Установка средств криптографической защиты (СКЗИ)

Для работы с сертификатами и подписания отчетов ЭП необходимо установить одно из следующих средств криптографической защиты информации (СКЗИ): КриптоПро CSP, VipNet CSP, Signal-COM CSP, ЛИССИ-CSP.

В качестве СКЗИ рекомендуется использовать следующие СКЗИ:

1) КриптоПро CSP. Информацию о порядке приобретения КриптоПро CSP и инструкцию по установке можно получить на официальном сайте компании «Крипто-Про» http://www.cryptopro.ru/.

2) VipNet CSP. Информацию о порядке приобретения VipNet CSP и инструкцию по установке можно получить на официальном сайте компании «ИнфоТеКС» http://www.infotecs.ru/downloads.

3) Signal-COM CSP. Информацию о порядке приобретения Signal-COM CSP и инструкцию по установке можно получить на официальном сайте компании «Сигнал-КОМ» http://www.signal-com.ru/products/crypt/signal-com.

4) ЛИССИ-CSP. Информацию о порядке приобретения ЛИССИ-CSP и инструкцию по установке можно получить на официальном сайте компании «ЛИССИ-Софт» http://soft.lissi.ru/products/skzi/lissi-csp/.

Плагин подписи позволяет подписывать и выполнять проверку ЭП в операционных системах не ниже следующих версий:

- MacOS 10.14;
- Linux Ubuntu Bionic Beaver 18.04;
- Linux Debian 9.0 Stretch;
- Linux CentOS 8;
- ОС Windows 7.

Электронная подпись работает корректно в браузерах не ниже перечисленных версий:

- Google Chrome (версия не ниже 71);
- Mozilla Firefox (версия не ниже 67);
- Safari (версия не ниже 12);
- Opera 78.

Получение закрытого ключа и сертификата открытого ключа электронной подписи

В целях обеспечения безопасности и достоверности статистической отчетности, формируемой и отсылаемой организацией, в т.ч. уполномоченным лицом в процессе электронного сбора статистической отчетности, все отчеты, перед оправкой в ТОГС, должны быть подписаны электронной подписью (ЭП) организации.

Для предоставления статистической отчетности в электронном виде необходимо получить:

– закрытый ключ, при помощи которого будет формироваться ЭП и который будет гарантировать подлинность заполнения и предоставления отчетов организацией;

– сертификат открытого ключа организации, который необходимо передать в ТОГС, для осуществления проверки подлинности отчетности, присланной организацией.

Порядок получения закрытого ключа и сертификата открытого ключа выглядит следующим образом:

1) Индивидуальные предприниматели, юридические лица и нотариусы могут сделать электронную подпись бесплатно в ФНС России.

2) ЭП можно получить платно в любом из аккредитованных УЦ.

3) Информация по порядку получения ключа ЭП размещена на сайте выбранного УЦ.

4) После получения закрытого ключа и сертификата открытого ключа ЭП в одном из доверенных УЦ необходимо установить сертификат закрытого ключа в системное хранилище сертификатов на компьютере, где планируется использование ON-line модуля или хранить на ключевом носителе.

5) Сертификат открытого ключа ЭП необходимо загрузить в ON-line-модуль при регистрации или загрузить позднее в разделе «Профиль» списка «Сертификаты» перед отправкой первого отчета. При помощи данного сертификата будет осуществляться проверка подлинности отчетов, полученных от организации.

Установка сертификата, полученного в ФНС России

Полученную в ФНС России электронную подпись, необходимо извлечь из ключевого контейнера средствами КриптоПро CSP. Для этого требуется выполнить следующие действия:

1) Запустить КриптоПРО CSP (Рисунок 1):

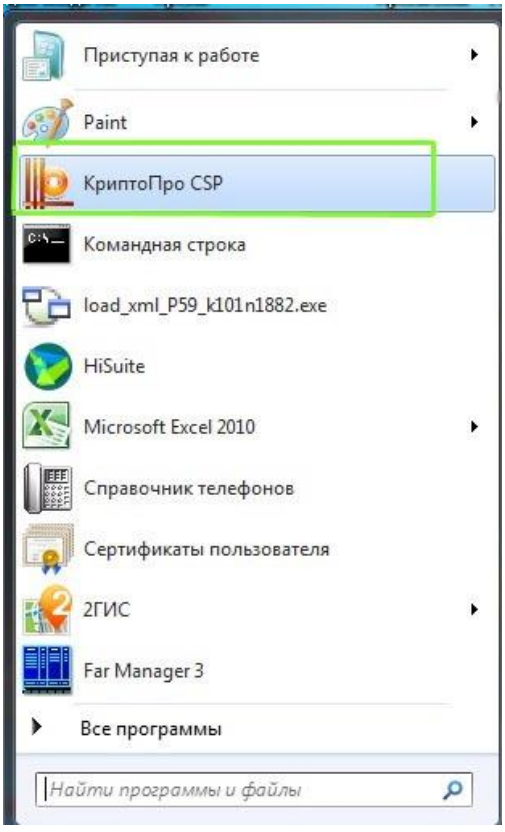

Рисунок 1 –Запуск КриптоПро CSP

2) В открывшемся окне перейти на вкладку «Сервис» (Рисунок 2):

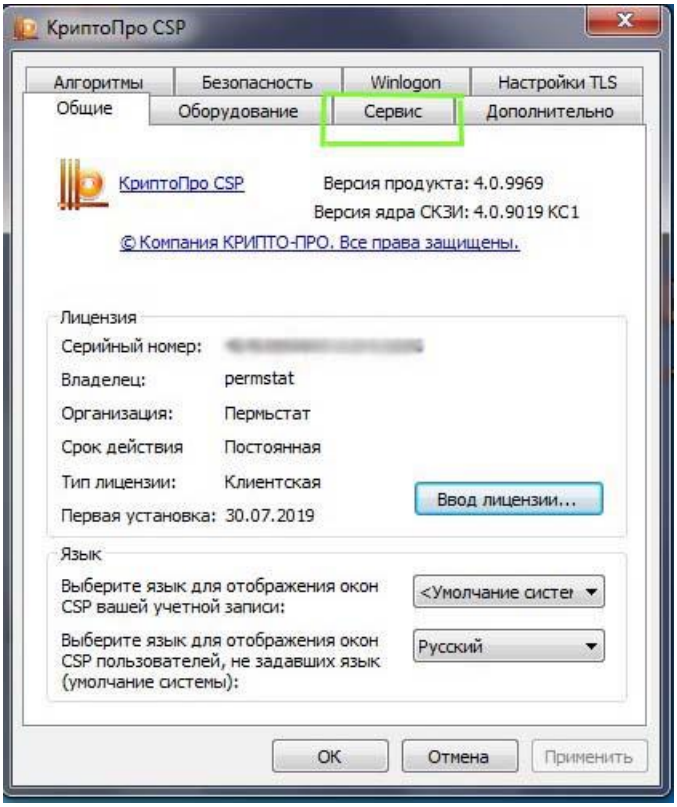

Рисунок 2 – Переход на вкладку «Сервис»

3) Нажать кнопку «Просмотреть сертификаты в контейнере» (Рисунок 3):

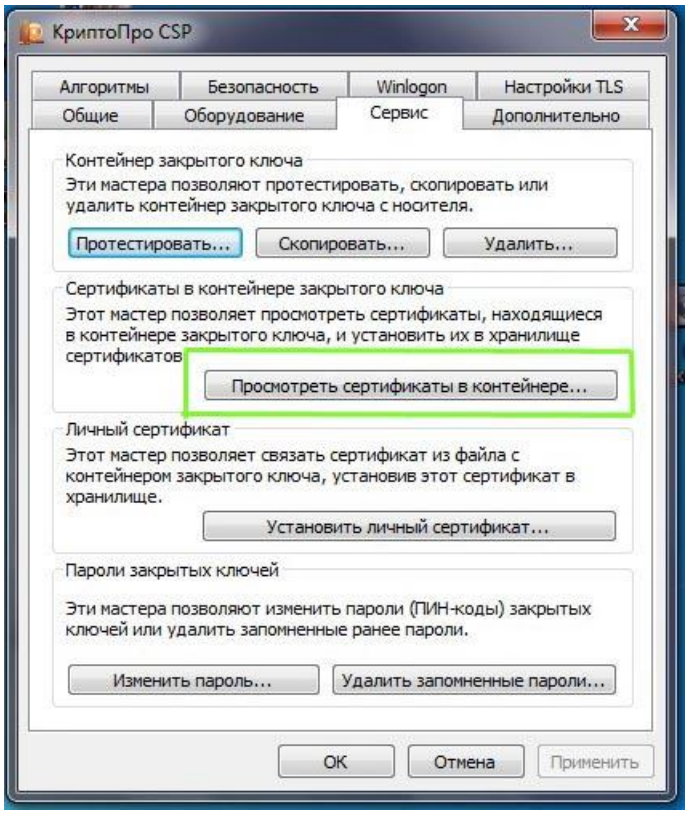

Рисунок 3 – Кнопка «Просмотреть сертификаты в контейнере»

4) В открывшемся окне выбрать кнопку «Обзор»:

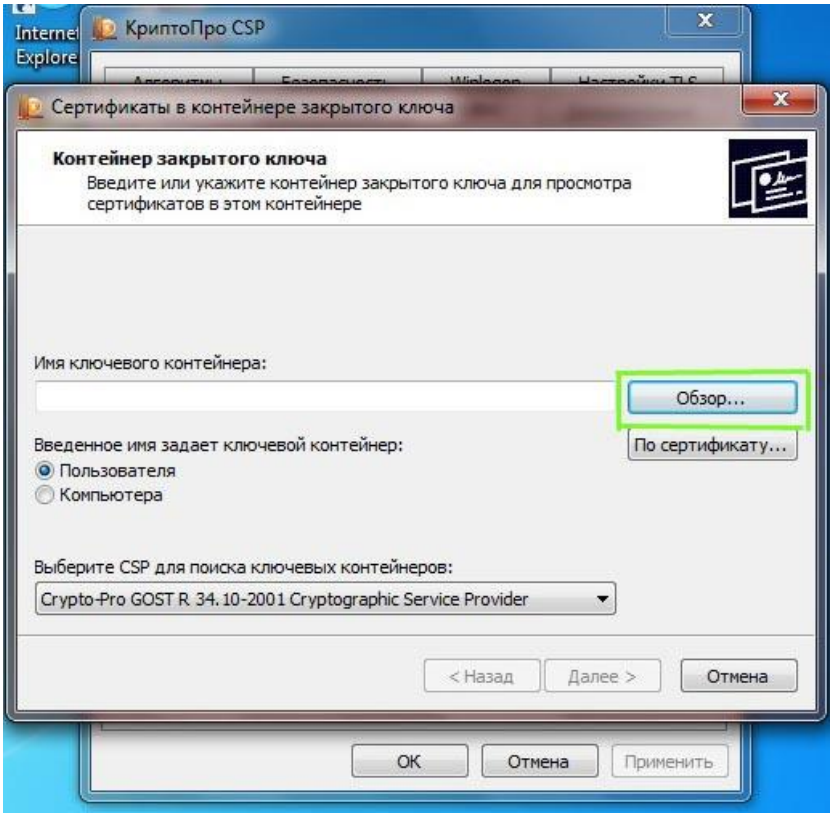

Рисунок 4 – Выбор кнопки «Обзор»

