Инструкция по настройке формирования ЭЦП для работы в программном комплексе «ТрастМед»

На 56 листах

2021 г.

Оглавление

1 НАСТРОЙКА ФОРМИРОВАНИЯ ЭЦП

1.1 Настройка серверной части

Сервис подписи используется для формирования ЭЦП медицинской организации. На компьютере, на котором планируется установить сервис подписи, должен быть установлен .NET Framework 4.5.2 или выше (версия 4.5.2 не работает на всех версиях ОС, в этом случае следует установить последнюю версию), а также компонент ASP.NET (например, не подойдёт операционная система Windows 7 Home Basic, Windows RT).

1.1.1 Настройка сервера IIS

Далее следует настроить сервер IIS. Для этого необходимо зайти в «Панель управления» → «Программы» → «Включение или отключение компонентов Windows» (Рисунок 1).

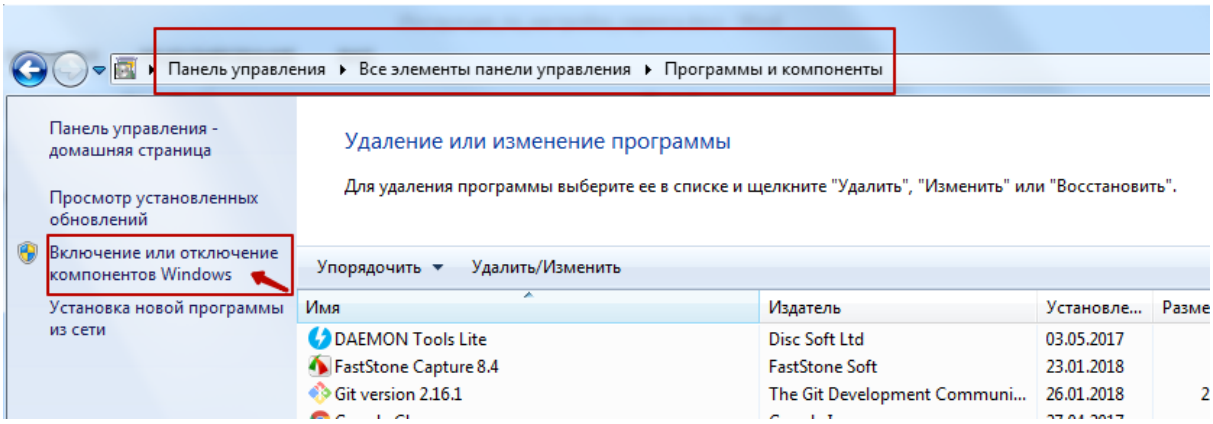

Рисунок 1. Окно «Программы и компоненты»

Далее следует установить флажки: .NET Framework 4 или выше и ASP.NET 4 или выше (Рисунок 2).

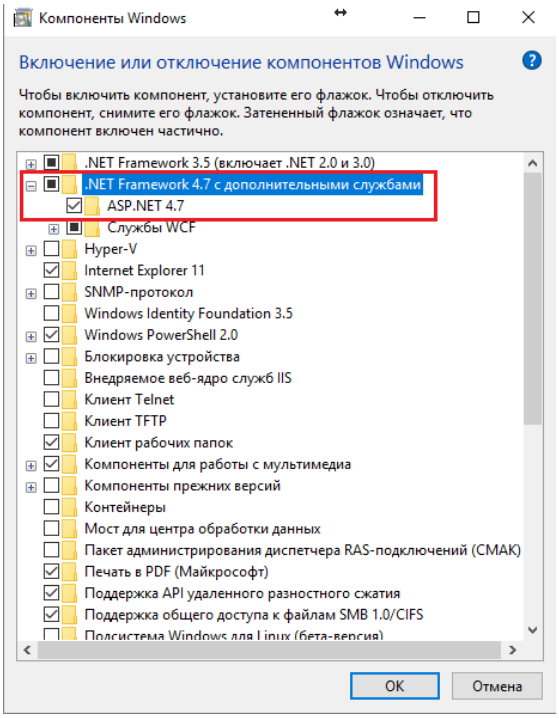

Рисунок 2. Окно «Компоненты Windows»

Далее в этом же окне следует установить службы IIS, как показано на Рисунок 3 (Службы IIS →Службы интернета →Компоненты разработки приложений →ASP.NET 4 или выше).

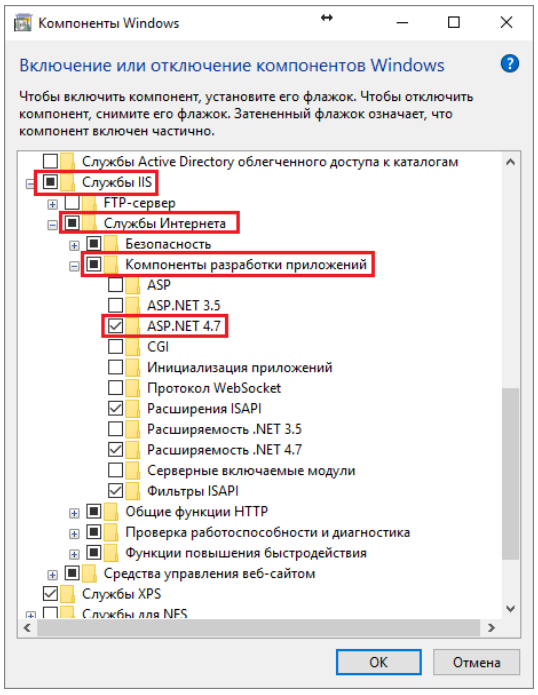

Рисунок 3. Окно «Компоненты Windows». Службы IIS

Затем установить флажок Службы IIS → Средства управления веб-сайтом → Консоль управления веб-сайтом (в случае если автоматически не выбралось) (Рисунок 4).

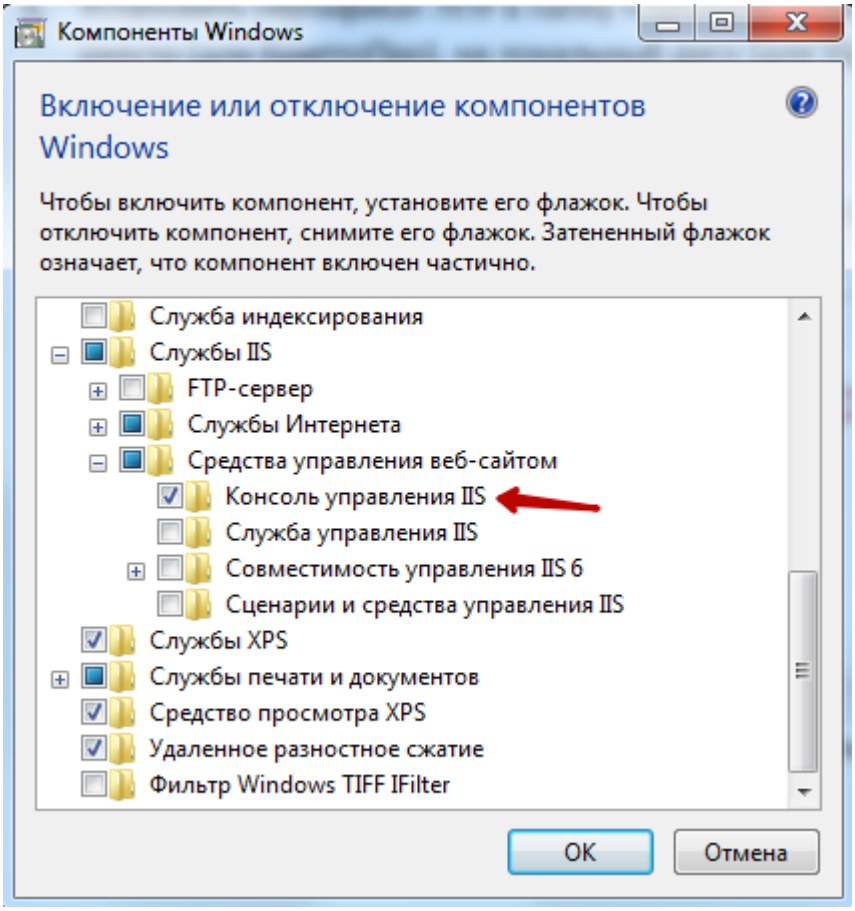

Рисунок 4. Окно «Компоненты Windows». Службы IIS

1.1.2 Установка криптопровайдера

На выделенном сервере ЛПУ под управлением ОС Windows установить КриптоПро CSP версии 3.6 или выше или VipNet CSP версии 4.2 или 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).

1.1.3 Установка сертификата ЛПУ в хранилище текущего пользователя

Рассмотрим установку сертификата ЛПУ на примере программы КриптоПро CSP. Перед установкой сертификата следует вставить флешку с ключом в компьютер.

После установки КриптоПро CSP следует нажать левой кнопкой мыши по установленной программе КриптоПро CSP. Программа может располагаться в Пуске, на рабочем столе (если была установлена иконка), или ее можно найти поиском, нажав win+F.

В открывшемся окне (Рисунок 5) следует перейти на вкладку «Сервис», далее нажать кнопку «Скопировать»

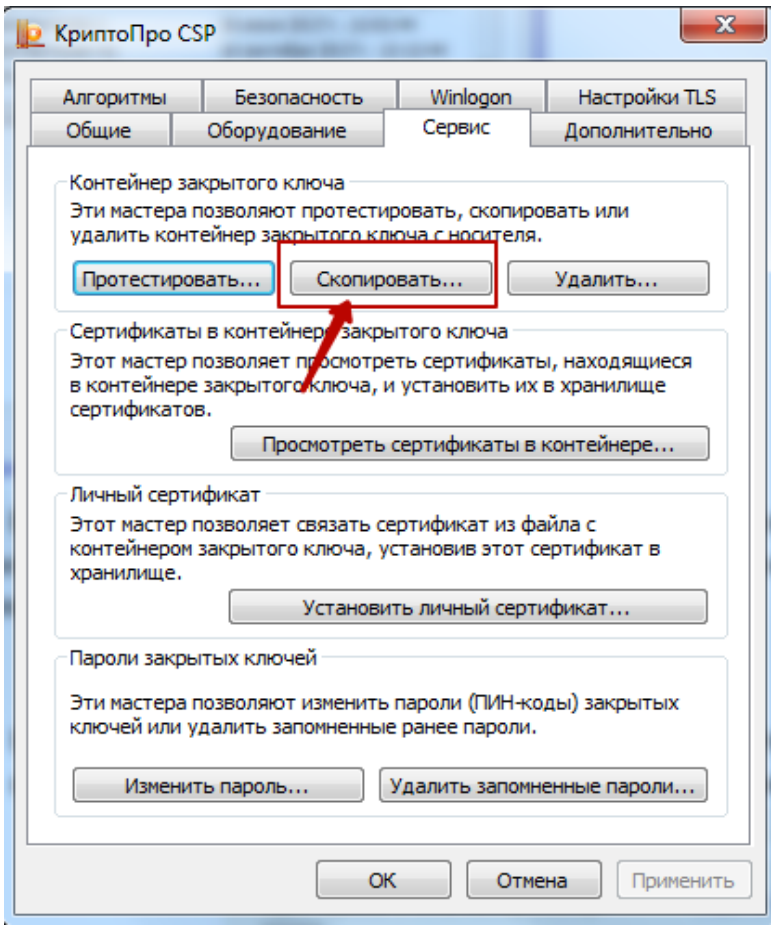

Рисунок 5. Копирование контейнера в реестр на компьютер

В результате откроется окно (Рисунок 6), в котором необходимо указать имя ключевого контейнера.

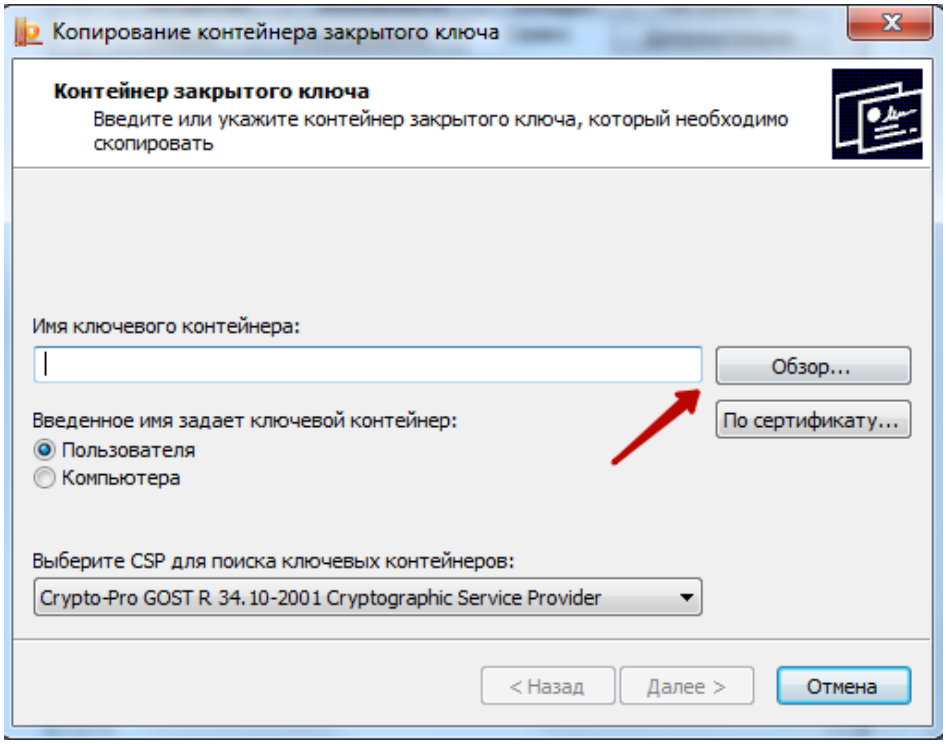

Рисунок 6. Окно ввода имени ключевого контейнера

Для того чтобы ввести имя контейнера следует нажать кнопку «Обзор». В результате откроется окно выбора контейнера (Рисунок 7).

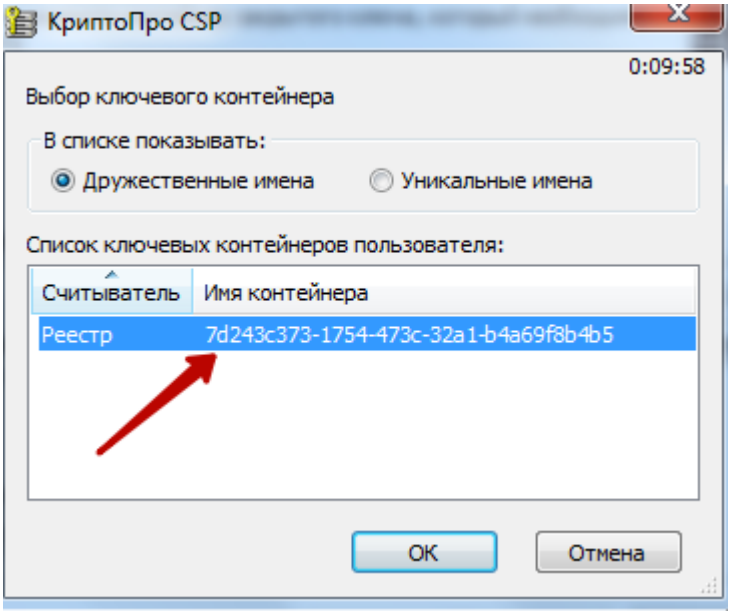

Рисунок 7. Выбор ключевого контейнера

В данном окне необходимо выбрать имя реестра и нажать кнопку «ОК». В результате заполнится поле «Имя ключевого контейнера» (Рисунок 8).

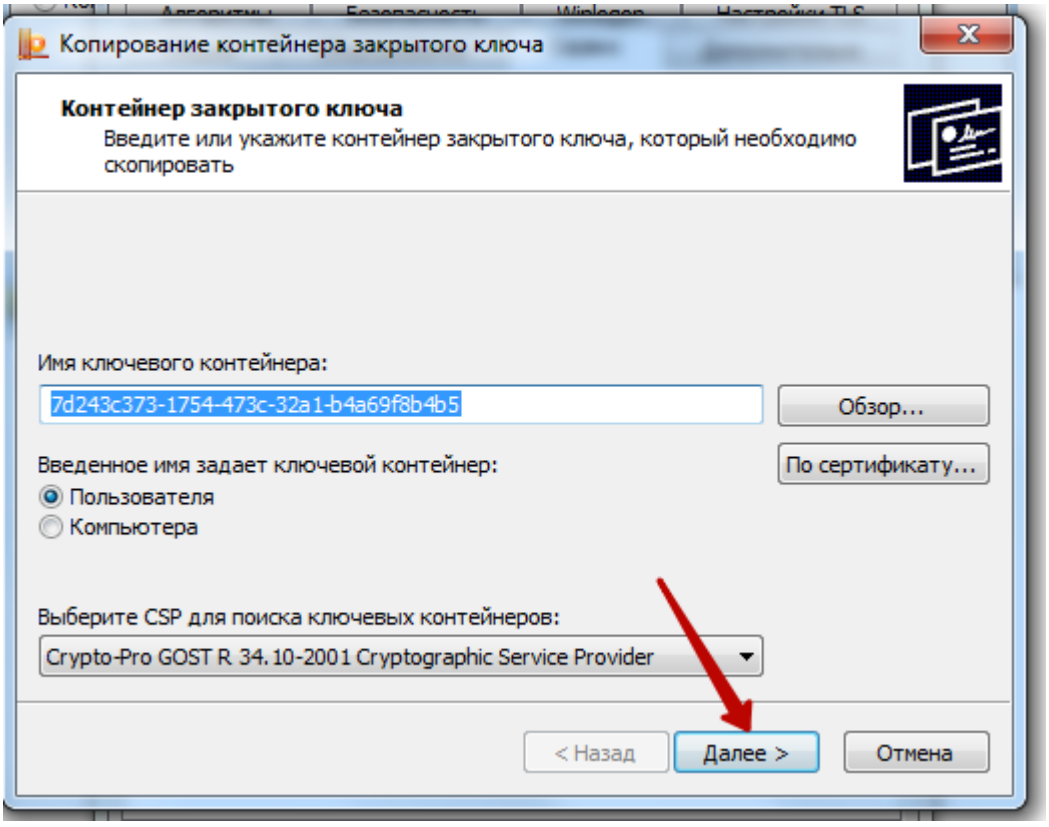

Рисунок 8. Заполнено поле «Имя ключевого контейнера»

После того как имя задано следует нажать кнопку «Далее». В результате отроется окно (Рисунок 9), в котором необходимо указать имя для создаваемого ключевого контейнера.

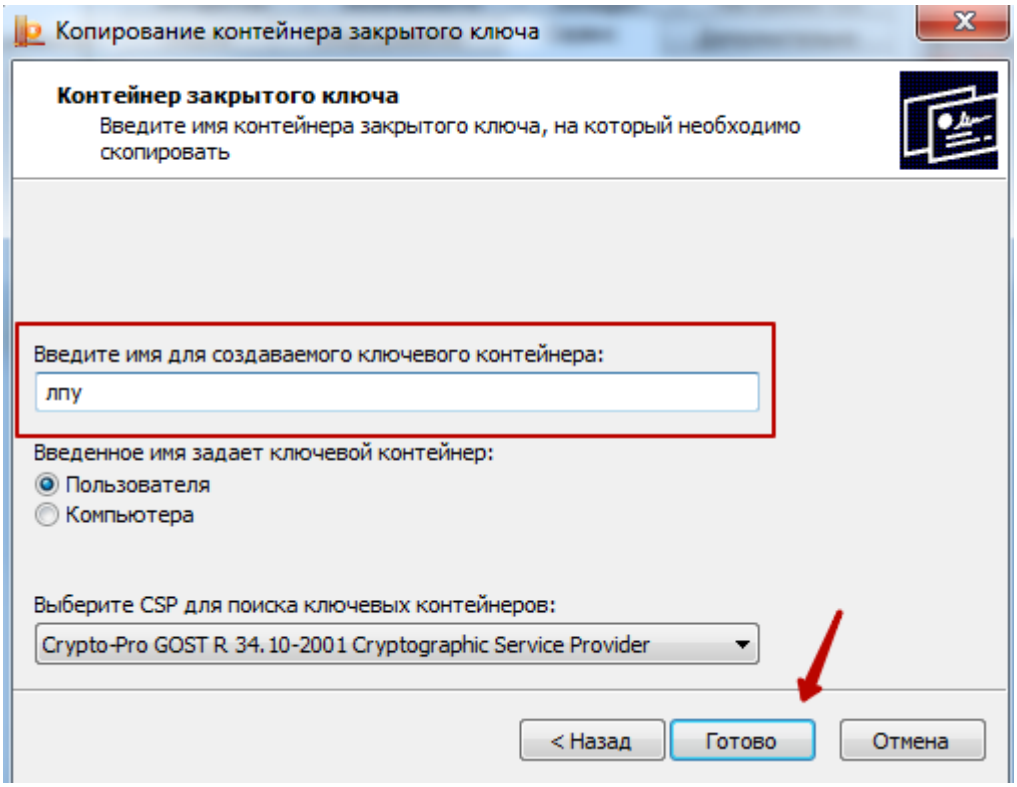

Рисунок 9. Заполнение поля «Введите имя для создаваемого ключевого контейнера

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 10), в котором необходимо выбрать носитель для хранения контейнера закрытого ключа.

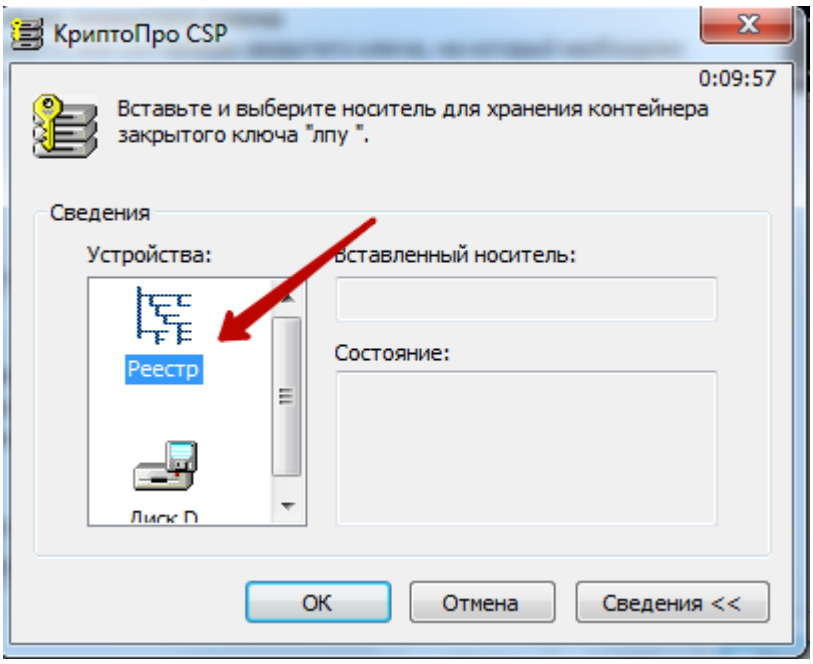

Рисунок 10. Выбор носитель для хранения контейнера

В данном окне следует выбрать устройство. В данном случае, в качестве устройства следует выбрать «Реестр» и нажать кнопку «ОК». После чего откроется окно (Рисунок 11), в котором необходимо задать пароль для создаваемого контейнера.

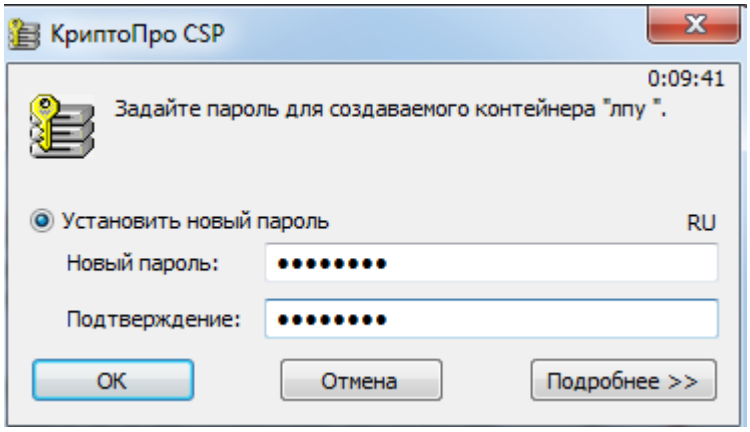

Рисунок 11. Окно задания пароля для контейнера

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.

1.1.4 Установка сертификата ЛПУ из контейнера в реестре на компьютере

Для установки сертификата следует на вкладке «Сервис» нажать кнопку «Просмотреть сертификаты в контейнере» (Рисунок 12).

