



Средство
Криптографической
Защиты
Информации

КриптоПро CSP
(версия 2.0)

Информация по эксплуатации

Аннотация

Данный документ является руководством по эксплуатации средства криптографической защиты информации «КриптоПро CSP» и содержит описание сервисных функций, процесса установки и настройки СКЗИ «КриптоПро CSP».

Дополнительно документ содержит описание действий по установке сертификатов уполномоченных лиц Удостоверяющих центров (сертификатов Центров сертификации), списков отозванных сертификатов (CRL), а также действия по просмотру установленных на компьютере сертификатов и списков отозванных сертификатов.

Информация о разработчике СКЗИ «КриптоПро CSP»:

ООО "Крипто-Про"

127 018, Москва, Улица Образцова, 38

Телефон: (495) 933 1168

Факс: (495) 933 1168

<http://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

Содержание

1.	Установка СКЗИ «КриптоПро CSP»	5
1.1.	Установка криптопровайдера «КриптоПро CSP».....	5
1.2.	Установка средства сетевой аутентификации «КриптоПро TLS»	8
1.3.	Установка всех компонент СКЗИ «КриптоПро CSP»	11
2.	Ввод серийного номера лицензии и ключа активации СКЗИ «КриптоПро CSP». Регистрация СКЗИ «КриптоПро CSP»	13
2.1.	Ввод серийного номера лицензии и ключа активации криптопровайдера «КриптоПро CSP»	13
2.2.	Ввод серийного номера лицензии и ключа активации средства сетевой аутентификации «КриптоПро TLS».....	14
2.3.	Регистрация СКЗИ «КриптоПро CSP»	14
3.	Настройка считывателей носителей секретных ключей	15
3.1.	Добавление считывателя	15
3.2.	Удаление считывателя.....	18
3.3.	Просмотр свойств считывателя.....	18
4.	Настройка датчиков случайных чисел (ДСЧ)	20
4.1.	Добавление ДСЧ	20
4.2.	Удаление ДСЧ.....	23
4.3.	Просмотр свойств ДСЧ.....	23
5.	Копирование и удаление контейнера секретного ключа	25
5.1.	Копирование контейнера секретного ключа	25
5.2.	Удаление контейнера секретного ключа.....	27
6.	Просмотр и установка личного сертификата, хранящегося в контейнере секретного ключа	29
6.1.	Просмотр сертификата, хранящегося в контейнере секретного ключа	29
6.2.	Установка личного сертификата, хранящегося в контейнере секретного ключа32	
7.	Установка личного сертификата, хранящегося в файле	35
8.	Управление паролями доступа к секретным ключам	40
8.1.	Изменение пароля на доступ к секретному ключу	40
8.2.	Удаление запомненных паролей.....	42
9.	Установка режимов хранения секретных ключей	44
10.	Просмотр версий используемых файлов	46
11.	Установка времени ожидания ввода информации от пользователя	47
12.	Установка параметров криптографических алгоритмов	50
13.	Установка сертификата Центра сертификации	51
13.1.	Установка сертификата корневого центра сертификации	51
13.2.	Установка сертификата подчиненного центра сертификации.....	54
14.	Установка списка отозванных сертификатов (CRL)	58
15.	Просмотр установленных на компьютере сертификатов и списков отозванных сертификатов	61
15.1.	Просмотр установленных сертификатов в окне свойств обозревателя Microsoft Internet Explorer (IE)	61
15.2.	Просмотр установленных сертификатов с помощью оснастки Сертификаты Microsoft Management Console (MMC) (только для Windows 2000, XP, 2003)	64

15.3.Просмотр установленных сертификатов с помощью утилиты CertMgr.exe,
разработанной ООО «КРИПТО-ПРО»..... 67

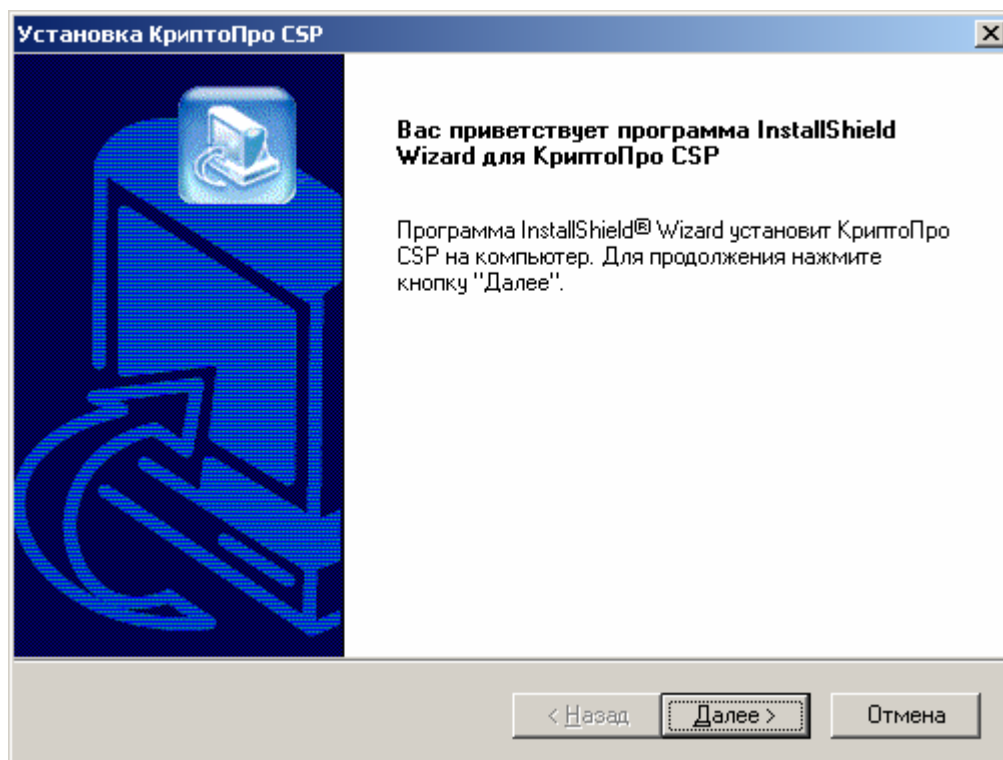
1. Установка СКЗИ «КриптоПро CSP»

1.1. Установка криптопровайдера «КриптоПро CSP»

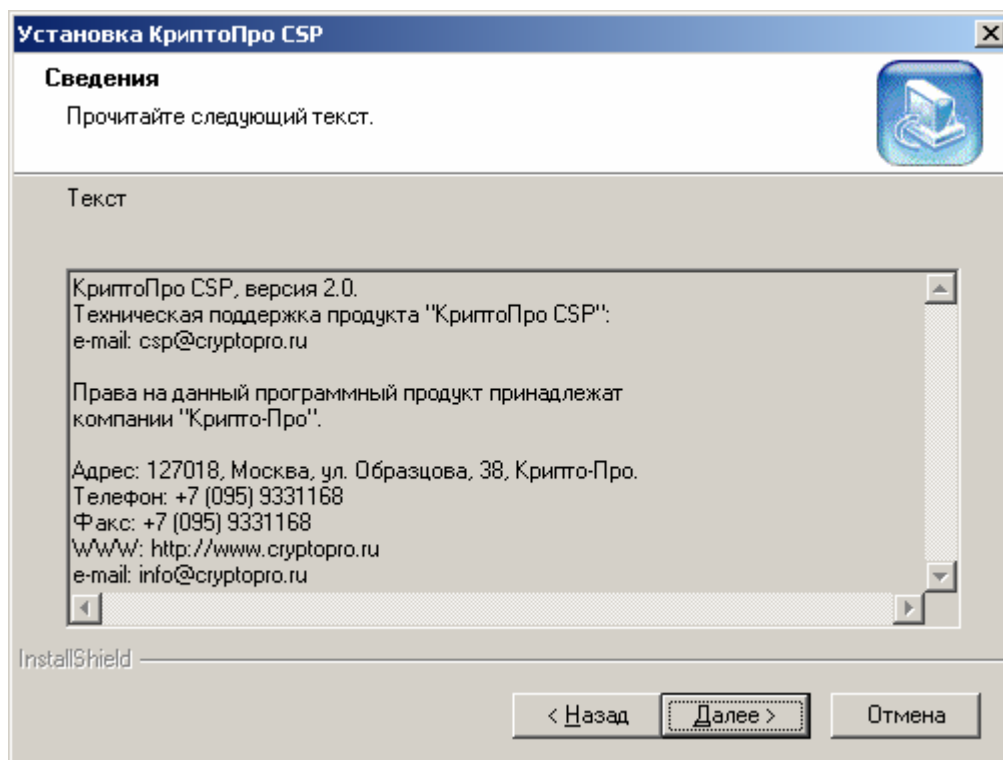
1. Для установки криптопровайдера «КриптоПро CSP» вставьте компакт-диск с дистрибутивом СКЗИ «КриптоПро CSP» в привод считывателя. Программа установки запустится автоматически. Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска. Откроется окно **Продукты КриптоПро**. Для установки криптопровайдера нажмите кнопку **Установить КриптоПро CSP**



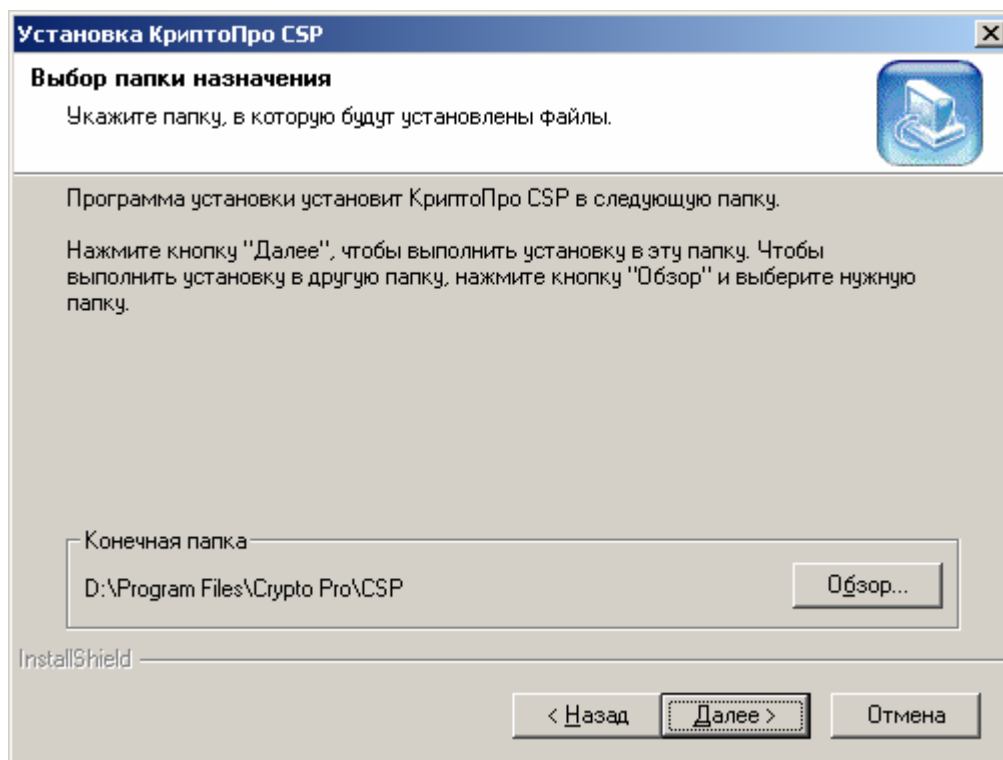
2. Откроется окно **Установка КриптоПро CSP**. Нажмите кнопку **Далее**



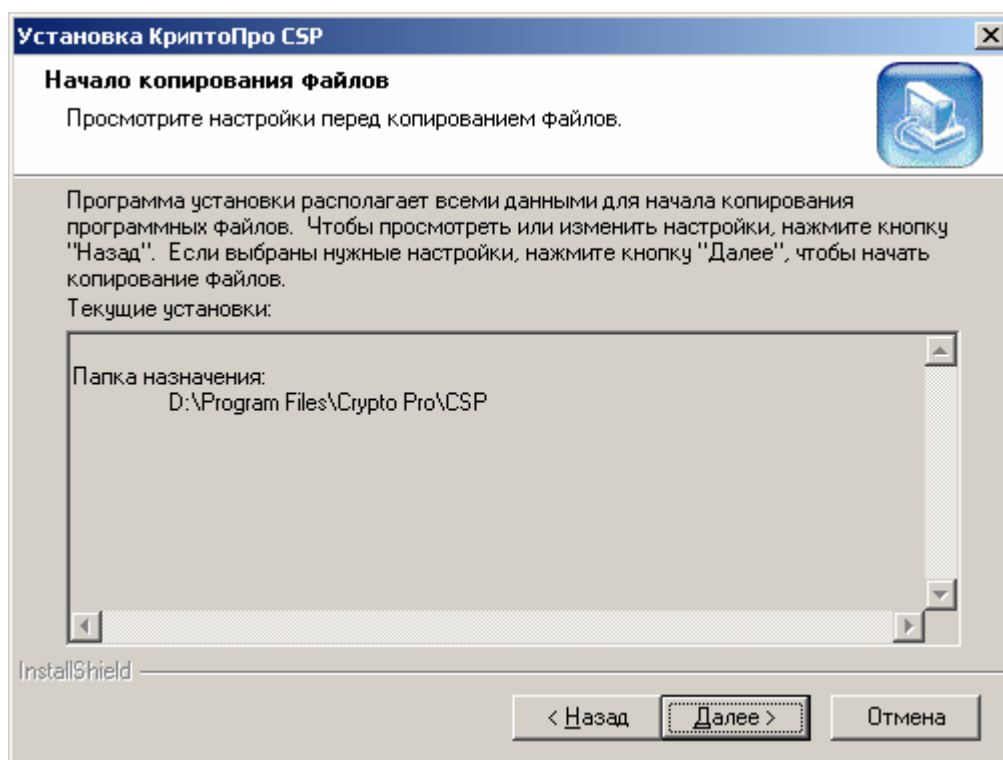
3. В окне **Сведения** ознакомьтесь с текстом сообщения и нажмите кнопку **Далее**



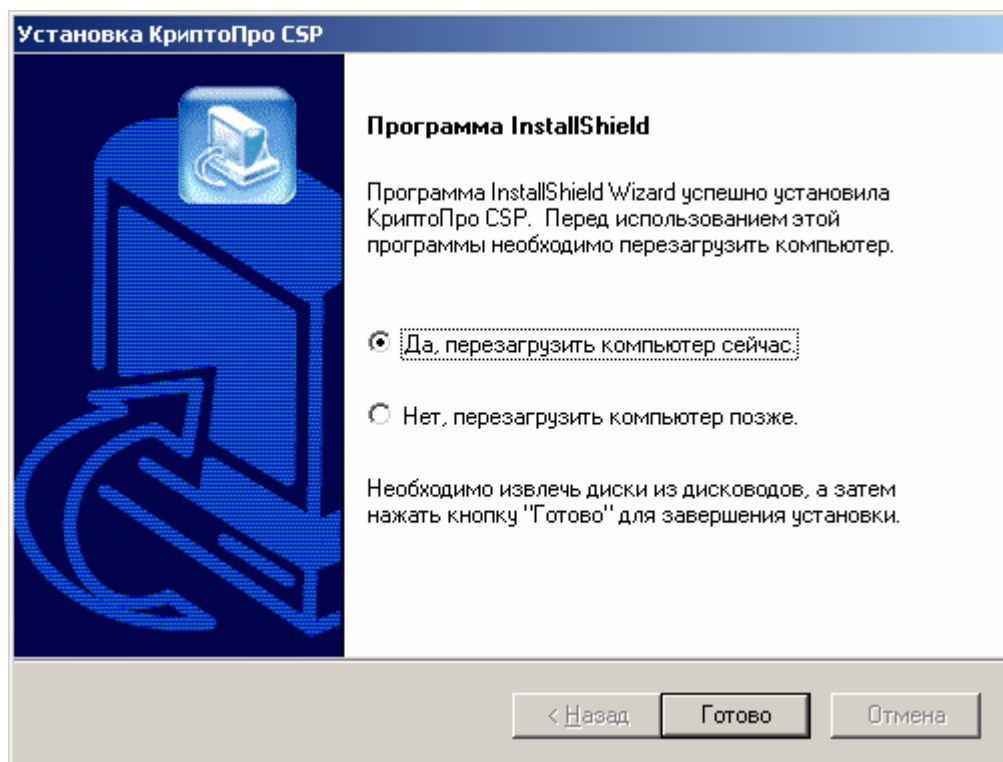
4. В окне **Выбор папки назначения** с помощью кнопки **Обзор** определите место установки файлов и нажмите кнопку **Далее**



5. В окне **Начало копирования файлов** осуществите проверку правильности ввода параметров и нажмите кнопку **Далее**

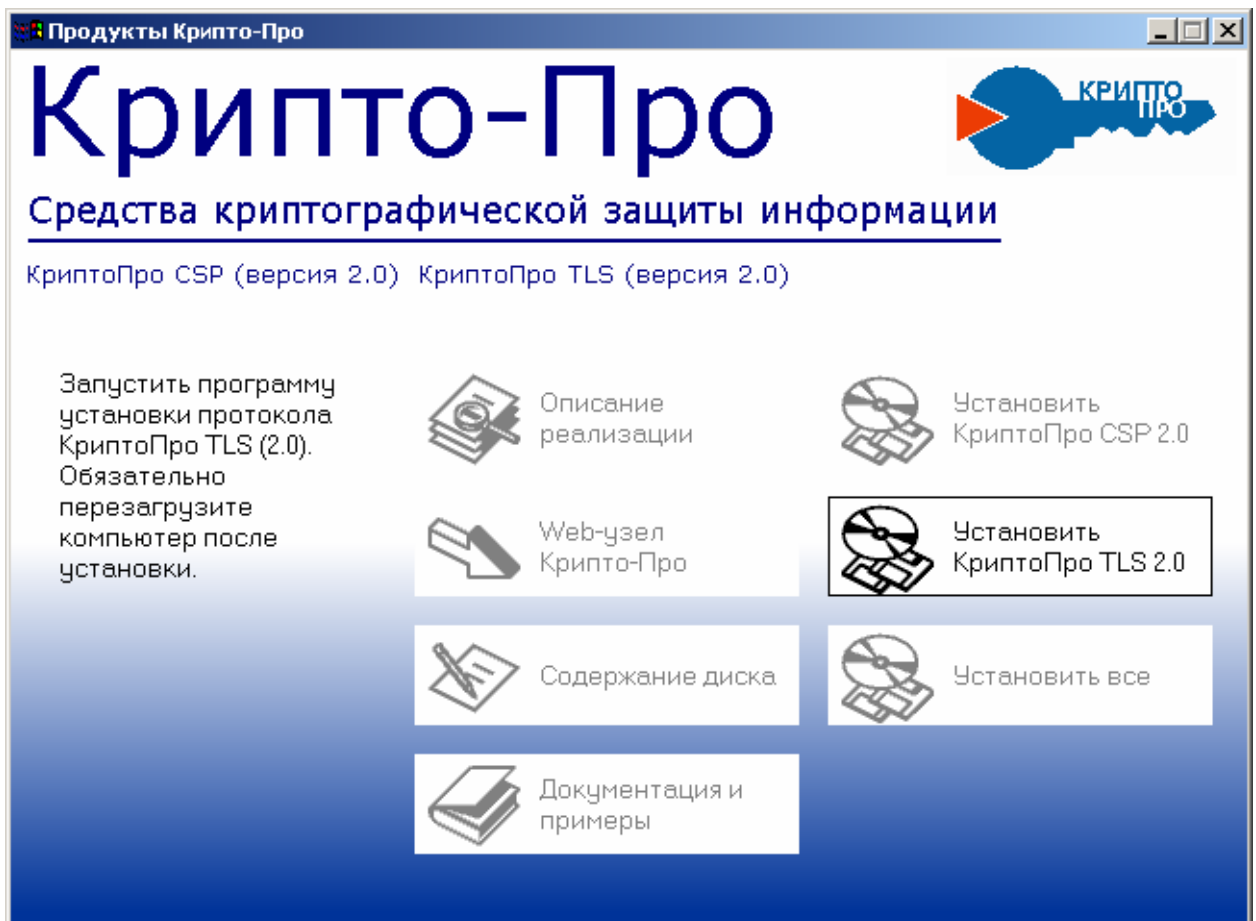


6. Начнется инсталляция криптопровайдера «КриптоПро CSP», сопровождающаяся выводом информации о процессе установки. После успешной инсталляции откроется окно, предлагающее пользователю осуществить перезагрузку компьютера. Выберите переключатель **Да**, **перезагрузить компьютер сейчас** и нажмите кнопку **Готово**

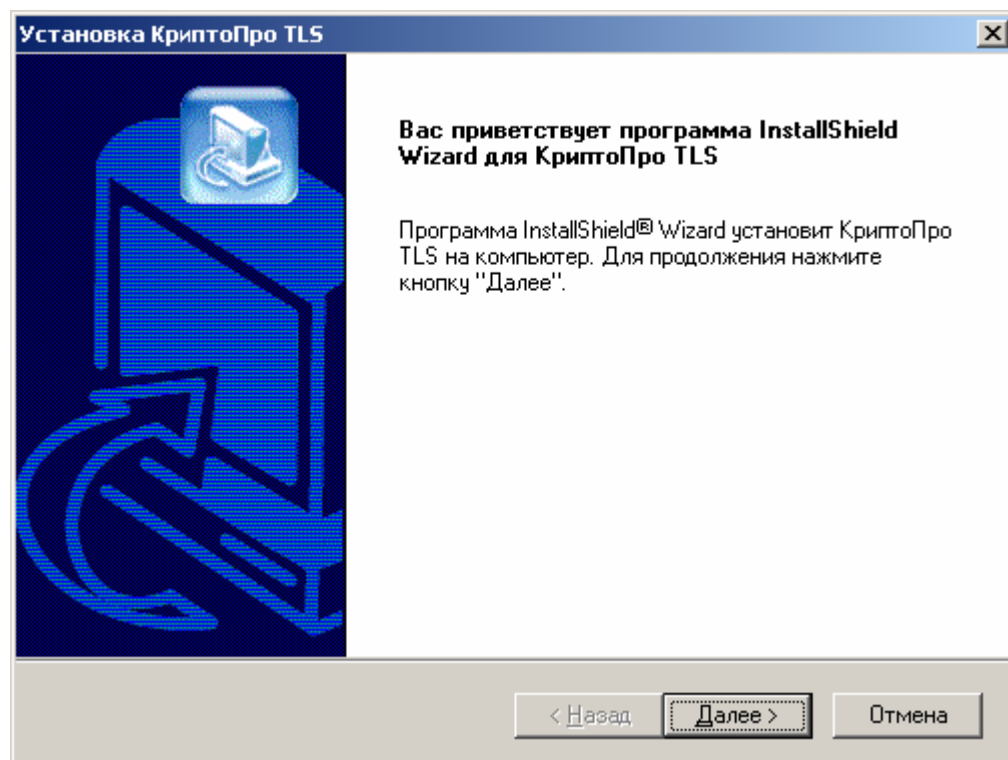


1.2. Установка средства сетевой аутентификации «КриптоПро TLS»

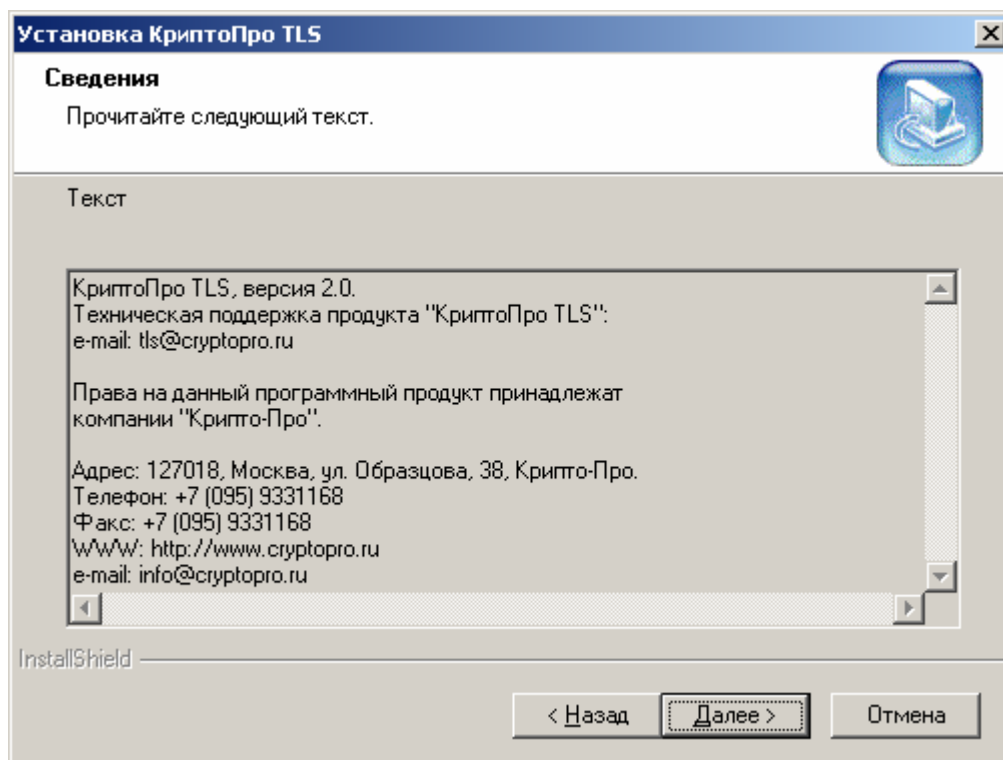
1. Для установки средства сетевой аутентификации «КриптоПро TLS» вставьте компакт-диск с дистрибутивом СКЗИ «КриптоПро CSP» в привод считывателя. Программа установки запустится автоматически. Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска. Откроется окно **Продукты КриптоПро**. Для установки криптопровайдера нажмите кнопку **Установить КриптоПро TLS**



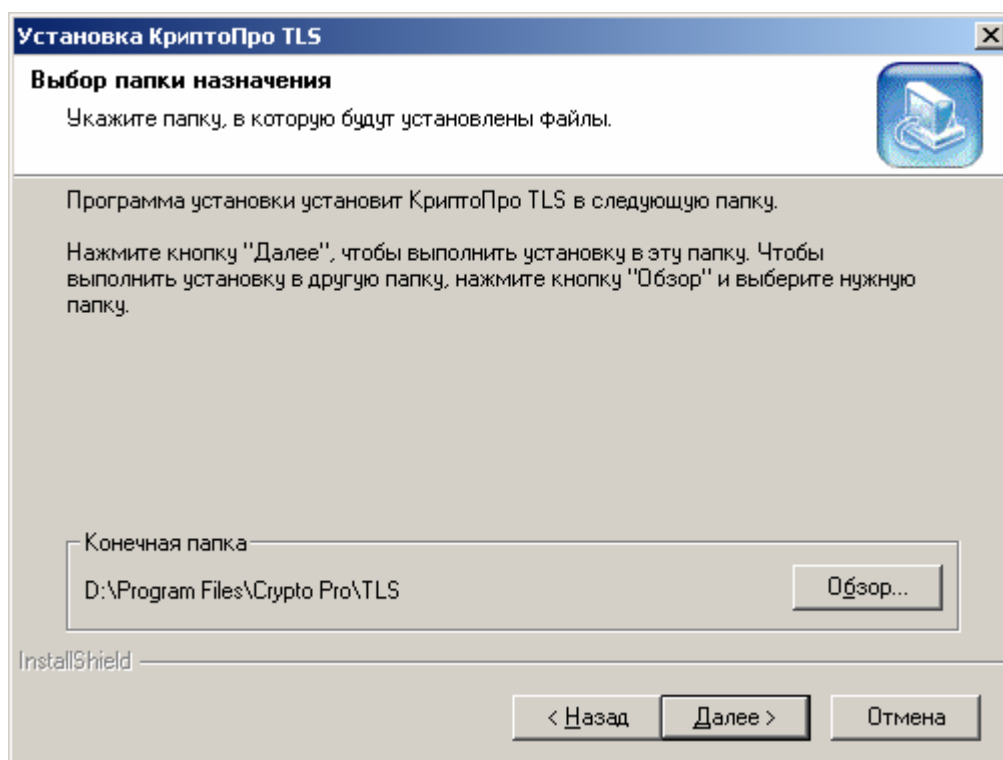
2. Откроется окно **Установка КриптоПро TLS**. Нажмите кнопку **Далее**



