Инструкция по настройке подписи в заявлении на прикрепление

На 31 листах

2020 г.

Оглавление

1 УСТАНОВКА КРИПТОПРО CSP

На рабочем месте оператора под управлением ОС Windows установить КриптоПро CSP версии 3.6 и выше или VipNet CSP версии 4.2 и выше, в зависимости от типа ЭЦП, используемой в медицинской организации.

Далее необходимо установить сертификат ЛПУ в папку «Личное», скопировать контейнер закрытого ключа в реестр (для КриптоПро), на локальный диск (для VipNet).

1.1 Установка сертификата ЛПУ в хранилище текущего пользователя

Перед установкой сертификата следует вставить USB-флеш-накопитель с ключом в компьютер.

После установки КриптоПро CSP следует нажать левой кнопкой мыши по установленной программе КриптоПро CSP. Программа может располагаться в меню «Пуск», на рабочем столе (если была установлена иконка), или ее можно найти при помощи поиска (сочетание клавиш WIN+F).

В открывшемся окне (Рисунок 1) следует перейти на вкладку «Сервис», далее нажать кнопку «Скопировать».

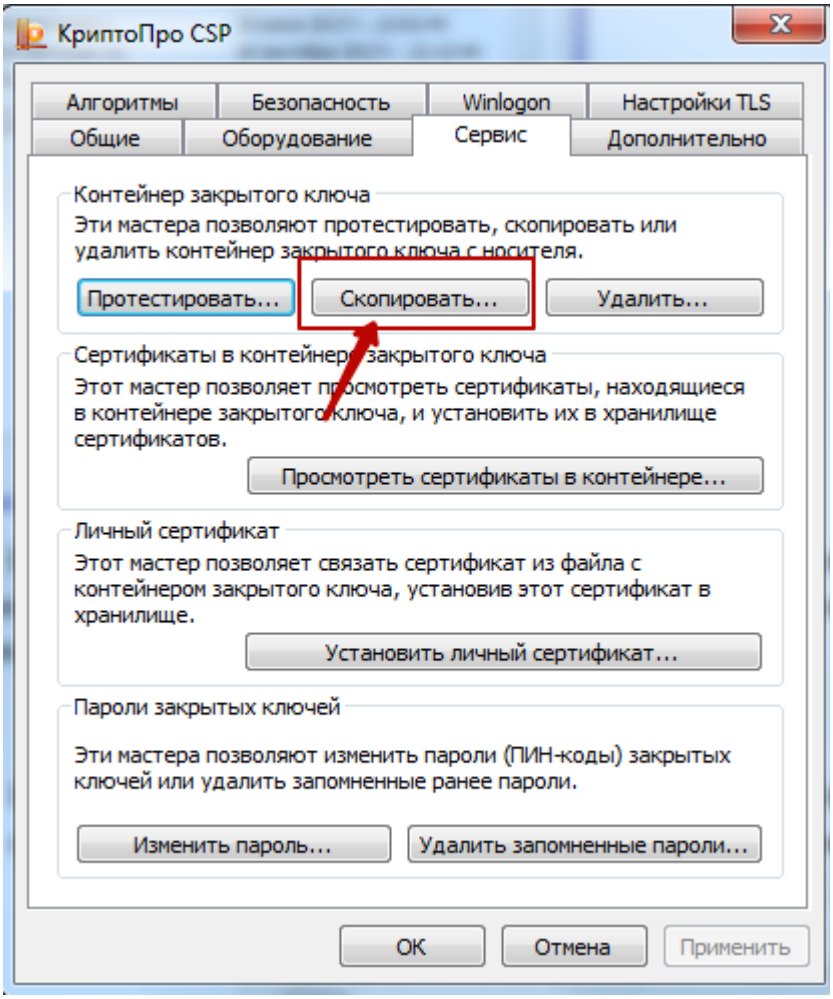

Рисунок 1. Копирование контейнера в реестр на компьютер

В результате откроется окно (Рисунок 2), в котором необходимо указать имя ключевого контейнера.

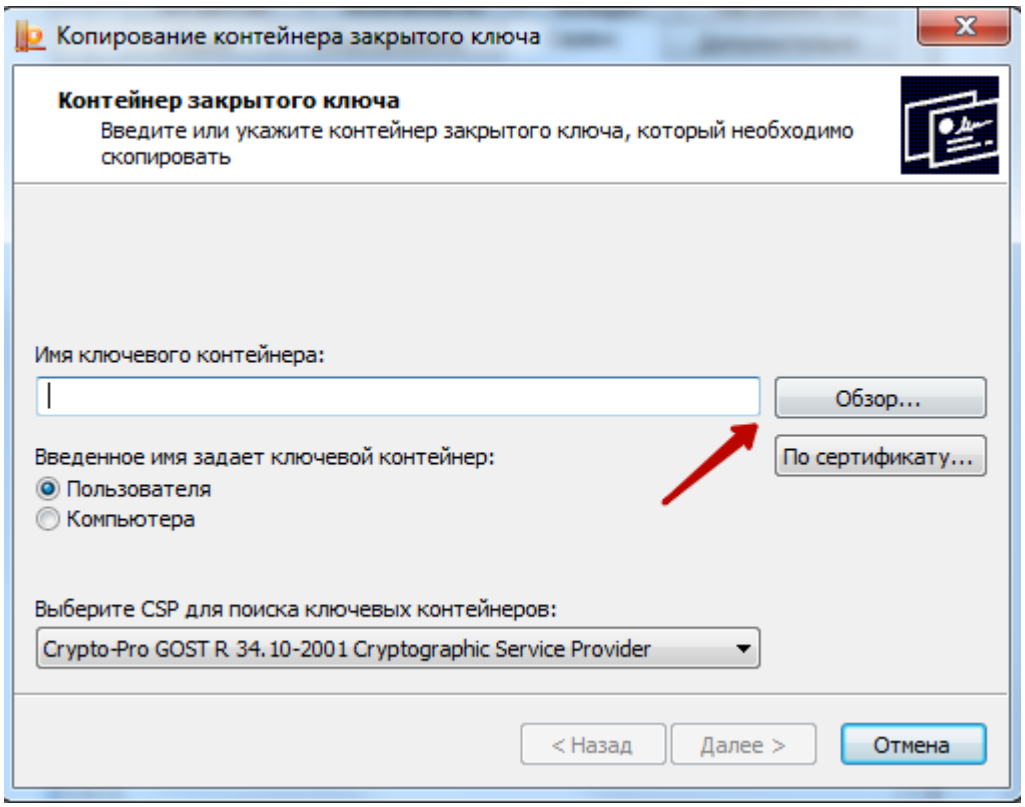

Рисунок 2. Окно ввода имени ключевого контейнера

Для того чтобы ввести имя контейнера следует нажать кнопку «Обзор». В результате откроется окно выбора контейнера (Рисунок 3).

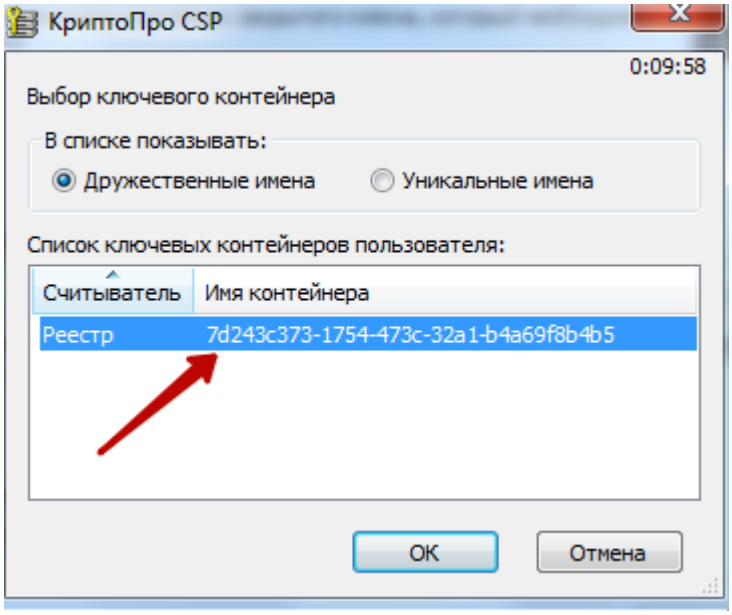

Рисунок 3. Выбор ключевого контейнера

В данном окне необходимо выбрать имя реестра и нажать кнопку «ОК». В результате заполнится поле «Имя ключевого контейнера» (Рисунок 4).

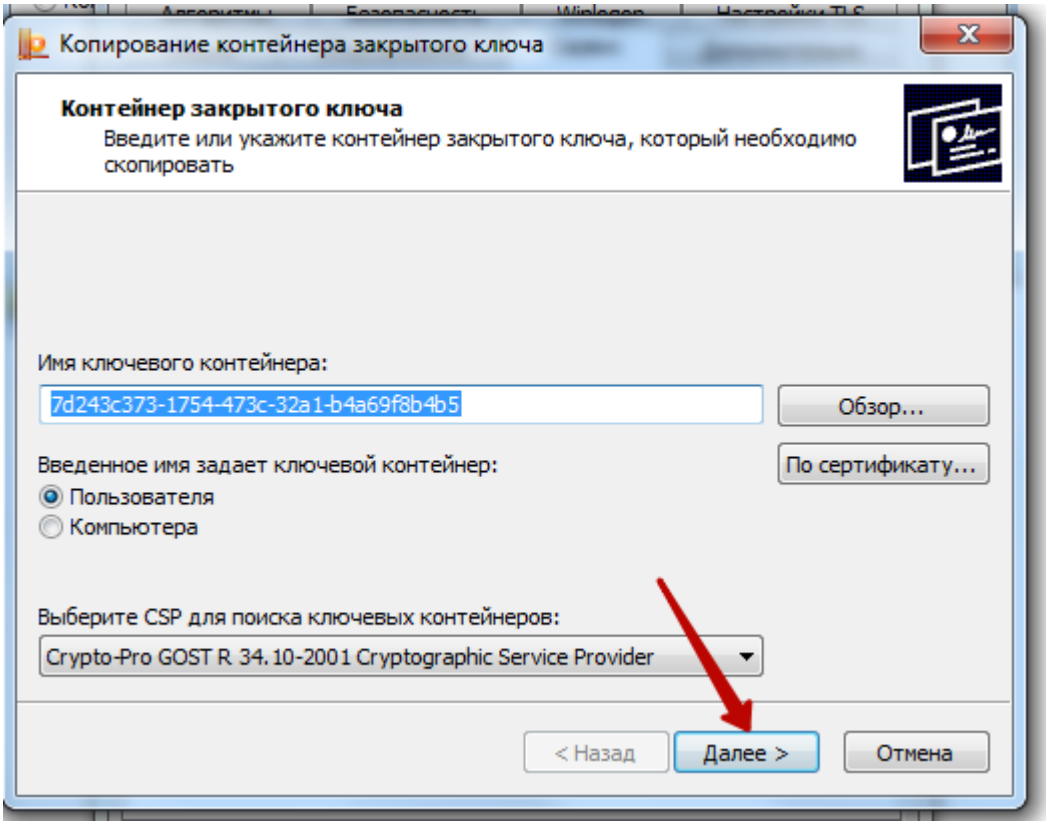

Рисунок 4. Заполнено поле «Имя ключевого контейнера»

После того как имя задано следует нажать кнопку «Далее». В результате отроется окно (Рисунок 5), в котором необходимо указать имя для создаваемого ключевого контейнера.

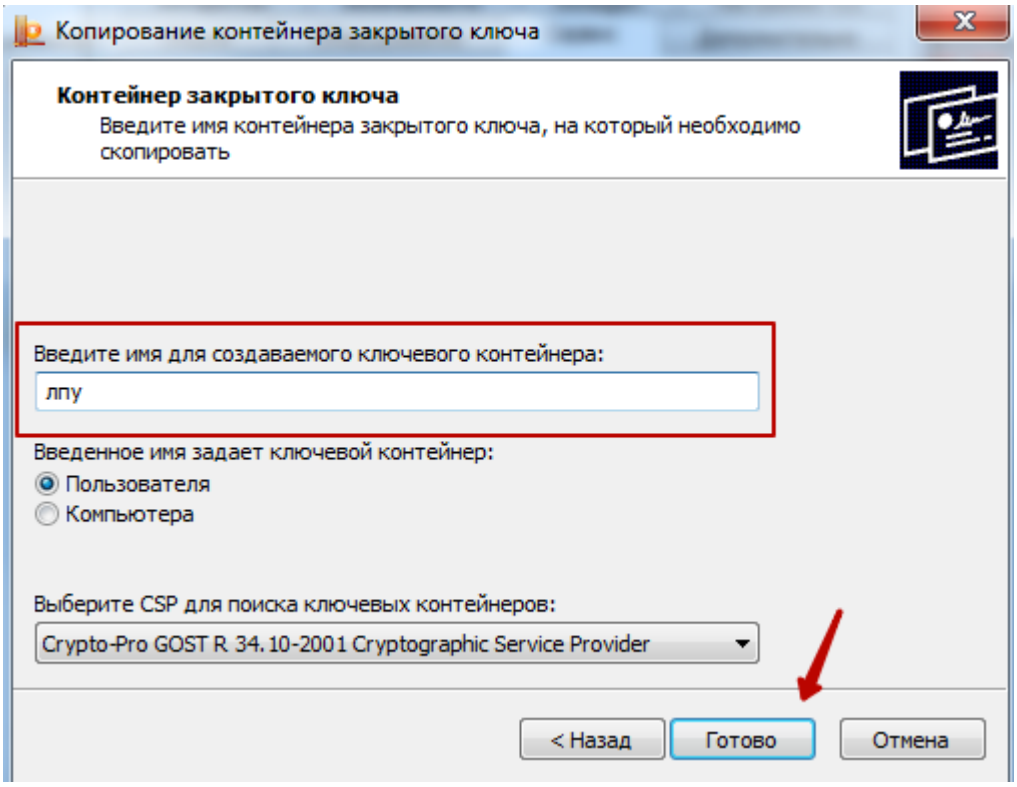

Рисунок 5. Заполнение поля «Введите имя для создаваемого ключевого контейнера

В качестве имени создаваемого ключевого контейнера можно указать любое имя, в том числе и то, которое указано по умолчанию. После задания имени следует нажать кнопку «Готово». В результате откроется окно (Рисунок 6), в котором необходимо выбрать носитель для хранения контейнера закрытого ключа.