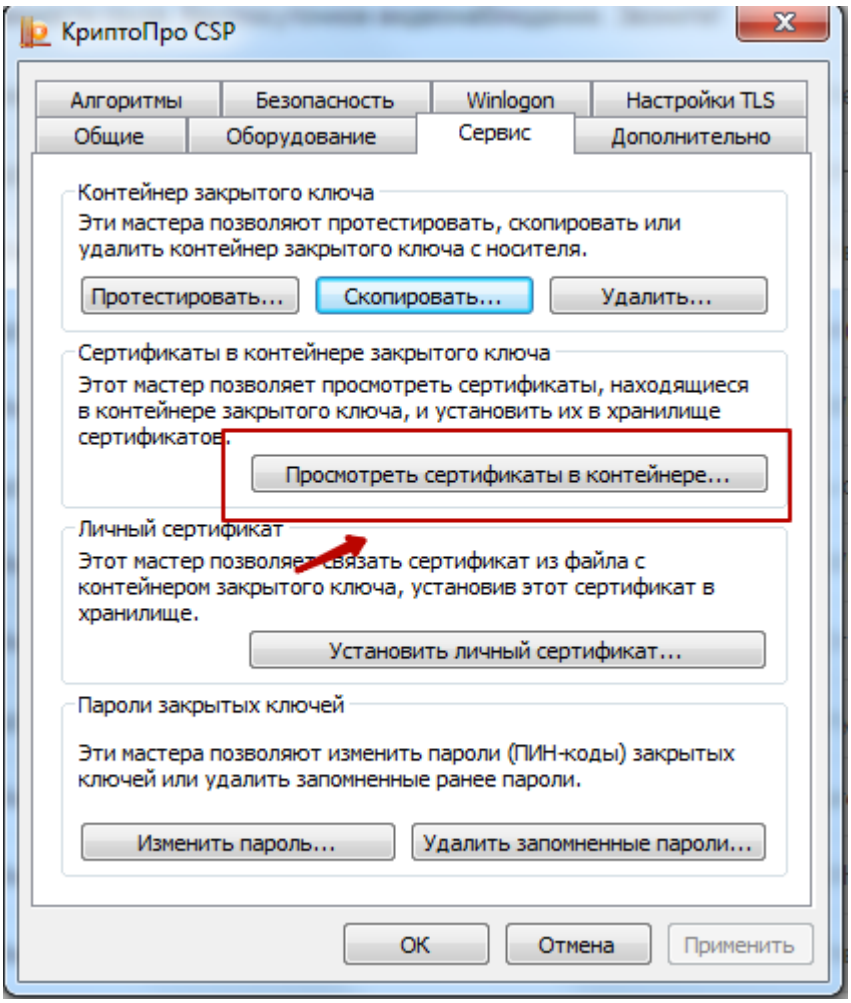

Рисунок 12. Окно «КриптоПро CSP», вкладка «Сервис»

В результате откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 13).

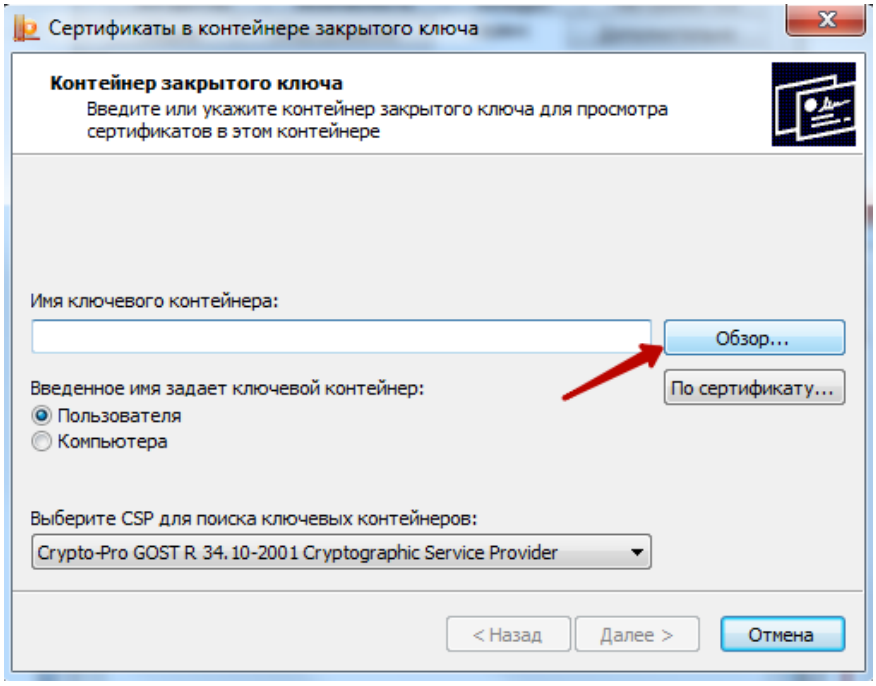

Рисунок 13. Окно «Сертификаты закрытого ключа»

В данном окне следует установить имя ключевого контейнера, нажав кнопку «Обзор». В результате откроется окно выбора ключевого контейнера (Рисунок 14).

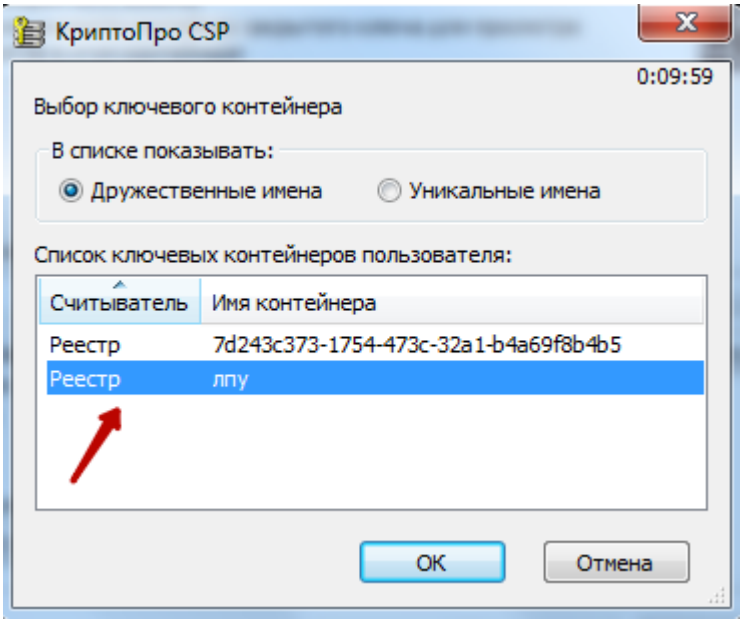

Рисунок 14. Окно выбора ключевого контейнера»

В открывшемся окне следует выбрать имя контейнер, который был создан, и нажать кнопку «ОК». В результате имя ключевого контейнера будет задано (Рисунок 15).

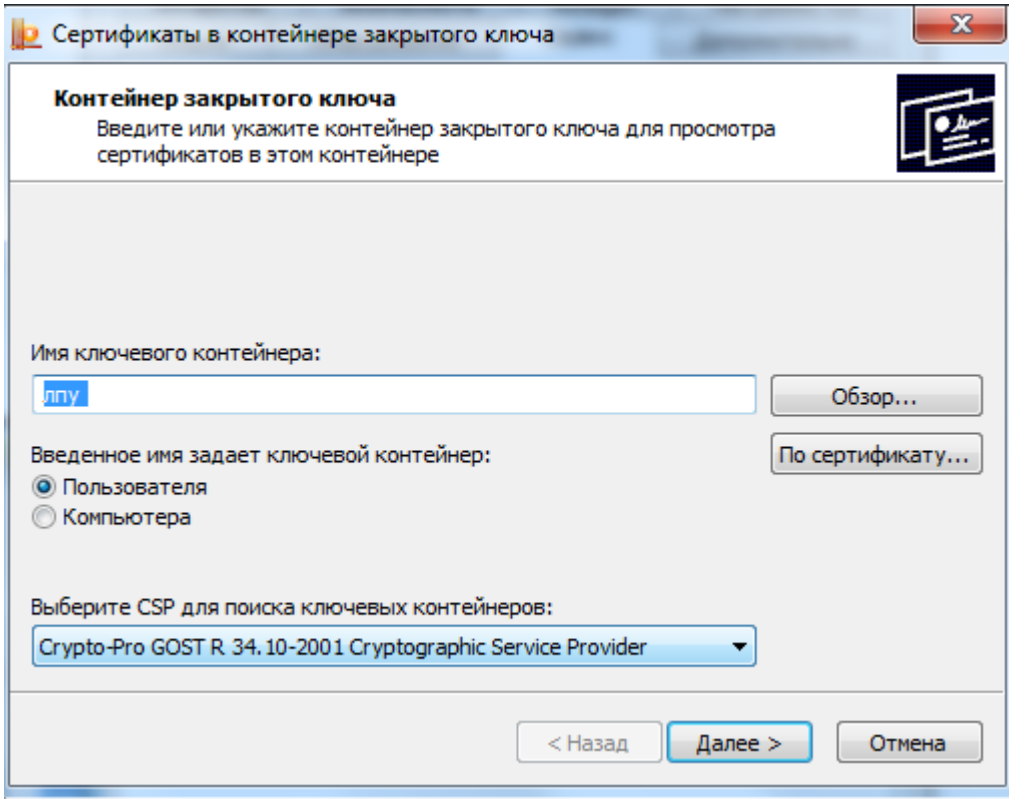

Рисунок 15. Установлено имя ключевого контейнера

Для продолжения следует нажать кнопку «Далее». В результате откроется окно для просмотра сертификата (Рисунок 16).

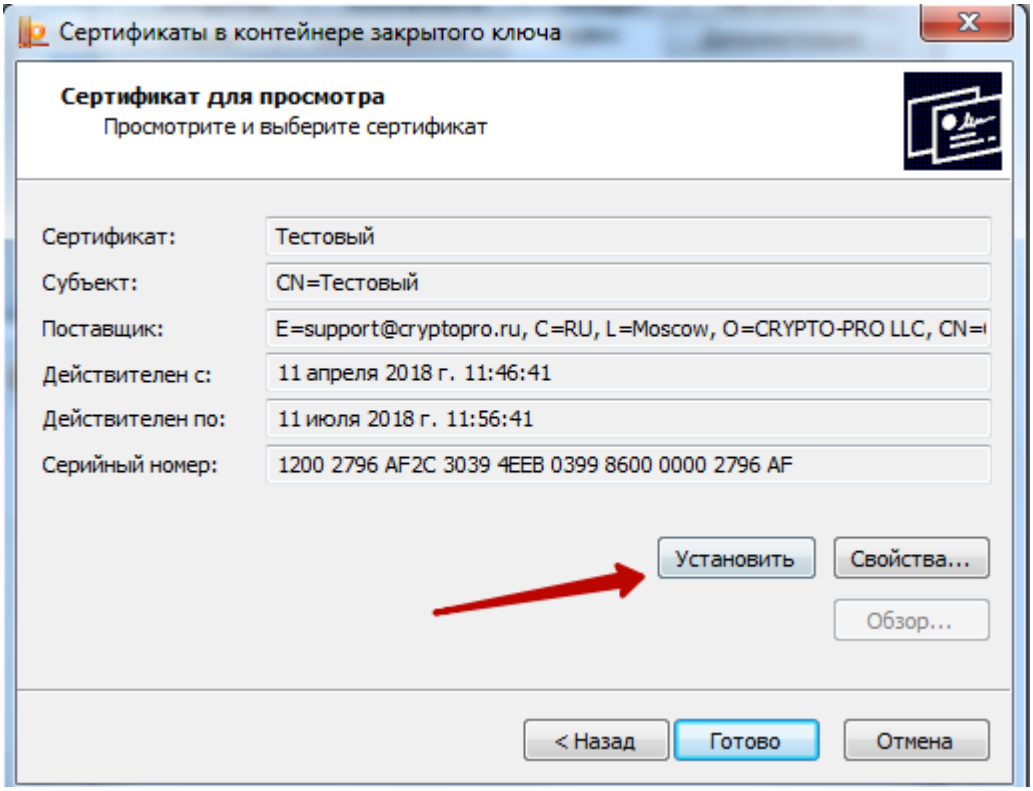

Рисунок 16. Окно просмотра сертификата

Для установки сертификата следует нажать кнопку «Установить». После чего откроется окно (Рисунок 17) с сообщением, что в хранилище уже присутствует сертификат. Следует заметить существующий сертификат новым, нажав кнопку «Да».

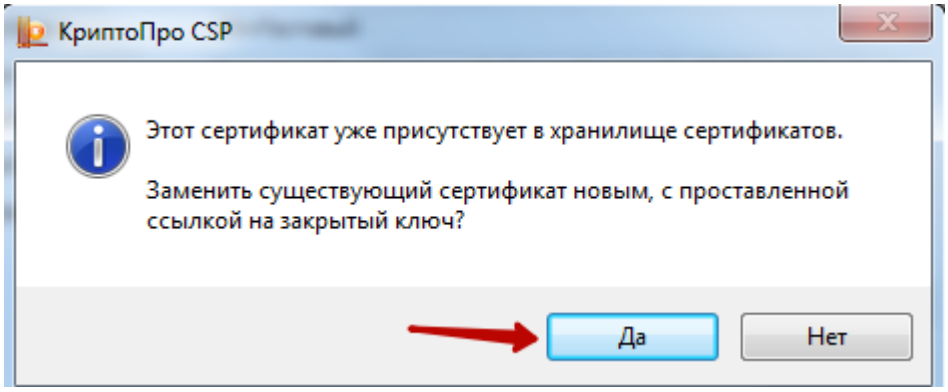

Рисунок 17. Диалоговое окно о замене существующего сертификата

В результате сертификат установится, появится информационное окно об успешной установке (Рисунок 18).

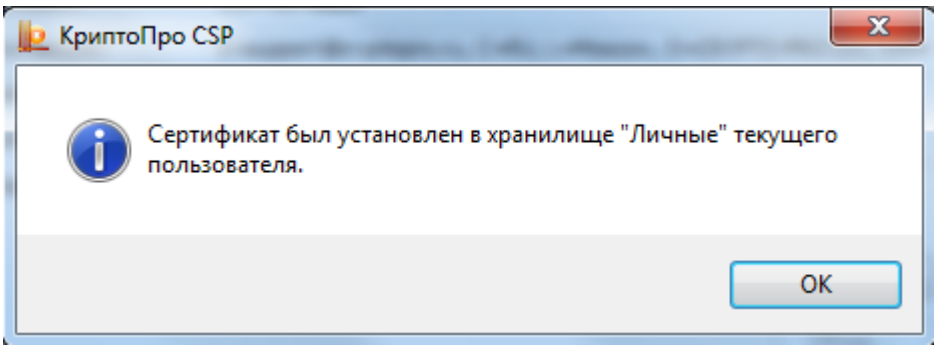

Рисунок 18. Информационное окно об успешной установке сертификата

Далее следует протестировать контейнер.

1.1.5 Тестирование контейнера ЛПУ из реестра для сохранения пароля

Для тестирования контейнера следует на вкладке «Сервис» нажать кнопку «Протестировать» (Рисунок 19).

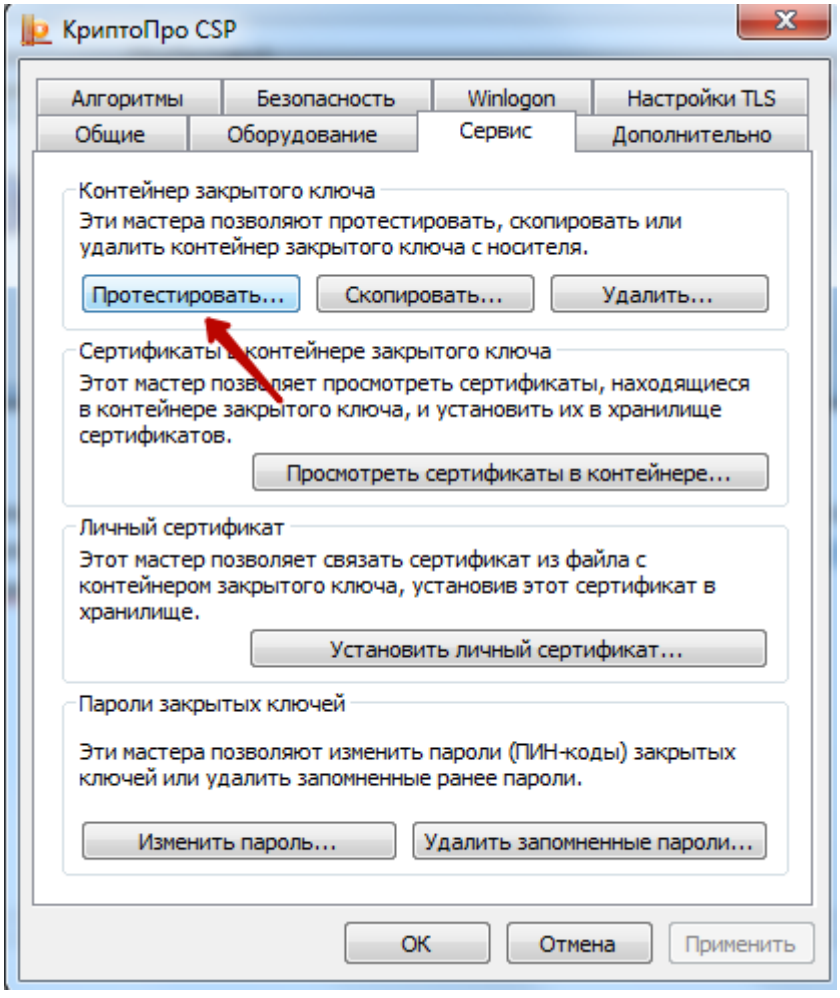

Рисунок 19. Окно «КриптоПро CSP», вкладка «Сервис»

Откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 20).

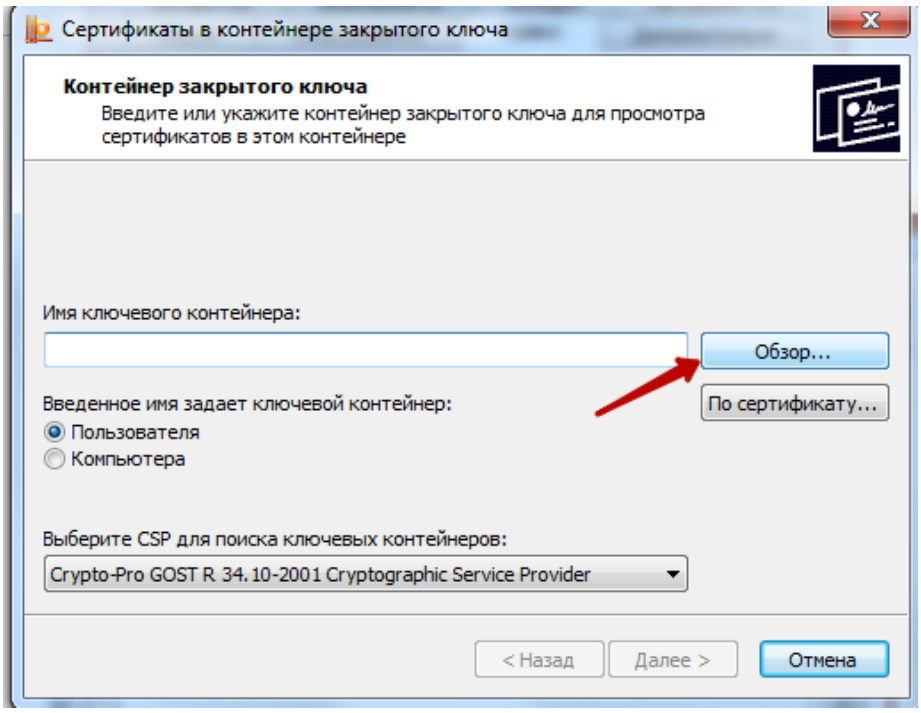

Рисунок 20. Окно «Сертификаты в контейнере закрытого ключа»

В данном окне следует нажать кнопку «Обзор» и в открывшемся окне следует выбрать созданный контейнер (Рисунок 21).

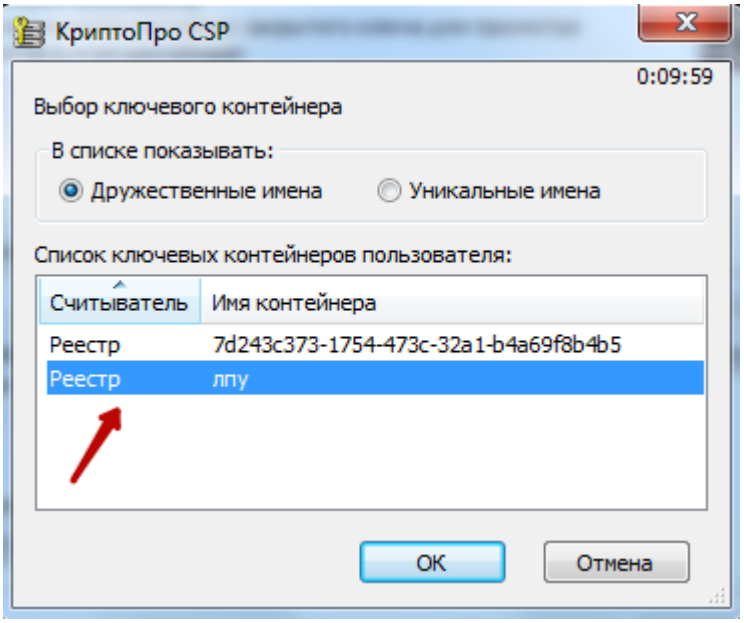

Рисунок 21. Выбор контейнера

После выбора контейнера следует нажать кнопку «ОК». В результате поле «Имя ключевого контейнера» заполнится (Рисунок 22).

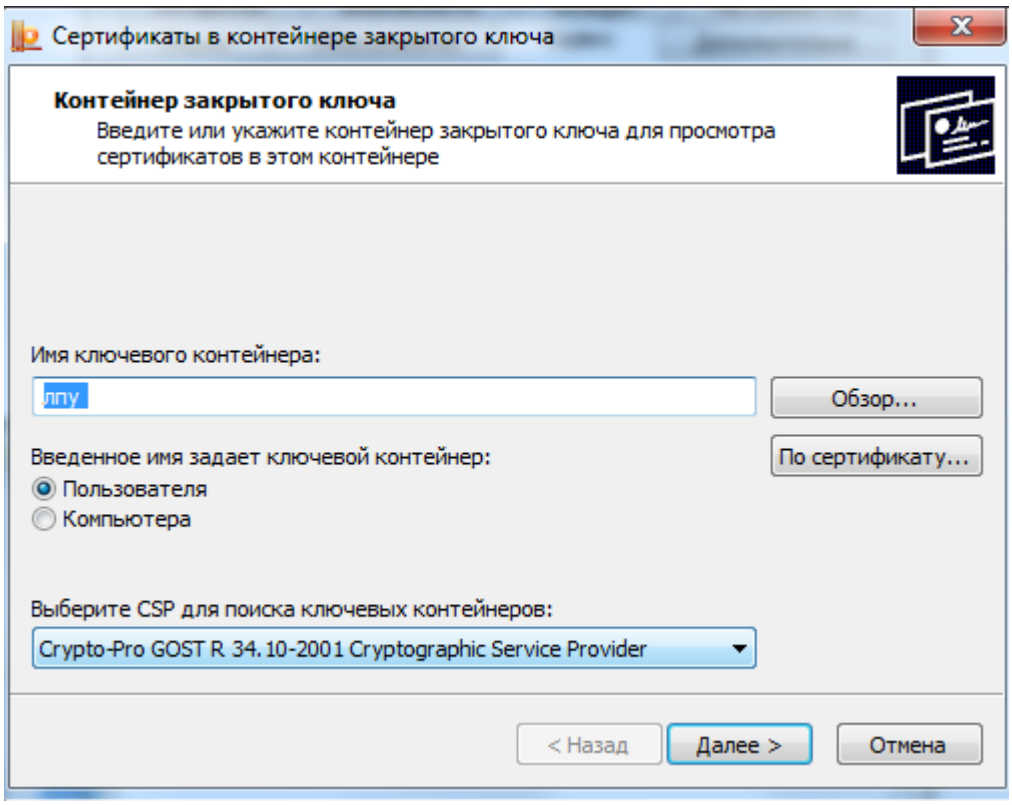

Рисунок 22. Окно «Сертификаты в контейнере закрытого ключа»

Затем следует нажать кнопку «Далее». В результате откроется окно для ввода пароля для контейнера (Рисунок 23).

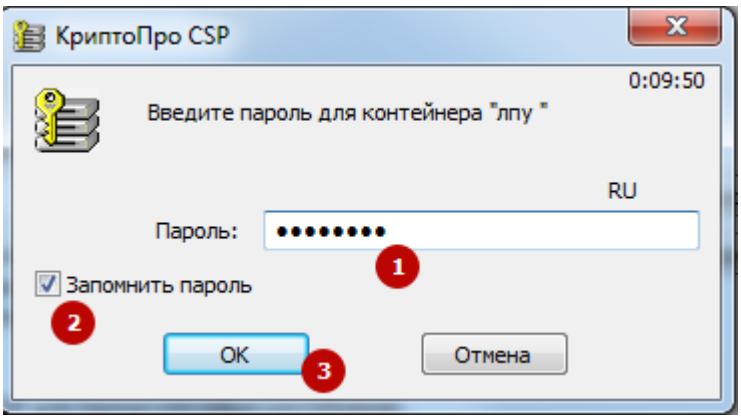

Рисунок 23. Окно ввода пароля для контейнера

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 24).