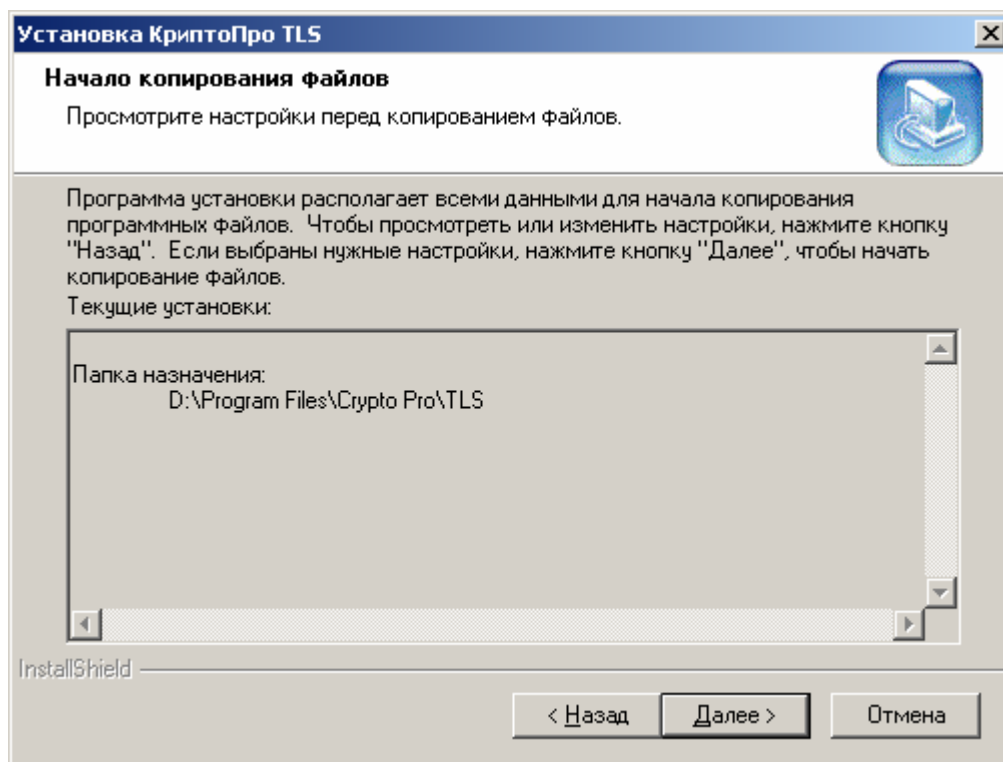
3. В окне **Сведения** ознакомьтесь с текстом сообщения и нажмите кнопку **Далее**



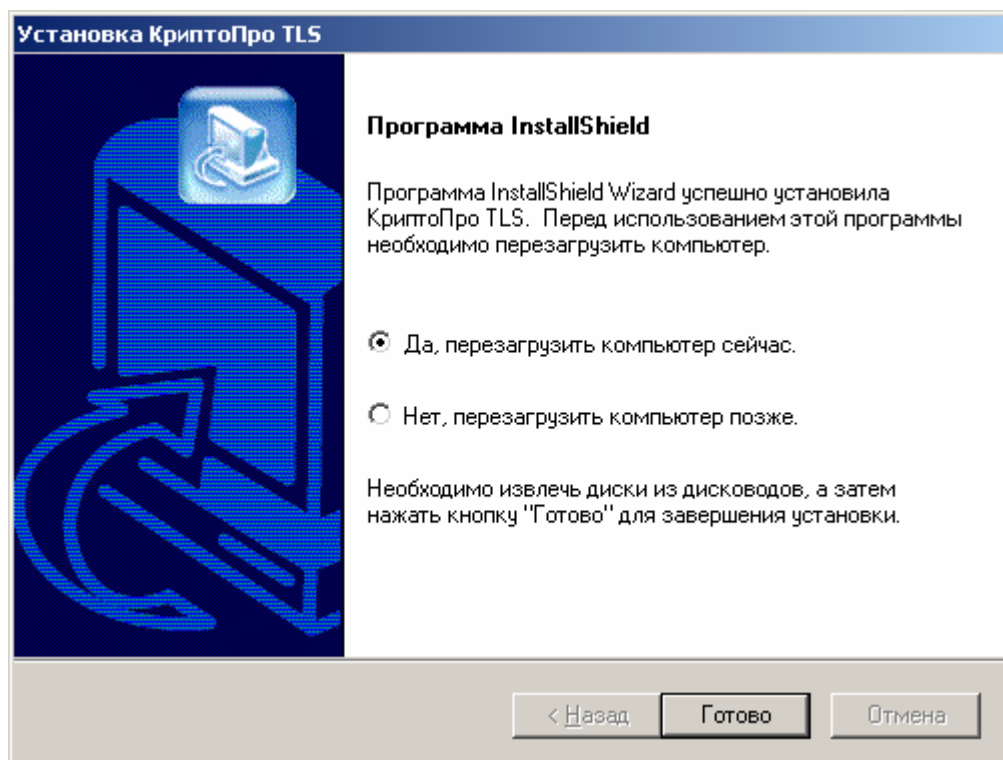
4. В окне **Выбор папки назначения** с помощью кнопки **Обзор** определите место установки файлов и нажмите кнопку **Далее**



5. В окне **Начало копирования файлов** осуществите проверку правильности ввода параметров и нажмите кнопку **Далее**



6. Начнется инсталляция средства сетевой аутентификации «КриптоПро TLS», сопровождающаяся выводом информации о процессе установки. После успешной инсталляции откроется окно, предлагающее пользователю осуществить перезагрузку компьютера. Выберите переключатель **Да, перезагрузить компьютер сейчас** и нажмите кнопку **Готово**



1.3. Установка всех компонент СКЗИ «КриптоПро CSP»

1. Для установки всех компонент СКЗИ «КриптоПро CSP» вставьте компакт-диск с дистрибутивом СКЗИ «КриптоПро CSP» в привод считывателя. Программа установки запустится автоматически. Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска. Откроется окно **Продукты КриптоПро**. Для установки всех компонент СКЗИ «КриптоПро CSP» нажмите кнопку **Установить все**

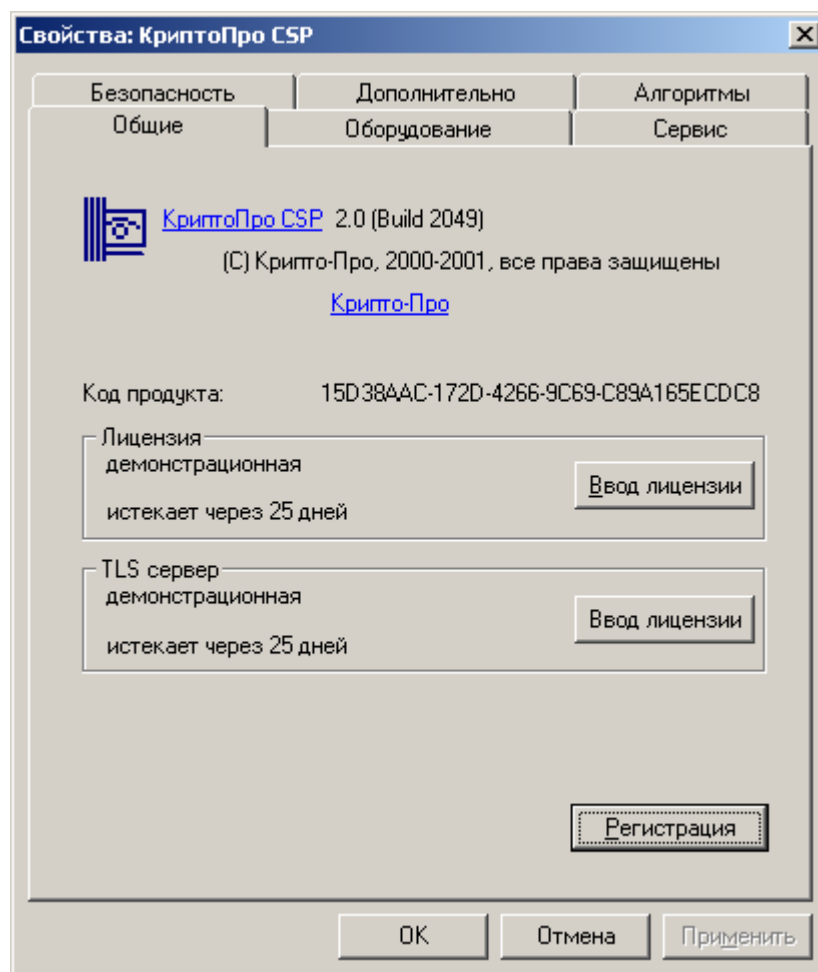


2. Программа установки последовательно осуществит инсталляцию криптопровайдера «КриптоПро CSP» и средства сетевой аутентификации «КриптоПро TLS» в соответствии с пунктами 1.2 и 1.3 данного руководства

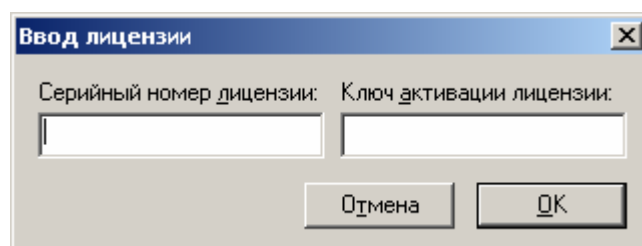
2. Ввод серийного номера лицензии и ключа активации СКЗИ «КриптоПро CSP». Регистрация СКЗИ «КриптоПро CSP»

2.1. Ввод серийного номера лицензии и ключа активации криптопровайдера «КриптоПро CSP»

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**



2. На вкладке **Общие** в области **Лицензия** нажмите кнопку **Ввод лицензии** и введите в поля **Серийный номер лицензии** и **Ключ активации лицензии** соответствующие значения с бланка Лицензии на использование программного продукта КриптоПро CSP. После ввода необходимых данных нажмите кнопку **OK**

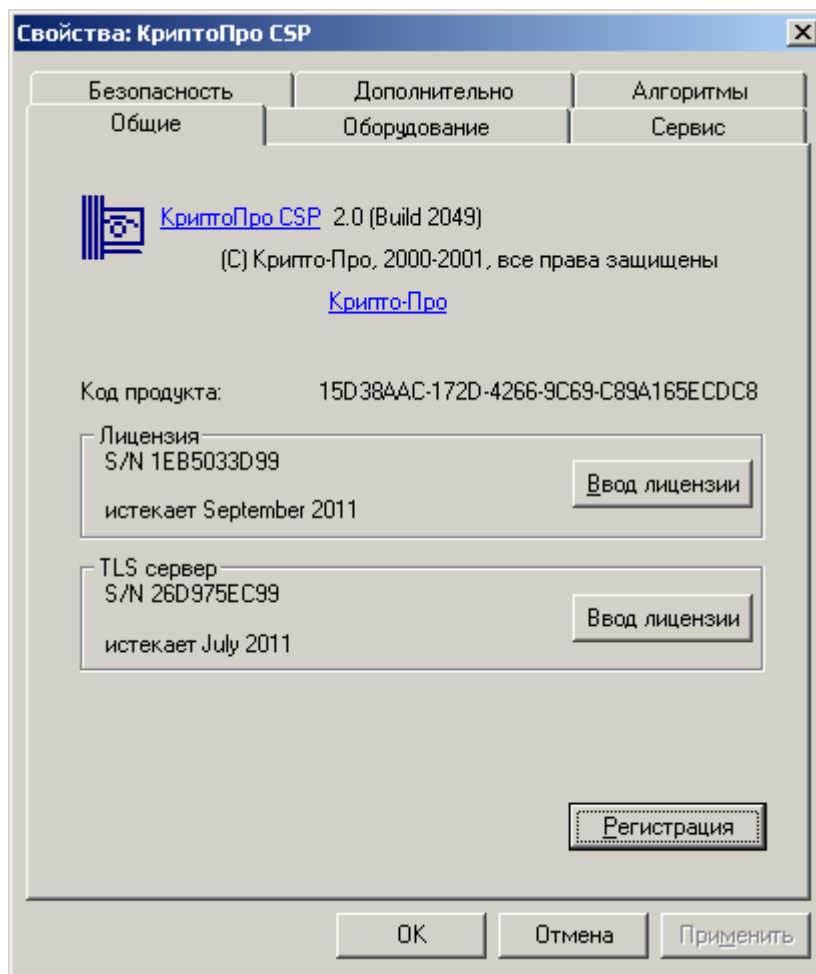


2.2. Ввод серийного номера лицензии и ключа активации средства сетевой аутентификации «КриптоПро TLS»

1. Выполните действия аналогичные пункту 2.1 для области **TLS сервер**. Серийный номер лицензии и ключ активации лицензии введите с бланка Лицензии на использование программного продукта КриптоПро TLS

2.3. Регистрация СКЗИ «КриптоПро CSP»

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**

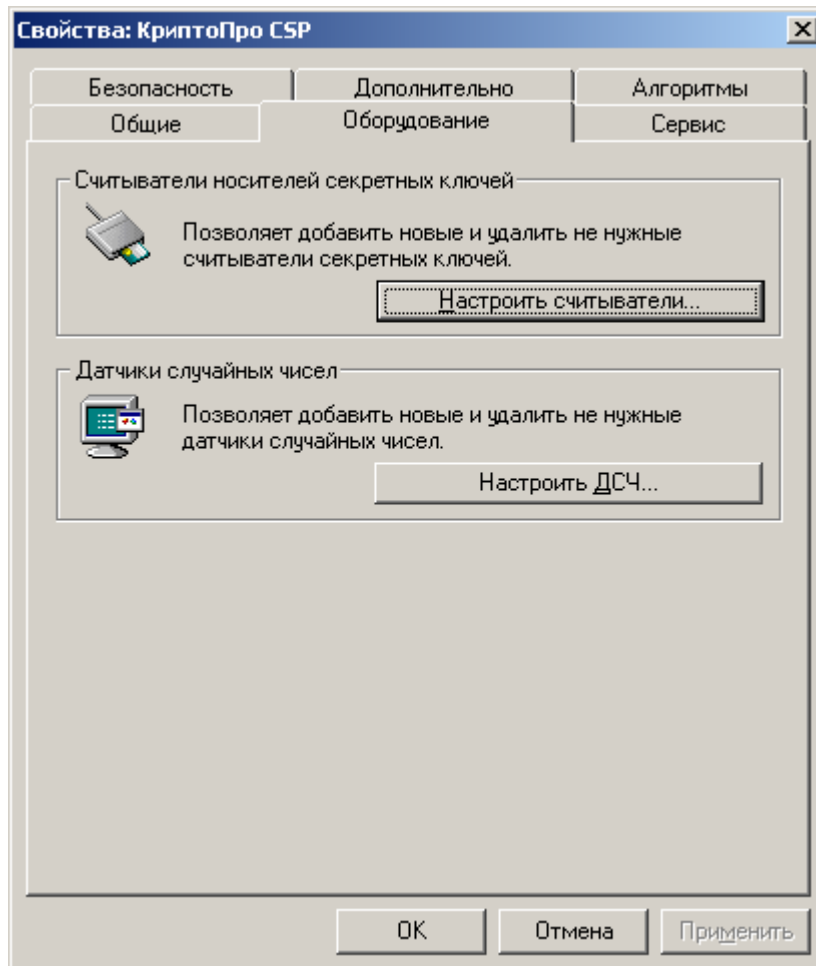


2. На вкладке **Общие** нажмите кнопку **Регистрация**. Откроется окно браузера с предложением отправить регистрационные данные. Выберите удобный для Вас способ отправки регистрационной карточки и либо распечатайте данный документ (кнопка **Напечатать**), либо отправьте его по электронной почте (кнопка **Отправить по e-mail**)

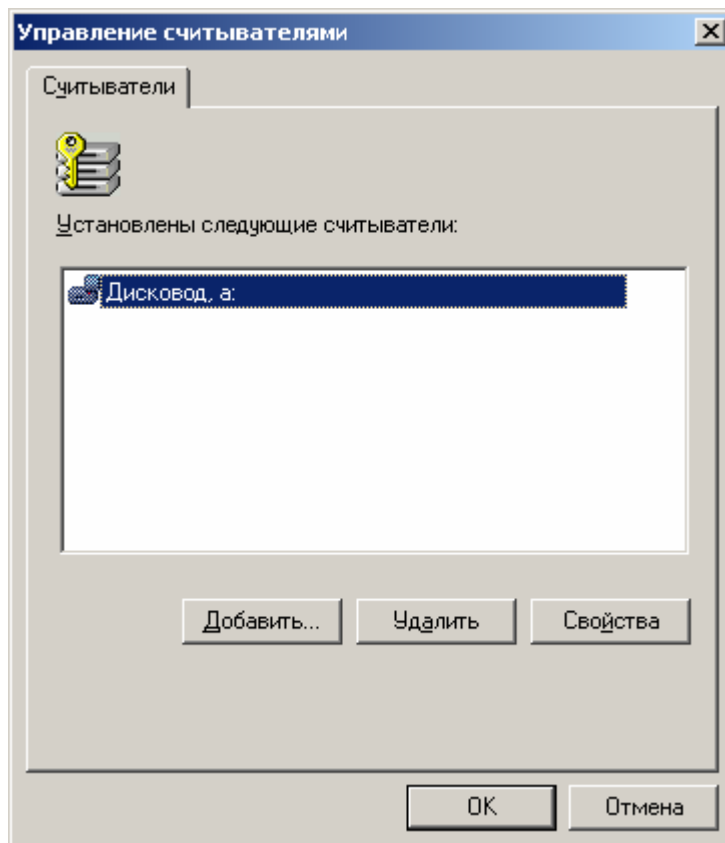
3. Настройка считывателей носителей секретных ключей

3.1. Добавление считывателя

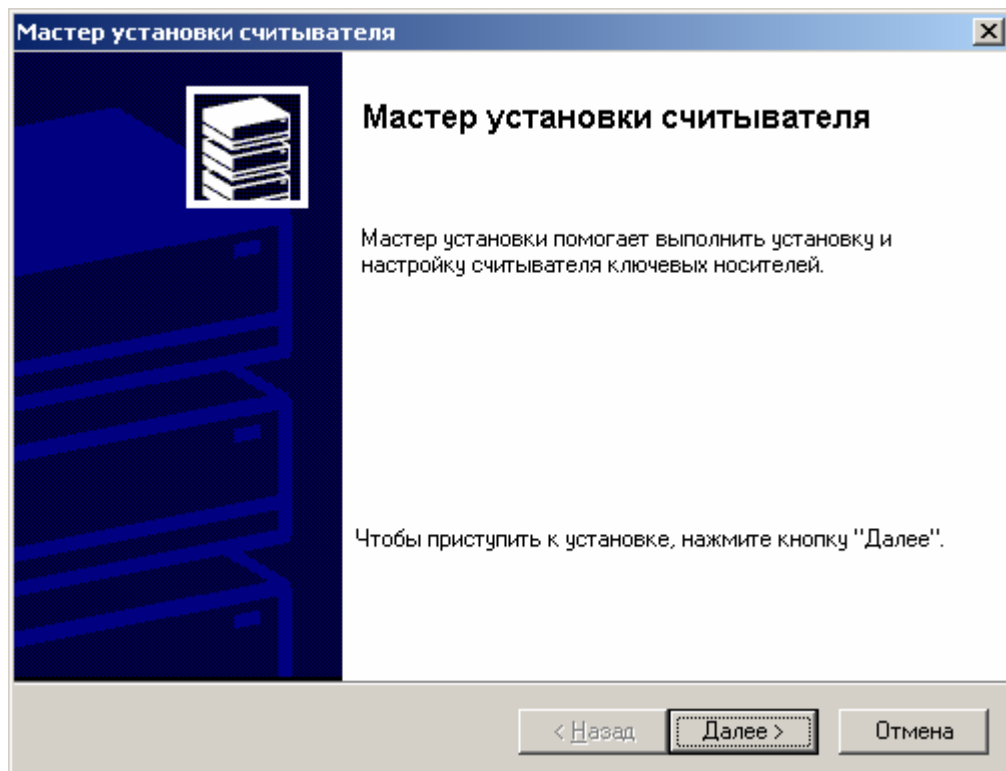
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**



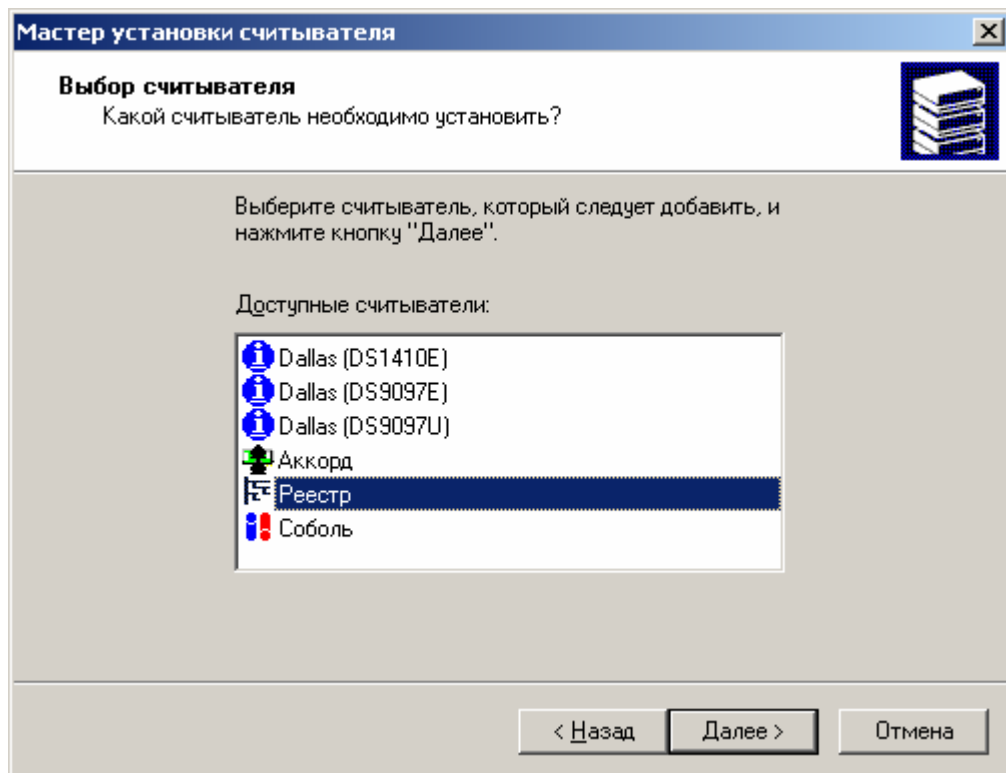
2. Нажмите кнопку **Настроить считыватели**. Откроется окно **Управление считывателями**



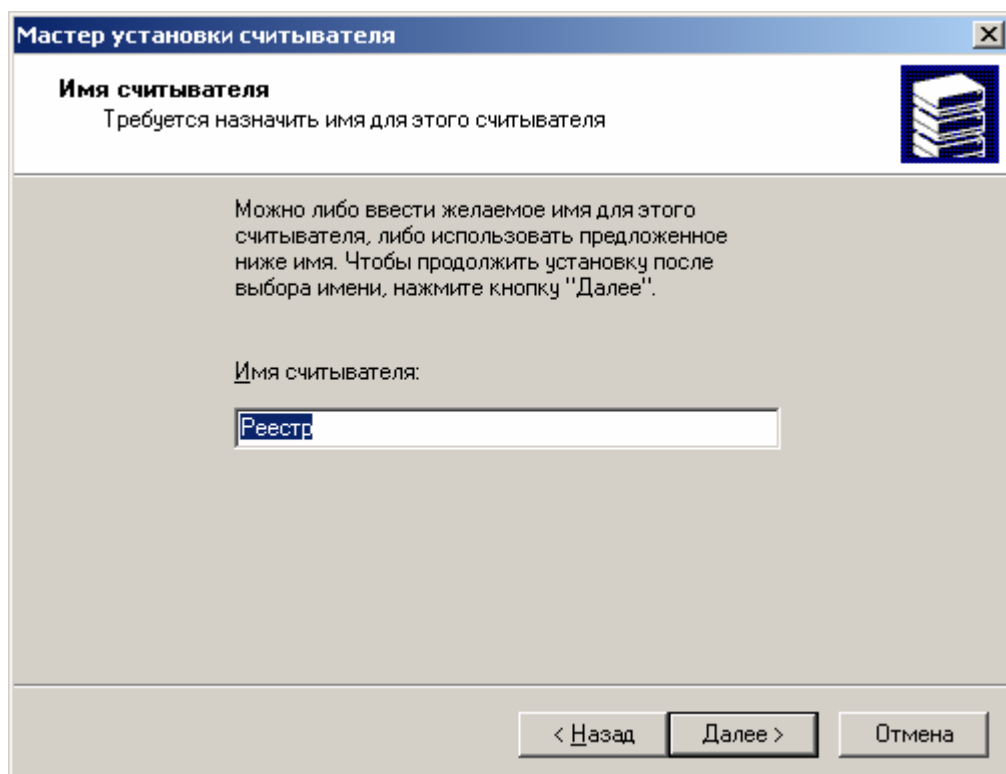
3. Нажмите кнопку **Добавить**. Запустится **Мастер установки считывателя**. Нажмите кнопку **Далее**



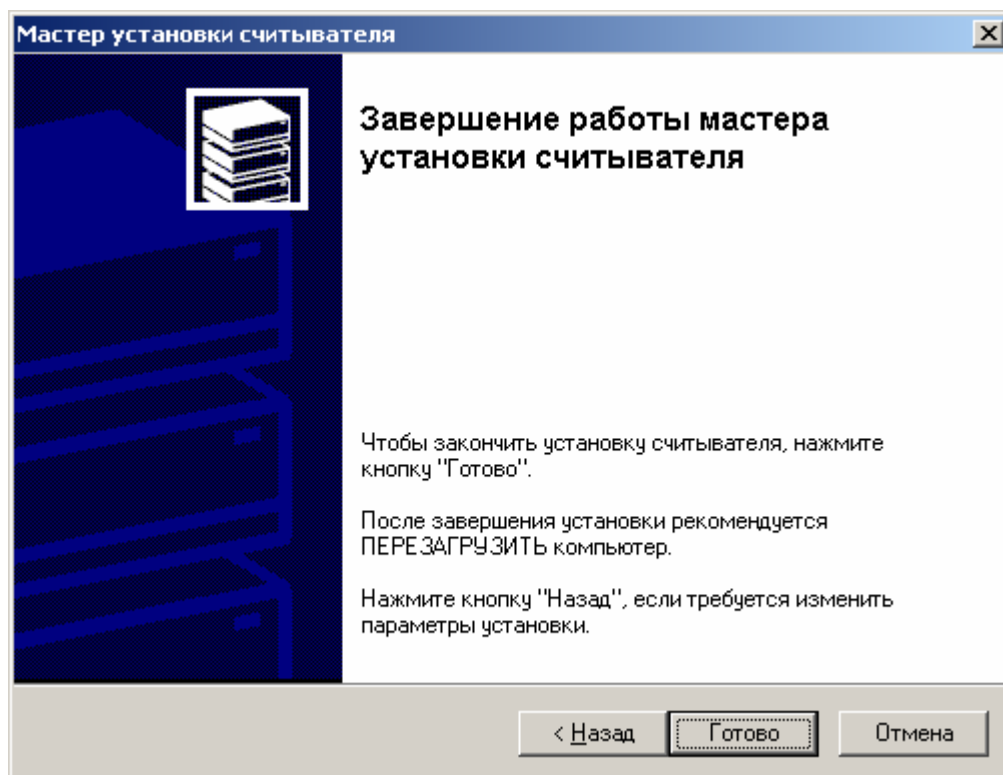
4. В окне **Выбор считывателя** выберите считыватель, который следует добавить и нажмите кнопку **Далее**



5. В окне **Имя считывателя** введите имя выбранного считывателя и нажмите кнопку **Далее**