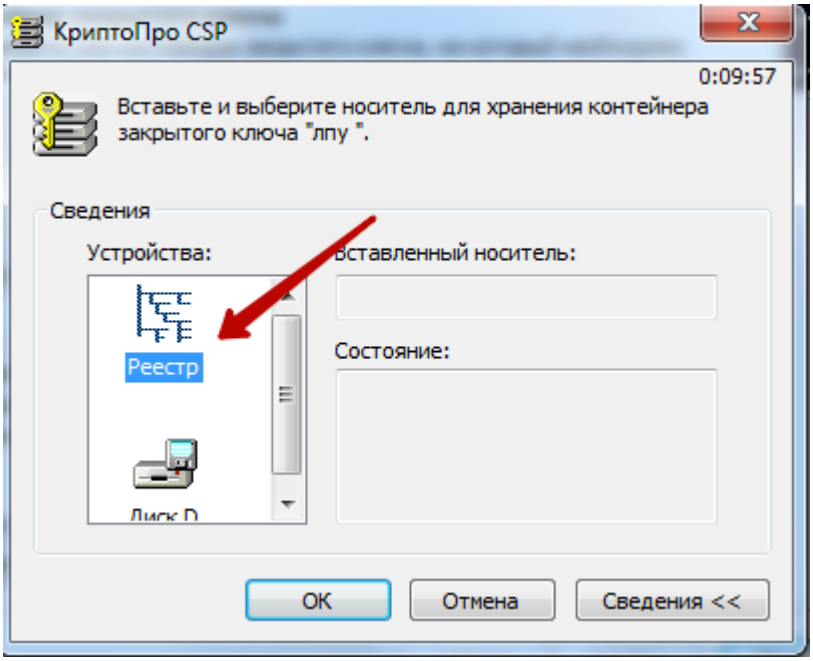

Рисунок 6. Выбор носитель для хранения контейнера

В данном окне следует выбрать устройство. В данном случае, в качестве устройства следует выбрать «Реестр» и нажать кнопку «ОК». После чего откроется окно (Рисунок 7), в котором необходимо задать пароль для создаваемого контейнера.

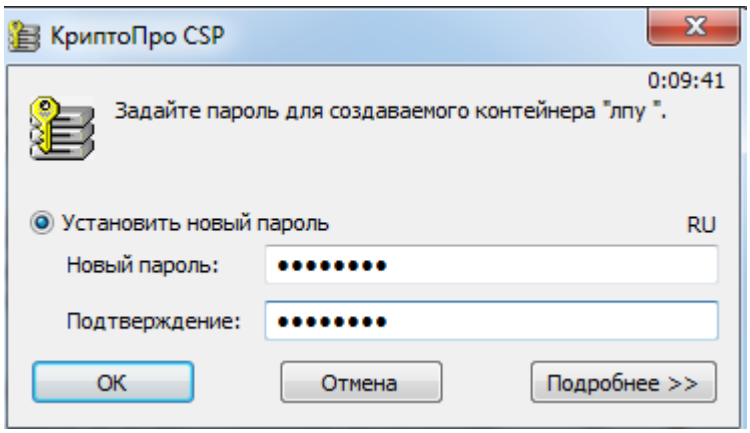

Рисунок 7. Окно задания пароля для контейнера

В поле «Новый пароль» следует ввести пароль на создаваемый контейнер. В поле «Подтверждение» следует повторно ввести этот же пароль. Затем нажать кнопку «ОК».

Контейнер создан, далее следует установить сертификат из контейнера в реестре на компьютере.

1.2 Установка сертификата из контейнера в реестре на компьютере

Для установки сертификата следует на вкладке «Сервис» нажать кнопку «Просмотреть сертификаты в контейнере» (Рисунок 8).

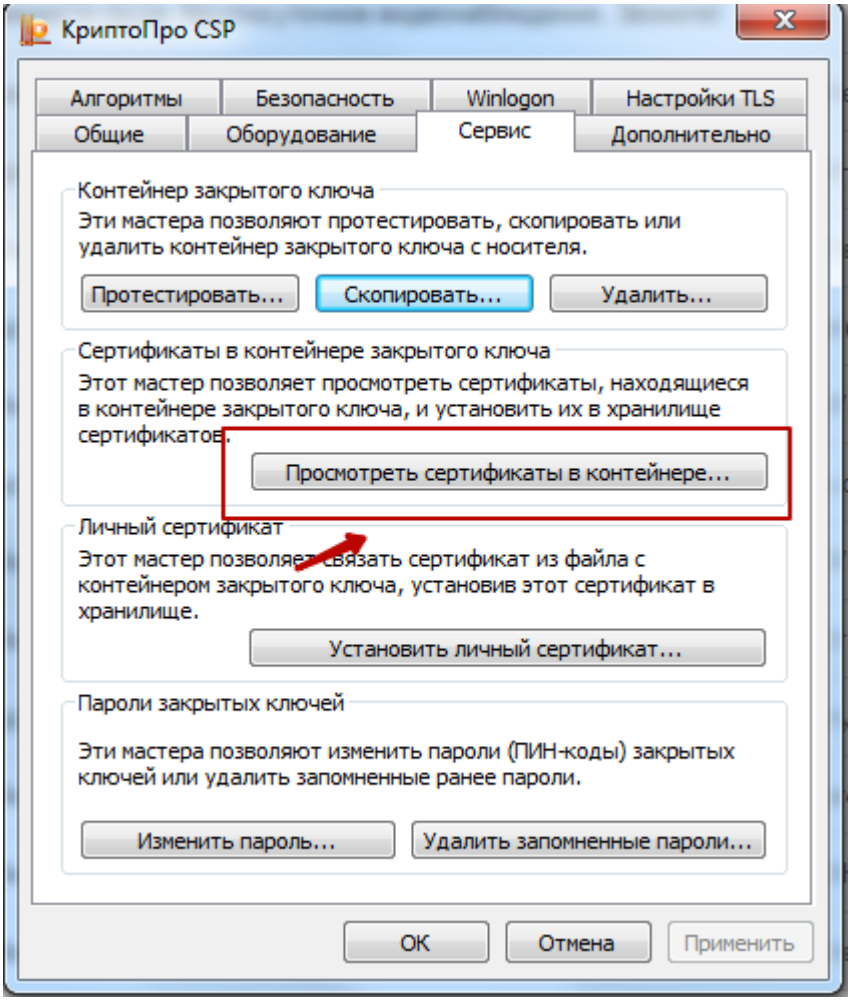

Рисунок 8. Окно «КриптоПро CSP», вкладка «Сервис»

В результате откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 9).

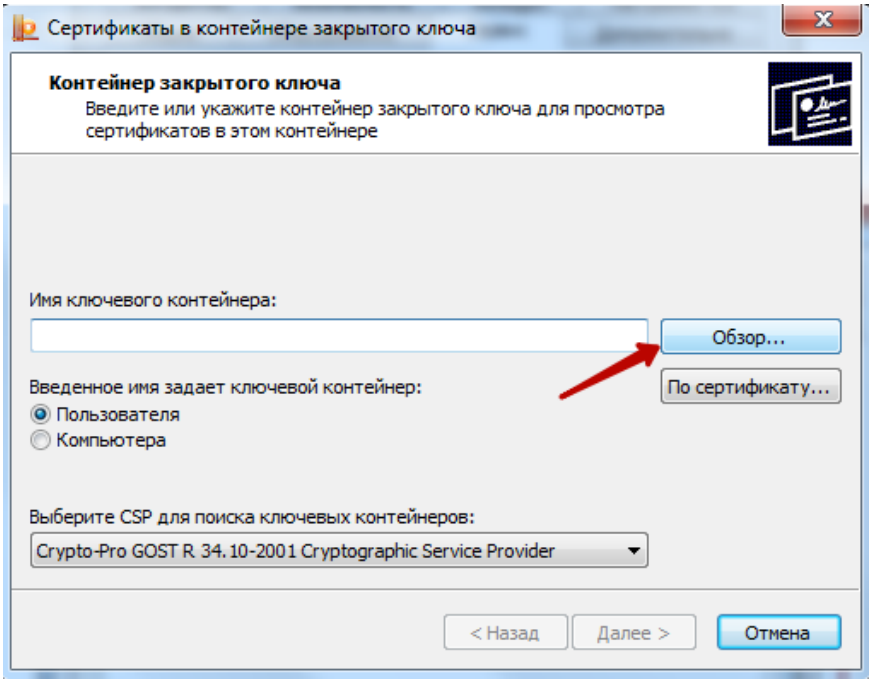

Рисунок 9. Окно «Сертификаты закрытого ключа»

В данном окне следует установить имя ключевого контейнера, нажав кнопку «Обзор». В результате откроется окно выбора ключевого контейнера (Рисунок 10).

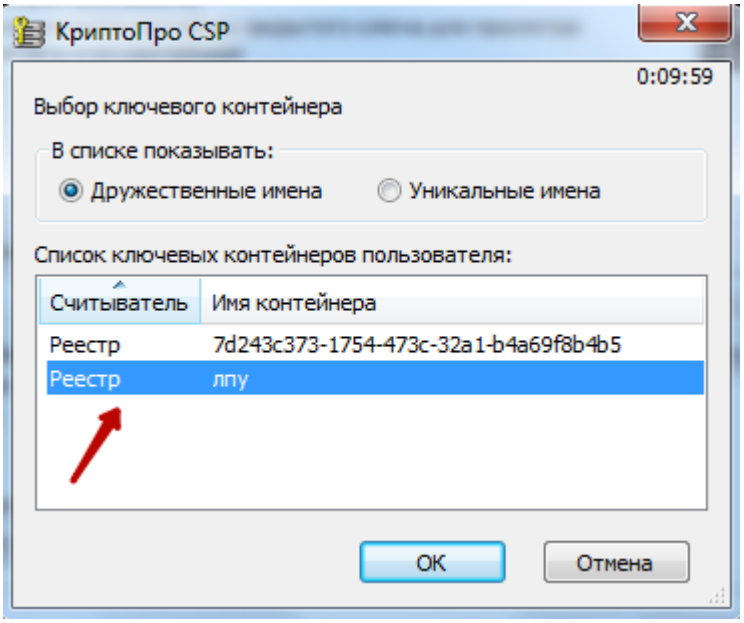

Рисунок 10. Окно выбора ключевого контейнера»

В открывшемся окне следует выбрать имя контейнер, который был создан, и нажать кнопку «ОК». В результате имя ключевого контейнера будет задано (Рисунок 11).

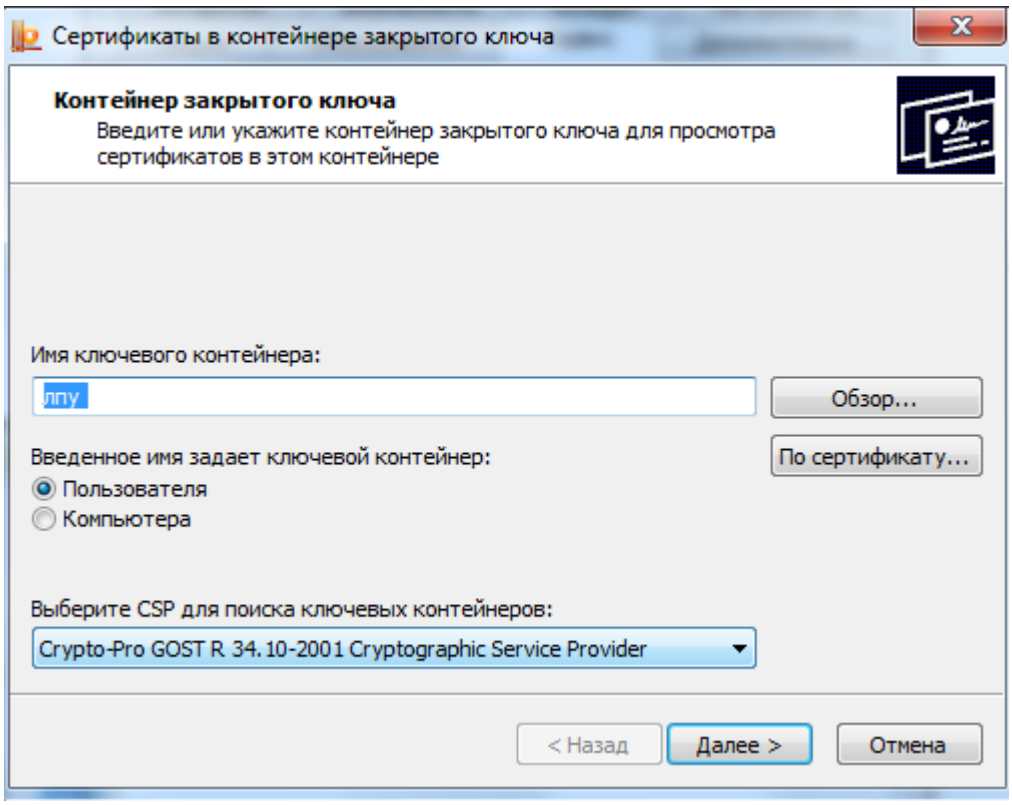

Рисунок 11. Установлено имя ключевого контейнера

Для продолжения следует нажать кнопку «Далее». В результате откроется окно для просмотра сертификата (Рисунок 12).

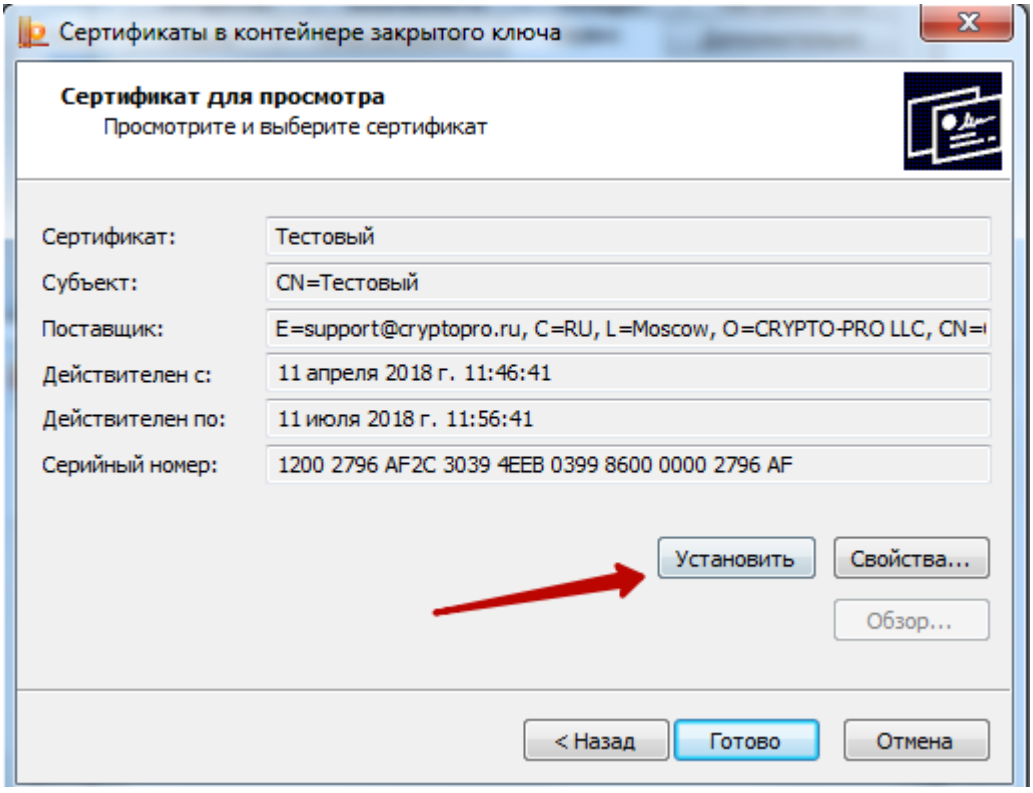

Рисунок 12. Окно просмотра сертификата

Для установки сертификата следует нажать кнопку «Установить». После чего откроется окно (Рисунок 13) с сообщением, что в хранилище уже присутствует сертификат. Следует заметить существующий сертификат новым, нажав кнопку «Да».