5) В окне выбрать контейнер и нажать «ОК» (Рисунок 5):

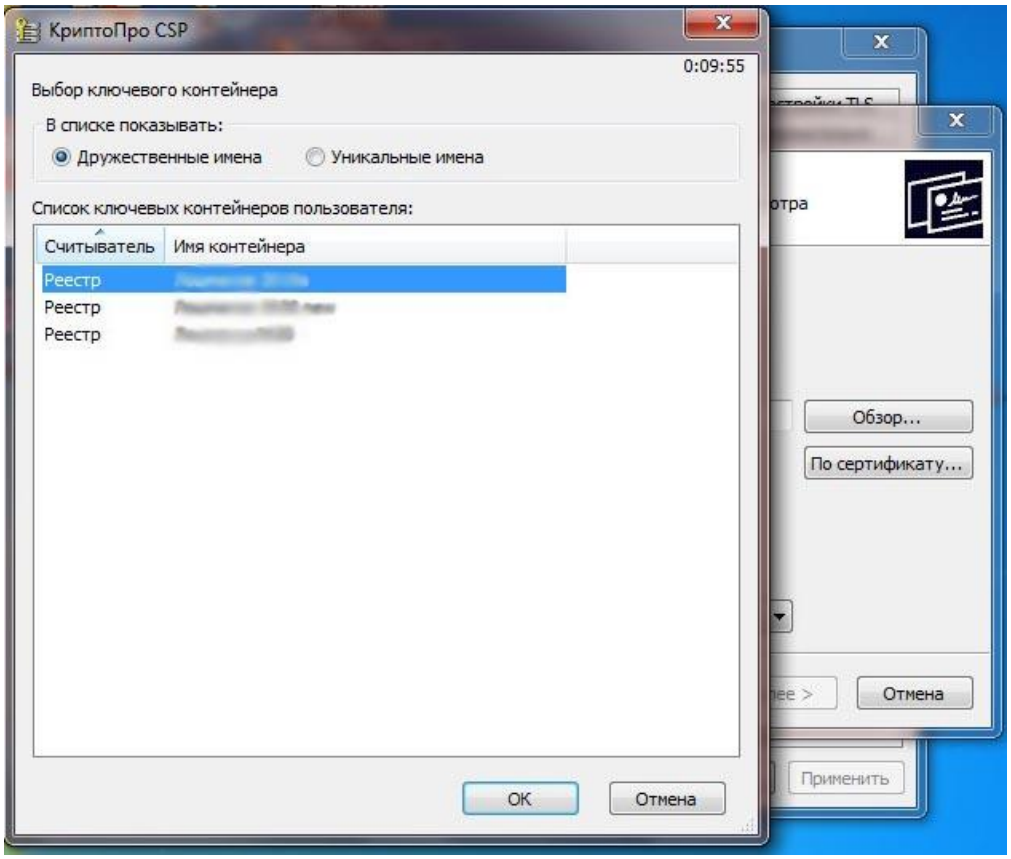

Рисунок 5 – Выбор контейнера

6) После выбора контейнера нажать кнопку «Далее» (Рисунок 6):

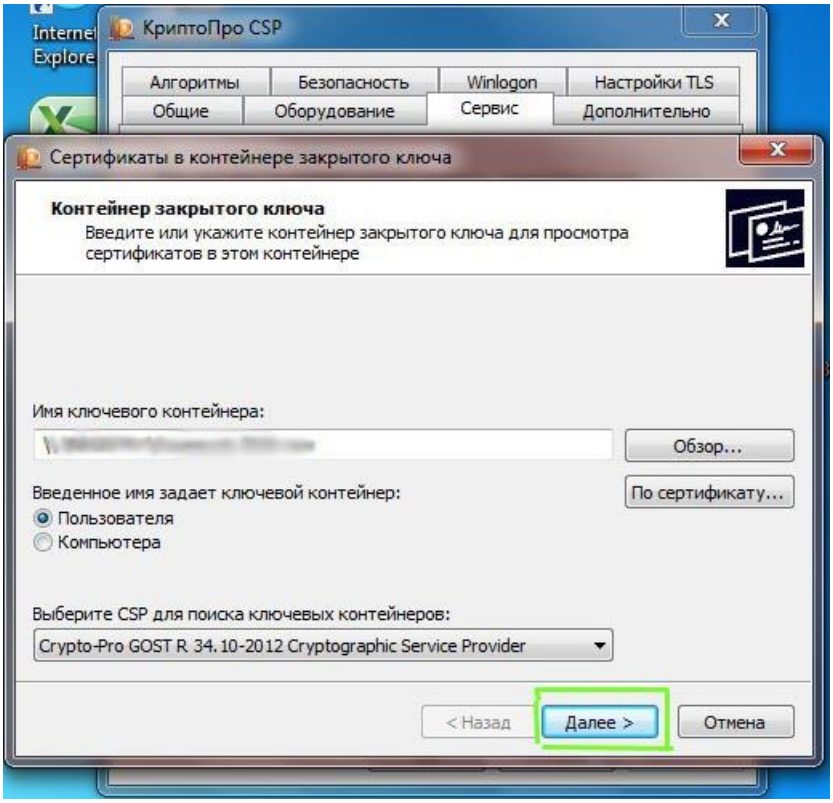

Рисунок 6 – Переход к следующему шагу

7) В окне «Сертификат для просмотра» нажать кнопку «Свойства» (Рисунок 7):

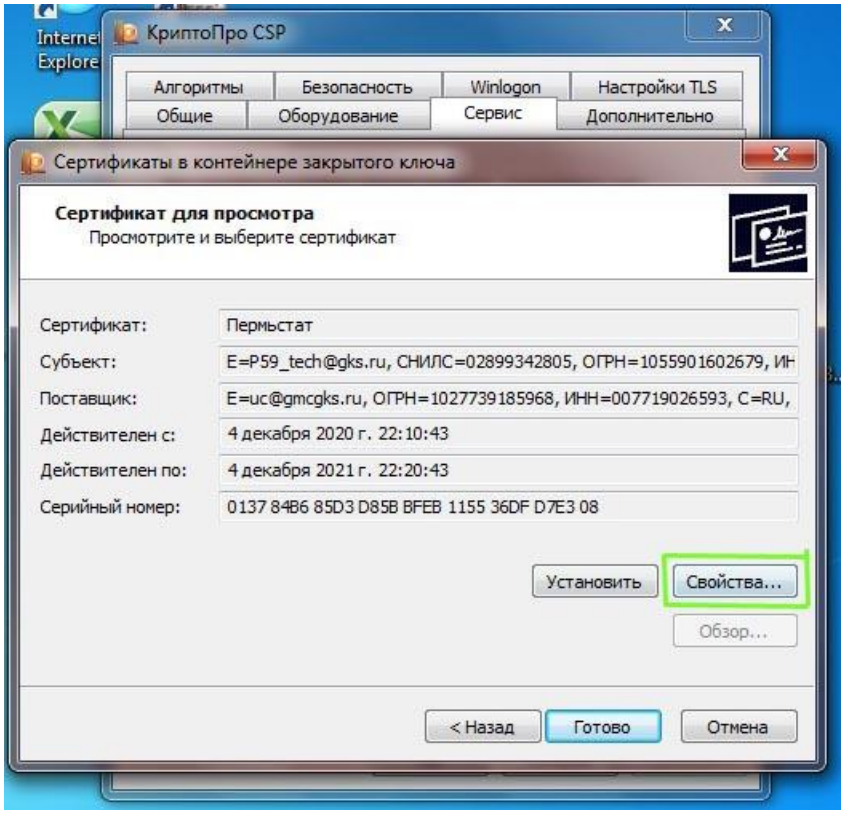

Рисунок 7 – Окно «Сертификат для просмотра»

8) В открывшемся окне «Сведения о сертификате» перейти на вкладку «Состав»:

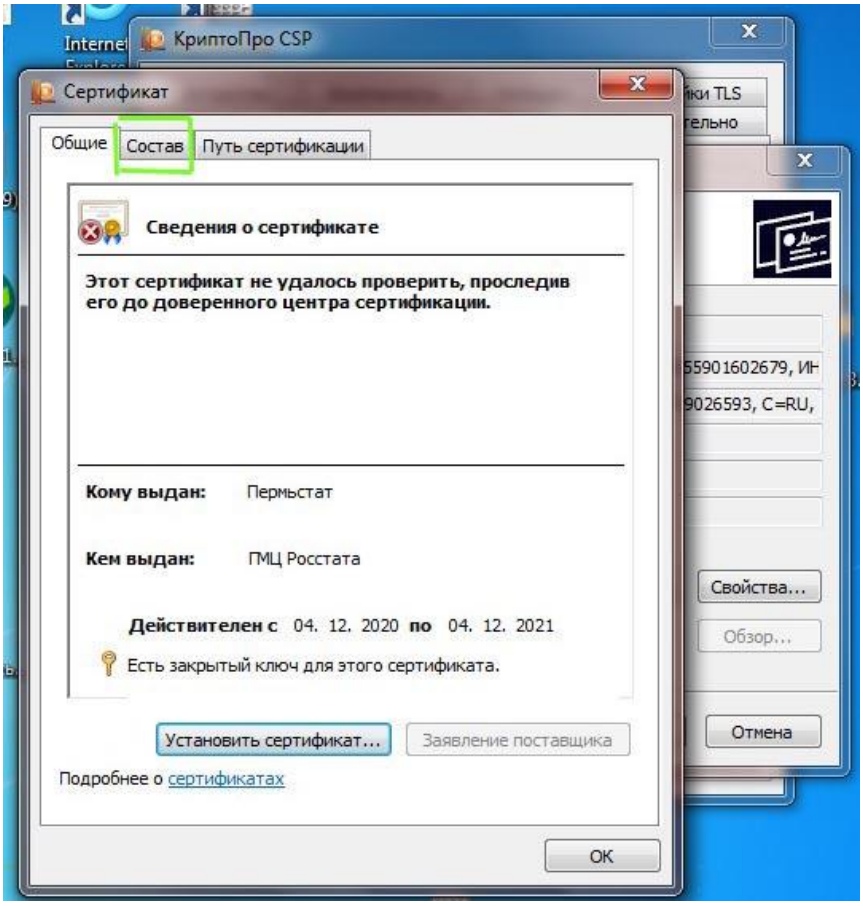

Рисунок 8 – Переход на вкладку «Состав»

9) На вкладке «Состав» нажать кнопку «Копировать в файл» (Рисунок 9):