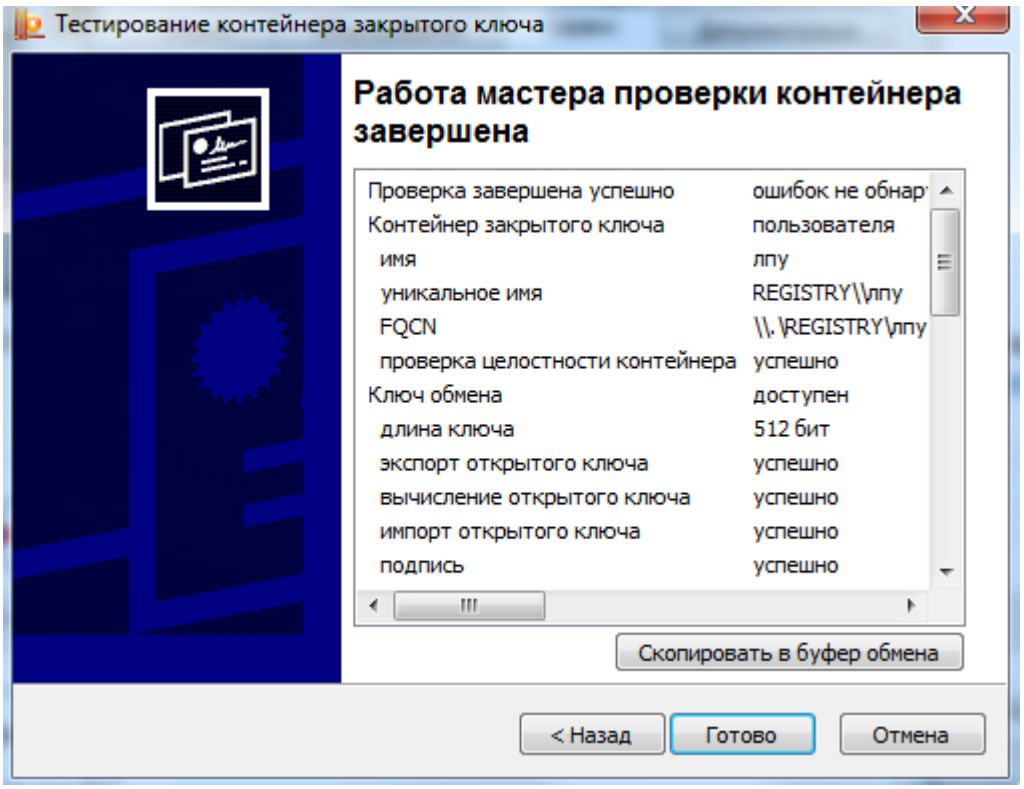

Рисунок 24. «Тестирование контейнера закрытого ключа»

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 всех сертификатов следует убедиться, что они установлены для текущего пользователя, а не для локального компьютера.

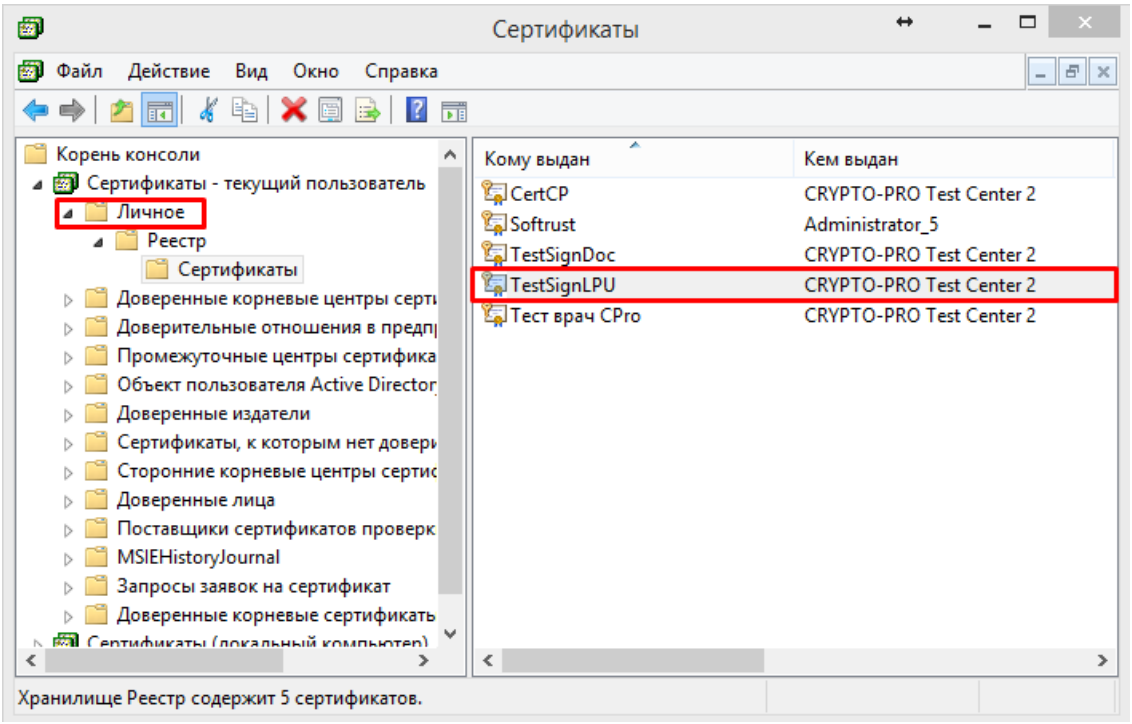

Рисунок 25. Сертификаты установлены для текущего пользователя

1.1.6 Установка Сертификата уполномоченного лица ФСС

Установка необходима только для настройки взаимодействия листков нетрудоспособности с Фондом Социального Страхования.

Сертификат уполномоченного лица необходимо скачать с сайта http://cabinets.fss.ru/eln.html (Рисунок 26).

Рисунок 26. Сайт ФСС (версия сайта на 20.09.2019)

Внимание! При скачивании сертификата может возникнуть ситуация, когда браузер отображает зашифрованный текст (Рисунок 27).

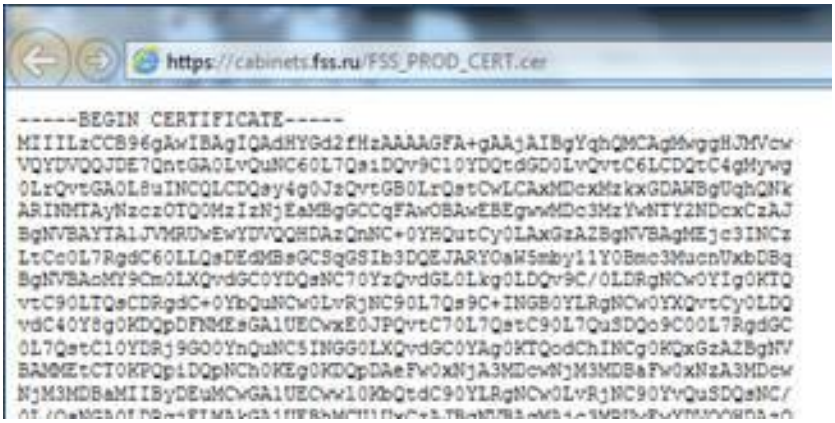

Рисунок 27. Зашифрованный текст при скачивании сертификата

Для того чтобы этого избежать, необходимо щелкнуть правой кнопкой мыши на ссылке для скачивания сертификата, и в открывшемся контекстном меню выбрать пункт «Сохранить объект как…» (Рисунок 28). Затем сохранить файл в выбранную директорию, тип сохраняемого файла должен быть с расширением .cer.

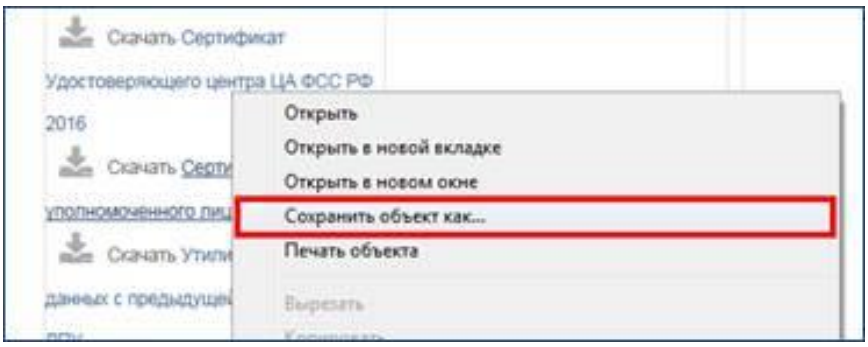

Рисунок 28. Контекстное меню при скачивании сертификата

После скачивания необходимо установить сертификат, нажав двойным щелчком мыши по скачанному файлу. В результате откроется окно «Сертификат» (Рисунок 29).

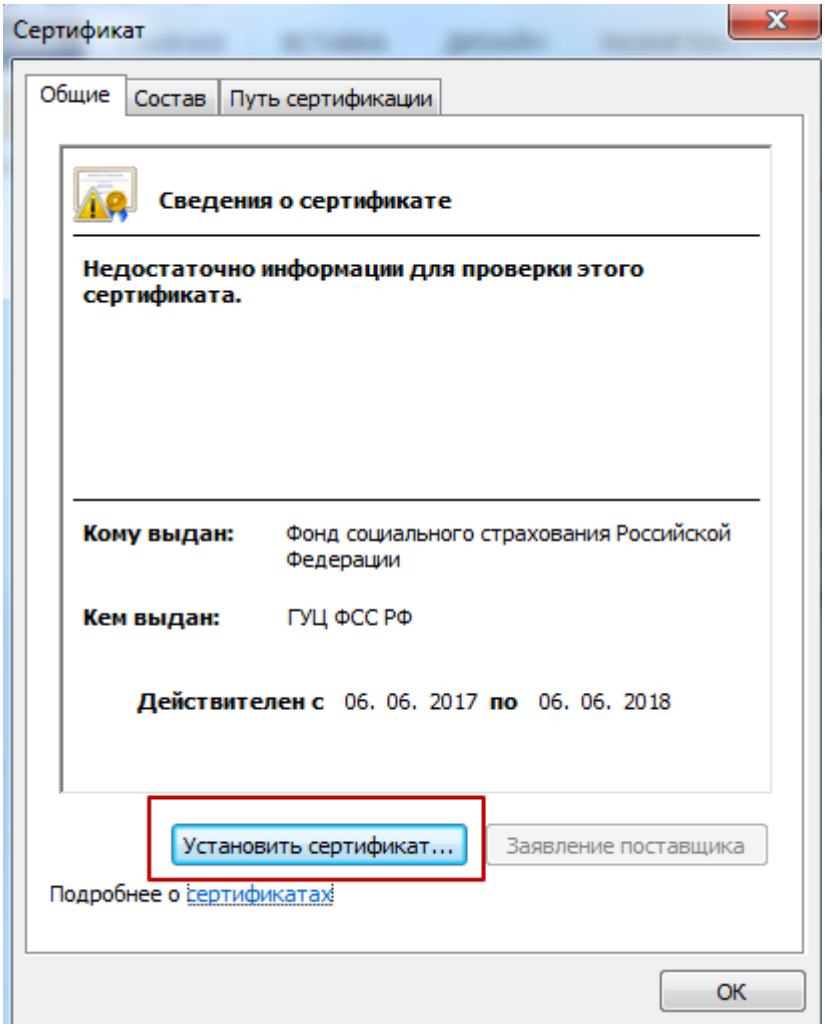

Рисунок 29. Окно установки сертификата

В окне «Сертификат» следует нажать кнопку «Установить сертификат». В результате откроется окно «Мастер импорта сертификатов» (Рисунок 30).

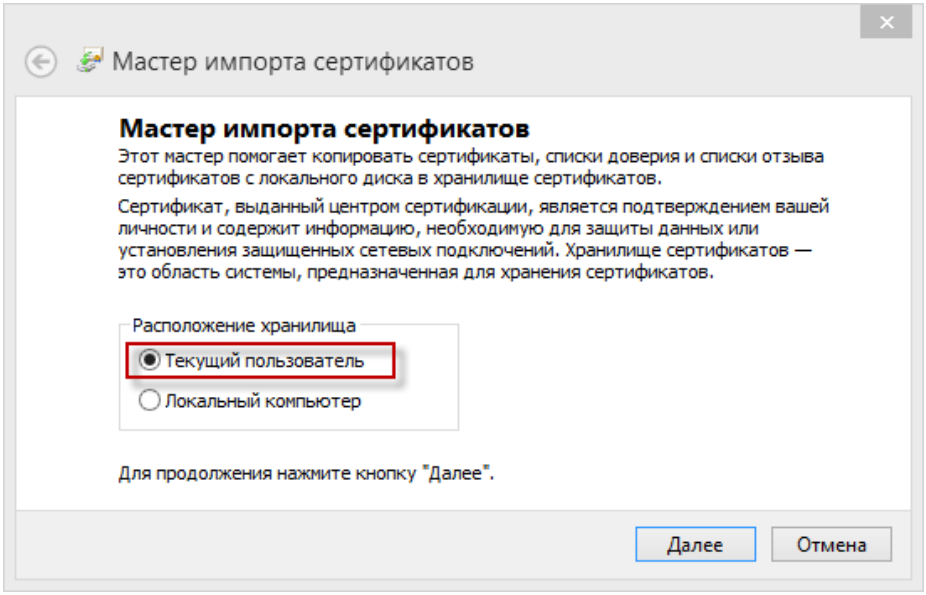

Рисунок 30. Окно «Мастер импорта сертификатов»

В данном окне необходимо установить метку «Текущий пользователь» и нажать кнопку «Далее». В результате откроется окно (Рисунок 31), в котором необходимо выбрать хранилище для установки сертификата

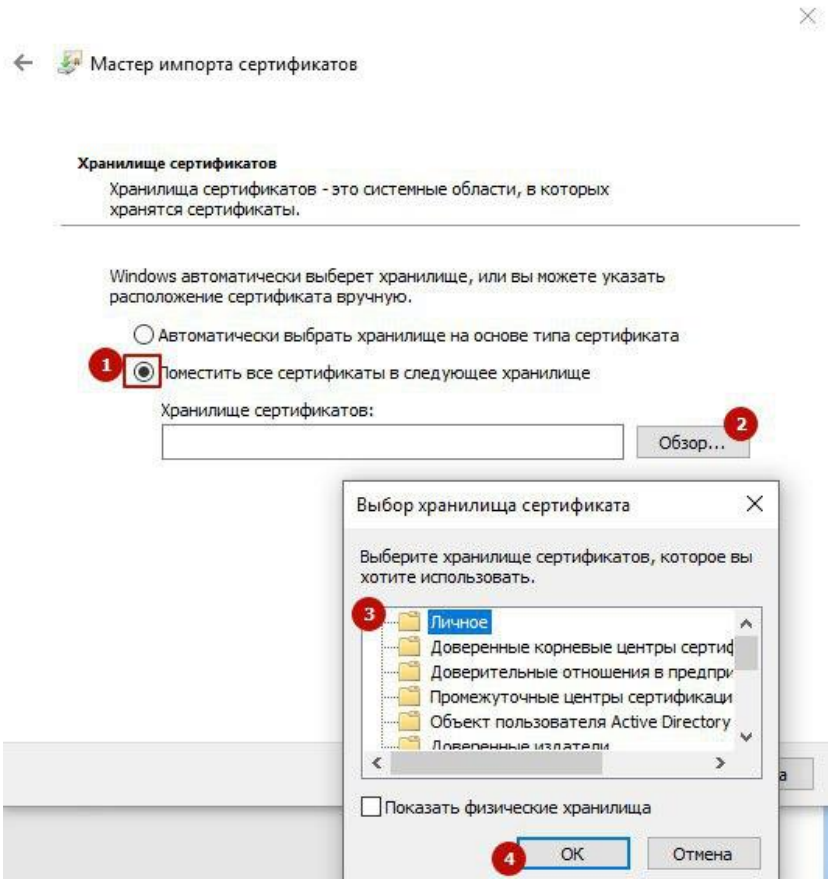

Рисунок 31. Выбор хранилища для установки сертификата

В данном окне следует установить метку «Поместить все сертификаты в следующее хранилище». Затем нажать кнопку «Обзор». В открывшемся окне следует выбрать папку «Личное» и нажать кнопку «ОК». После чего нажать кнопку «Далее». В результате откроется окно завершения установки (Рисунок 32).

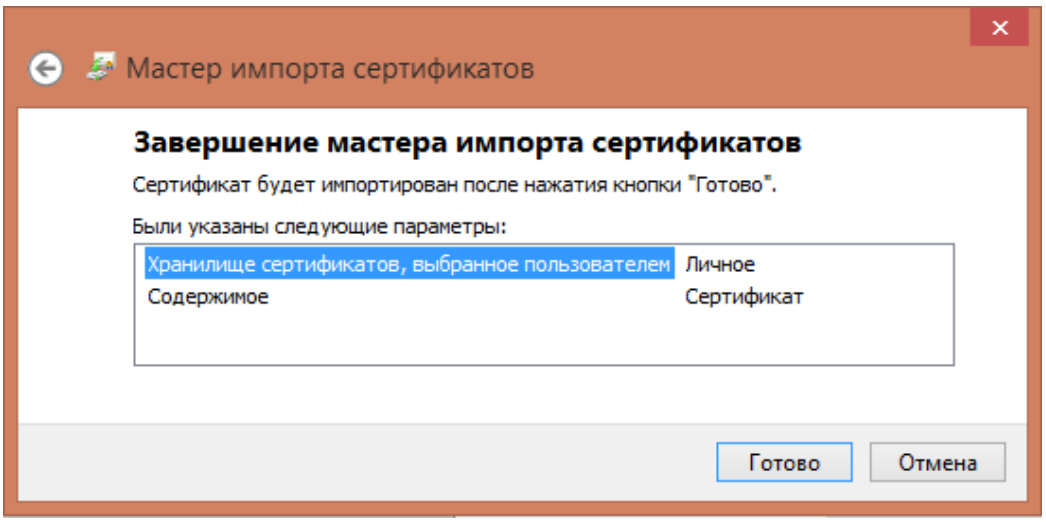

Рисунок 32. Окно завершения установки сертификата

Для завершения установки следует нажать кнопку «Готово». В результате откроется информационное окно с подтверждением успешного импорта сертификата (Рисунок 33).

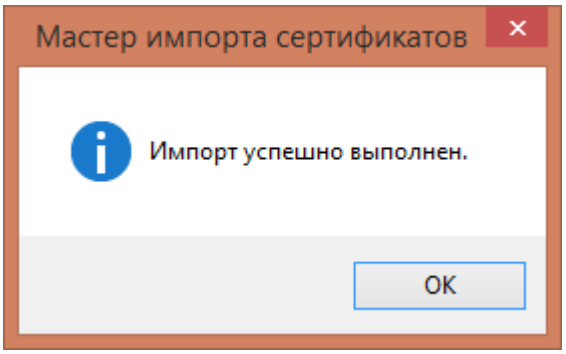

Рисунок 33. Информационное окно «Мастер импорта сертификатов»

Далее следует нажать кнопку «ОК». В результате станет доступно окно «Сертификат» (Рисунок 29), в котором следует нажать кнопку «ОК». Окно «Сертификат» закроется.

После установки сертификата можно проверить, что сертификат ФСС установился. Для этого необходимо зайти в управление сертификатами, например, в строке Выполнить ввести certmgr.msc. Далее зайти в папку «Личное» (Рисунок 34).

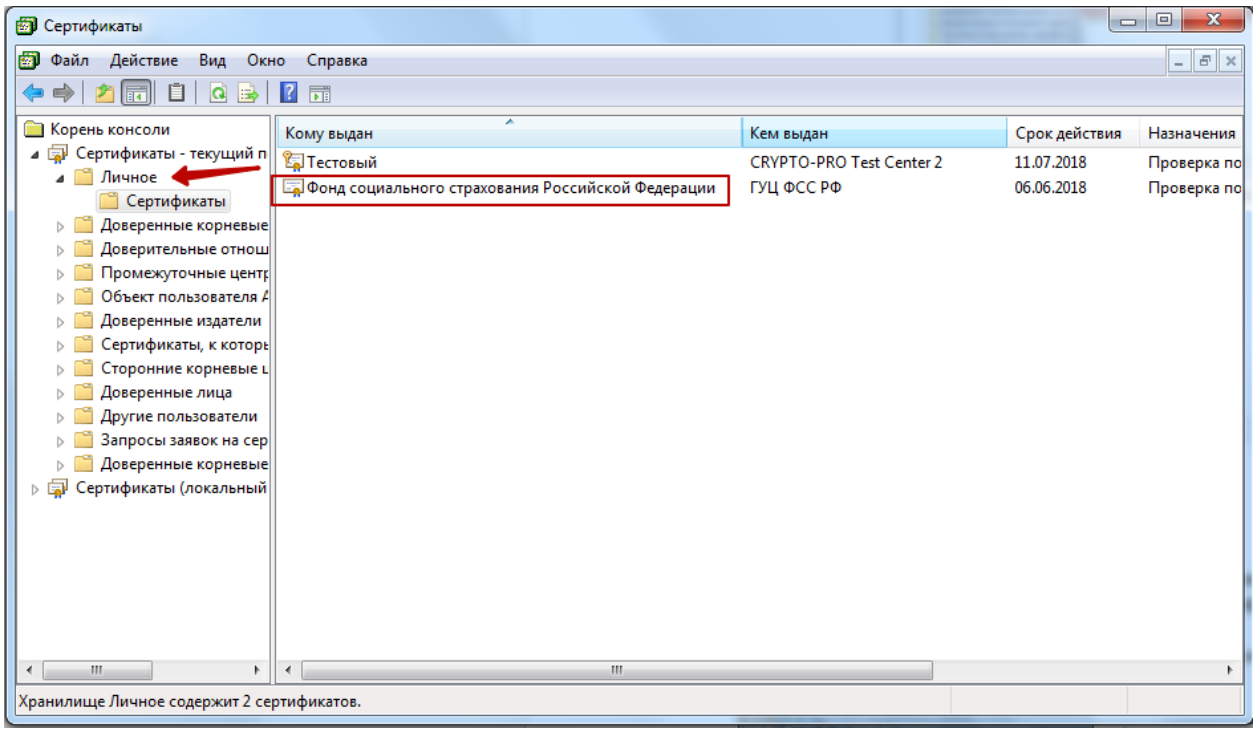

Рисунок 34. Управление сертификатами пользователей

1.1.7 Разворачивание сервиса подписи в IIS

Перед разворачиванием сервиса следует распаковать файлы сервиса из архива «Сервис подписи – [номер версии].zip».

Для разворачивания сервиса взаимодействия следует зайти в службы IIS, выбрав Панель управления – Администрирование – Диспетчер служб ISS. В результате откроется окно «Диспетчер служб IIS» (Рисунок 35), в котором необходимо щелкнуть правой кнопкой мыши по «сайты» и в контекстном меню выбрать «Добавить веб-сайт».

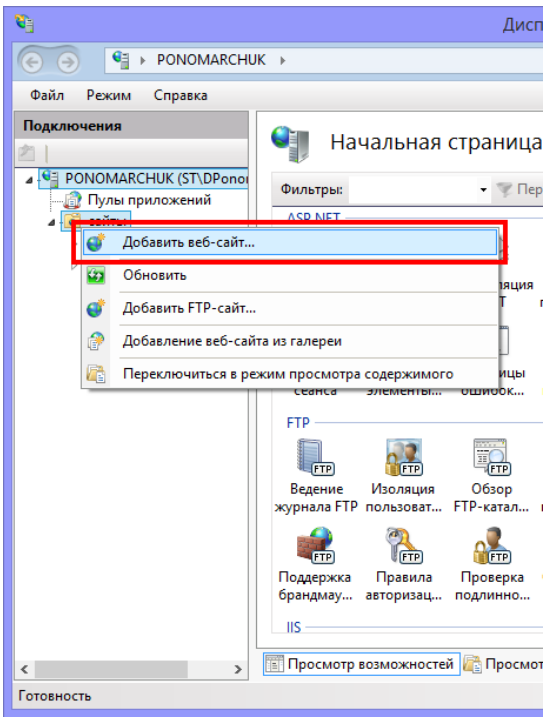

Рисунок 35. Диспетчер служб IIS

После чего откроется окно добавления веб-сайта (Рисунок 36).

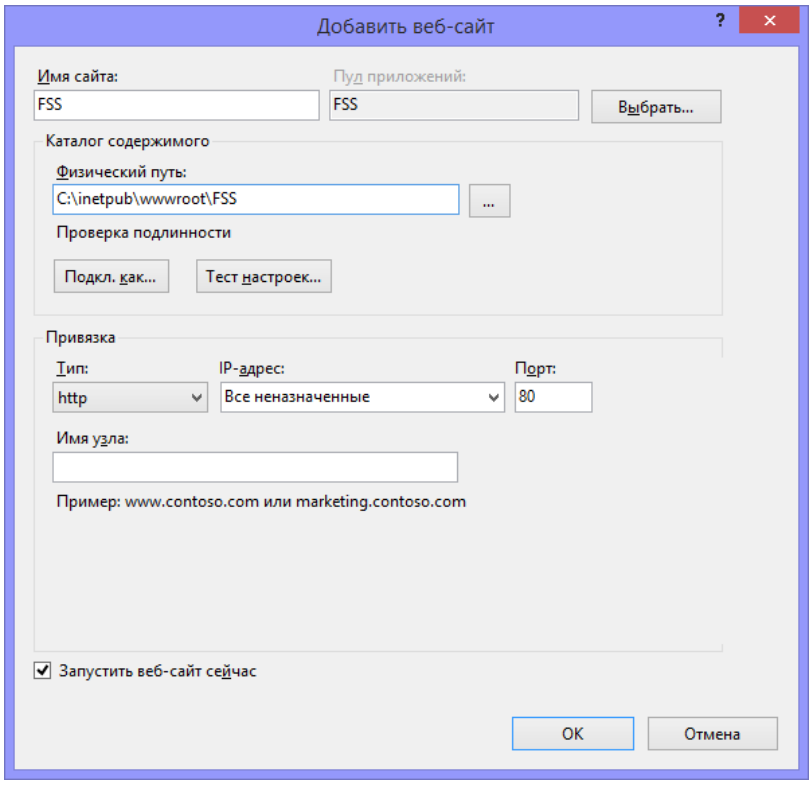

Рисунок 36.Окно добавления веб-сайта

В поле «Имя сайта» необходимо указать наименование сервиса (например, «FSS»), в поле «Физический путь» указать папку, в которой распакован сервис взаимодействия из архива. Далее нажать кнопку «ОК».

После создания веб-сайта необходимо указать пользователя, под которым будет храниться сертификат ЛПУ. Для этого следует зайти в «Пулы приложений», в списке выделить сайт FSS и нажать «Дополнительные параметры». Откроется окно «Дополнительные параметры» (Рисунок 37), в котором в разделе «Модель процесса» необходимо установить параметр «Удостоверение».