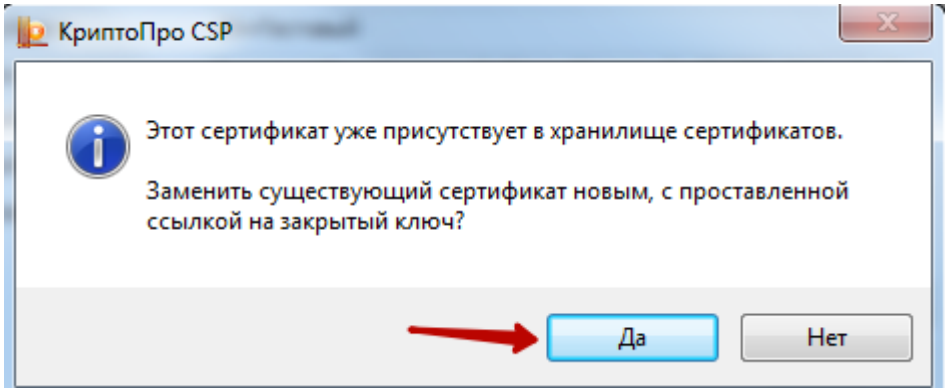

Рисунок 13. Диалоговое окно о замене существующего сертификата

В результате сертификат установится, появится информационное окно об успешной установке (Рисунок 14).

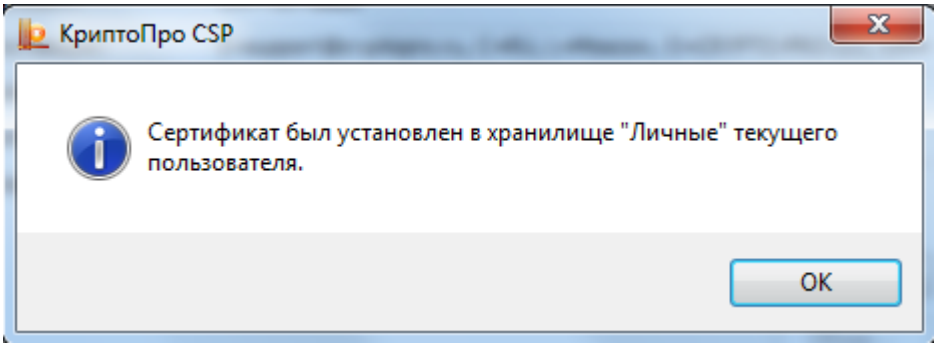

Рисунок 14. Информационное окно об успешной установке сертификата

Далее следует протестировать контейнер.

1.3 Тестирование контейнера из реестра для сохранения пароля

Для тестирования контейнера следует на вкладке «Сервис» нажать кнопку «Протестировать» (Рисунок 15).

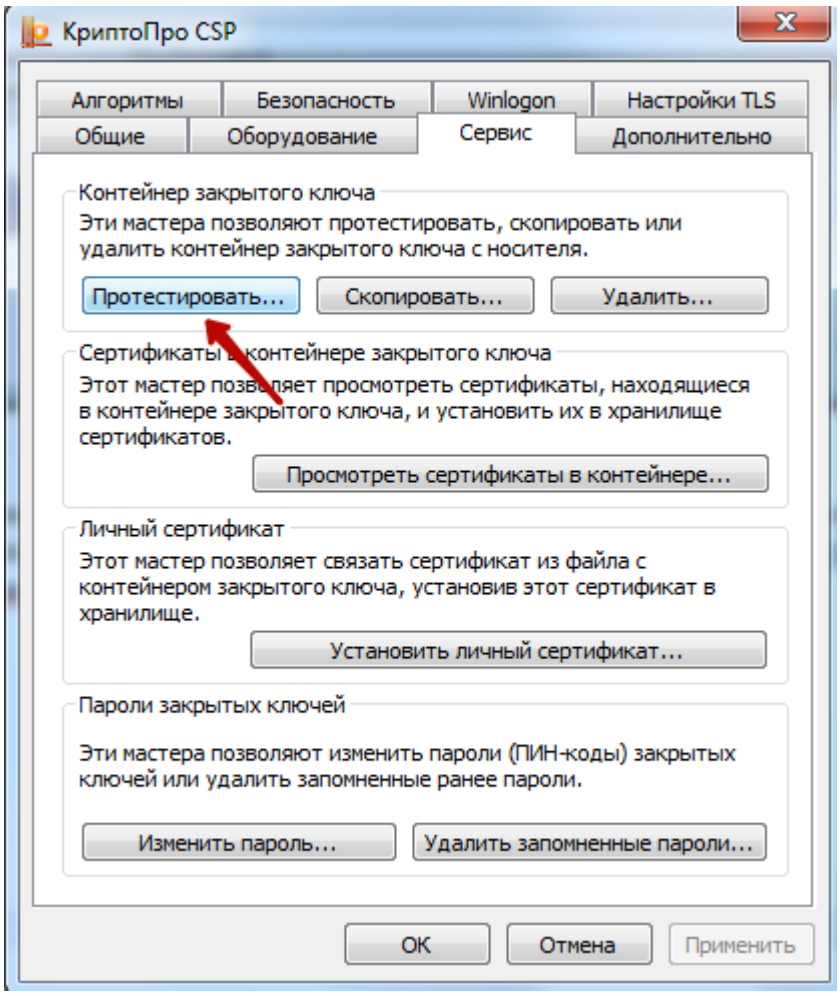

Рисунок 15. Окно «КриптоПро CSP», вкладка «Сервис»

Откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 16).

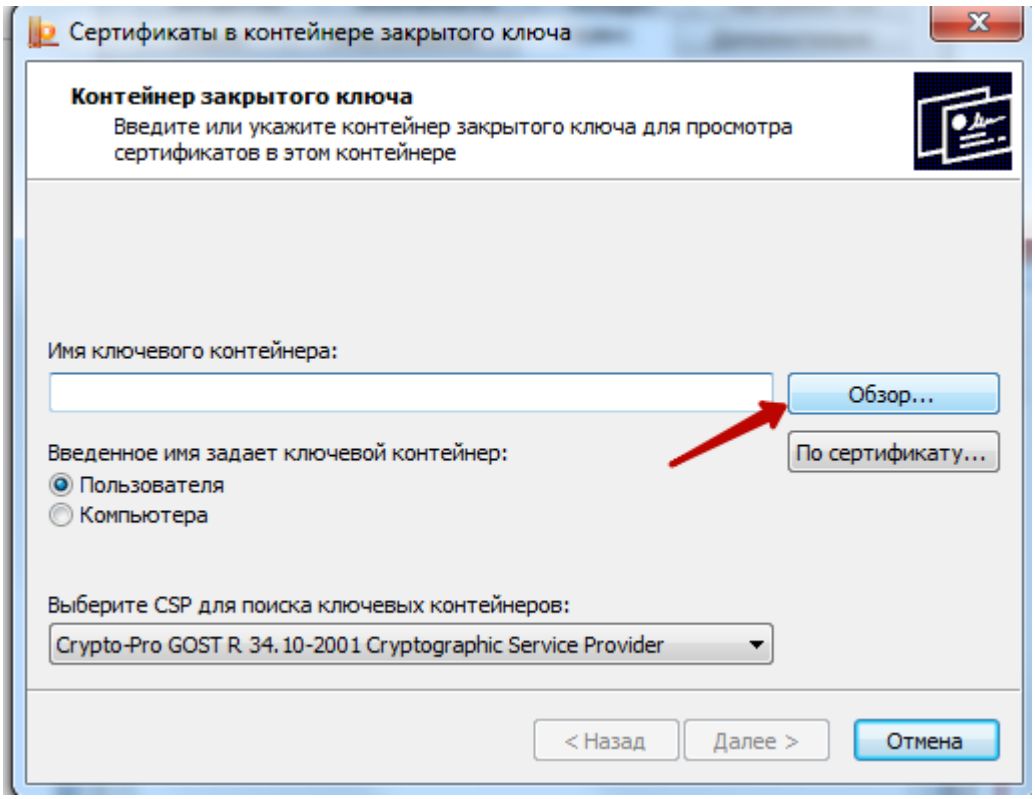

Рисунок 16. Окно «Сертификаты в контейнере закрытого ключа»

В данном окне следует нажать кнопку «Обзор» и в открывшемся окне следует выбрать созданный контейнер (Рисунок 17).

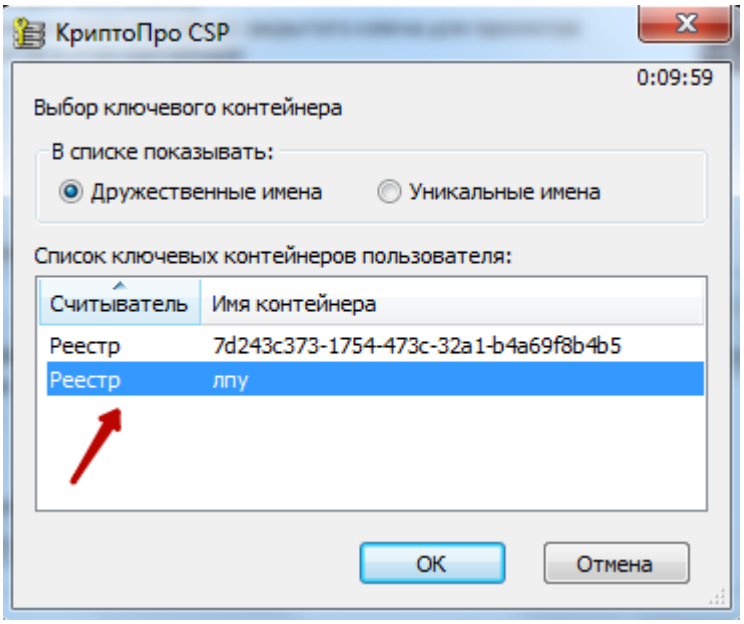

Рисунок 17. Выбор контейнера

После выбора контейнера следует нажать кнопку «ОК». В результате поле «Имя ключевого контейнера» заполнится (Рисунок 18).

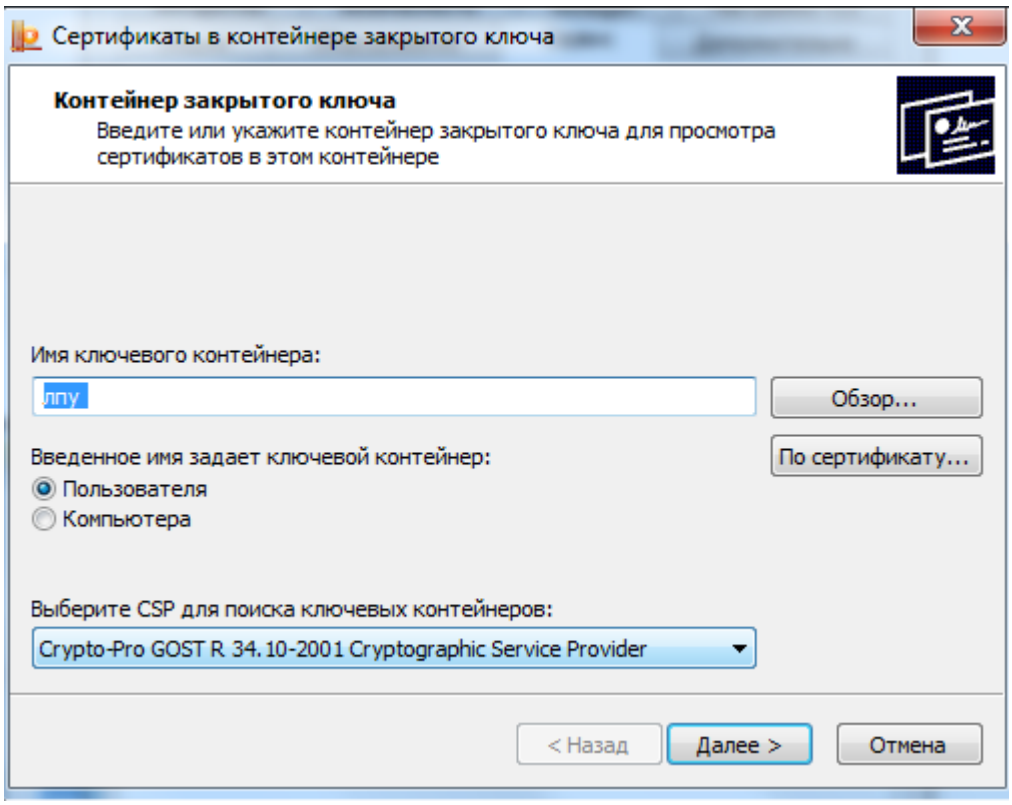

Рисунок 18. Окно «Сертификаты в контейнере закрытого ключа»

Затем следует нажать кнопку «Далее». В результате откроется окно для ввода пароля для контейнера (Рисунок 19).

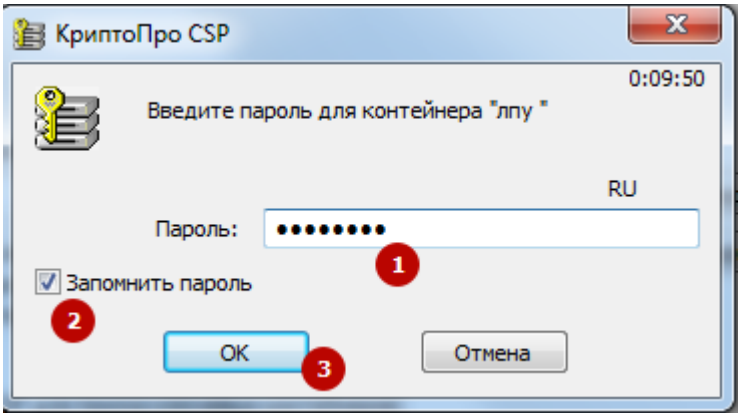

Рисунок 19. Окно ввода пароля для контейнера

В данном окне в поле «Пароль» следует ввести пароль на контейнер, который был установлен при создании контейнера. Далее следует установить флажок в поле «Запомнить пароль» и нажать кнопку «ОК». В результате появится окно «Тестирование контейнера закрытого ключа» (Рисунок 20).