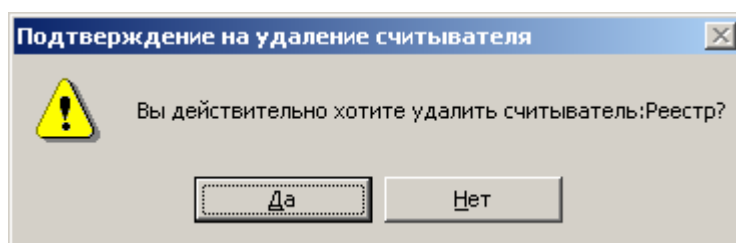


6. В окне **Завершение работы мастера установки считывателя** нажмите кнопку **Готово** и перезагрузите компьютер



3.2. Удаление считывателя

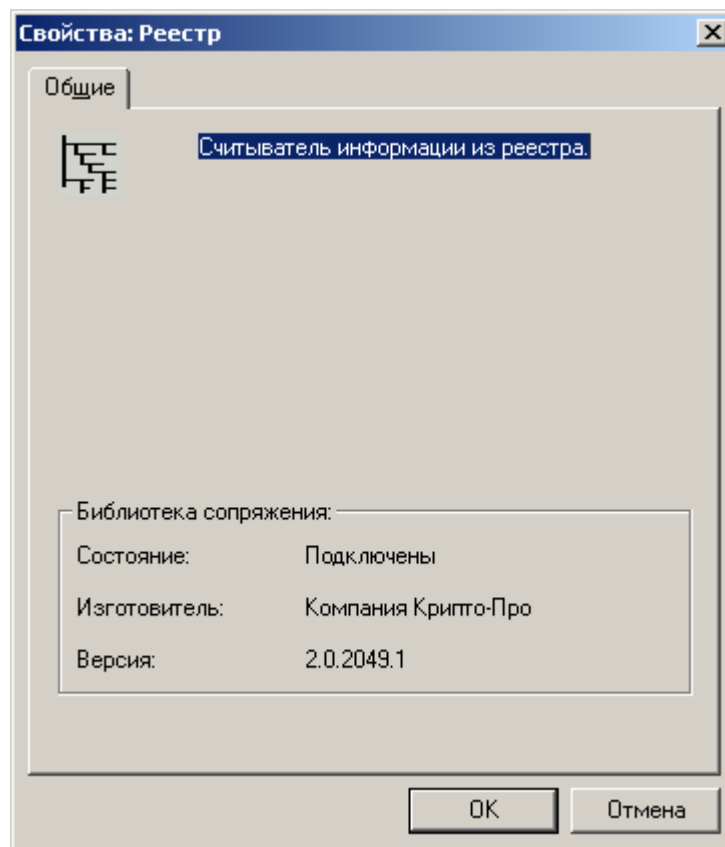
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления**, и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**
2. Нажмите кнопку **Настроить считыватели**. Откроется окно **Управление считывателями**. Выберите считыватель, который требуется удалить и нажмите кнопку **Удалить**
3. Откроется диалоговое окно **Подтверждение на удаление считывателя**. Нажмите кнопку **Да**. Считыватель будет удален



3.3. Просмотр свойств считывателя

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**
2. Нажмите кнопку **Настроить считыватели**. Откроется окно **Управление считывателями**. Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**
3. Откроется окно **Свойства: Имя считывателя**, в котором отображается справочная информация о выбранном считывателе, в том числе и данные о

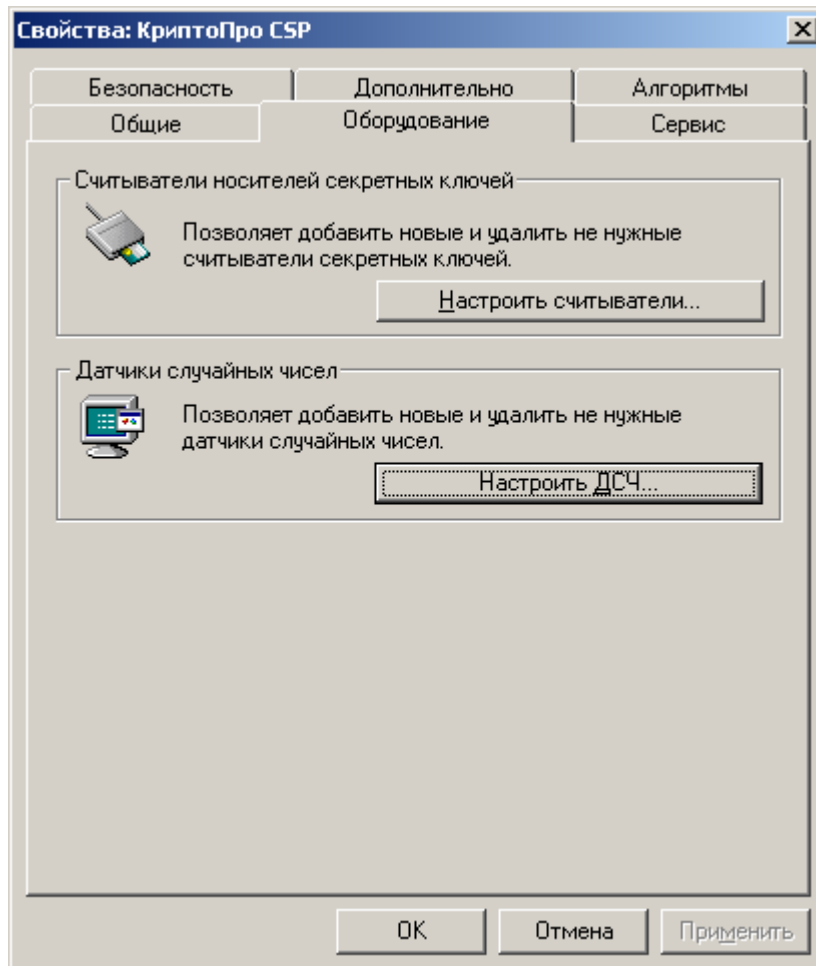
состоянии устройства. После просмотра свойств считывателя нажмите кнопку **ОК**



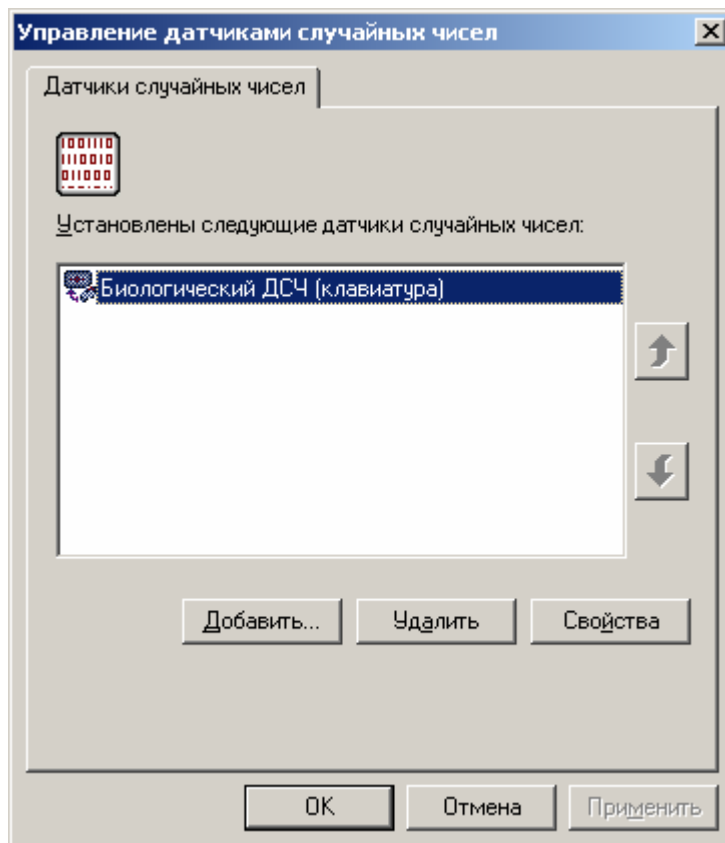
4. Настройка датчиков случайных чисел (ДСЧ)

4.1. Добавление ДСЧ

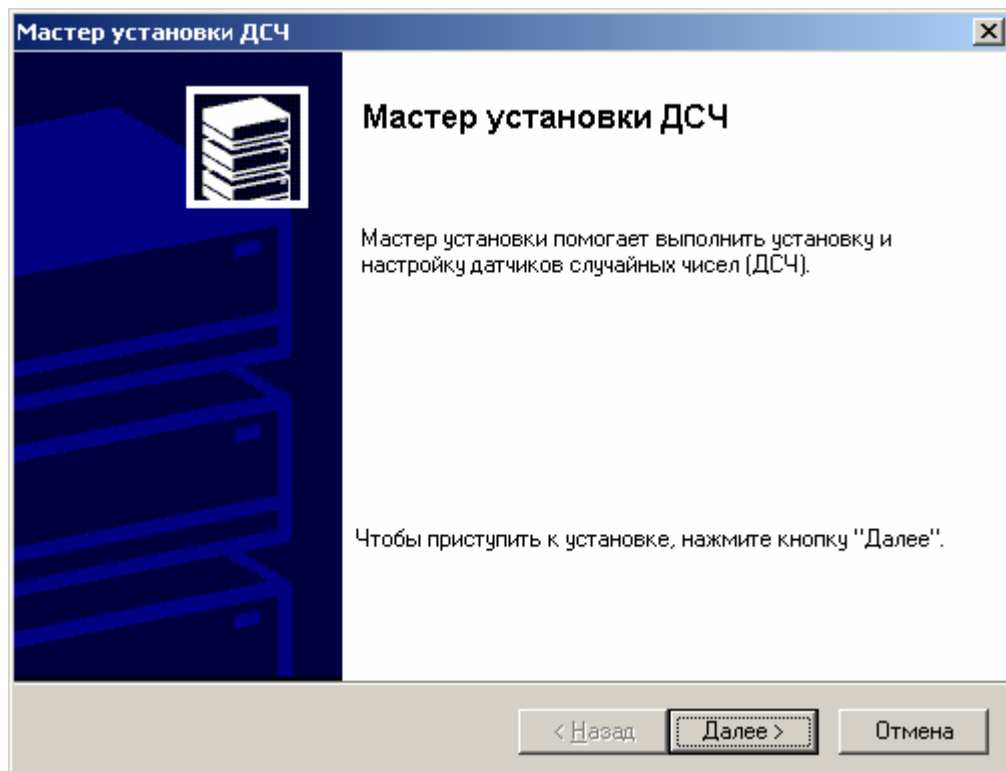
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**



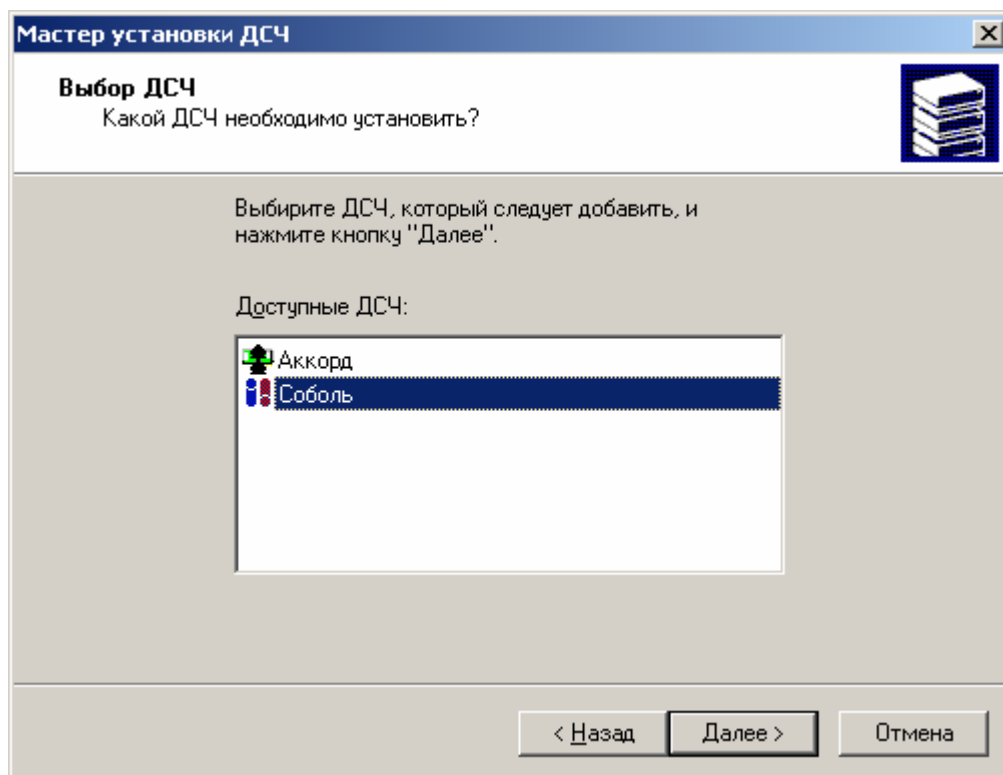
2. Нажмите кнопку **Настроить ДСЧ**. Откроется окно **Управление датчиками случайных чисел**



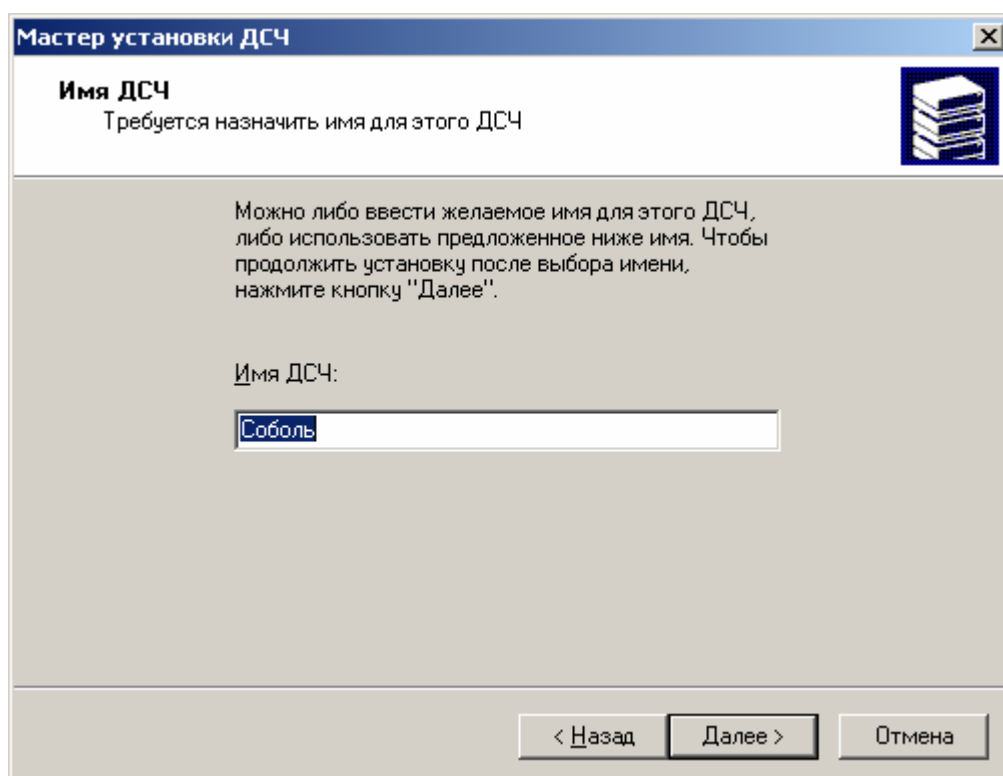
3. Нажмите кнопку **Добавить**. Запустится **Мастер установки ДСЧ**. Нажмите кнопку **Далее**



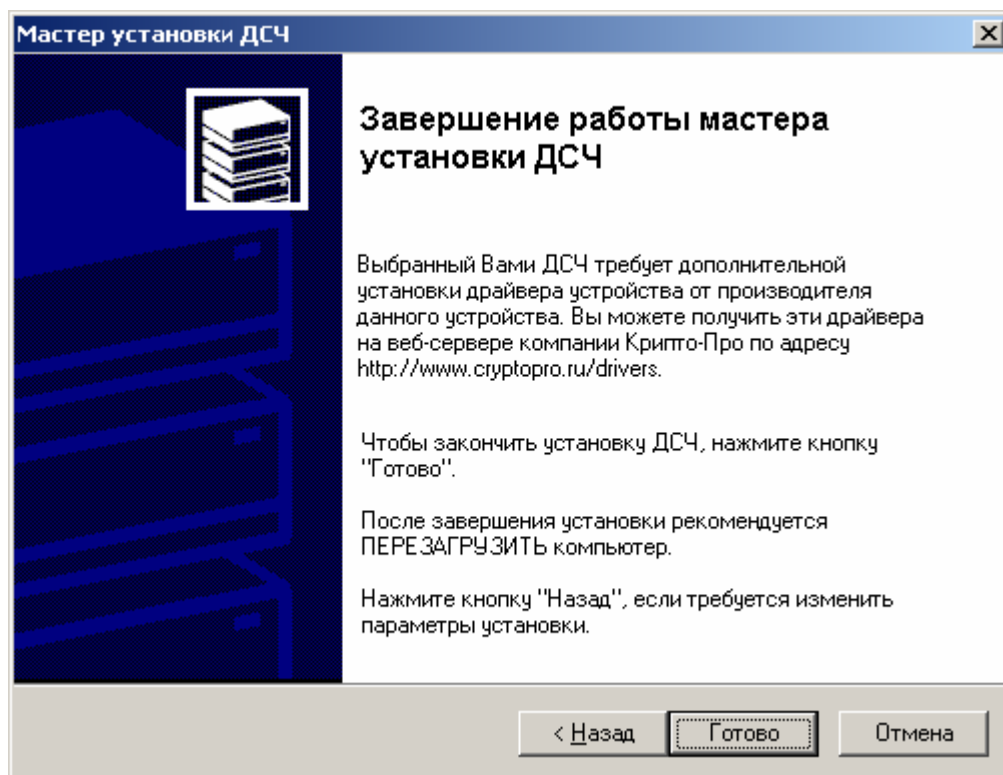
4. В окне **Выбор ДСЧ** выберите датчик случайных чисел, который следует добавить, и нажмите кнопку **Далее**



5. В окне **Имя ДСЧ** введите имя выбранного датчика случайных чисел и нажмите кнопку **Далее**

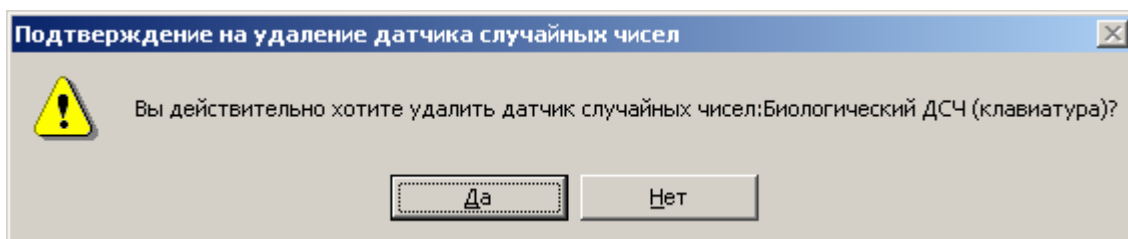


6. В окне **Завершение работы мастера установки ДСЧ** нажмите кнопку **Готово** и перезагрузите компьютер



4.2. Удаление ДСЧ

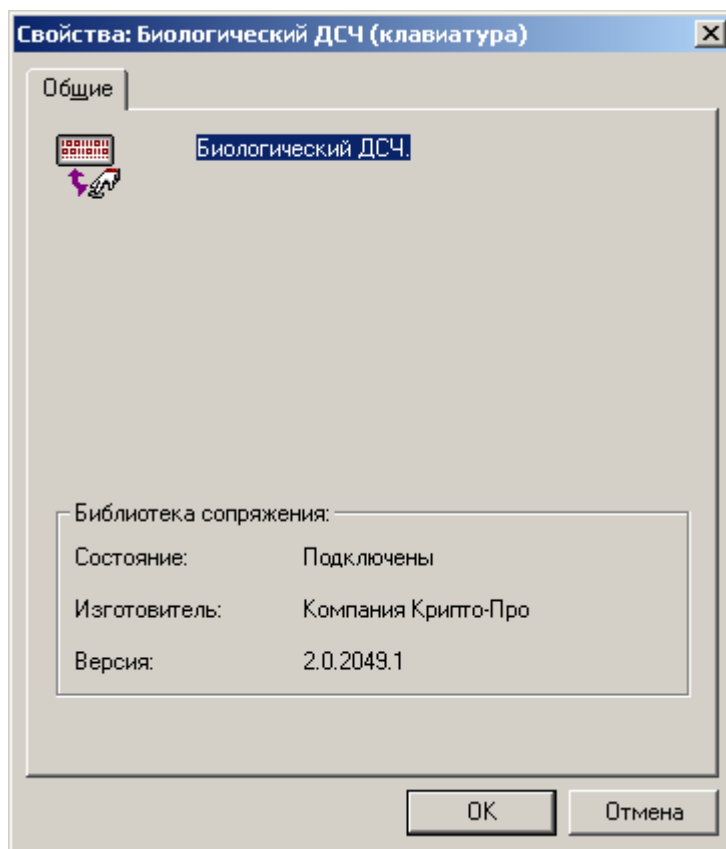
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**
2. Нажмите кнопку **Настроить ДСЧ**. Откроется окно **Управление датчиками случайных чисел**. Выберите ДСЧ, который требуется удалить, и нажмите кнопку **Удалить**
3. Откроется диалоговое окно **Подтверждение на удаление датчика случайных чисел**. Нажмите кнопку **Да**. ДСЧ будет удален





4.3. Просмотр свойств ДСЧ

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Оборудование**
2. Нажмите кнопку **Настроить ДСЧ**. Откроется окно **Управление датчиками случайных чисел**. Выберите ДСЧ, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**

3. Откроется окно **Свойства: Имя ДСЧ**, в котором отображается справочная информация о выбранном датчике случайных чисел, в том числе и данные о состоянии устройства. После просмотра свойств ДСЧ нажмите кнопку **ОК**

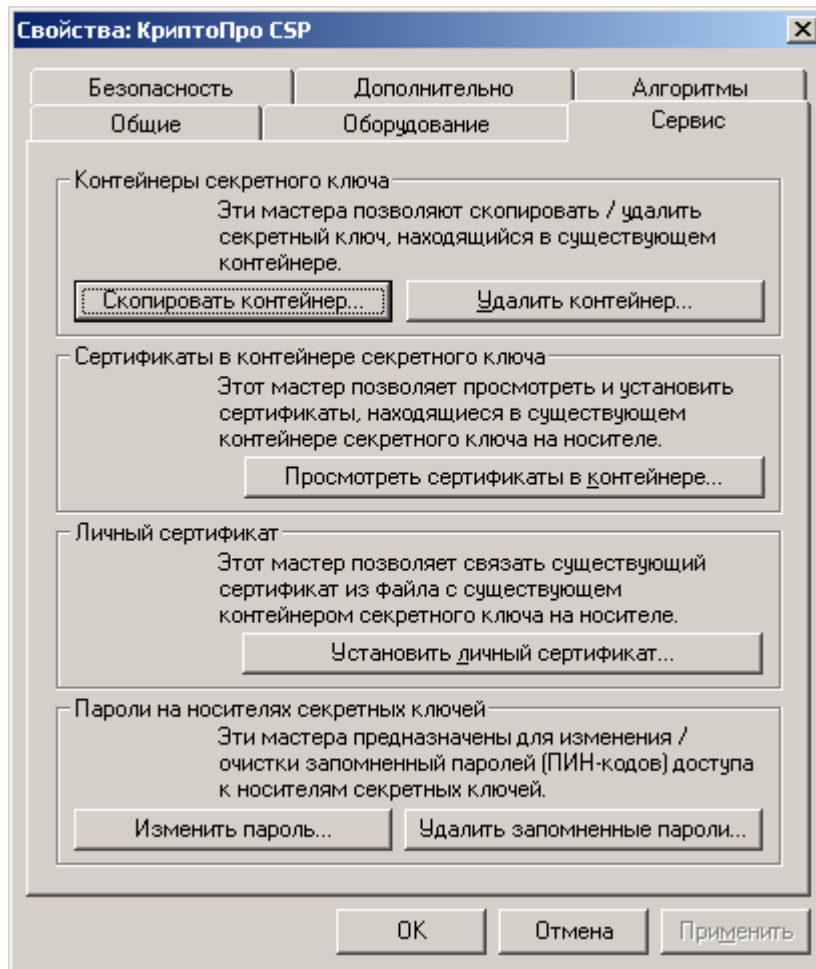


Примечание: Если в СКЗИ «КриптоПро CSP» настроено несколько датчиков случайных чисел, то при формировании исходной ключевой информации будет использоваться ДСЧ, находящийся в списке установленных ДСЧ в самой верхней строке. Например, если установлено два датчика случайных чисел - Биологический ДСЧ и ДСЧ Электронного замка «Соболь», они находятся в состоянии «подключен», и в верхней строке списка датчиков случайных чисел указан ДСЧ Электронного замка «Соболь», то формирование исходной ключевой информации будет осуществляться на ДСЧ Электронного замка «Соболь». Для использования Биологического ДСЧ, необходимо с помощью кнопок   переместить его на верхнюю позицию в списке.