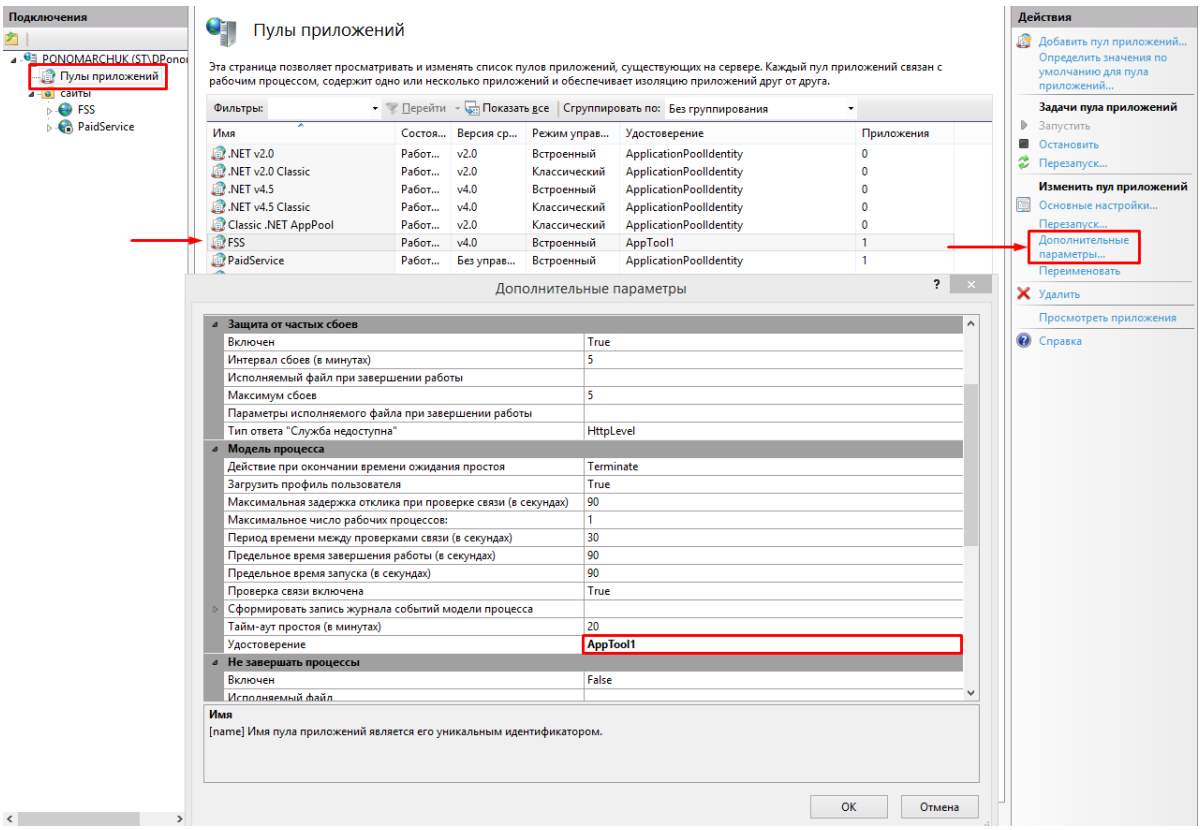

Рисунок 37. Пулы приложений

В качестве значения параметра «Удостоверения» выступает пользователь, под которым установлены ЭЦП. Чтобы заполнить данный параметр необходимо нажать ... справа от поля. В результате откроется окно «Удостоверение пула приложений» (Рисунок 38).

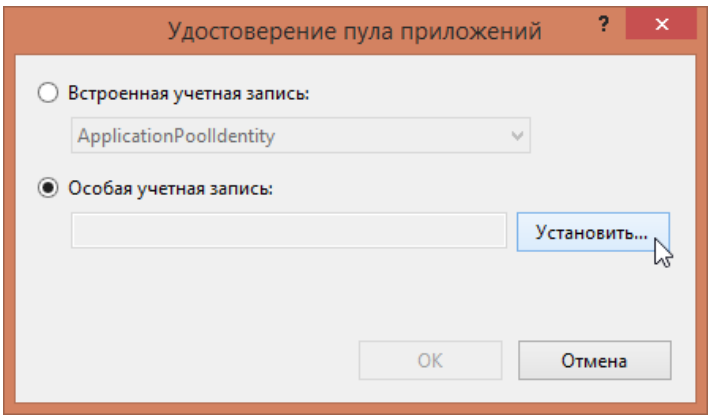

Рисунок 38. Окно «Удостоверение пула приложений»

В открывшемся окне следует поставить метку «Особая учетная запись» и нажать кнопку «Установить». В результате откроется окно «Задание учетных данных» (Рисунок 39).

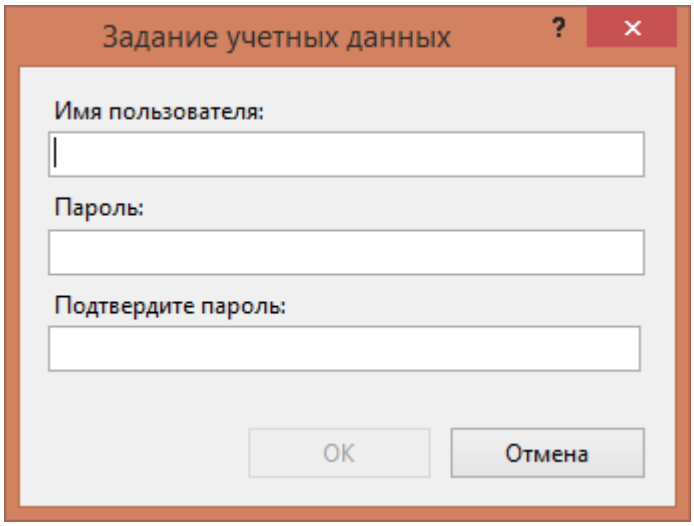

Рисунок 39. Окно «Задание учетных данных

В поле «Имя пользователя» необходимо ввести логин, под которым осуществляется вход в систему Windows. Если логин пользователя при входе в Windows осуществляется в виде «домен\логин», то в поле «Имя пользователя» указывается доменное имя.

В поле «Пароль» необходимо ввести пароль пользователя, который указывается при входе в систему Windows. В поле «Подтвердите пароль» необходимо повторить пароль, введенный в поле «Пароль».

После заполнения всех полей следует нажать кнопку «ОК». Если имя пользователя введено некорректно, то появится сообщение об ошибочном пароле или о том, что имя пользователя не существует (Рисунок 40).

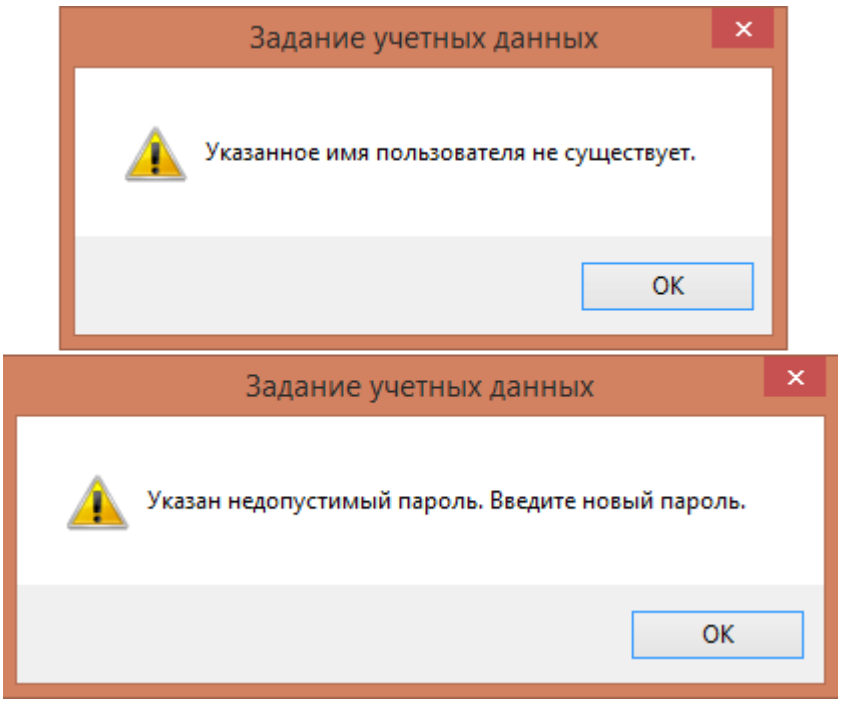

Рисунок 40. Информационные сообщения о неверно введенном пользователе

Пользователь будет задан в поле «Особая учетная запись» (Рисунок 38). Следует нажать кнопку «ОК». Параметр «Удостоверение» будет заполнено.

Проверить работоспособность сервиса можно по адресу http://localhost/api/notwork/. Если на сервере отображается сообщение, изображенное на (Рисунок 41), то всё настроено верно.

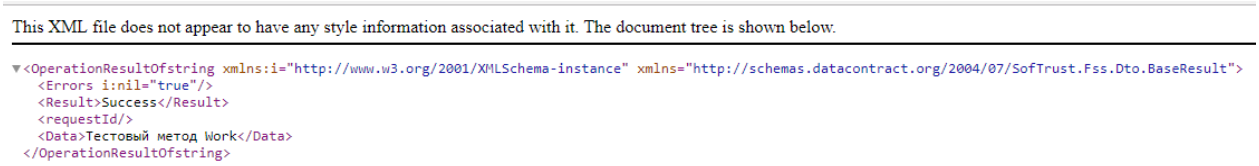

Рисунок 41. Проверка работоспособность сервиса

Проверить настройки сервиса можно по адресу http://localhost/api/sysinfo. В результате должна отобразиться страница, изображенная на Рисунок 42.

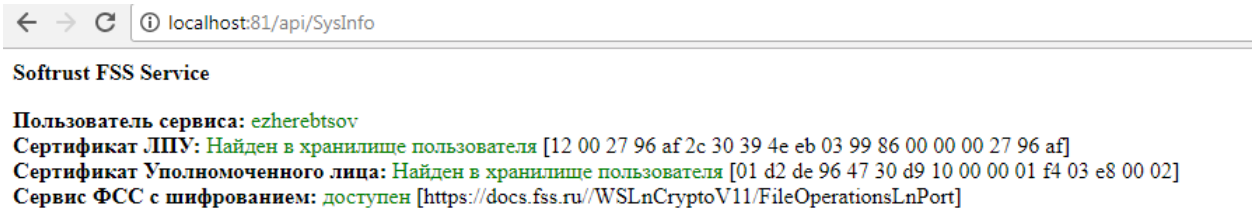

Рисунок 42. Проверка настройки сервиса

Проверить настройки можно иным способом. Для этого выделить в IIS сайт fss и нажать «Обзор» (Рисунок 43).

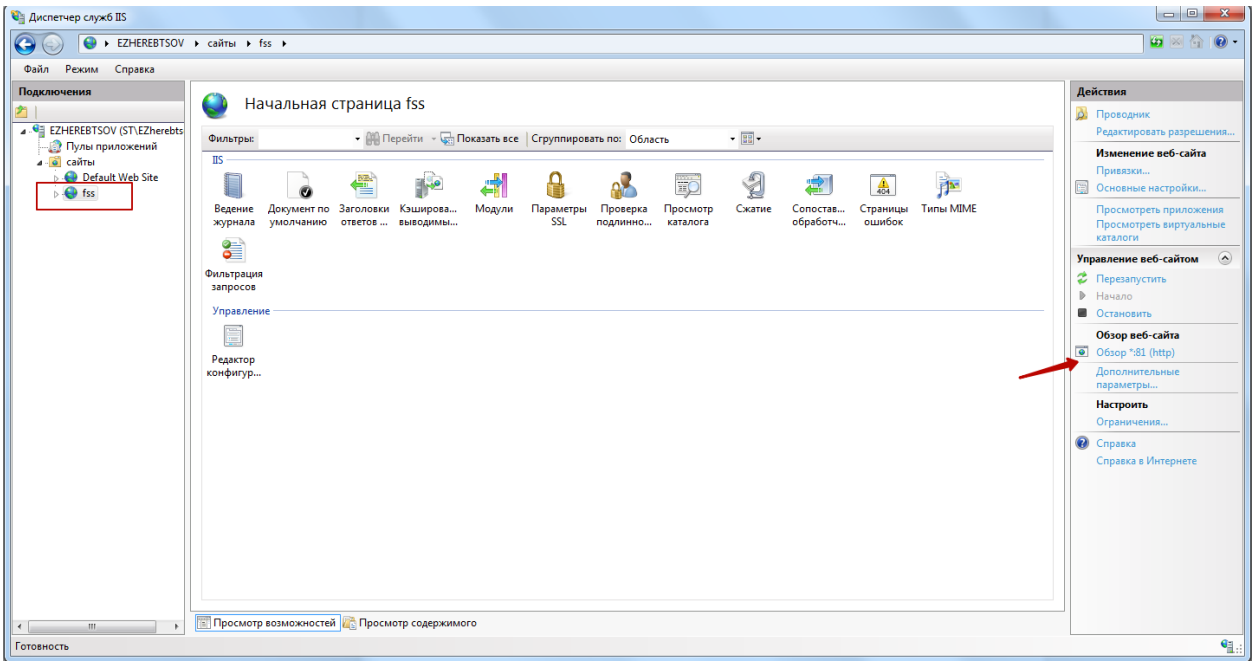

Рисунок 43. Диспетчер служб IIS.

В результате загрузится страница вида, изображенного на Рисунок 44. Далее следует нажать ссылку «Проверить настройки». В результате загрузится страница, изображенная на Рисунок 42.

Рисунок 44. Страница проверки настроек

Если возникает ошибка в работе ASP или он не отображается в списке (Рисунок 45), нужно выполнить одно из действий:

1) Установить обновления Windows.
2) Перезагрузить ПК после свежей установки.
3) В отдельных случаях помогает автономный пакет последней версии ASP.Net.

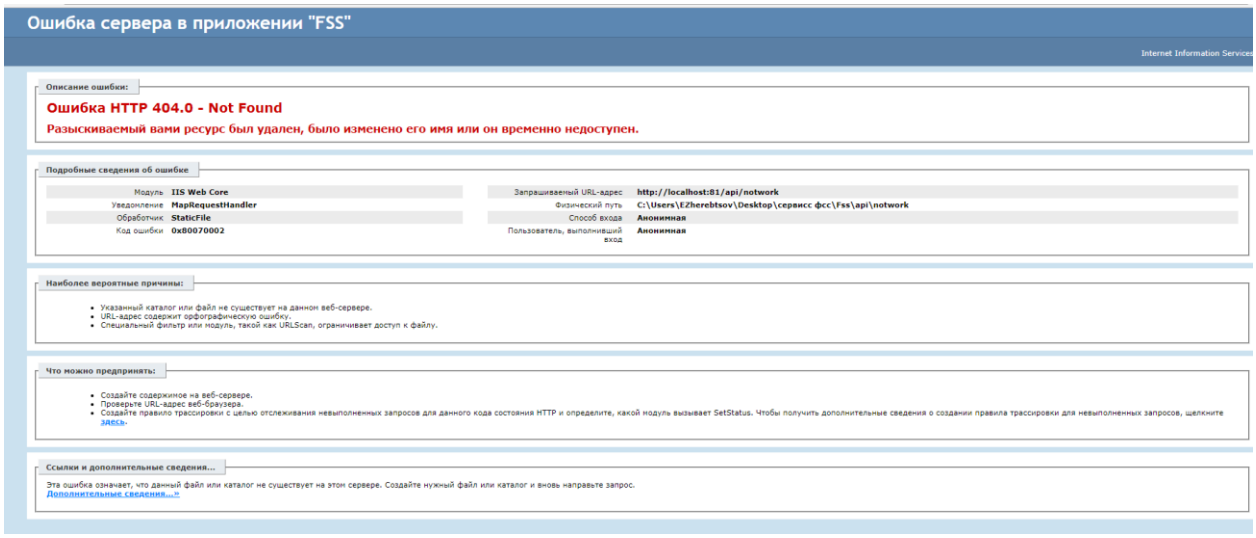

Рисунок 45. Ошибка в работе сайта

4) Запуск команд в консоли от имени администратора.

Для открытия консоли следует вызвать командную строку под администратором, например, щелкнув правой кнопкой мыши по Пуску (Рисунок 46).

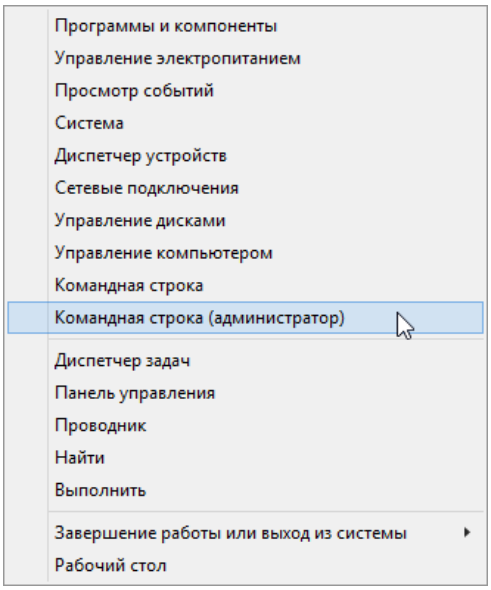

Рисунок 46. Контекстное меню Пуска

В консоли ввести команду (Рисунок 47):

Для 64-разрядных систем:

%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -iru

Для 32-разрядных систем:

%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -iru

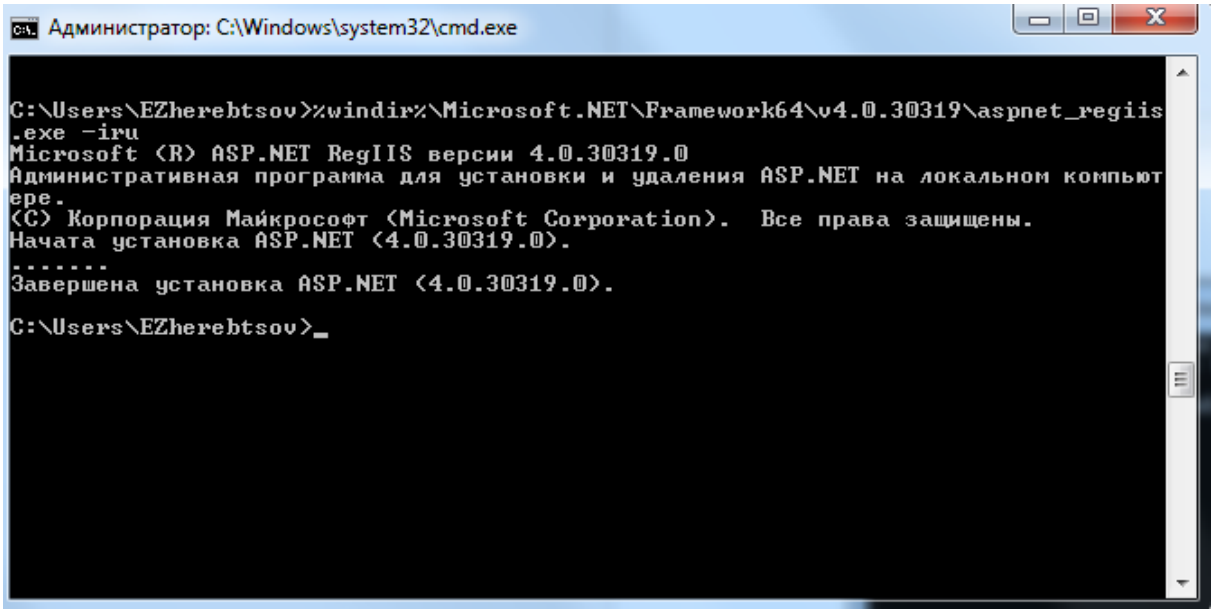

Рисунок 47. Команда регистрации ASP.NET в консоли

Далее следует настроить правильно конфигурационный файл развернутого сервиса. Для этого следует в папке, которая указана при настройке сайта (см. Рисунок 36) найти файл Web.config (Рисунок 48) и открыть его на редактирование.

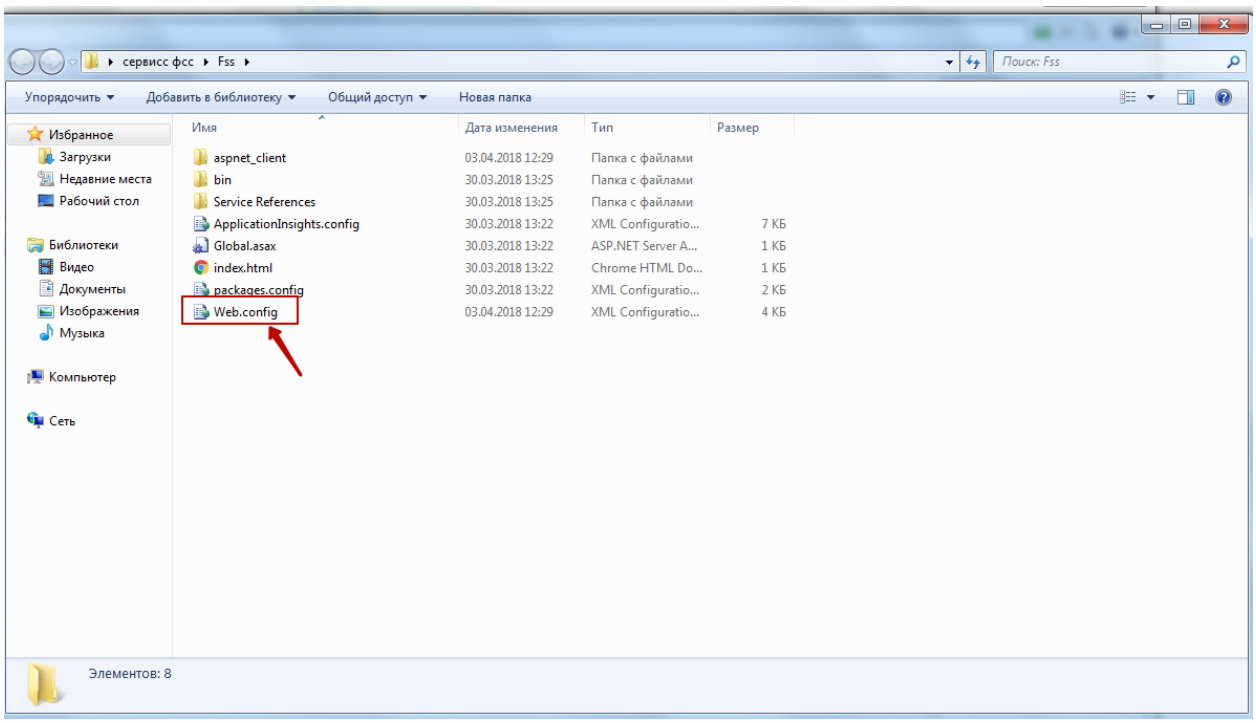

Рисунок 48. Папка с сервисом подписи

В файле Web.config найти параметр «numCertLPU» – серийный номер сертификата подписи ЛПУ. В качестве значения необходимо указать серийный номер сертификата, например, <add key="numCertLPU" value="12 00 20 a4 17 85 2e ac 06 ea 91 a6 5a 17" /> (Рисунок 49).

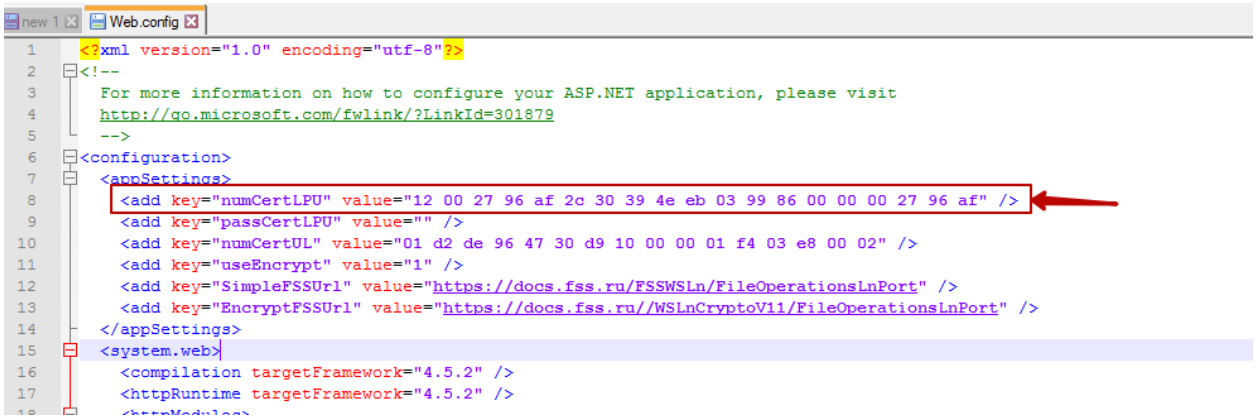

Рисунок 49. Параметр «numCertLPU», пример

Далее в файле Web.config следует найти параметр «numCertUL» – серийный номер сертификата Уполномоченного лица ФСС, установленного в п. 1.1.6. В качестве значения необходимо указать серийный номер сертификата, например, <add key="numCertUL" value="01 d2 de 96 47 30 d9 10 00 00 01 f4 03 e8 00 02" /> (Рисунок 50).

