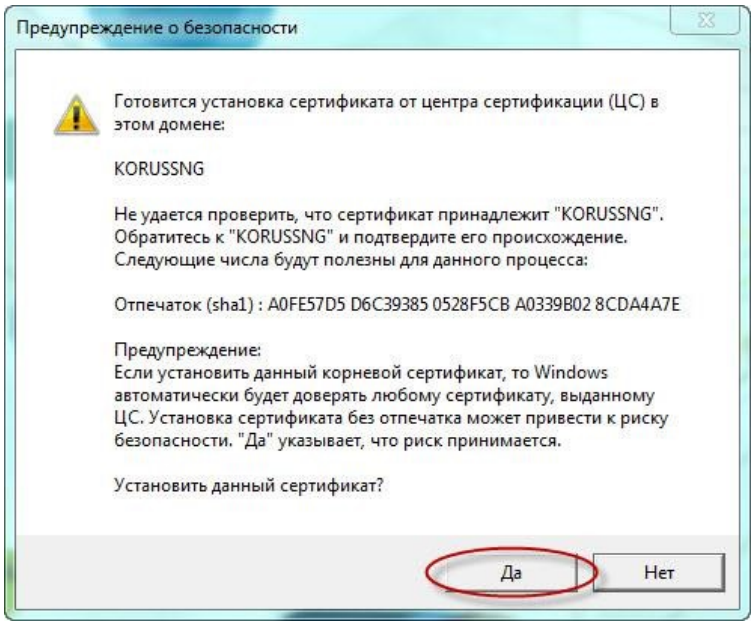

Рисунок 26. Предупреждение о безопасности

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

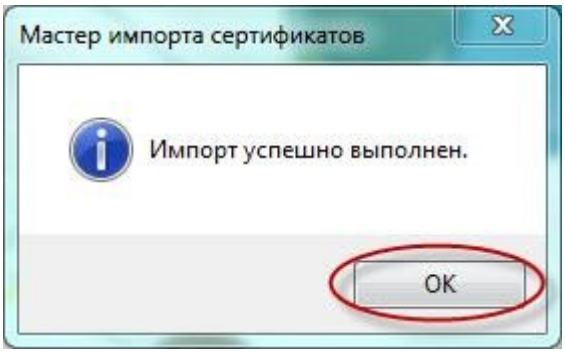

Рисунок 27. Успешное завершение импорта

9. Установка сертификата, аккредитованного УЦ ООО «КОРУС Консалтинг СНГ».
   Установка сертификата «ООО КОРУС Консалтинг СНГ» (скачать) производится аналогично пункту 2-8, но сертификат устанавливается в хранилище **«Промежуточные центры сертификации»**.