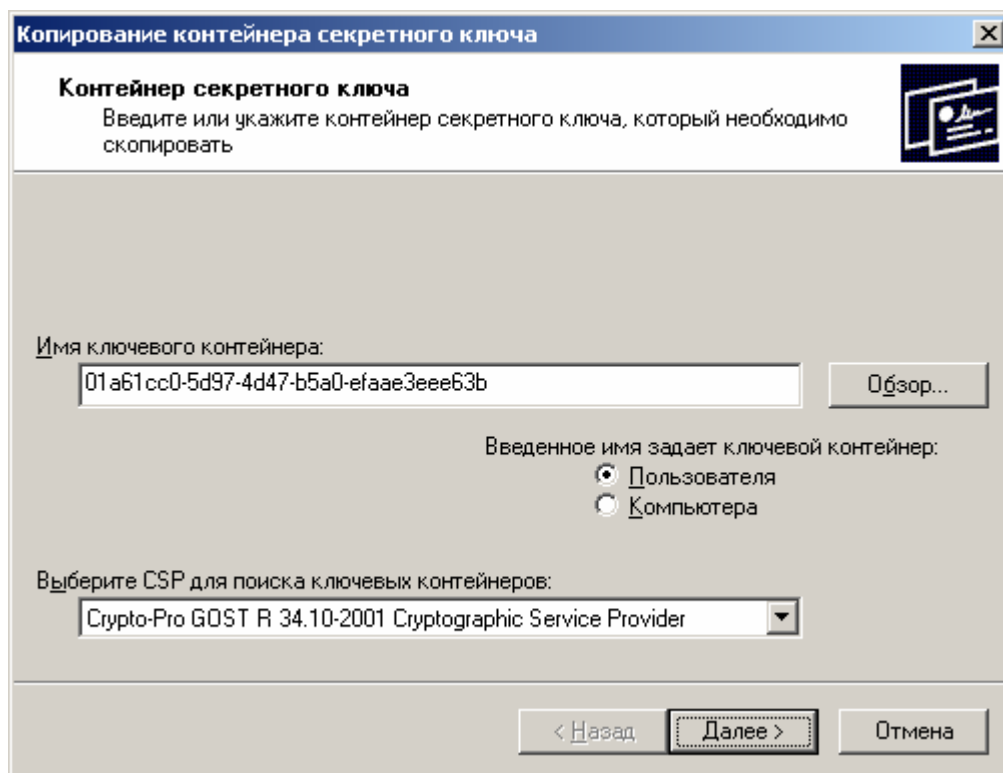
5. Копирование и удаление контейнера секретного ключа

5.1. Копирование контейнера секретного ключа

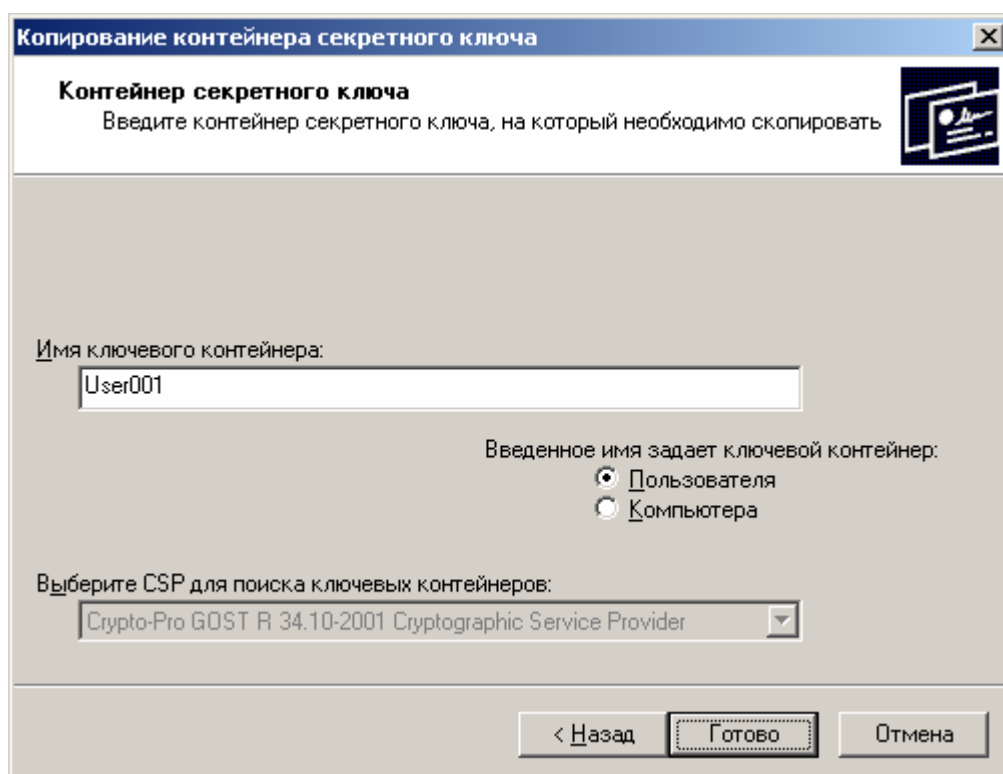
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Скопировать контейнер**



2. В окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер, и выберите необходимый криптопровайдер (CSP) из предлагаемого списка. Введите имя контейнера секретного ключа или с помощью кнопки **Обзор** выберите его из списка, нажмите кнопку **Далее**. При выводе окна **Введите пароль для контейнера** введите установленный пароль на доступ к секретному ключу

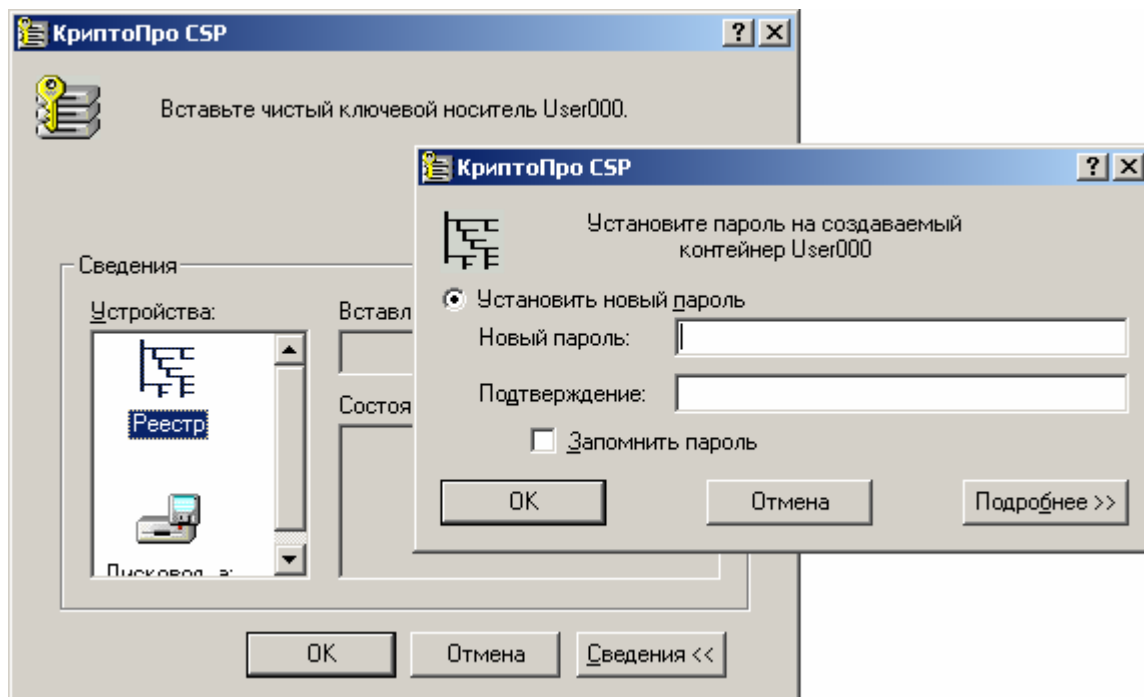


3. В открывшемся окне **Контейнер секретного ключа** введите имя нового ключевого контейнера и установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище требуется разместить скопированный контейнер. Нажмите кнопку **Готово**



4. В открывшемся окне выберите носитель, на котором требуется разместить скопированный контейнер. Вставьте носитель в считыватель и нажмите

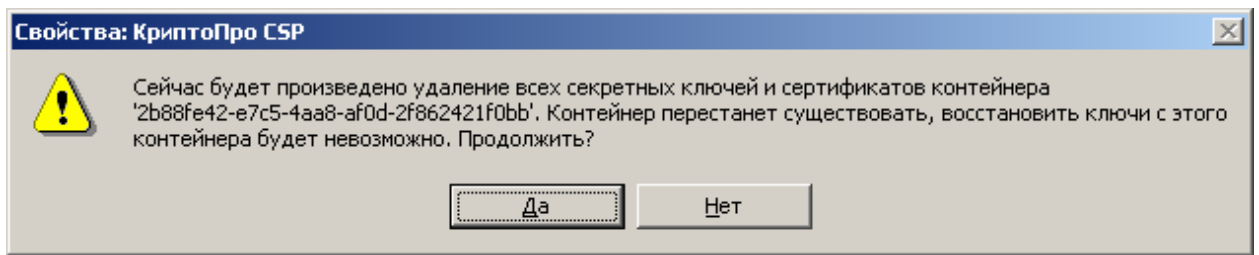
кнопку **ОК**. Откроется окно установки пароля на доступ к секретному ключу. Введите пароль, подтвердите его, при необходимости установите флаг **Запомнить пароль** (если данный флаг будет установлен, то пароль сохранится в специальном хранилище на локальном компьютере и при обращении к секретному ключу пароль будет автоматически считываться из этого хранилища а не вводиться пользователем). После ввода необходимых данных нажмите кнопку **ОК**



5. СКЗИ «КриптоПро CSP» осуществит копирование контейнера секретного ключа

5.2. Удаление контейнера секретного ключа

1. Откройте панель управления компьютером, используя пункты меню **Пуск, Настройка, Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Удалить контейнер**
2. В окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер, и выберите необходимый криптопровайдер (CSP) из предлагаемого списка. Введите имя контейнера секретного ключа, который необходимо удалить, или с помощью кнопки **Обзор** выберите его из списка, нажмите кнопку **Готово**
3. Откроется диалоговое окно подтверждения удаления ключевого контейнера. Нажмите кнопку **Да**

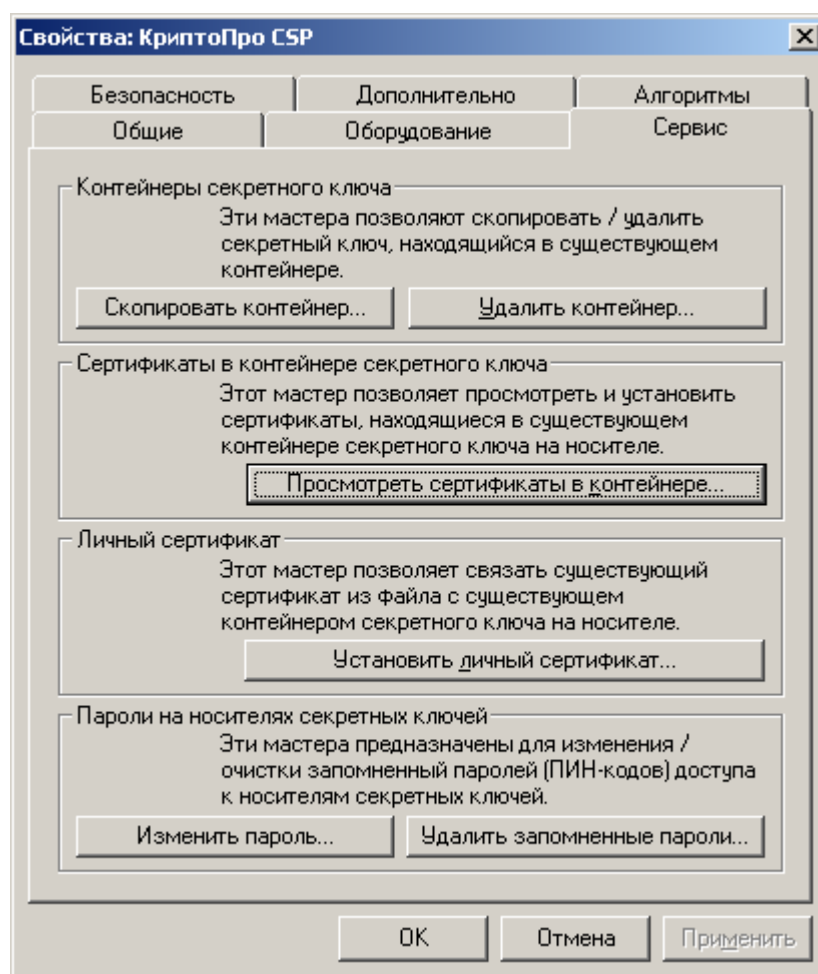


4. СКЗИ «КриптоПро CSP» произведет удаление ключевого контейнера

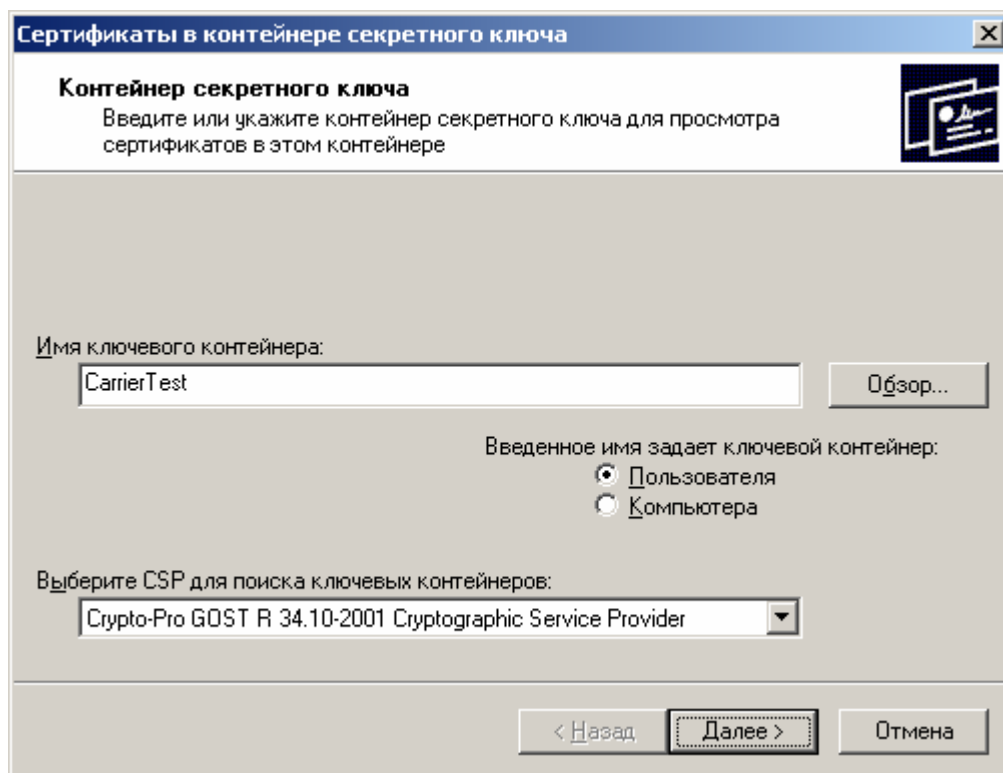
6. Просмотр и установка личного сертификата, хранящегося в контейнере секретного ключа

6.1. Просмотр сертификата, хранящегося в контейнере секретного ключа

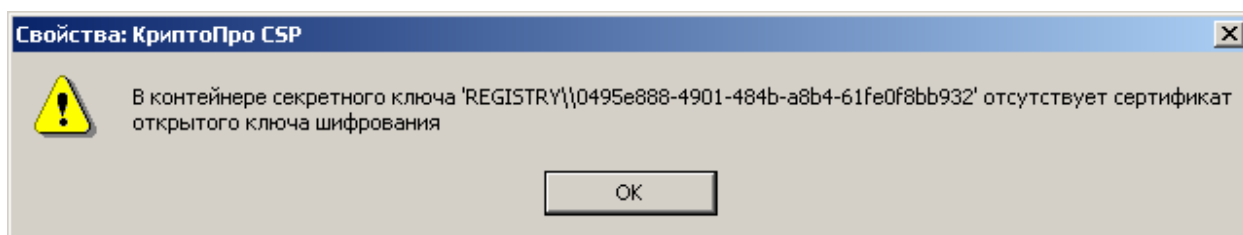
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Просмотреть сертификаты в контейнере**



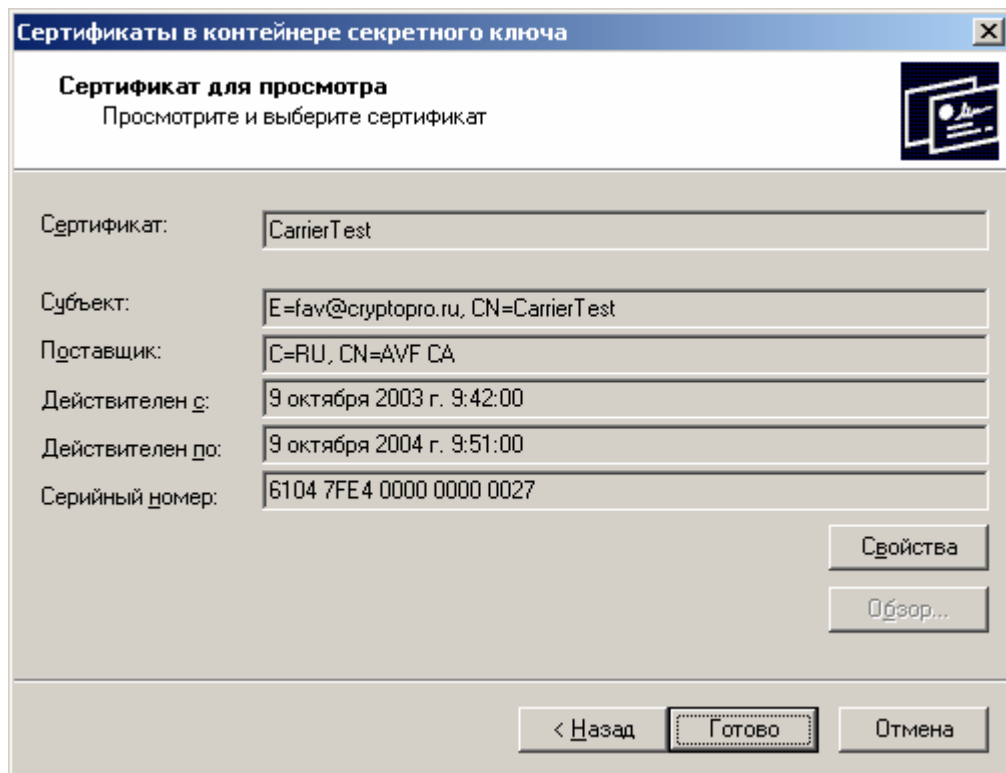
2. В окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер, и выберите необходимый криптопровайдер (CSP) из предлагаемого списка. Введите имя контейнера секретного ключа, в котором содержится сертификат, или с помощью кнопки **Обзор** выберите его из списка, нажмите кнопку **Далее**. При выводе окна **Введите пароль для контейнера** введите установленный пароль на доступ к секретному ключу



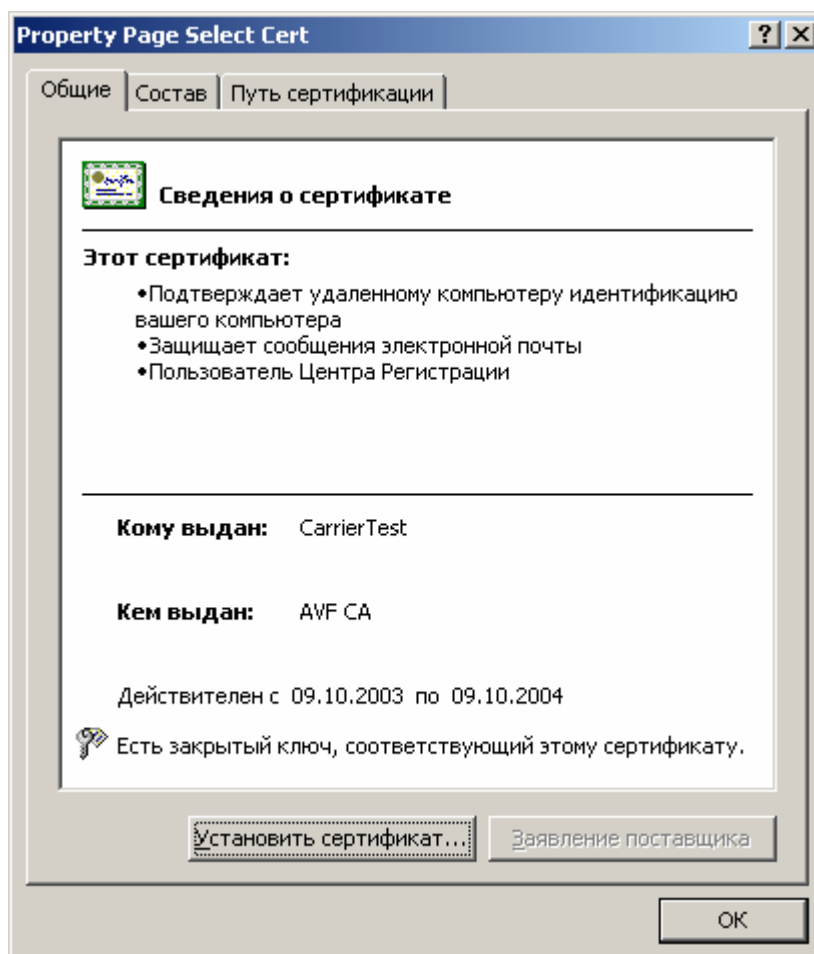
3. Если сертификата в контейнере секретного ключа нет, то откроется окно, информирующее пользователя об отсутствии сертификата в контейнере.



Если сертификат есть, то откроется окно **Сертификат для просмотра**



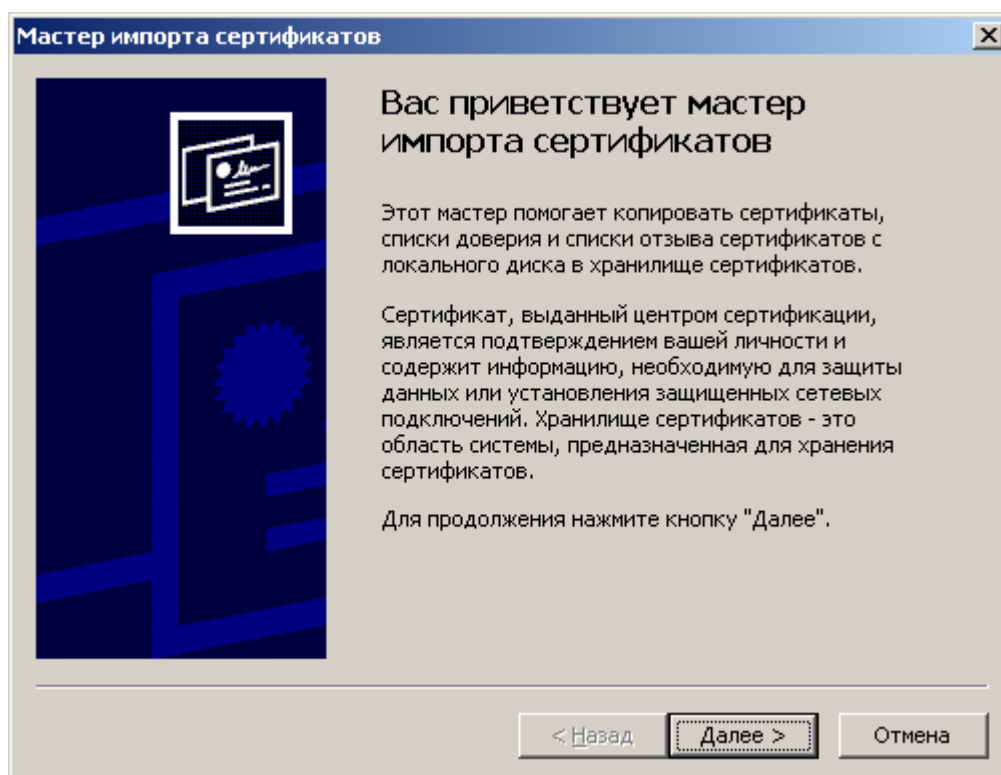
4. При нажатии на кнопку **Свойства** окна **Сертификат для просмотра** откроется стандартное окно просмотра сертификата



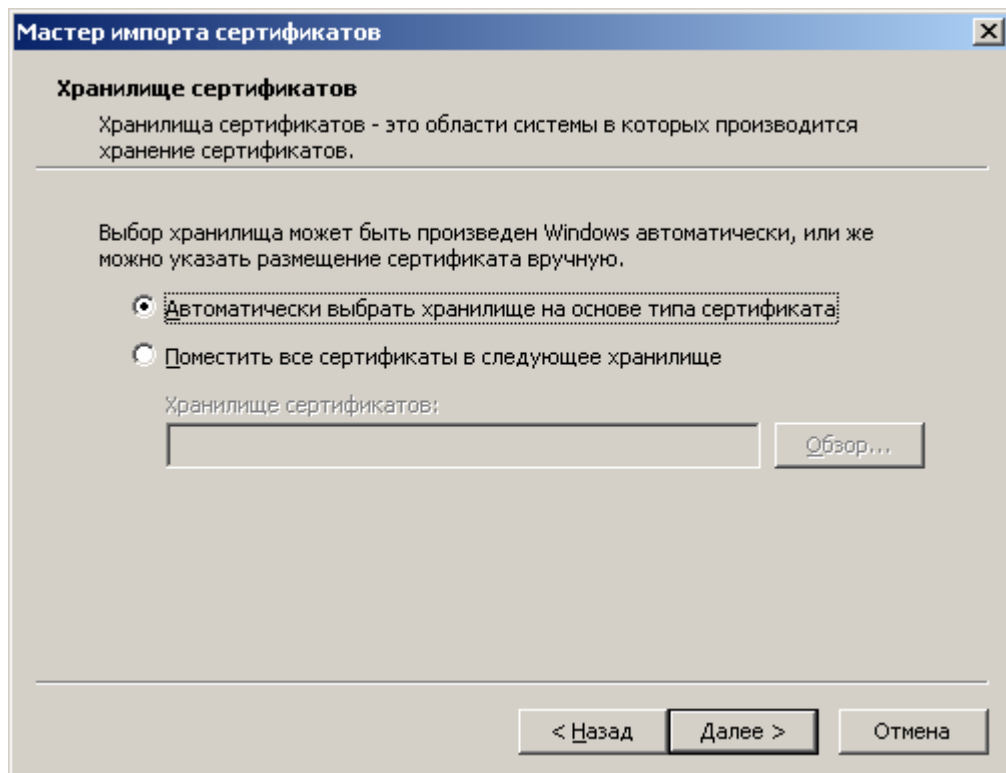
6.2. Установка личного сертификата, хранящегося в контейнере секретного ключа

Примечание: В данном разделе руководства под установкой личного сертификата понимается установка сертификата в хранилище Личные с формированием ссылки на секретный ключ, соответствующий данному сертификату.