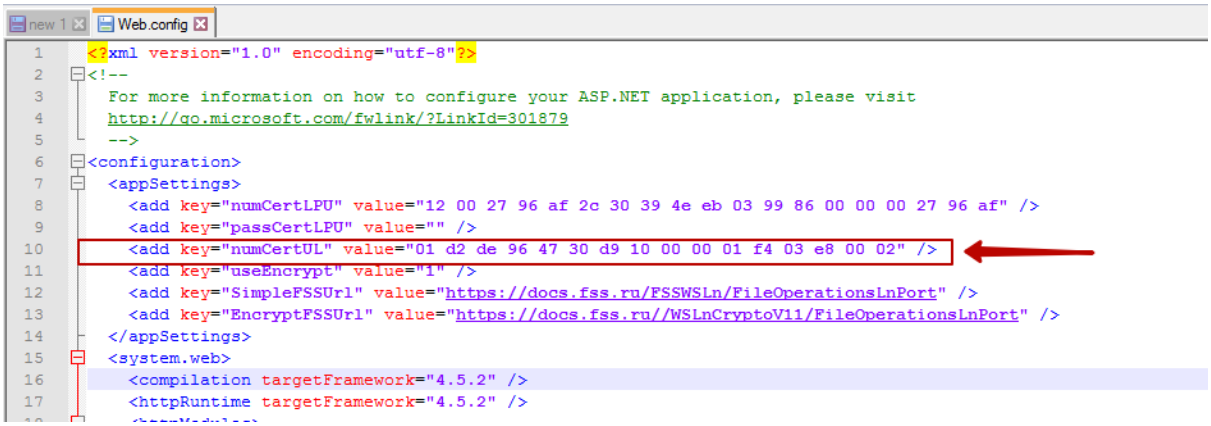

Рисунок 50. Параметр «numCertUL», пример

Далее в файле Web.config следует найти параметр «EncryptFSSUrl» – адрес сервиса ФСС с шифрованием (возможен тестовый и продуктивный). В качестве значения необходимо указать тестовый адрес сервиса (Рисунок 51):

<add key="EncryptFSSUrl" value="https://docs-test.fss.ru/WSLnCrypto/FileOperationsLnPort" />

или продуктивный (Рисунок 52):

<add key="EncryptFSSUrl" value="https://docs.fss.ru//WSLnCryptoV11/FileOperationsLnPort" />.

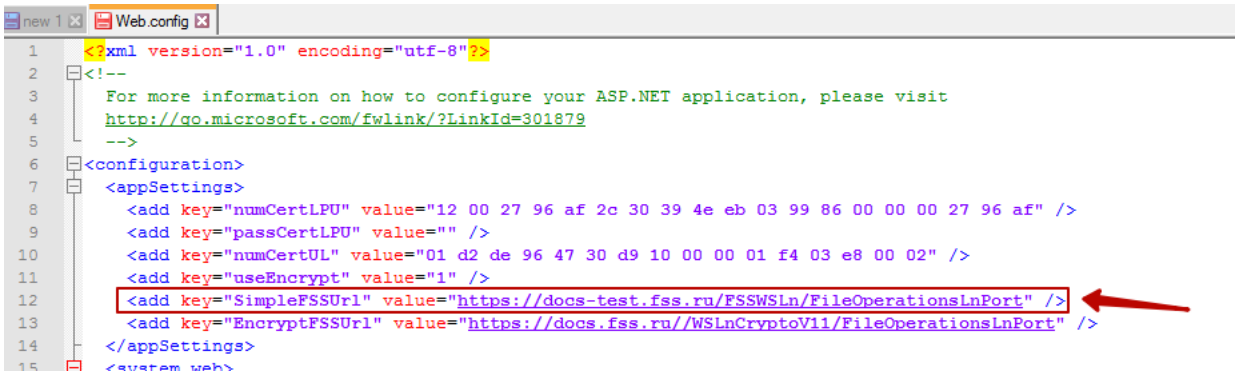

Рисунок 51. Параметр «EncryptFSSUrl». Тестовый адрес сервиса

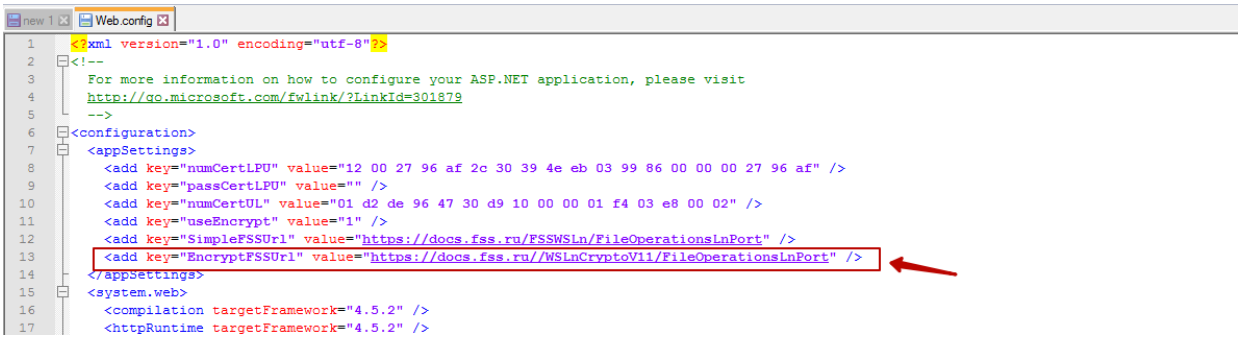

Рисунок 52. Параметр «EncryptFSSUrl». Продуктивный адрес сервиса

1.2 Настройка рабочего места врача

Для подписи ЭЛН на рабочем месте врача требуется установить КриптоПро CSP версии 3.6 или выше или VipNet CSP версии 4.2 или выше.

Далее следует установить сертификат врача в хранилище пользователя. Рассмотрим установку сертификата ЛПУ на примере программы КриптоПро CSP. Перед установкой сертификата следует вставить флешку с ключом в компьютер.

1.2.1 Установка сертификата врача в хранилище текущего пользователя

После установки КриптоПро CSP следует нажать левой кнопкой мыши по установленной программе КриптоПро CSP. Программа может располагаться в Пуске, на рабочем столе (если была установлена иконка), или ее можно найти поиском, нажав win+F.

В открывшемся окне (Рисунок 53) следует перейти на вкладку «Сервис», далее нажать кнопку «Скопировать»

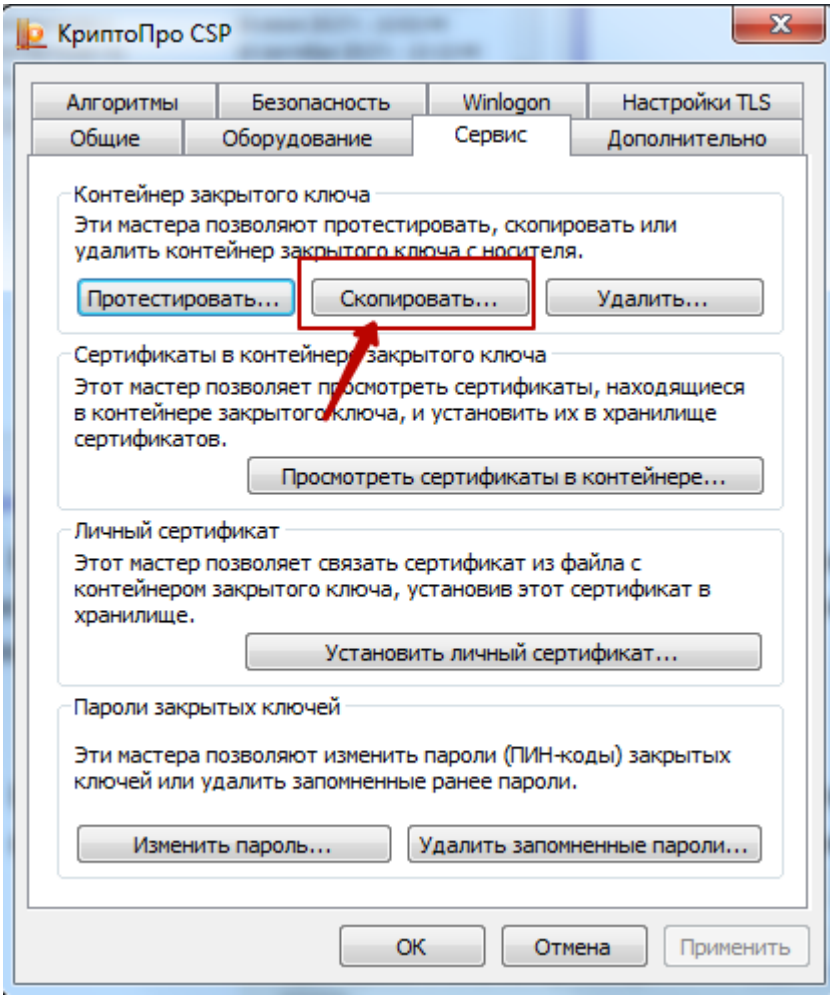

Рисунок 53. Копирование контейнера в реестр на компьютер

В результате откроется окно (Рисунок 54), в котором необходимо указать имя ключевого контейнера.

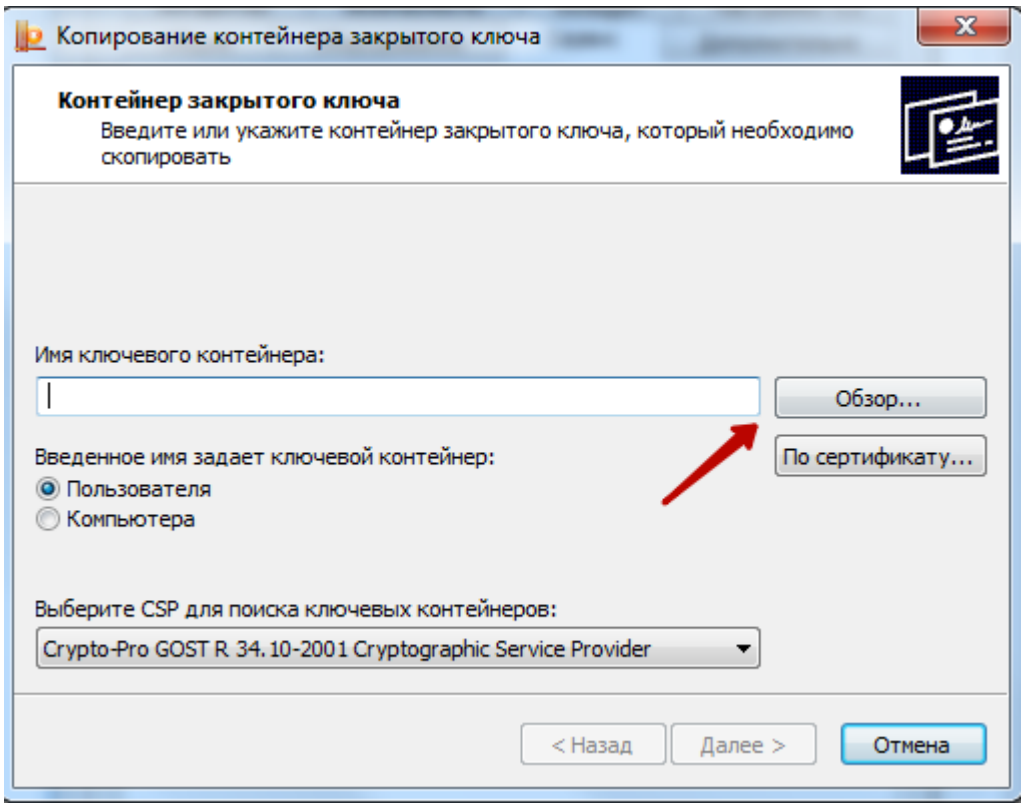

Рисунок 54. Окно ввода имени ключевого контейнера

Для того чтобы ввести имя контейнера следует нажать кнопку «Обзор». В результате откроется окно выбора контейнера (Рисунок 55).

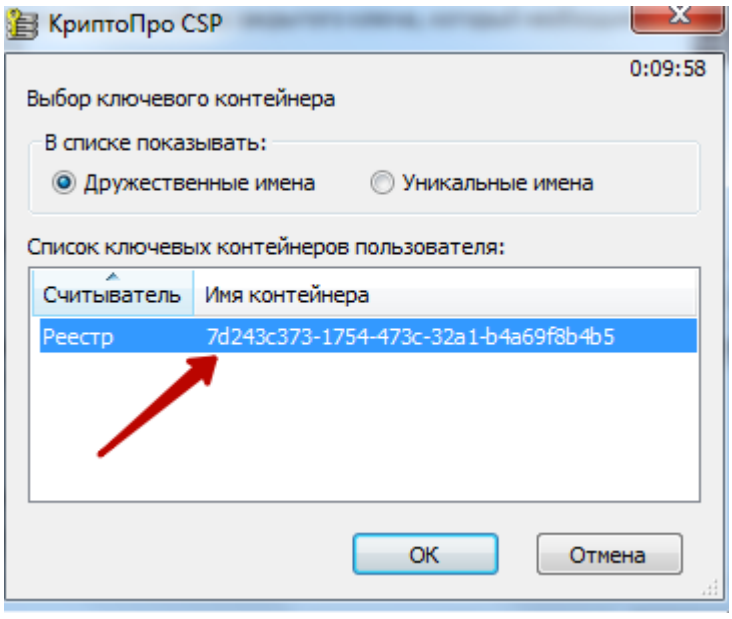

Рисунок 55. Выбор ключевого контейнера

В данном окне необходимо выбрать имя реестра и нажать кнопку «ОК». В результате заполнится поле «Имя ключевого контейнера» (Рисунок 56).

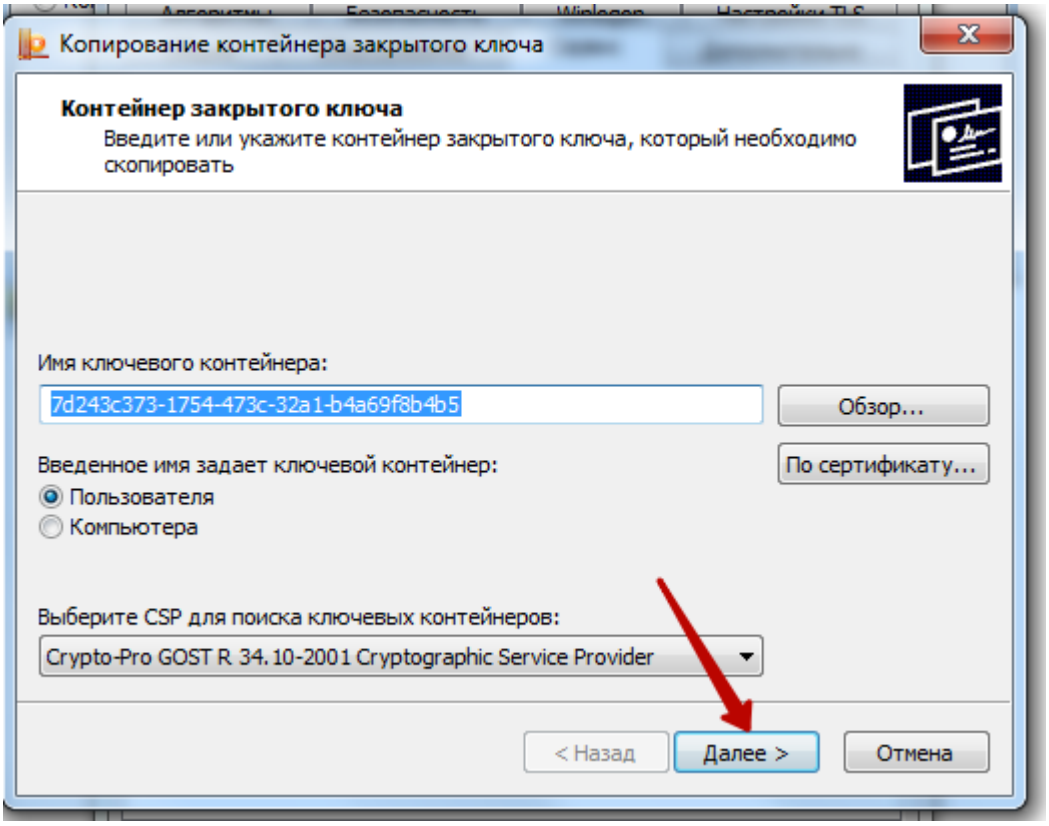

Рисунок 56. Заполнено поле «Имя ключевого контейнера»

После того как имя задано следует нажать кнопку «Далее». В результате отроется окно (Рисунок 57), в котором необходимо указать имя для создаваемого ключевого контейнера.

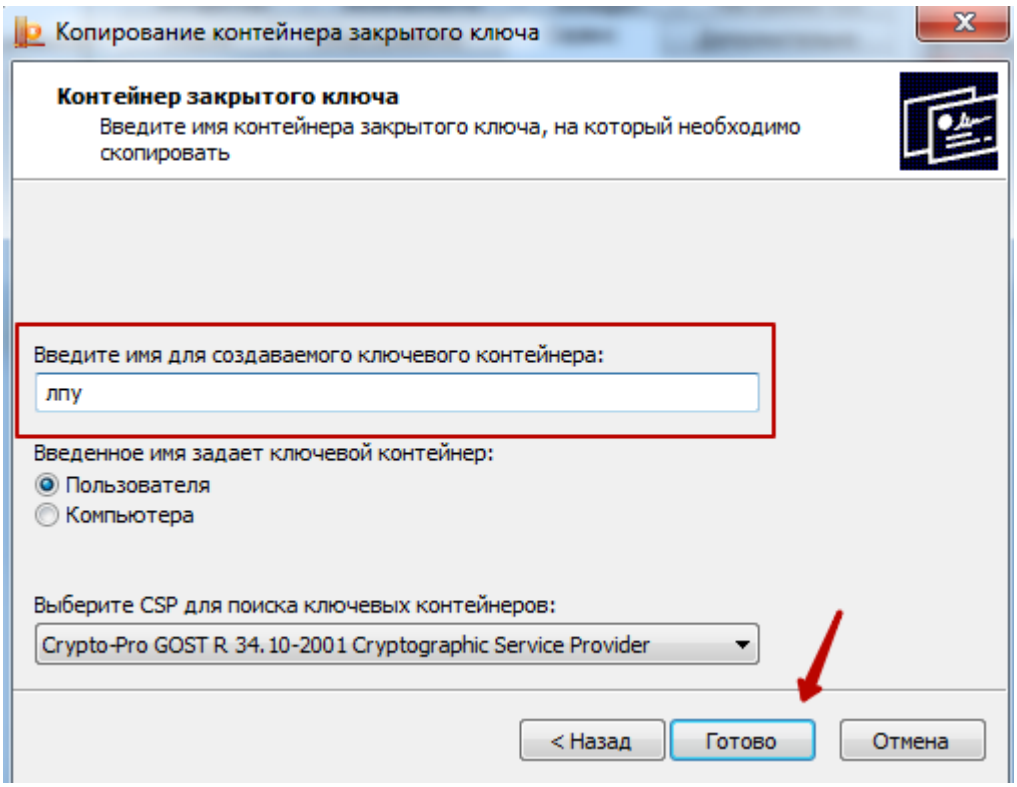

Рисунок 57. Заполнение поля «Введите имя для создаваемого ключевого контейнера

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 58), в котором необходимо выбрать носитель для хранения контейнера закрытого ключа.

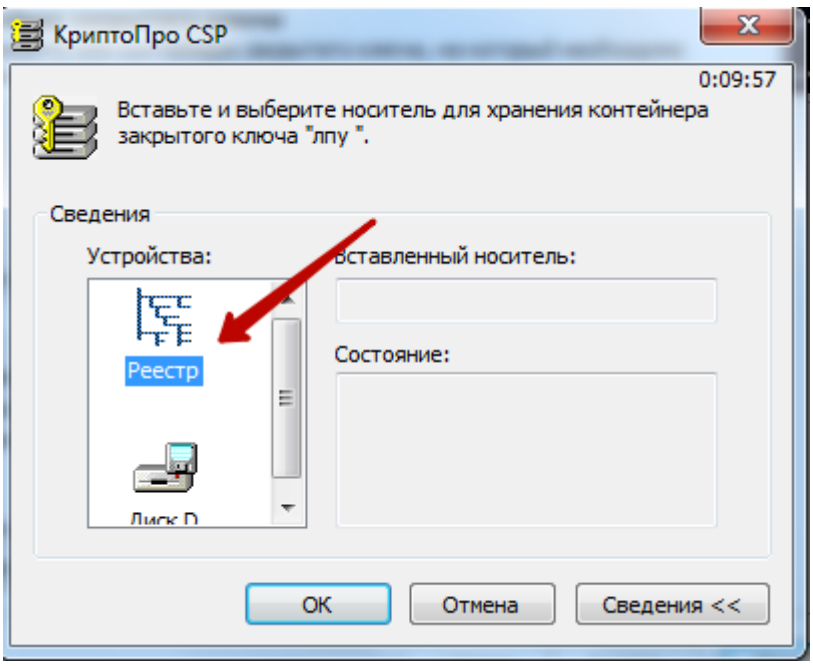

Рисунок 58. Выбор носитель для хранения контейнера

В данном окне следует выбрать устройство. В данном случае, в качестве устройства следует выбрать «Реестр» и нажать кнопку «ОК». После чего откроется окно (Рисунок 59), в котором необходимо задать пароль для создаваемого контейнера.

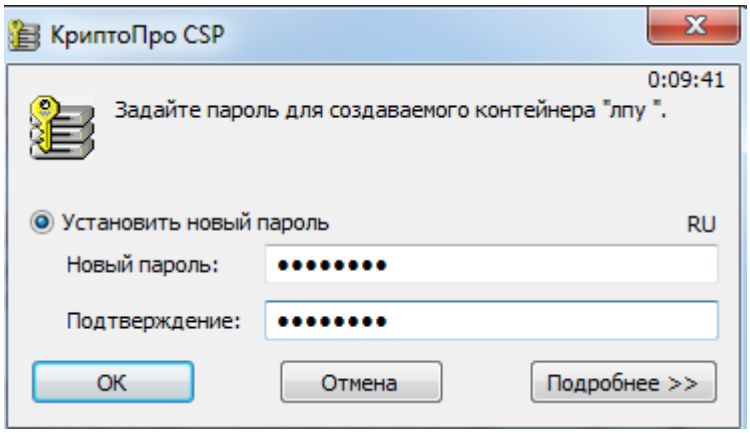

Рисунок 59. Окно задания пароля для контейнера

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.

1.2.2 Установка сертификата врача из контейнера в реестре на компьютере

Для установки сертификата следует на вкладке «Сервис» нажать кнопку «Просмотреть сертификаты в контейнере» (Рисунок 60).

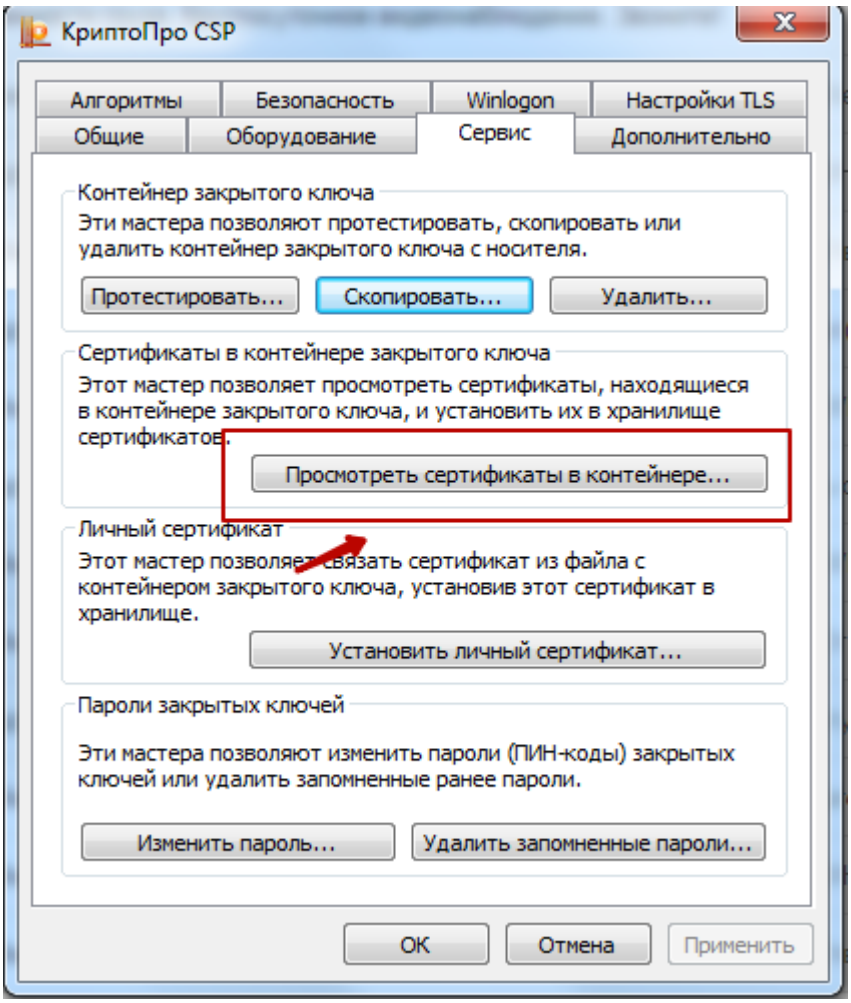

Рисунок 60. Окно «КриптоПро CSP», вкладка «Сервис»

В результате откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 61).