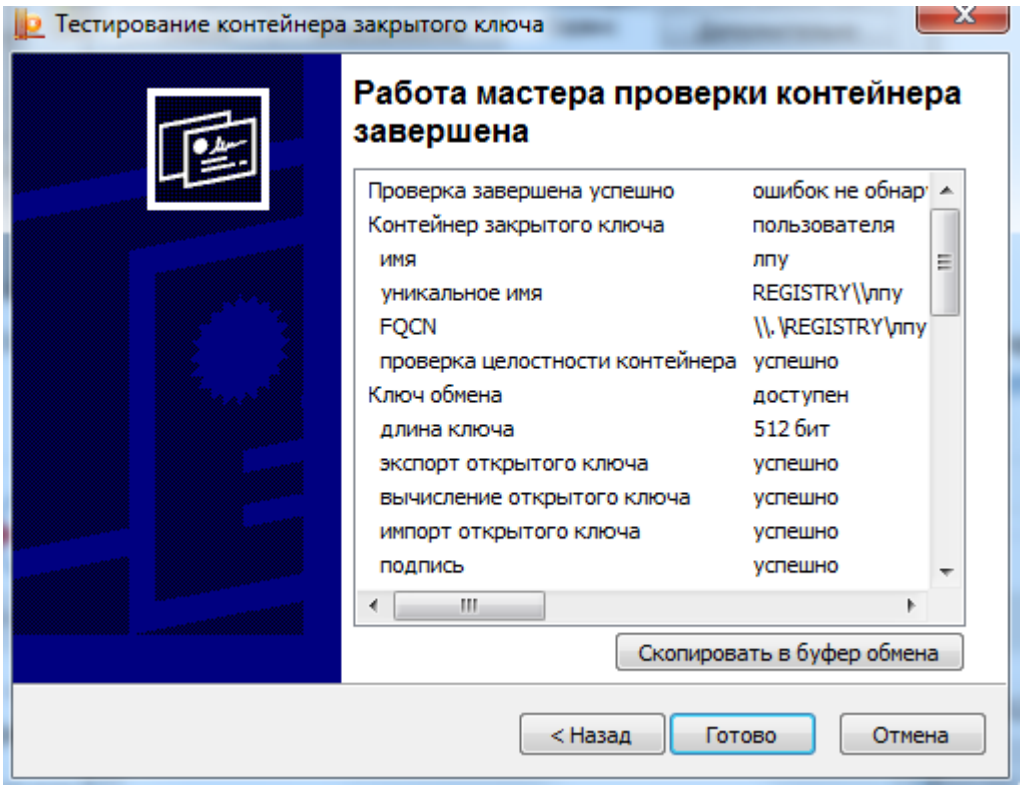

Рисунок 20. «Тестирование контейнера закрытого ключа»

В данном окне содержится информация о тестировании контейнера. В случае успешного тестирования будет сообщение «Ошибок не обнаружено». Для завершения тестирования следует нажать кнопку «Готово».

После установки сертификата ЛПУ следует убедиться, что он установлен для текущего пользователя, а не для локального компьютера.

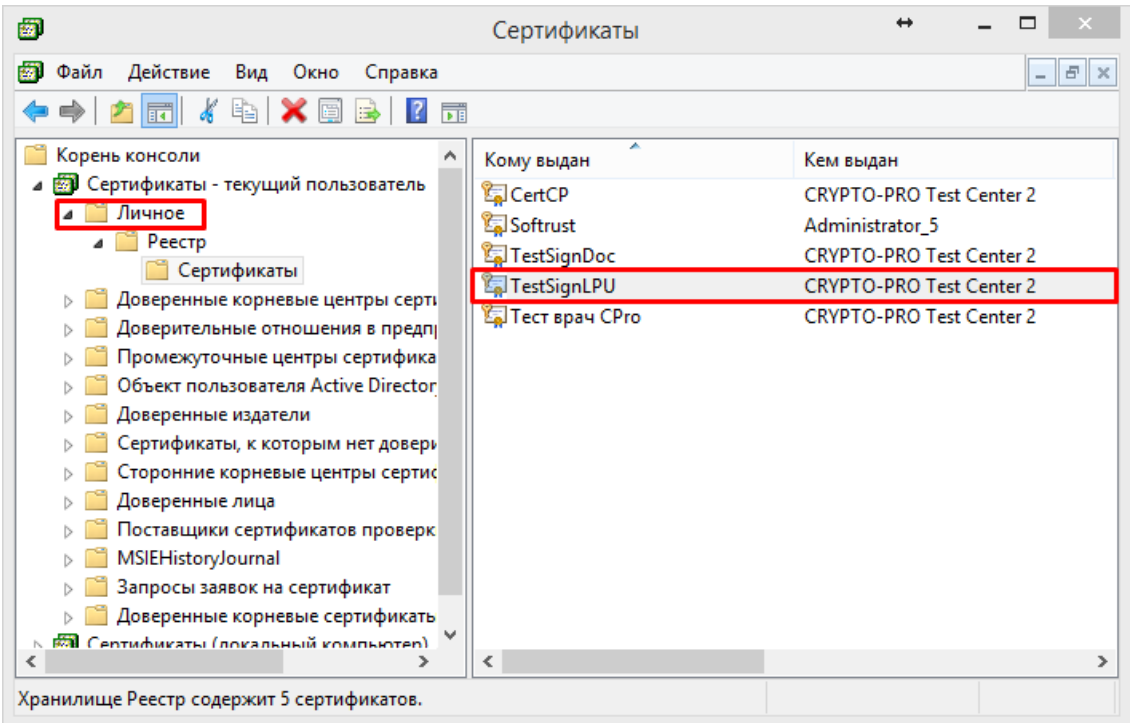

Рисунок 21. Сертификаты установлены для текущего пользователя

Далее необходимо просмотреть пути сертификации (Рисунок 22).

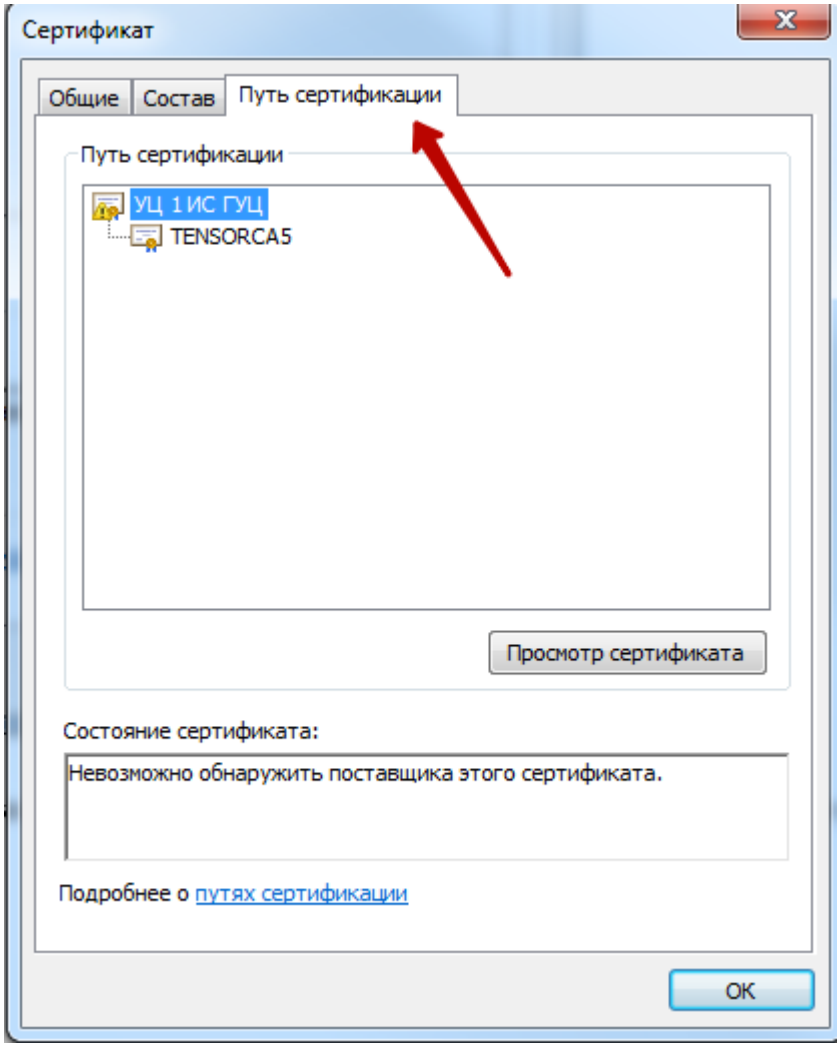

Рисунок 22. Отображение пути сертификации

1.4 Установка корневого сертификата УЦ

В случае, если у сертификата отсутствует корневой сертификат УЦ, то требуется скачать с сайта УЦ (выдавшего ЭЦП) список отозванных сертификатов и корневой сертификат, после этого следует установить данные сертификаты.

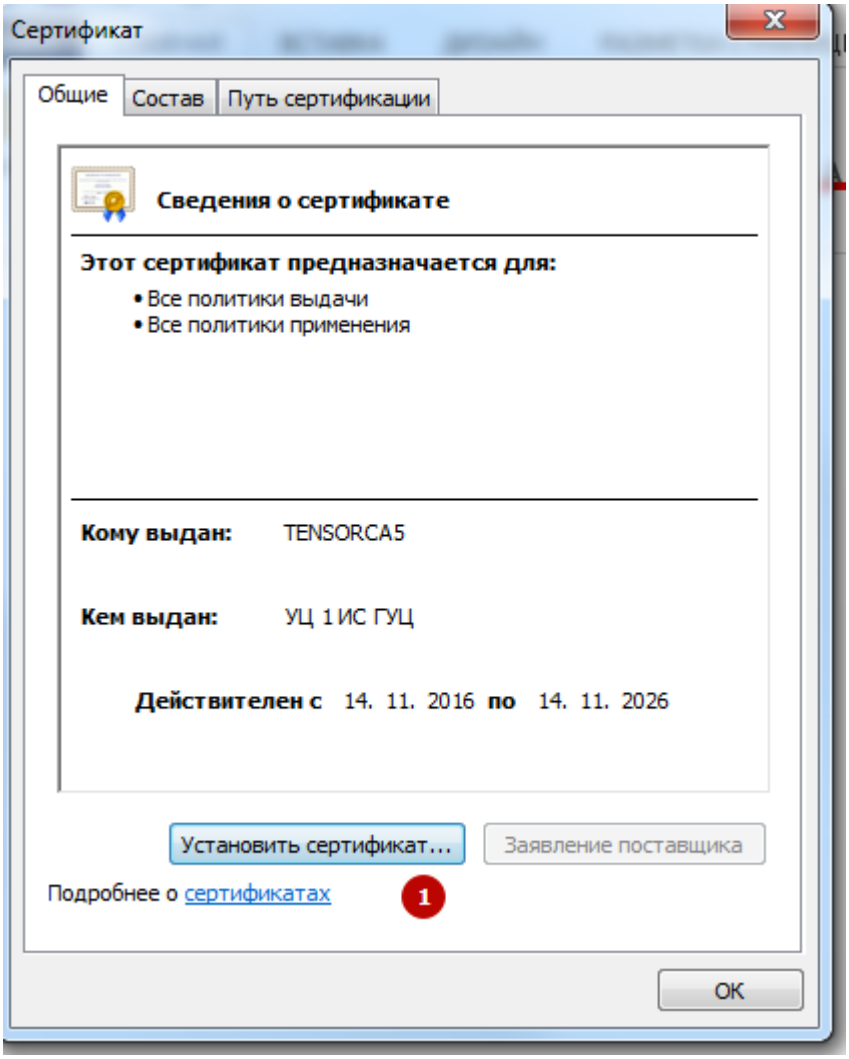

Рисунок 23. Установка сертификата

В открывшемся окне нажать «Далее» (Рисунок 24).

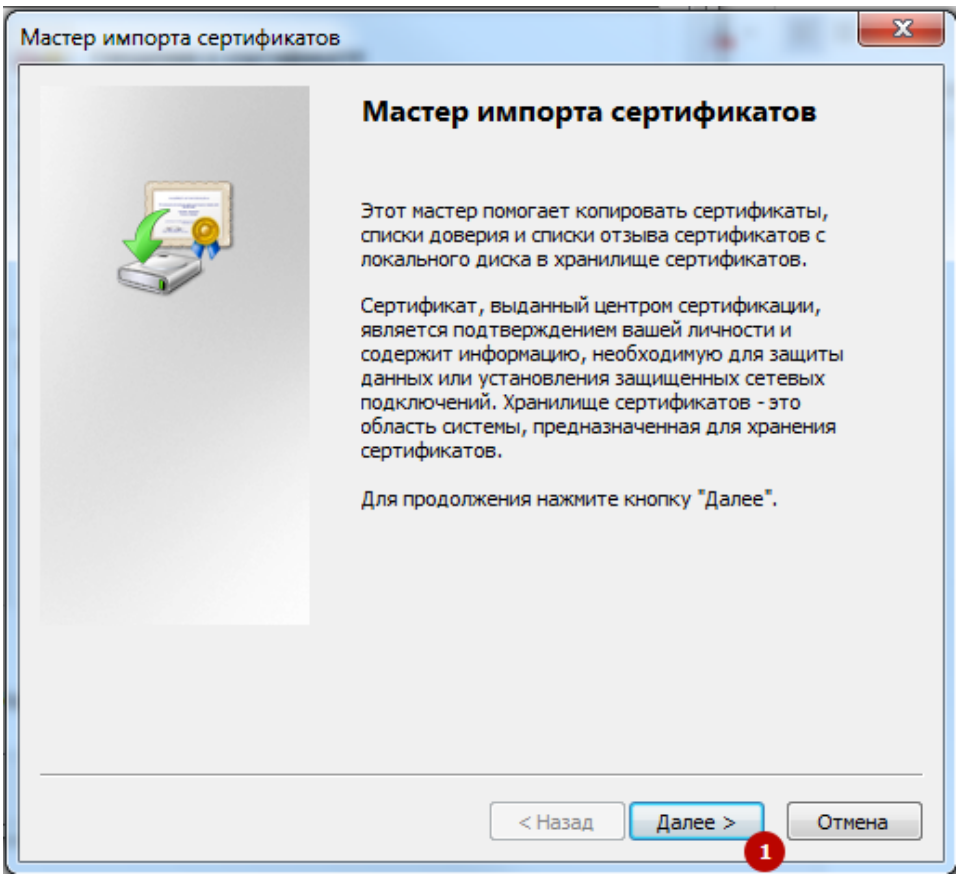

Рисунок 24. Окно «Мастер импорта сертификата»

Далее необходимо выбрать хранилище сертификатов (Рисунок 25, Рисунок 26).

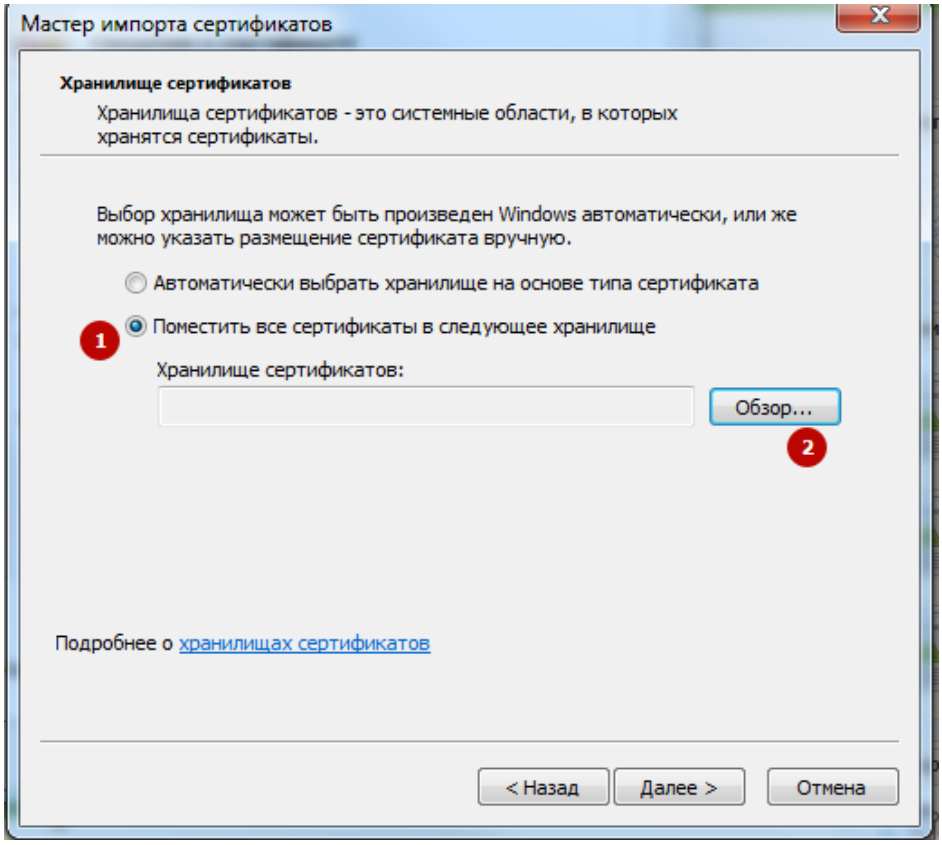

Рисунок 25. Выбор хранилища сертификатов

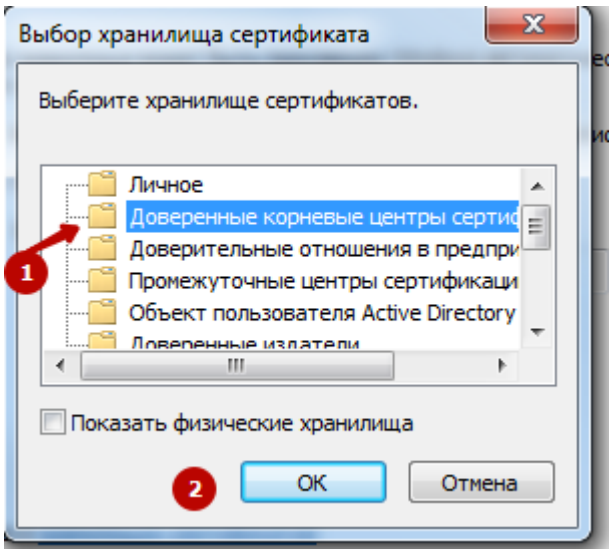

Рисунок 26. Выбор хранилища сертификатов

После выбора хранилища сертификатов нажать «Далее» (Рисунок 27).

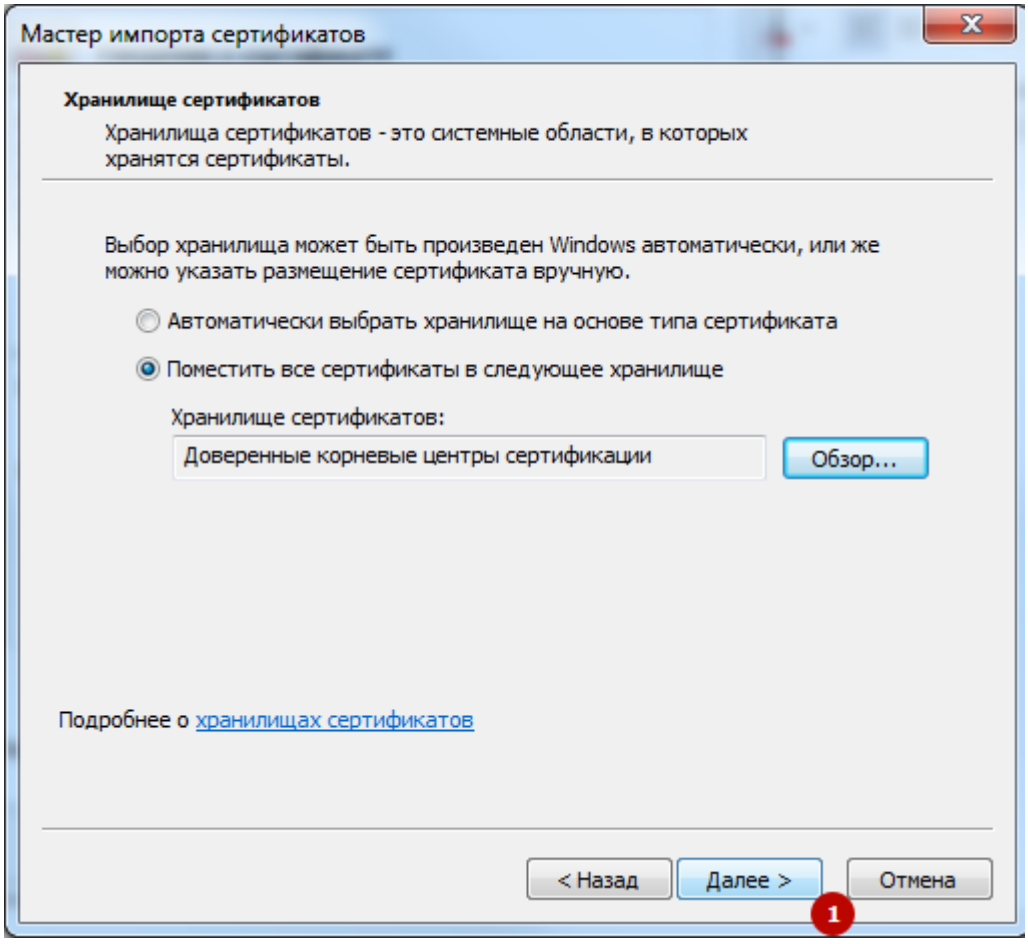

Рисунок 27. Окно «Мастер импорта сертификата»

Для завершения установки сертификата в открывшемся окне следует нажать «Готово» (Рисунок 28).

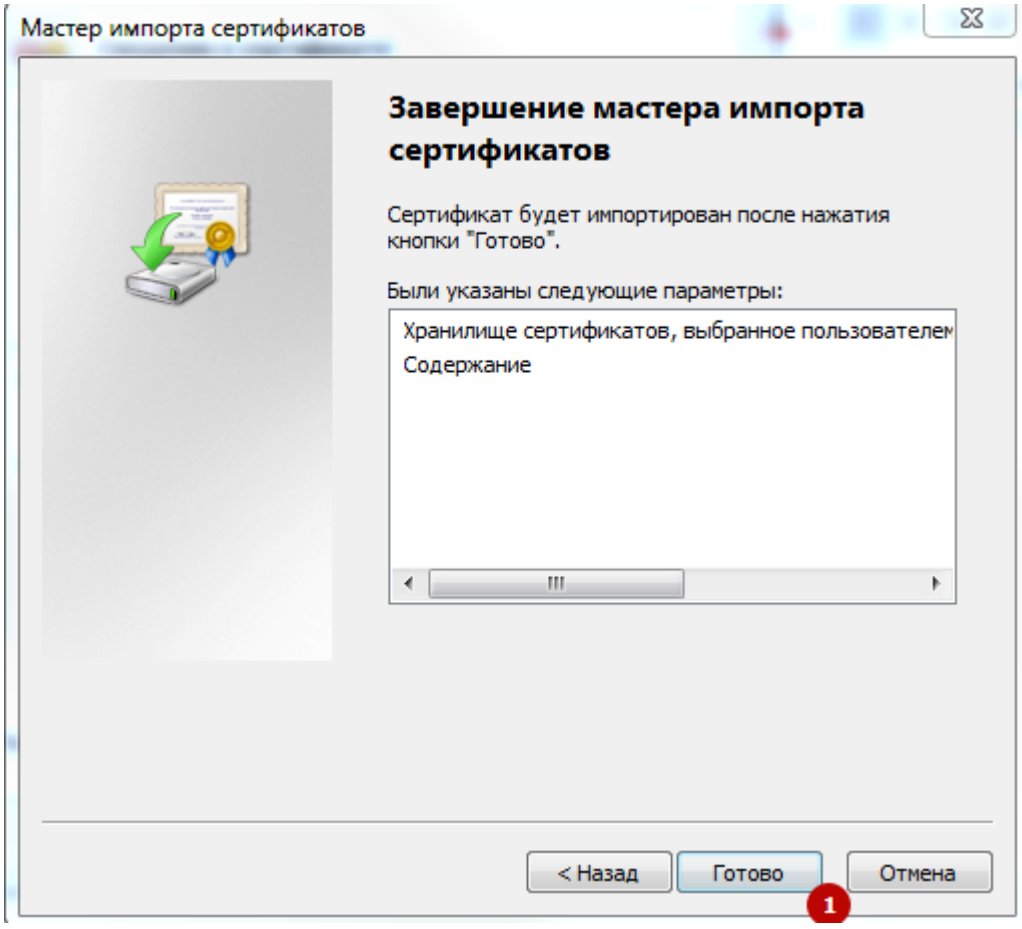

Рисунок 28. Завершение мастера импорта сертификатов

После завершения установки отобразится окно с предупреждением о безопасности, необходимо нажать «Да» (Рисунок 29).

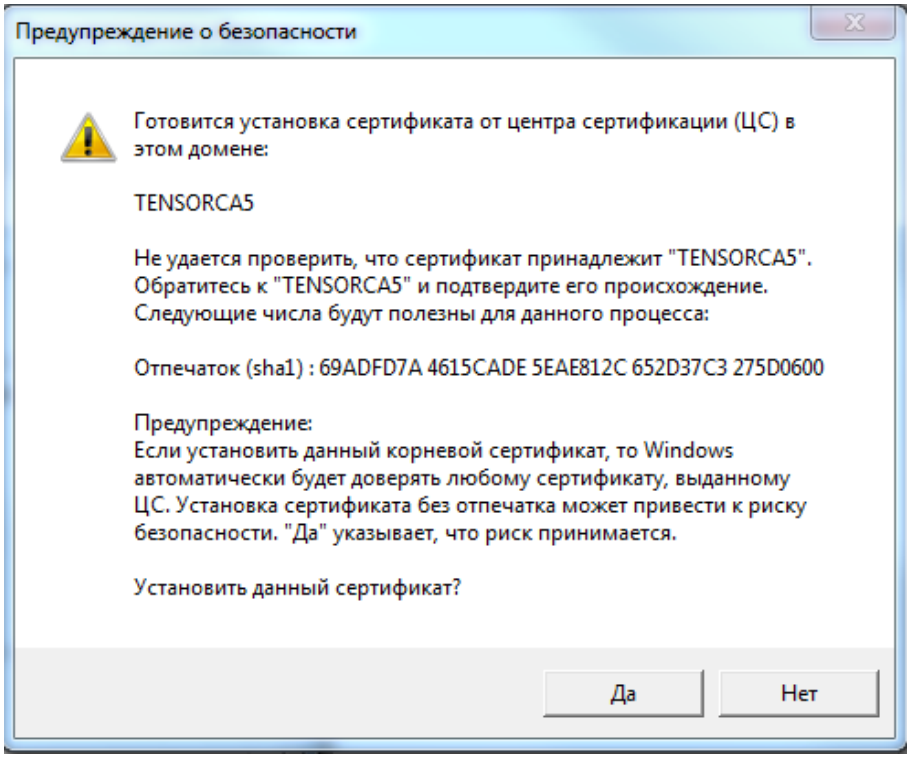

Рисунок 29.Предупреждение о безопасности

После успешной установки сертификата отобразится соответствующее сообщение (Рисунок 30).

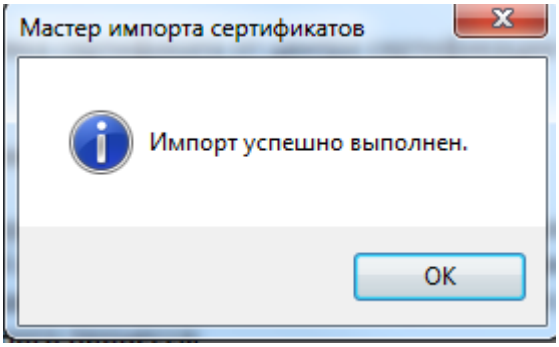

Рисунок 30. Сообщение об успешном импорте

1.5 Установка корневого сертификата головного УЦ

Далее необходимо установить корневой сертификат головного удостоверяющего центра, ссылка для скачивания – https://e-trust.gosuslugi.ru/MainCA

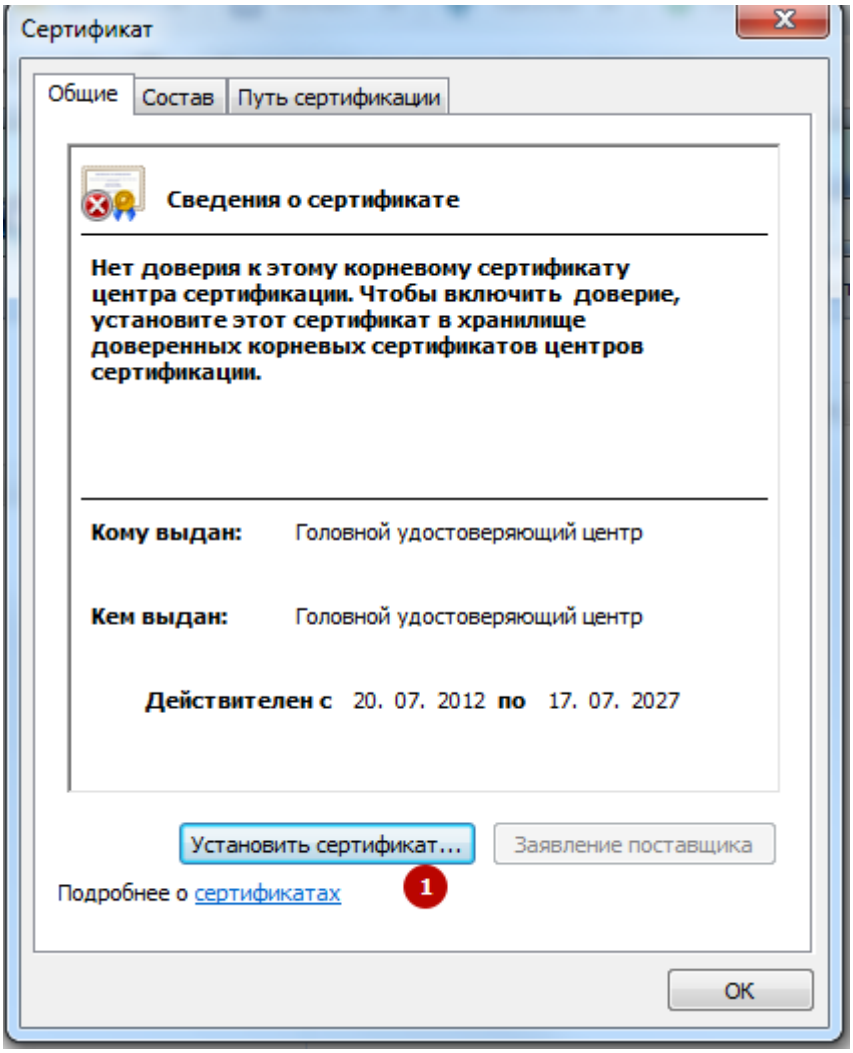

Рисунок 31. Установка сертификата

В открывшемся окне нажать «Далее» (Рисунок 32).