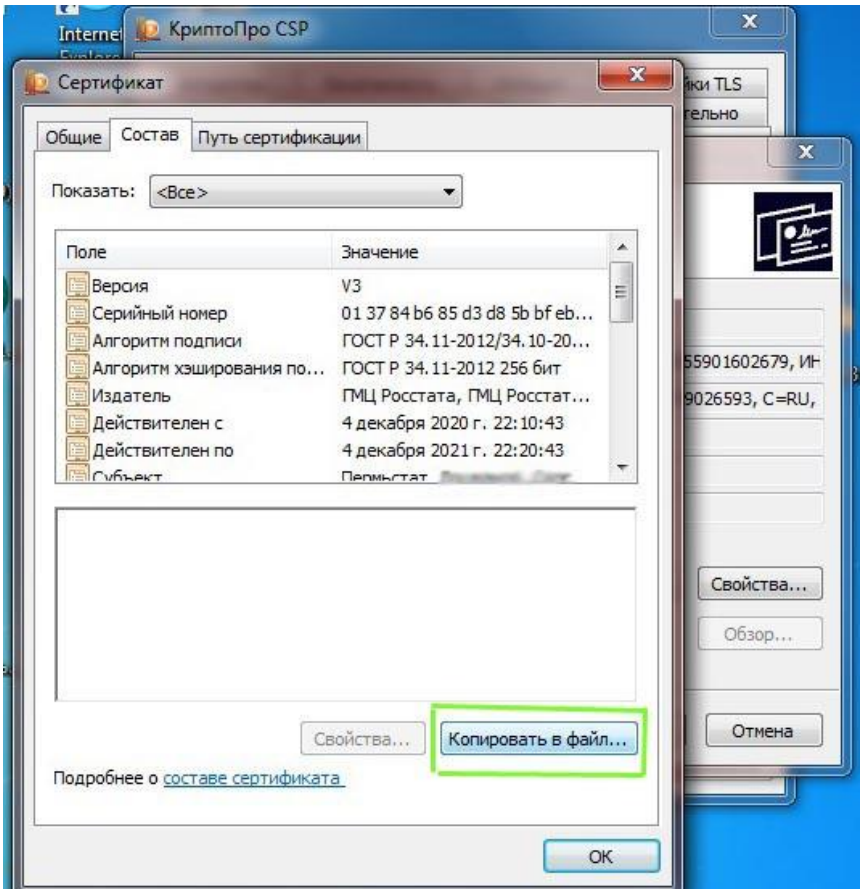

Рисунок 9 – Выбор кнопки «Копировать в файл»

10) В открывшемся окне «Мастер экспорта сертификатов» нажать кнопку «Далее» (Рисунок 10):

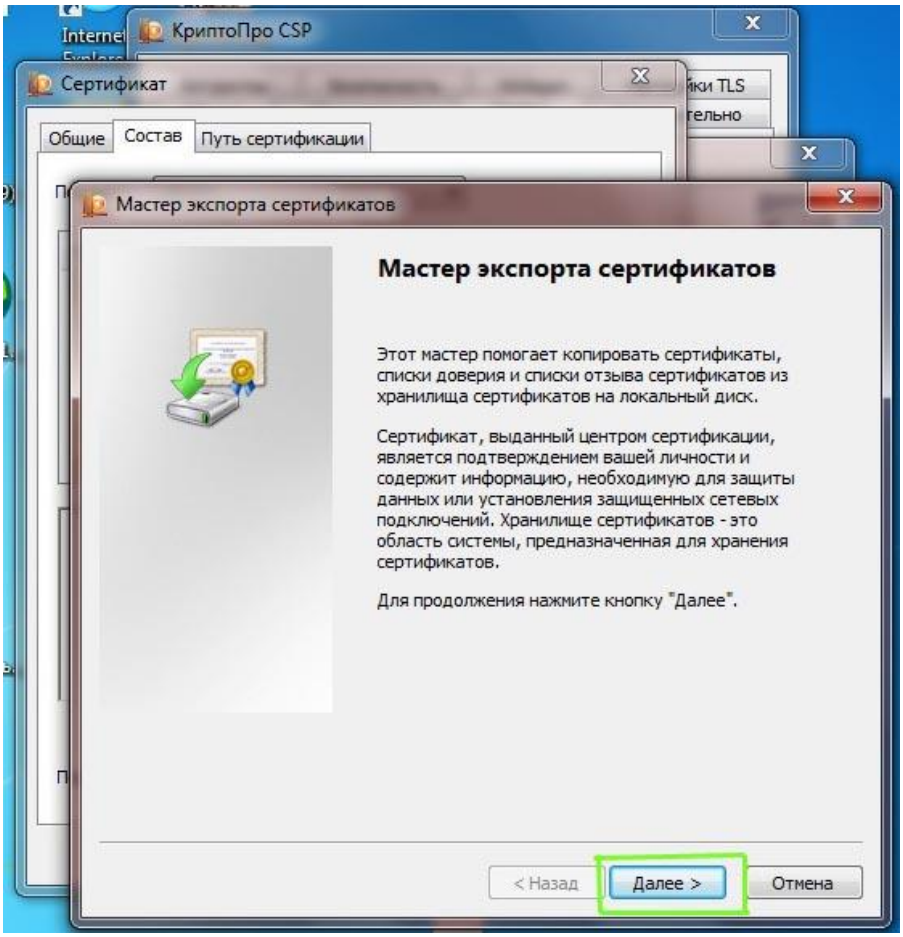

Рисунок 10 – Окно «Мастер экспорта сертификатов»

11) В следующем окне выбрать параметр «Нет, не экспортировать закрытый ключ» и нажать «Далее»:

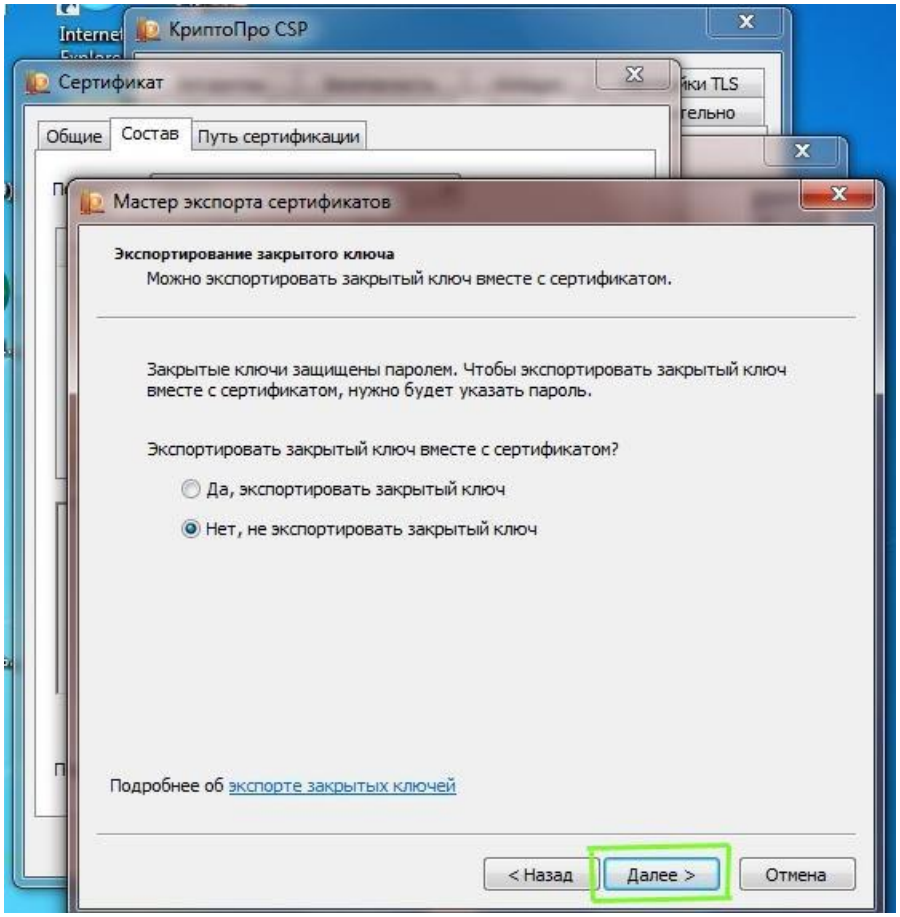

Рисунок 11 – Выбор параметра «Нет, не экспортировать закрытый ключ»

12) В следующем окне выбрать параметр «Файлы X.509 (.CER) в кодировке DER» и нажать кнопку «Далее» (Рисунок 12):

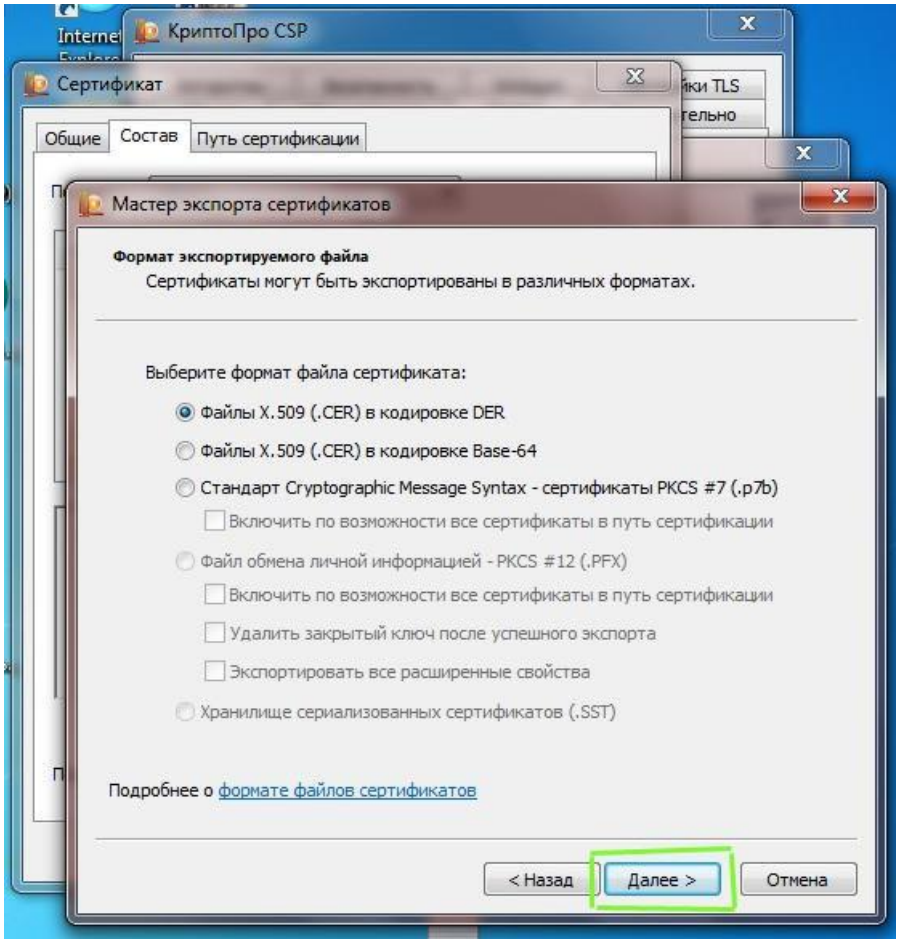

Рисунок 12 - Выбор параметра «Файлы X.509 (.CER) в кодировке DER»

13) В открывшемся окне «Имя экспортируемого файла» нажать кнопку «Обзор» (Рисунок 13):