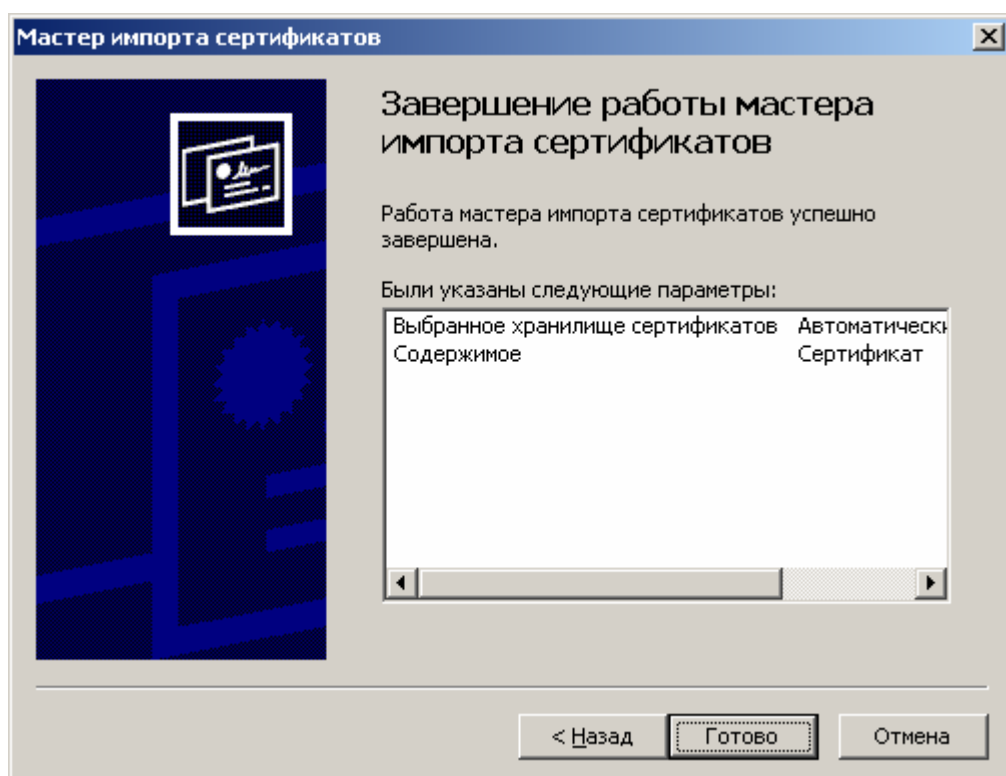
1. Осуществите последовательность действий, изложенных в пункте 6.1.
2. В стандартном окне просмотра сертификата нажмите кнопку **Установить сертификат**. Запустится **Мастер импорта сертификатов**. Нажмите кнопку **Далее**



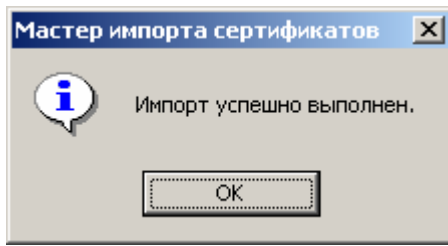
3. Откроется окно **Хранилище сертификатов**, в котором необходимо указать, в какое хранилище требуется поместить сертификат. Установите переключатель **Автоматически выбрать хранилище** на основе типа сертификата. Сертификат будет установлен в хранилище **Текущий пользователь/Личные** или в хранилище **Локальный компьютер/Личные** в зависимости от того, где расположен контейнер секретного ключа (см. п.2 пункта 6.1, переключатель **Компьютер/Пользователь**). Нажмите кнопку **Далее**



4. В окне **Завершение работы мастера импорта сертификатов** проверьте правильность выбранных параметров и нажмите кнопку **Готово**



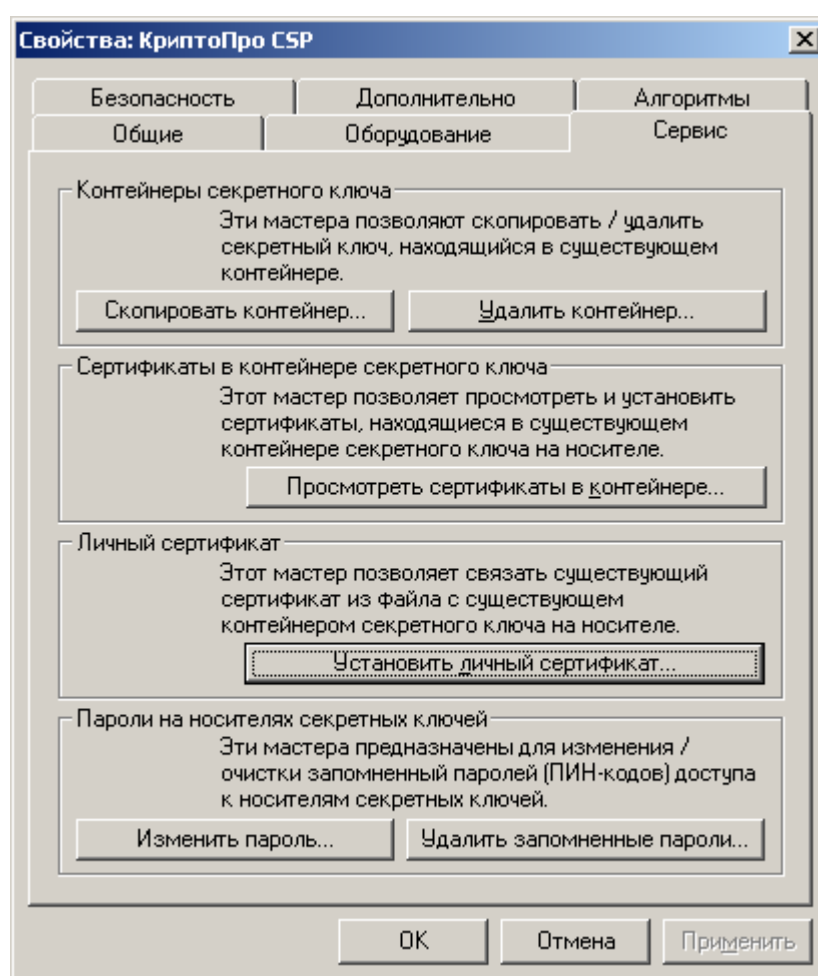
5. Появится окно, информирующее пользователя об успешной установке сертификата



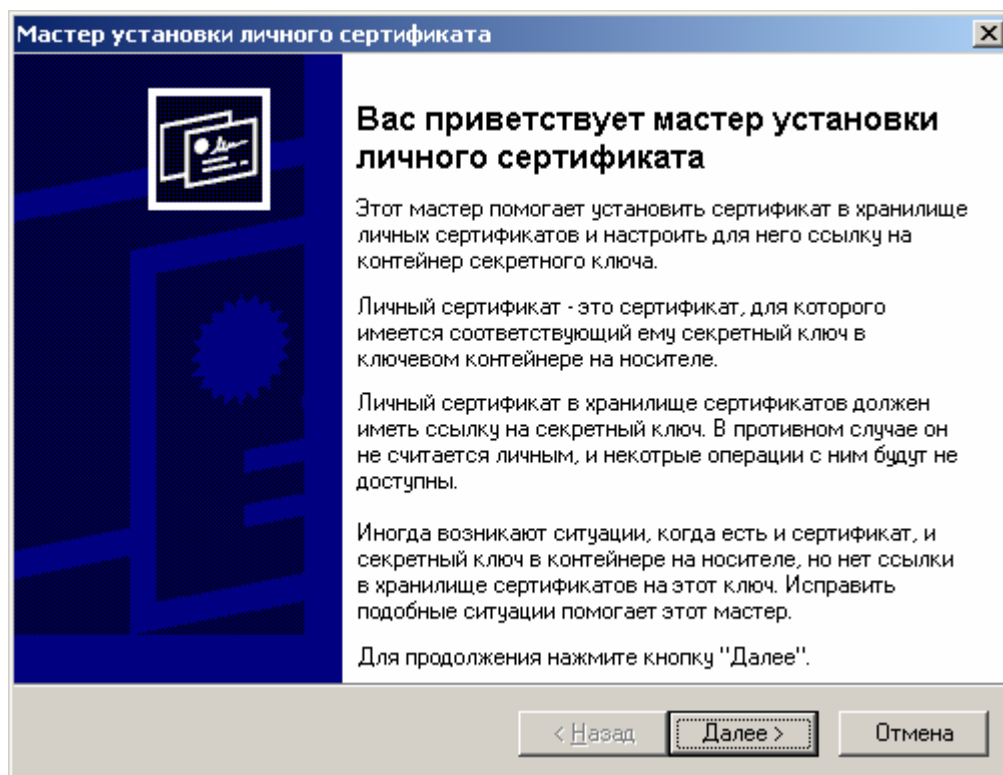
7. Установка личного сертификата, хранящегося в файле

Примечание: В данном разделе руководства под установкой личного сертификата понимается установка сертификата в хранилище Личные с формированием ссылки на секретный ключ, соответствующий данному сертификату.

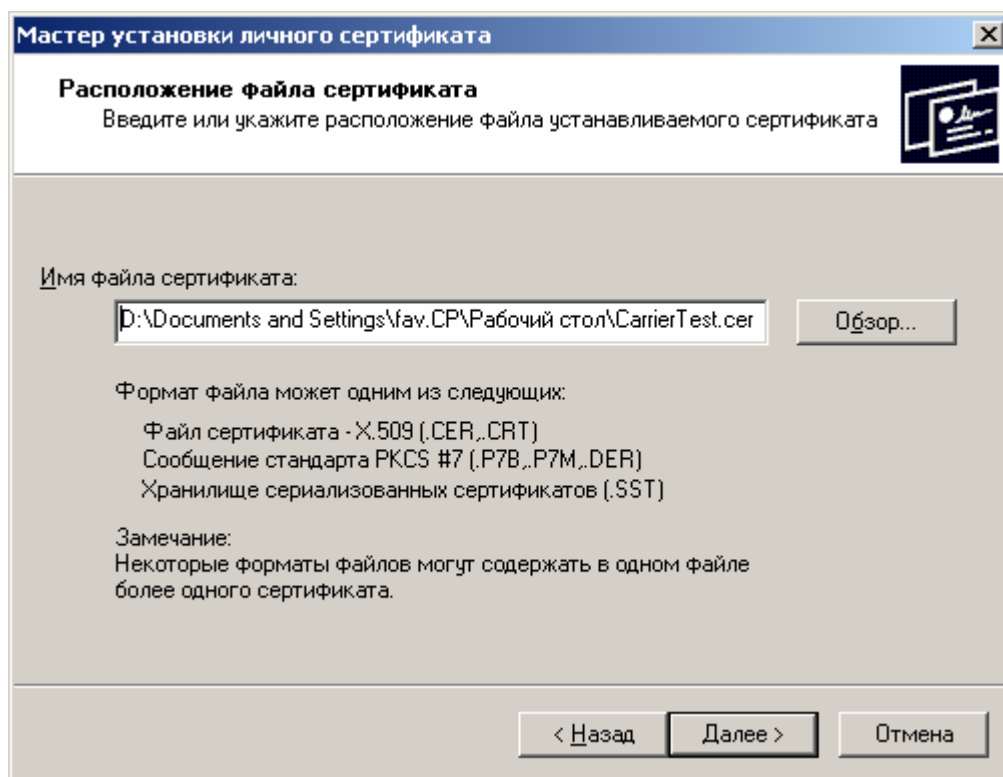
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Установить личный сертификат**



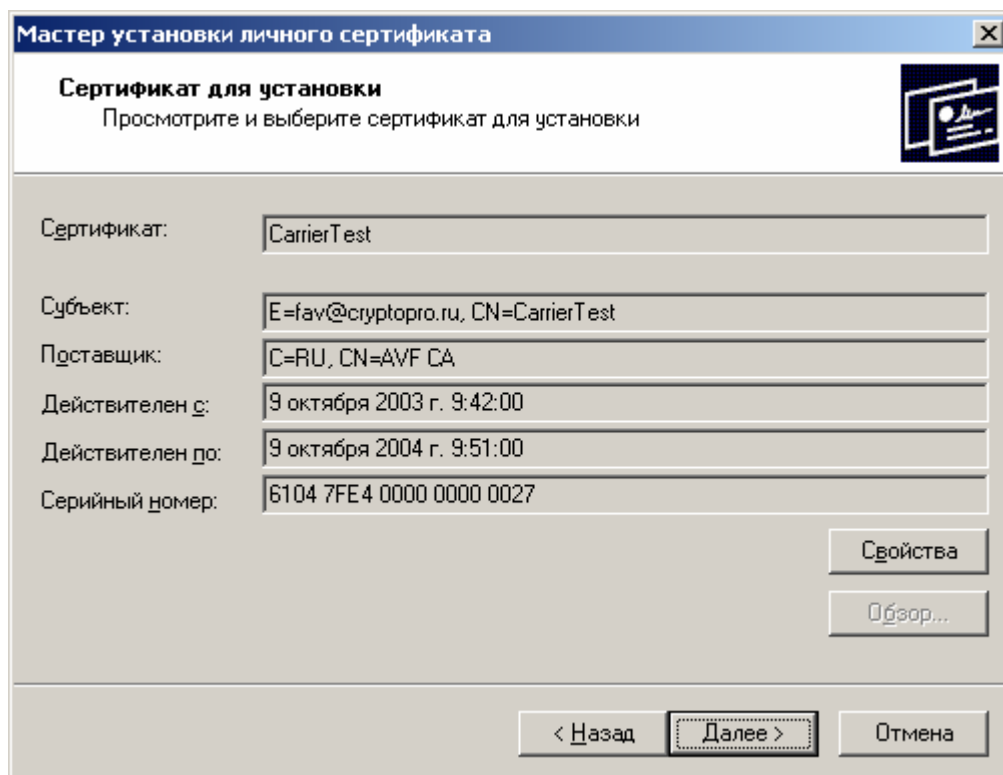
2. В появившемся окне **Мастер установки личного сертификата** ознакомьтесь с текстом и нажмите кнопку **Далее**



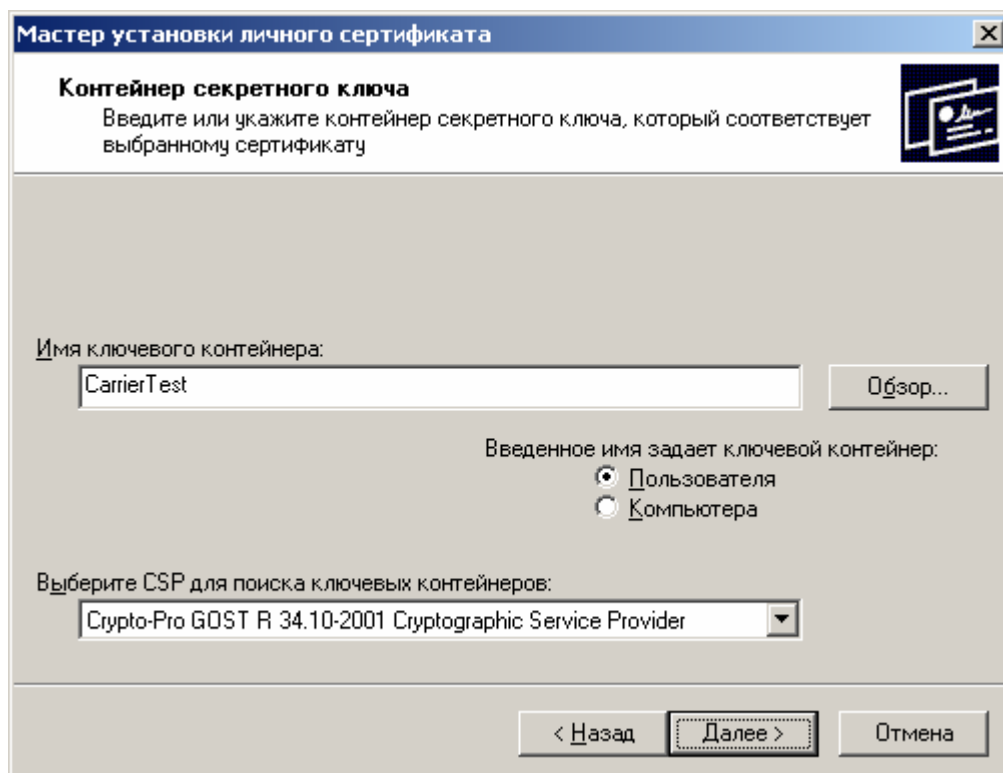
3. Откроется окно **Расположение файла сертификата**. Укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее**



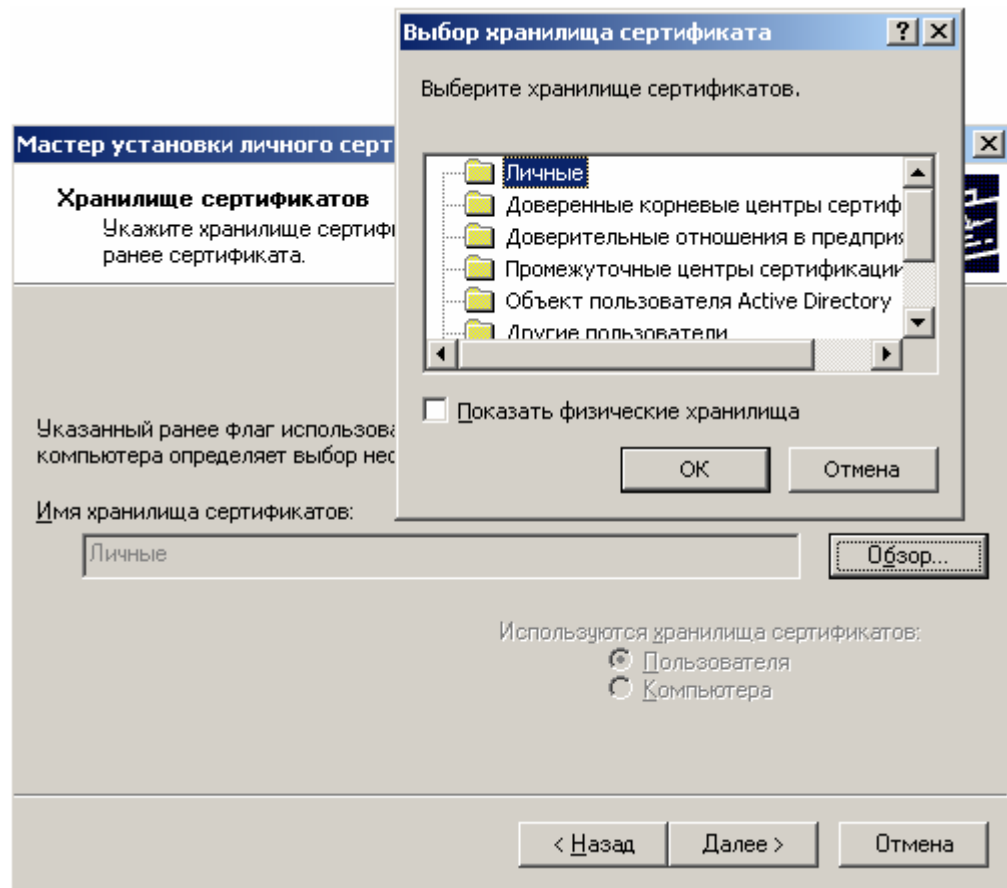
4. В окне **Сертификат для установки** выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть сертификат в стандартном окне просмотра сертификата. Нажмите кнопку **Далее**



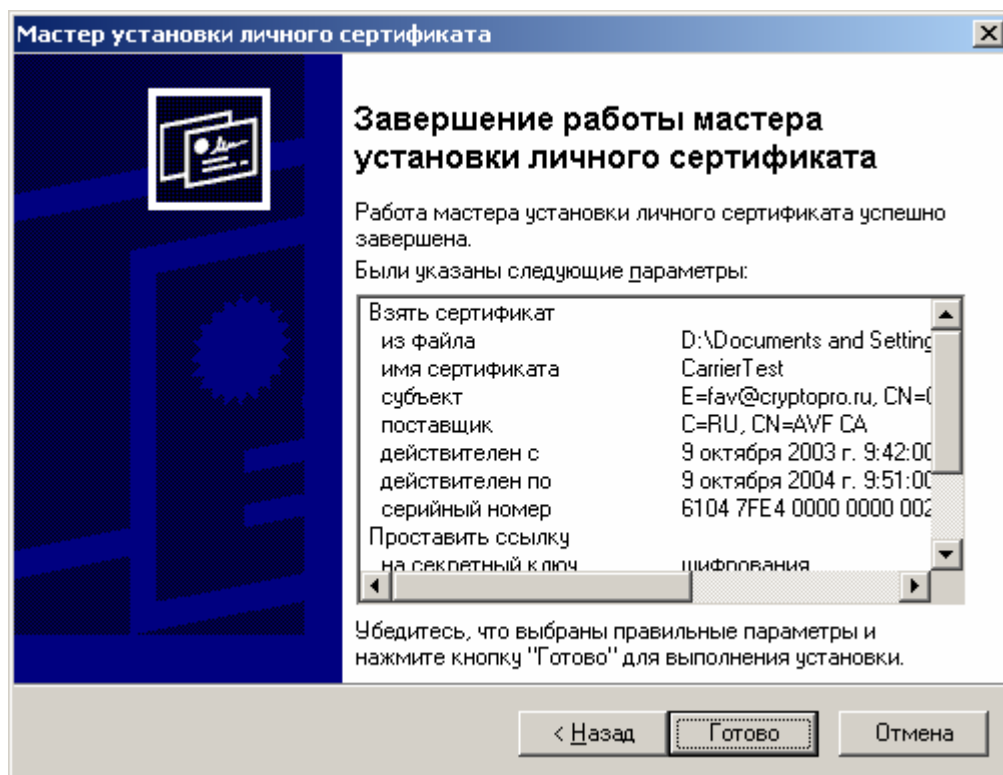
5. В появившемся окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер, и выберите необходимый криптопровайдер (CSP) из предлагаемого списка. Введите имя контейнера секретного ключа, связанного с устанавливаемым сертификатом, или с помощью кнопки **Обзор** выберите его из списка, нажмите кнопку **Далее**. При выводе окна **Введите пароль для контейнера** введите установленный пароль на доступ к секретному ключу



6. Откроется окно **Хранилище сертификатов**. С помощью кнопки **Обзор** выберите хранилище **Личные**. Сертификат будет установлен в хранилище **Текущий пользователь/Личные** или **Локальный компьютер/Личные** в зависимости от значения переключателя **Пользователь/Компьютер**. Изменить значение переключателя **Пользователь/Компьютер** нельзя, оно определяется расположением контейнера секретного ключа (см. предыдущий пункт)



7. Откроется окно **Завершение работы мастера установки личного сертификата**. Проверьте правильность указанных данных и нажмите кнопку **Готово**

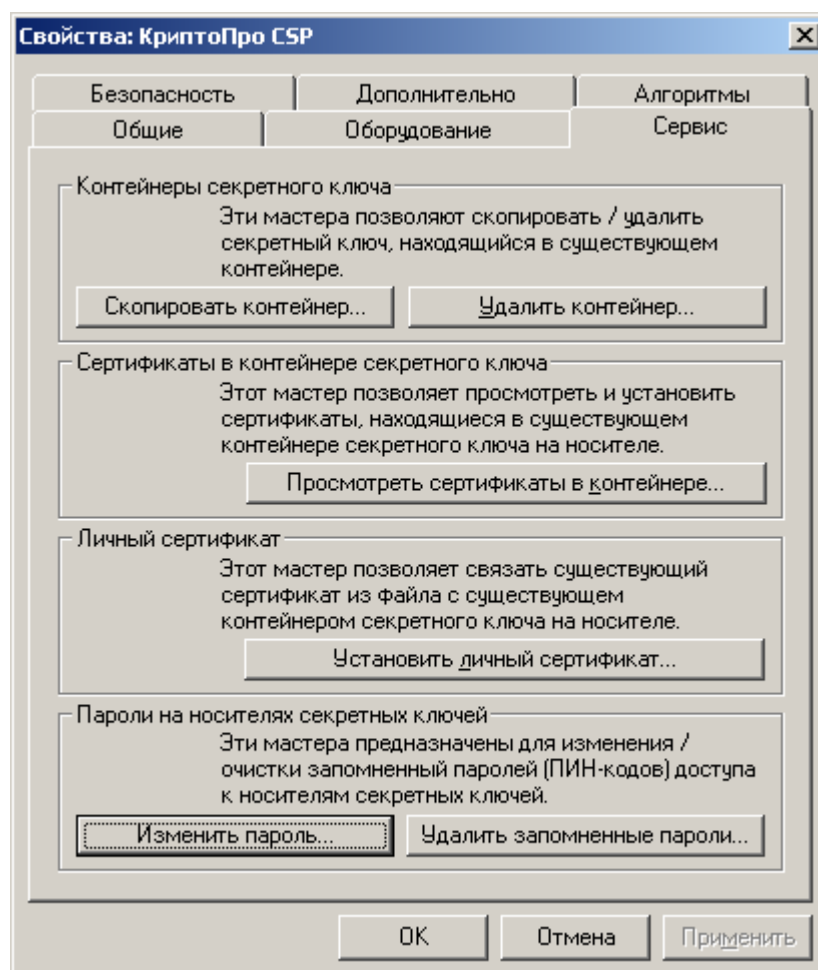


8. СКЗИ «КриптоПро CSP» произведет установку сертификата

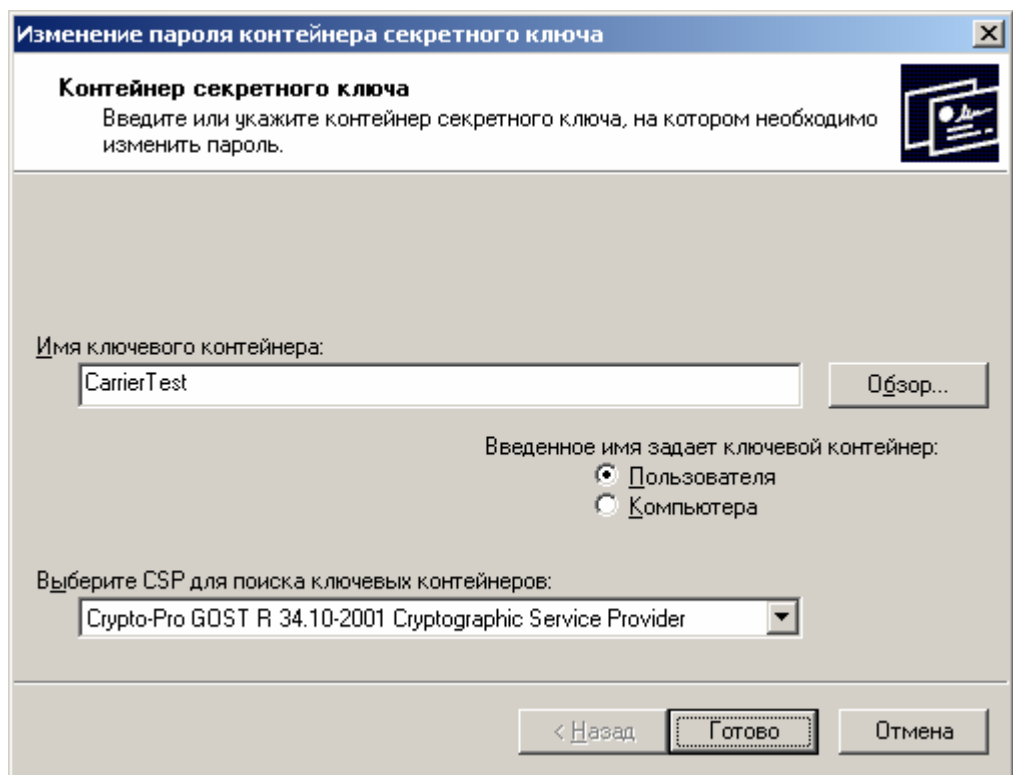
8. Управление паролями доступа к секретным ключам

8.1. Изменение пароля на доступ к секретному ключу

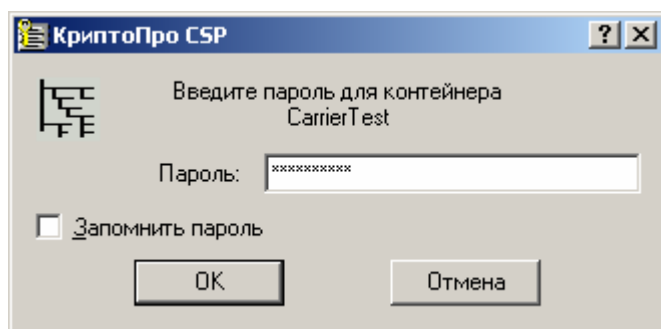
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Изменить пароль**



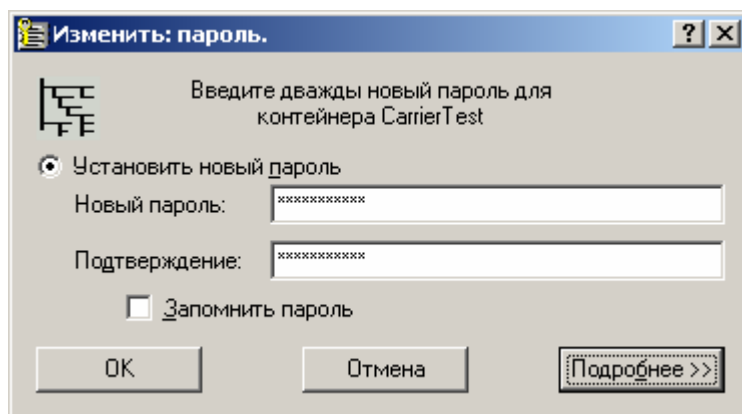
2. В появившемся окне **Контейнер секретного ключа** установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище расположен контейнер, и выберите необходимый криптопровайдер (CSP) из предлагаемого списка. Введите имя контейнера для смены пароля доступа к секретному ключу, или с помощью кнопки **Обзор** выберите его из списка, нажмите кнопку **Готово**



3. Откроется окно ввода пароля на доступ к секретному ключу выбранного контейнера. Введите указанный пароль и нажмите кнопку **OK**

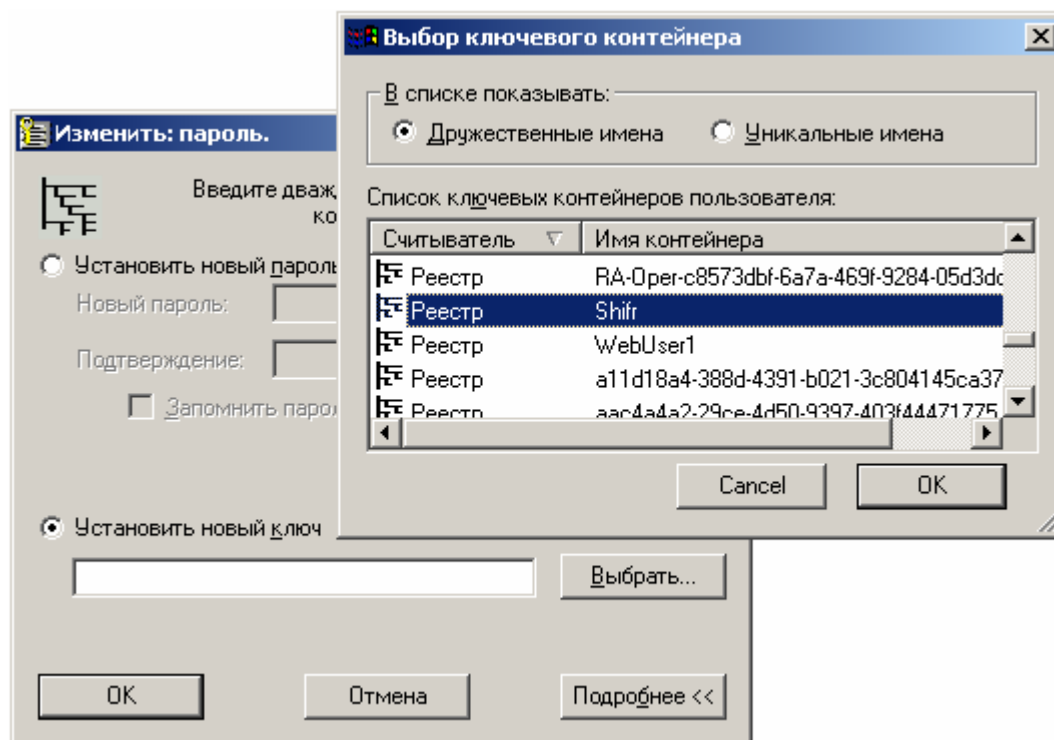


4. Откроется окно ввода нового пароля на доступ к секретному ключу. Введите дважды новый пароль и нажмите кнопку **OK**



5. СКЗИ «КриптоПро CSP» осуществит смену пароля на доступ к секретному ключу

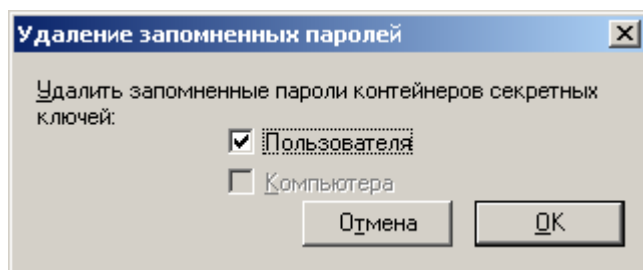
Примечание: Вместо установки пароля на доступ к секретному ключу СКЗИ «КриптоПро CSP» позволяет зашифровать данный секретный ключ на другом секретном ключе. Для этого необходимо в окне ввода нового пароля нажать кнопку **Подробнее**, выбрать переключатель **Установить новый ключ** и ввести имя контейнера (или выбрать контейнер из списка с помощью кнопки **Выбрать**), содержащего секретный ключ, на котором будет осуществлено шифрование исходного секретного ключа.