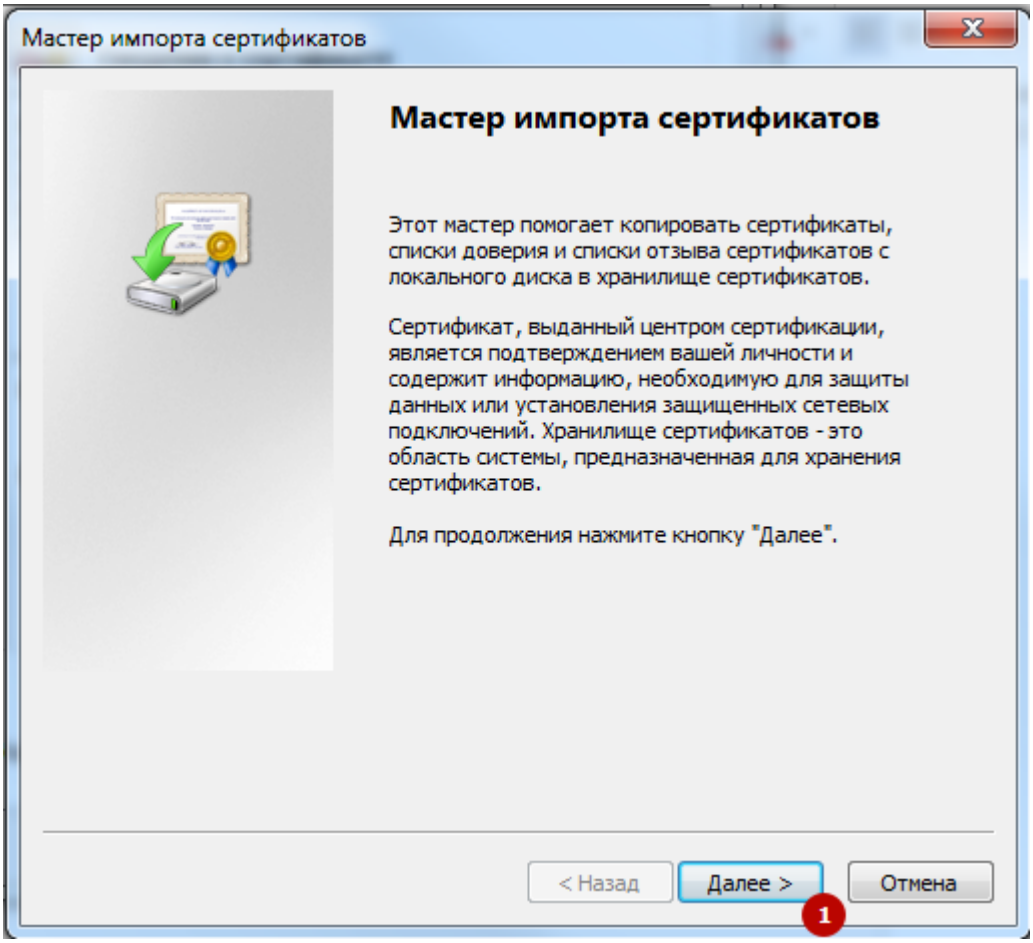

Рисунок 32. Окно «Мастер импорта сертификата»

Далее необходимо выбрать хранилище сертификатов (Рисунок 33, Рисунок 34).

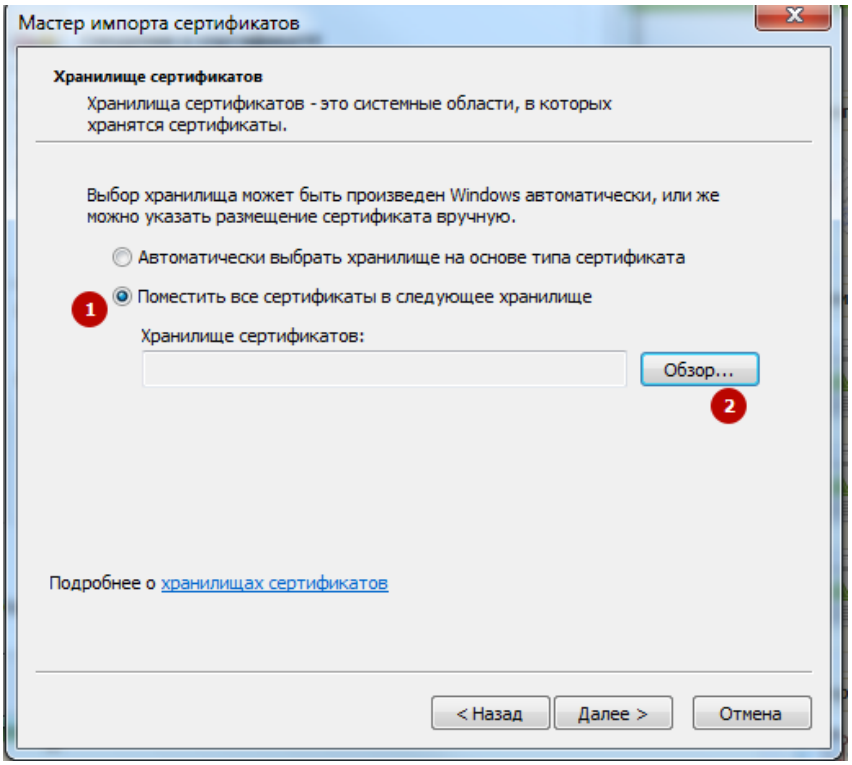

Рисунок 33. Выбор хранилища сертификатов

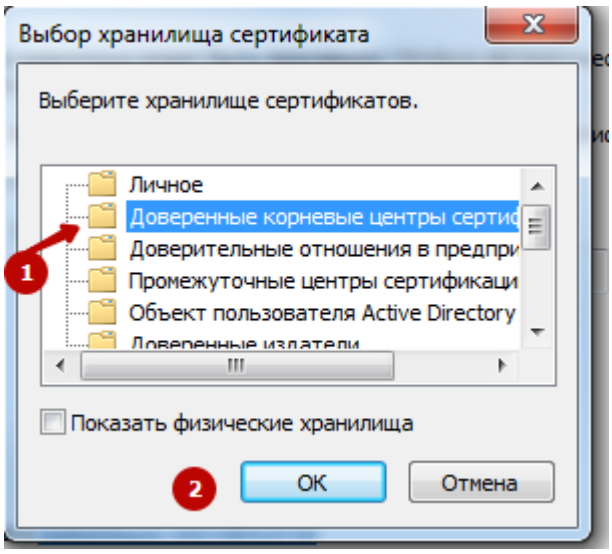

Рисунок 34. Выбор хранилища сертификатов

После выбора хранилища сертификатов нажать «Далее» (Рисунок 35).

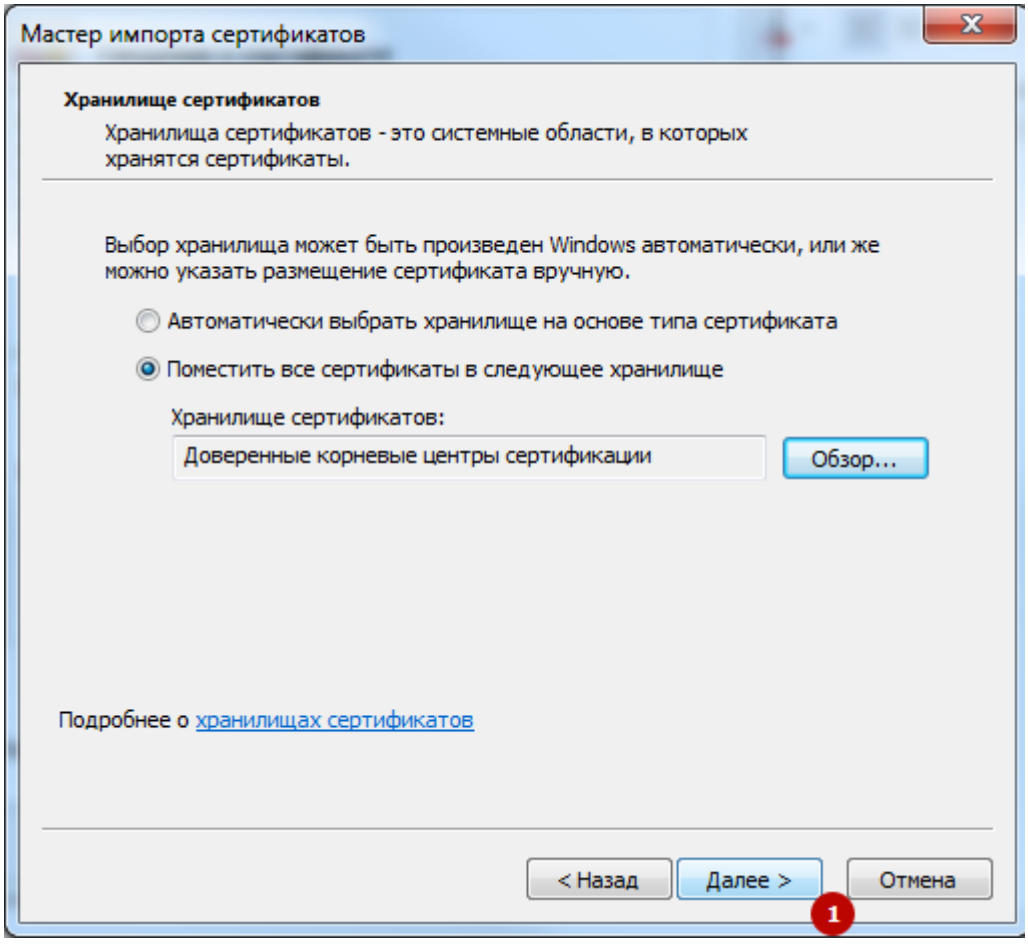

Рисунок 35. Окно «Мастер импорта сертификата»

Для завершения установки сертификата в открывшемся окне следует нажать «Готово» (Рисунок 36).

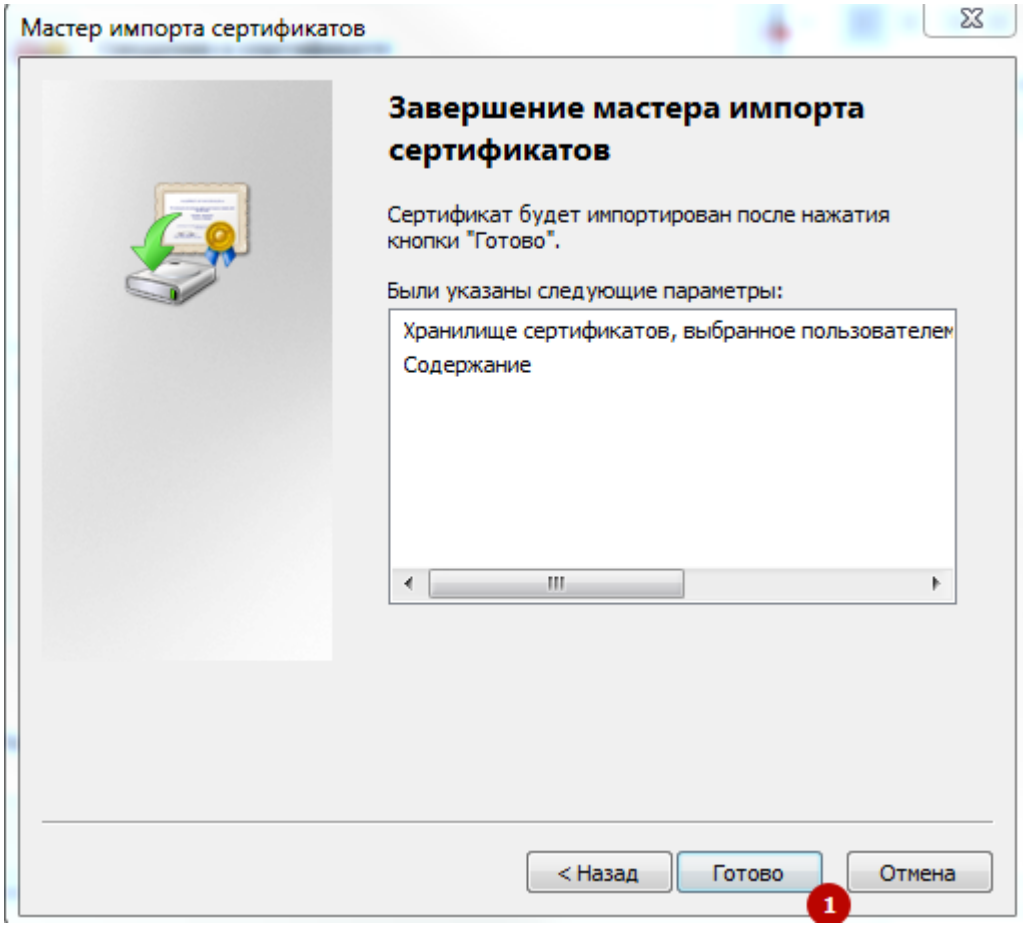

Рисунок 36. Завершение мастера импорта сертификатов

После завершения установки отобразится окно с предупреждением о безопасности, необходимо нажать «Да» (Рисунок 37).

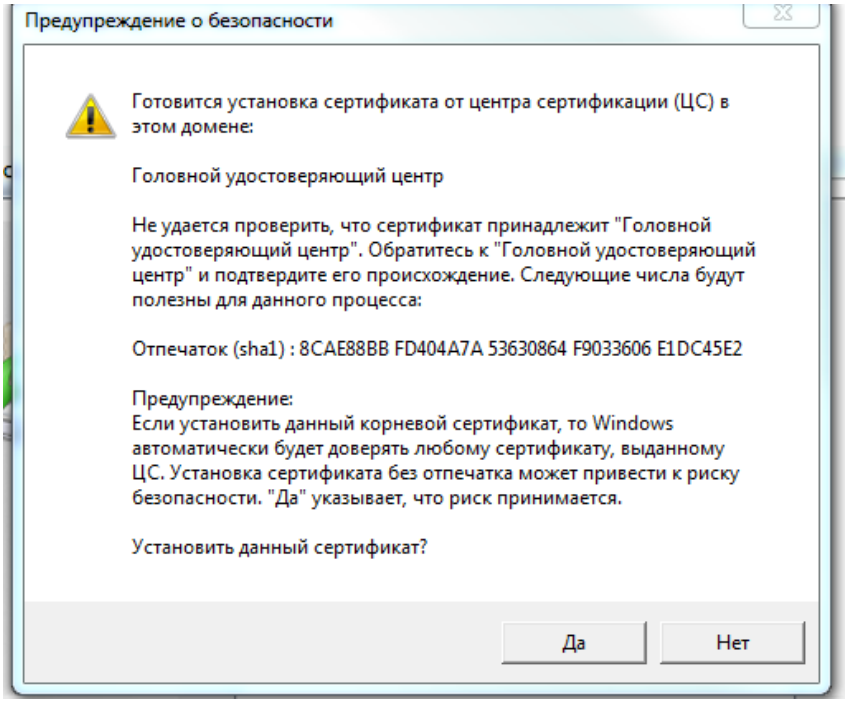

Рисунок 37. Предупреждение о безопасности

После успешной установки сертификата отобразится соответствующее сообщение (Рисунок 38).

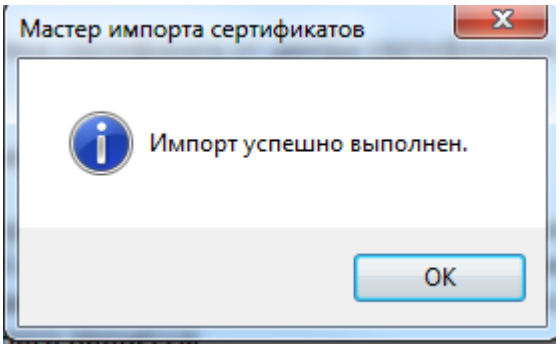

Рисунок 38. Сообщение об успешном импорте

После установки всех необходимых сертификатов вкладка «Петь сертификации» должна иметь следующий вид (Рисунок 39):

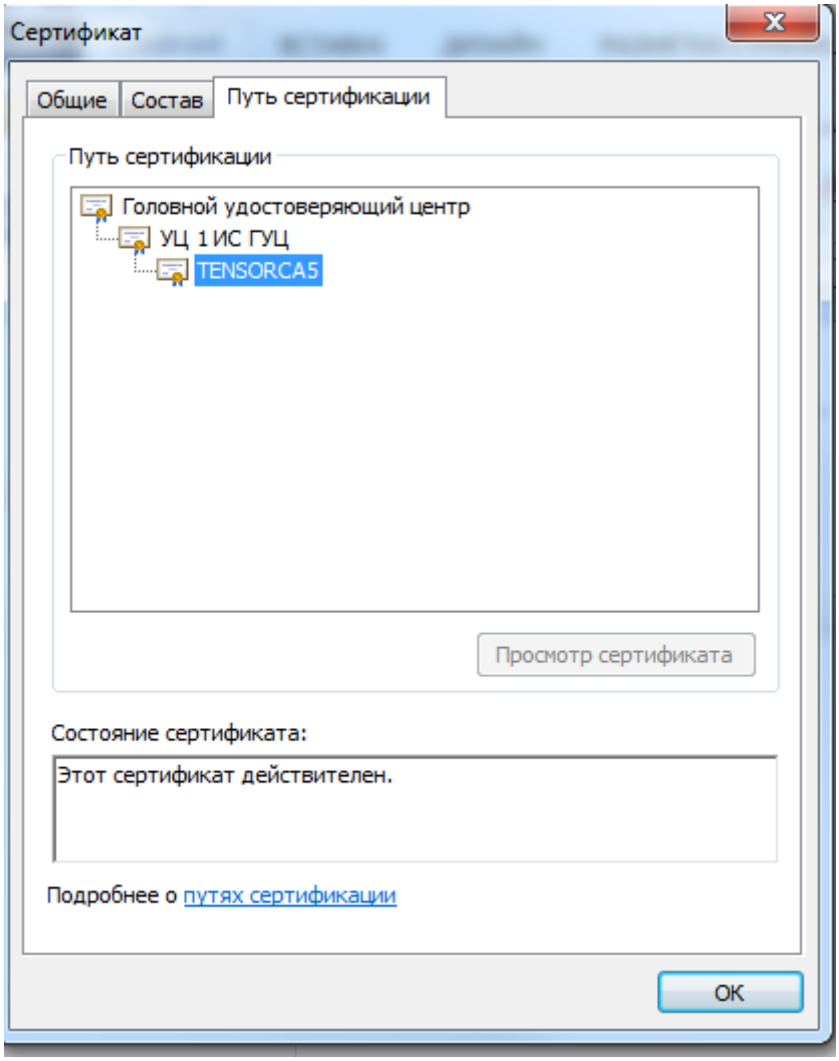

Рисунок 39. Вкладка «Путь сертификации»

2 УСТАНОВКА ПЛАГИНА КРИПТОПРО ЭЦП

Скачать плагин cadesplugin.exe можно с официального сайта КриптоПро по ссылке https://www.cryptopro.ru/products/cades/downloads, раздел «КриптоПро ЭЦП Browser plug-in 2.0» или установить плагин в браузере.

2.1 Установка плагина с сайта cryptopro.ru

Скачать плагин можно с сайта https://www.cryptopro.ru/products/cades/downloads (Рисунок 40), скачивание доступно только для авторизованных пользователей.

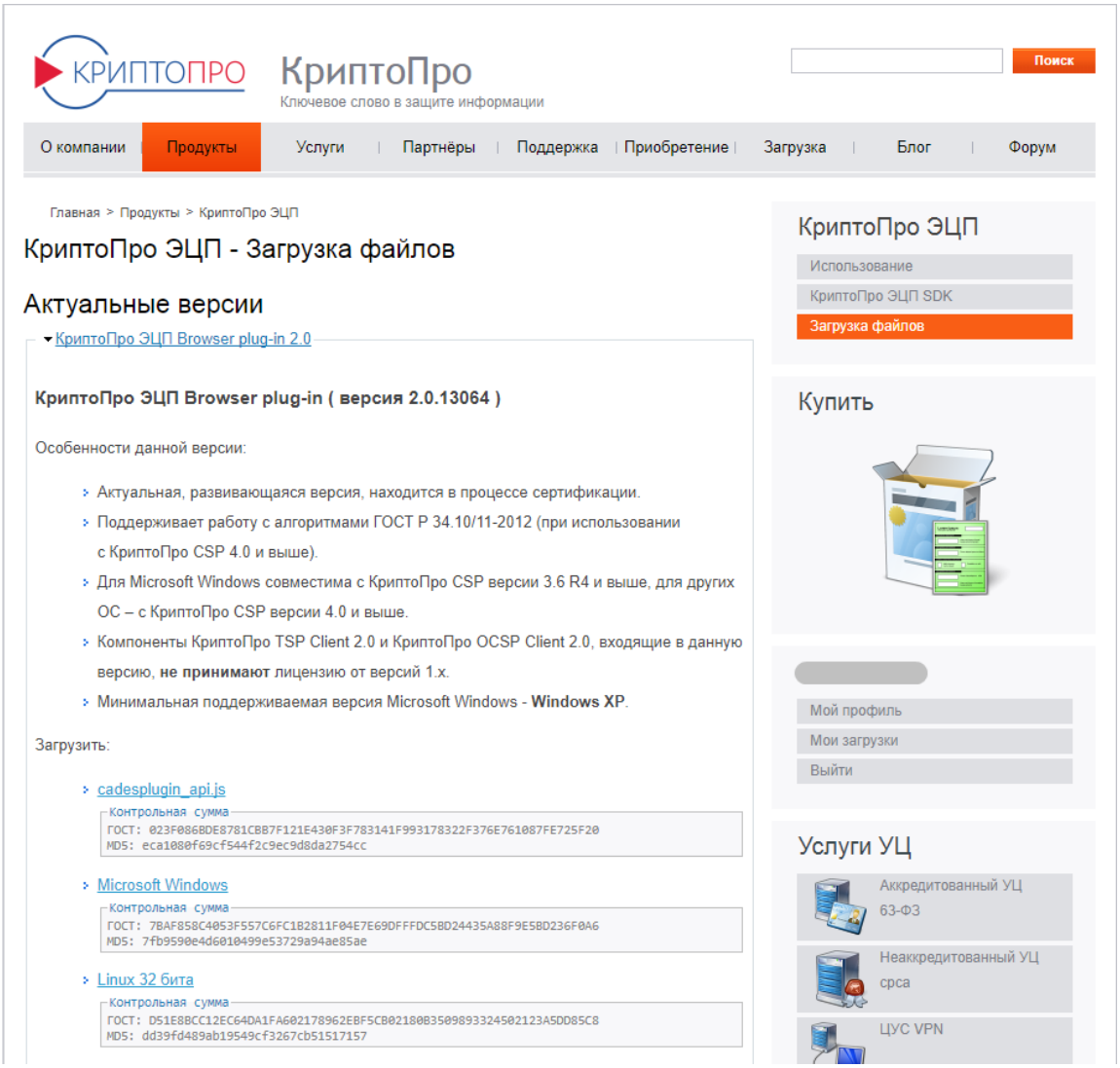

Рисунок 40. Сайт cryptopro.ru

После скачивания плагина cadesplugin.exe его необходимо установить на компьютер средствами Windows.

2.2 Установка плагина для браузера Chrome

Для того чтобы установить плагин для браузера, следует зайти в интернет магазин Chrome https://chrome.google.com/webstore/category/extensions. В поле поиска ввести «CryptoPro Extension for CAdES Browser Plug-in» и нажать клавишу «Enter» на клавиатуре.

В результате будет найдено расширение (Рисунок 41). Далее следует нажать кнопку «Установить».

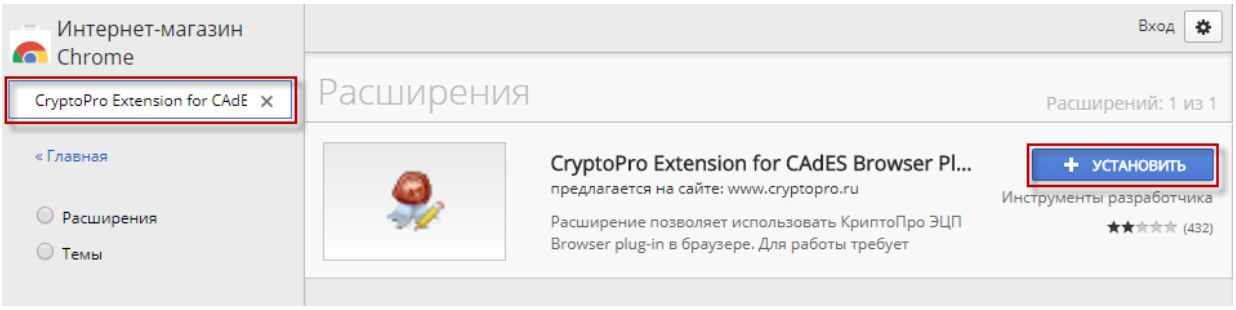

Рисунок 41. Установка расширения CryptoPro Extension for CAdES Browser Plug-in

Расширение для браузера Chrome будет установлено (Рисунок 42).

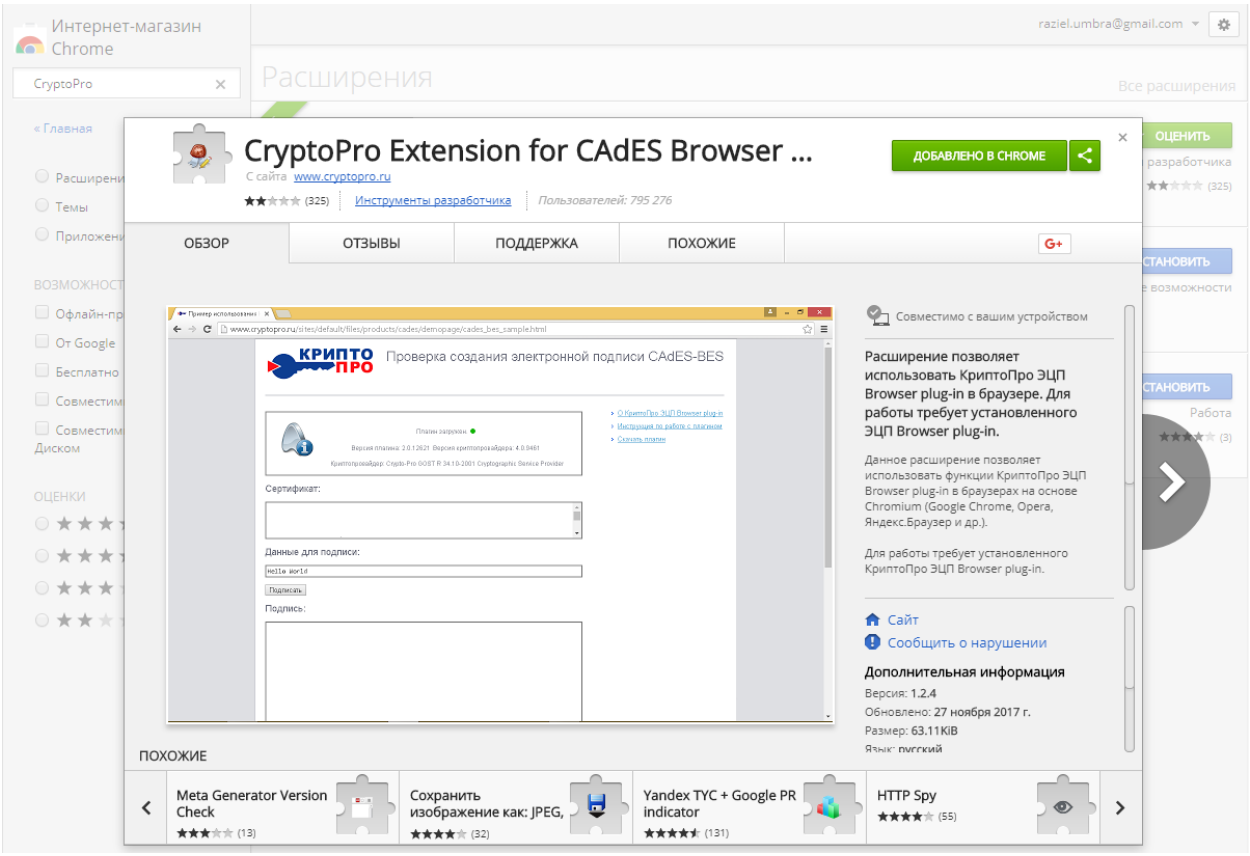

Рисунок 42. Расширение для Chrome установлено

2.3 Установка плагина для браузера Firefox

Для того чтобы установить плагин для браузера Firefox, следует зайти на сайт КриптоПро https://www.cryptopro.ru/products/cades/downloads (Рисунок 43). Сайт доступен только для авторизованных пользователей.

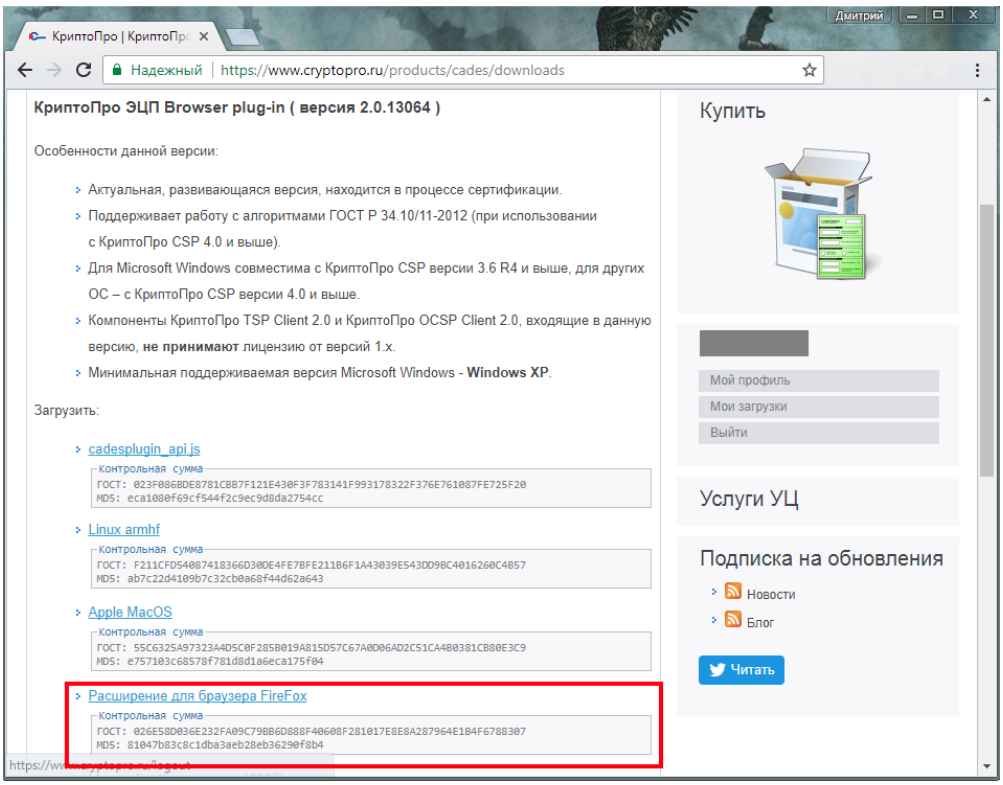

Рисунок 43. Сайт КриптоПро

Далее следует скачать расширение для браузера FireFox (файл firefox_cryptopro_extension_latest.xpi). Далее следует установить расширение, зайдя в «Дополнения» в браузере FireFox или нажав комбинацию клавиш Ctrl+Shift+A. Откроется страница с дополнениями (Рисунок 44).

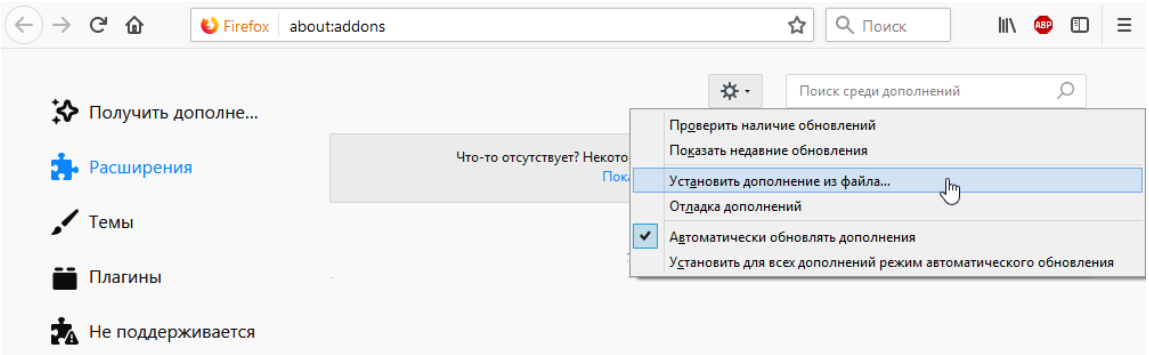

Рисунок 44. Страница дополнений браузера FireFox

Далее следует нажать кнопку «Инструменты для всех дополнений»  , затем выбрать «Установить дополнение из файла». Далее следует выбрать файл с дополнением, скачанный с сайта КриптоПро.

2.4 Установка плагина для браузера Opera

Для того чтобы установить плагин для браузера Opera, следует зайти в меню Opera, затем выбрать «Расширения» – «Загрузить расширения» (Рисунок 45).

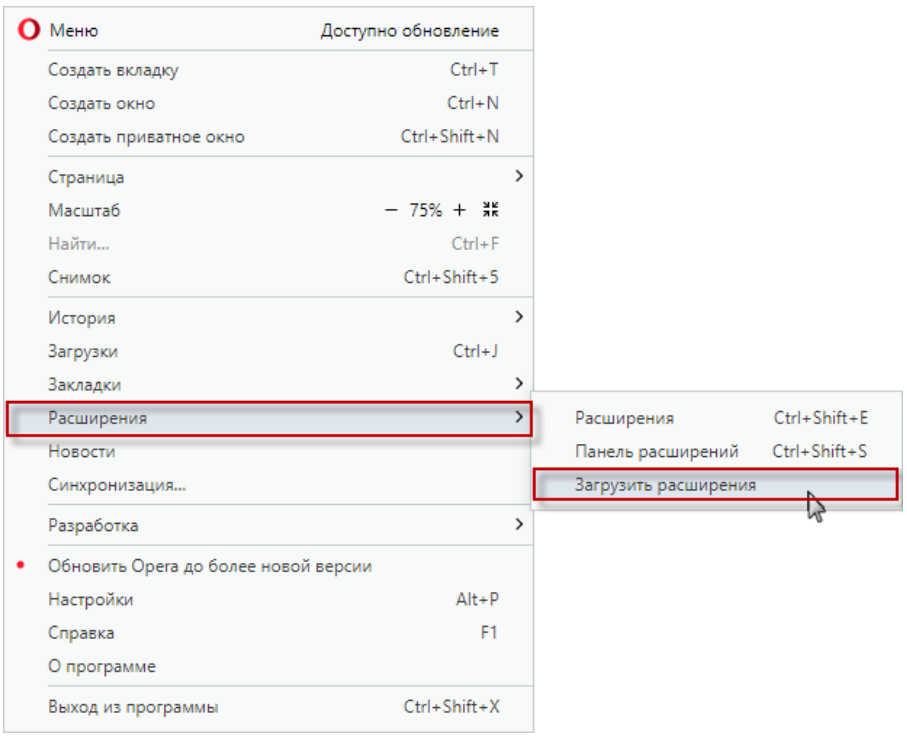

Рисунок 45. Меню браузера Opera

Откроется страница для установки дополнений браузера Opera (Рисунок 46). В поле поиска ввести «cades», затем в выпадающем списке выбрать «CryptoPro Extension for...».

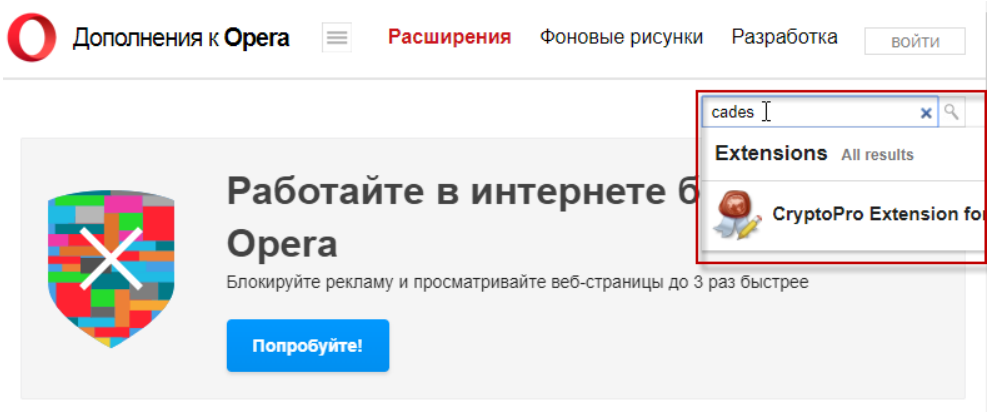

Рисунок 46. Страница дополнений браузера Opera

Затем нажать кнопку «Добавить в Opera» (Рисунок 47). Расширение установится.

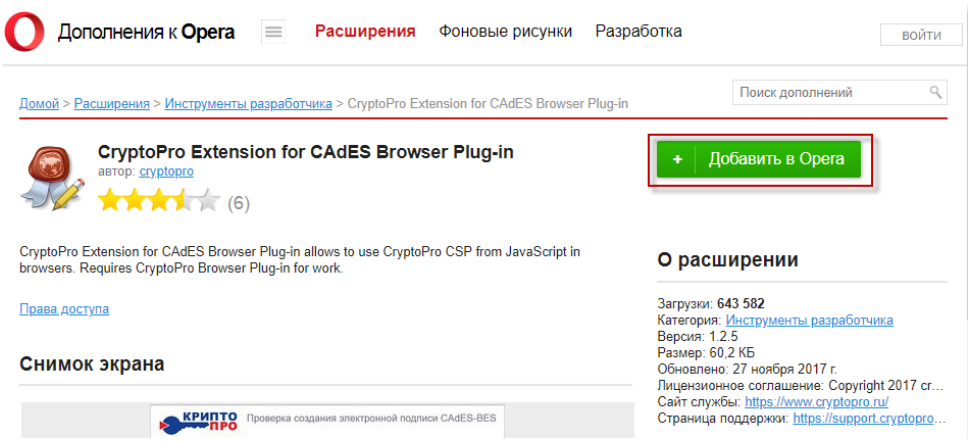

Рисунок 47. Установка расширения CryptoPro Extension for CAdES Browser Plug-in

3 НАСТРОЙКА СИСТЕМЫ

Для настройки Системы необходимо авторизоваться в системе под пользователем, для которого будут выставляться настройки.

После авторизации необходимо нажать «Настройки» в правом верхнем углу страницы (Рисунок 48).

Рисунок 48. Раздел «Настройки»

После чего откроется окно «Пользовательские настройки» (Рисунок 49), в котором необходимо установить настройку «Режим подписи файлов для РЛДД».

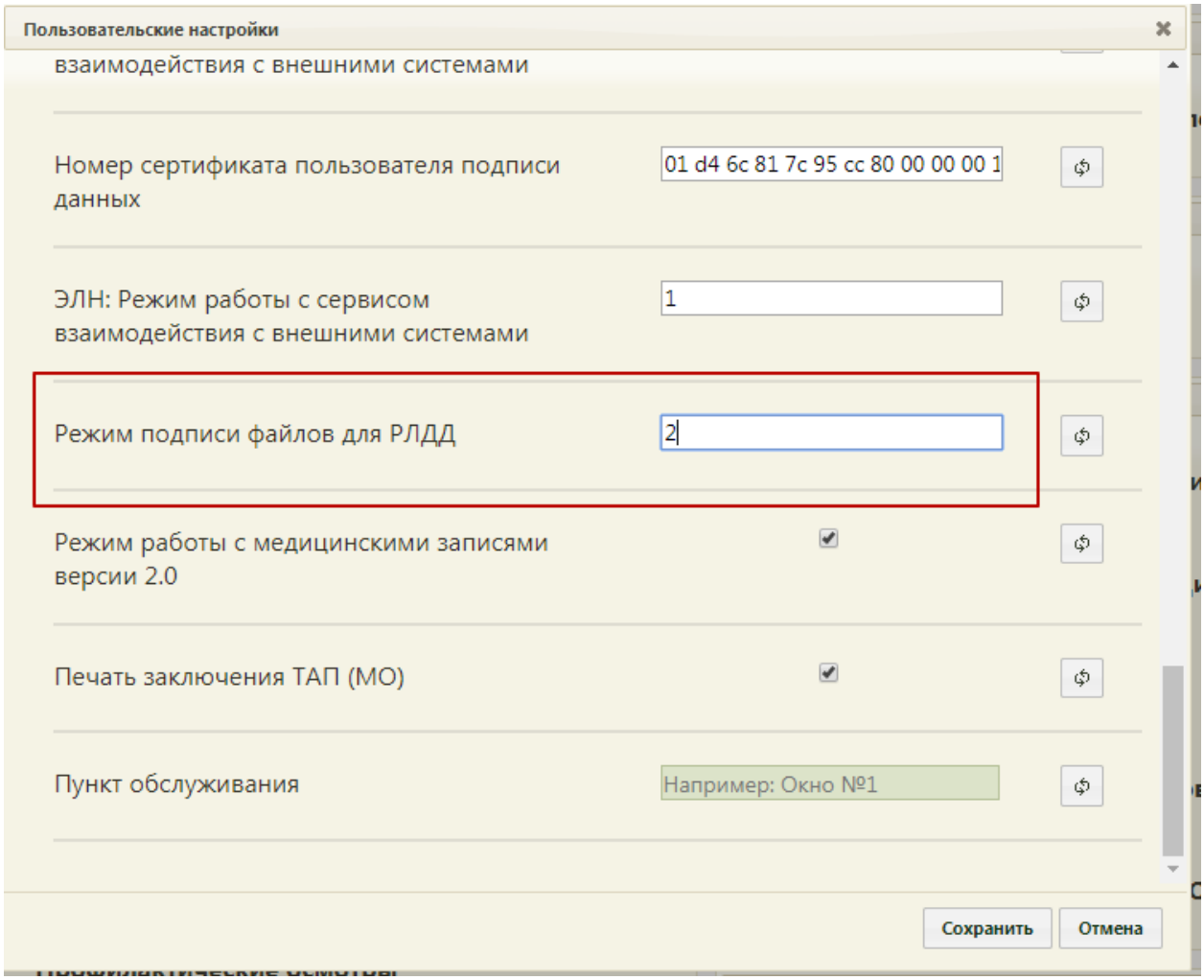

Рисунок 49. Указанием режима подписи файлов для РЛДД