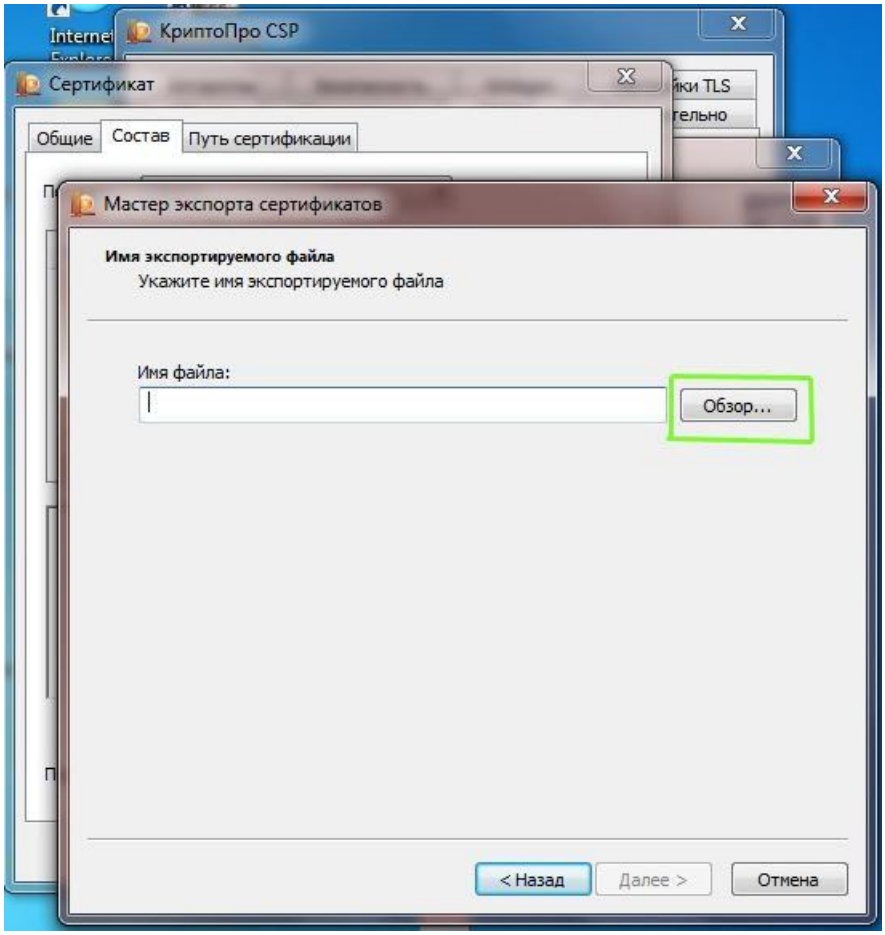

Рисунок 13 – Окно «Имя экспортируемого файла»

14) В открывшемся окне «Сохранить как» выбрать путь для сохранения файла и в поле «Имя файла» ввести любое имя для сохраняемого файла и нажать кнопку «Сохранить» (Рисунок 14):

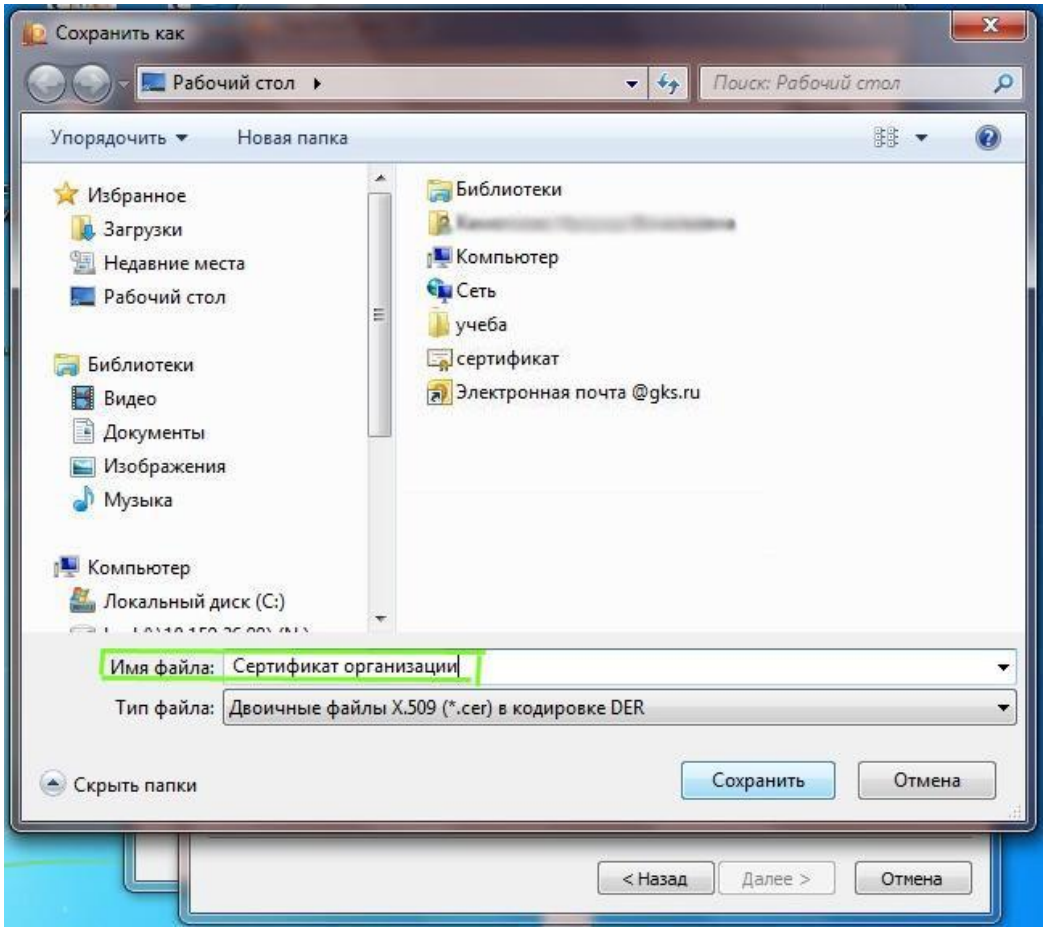

Рисунок 14 – Ввод названия сертификата

15) Для перехода к следующему шагу нажать кнопку «Далее» (Рисунок 15):

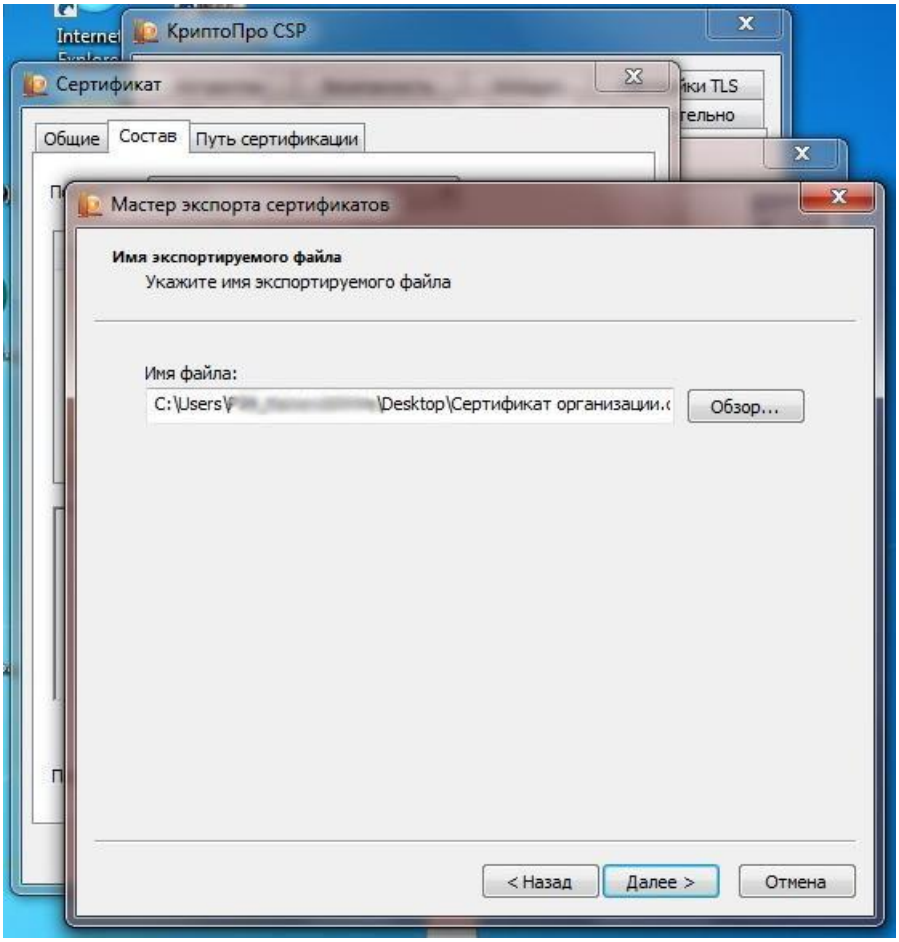

Рисунок 15- Переход к следующему шагу

16) Для завершения установки сертификата, необходимо нажать кнопку «Готово»:

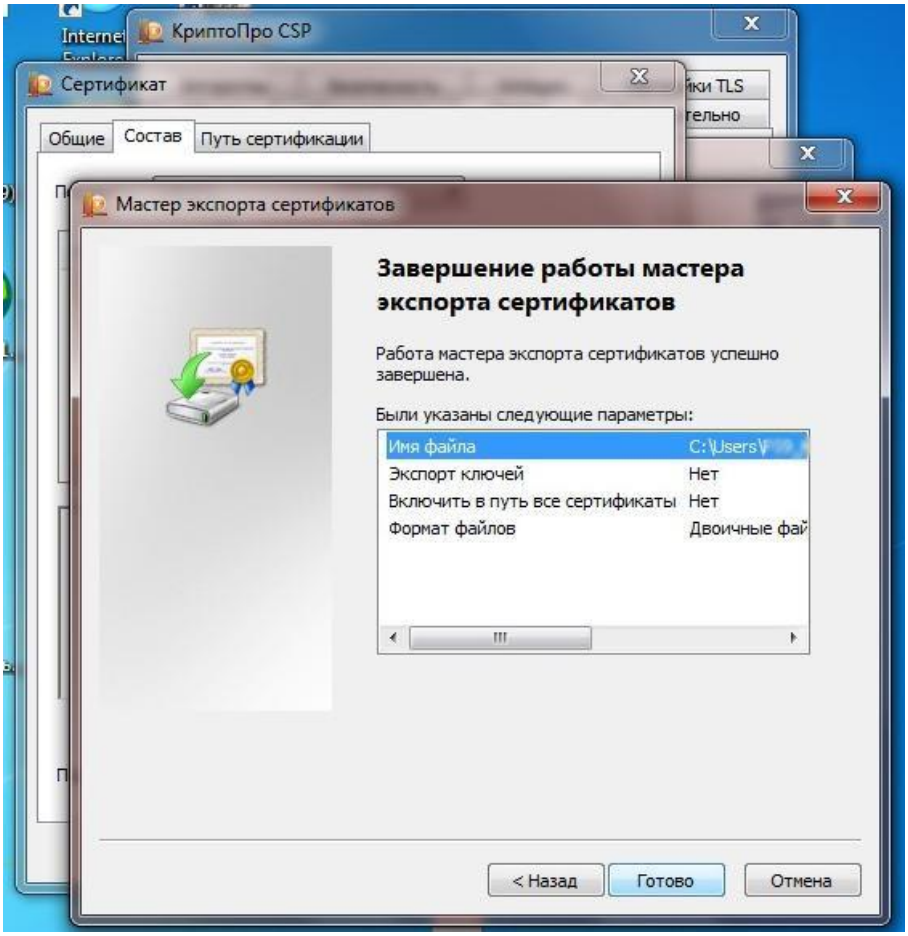

Рисунок 16 – Завершение работы мастера экспорта сертификатов

17) На экране появится сообщение об успешном экспорте. Для закрытия окна трбуется нажать кнопку «ОК» (Рисунок 17):

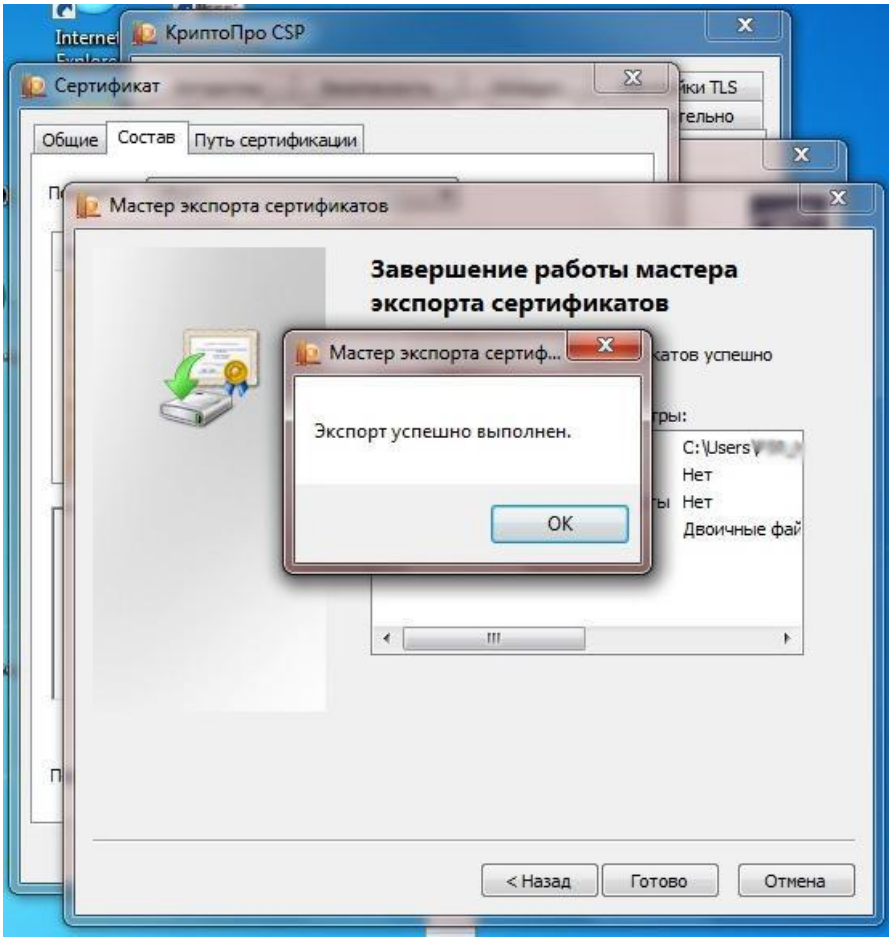

Рисунок 17 – Закрытие мастера установки сертификатов

18) Результатом работы мастера установки сертификатов является файл с расширением.cer, доступный в директории, заданной на шаге 14).

Установка сертификатов в системное хранилище

В данном разделе описан механизм установки сертификатов, которые являются секретными ключами на ключевых носителях и необходимы для реализации функционала проверки подлинности документов.

1) Запустить КриптоПро CSP.
2) Перейти на вкладку «Сервис».

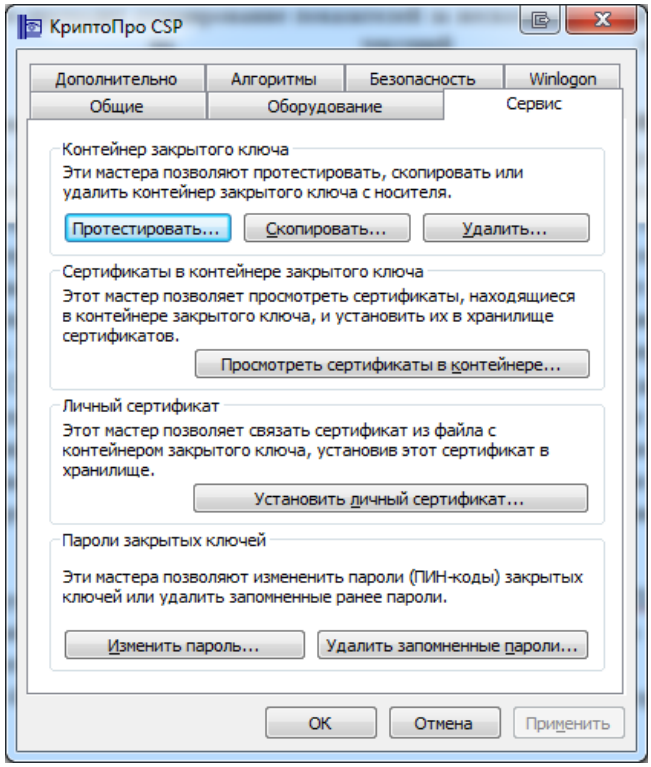

Рисунок 18 – Закладка «Сервис»

3) Нажать на кнопку «Просмотреть сертификаты в контейнеры».

4) В открывшемся окне нажать на кнопку «Обзор». Откроется список ключевых контейнеров.

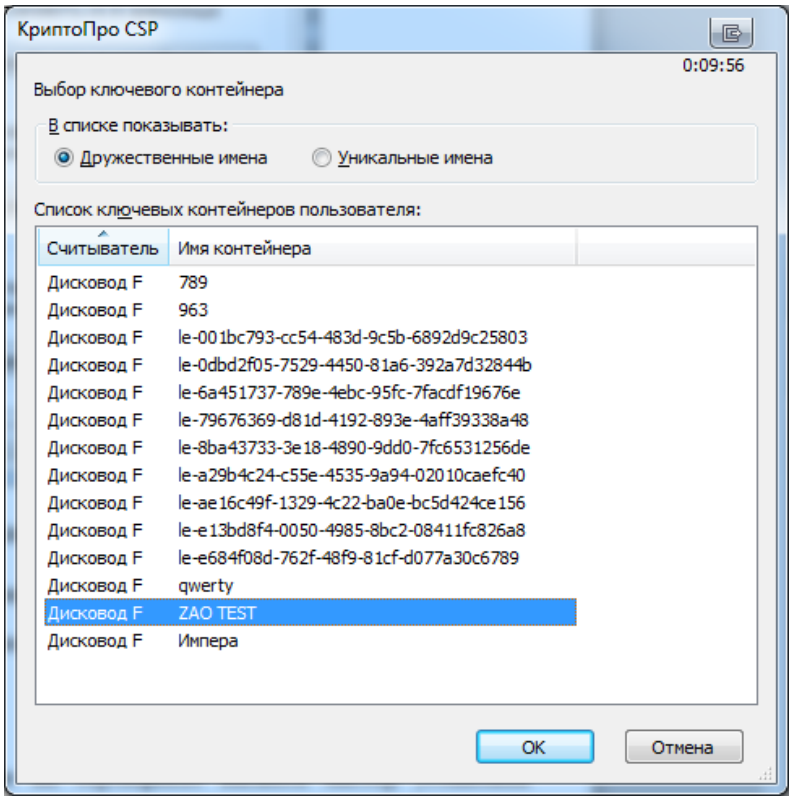

Рисунок 19 – Список контейнеров

5) Выбрать необходимый контейнер и нажать на кнопку «OK».

6) В результате в поле «Имя ключевого контейнера» отобразится наименование контейнера.

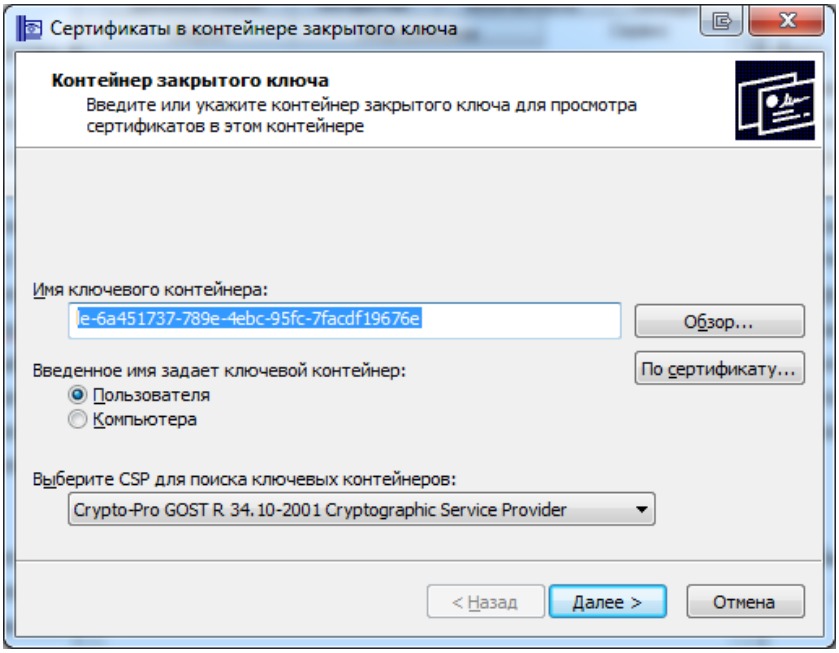

Рисунок 20 – Выбранный контейнер

7) Нажать на кнопку «Далее».

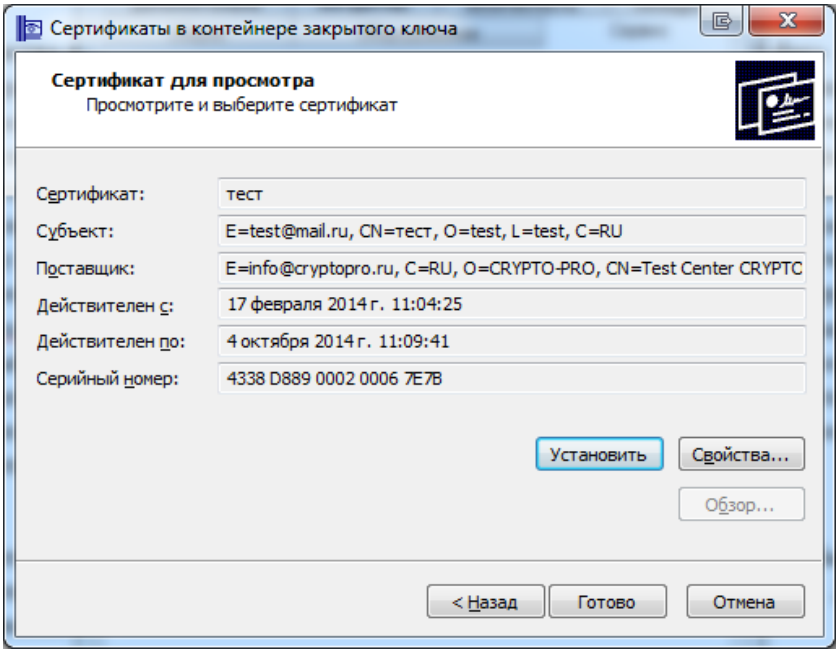

Рисунок 21 – Сведения о сертификате

8) Нажать на кнопку «Готово».

9) Сертификат будет установлен.

Вызвать мастер установки сертификата можно двойным нажатием левой кнопки мыши на сертификат (Рисунок 22).

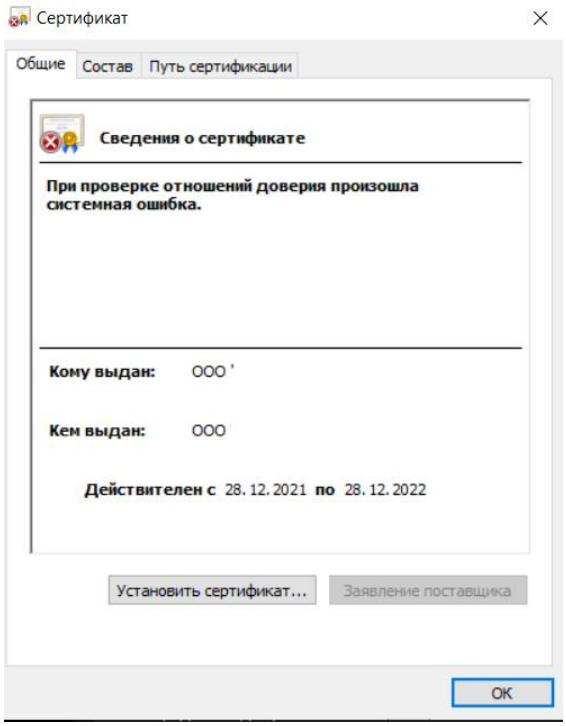

Рисунок 22 – Установка сертификата

В открывшемся окне нажать кнопку «Установить сертификат». Откроется окно «Мастер импорта сертификатов» в котором необходимо нажать кнопку «Далее» (Рисунок 23).

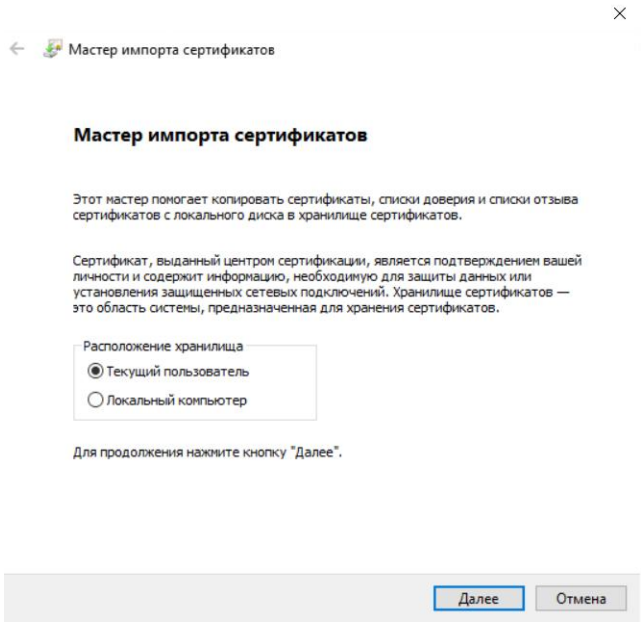

Рисунок 23 – Мастер установки сертификата

Для указания имени хранилища сертификатов нажать кнопку «Обзор» (Рисунок 24).

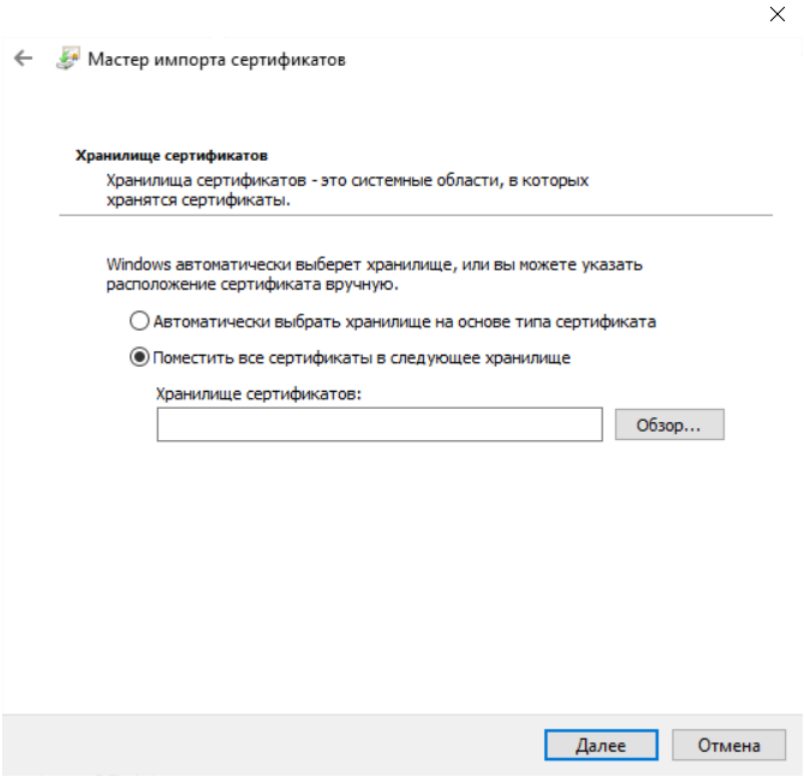

Рисунок 24 – Установка в хранилище текущего пользователя

В открывшемся окне выбрать «Выбор хранилища сертификатов» выбрать «Личное» и нажать кнопку «OK» (Рисунок 25).

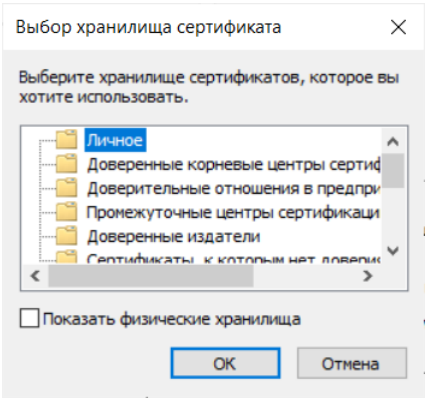

Рисунок 25 – Выбор хранилища «Личное»

В следующем окне нажать кнопку «Далее» (Рисунок 26).

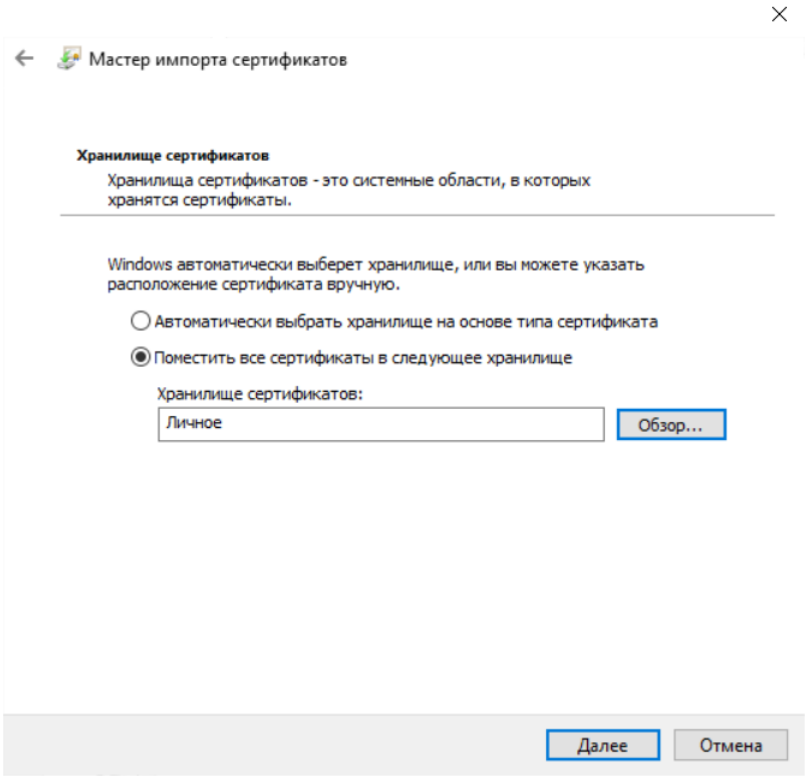

Рисунок 26- Переход к следующему шагу установки сертификата

Процесс установки сертификата завершен. Для закрытия мастера установки необходимо нажать кнопку «Готов» (Рисунок 27).

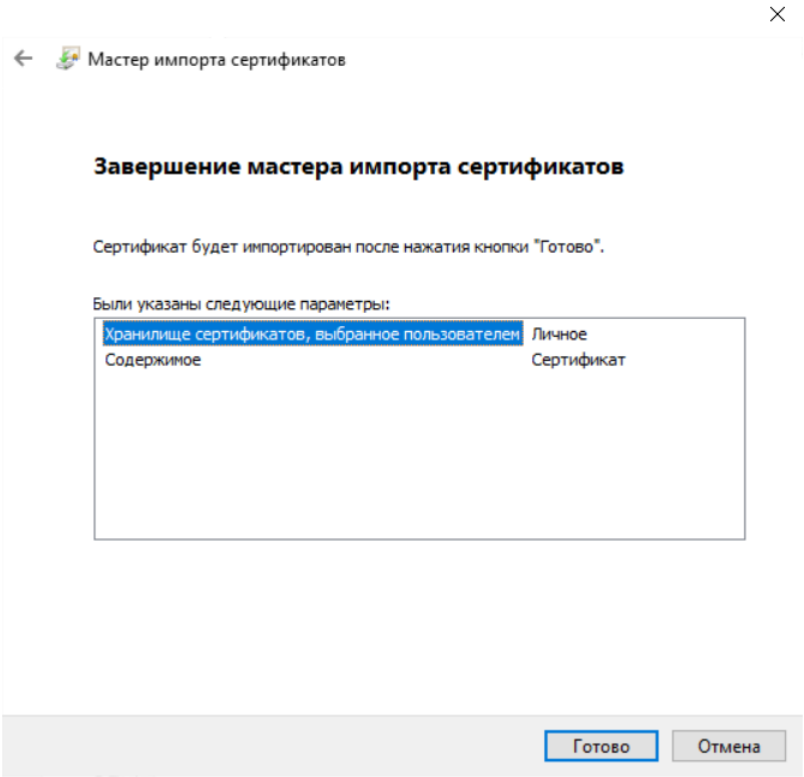

Рисунок 27 – Установка сертификата завершена

Работа с ключами на ключевых носителях

Обеспечение доступности секретного ключа сертификата в *КриптоПро CSP:*

1) Вставить флэш-диск в компьютер и посмотреть под какой буквой подключился диск.

2) Удостовериться, добавлен ли данный диск в КриптоПро как ключевой носитель. Для этого необходимо выполнить команду «Пуск» → «Все программы» → «CryptoPro» → «КриптоПро CSP» и перейти на закладку «Оборудование» и нажать кнопку «Настроить считыватели».

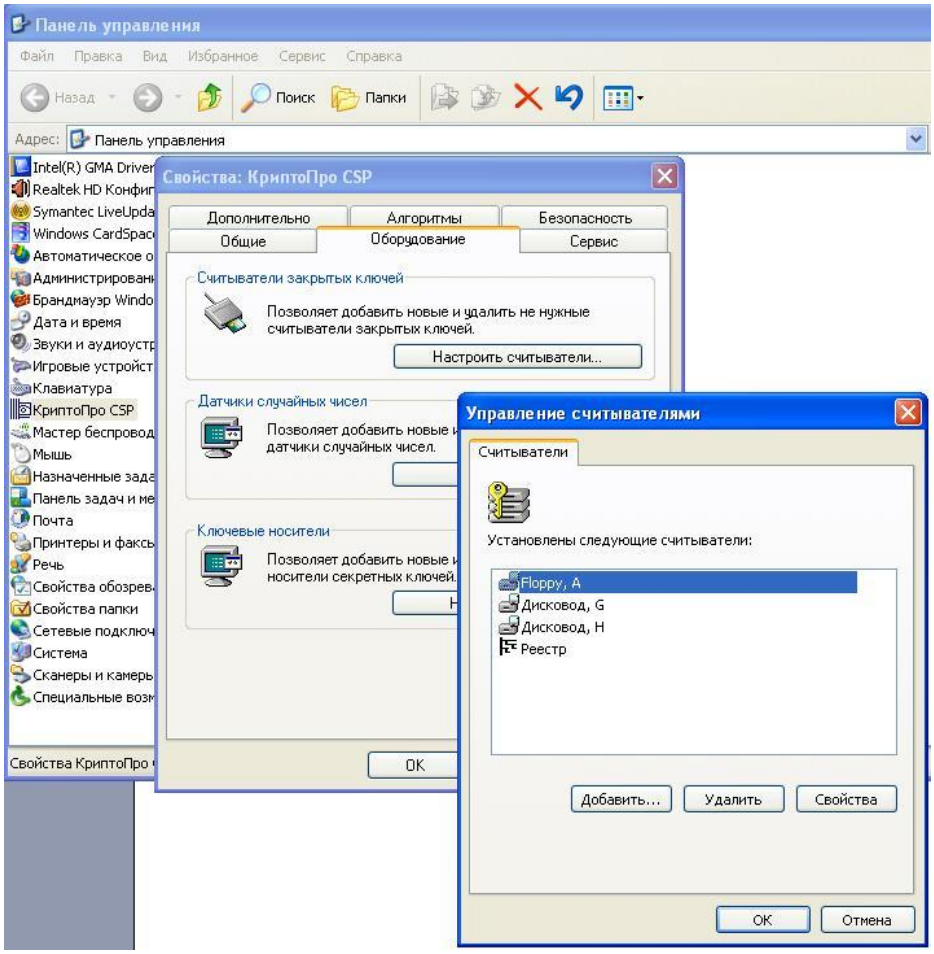

Рисунок 28 – Проверка ключевого носителя

В списке «Установлены следующие считыватели» должен присутствовать дисковод с именем подключенного диска.

3) Если дисковода с таким именем в списке нет, то его следует добавить, нажав кнопку «Добавить…». Начнет работать мастер установки считывателя. В первом окне мастера установки считывателя необходимо нажать кнопку «Далее >». Откроется окно для выбора считывателя.

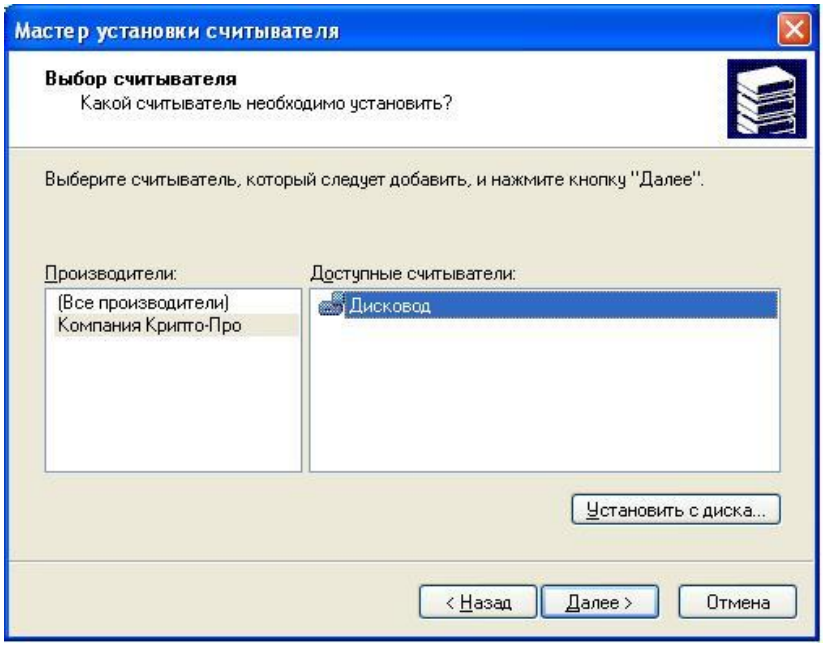

Рисунок 29 – Выбор считывателя

4) В списке «Производители» выбрать «Компания КриптоПро», а в Списке «Доступные считыватели» выбрать «Дисковод» и нажать кнопку «Далее >». Откроется окно выбора соединения (Рисунок 30).

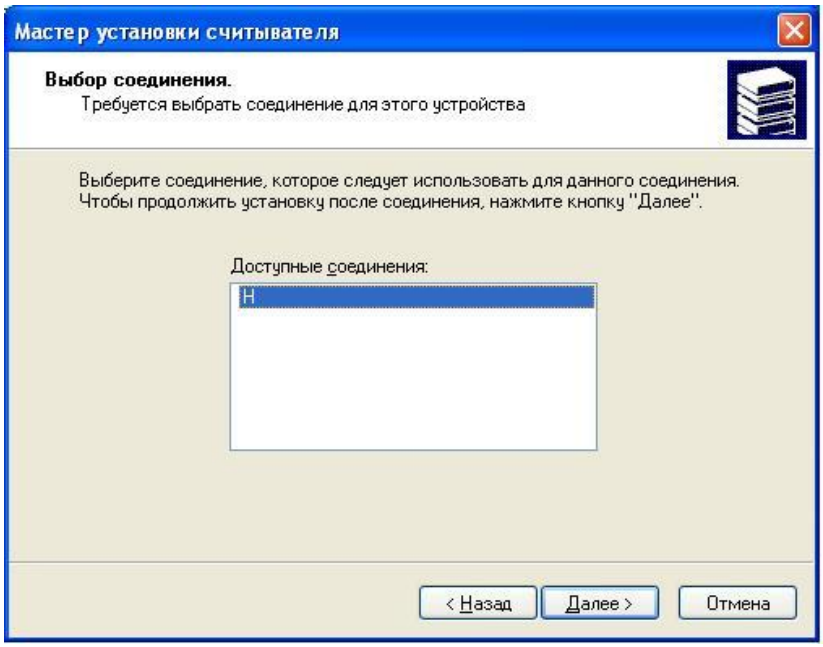

Рисунок 30 – Выбор соединения

5) В списке «Доступные соединения» выбрать название (букву) флеш-диска, подключенного к системе, и нажать кнопку «Далее >». Откроется окно «Имя считывателя».

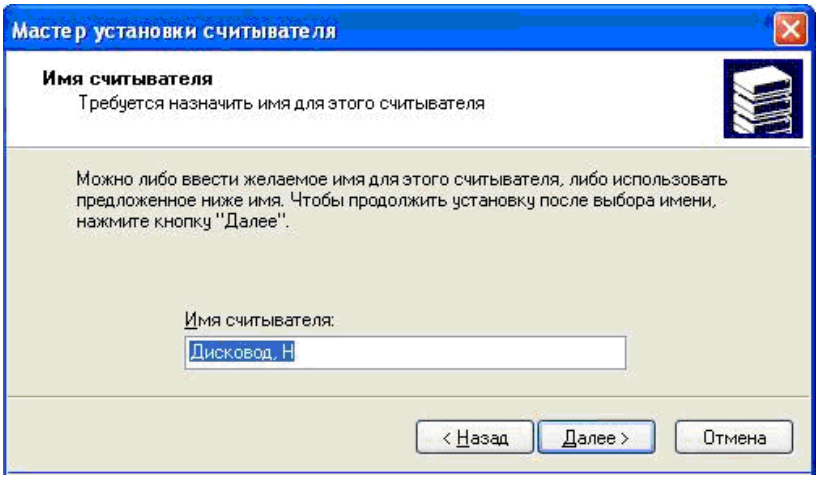

Рисунок 31 – Выбор имени считывателя

6) В случае необходимости изменить «Имя считывателя» и нажать кнопку «Далее >». Откроется окно завершения работы мастера установки считывателя.

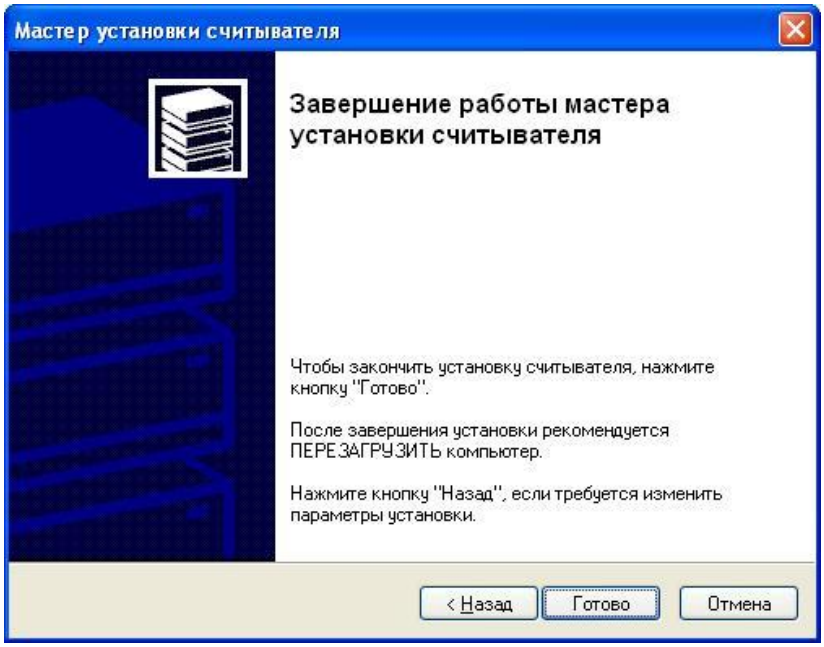

Рисунок 32 – Окно завершения работы мастера установки считывателя

7) Для завершения установки необходимо закрыть окно по кнопке «Готово».