8.2. Удаление запомненных паролей

СКЗИ «КриптоПро CSP» позволяет сохранить в специальном хранилище локального компьютера пароли на доступ к контейнеру секретного ключа (сохранение осуществляется установкой флага **Запомнить пароль** в окне ввода пароля на доступ к секретному ключу). Если пароль сохранен в данном хранилище, то при обращении к секретному ключу пароль автоматически будет считан из контейнера без появления окна для ввода пароля. Для удаления сохраненных паролей необходимо осуществить следующие действия:

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Сервис**. Нажмите кнопку **Удалить запомненные пароли**
2. В появившемся окне **Удаление запомненных паролей** установите флаги **Пользователя/Компьютера** для удаления сохраненных на локальном компьютере в специальном хранилище паролей и нажмите кнопку **OK**. Если сохраненных паролей нет, то соответствующая область будет затемнена



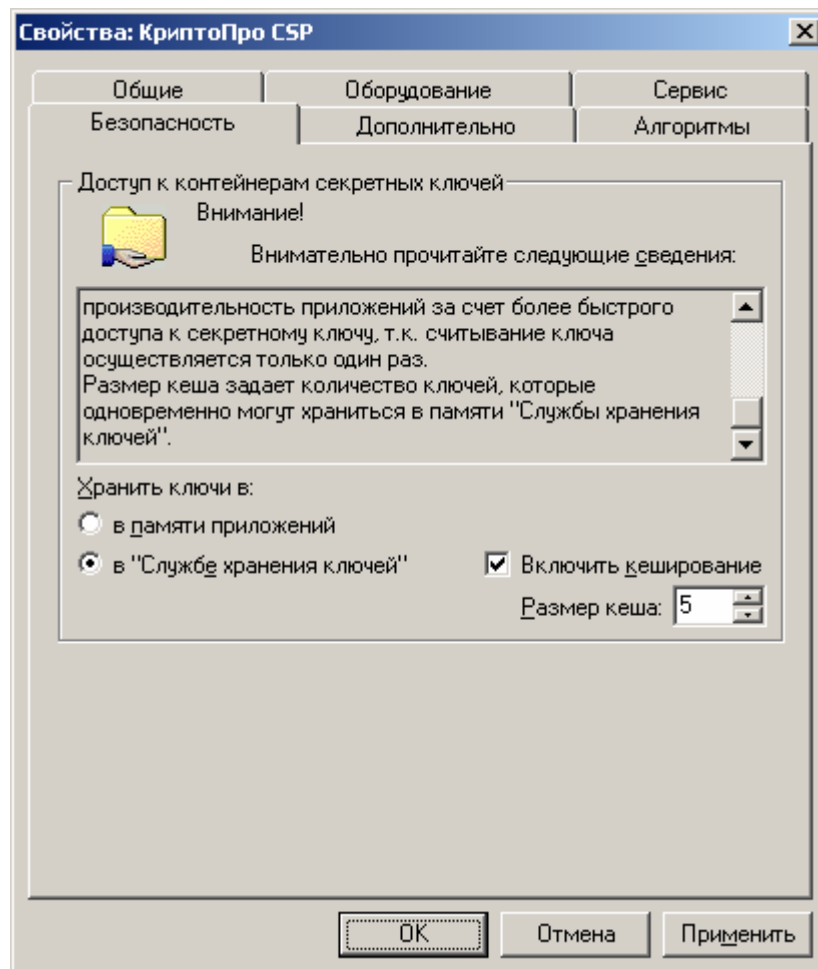
3. СКЗИ «КриптоПро CSP» осуществит удаление сохраненных паролей только из специального хранилища на локальном компьютере, пароль на доступ к секретному ключу не удаляется.

9. Установка режимов хранения секретных ключей

СКЗИ «КриптоПро CSP» обеспечивает два режима хранения ключей: в памяти приложений и в «Службе хранения ключей». Хранение ключей в «Службе хранения ключей» обеспечивает дополнительную их защиту от других приложений. При использовании «Службы хранения ключей» возможно применение кэширования контейнеров секретных ключей. Это кэширование заключается в том, что считанные с носителя ключи запоминаются в памяти «Службы хранения ключей» в кеше. Кэширование контейнеров позволяет увеличить производительность приложений за счет более быстрого доступа к секретному ключу, т.к. считывание ключа осуществляется только один раз. Размер кеша задает количество ключей, которые одновременно могут храниться в памяти «Службы хранения ключей»

Для установки режима службы хранения секретных ключей необходимо осуществить следующие действия:

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Безопасность**



2. Внимательно ознакомьтесь со сведениями, приведенными в этом окне. Осуществите установку необходимого режима хранения секретных ключей.

Примечание: Если на доступ к секретному ключу установлен пароль, пароль не сохранен на локальном компьютере, секретный ключ находится в кеше «Службы

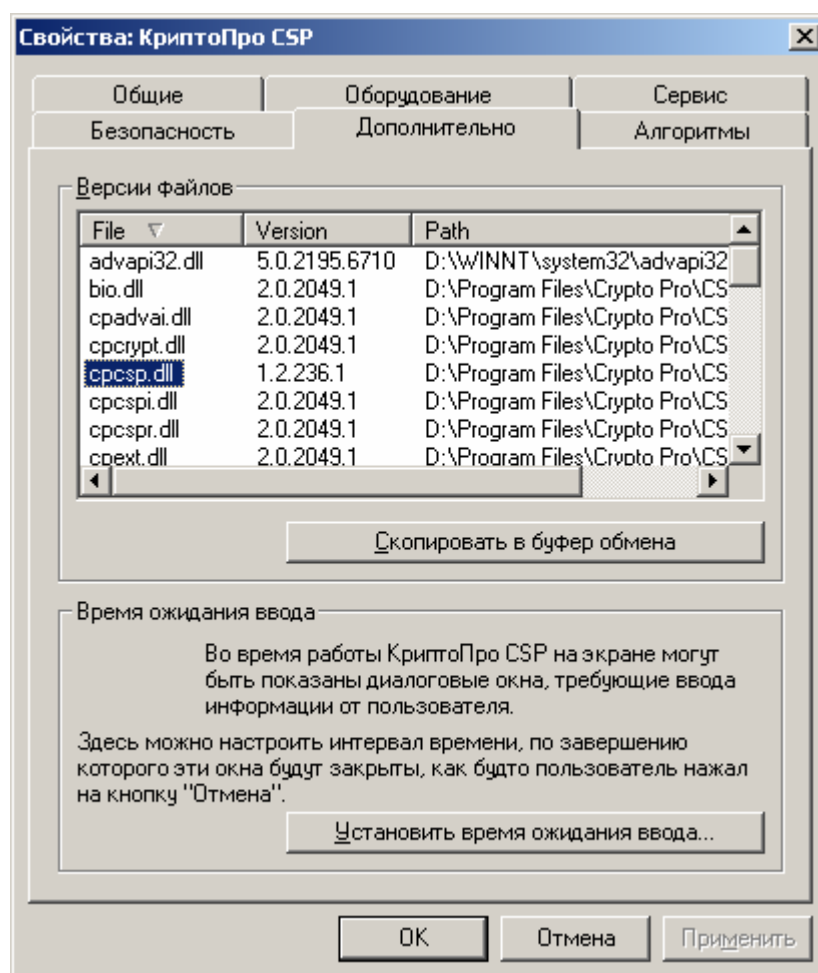
хранения ключей» (ранее к нему уже был осуществлен доступ), то обращение к данному секретному ключу произойдет без появления окна ввода пароля пользователя – ключ автоматически считывается из кеша.

СКЗИ «КриптоПро CSP» не осуществляет кеширование секретных ключей, связанных с сертификатами, установленными в хранилище сертификатов Локального компьютера (например, секретных ключей Центра сертификации, Web-сервера).

10. Просмотр версий используемых файлов

Для просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов:

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Дополнительно**

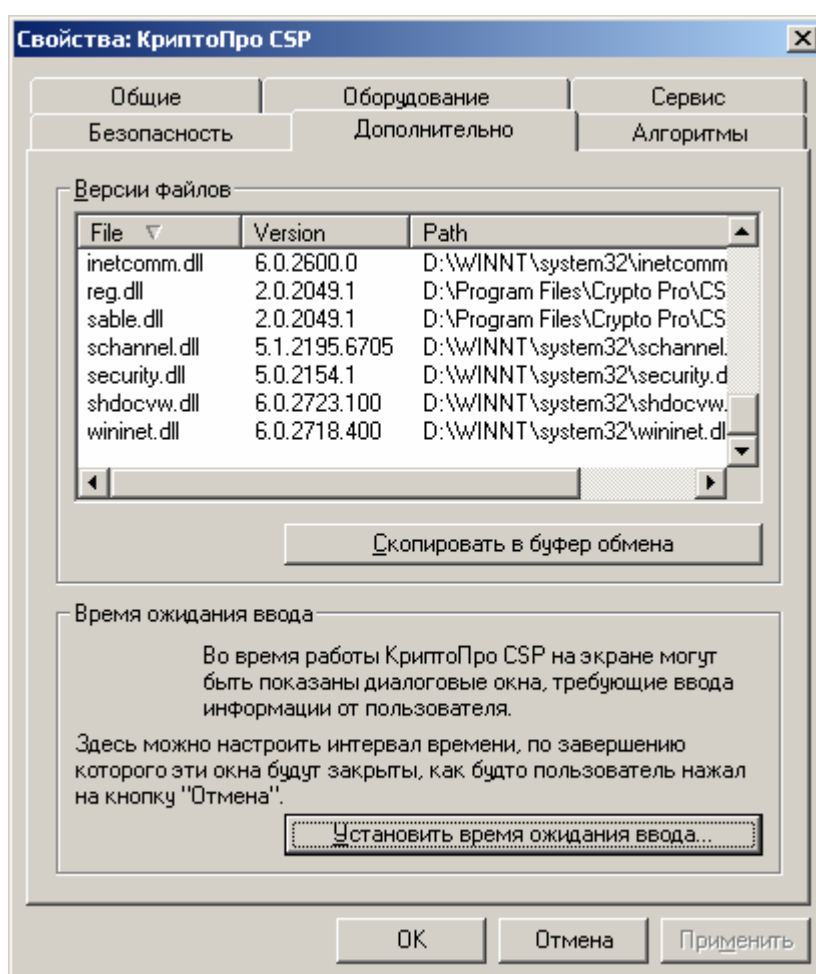


2. В области **Версии файлов** в табличной форме представлена информация о версиях и путях размещения используемых СКЗИ «КриптоПро CSP» файлов. Нажатие на кнопку **Скопировать в буфер обмена** приведет к сохранению данной информации в буфер обмена.

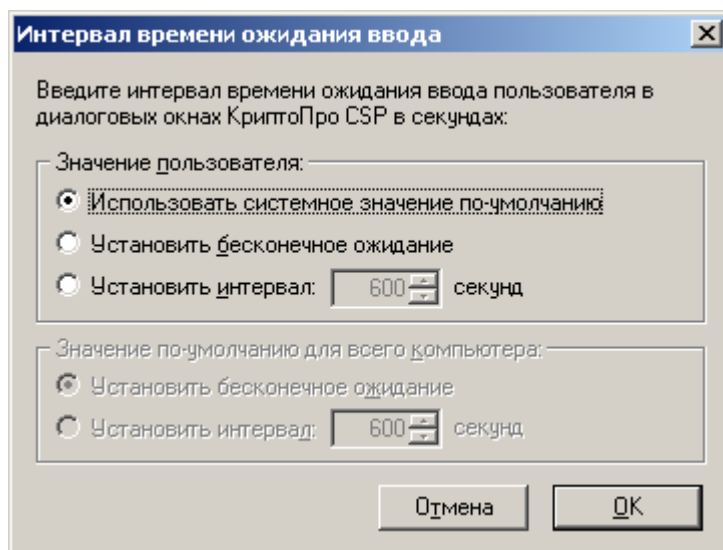
11. Установка времени ожидания ввода информации от пользователя

Во время работы СКЗИ «КриптоПро CSP» на экране могут появляться диалоговые окна, требующие ввода пользователем определенных данных (например, ввод пароля на доступ к секретному ключу). Для установки интервала времени по завершении которого эти окна будут автоматически закрыты (действие, эквивалентное нажатию пользователем кнопки **Отмена**) необходимо произвести следующие действия:

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Дополнительно**. Нажмите кнопку **Установить время ожидания ввода**



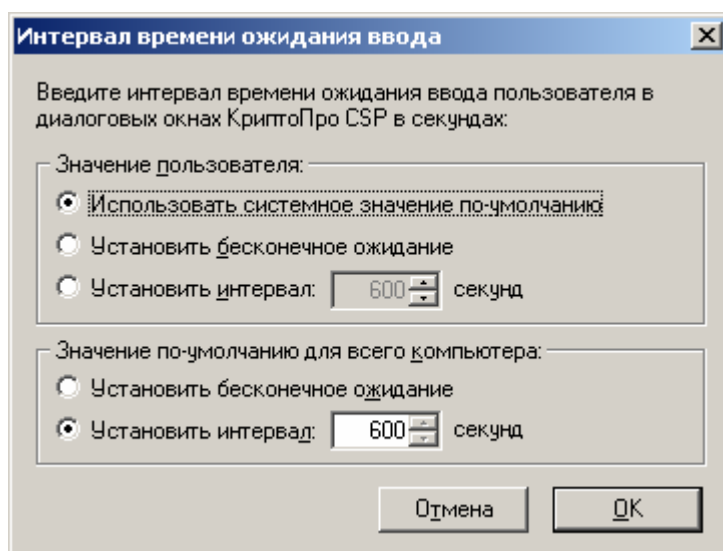
2. Откроется окно **Интервал времени ожидания ввода**. Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**



Пользователь, не являющийся администратором на локальном компьютере может осуществить только установку переключателя **Значение пользователя** (переключатель **Значение по умолчанию для всего компьютера** будет затемнен) в одно из следующих положений:

- **Использовать системное значение по умолчанию** – устанавливает значение, определенное переключателем **Значение по умолчанию для всего компьютера**;
- **Установить бесконечное ожидание** – устанавливает бесконечное ожидание ввода данных пользователя;
- **Установить интервал** – определяет интервал времени, во время которого пользователь должен ввести данные.

3. Изменить переключатель **Значение по умолчанию для всего компьютера** может только пользователь, являющийся администратором локального компьютера



Примечание: **Значение пользователя** имеет больший приоритет по отношению к **Значению по умолчанию для всего компьютера** (например, если значение переключателя **Значение по умолчанию для всего компьютера** установлено в положение **Установить интервал - 600 секунд**, а переключатель **Значение пользователя** в положение

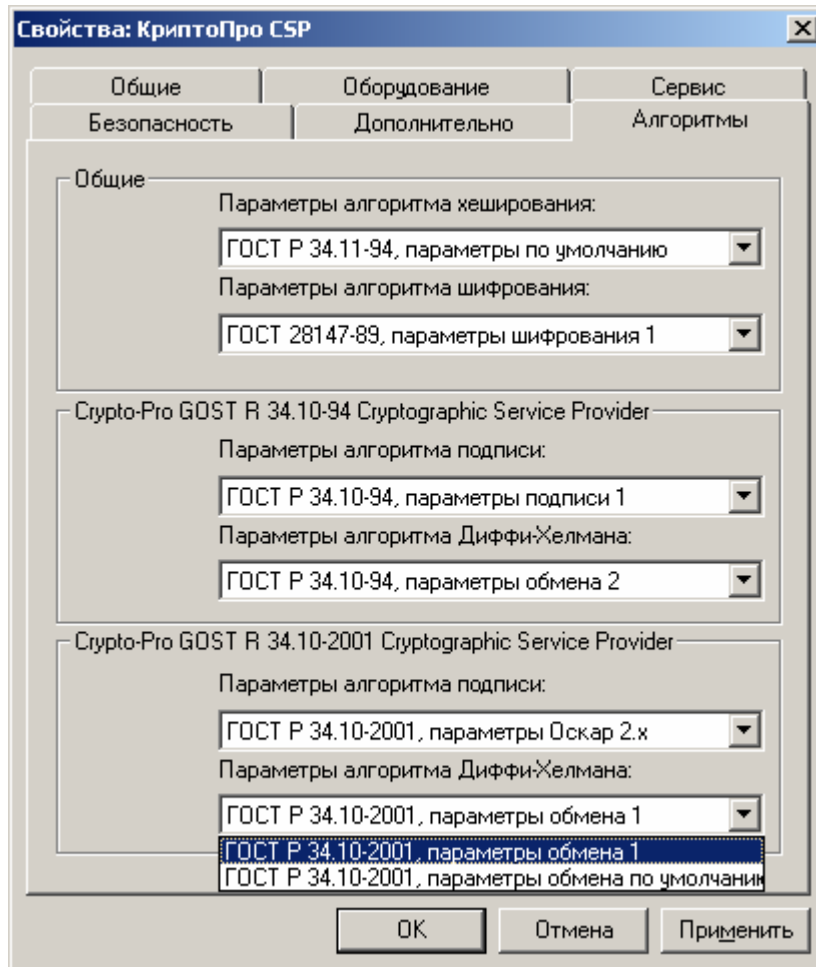
Установить бесконечное ожидание, то действительным будет значение – **Установить бесконечное ожидание**).

12. Установка параметров криптографических алгоритмов

СКЗИ «КриптоПро CSP» обеспечивает возможность установки различных параметров реализованных криптографических алгоритмов.

Для установки параметров криптографических алгоритмов необходимо осуществить следующую последовательность действий:

1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите значок **КриптоПро CSP**. Откроется окно **Свойства: КриптоПро CSP**. Выберите вкладку **Алгоритмы**

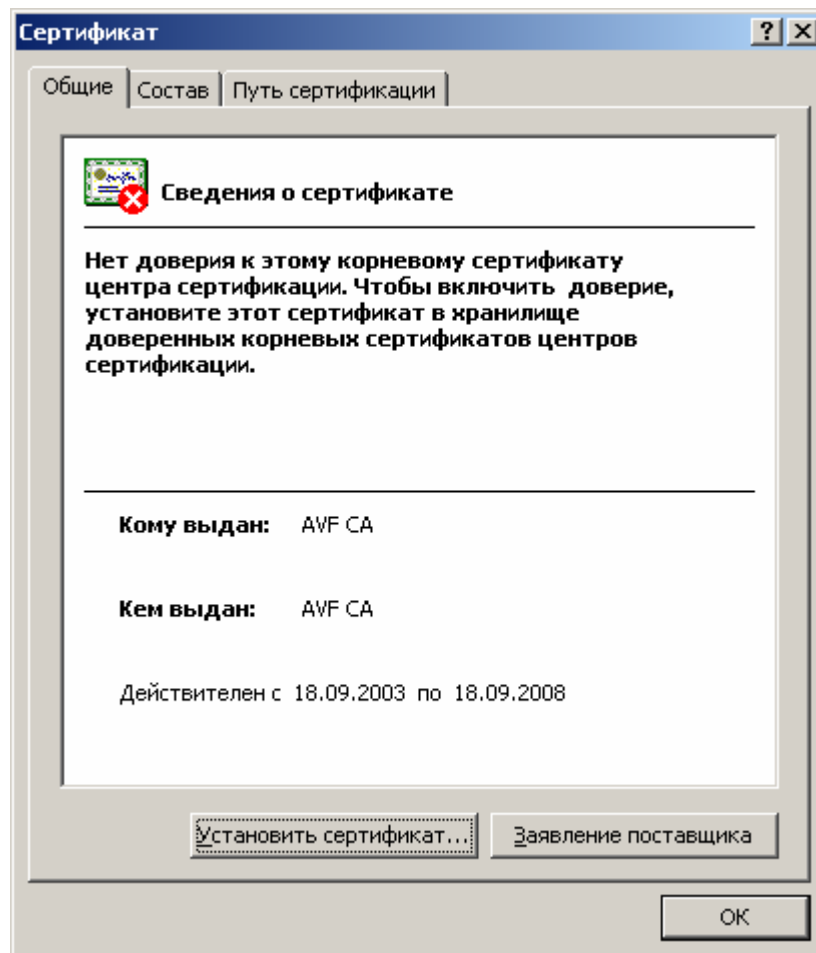


2. На вкладке **Алгоритмы** в области **Общие** осуществляется установка параметров алгоритма хэширования – ГОСТ Р 34.11-94 и параметров алгоритма шифрования – ГОСТ 28147-89 (начальный вектор хэширования и блок подстановок). В области **Crypto-Pro GOST R 34.10-94 Cryptographic Service Provider** – установка параметров алгоритма выработки и проверки электронной цифровой подписи – ГОСТ Р 34.10-94 (параметры **a, p, q**) и параметров алгоритма Диффи-Хелмана для ГОСТ Р 34.10-94. В области **Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider** – установка параметров алгоритма формирования и проверки электронной цифровой подписи – ГОСТ Р 34.10-2001 (параметры **p, (a, b; J), m, q, P(x_p, y_p)**) и параметров алгоритма Диффи-Хелмана для ГОСТ Р 34.10-2001.

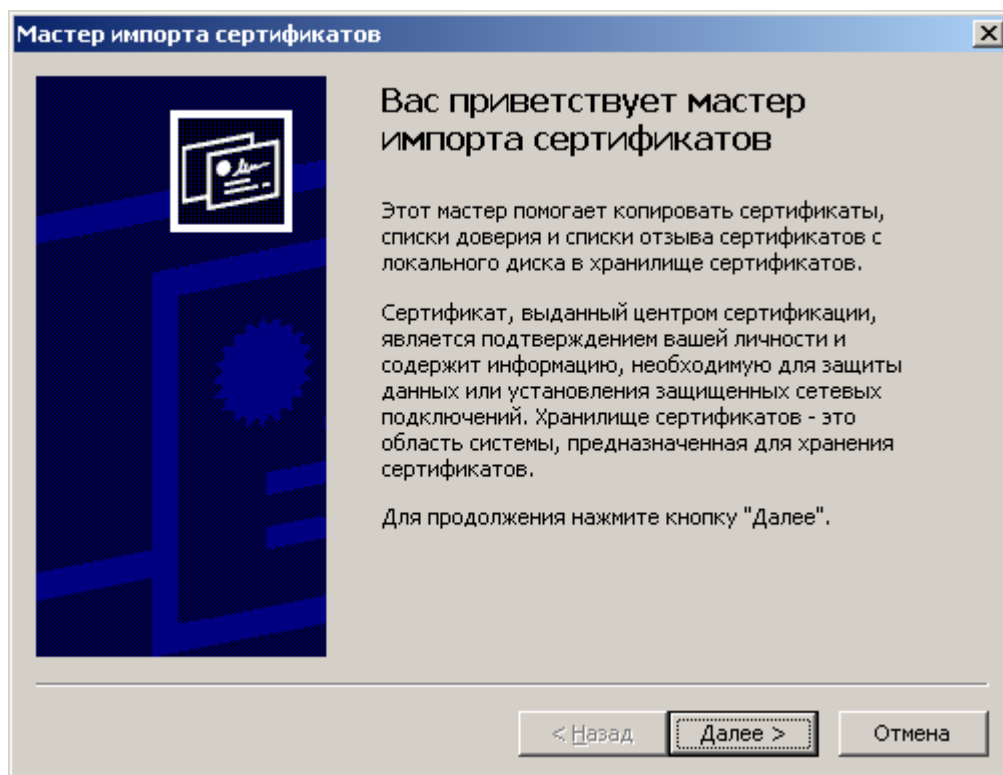
13. Установка сертификата Центра сертификации

13.1. Установка сертификата корневого центра сертификации

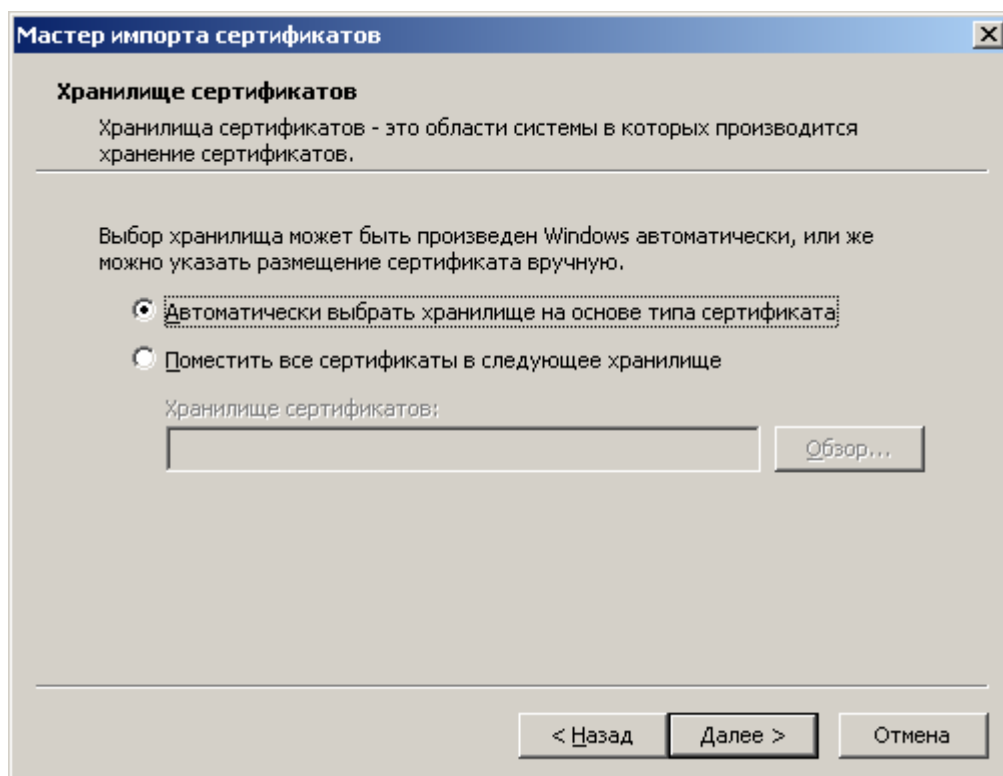
1. В стандартном проводнике MS Windows выберите файл, содержащий сертификат корневого центра сертификации, двойным нажатием левой кнопки мыши запустите его. Откроется стандартное окно просмотра сертификатов. Нажмите кнопку **Установить сертификат**



2. Откроется окно **Мастер импорта сертификатов**. Нажмите кнопку **Далее**



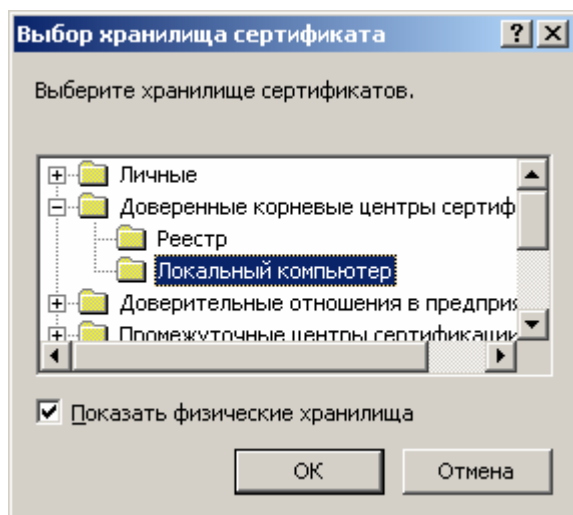
3. Откроется окно **Хранилище сертификатов**



При установке переключателя в положение **Автоматически выбрать хранилище на основе типа сертификата** сертификат корневого центра сертификации будет установлен в хранилище **Текущий пользователь/Доверенные корневые центры сертификации**.