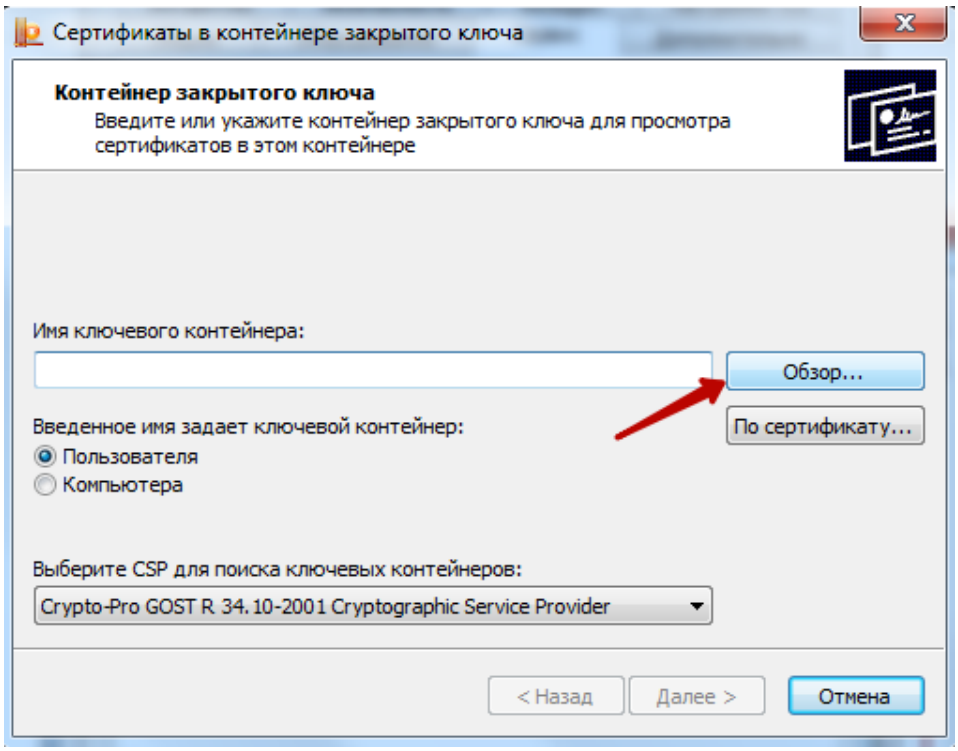

Рисунок 61. Окно «Сертификаты закрытого ключа»

В данном окне следует установить имя ключевого контейнера, нажав кнопку «Обзор». В результате откроется окно выбора ключевого контейнера (Рисунок 62).

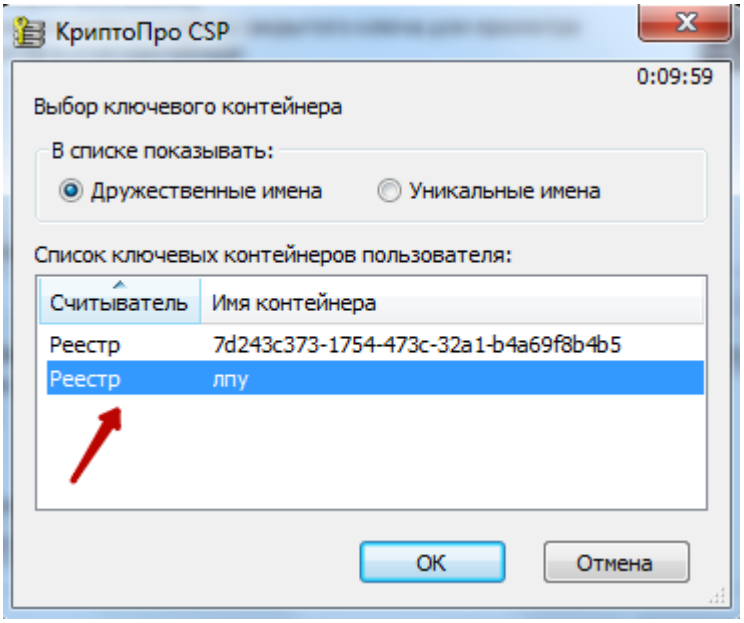

Рисунок 62. Окно выбора ключевого контейнера»

В открывшемся окне следует выбрать имя контейнер, который был создан, и нажать кнопку «ОК». В результате имя ключевого контейнера будет задано (Рисунок 63).

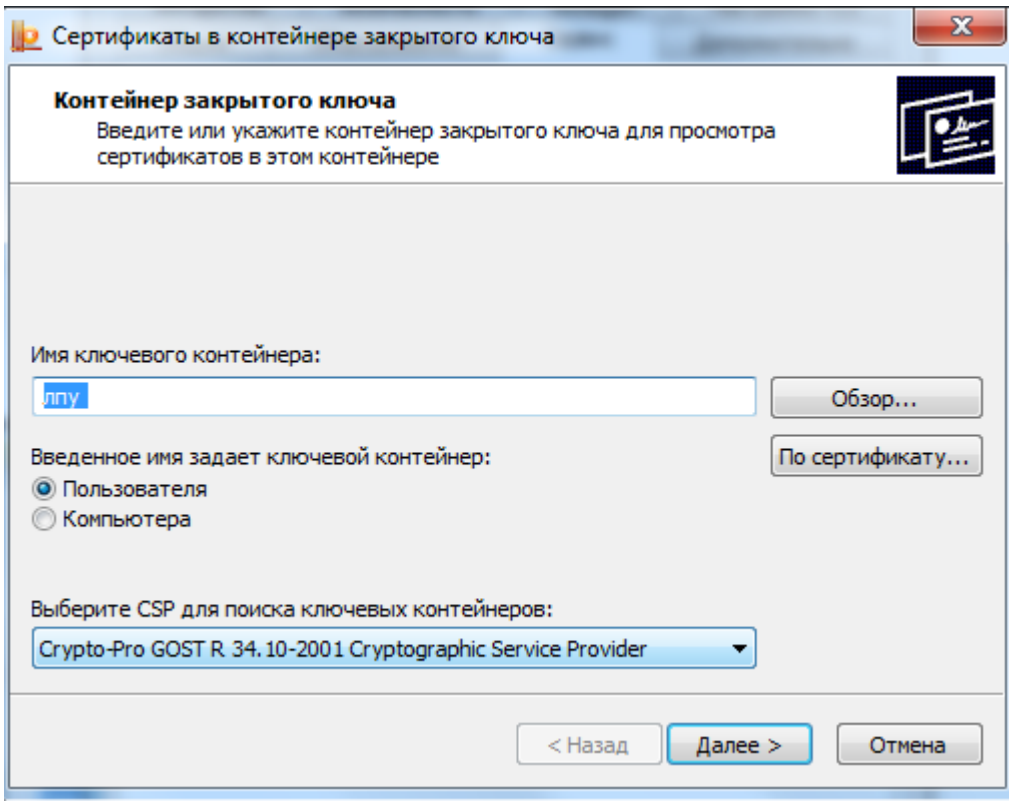

Рисунок 63. Установлено имя ключевого контейнера

Для продолжения следует нажать кнопку «Далее». В результате откроется окно для просмотра сертификата (Рисунок 64).

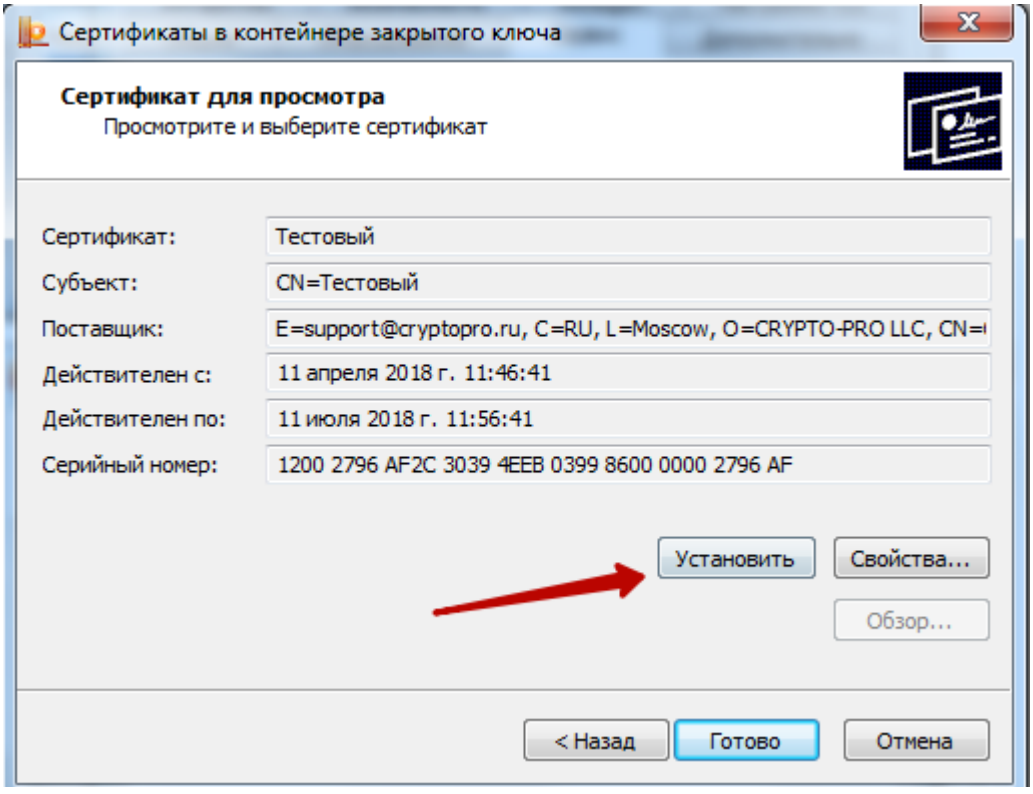

Рисунок 64. Окно просмотра сертификата

Для установки сертификата следует нажать кнопку «Установить». После чего откроется окно (Рисунок 65) с сообщением, что в хранилище уже присутствует сертификат. Следует заметить существующий сертификат новым, нажав кнопку «Да».

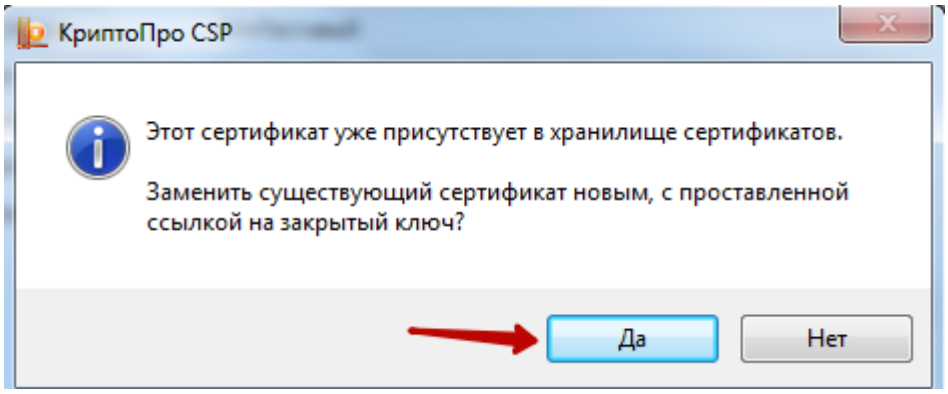

Рисунок 65. Диалоговое окно о замене существующего сертификата

В результате сертификат установится, появится информационное окно об успешной установке (Рисунок 66).

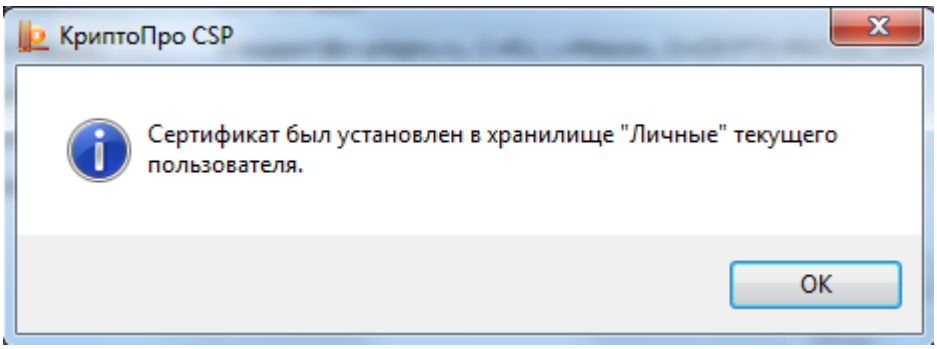

Рисунок 66. Информационное окно об успешной установке сертификата

Далее следует протестировать контейнер.

1.2.3 Тестирование контейнера врача из реестра для сохранения пароля

Для тестирования контейнера следует на вкладке «Сервис» нажать кнопку «Протестировать» (Рисунок 67).

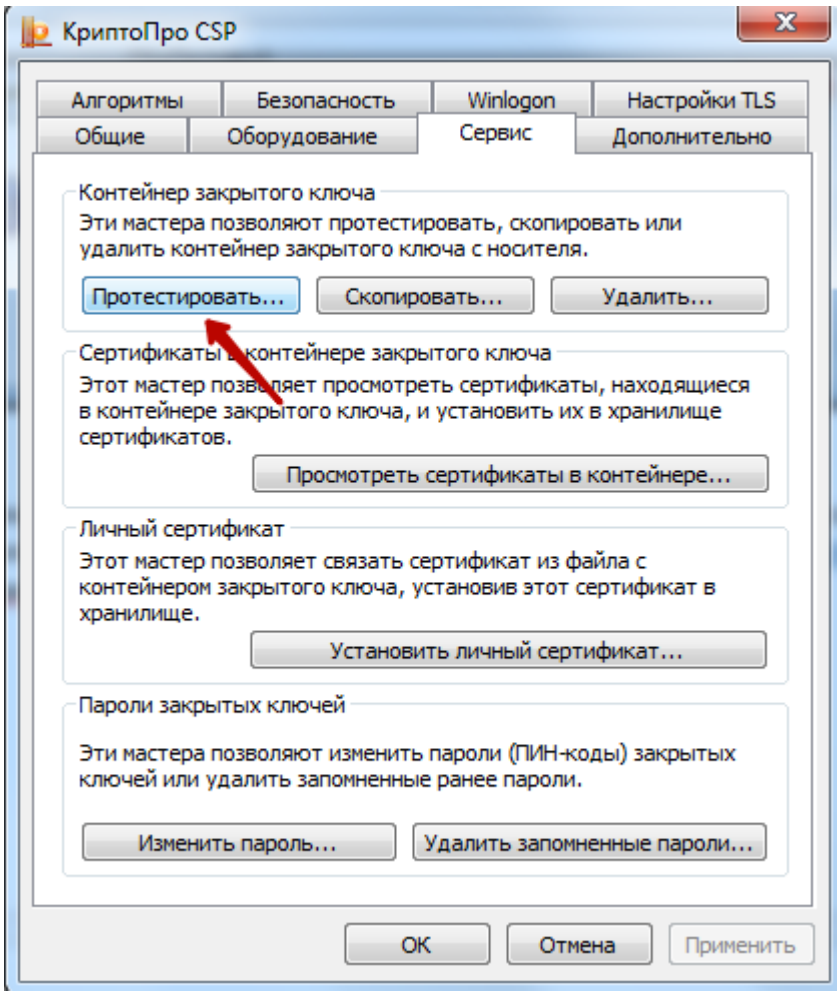

Рисунок 67. Окно «КриптоПро CSP», вкладка «Сервис»

Откроется окно «Сертификаты в контейнере закрытого ключа» (Рисунок 68).

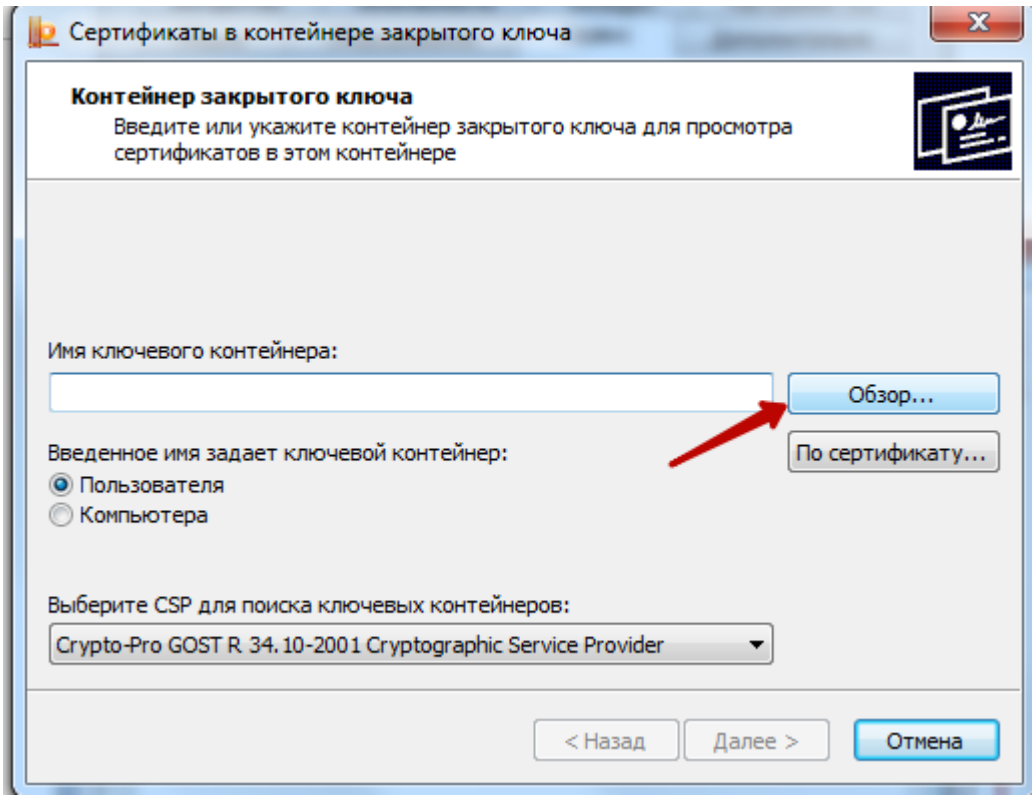

Рисунок 68. Окно «Сертификаты в контейнере закрытого ключа»

В данном окне следует нажать кнопку «Обзор» и в открывшемся окне следует выбрать созданный контейнер (Рисунок 69).

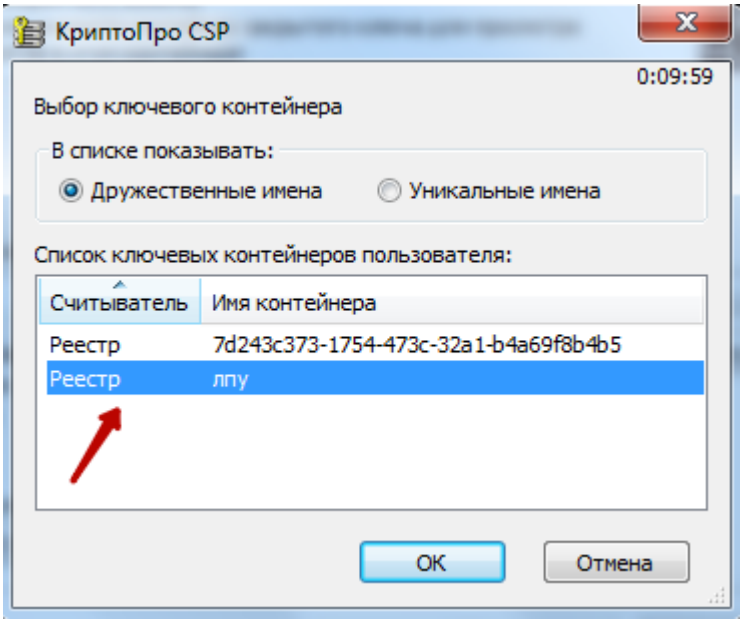

Рисунок 69. Выбор контейнера

После выбора контейнера следует нажать кнопку «ОК». В результате поле «Имя ключевого контейнера» заполнится (Рисунок 70).

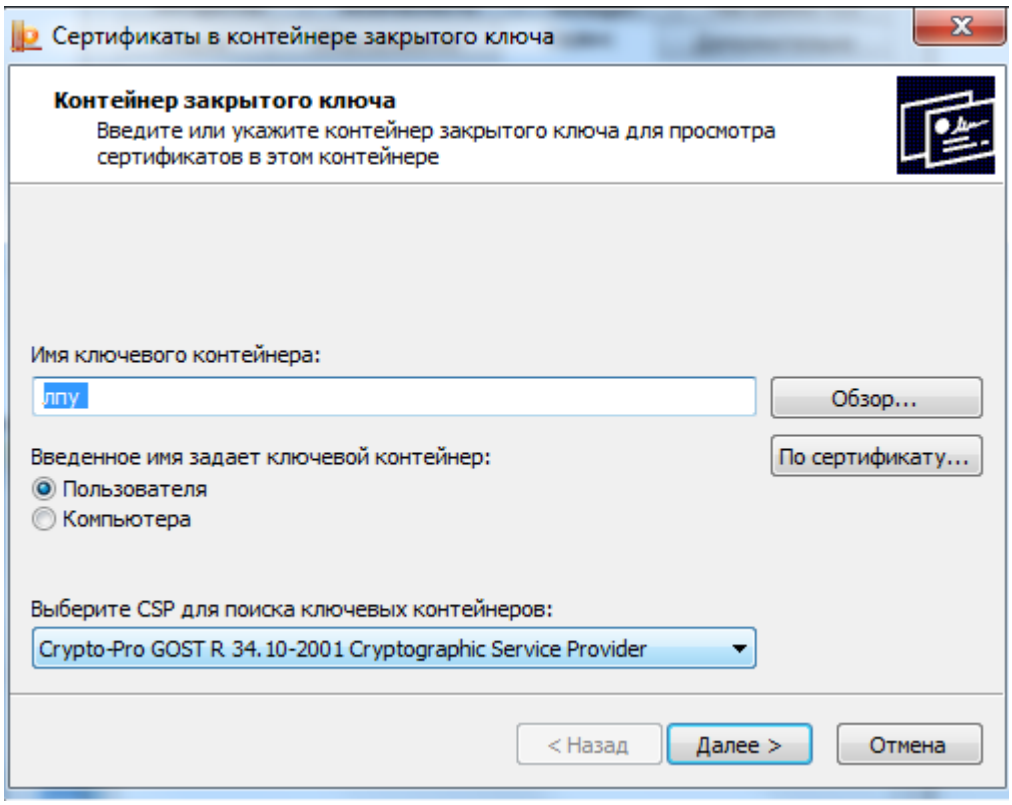

Рисунок 70. Окно «Сертификаты в контейнере закрытого ключа»

Затем следует нажать кнопку «Далее». В результате откроется окно для ввода пароля для контейнера (Рисунок 71).

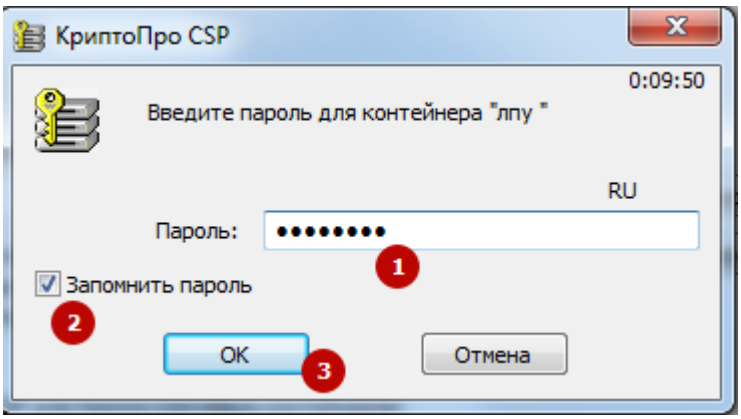

Рисунок 71. Окно ввода пароля для контейнера

В данном окне в поле «Пароль» следует ввести пароль на контейнер, который был установлен при создании контейнера. Далее следует нажать кнопку «ОК», дополнительно можно установить флажок в поле «Запомнить пароль», чтобы пароль не запрашивался при каждом вызове подписи документа. В результате появится окно «Тестирование контейнера закрытого ключа» (Рисунок 72).

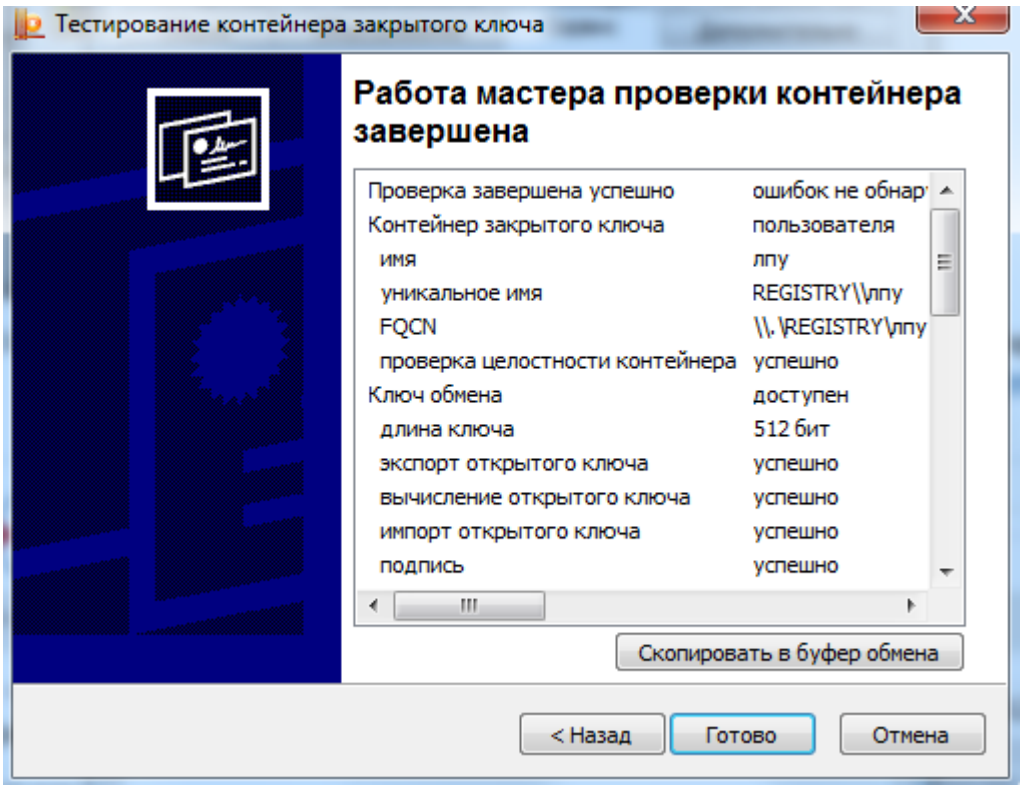

Рисунок 72. «Тестирование контейнера закрытого ключа»

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

Далее следует установить плагин для работы с электронной цифровой подписью.

1.3 Установка плагина КриптоПро ЭЦП

Для ПК «ТрастМед» необходимо скачать плагин cadesplugin.exe 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.

1.3.1 Установка плагина с сайта cryptopro.ru

Скачать плагин можно с сайта https://www.cryptopro.ru/products/cades/downloads (Рисунок 73), скачивание доступно только для авторизованных пользователей.

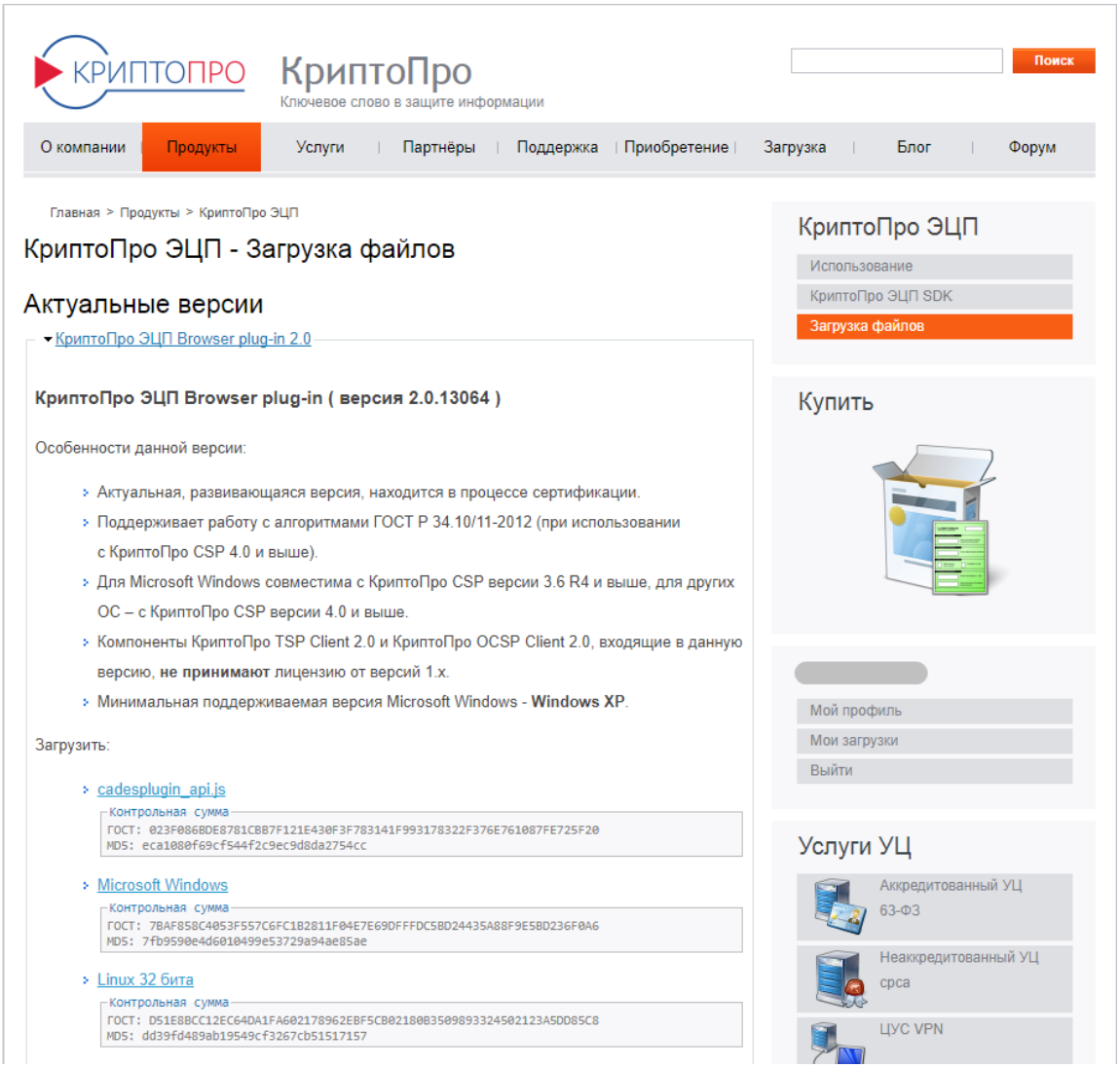

Рисунок 73. Сайт cryptopro.ru

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

1.3.2 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 74). Далее следует нажать кнопку «Установить».

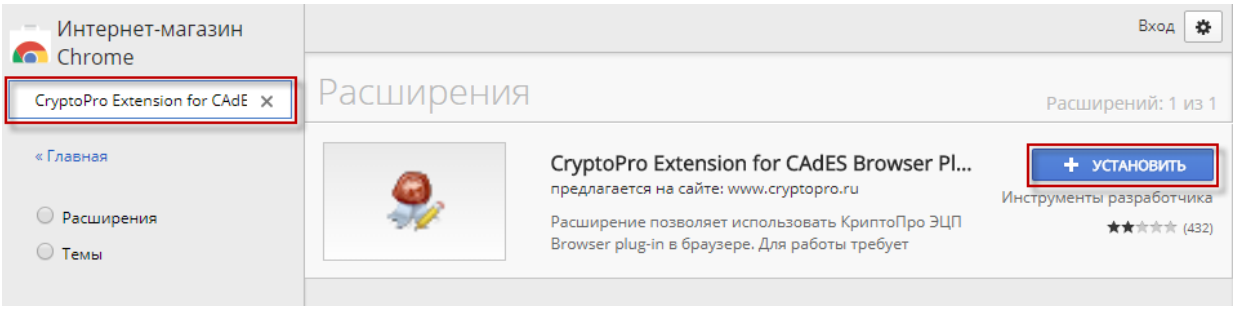

Рисунок 74. Установка расширения CryptoPro Extension for CAdES Browser Plug-in

Расширение для браузера Chrome будет установлено (Рисунок 75).

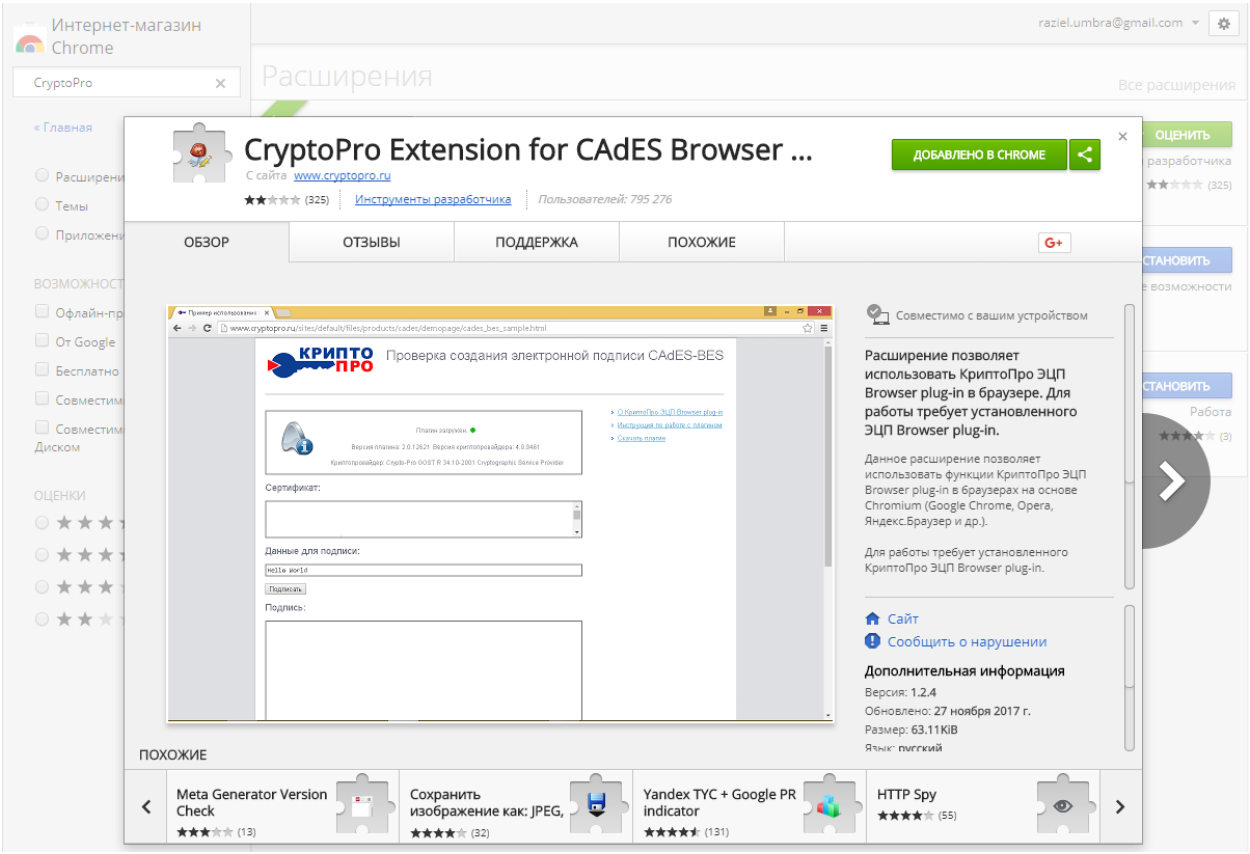

Рисунок 75. Расширение для Chrome установлено

1.3.3 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 76). Сайт доступен только для авторизованных пользователей.

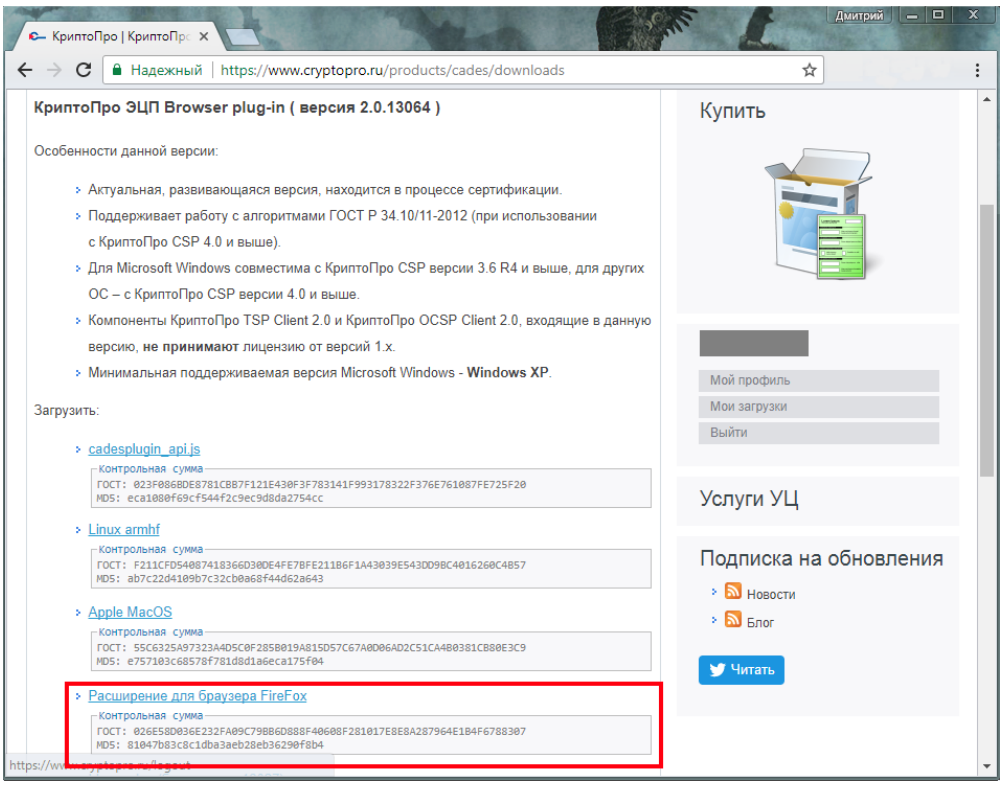

Рисунок 76. Сайт КриптоПро

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 77).

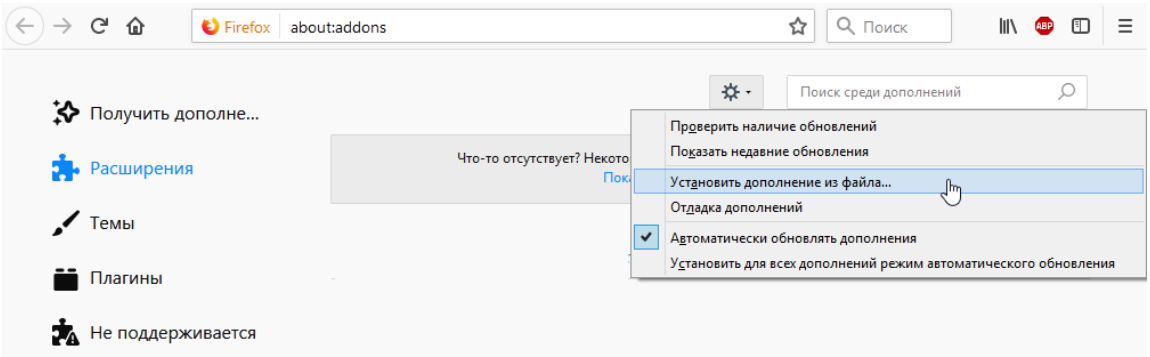

Рисунок 77. Страница дополнений браузера FireFox

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

1.3.4 Установка плагина для браузера Opera

Для того чтобы установить плагин для браузера Opera, следует зайти в меню Opera, затем выбрать «Расширения» – «Загрузить расширения» (Рисунок 78).

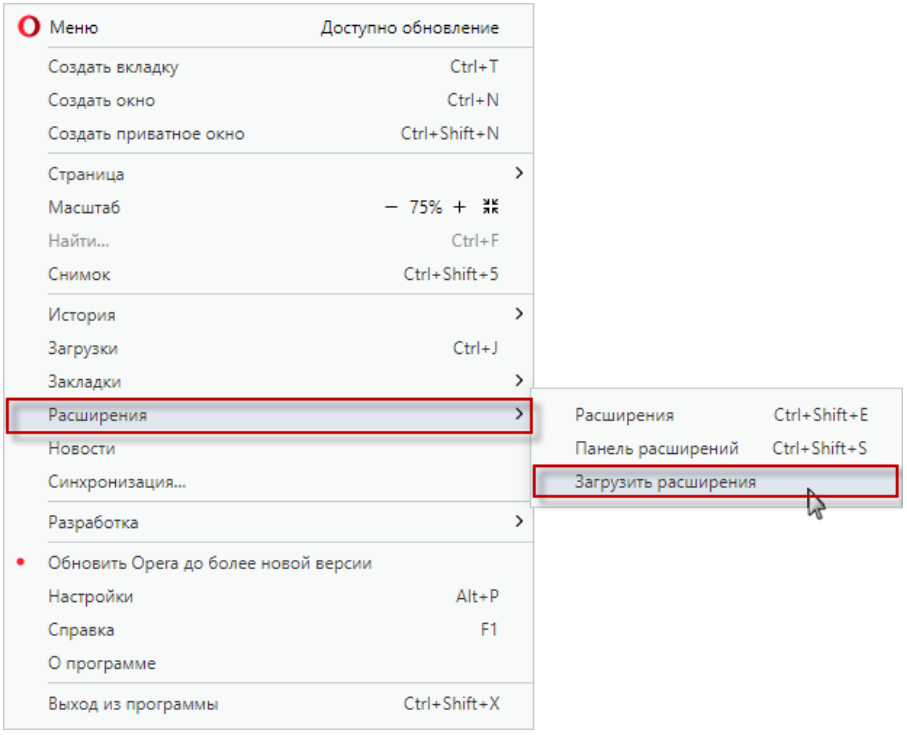

Рисунок 78. Меню браузера Opera

Откроется страница для установки дополнений браузера Opera (Рисунок 79). В поле поиска ввести «cades», затем в выпадающем списке выбрать «CryptoPro Extension for...».

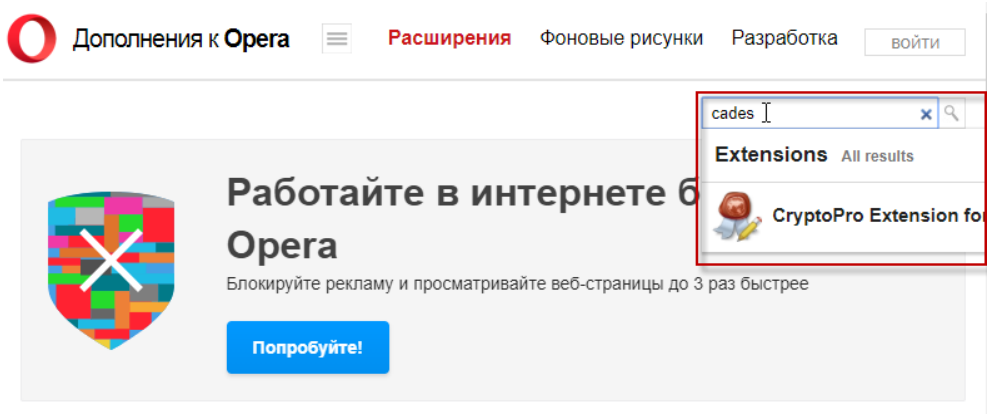

Рисунок 79. Страница дополнений браузера Opera

Затем нажать кнопку «Добавить в Opera» (Рисунок 80). Расширение установится.

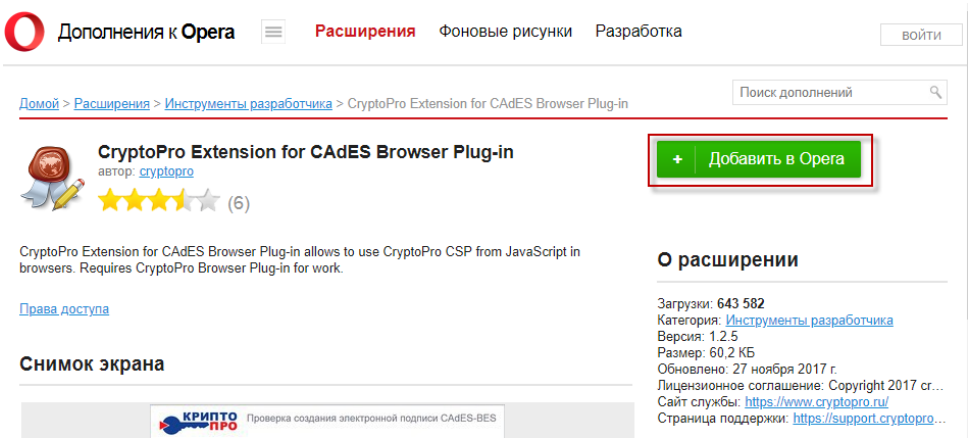

Рисунок 80. Установка расширения CryptoPro Extension for CAdES Browser Plug-in

1.4 Настройка программного комплекса «ТрастМед» для работы с ЭЦП

1.4.1 Настройка desktop-приложения в режиме администрирования

Для настройки «ТМ:МИС» необходимо авторизоваться в системе в режиме администрирования и заполнить необходимые настройки системы.

Важно! Все выполненные настройки будут автоматически транслированы в настройки пользователей при условии, что аналогичные настройки не были изменены самими пользователями.

После авторизации необходимо нажать кнопку «Настройки» в АРМе «Администрирование» и заполнить настройки сервиса подписи (Рисунок 81).

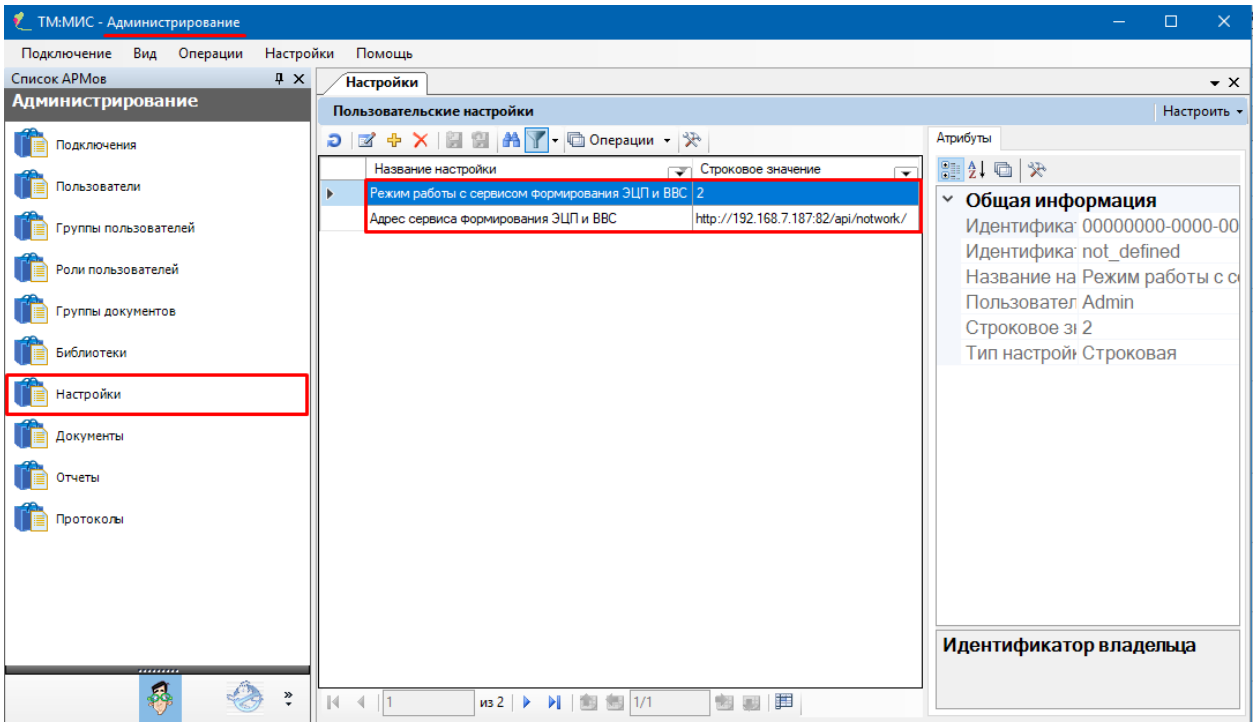

Рисунок 81. Добавление настроек в режиме администрирования

Для строковой настройки «Режим работы с сервисом формирования ЭЦП и ВВС» необходимо указать значение «2».

Далее необходимо заполнить настройку «Адрес сервиса формирования ЭЦП и ВВС». В ней указывается адрес, по которому развернут сервис взаимодействия с внешними системами «адрес сервиса»+ «/api/» (например, http://192.168.7.135/api/). В конце адреса обязательно должен стоять символ «/».

Также необходимо добавить пользовательскую настройку «Номер сертификата пользователя», в строковом значении которой указать значение серийного номера сертификата врача (Рисунок 82).

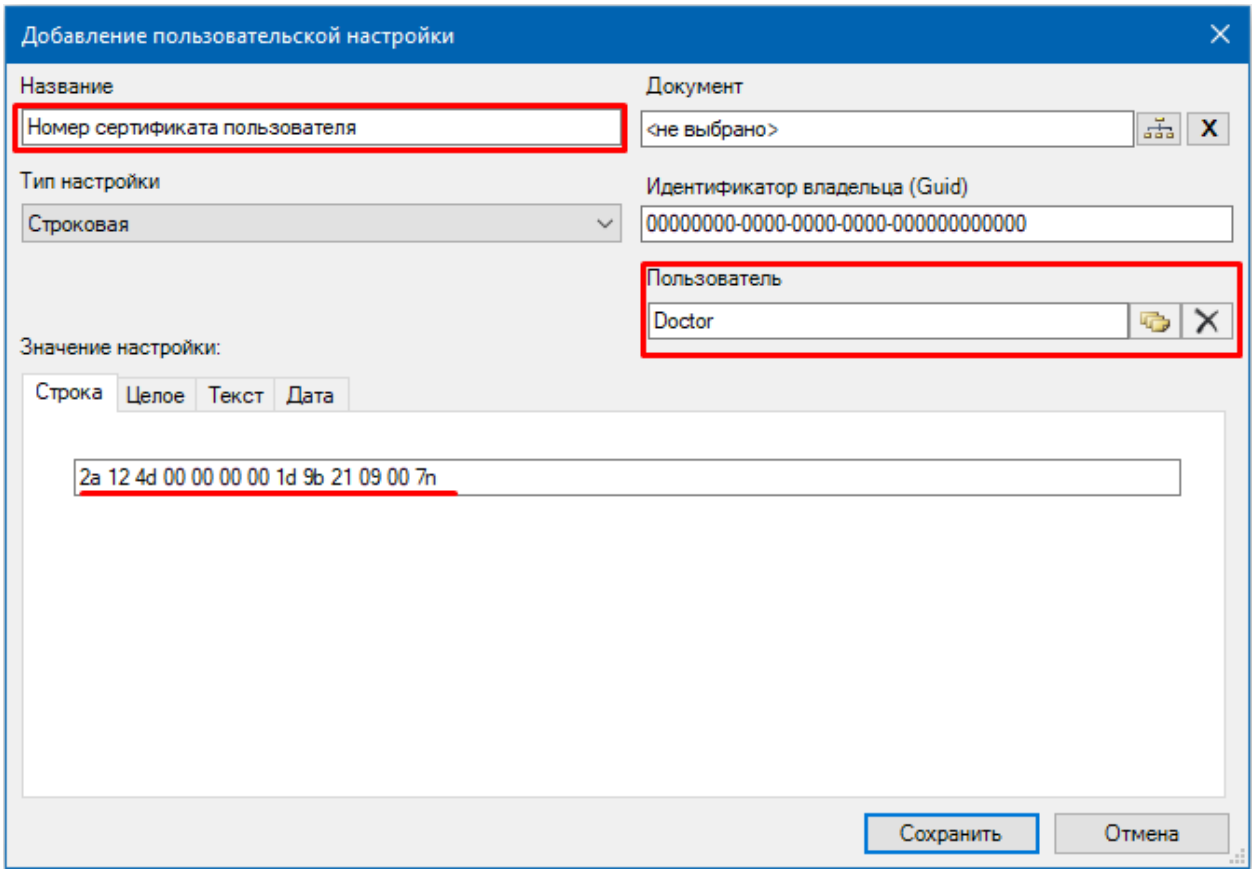

Рисунок 82. Добавление настройки «Номер сертификата пользователя»

1.4.2 Настройка web-приложения в режиме администрирования

Для настройки «ТМ:МИС SaaS» необходимо авторизоваться в системе и заполнить необходимые настройки системы. Для перехода в раздел с настройками необходимо нажать «Администрирование» в левом верхнем углу страницы (Рисунок 83).