Обеспечение доступности секретного ключа сертификата в VipNet CSP:

1) Вставить флэш-диск в компьютер и посмотреть, под какой буквой подключился диск.

2) Удостовериться, добавлен ли данный диск в ViPNet как ключевой носитель. Для этого необходимо выполнить команду «Пуск» → «Все программы» → «ViPNet» → «ViPNet CSP».

3) В окне программы ViPNet CSP выбрать раздел «Контейнеры» (Рисунок 33).

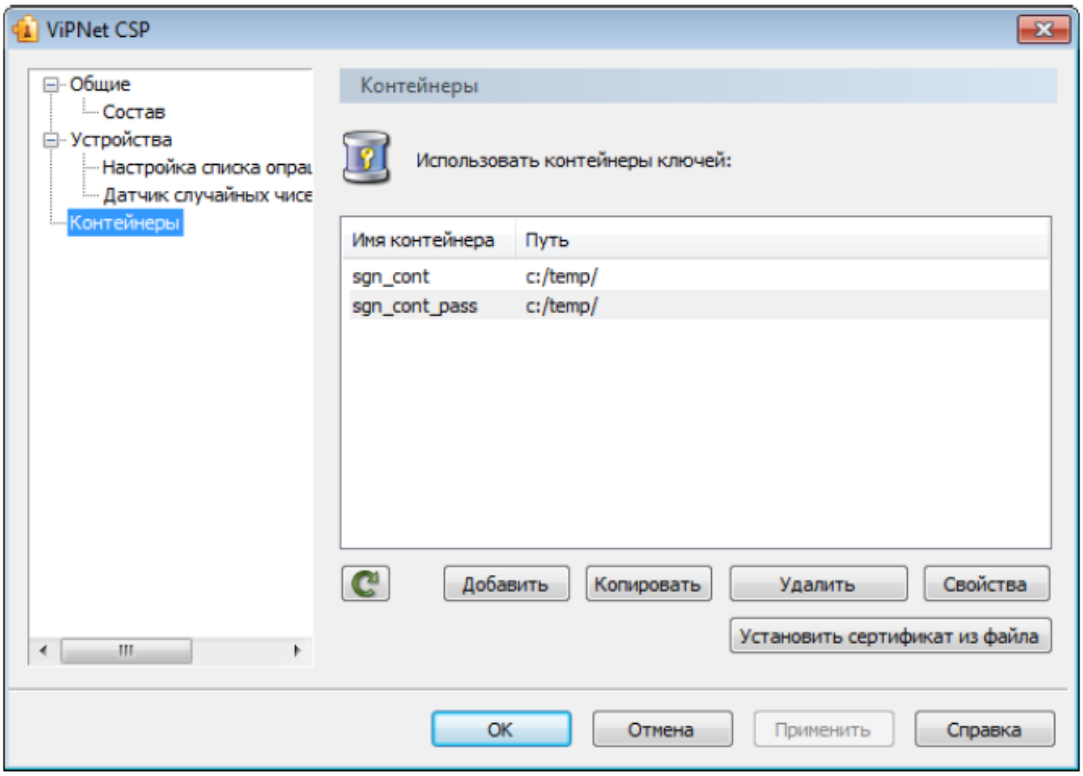

Рисунок 33 – Панель управления контейнерами

4) В разделе «Контейнеры» нажать кнопку «Добавить».

5) В окне ViPNet CSP - инициализация контейнера ключей нажать кнопку «Обзор» (Рисунок 34):

– если контейнер хранится на жестком диске, в окне «Обзор папок» необходимо указать путь к папке, содержащей контейнер;

– если контейнер хранится на съемном флэш-диске, в окне «Обзор папок» необходимо указать этот съемный диск. В поле «Папка» на диске автоматически будет подставлен путь, например, E:\Infotecs\Containers.

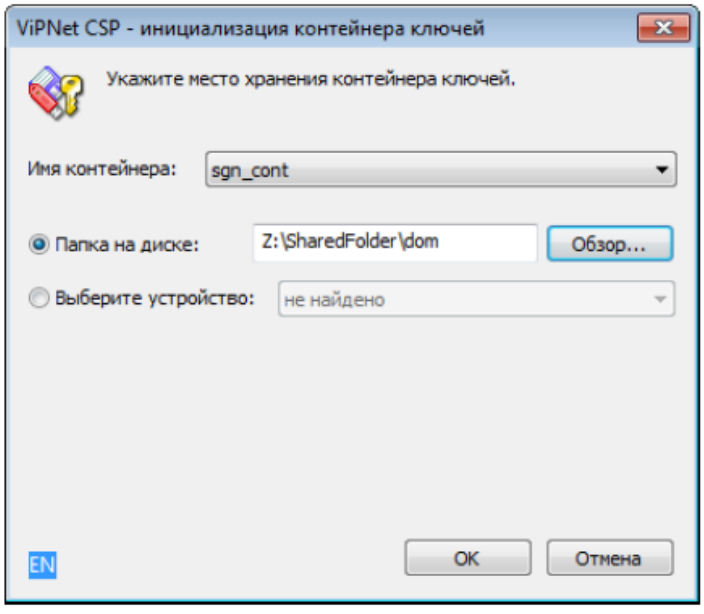

Рисунок 34 – Инициализация контейнера ключей из папки

6) Из списка «Имя контейнера» необходимо выбрать файл контейнера или оставить значение по умолчанию.

7) Нажать «ОК». В окне «Контейнер ключей» появится сообщение об успешном добавлении контейнера и предложение по установке сертификата в хранилище. Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.

При нажатии кнопки «Да», сертификаты будут автоматически установлены в хранилище пользователя.

Если сертификаты устанавливать не требуется (или установка будет происходить вручную), необходимо нажать «Нет».

Для просмотра списка сертификатов в контейнере необходимо нажать кнопку «Сертификаты» (Рисунок 35).

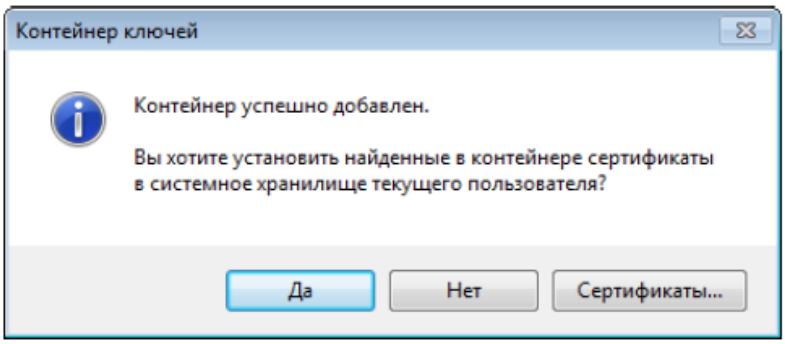

Рисунок 35 – Установка сертификатов из контейнера в хранилище

8) После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров появится добавленный контейнер.

Обеспечение доступности секретного ключа сертификата в Signal-COM CSP:

Если в качестве носителя ключевой информации используется дискета или flash-носитель, не требуется выполнять никаких дополнительных настроек - программа сама обнаружит и запомнит используемый носитель ключевой информации.

Обеспечение доступности секретного ключа сертификата в ЛИССИ-CSP:

Для управления ключевыми контейнерами «ЛИССИ-CSP» используется утилита «Управление контейнерами». Для запуска утилиты необходимо выполнить команду «Пуск» → «Все программы» → «LISSI» → «ЛИССИ-CSP» → «Управление контейнерами» (Рисунок 36).

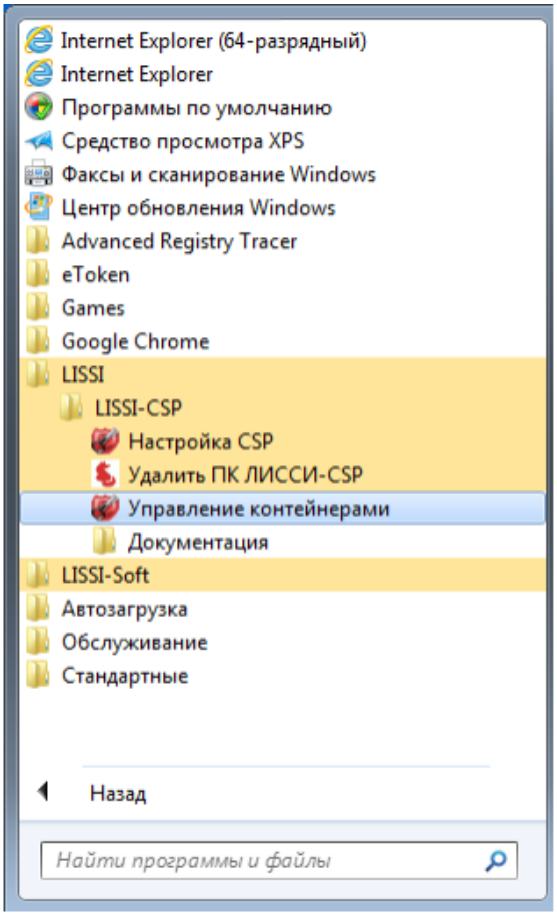

Рисунок 36 – Управление контейнерами

После запуска утилиты в окне «Контейнеры» появится иерархический список носителей, поддерживаемых «ЛИССИ-CSP» и присутствующих в данный момент. Для отображения съёмных носителей (электронные USB ключи, флэшка, дискета) необходимо, чтобы они были вставлены в USB-порт (в случае с дискетой в дисковод) компьютера.

Носитель может содержать список представленных на нём ключевых контейнеров. Если носитель не содержит список, то это означает, что на нём нет ключевых контейнеров «ЛИССИ-CSP» (Рисунок 37).

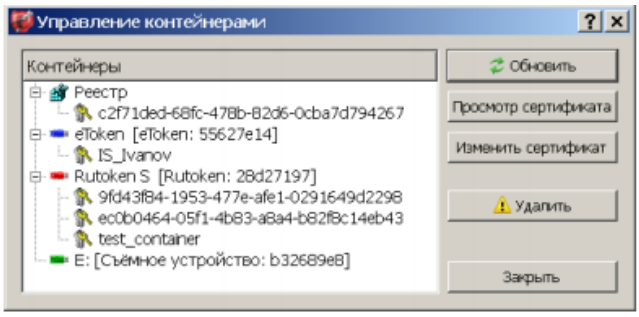

Рисунок 37 – Контейнеры

Если ключевой носитель был вставлен в порт компьютера после запуска утилиты, то для его отображения в окне утилиты необходимо нажать кнопку «Обновить».