При установке переключателя в положение **Поместить все сертификаты в следующее хранилище** возможно установить сертификат в хранилище, выбираемое из списка.

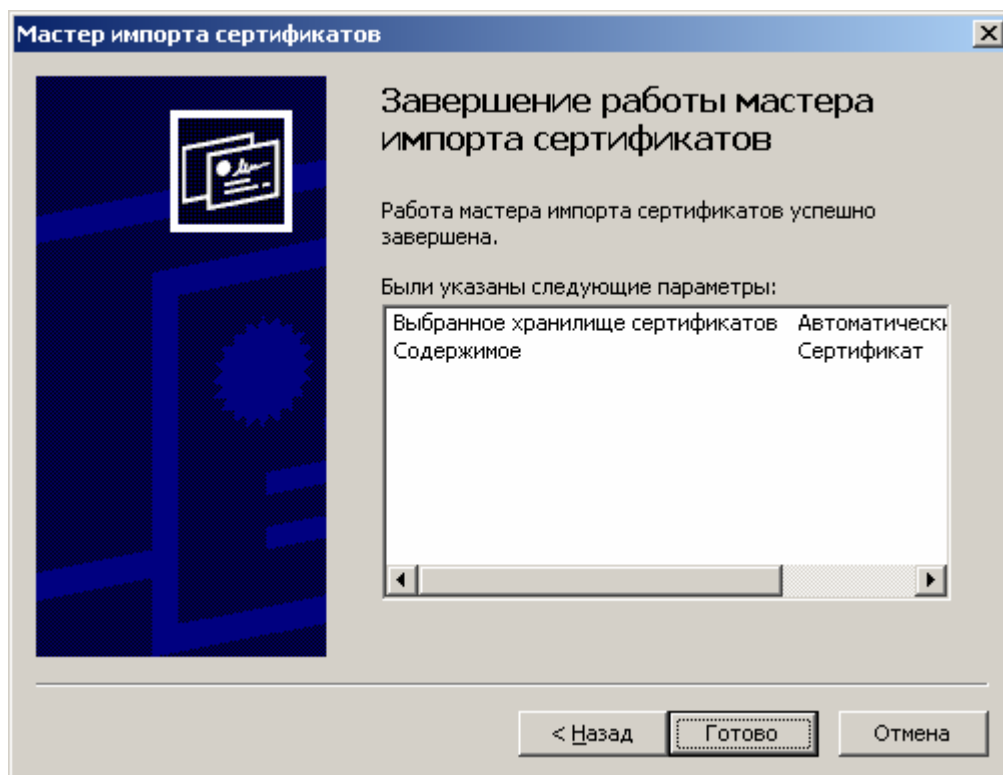
Для установки сертификата корневого центра сертификации в хранилище **Локальный компьютер/Доверенные корневые центры сертификации** необходимо в окне **Выбор хранилища сертификата** установить флаг **Показать физические хранилища** и выбрать хранилище **Доверенные корневые центры сертификации/Локальный компьютер**



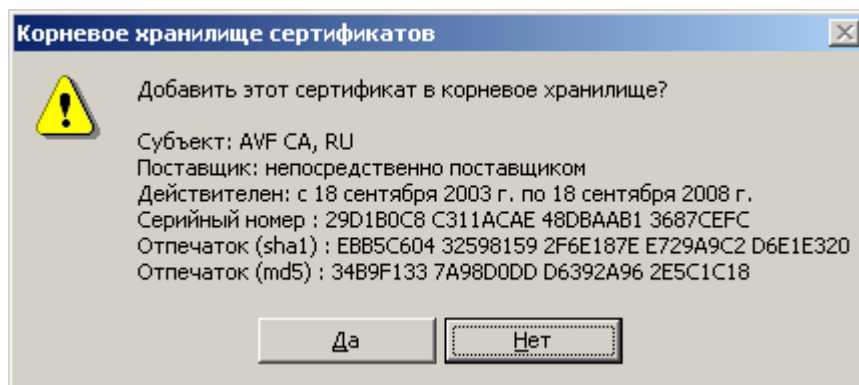
После выбора необходимого хранилища в окне **Хранилище сертификатов** нажмите кнопку **Далее**.

Примечание: При установке сертификата корневого центра сертификации в хранилище **Локальный компьютер/Доверенные корневые центры сертификации** данный сертификат автоматически будет установлен в хранилище **Текущий пользователь/Доверенные корневые центры сертификации**

4. В открывшемся окне **Завершение работы мастера импорта сертификатов** проверьте правильность указанных параметров и нажмите кнопку **Готово**.



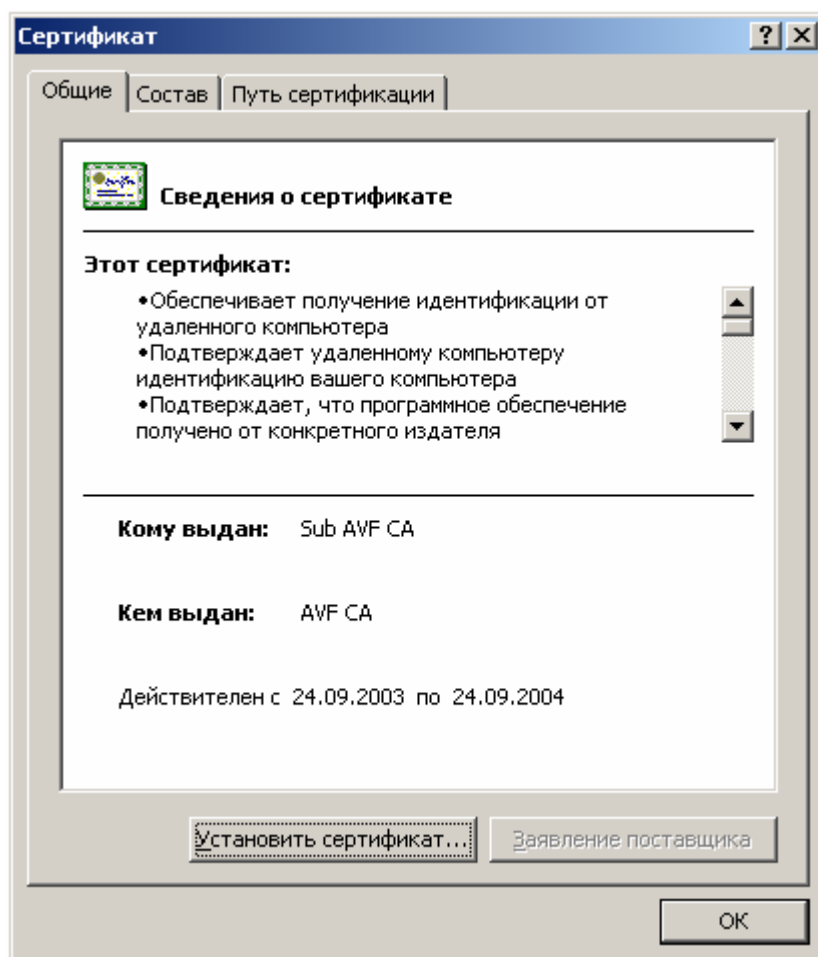
5. При установке переключателя **Автоматически выбрать хранилище на основе типа сертификата** откроется окно **Корневое хранилище сертификатов**, информирующее о добавлении сертификата корневого центра сертификации в корневое хранилище. Нажмите кнопку **Да**



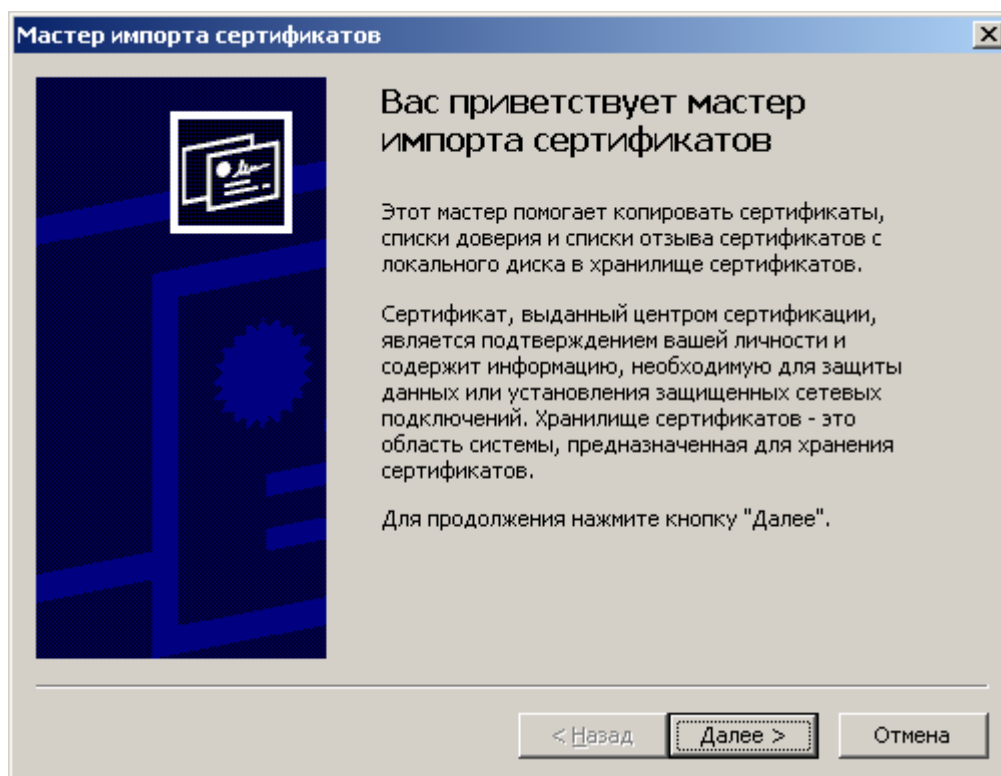
6. Проверьте правильность установки сертификата корневого центра сертификации на персональный компьютер.

13.2. Установка сертификата подчиненного центра сертификации

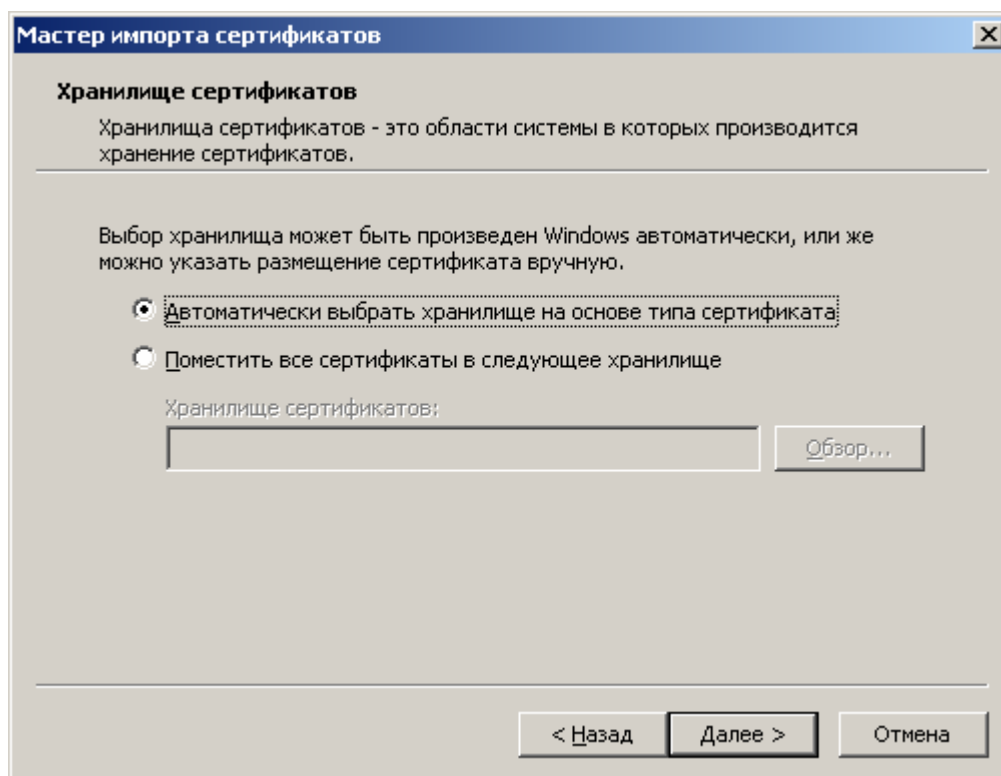
1. В стандартном проводнике MS Windows выберите файл, содержащий сертификат подчиненного центра сертификации, двойным нажатием левой кнопки мыши запустите его. Откроется стандартное окно просмотра сертификатов. Нажмите кнопку **Установить сертификат**



2. Откроется окно **Мастер импорта сертификатов**. Нажмите кнопку **Далее**



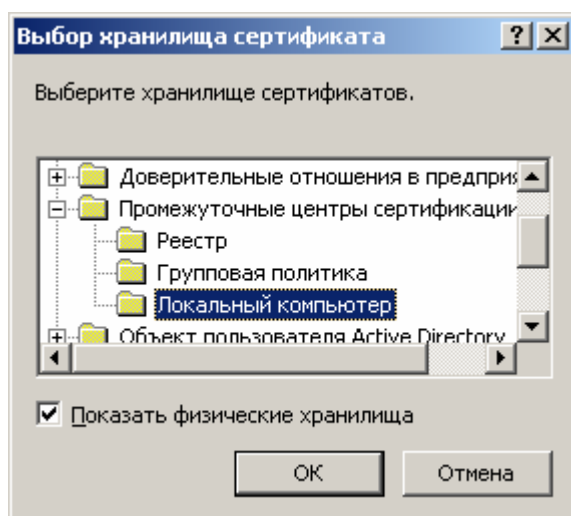
3. Откроется окно **Хранилище сертификатов**



При установке переключателя в положение **Автоматически выбрать хранилище на основе типа сертификата** сертификат подчиненного центра сертификации будет установлен в хранилище **Текущий пользователь/Промежуточные центры сертификации**.

При установке переключателя в положение **Поместить все сертификаты в следующее хранилище** возможно установить сертификат в хранилище, выбираемое из списка.

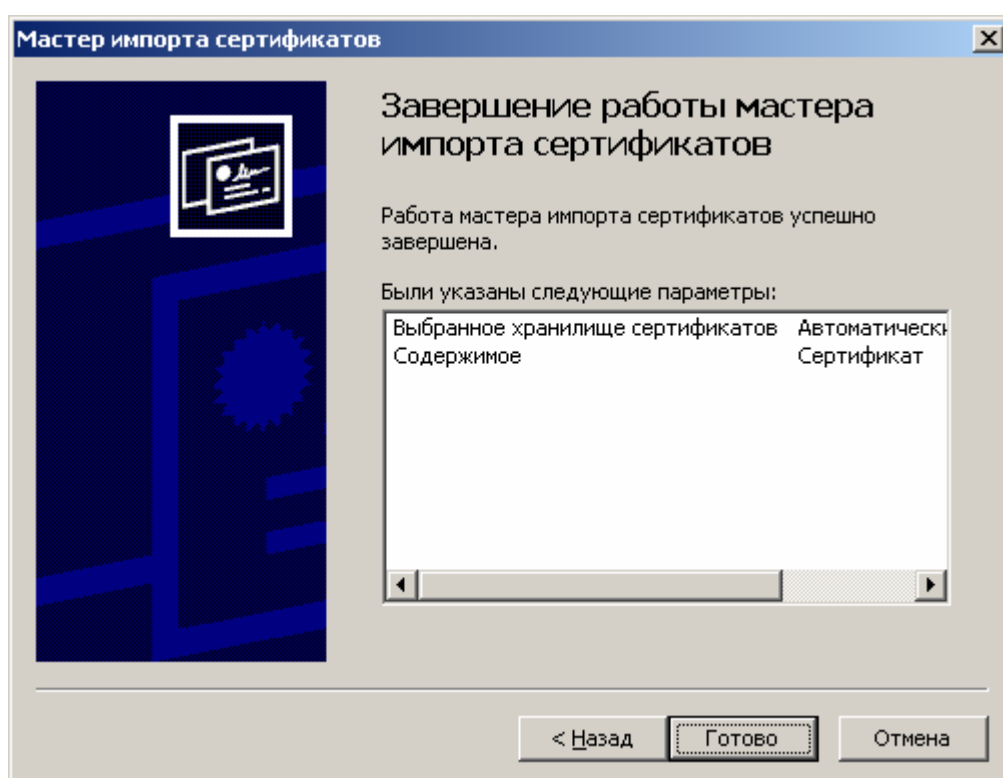
Для установки сертификата подчиненного центра сертификации в хранилище **Локальный компьютер/Промежуточные центры сертификации** необходимо в окне **Выбор хранилища сертификата** установить флаг **Показать физические хранилища** и выбрать хранилище **Промежуточные центры сертификации/Локальный компьютер**



После выбора необходимого хранилища в окне **Хранилище сертификатов** нажмите кнопку **Далее**

Примечание: При установке сертификата подчиненного центра сертификации в хранилище **Локальный компьютер/Промежуточные центры сертификации** данный сертификат автоматически будет установлен в хранилище **Текущий пользователь/Промежуточные центры сертификации**

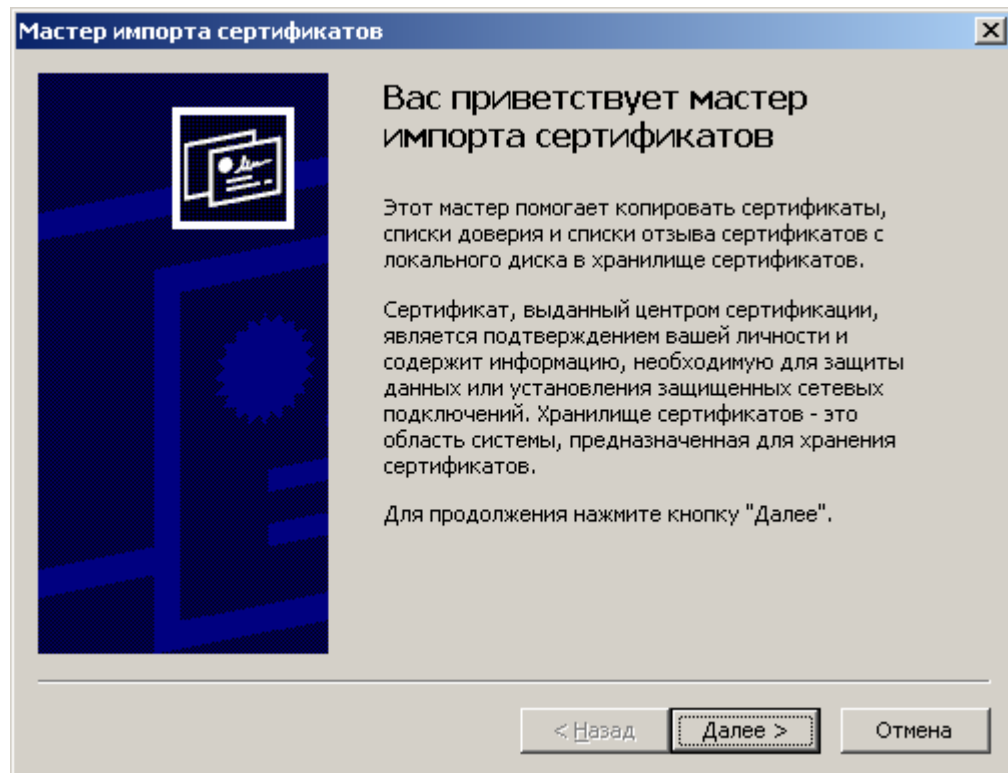
4. В открывшемся окне **Завершение работы мастера импорта сертификатов** проверьте правильность указанных параметров и нажмите кнопку **Готово**.



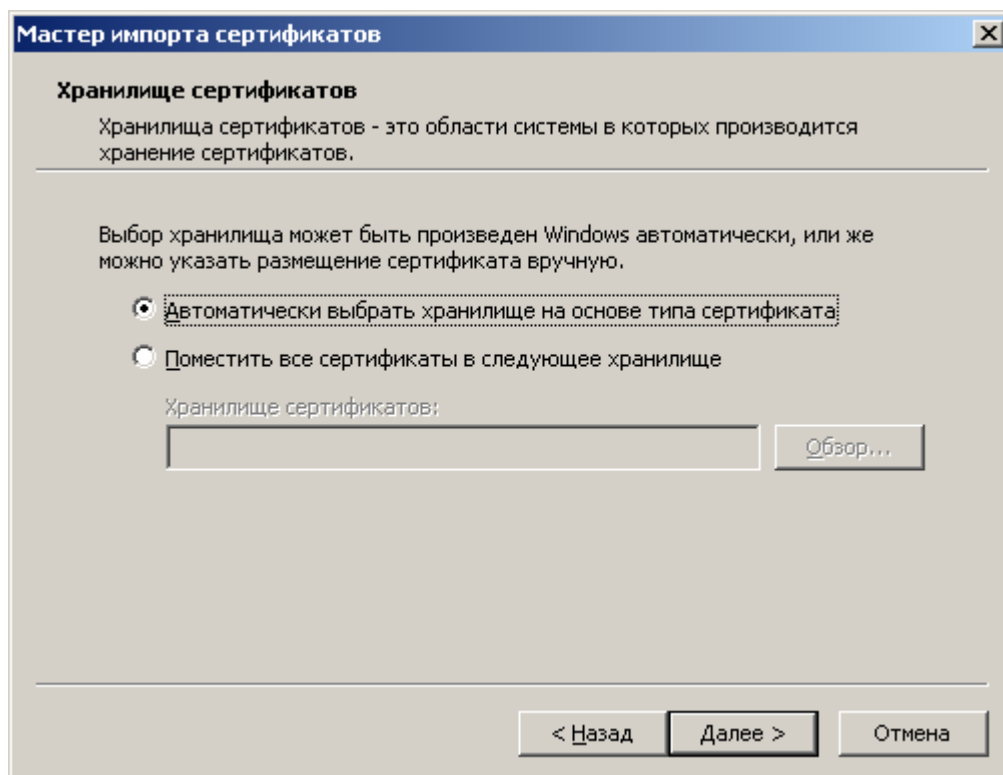
5. Проверьте правильность установки сертификата подчиненного центра сертификации на персональный компьютер

14. Установка списка отозванных сертификатов (CRL)

1. В стандартном проводнике MS Windows выбрать файл, содержащий список отозванных сертификатов, нажатием правой кнопки мыши.
2. В раскрывшемся меню выбрать команду **Установить список отзыва (CRL)**.
3. Откроется окно **Мастер импорта сертификатов**. Нажмите кнопку **Далее**.



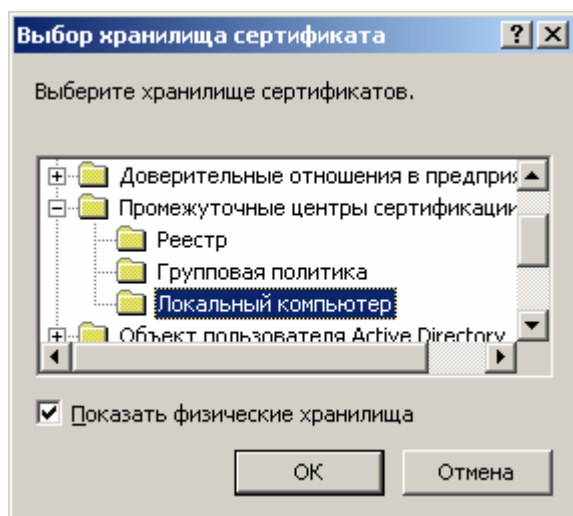
4. Откроется окно **Хранилище сертификатов**



При установке переключателя в положение **Автоматически выбрать хранилище на основе типа сертификата** список отозванных сертификатов будет установлен в хранилище **Сертификаты-Текущий пользователь/Промежуточные центры сертификации**.

При установке переключателя в положение **Поместить все сертификаты в следующее хранилище** возможно установить сертификат в хранилище, выбираемое из списка.

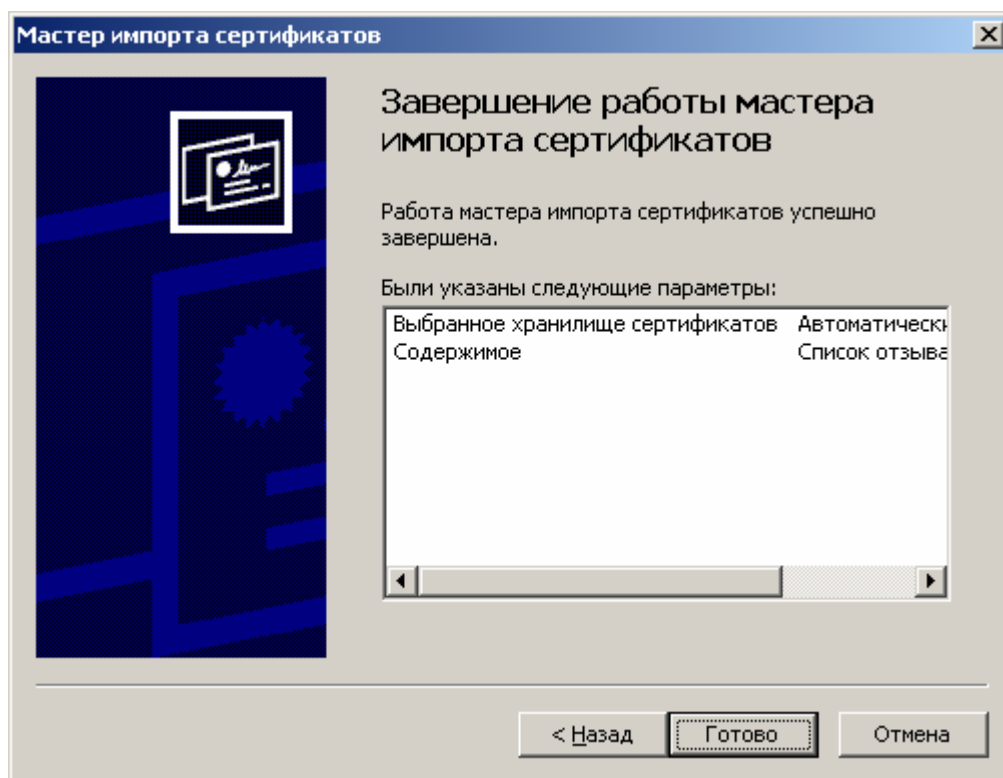
Для установки списка отозванных сертификатов в хранилище **Локальный компьютер/Промежуточные центры сертификации** необходимо в окне **Выбор хранилища сертификата** установить флаг **Показать физические хранилища** и выбрать хранилище **Промежуточные центры сертификации/Локальный компьютер**



После выбора хранилища нажмите кнопку **Далее**.

Примечание: При установке списка отозванных сертификатов в хранилище **Локальный компьютер/Промежуточные центры сертификации** список отозванных сертификатов автоматически будет установлен в хранилище **Текущий пользователь/Промежуточные центры сертификации**

5. В открывшемся окне **Завершение работы мастера импорта сертификатов** проверьте правильность указанных параметров и нажмите кнопку **Готово**.