Рисунок 83. Раздел «Администрирование»

Откроется страница администрирования, на которой необходимо выбрать пункт «Системные настройки». В результате чего откроется страница с системными настройками системы (Рисунок 84).

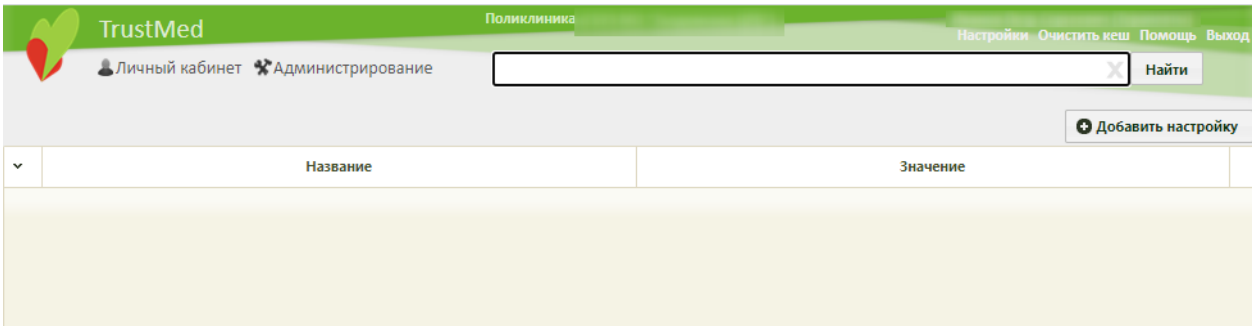

Рисунок 84. Страница с системными настройками

1.4.2.1 Адрес сервиса подписи

В настройке «Адрес сервиса подписи» указывается url-адрес сервиса, который осуществляет взаимодействие с сервисом подписи данных.

На странице раздела с системными настройками в поле поиска необходимо ввести наименование или часть наименования настройки «Адрес сервиса подписи», нажать кнопку «Найти» (Рисунок 85). Отобразится список настроек в соответствии с условием поиска.

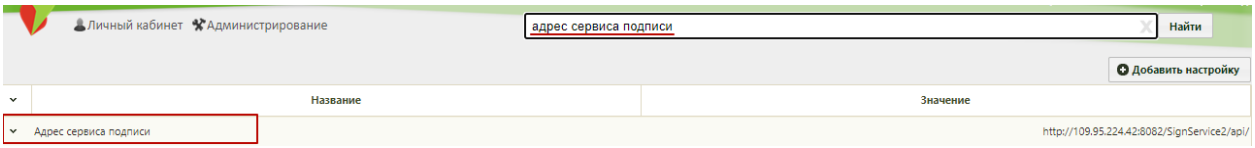

Рисунок 85. Поиск настройки «Адрес сервиса подписи»

Необходимо открыть настройку на редактирование, вызвав правой кнопкой мыши контекстное меню и выбрав в нем пункт «Редактировать» (Рисунок 86).

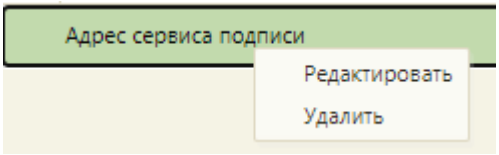

Рисунок 86. Открытие настройки на редактирование

Отобразится форма «Системная настройка» для настройки «Адрес сервиса подписи». Необходимо в поле «Тип данных» указать «Строковый», в поле «Значение» указать url-адрес сервиса, нажать кнопку «Сохранить» (Рисунок 87).

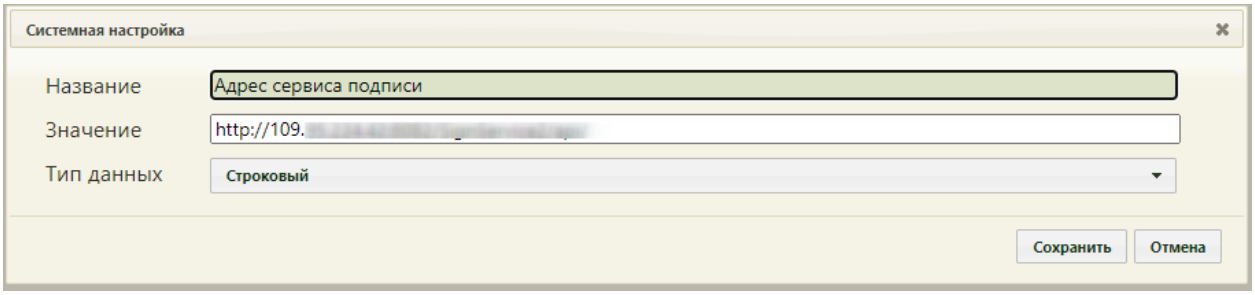

Рисунок 87. Системная настройка «Адрес сервиса подписи»

Форма настройки закроется. Настройка будет включена.

1.4.2.2 IBS: Номер сертификата ЛПУ

Настройка «IBS: Номер сертификата ЛПУ» задает номер сертификата ЛПУ. Данная настройка нужна для полноценной работы пользователя с модулем учета нетрудоспособности.

На странице раздела с системными настройками в поле поиска необходимо ввести наименование или часть наименования настройки «IBS: Номер сертификата ЛПУ», нажать кнопку «Найти» (Рисунок 88). Отобразится список настроек в соответствии с условием поиска.

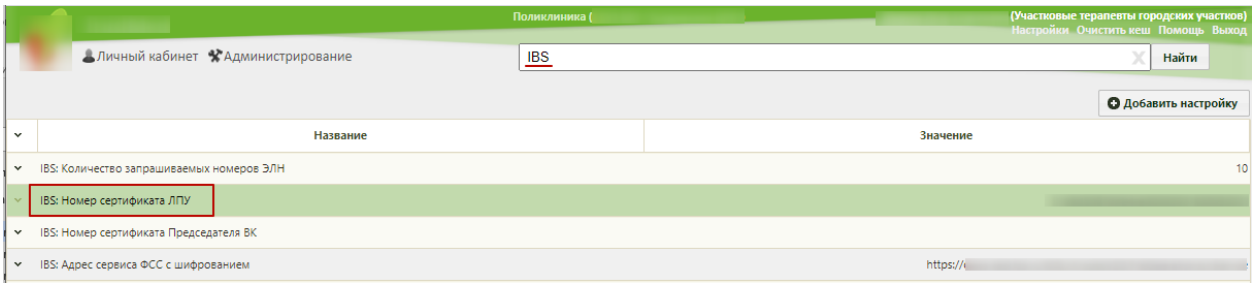

Рисунок 88. Поиск настройки «IBS: Номер сертификата ЛПУ»

Необходимо открыть настройку на редактирование, вызвав правой кнопкой мыши контекстное меню и выбрав в нем пункт «Редактировать» (Рисунок 89).

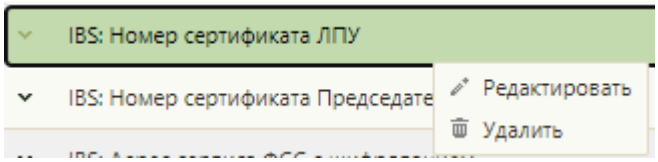

Рисунок 89. Открытие настройки на редактирование

Отобразится форма «Системная настройка» для настройки «IBS: Номер сертификата ЛПУ». Необходимо в поле «Тип данных» указать «Строковый», в поле «Значение» указать номер сертификата ЛПУ, нажать кнопку «Сохранить» (Рисунок 90).

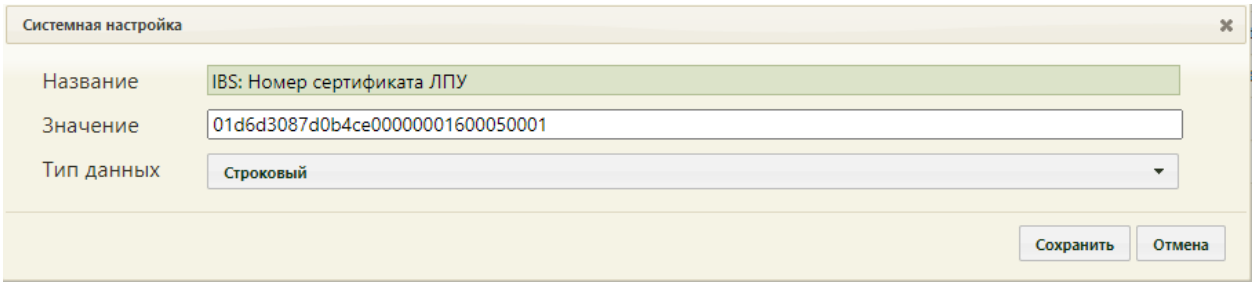

Рисунок 90. Системная настройка «IBS: Номер сертификата ЛПУ»

Форма настройки закроется. Настройка будет включена.

1.4.2.3 IBS: Номер сертификата уполномоченного лица

Настройка «IBS: Номер сертификата уполномоченного лица» задает номер сертификата уполномоченного лица. Данная настройка необходима для полноценной работы пользователя с модулем учета нетрудоспособности.

На странице раздела с системными настройками в поле поиска необходимо ввести наименование или часть наименования настройки «IBS: Номер сертификата уполномоченного лица», нажать кнопку «Найти» (Рисунок 91Рисунок 88). Отобразится список настроек в соответствии с условием поиска.

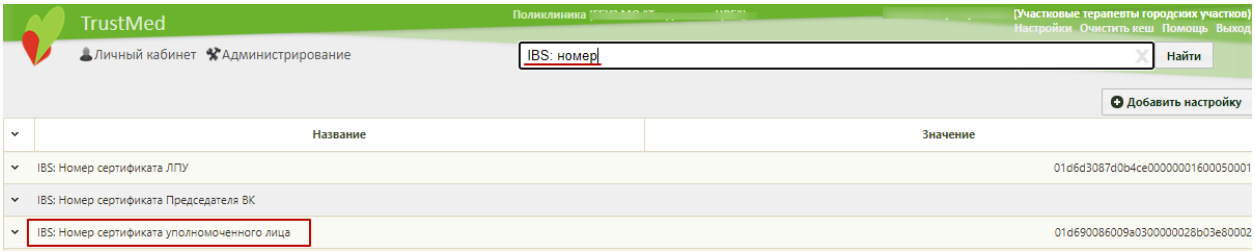

Рисунок 91. Поиск настройки «IBS: Номер сертификата уполномоченного лица»

Необходимо открыть настройку на редактирование, вызвав правой кнопкой мыши контекстное меню и выбрав в нем пункт «Редактировать» (Рисунок 92).

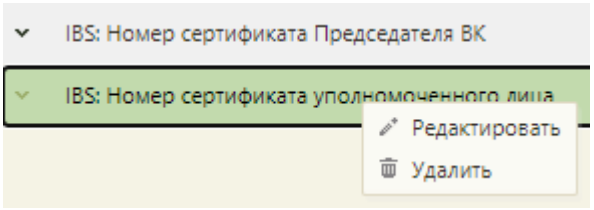

Рисунок 92. Открытие настройки на редактирование

Отобразится форма «Системная настройка» для настройки «IBS: Номер сертификата уполномоченного лица». Необходимо в поле «Тип данных» указать «Строковый», в поле «Значение» указать номер сертификата ЛПУ, нажать кнопку «Сохранить» (Рисунок 93).

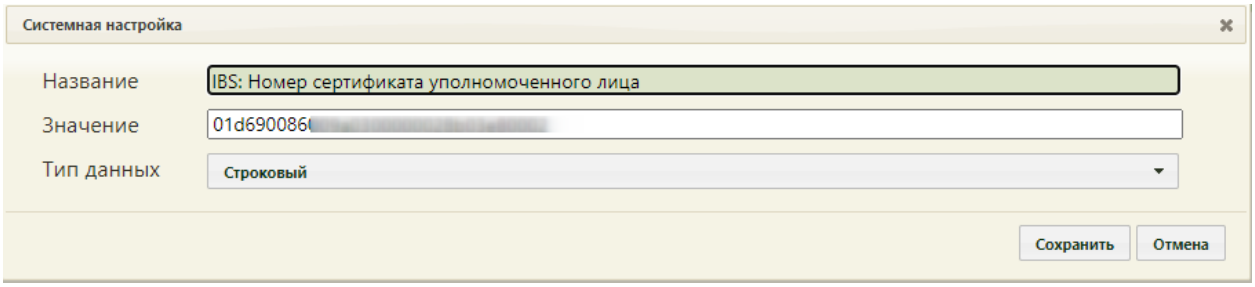

Рисунок 93. Системная настройка «IBS: Номер сертификата уполномоченного лица»

Форма настройки закроется. Настройка будет включена.

1.4.3 Настройка web-приложения через рабочее место врача

Для настройки «ТМ:МИС SaaS» необходимо авторизоваться в системе под пользователем, для которого будут выставляться настройки.

После авторизации необходимо нажать «Настройки» в правом верхнем углу страницы (Рисунок 94).

Рисунок 94. Раздел «Настройки»

После чего откроется окно «Пользовательские настройки» (Рисунок 95), в котором необходимо установить четыре настройки «Адрес сервиса подписи», «Номер сертификата пользователя подписи» и «ЭЛН: Режим работы с сервисом взаимодействия ФСС», «Режим подписи файлов для РЛДД».

В поле «Адрес сервиса подписи» указывается адрес, по которому развернут сервис подписи «адрес сервиса»+ «/api/» (например, http://192.168.7.135/api/). В конце адреса обязательно должен стоять символ «/».

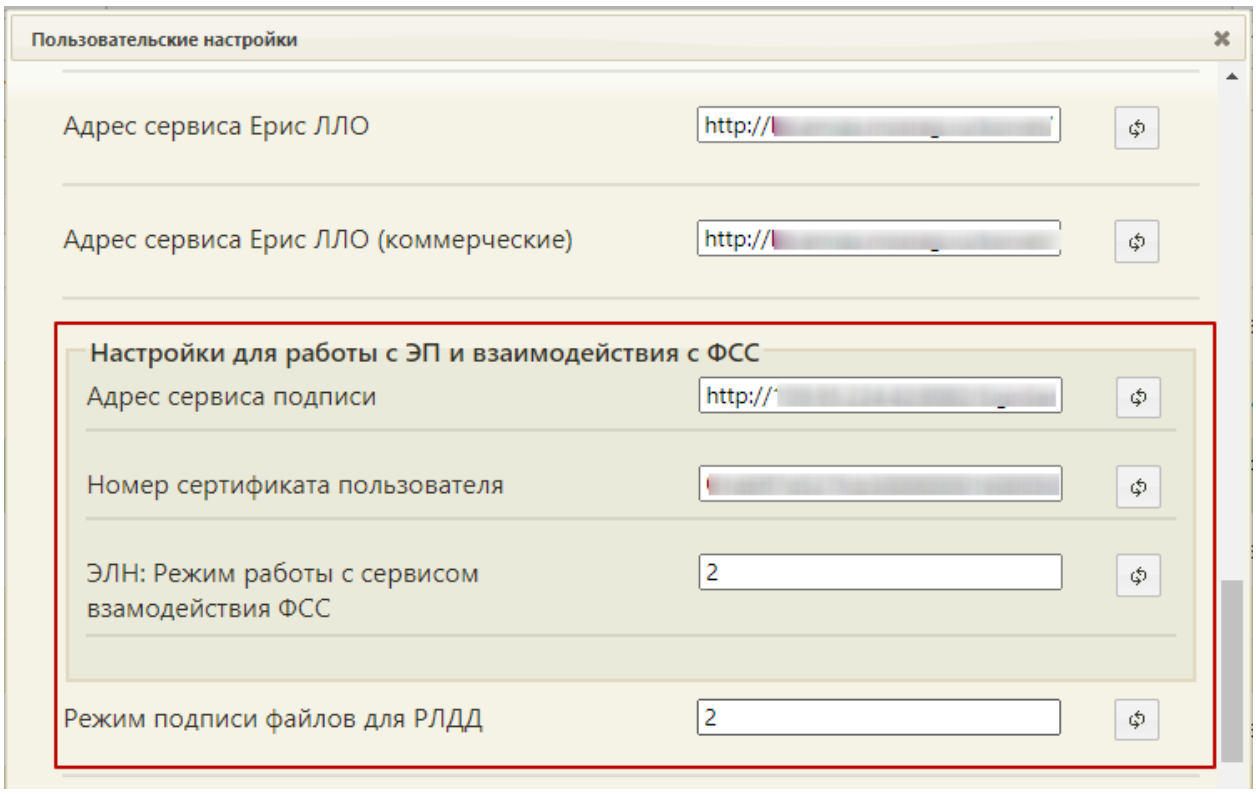

Рисунок 95. Окно «Пользовательские настройки»

В поле «Номер сертификата пользователя» необходимо указать значение серийного номера сертификата врача.

В случае если настройка «Номер сертификата пользователя подписи данных» не заполнена или указано «Все», для подписи будет предложен список всех доступных сертификатов текущего пользователя (Рисунок 96).

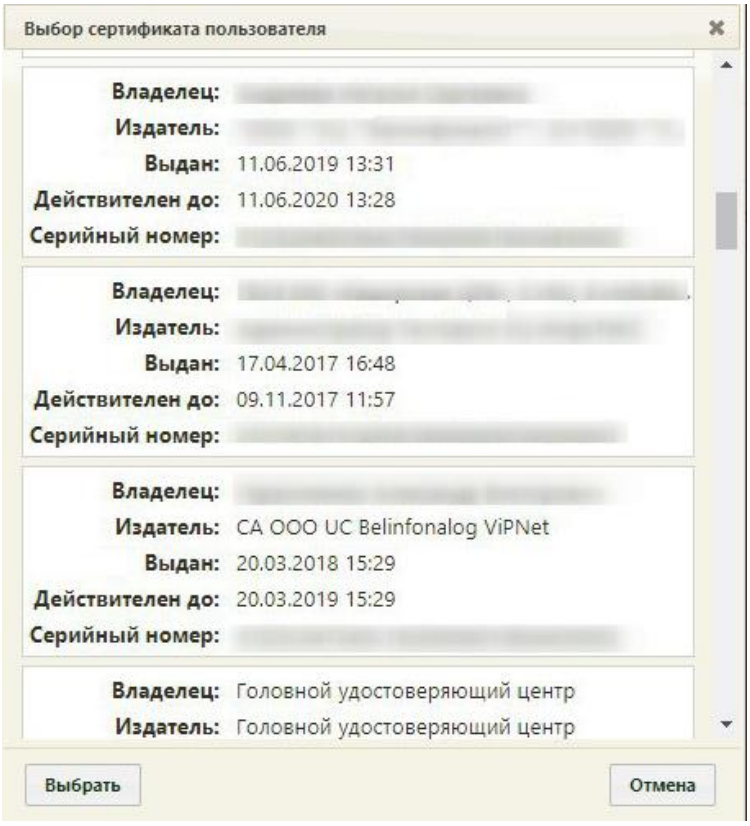

Рисунок 96. Просмотр сведений о сертификате

В настройках «ЭЛН: Режим работы с сервисом взаимодействия с внешними системами» и «Режим подписи файлов для РЛДД» следует установить режим работы «2».

После выставления настроек следует нажать кнопку «Сохранить».

2 ОБНОВЛЕНИЕ СЕРВИСА ПОДПИСИ

Для обновления сервисов необходимо перейти в папку, указанную при настройке сайта. По умолчанию, существующий сервис располагается в директории: C:\inetpub\wwwroot\FSS (Рисунок 97).

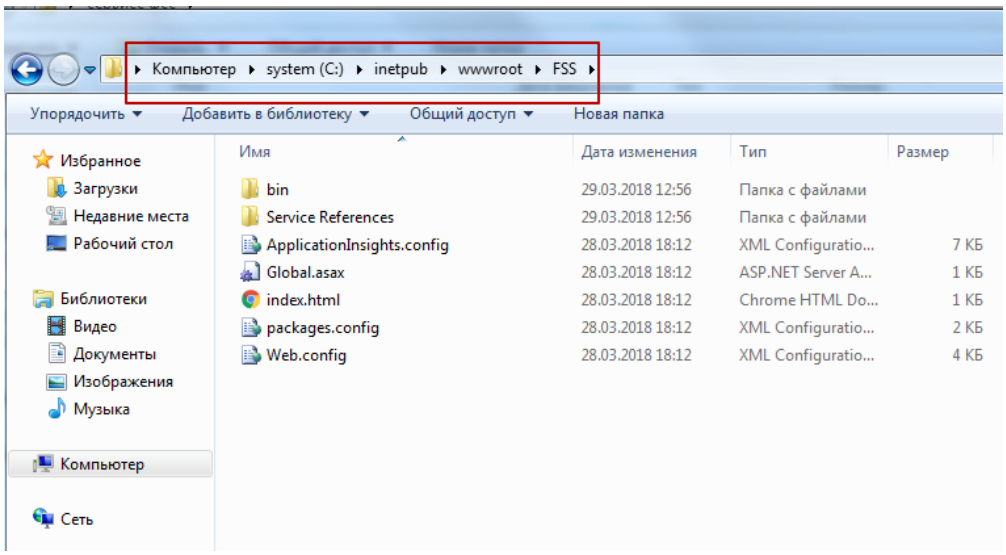

Рисунок 97. Директория сервиса

Если папке назначался путь не по умолчанию, то узнать, где именно находится сервис, можно при помощи консоли IIS. Для этого следует зайти в службы IIS, выбрав Панель управления – Администрирование – Диспетчер служб ISS. В результате откроется окно «Диспетчер служб IIS». Далее нужно найти необходимый сайт и во вкладке «Действия» нажать кнопку «Проводник» (Рисунок 98). Будет открыта папка с развёрнутым сервисом.

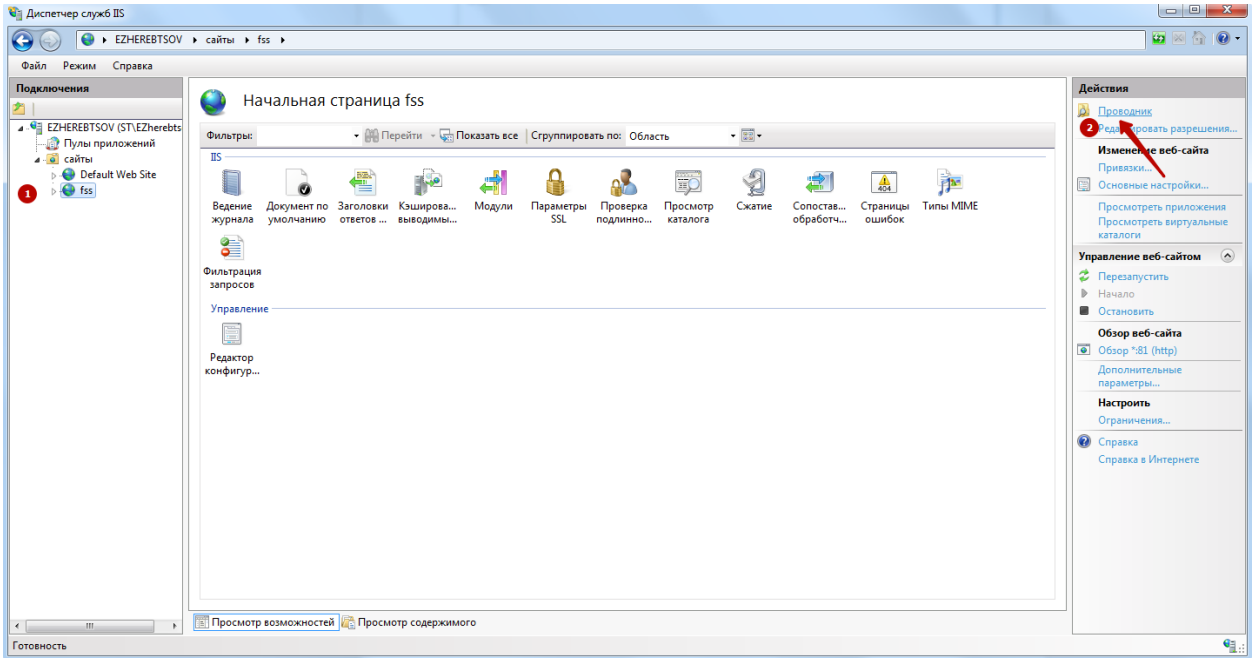

Рисунок 98. Консоль ISS

Для обновления необходимо удалить содержимое папки с устаревшей версией сервиса. Удалению подлежат все файлы в папке, кроме файла Web.config. После этого необходимо скопировать файлы сервиса новой версии и вставить их в исходную папку, не заменяя файл Web.config.