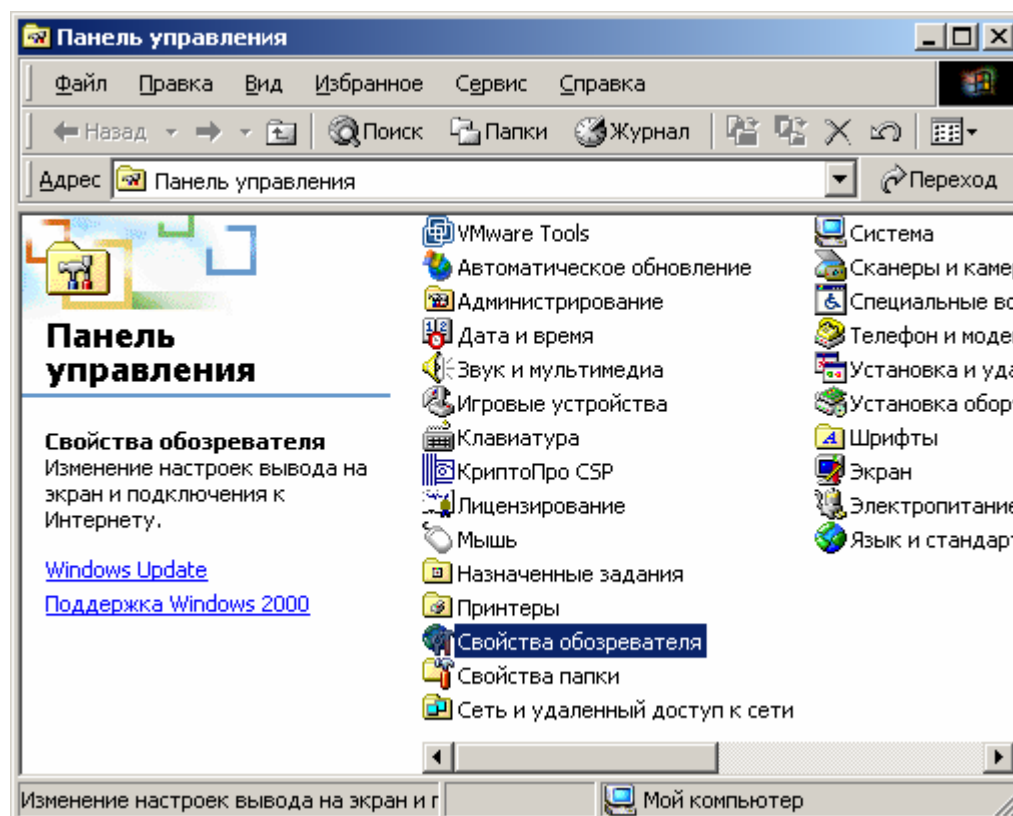


6. Проверьте правильность установки списка отозванных сертификатов на персональный компьютер

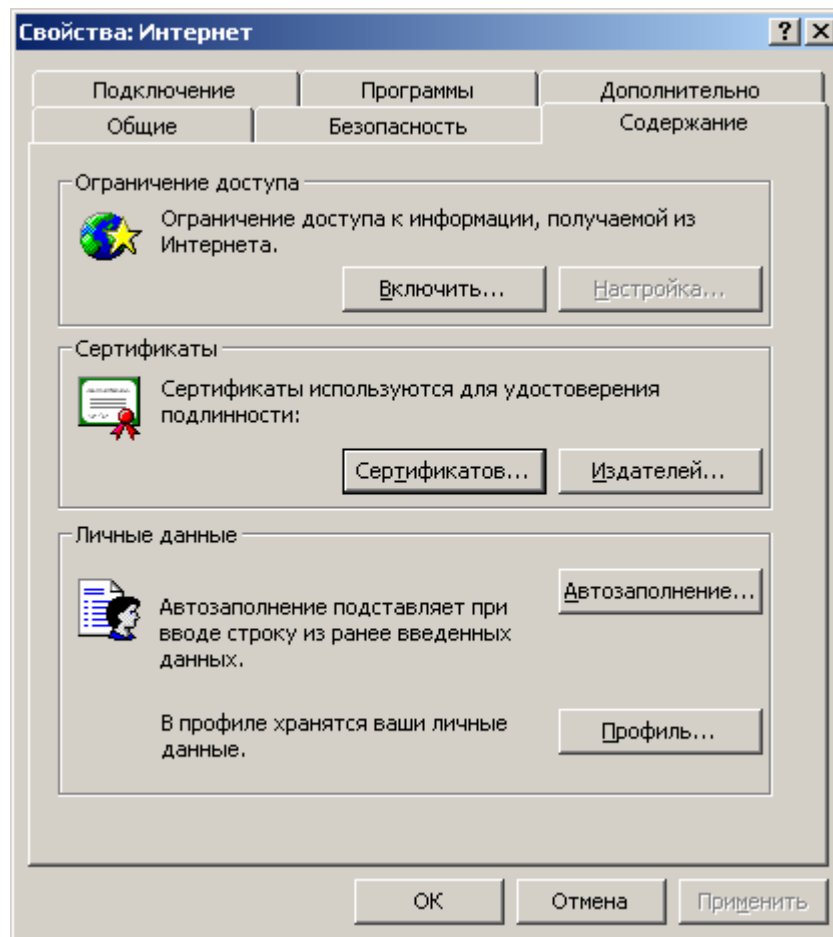
15. Просмотр установленных на компьютере сертификатов и списков отозванных сертификатов

15.1. Просмотр установленных сертификатов в окне свойств обозревателя Microsoft Internet Explorer (IE)

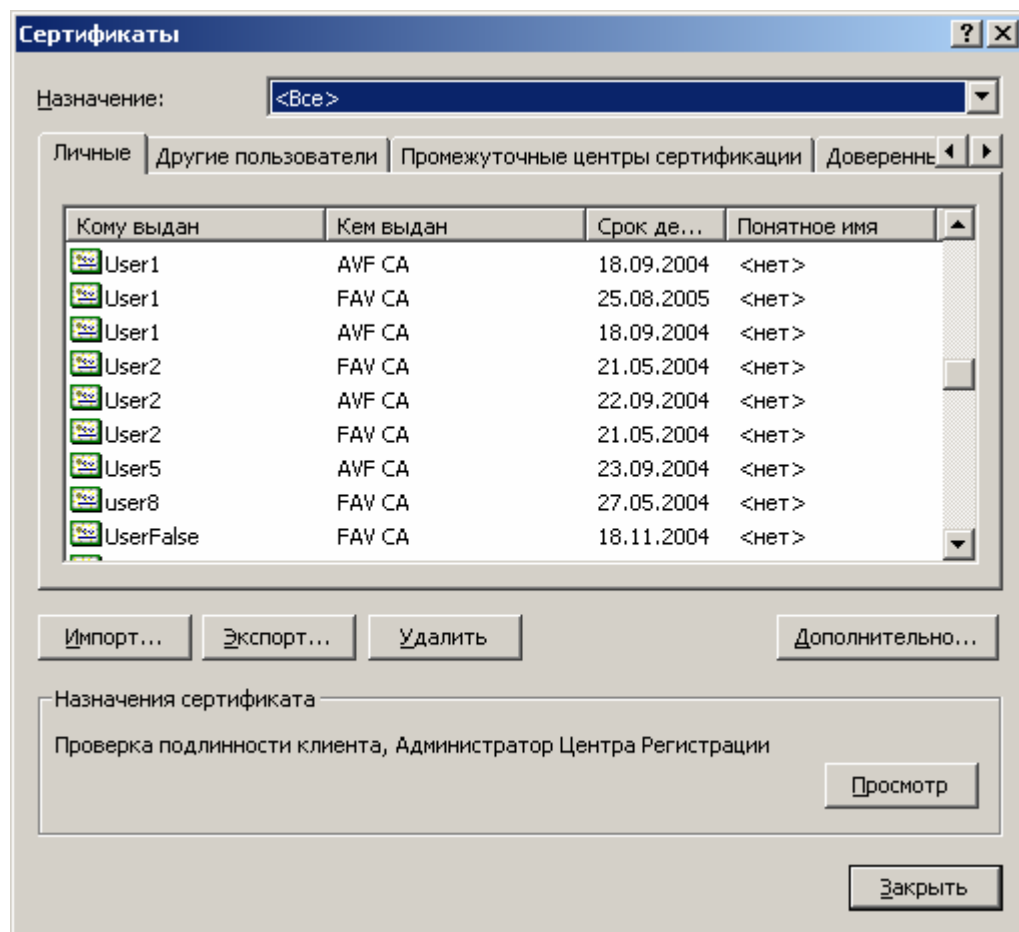
1. Откройте панель управления компьютером, используя пункты меню **Пуск -> Настройка -> Панель управления** и в окне панели управления выберите **Свойства обозревателя**



2. В открывшемся окне **Свойства: Интернет** выберите вкладку **Содержание** и нажмите кнопку **Сертификатов**



3. Откроется окно **Сертификаты**



В этом окне можно просмотреть Личные сертификаты (т.е. сертификаты, связанные с соответствующим закрытым ключом) – вкладка **Личные**, сертификаты других пользователей – вкладка **Другие пользователи**, сертификаты подчиненных центров сертификации – вкладка **Промежуточные центры сертификации**, сертификаты корневых центров сертификации – вкладка **Доверенные корневые центры сертификации**.

Поле **Назначение** позволяет фильтровать сертификаты по их области использования (использующиеся фильтры – **Все**, **Защищенная электронная почта**, **Проверка подлинности клиента**, **Дополнительные назначения**). С помощью кнопки **Дополнительно** осуществляется установка областей использования сертификатов для выбора и просмотра сертификатов с помощью фильтра **Дополнительные назначения**.

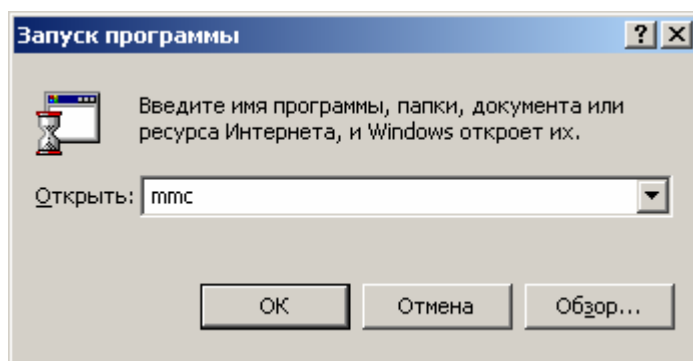
Кнопки **Импорт**, **Экспорт**, **Удалить** позволяют соответственно импортировать сертификат в файл, экспортировать сертификат из файла, удалять сертификат из хранилища. Также с помощью кнопки **Дополнительно** осуществляется установка параметров экспорта сертификатов.

Кнопка **Просмотр** служит для просмотра выделенного сертификата в стандартном окне просмотра сертификатов.

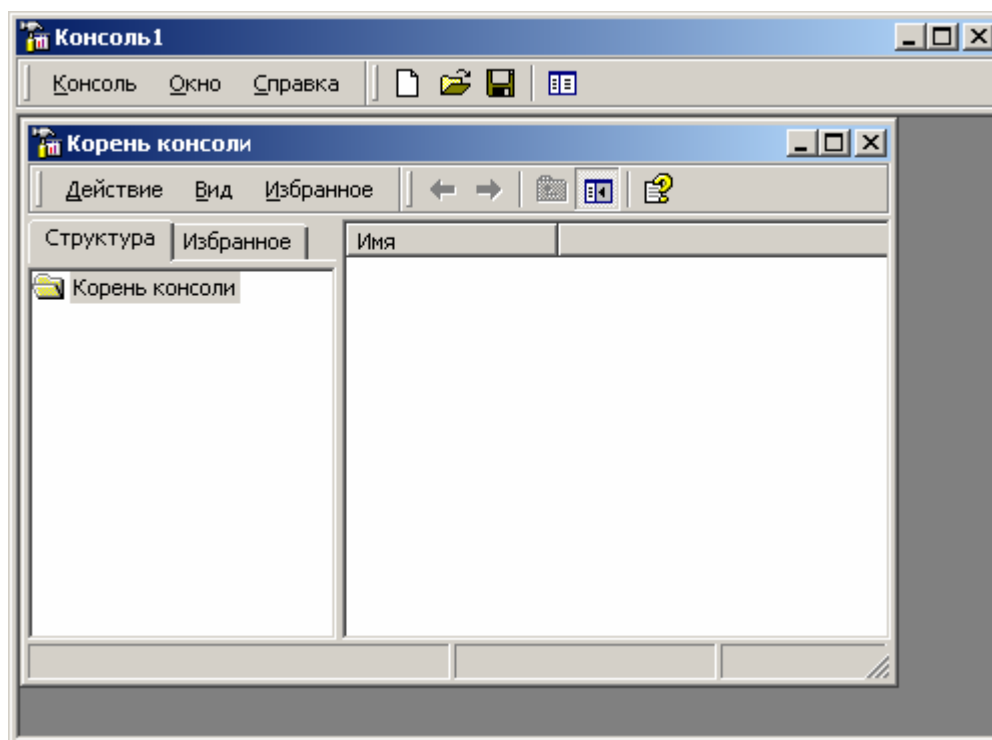
Примечание: В окне **Сертификаты** отображаются только сертификаты, установленные в хранилище **Текущий пользователь**. Также с помощью данного сервиса нельзя просмотреть установленные списки отозванных сертификатов.

15.2. Просмотр установленных сертификатов с помощью оснастки Сертификаты Microsoft Management Console (MMC) (только для Windows 2000, XP, 2003)

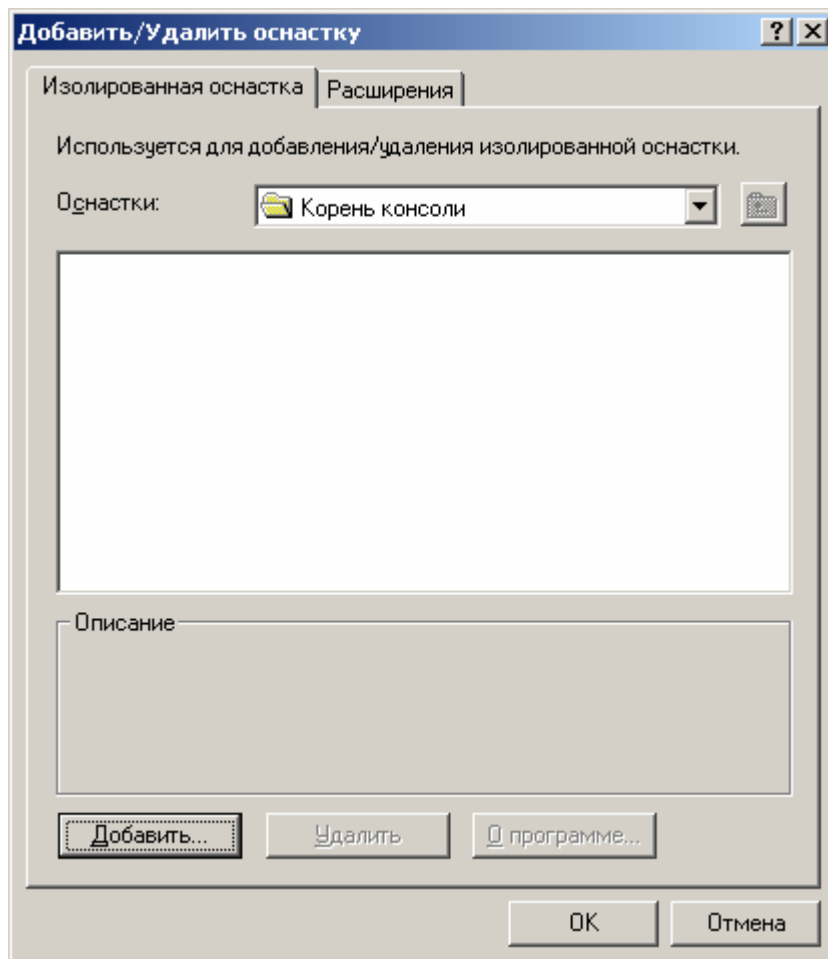
1. В окне **Запуск программы (Пуск -> Выполнить)** введите **mmc**.



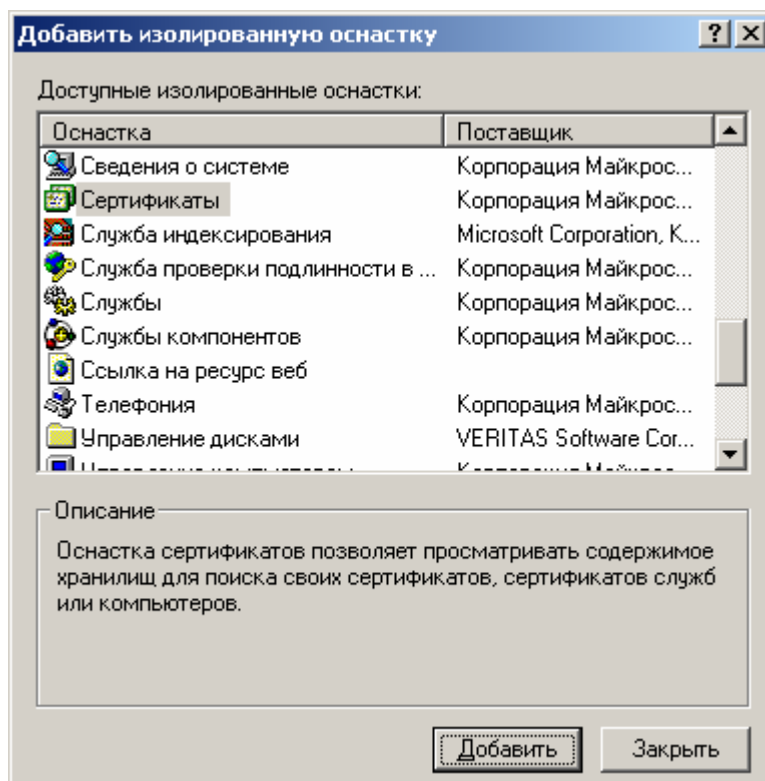
2. Откроется окно консоли управления **Консоль1**.



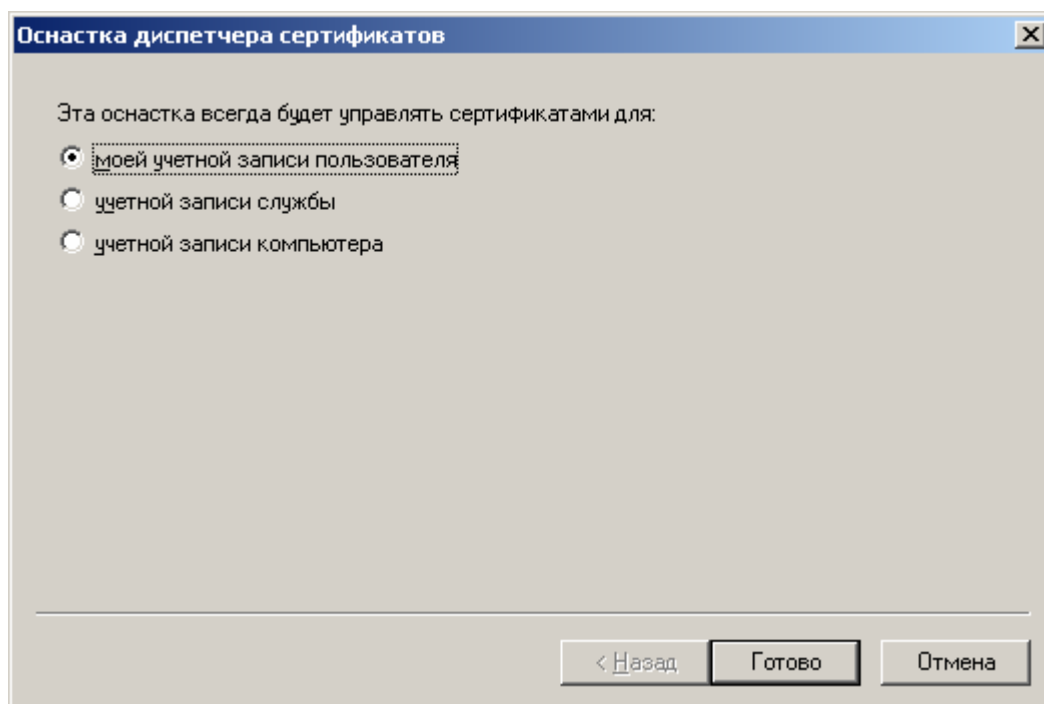
3. В пункте меню **Консоль** выбрать **Добавить/Удалить оснастку**, в открывшемся окне **Добавить/Удалить оснастку** нажать кнопку **Добавить**



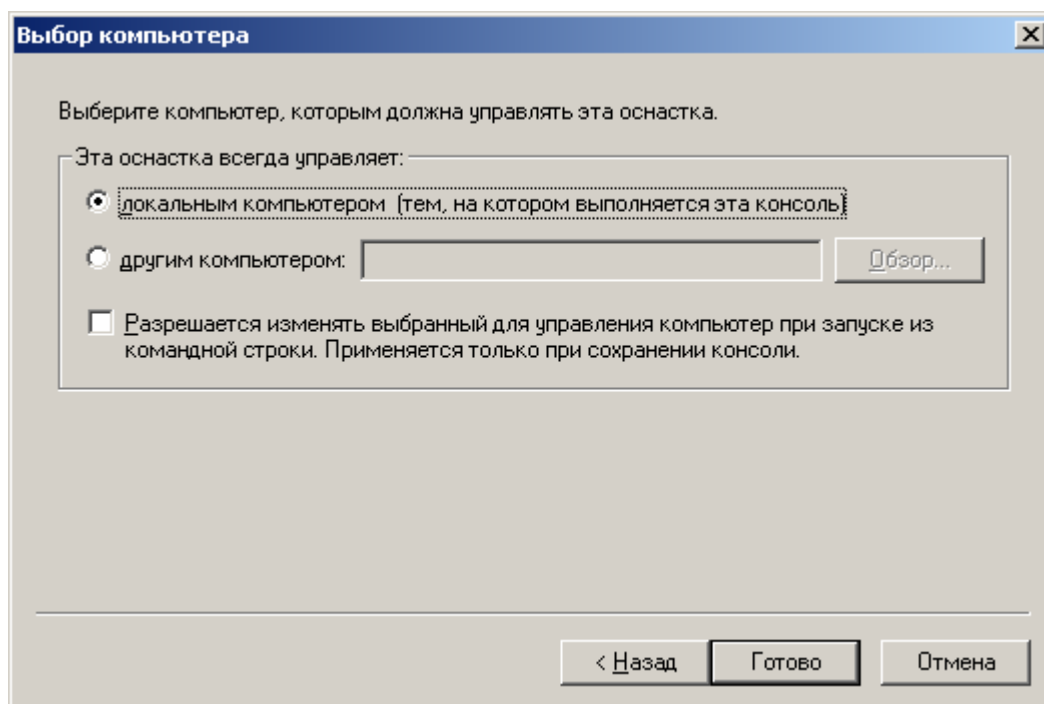
4. Выберите в открывшемся окне **Добавить изолированную оснастку** оснастку **Сертификаты** и нажмите кнопку **Добавить**



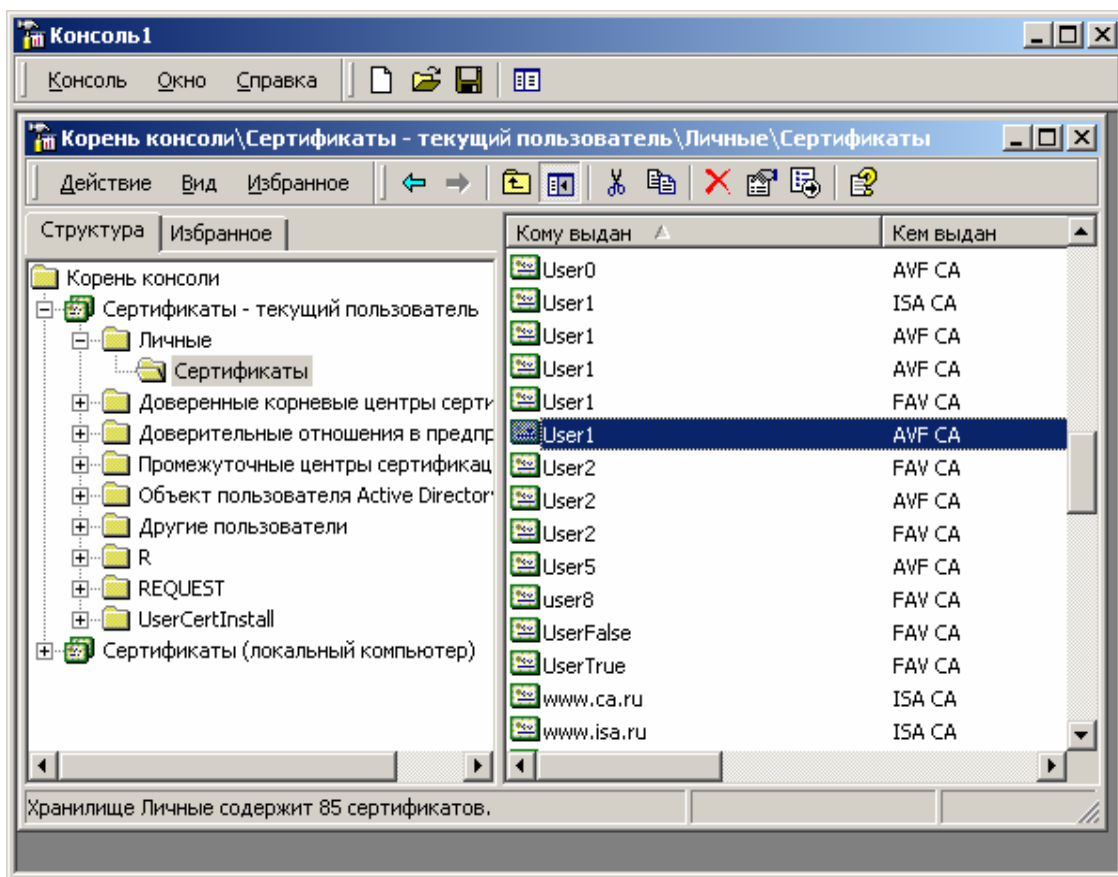
5. В окне **Оснастка диспетчера сертификатов** установите переключатель в положение **Моей учетной записи пользователя** и нажмите кнопку **Готово**.



6. В окне **Добавить изолированную оснастку** еще раз нажмите кнопку **добавить**, в открывшемся окне **Оснастка диспетчера сертификатов** выберите переключатель **Учетной записи компьютера**, нажмите кнопку **Далее**, в окне **Выбор компьютера** установите переключатель в положение **Локальным компьютером** и нажмите кнопку **Готово**



7. В окне **Добавить изолированную оснастку** нажмите кнопку **Заккрыть**, в окне **Добавить/Удалить оснастку** нажмите кнопку **ОК**. Консоль управления **Консоль1** примет следующий вид:



С помощью данной консоли управления можно осуществлять просмотр установленных сертификатов в отображающихся хранилищах, производить необходимые операции по управлению сертификатами и списками отозванных сертификатов на персональном компьютере (перемещение, копирование, удаление, импорт, экспорт и т.д.).

Примечание: Подробное описание по работе с оснасткой **Сертификаты** приведено в справочном руководстве ОС Windows 2000, XP, 2003 в разделе **Использование оснастки «Сертификаты»**.

15.3. Просмотр установленных сертификатов с помощью утилиты CertMgr.exe, разработанной ООО «КРИПТО-ПРО»

Данная утилита функционирует под управлением ОС семейства Windows, начиная с Windows 98, и позволяет осуществлять просмотр установленных сертификатов, списков отозванных сертификатов и производить необходимые операции по их перемещению, копированию, удалению на персональном компьютере пользователя.

Получить эту утилиту можно бесплатно на сайте компании «Крипто-Про» в разделе Download (<http://www.cryptopro.ru/CryptoPro/download/default.asp>).

Окно утилиты CertMgr.exe:

