127 018, Москва, Улица Образцова, 38
Телефон: (095) 933 1168
Факс: (095) 933 1168
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru



Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 3.0

Инструкция по использованию КриптоПро CSP и TLS

ЖТЯИ.00015-01 90 02-05

Листов 63

2005 г.

© ООО "Крипто-Про", 2000-2005. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Свидетельство об официальной регистрации программ для ЭВМ № 2001610275 от 14 марта 2001 года.

Документ входит в комплект поставки программного обеспечения КриптоПро CSP, и на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "Крипто-Про" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

1. Инсталляция СКЗИ КриптоПро CSP 5
2. Интерфейс контрольной панели СКЗИ КриптоПро CSP 6
2.1. Доступ к контрольной панели СКЗИ КриптоПро CSP 6
2.2. Настройка общих свойств СКЗИ КриптоПро CSP 7
2.2.1. Ввод серийного номера лицензии КриптоПровайдера «КриптоПро CSP» 7
2.2.2. Регистрация ПО СКЗИ 9
2.3. Настройка оборудования СКЗИ КриптоПро CSP 9
2.3.1. Изменение набора устройств считывания ключевой информации 9
2.3.1.1. Добавление считывателя 9
2.3.1.2. Удаление считывателя 16
2.3.1.3. Просмотр свойств считывателя 16
2.3.2. Изменение набора устройств хранения ключевой информации 17
2.3.2.1. Добавление носителя 17
2.3.2.2. Удаление ключевого носителя 21
2.3.2.3. Просмотр свойств ключевого носителя 21
2.3.3. Настройка датчиков случайных чисел (ДСЧ) 22
2.3.3.1. Добавление ДСЧ 22
2.3.3.2. Удаление ДСЧ 25
2.3.3.3. Просмотр свойств ДСЧ 25
2.4. Работа с контейнерами и сертификатами 26
2.4.1. Копирование и удаление контейнера закрытого ключа 27
2.4.1.1. Копирование контейнера закрытого ключа 27
2.4.1.2. Удаление контейнера закрытого ключа 30
2.4.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа 31
2.4.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа 31
2.4.2.2. Установка личного сертификата, хранящегося в контейнере закрытого ключа 33
2.4.3. Установка личного сертификата, хранящегося в файле 35
2.4.4. Управление паролями доступа к закрытым ключам 39
2.4.4.1. Изменение пароля на доступ к закрытому ключу 39
2.4.4.2. Удаление запомненных паролей 40
2.5. Установка параметров безопасности 41
2.6. Дополнительные настройки 43
2.6.1. Просмотр версий используемых файлов 43
2.6.2. Установка времени ожидания ввода информации от пользователя 44
2.7. Установка параметров криптографических алгоритмов 46
3. Интерфейс генерации ключей 48
3.1. Создание ключевого контейнера 48
3.1.1. Выбор ключевого носителя 48
3.1.2. Генерация начальной последовательности ДСЧ 48

3.1.3. Ввод пароля на доступ к закрытому ключу 49
3.1.4. Выбор способа защиты доступа к закрытому ключу 49
3.1.4.1. Установка нового пароля 50
3.1.4.2. Установка нового ключа 50
3.1.4.3. Разделение ключа на несколько носителей 51
3.2. Открытие ключевого контейнера 52
3.2.1. Отсутствие ключевого носителя 52
3.2.2. Проверка пароля на доступ к закрытому ключу 52
3.2.2.1. Проверка текстового пароля 52
3.2.2.2. Проверка пароля при зашифровании ключа на другом ключе 53
3.2.2.3. Проверка пароля при разделении ключа между несколькими носителями 53
3.2.3. Ввод нового пароля на доступ к закрытому ключу 53
3.3. Генерация ключей и получение сертификата при помощи УЦ 54
4. Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS 55
4.1. Размещение сертификата на сервере ISA 55
4.2. Настройка соединения с Web-клиентом 58
4.3. Публикация Web-сервера в сети Интернет 60

1. Инсталляция СКЗИ КриптоПро CSP

Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора. Перед установкой дистрибутива, удалите все ранее существующие версии устанавливаемого программного обеспечения. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используйте пункты основного меню Windows **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **Установка и удаление программ**.

Для установки программного обеспечения вставьте компакт-диск в дисковод. Программа установки запуститься автоматически. Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска.



Рис. 1. Содержание диска КриптоПро CSP

Для дальнейшей установки КриптоПро CSP, выберите значок **Установить КриптоПро CSP**.

Последующая установка производится в интерактивном режиме. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

2. Интерфейс контрольной панели СКЗИ КриптоПро CSP

2.1. Доступ к контрольной панели СКЗИ КриптоПро CSP

Данный раздел является инструкцией по использованию контрольной панели (панели настройки) средства криптографической защиты информации (СКЗИ) КриптоПро CSP. Для перехода к панели настройки КриптоПро CSP откройте панель управления компьютером, используя пункты меню **Пуск** ⇒ **Настройка** ⇒ **Панель управления** и в окне панели управления (см. Рис. 2) выберите значок **КриптоПро CSP.**

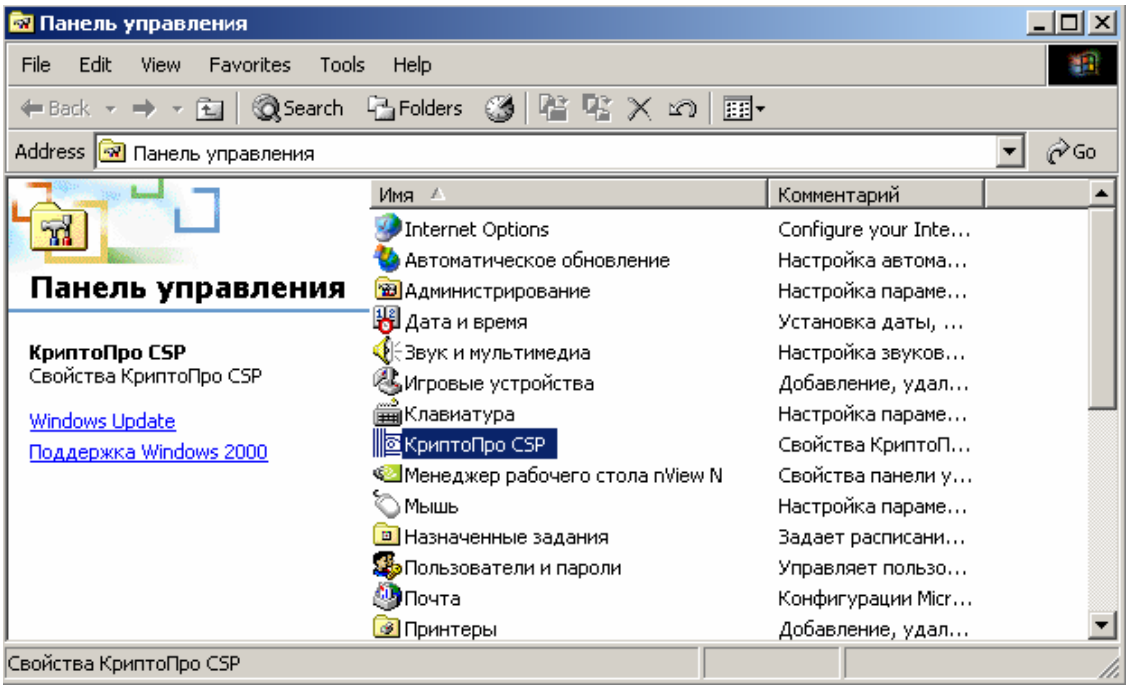


Рис. 2. Панель управления

Система перейдет к контрольной панели СКЗИ КриптоПро CSP «**Свойства: КриптоПро CSP**» (см.Рис. 3), которая состоит из шести закладок:

- общие;
- оборудование;
- сервис;
- безопасность;
- дополнительно;
- алгоритмы.

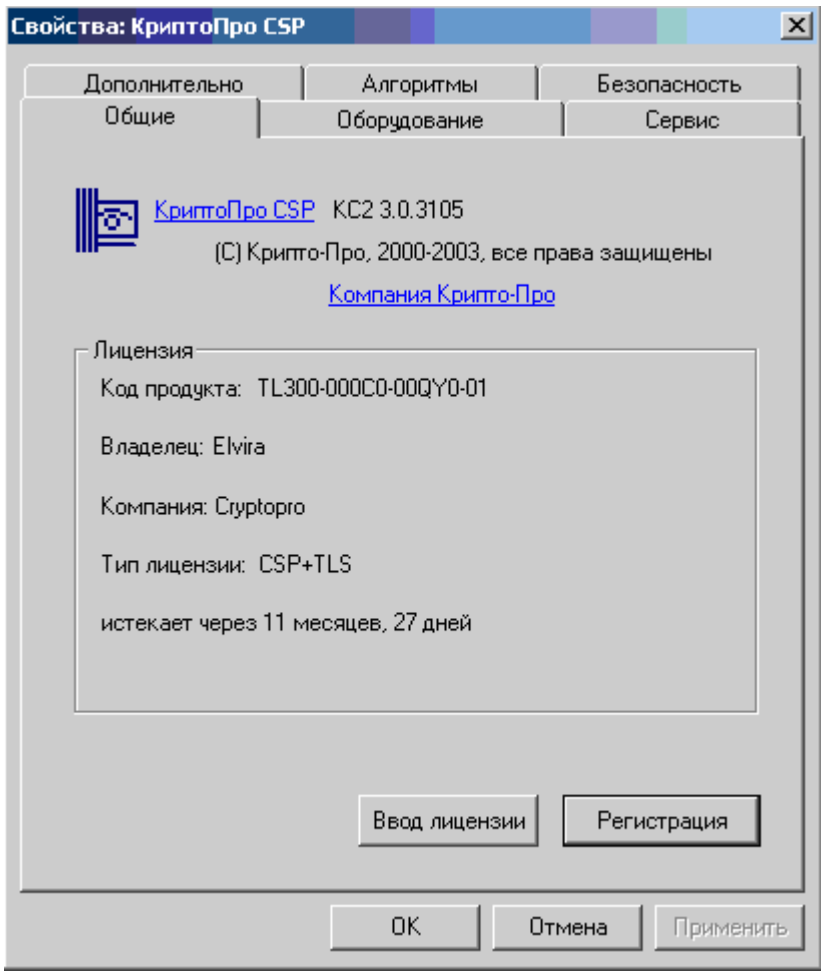


Рис. 3. Панель настройки

2.2. Настройка общих свойств СКЗИ КриптоПро CSP

Закладка **Общие** контрольной панели СКЗИ КриптоПро CSP предназначена для ввода лицензии и регистрации ПО СКЗИ КриптоПро CSP.

2.2.1. Ввод серийного номера лицензии КриптоПровайдера «КриптоПро CSP»

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока (см. Рис. 5) пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (Дилера).

Для ввода лицензии в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Общие.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 5) нажмите кнопку **Ввод лицензии.**

Система отобразит окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести **серийный номер** с бланка **Лицензии** в соответствующие поля ввода (см.Рис. 4).

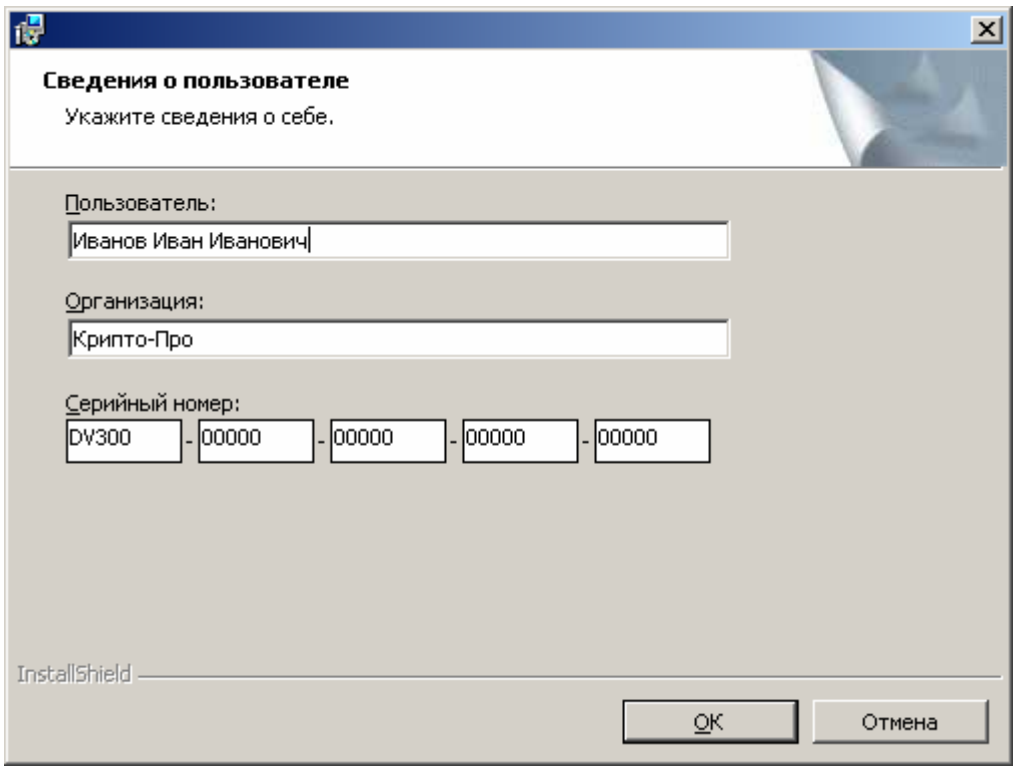


Рис. 4. Ввод данных лицензии

После ввода и нажатия клавиши OK произойдет возврат к контрольной панели с указанным типом лицензии и сроком ее действия (см. Рис. 3).

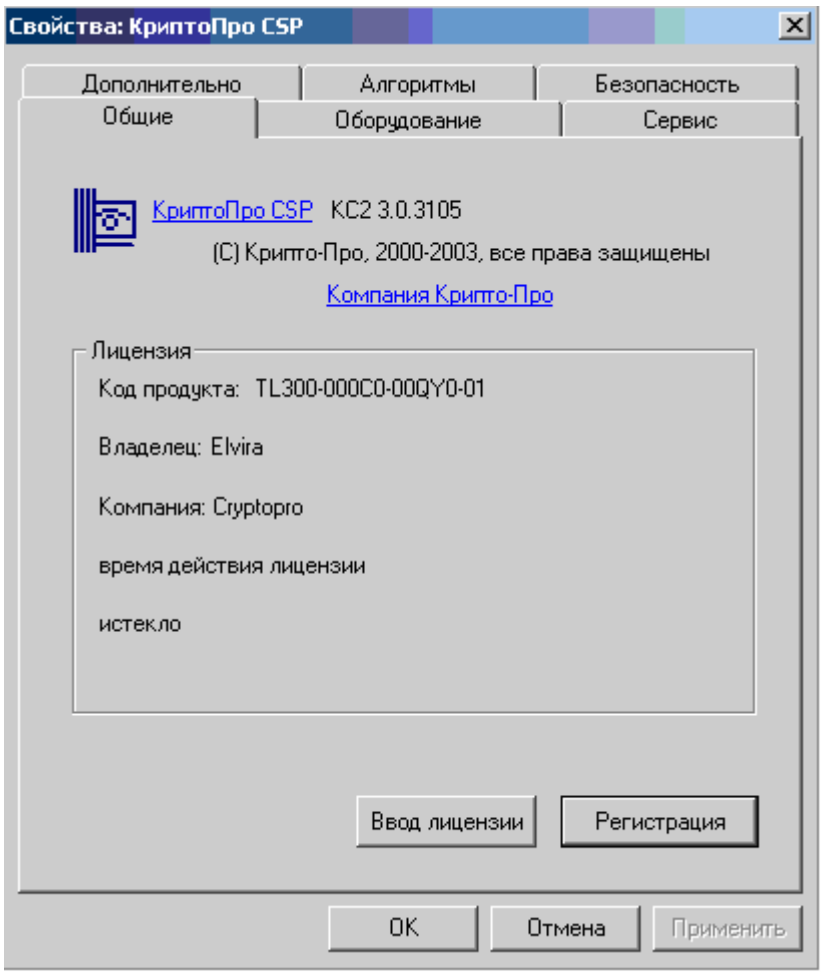


Рис. 5. Контрольная панель. Закладка «Общие»

2.2.2. Регистрация ПО СКЗИ

После завершения программы установки рекомендуется зарегистрировать установленное программное обеспечение КриптоПро CSP у организации-разработчика. Для этого в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Общие.** В панели настройки СКЗИ КриптоПро CSP (см.Рис. 5 Рис. 3) нажмите кнопку **Регистрация.**

Откроется окно браузера с предложением отправить регистрационные данные (см.Рис. 6). 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**).

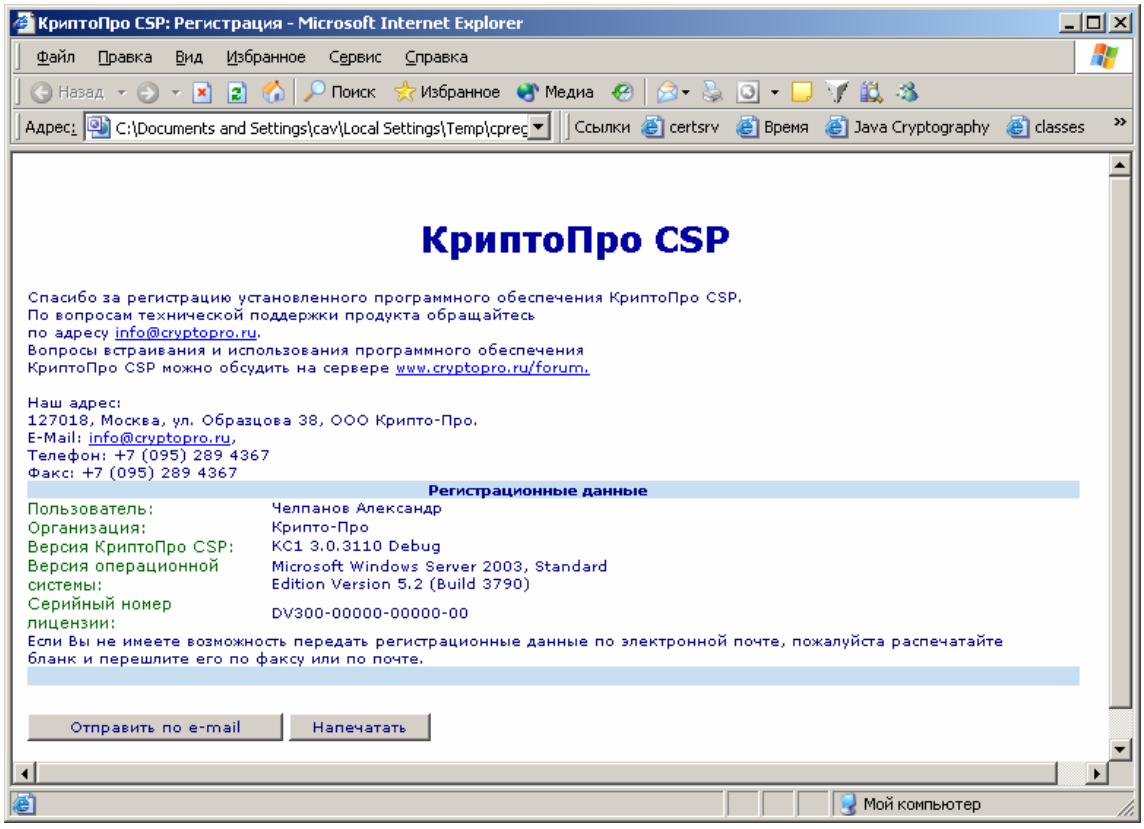


Рис. 6. Выполнение регистрации

2.3. Настройка оборудования СКЗИ КриптоПро CSP

Закладка **Оборудование** контрольной панели СКЗИ КриптоПро CSP предназначена для изменения набора устройств хранения и считывания ключевой информации и датчиков случайных чисел (ДЧС).

2.3.1. Изменение набора устройств считывания ключевой информации

2.3.1.1. Добавление считывателя

Для того, чтобы добавить считыватель в меню, выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить считыватели.**

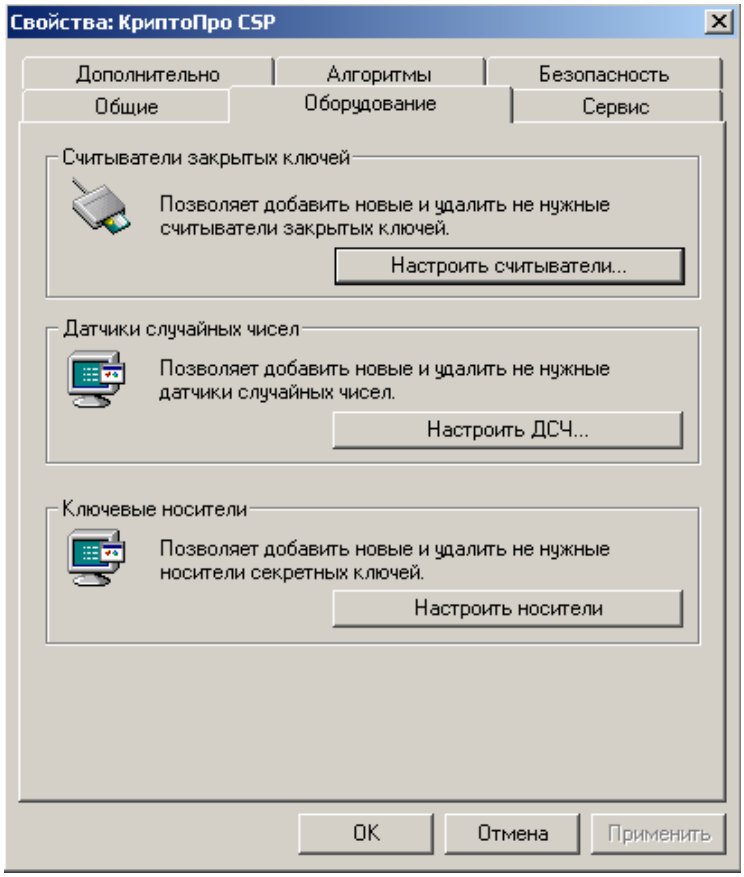


Рис. 7. Контрольная панель. Закладка «Оборудование»

Система отобразит окно «Управление считывателями» (см. Рис. 8).

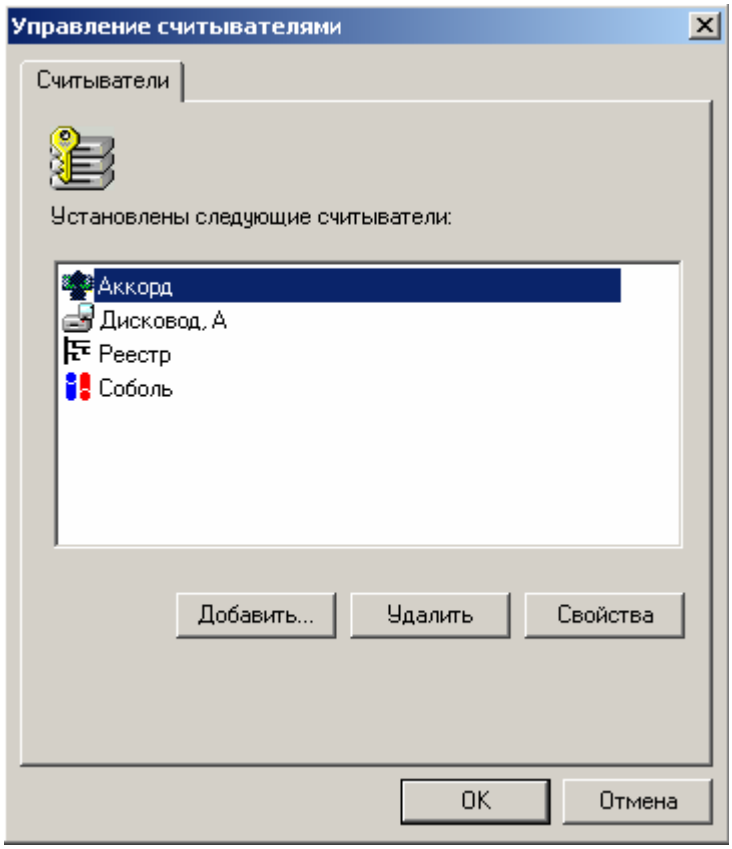


Рис. 8. Окно «Управление считывателями»

Для того чтобы добавить считыватель, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки считывателя (см.Рис. 9). В окне мастера установки нажмите кнопку **Далее**.

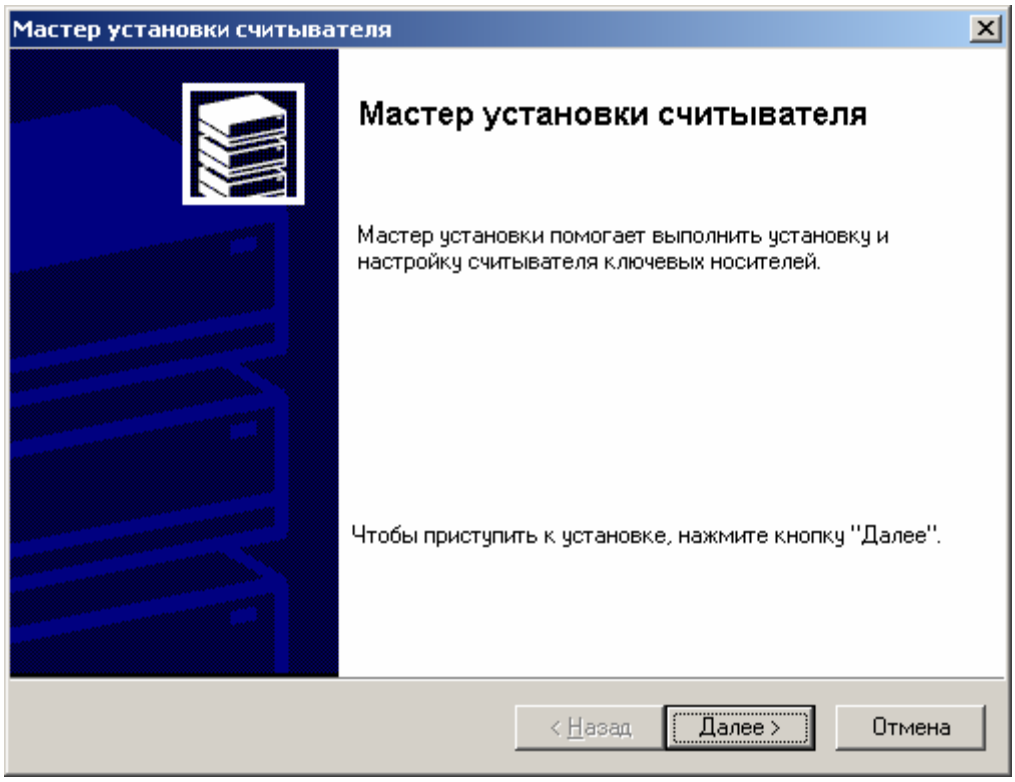


Рис. 9. Запуск мастера установки считывателя

Система отобразит окно «Выбор считывателя» (см.Рис. 10). Для того чтобы добавить считыватель, входящий в состав дистрибутива СКЗИ КриптоПро CSP, в этом окне выберите из списка считыватель, который следует добавить, и нажмите кнопку **Далее.**

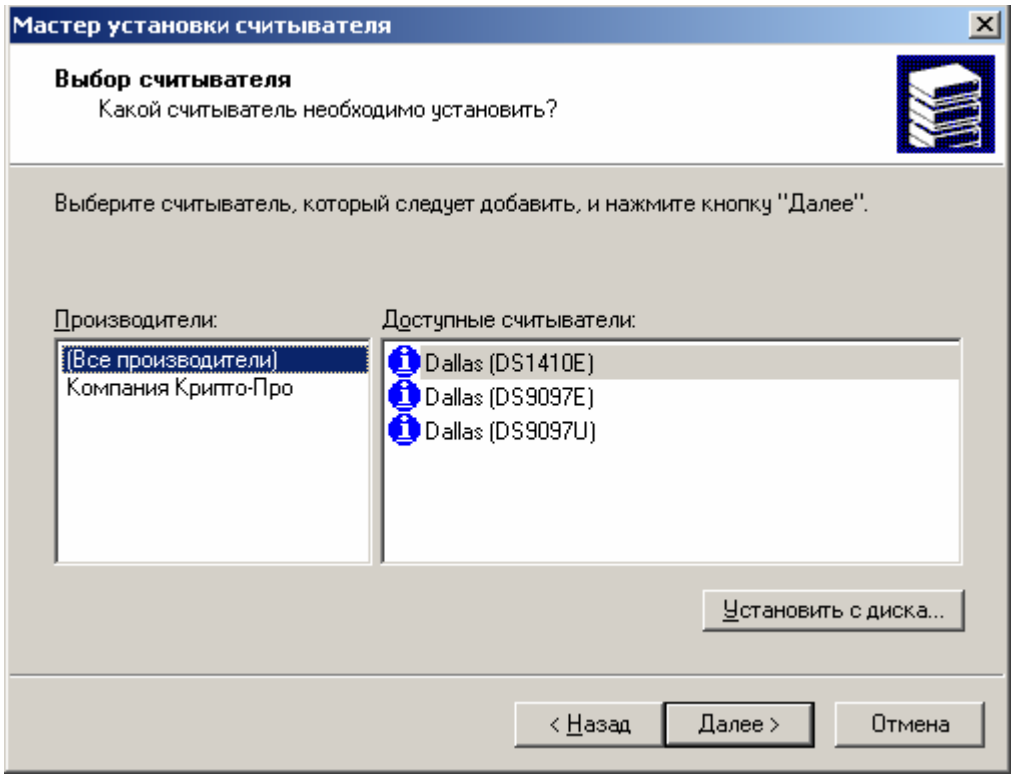


Рис. 10. Окно «Выбор считывателя»

В зависимости от выбранного считывателя может потребоваться выбор соединения для этого устройства. Тогда система отобразит окно «Выбор соединения» (см.Рис. 11). В этом окне выберите соединение для считывателя и нажмите кнопку **Далее.**

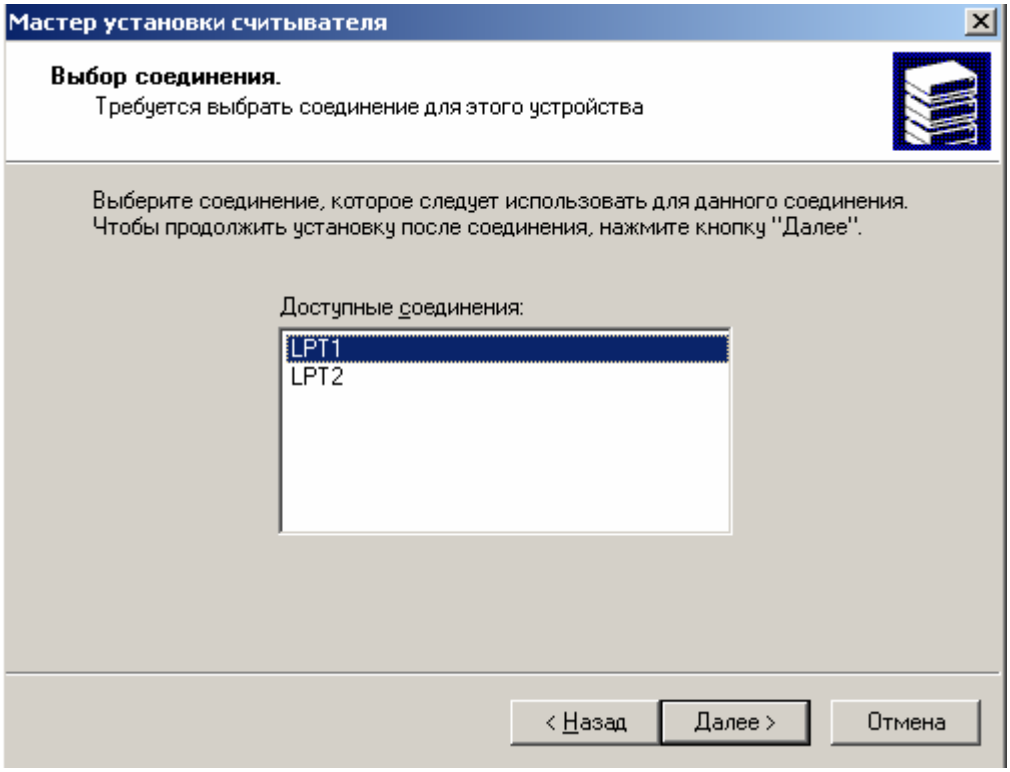


Рис. 11. Окно «Выбор считывателя»

Система отобразит окно «Имя считывателя» (см. Рис. 12). В этом окне введите имя выбранного считывателя и нажмите кнопку **Далее.**

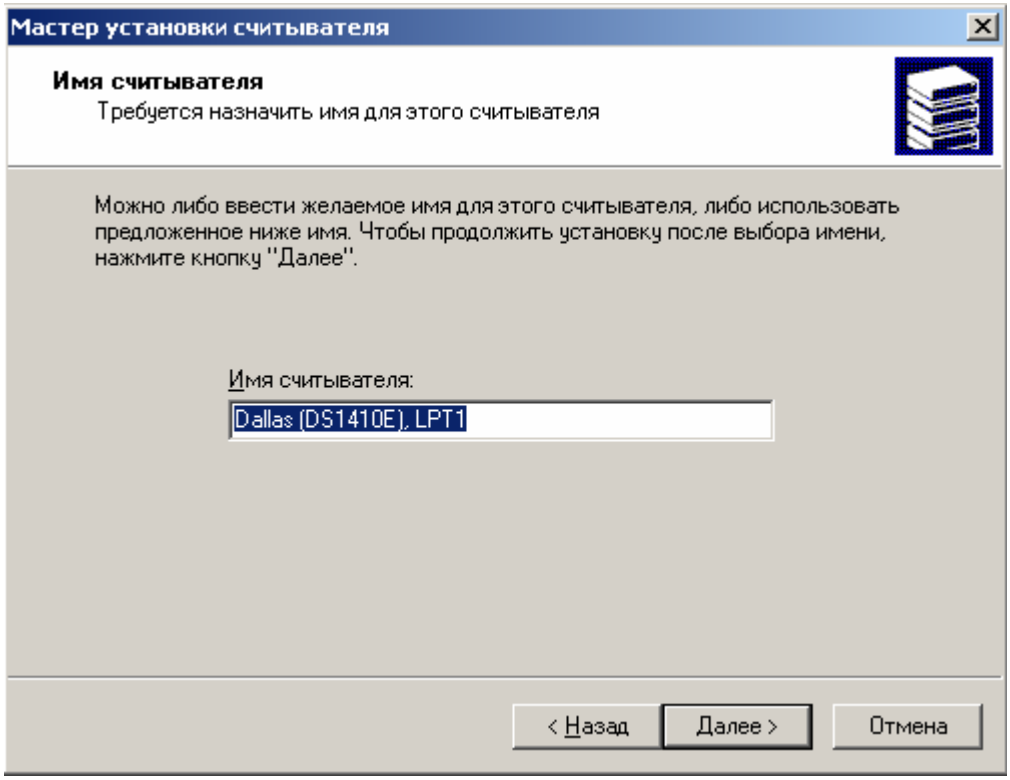


Рис. 12. Окно «Имя считывателя»

Система отобразит окно «Завершение работы мастера установки считывателя» (см.Рис. 13). Внимательно прочитайте текст в этом окне, нажмите в нем кнопку **Готово** и перезагрузите компьютер, если это требуется.

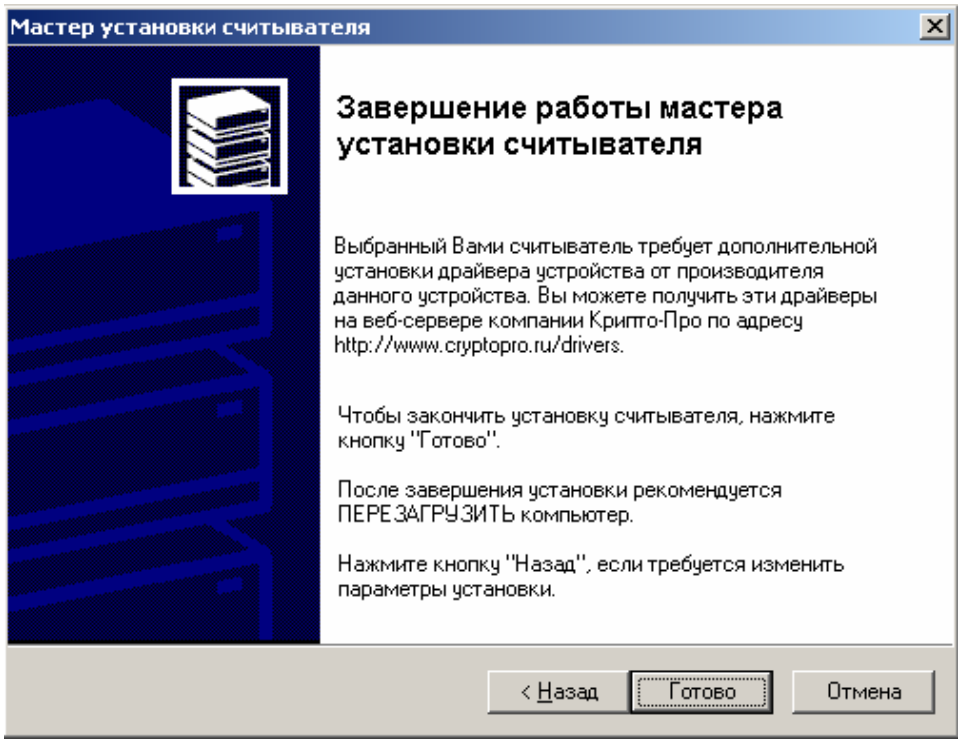


Рис. 13. Завершение мастера установки считывателя

Помимо считывателей, входящих в состав дистрибутива СКЗИ КриптоПро CSP, существует возможность установить считыватели с диска или с сервера КриптоПро.

Для этого в окне «Выбор считывателя» (см.Рис. 10) нажмите кнопку **Установить с диска**. Произойдет запуск Мастера установки считывателя с диска (см. Рис. 14). В окне мастера установки нажмите кнопку **Далее**.

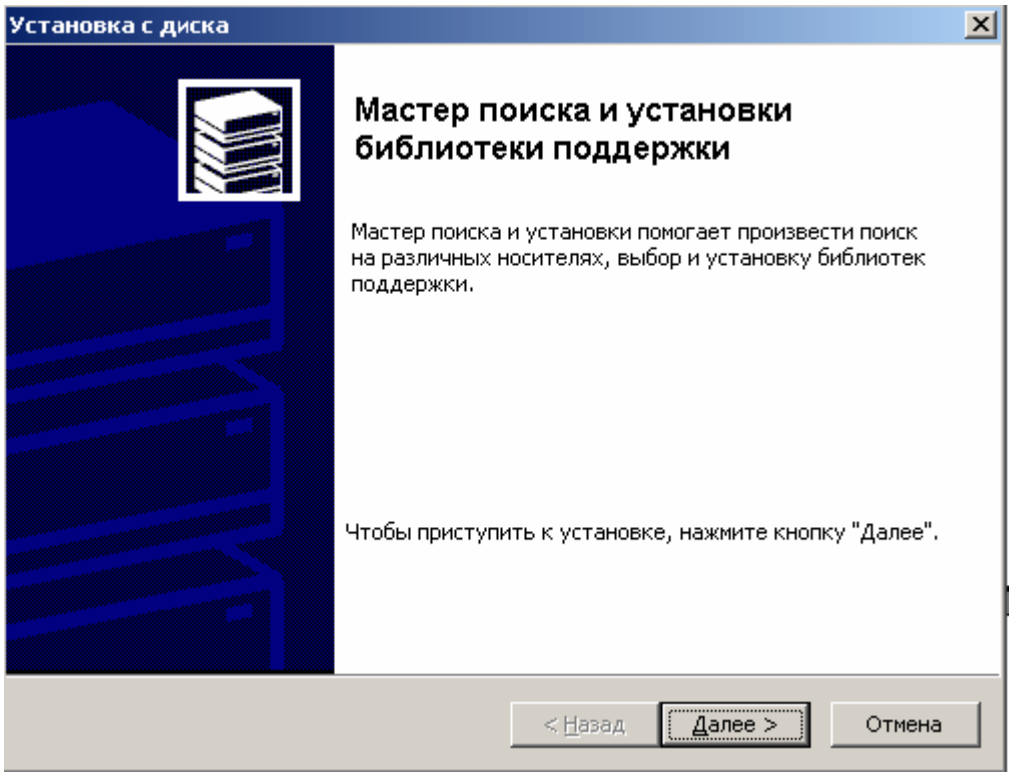


Рис. 14. Запуск мастера установки считывателя с диска

Система отобразит окно «Выбор размещения» (см. Рис. 15). В этом окне выберите размещение, с которого требуется установить считыватель (диск или сервер КриптоПро) и нажмите кнопку **Далее**.

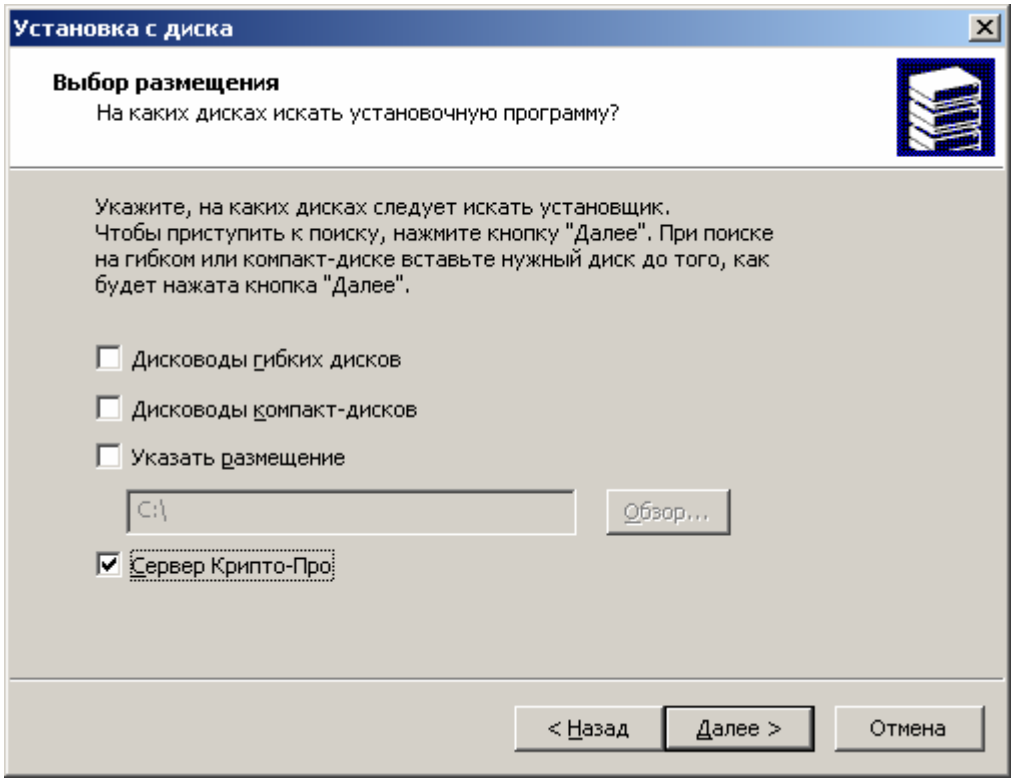


Рис. 15. Окно «Выбор размещения»

Система отобразит окно «Выбор установщика» (см. Рис. 16). В этом окне выберите установщик, который следует запустить, и нажмите кнопку **Далее**.

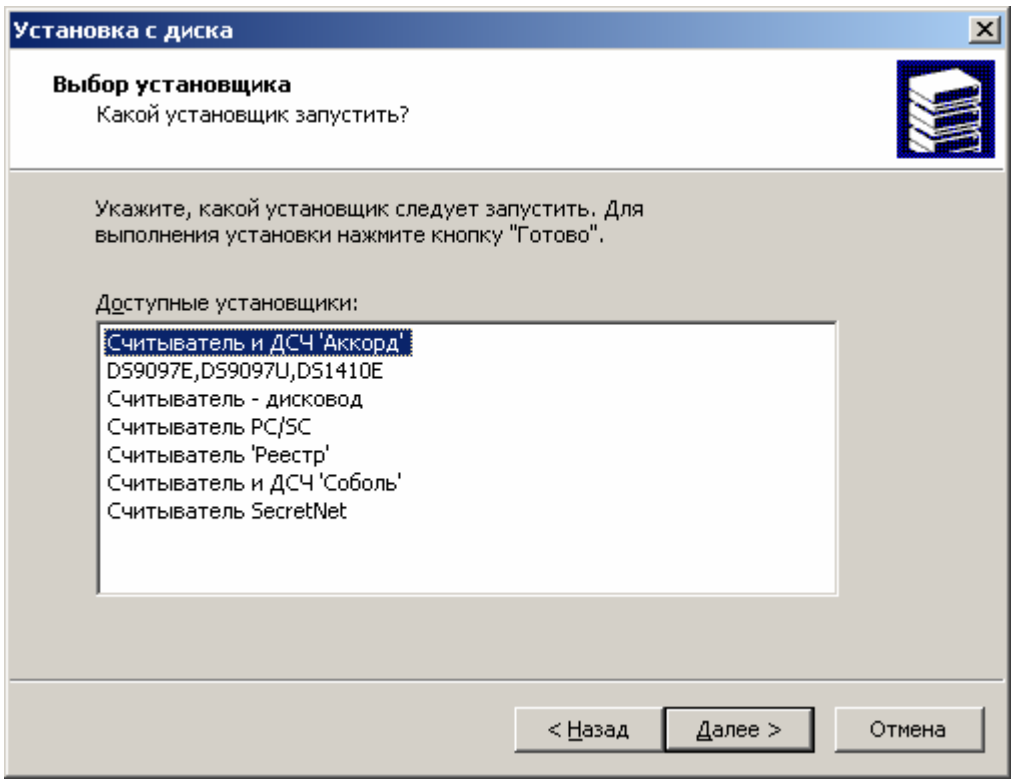


Рис. 16. Окно «Выбор установщика»

Произойдет запуск установщика считывателя (см. Рис. 17) После завершения установки нажмите кнопку **Готово**.

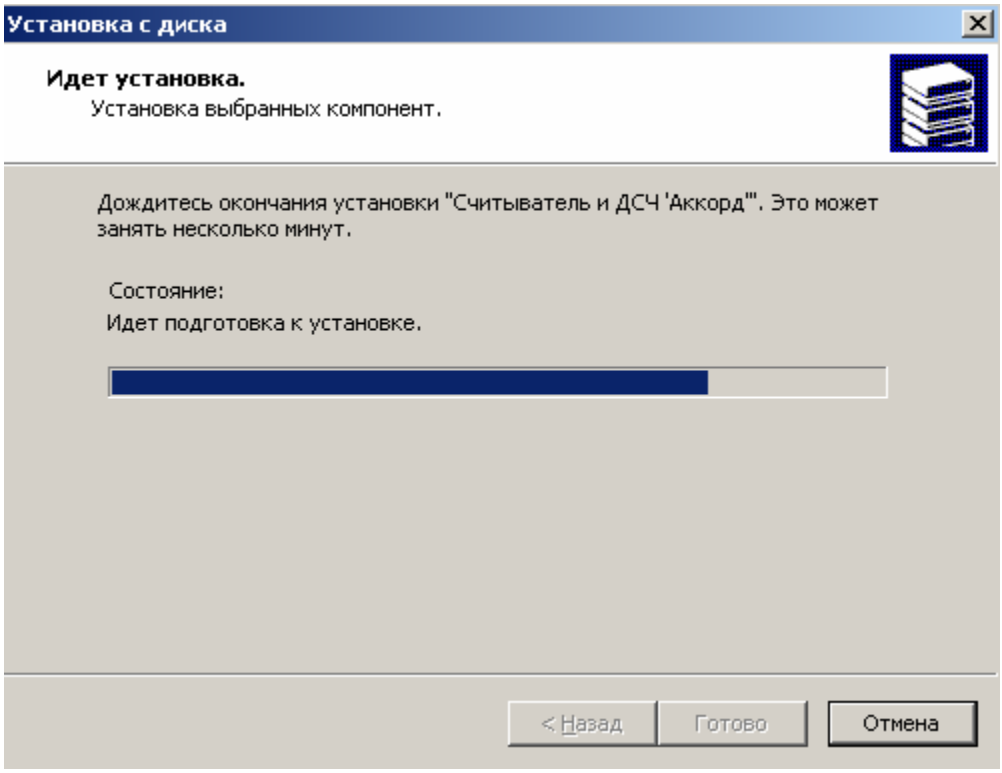


Рис. 17. Установка носителя с диска или с сервера

Примечание. В состав дистрибутива СКЗИ КриптоПро CSP не входят драйвера и другие модули третьих производителей, обеспечивающие взаимодействие КриптоПро CSP с аппаратной частью. Для их установки нужно воспользоваться программой установки, поставляемой производителями таких устройств. Например, если КриптоПро CSP уже установлено, и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

2.3.1.2. Удаление считывателя

Для того чтобы удалить считыватель в меню, выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить считыватели.**

Система отобразит окно «Управление считывателями» (см. Рис. 8). Выберите считыватель, который требуется удалить, и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление считывателя» (см. Рис. 18). Нажмите кнопку **Да**. Считыватель будет удален.

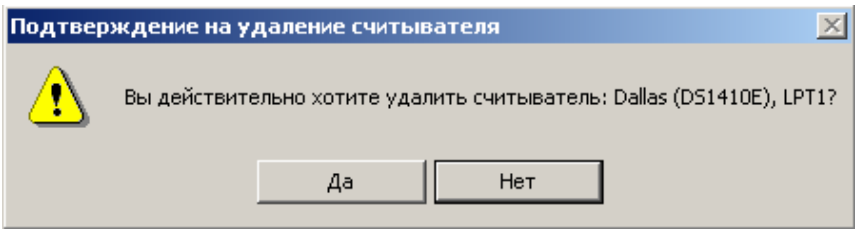


Рис. 18. Окно «Подтверждение на удаление считывателя»

2.3.1.3. Просмотр свойств считывателя

Для того чтобы просмотреть свойства считывателя, выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить считыватели.**

Система отобразит окно «Управление считывателями» (см. Рис. 8). Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя считывателя» (см.Рис. 19), в котором отображается справочная информация о выбранном считывателе, в том числе, и данные о состоянии устройства. После просмотра свойств считывателя нажмите кнопку **OK.**

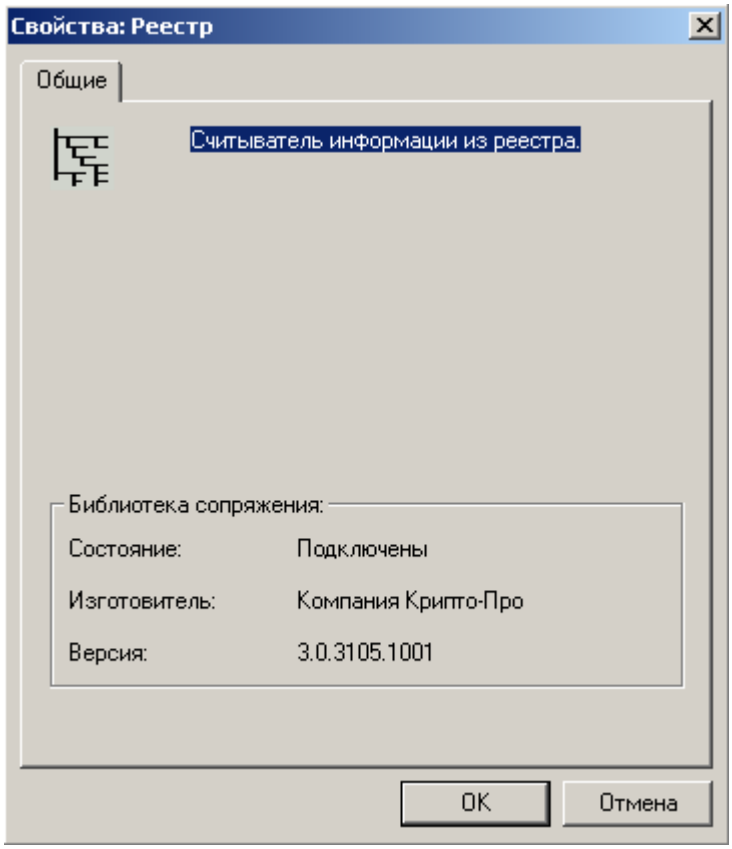


Рис. 19. Окно «Свойства: имя считывателя»

2.3.2. Изменение набора устройств хранения ключевой информации

2.3.2.1. Добавление носителя

Для того чтобы добавить носитель ключевой информации в меню, выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить носители.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 20).

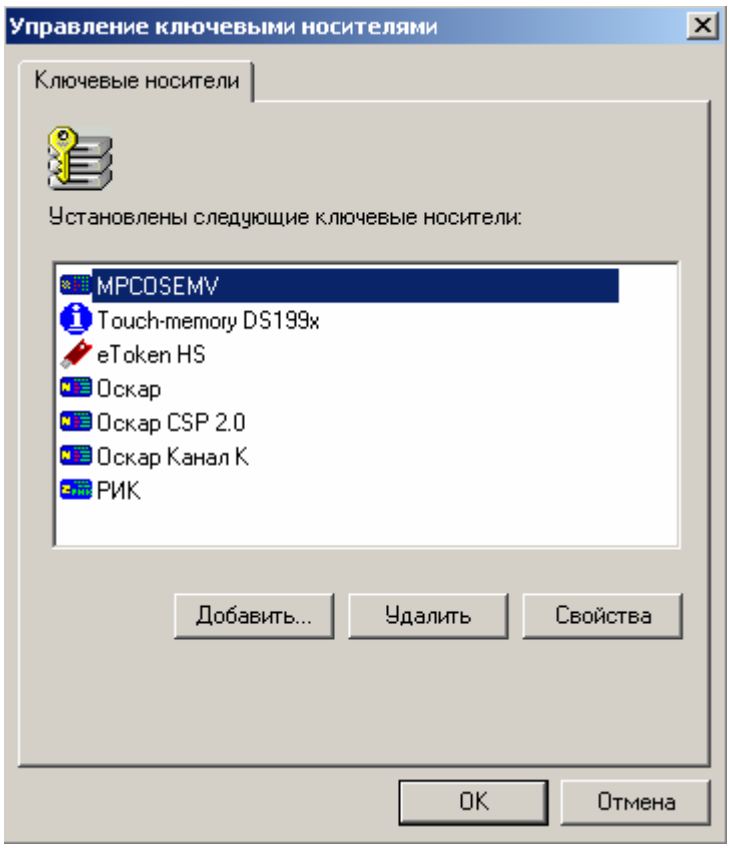


Рис. 20. Окно «Управление ключевыми носителями»

Для того чтобы добавить ключевой носитель, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки ключевого носителя (см. Рис. 21). В окне мастера установки нажмите кнопку **Далее**.

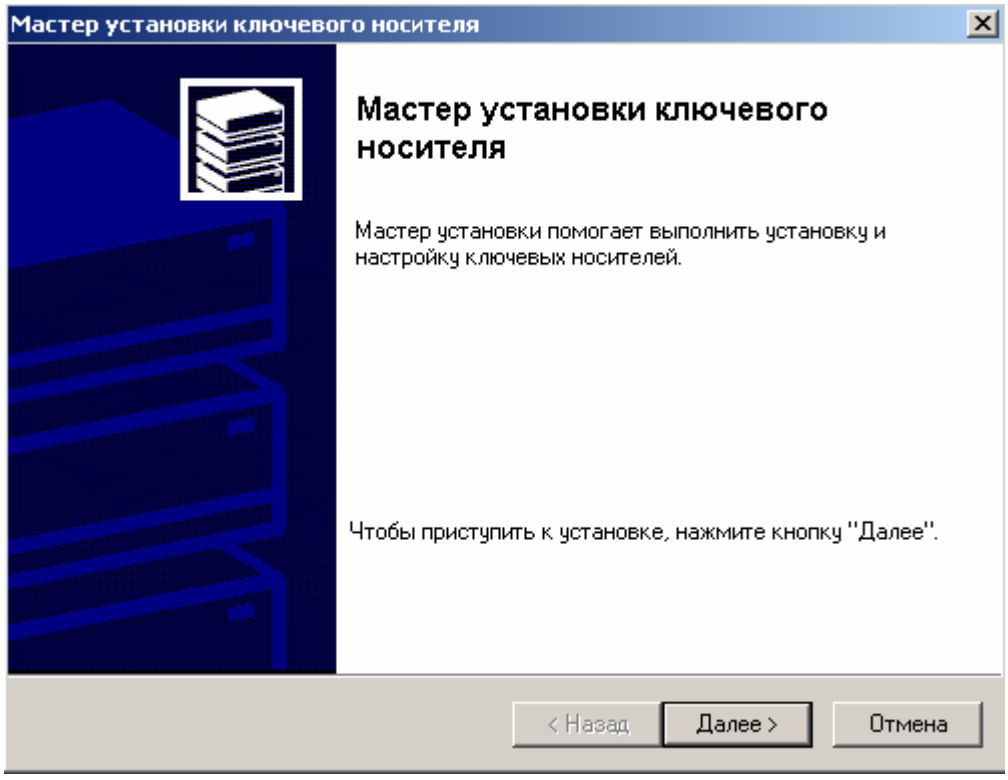


Рис. 21. Запуск мастера установки ключевого носителя

Система отобразит окно «Выбор ключевого носителя» (см. Рис. 22). В этом окне выберите ключевой носитель, который следует добавить, и нажмите кнопку **Далее.**

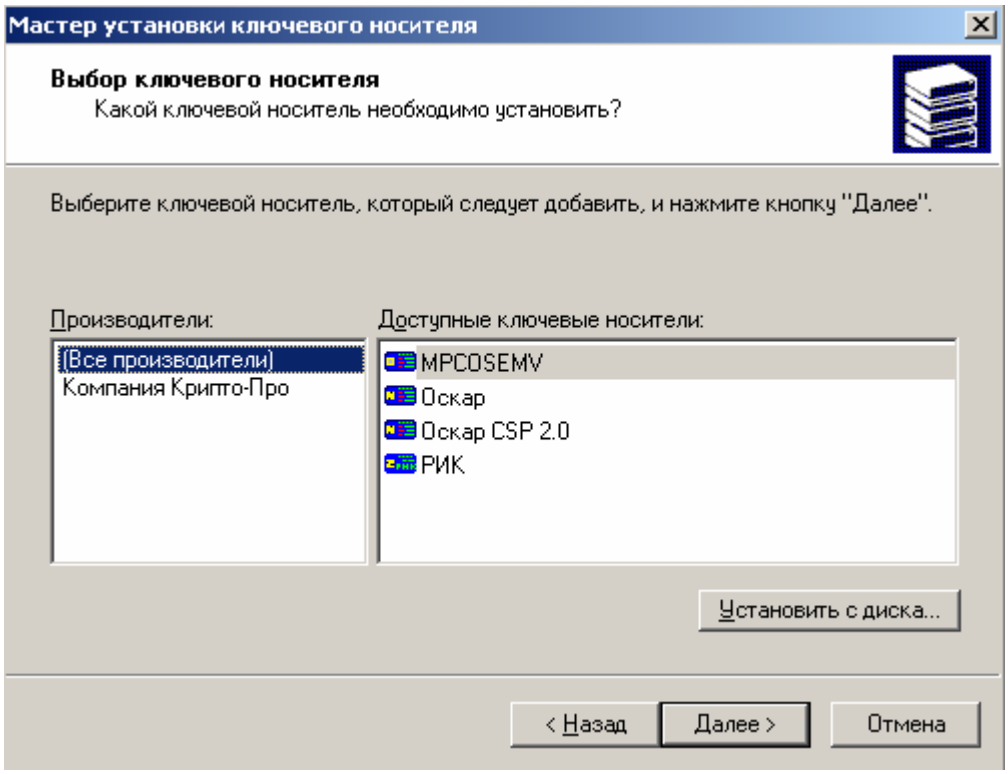


Рис. 22. Окно «Выбор ключевого носителя»

Система отобразит окно «Имя ключевого носителя» (см. Рис. 23). В этом окне введите имя выбранного носителя и нажмите кнопку **Далее.**

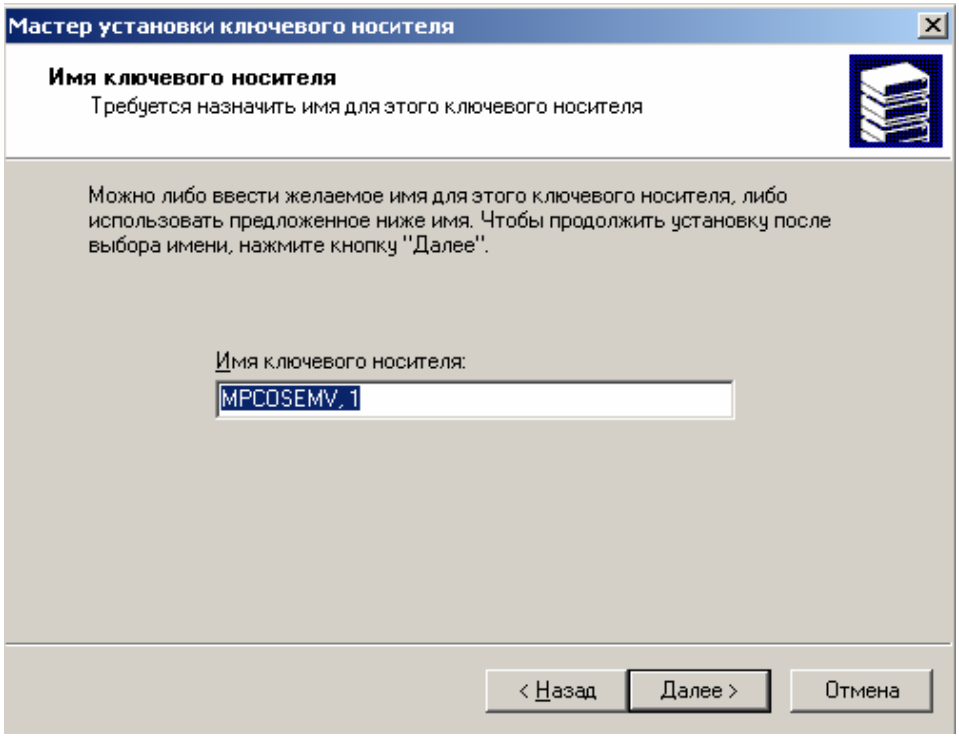


Рис. 23. Окно «Имя ключевого носителя»

Система может отобразить дополнительные окна в зависимости от типа ключевого носителя, так для MPCOS/EMV будет отображено окно «Разметка карты» (см. Рис. 24). В этом окне укажите разметку карты и нажмите кнопку **Далее.**

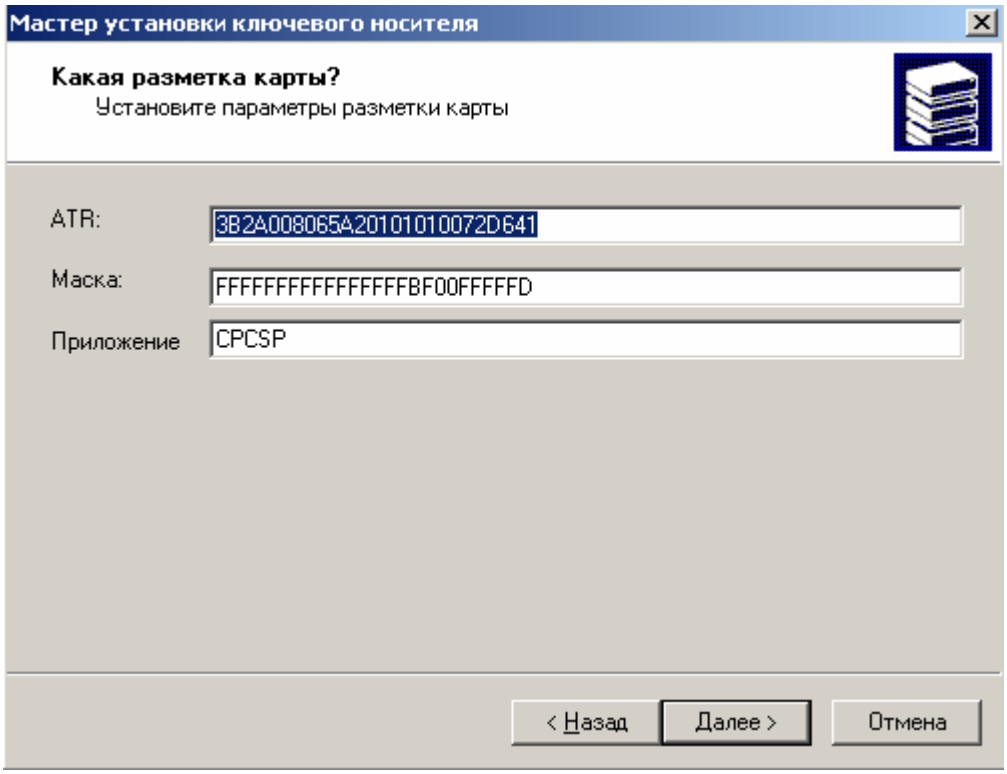


Рис. 24. Окно «Разметка карты»

Система отобразит окно «Завершение работы мастера установки ключевого носителя» (см. Рис. 25). Нажмите в нем кнопку **Готово**.

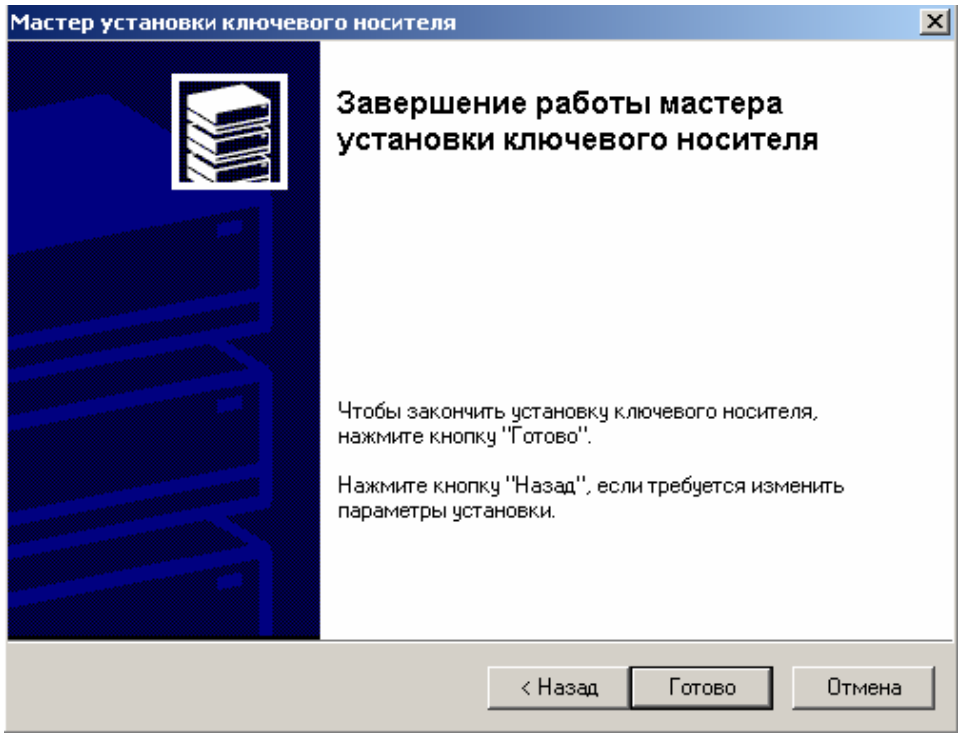


Рис. 25. Завершение мастера установки ключевого носителя

2.3.2.2. Удаление ключевого носителя

Для того чтобы удалить ключевой носитель, выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить носители.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 20). Выберите ключевой носитель, который требуется удалить, и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление ключевого носителя» (см. Рис. 26). Нажмите кнопку **Да**. Ключевой носитель будет удален.

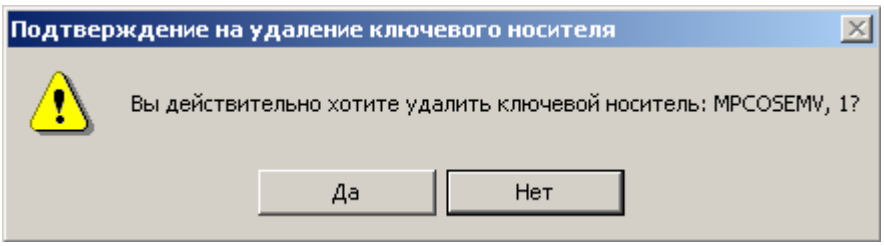


Рис. 26. Окно «Подтверждение на удаление ключевого носителя»

2.3.2.3. Просмотр свойств ключевого носителя

Для того чтобы просмотреть свойства ключевого носителя, выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить носители.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 20). Выберите ключевой носитель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя носителя» (см. Рис. 27), в котором отображается справочная информация о выбранном ключевом носителе, в том числе, и данные о состоянии устройства. После просмотра свойств ключевого носителя нажмите кнопку **OK.**

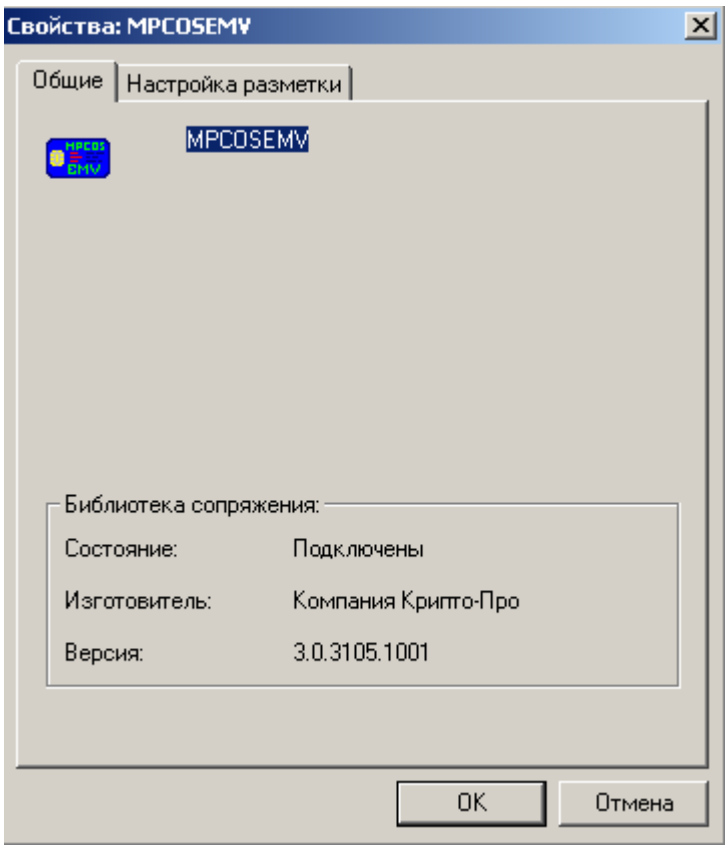


Рис. 27. Окно «Свойства: имя носителя»

2.3.3. Настройка датчиков случайных чисел (ДСЧ)

2.3.3.1. Добавление ДСЧ

Для того чтобы добавить ДСЧ в меню, выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 28).

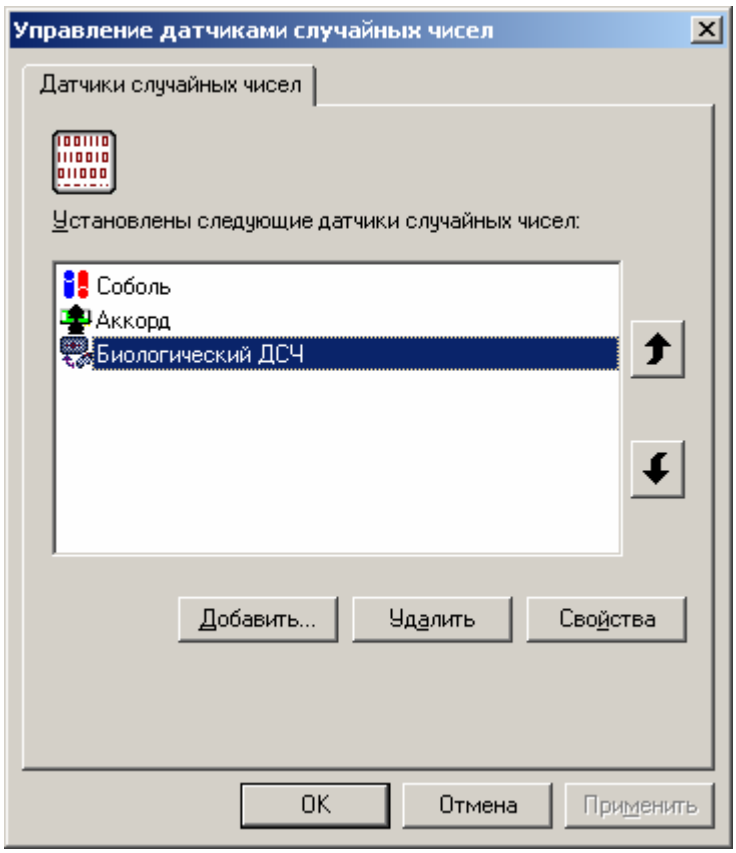


Рис. 28. Окно «Управление датчиками случайных чисел»

Для того чтобы добавить ДСЧ, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки ДСЧ (см. Рис. 29). В окне мастера установки нажмите кнопку **Далее**.

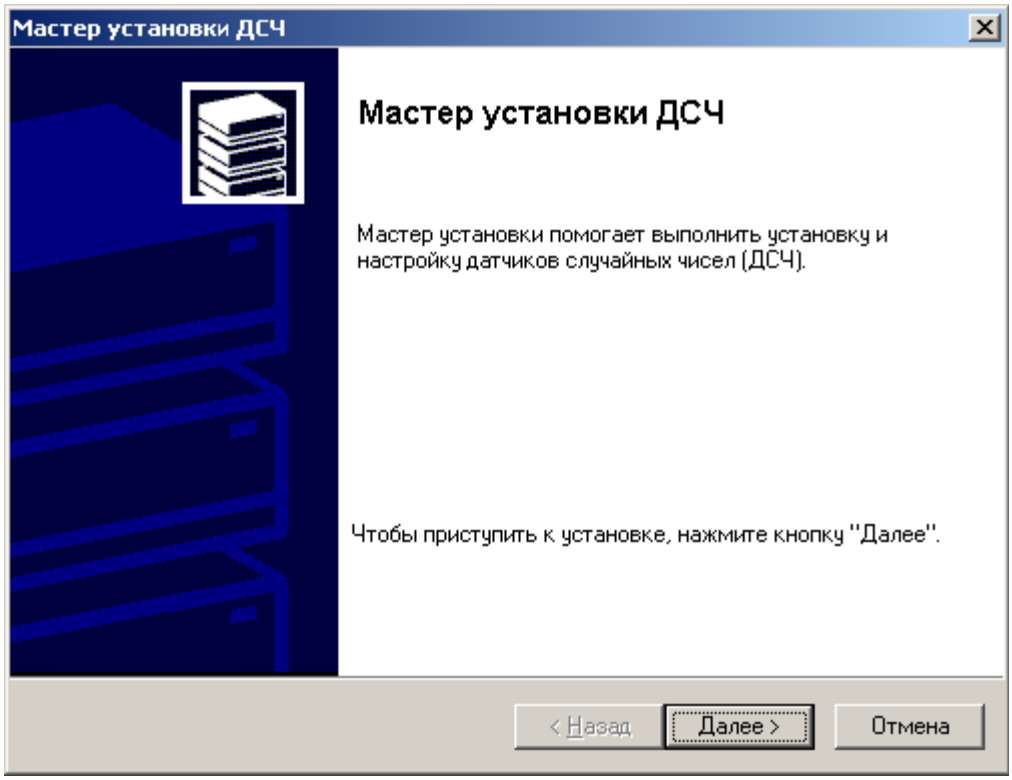


Рис. 29. Запуск мастера установки ДСЧ

Система отобразит окно «Выбор ДСЧ» (см. Рис. 30). В этом окне выберите датчик случайных чисел, который следует добавить и нажмите кнопку **Далее.**

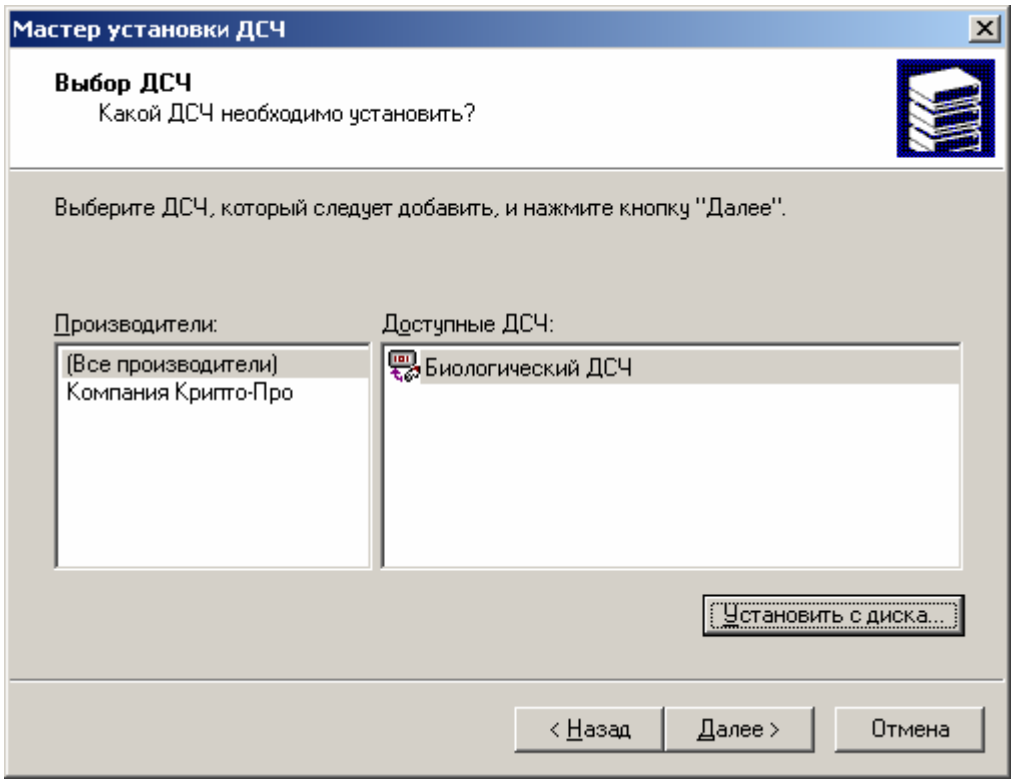


Рис. 30. Окно «Выбор ДСЧ»

Система отобразит окно «Имя ДСЧ» (см. Рис. 31). В этом окне введите имя выбранного датчика случайных чисел и нажмите кнопку **Далее.**

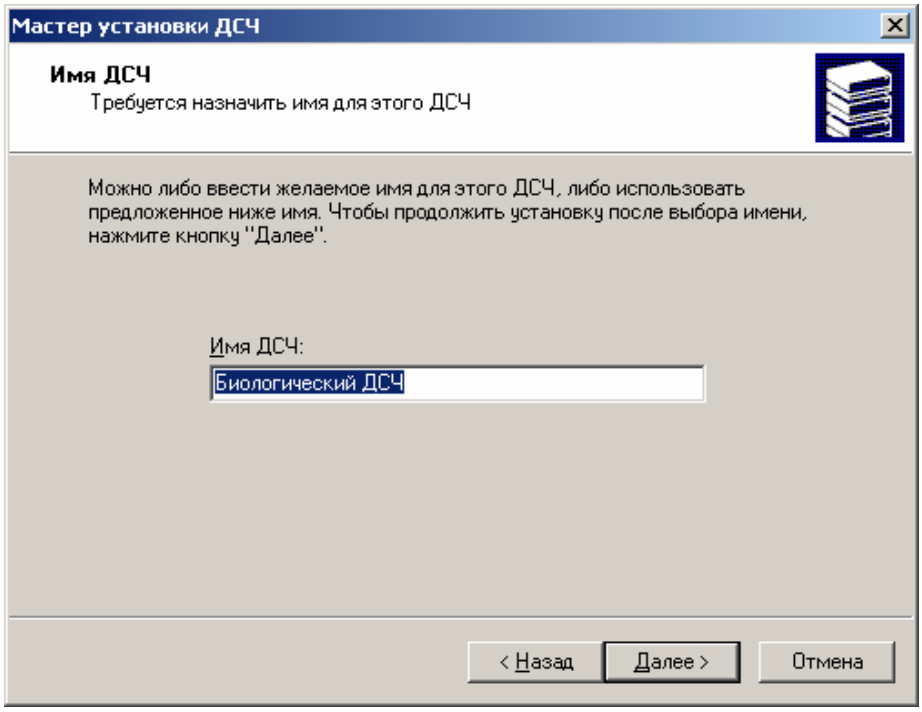


Рис. 31. Окно «Имя ДСЧ»

Система отобразит окно «Завершение работы мастера установки ДСЧ» (см. Рис. 32). Нажмите в нем кнопку **Готово** и перезагрузите компьютер**.**

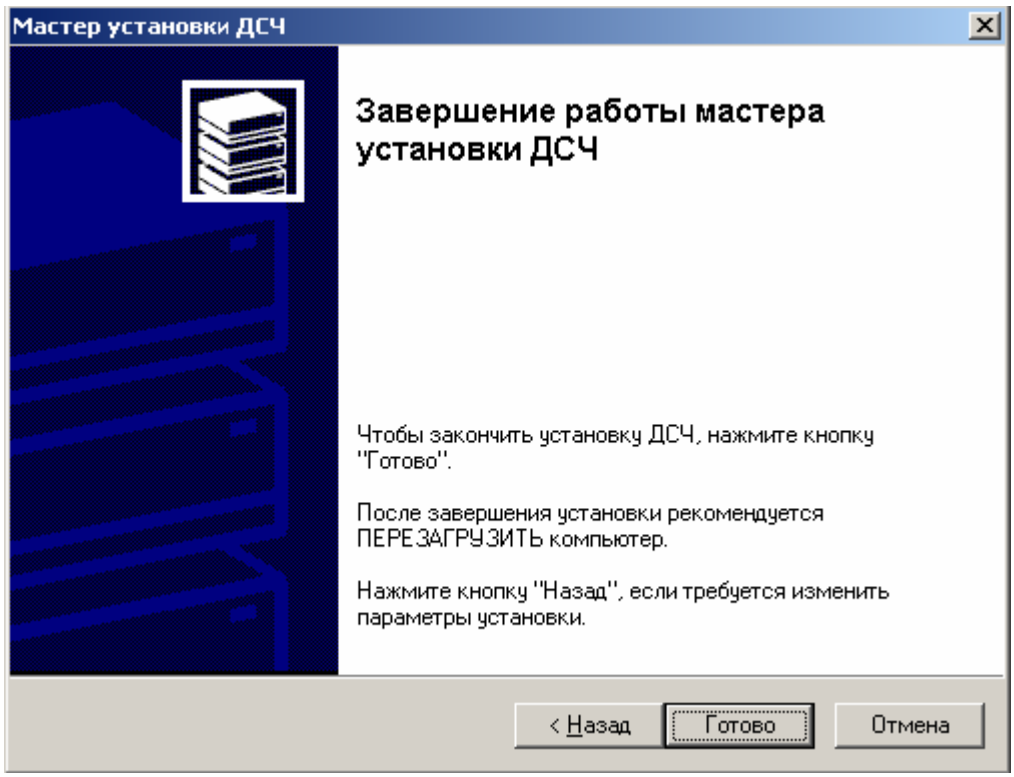


Рис. 32. Завершение мастера установки ДСЧ

2.3.3.2. Удаление ДСЧ

Для того чтобы удалить ДСЧ, выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 28). Выберите датчик, который требуется удалить и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление датчика случайных чисел» (см. Рис. 33). Нажмите кнопку **Да**. Датчик случайных чисел будет удален.

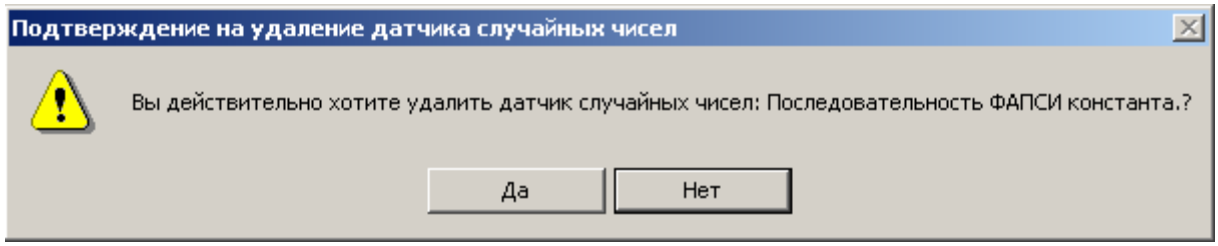


Рис. 33. Окно «Подтверждение на удаление ДСЧ»

2.3.3.3. Просмотр свойств ДСЧ

Для того чтобы просмотреть свойства ДСЧ, в меню выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Оборудование.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 7) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 28). Выберите датчик, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя ДСЧ» (см. Рис. 34), в котором отображается справочная информация о выбранном датчике случайных чисел, в том числе и данные о состоянии устройства. После просмотра свойств ДСЧ нажмите кнопку **OK.**

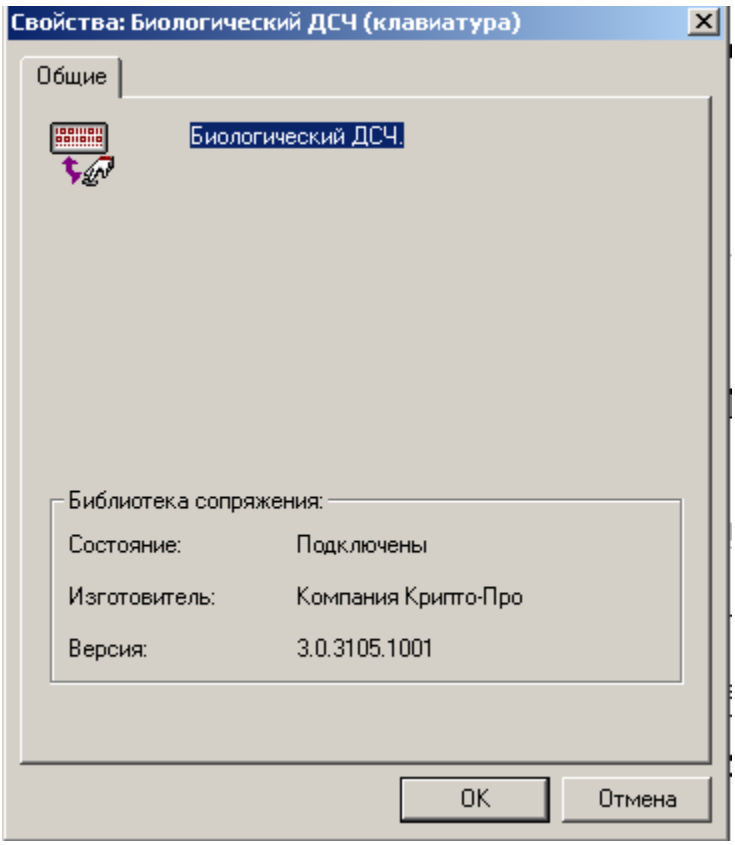


Рис. 34. Окно «Свойства: имя ДСЧ»

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, если ДСЧ не установлен, то будет использован следующий и т.д. Например, если установлено два датчика случайных чисел - БиоДСЧ 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 БиоДСЧ, необходимо с помощью кнопок   переместить его на верхнюю позицию в списке.

2.4. Работа с контейнерами и сертификатами

Закладка **Сервис** контрольной панели СКЗИ КриптоПро CSP предназначена для выполнения следующих операций:

- Копирование и удаление закрытого ключа, находящегося в существующем контейнере;
- Просмотр и установка сертификатов, находящихся в существующем контейнере закрытого ключа на носителе;
- Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе;
- Изменение и удаление запомненных паролей (PIN-кодов) доступа к носителям закрытых ключей.

2.4.1. Копирование и удаление контейнера закрытого ключа

2.4.1.1. Копирование контейнера закрытого ключа

Для того чтобы скопировать контейнер закрытого ключа, в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Сервис.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Скопировать контейнер**.

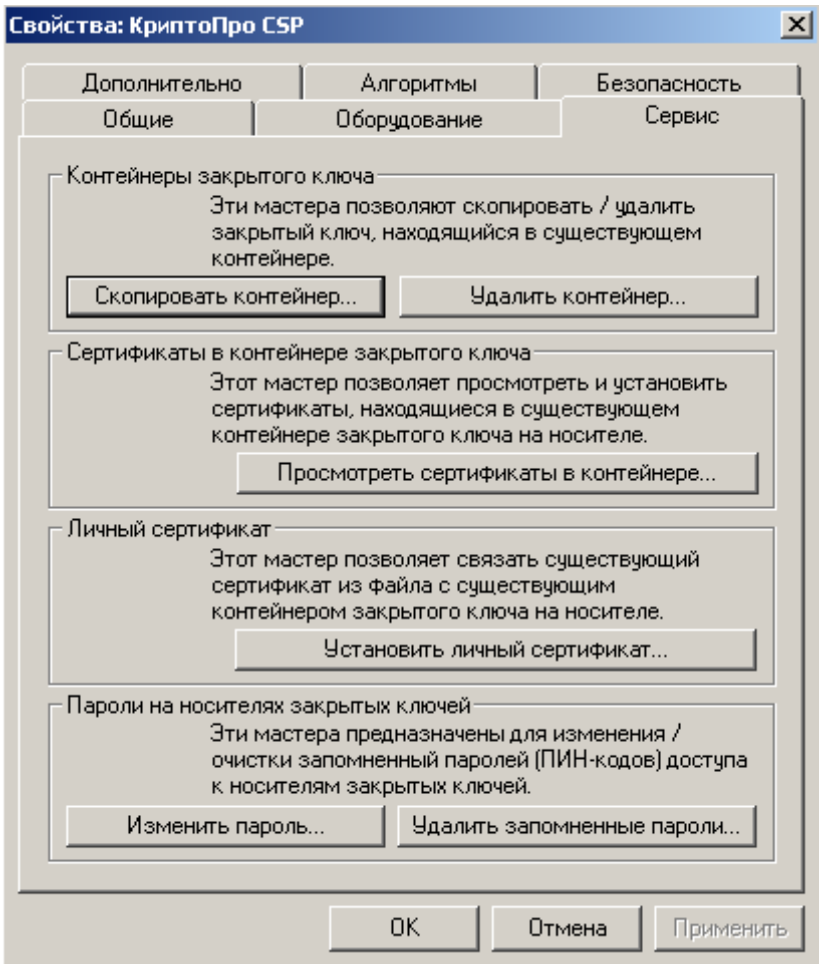


Рис. 35. Контрольная панель. Закладка «Сервис»

Система отобразит окно «Копирование контейнера закрытого ключа» (см. Рис. 36).

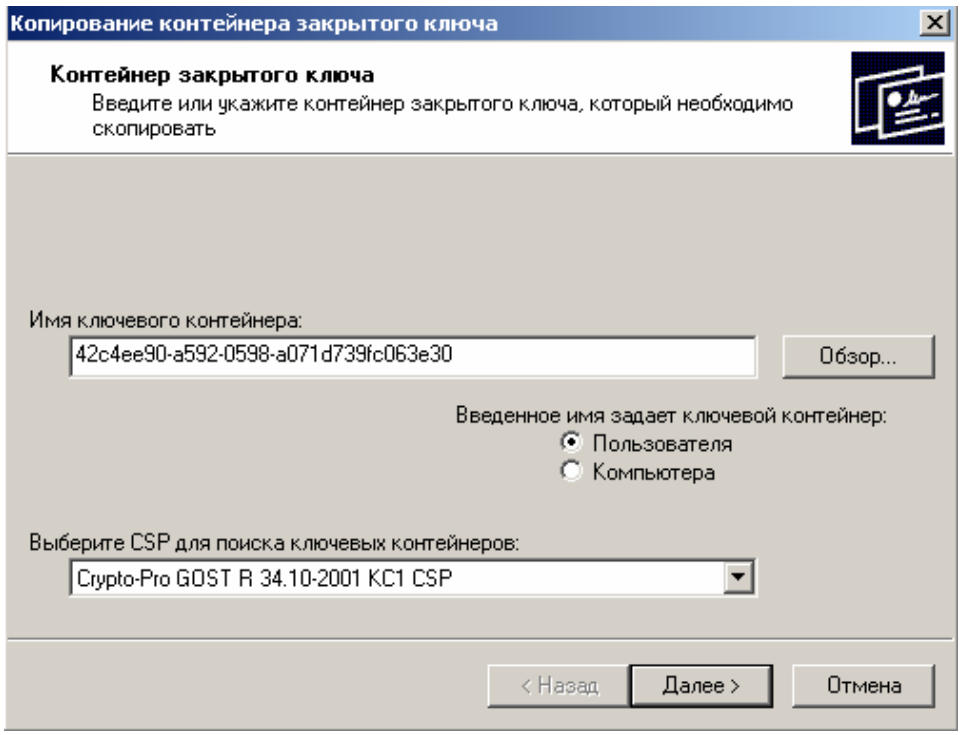


Рис. 36. Окно «Копирование контейнера закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор**;
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер;
- **Выберите CSP для поиска ключевых контейнеров** - необходимый КриптоПровайдер (CSP) выбирается из предлагаемого списка.

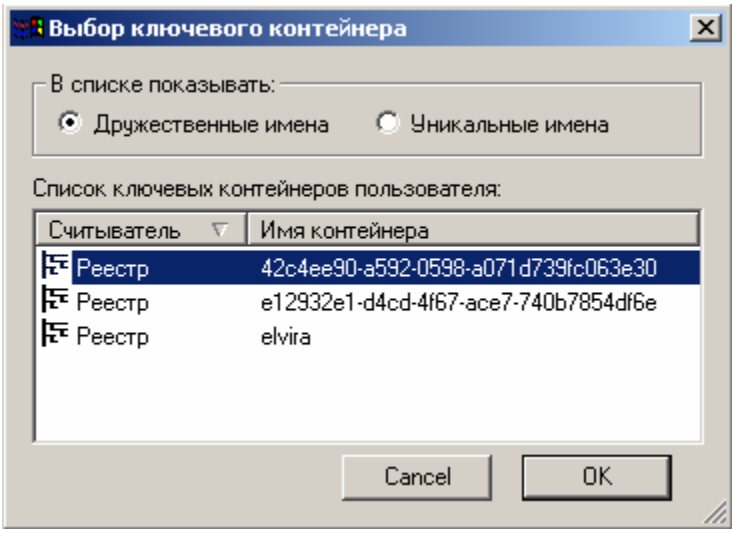


Рис. 37. Выбор ключевого контейнера

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Копирование контейнера закрытого ключа» (см. Рис. 38), в котором необходимо ввести имя нового ключевого контейнера и установить переключатель **Введенное имя задает ключевой контейнер** в положение

Пользователь или **Компьютер,** в зависимости от того, в каком хранилище требуется разместить скопированный контейнер.

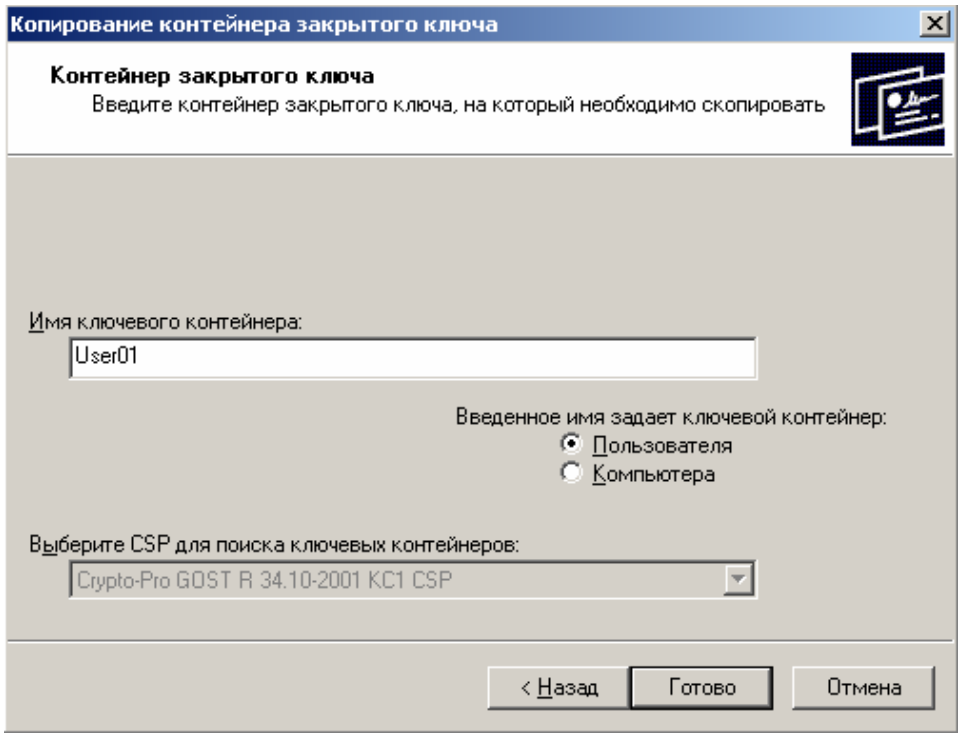


Рис. 38. Окно «Копирование контейнера закрытого ключа»

После ввода нажмите кнопку **Готово**. Система отобразит окно, в котором необходимо выбрать носитель для скопированного контейнера (см. Рис. 39).

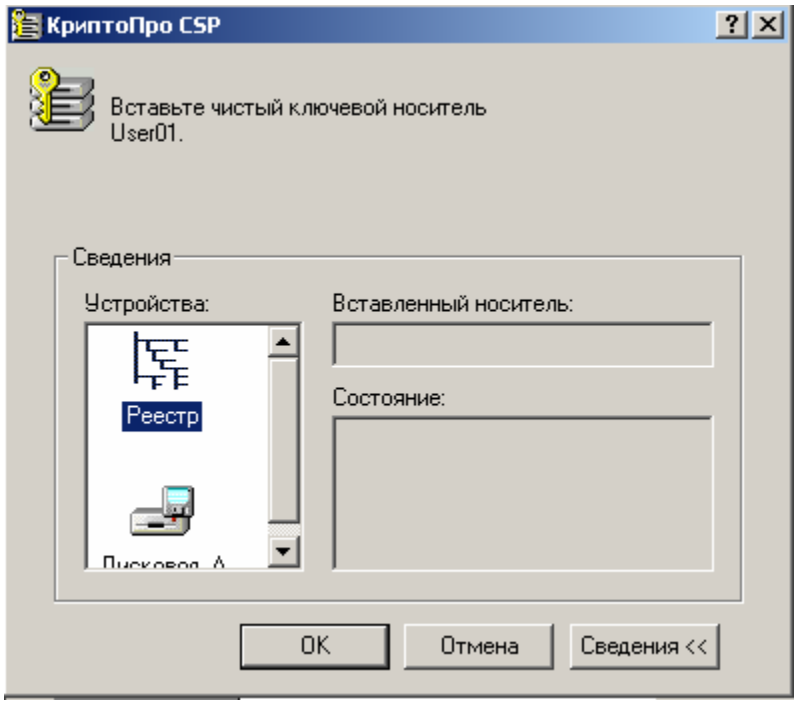


Рис. 39. Окно выбора носителя

Вставьте носитель в считыватель и нажмите кнопку **ОК**. Система отобразит окно установки пароля на доступ к закрытому ключу (см. Рис. 40). Введите пароль, подтвердите его, при необходимости установите флаг **Запомнить пароль** (если данный флаг будет установлен, то пароль сохранятся в специальном хранилище на локальном компьютере и при обращении к закрытому ключу пароль будет автоматически считываться из этого хранилища, а не вводиться пользователем).

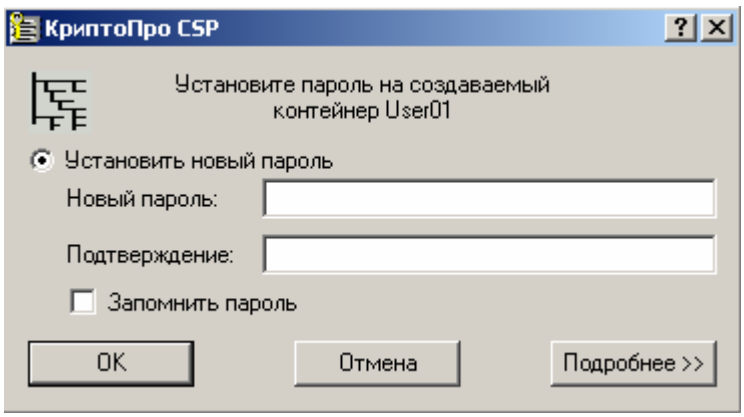


Рис. 40. Окно ввода пароля

После ввода необходимых данных нажмите кнопку **ОК**. СКЗИ «КриптоПро CSP» осуществит копирование контейнера закрытого ключа.

2.4.1.2. Удаление контейнера закрытого ключа

Для того чтобы скопировать контейнер закрытого ключа в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Сервис**. В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Удалить контейнер**.

Система отобразит окно «Копирование контейнера закрытого ключа» (см. Рис. 41).

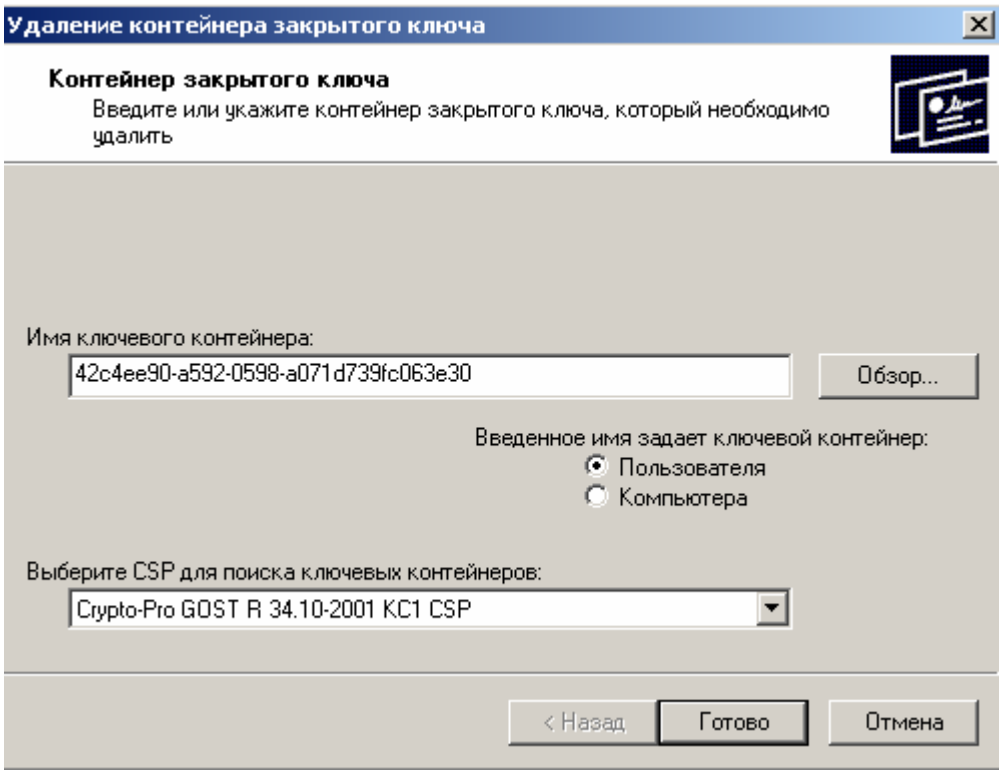


Рис. 41. Окно «Удаление контейнера закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор**;
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище расположен контейнер;
- **Выберите CSP для поиска ключевых контейнеров** - необходимый КриптоПровайдер (CSP) выбирается из предлагаемого списка.

После ввода всех данных нажмите кнопку **Готово**.

Система отобразит окно подтверждения удаления ключевого контейнера (см. Рис. 42). Нажмите кнопку **Да.** СКЗИ «КриптоПро CSP» произведет удаление ключевого контейнера.

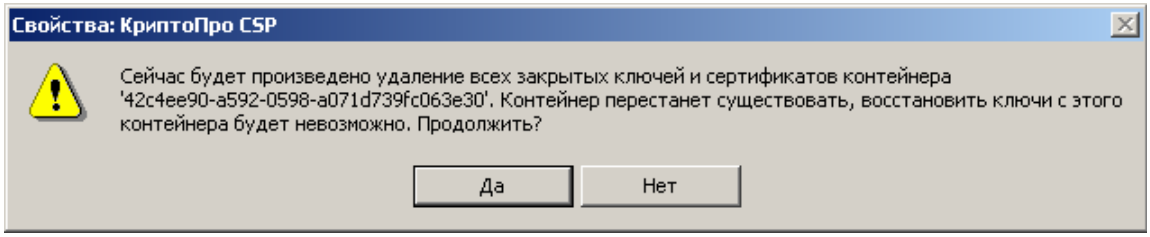


Рис. 42. Окно подтверждения удаления ключевого контейнера

2.4.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа

2.4.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа

Для того чтобы просмотреть сертификат, в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Сервис.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Просмотреть сертификаты в контейнере**.

Система отобразит окно «Сертификаты в контейнере закрытого ключа» (см. Рис. 43).

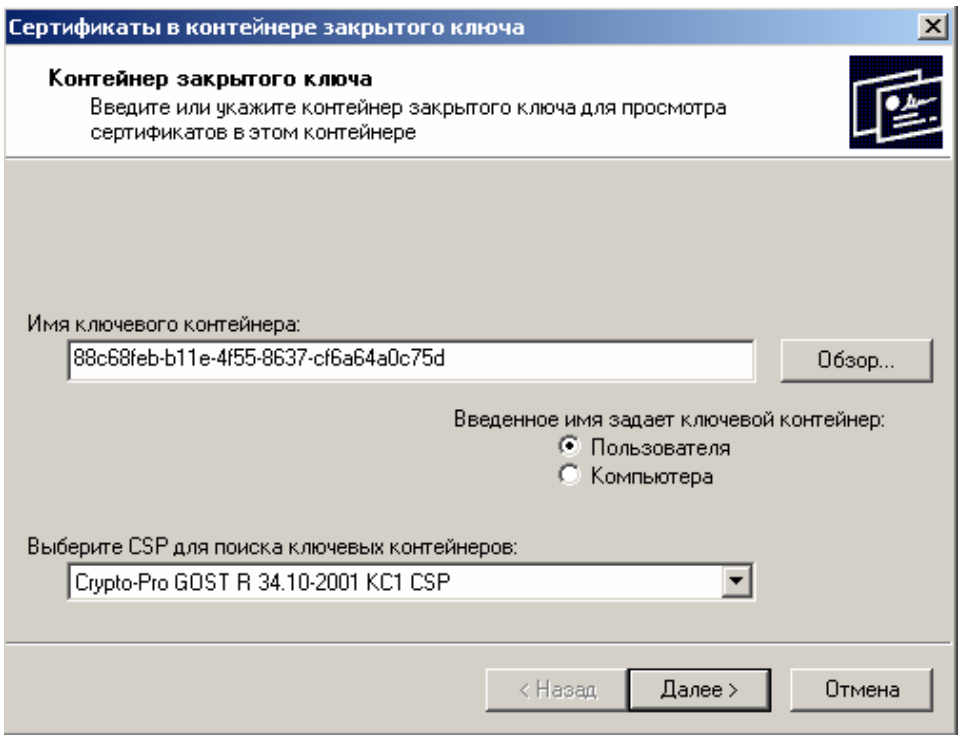


Рис. 43. Окно «Сертификаты в контейнере закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор**;
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище расположен контейнер;
- **Выберите CSP для поиска ключевых контейнеров** - необходимый КриптоПровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **OK**.

Если сертификата в контейнере закрытого ключа нет, то система отобразит окно, информирующее пользователя об отсутствии сертификата в контейнере (см. Рис. 44).

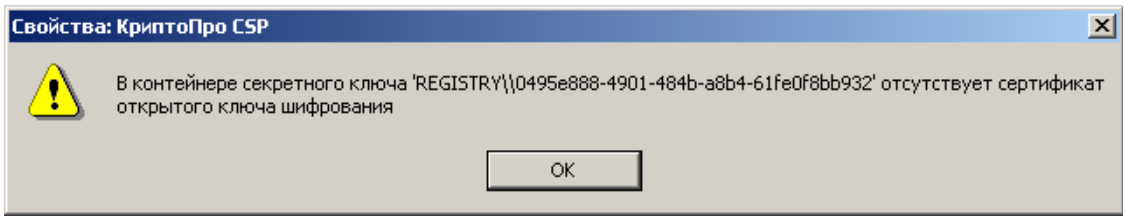


Рис. 44. Окно, информирующее об отсутствии сертификата

Если сертификат в выбранном контейнере имеется, то система отобразит окно «Сертификат для просмотра» (см. Рис. 45).

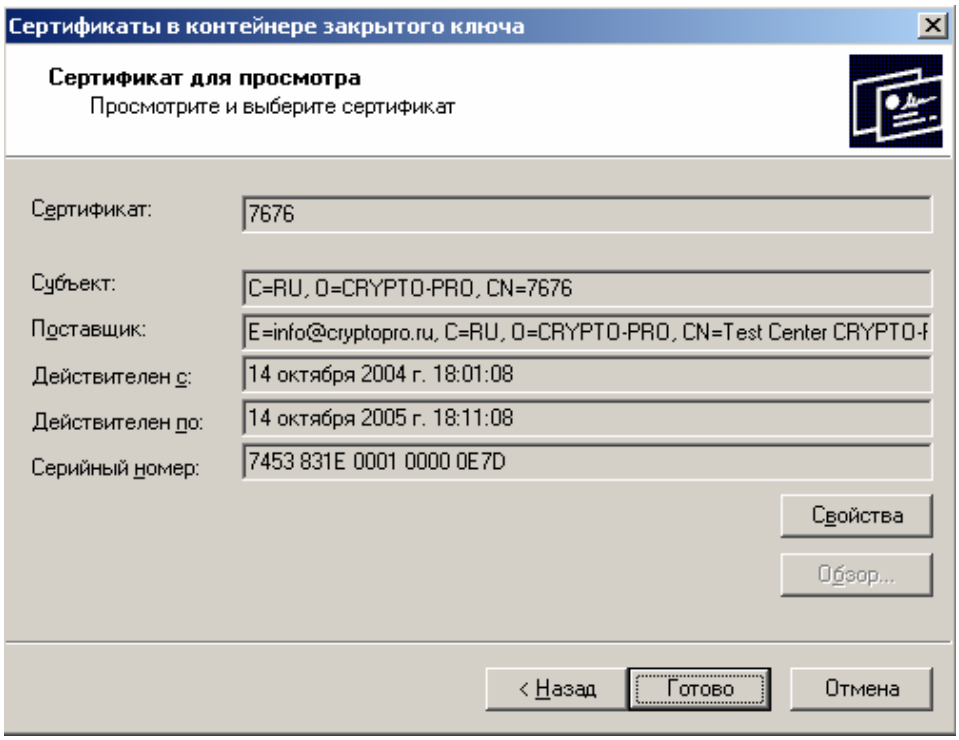


Рис. 45. Окно «Сертификат для просмотра»

Для просмотра основных свойств сертификата нажмите кнопку **Свойства** в окне «Сертификат для просмотра» (см. Рис. 45). Система отобразит свойства сертификата (см. Рис. 46).

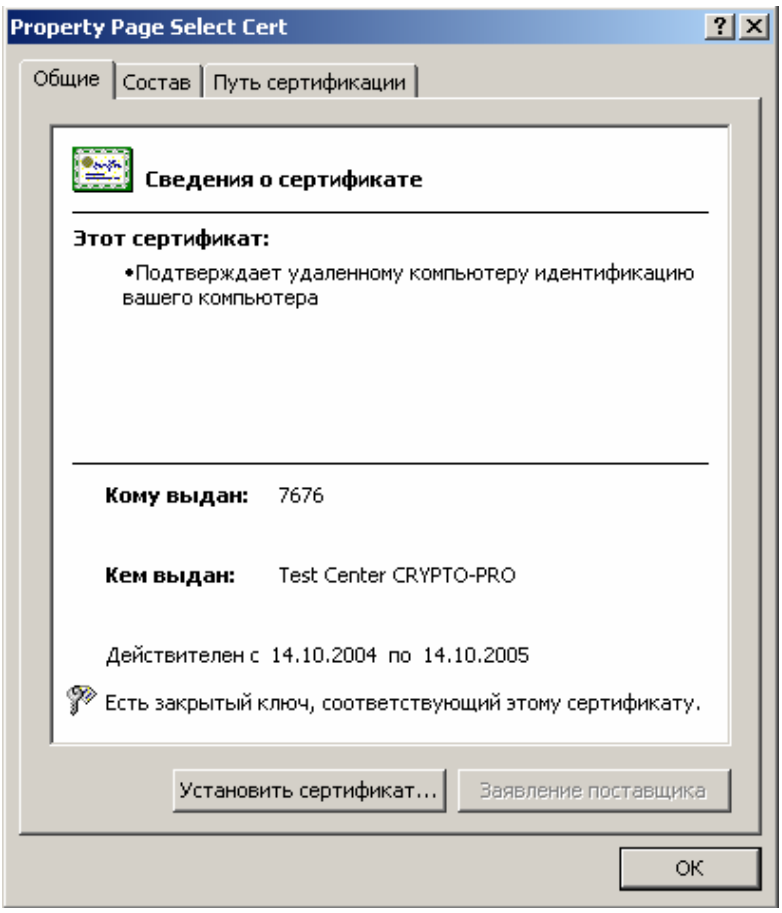


Рис. 46. Окно просмотра свойств сертификата

2.4.2.2. Установка личного сертификата, хранящегося в контейнере закрытого ключа



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

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

Для того чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальных справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для того чтобы установить личный сертификат, выполните последовательность действий, указанных в пункте 2.4.2.1.

В окне просмотра свойств сертификата (см. Рис. 46) нажмите кнопку **Установить сертификат**.

Осуществится запуск **Мастера импорта сертификатов** (см. Рис. 47).

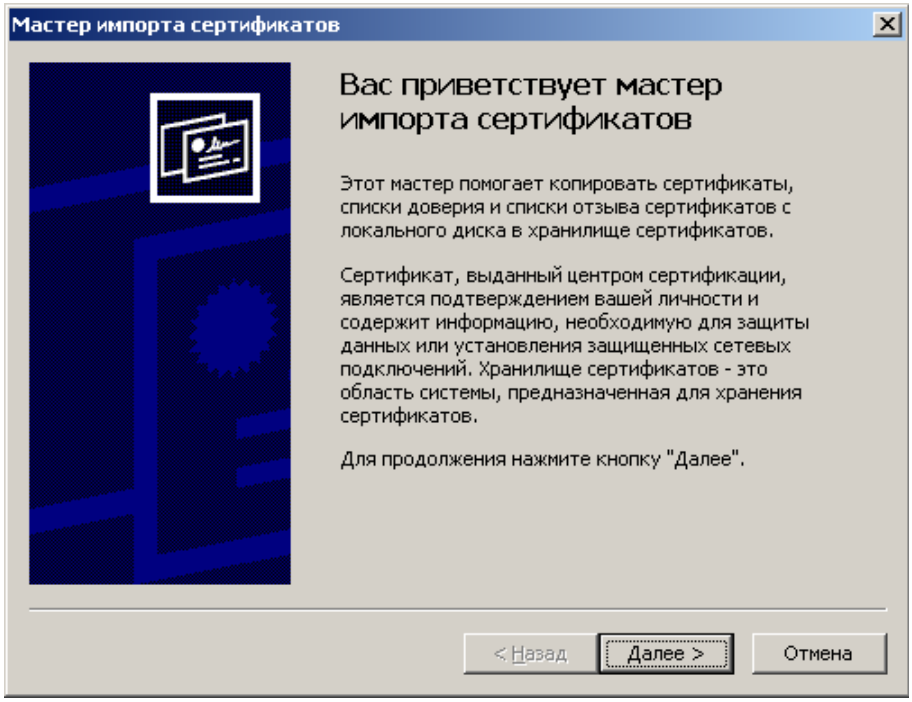


Рис. 47. Запуск мастера импорта сертификатов

Нажмите кнопку **Далее**. Система отобразит окно «Хранилище сертификатов», в котором необходимо указать, в какое хранилище требуется поместить сертификат (см. Рис. 48).

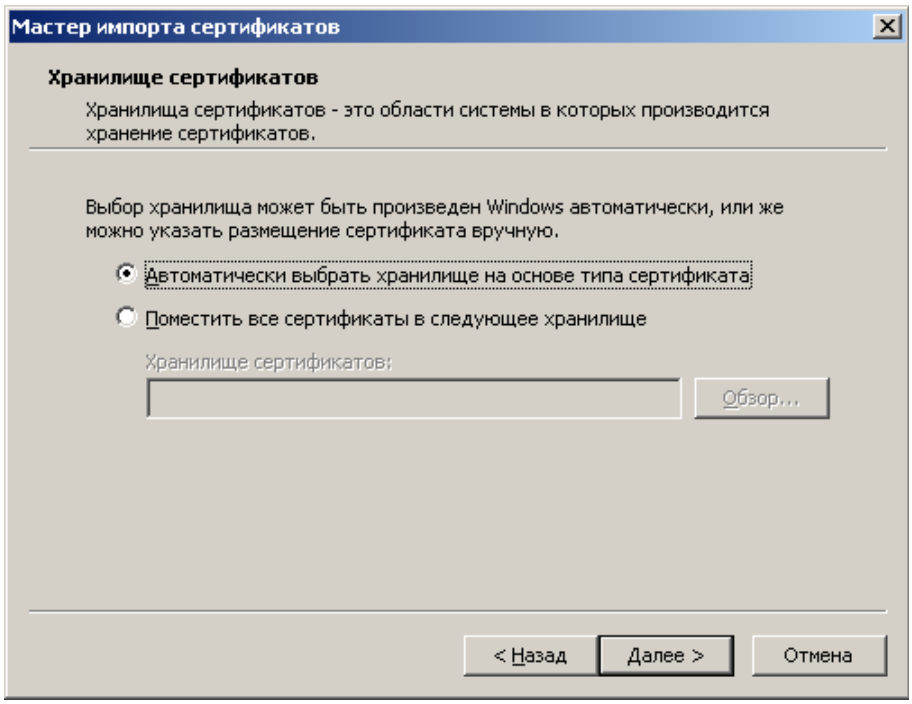


Рис. 48. Окно «Хранилище сертификатов»

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 закрытого ключа (расположение контейнера закрытого ключа определялось в пункте 2.4.2.1 с помощью переключателя **Введенное имя задает ключевой контейнер**).

После выполненных действий нажмите кнопку **Далее.**

Система отобразит окно «Завершение работы мастера импорта сертификатов» (см. Рис. 49).

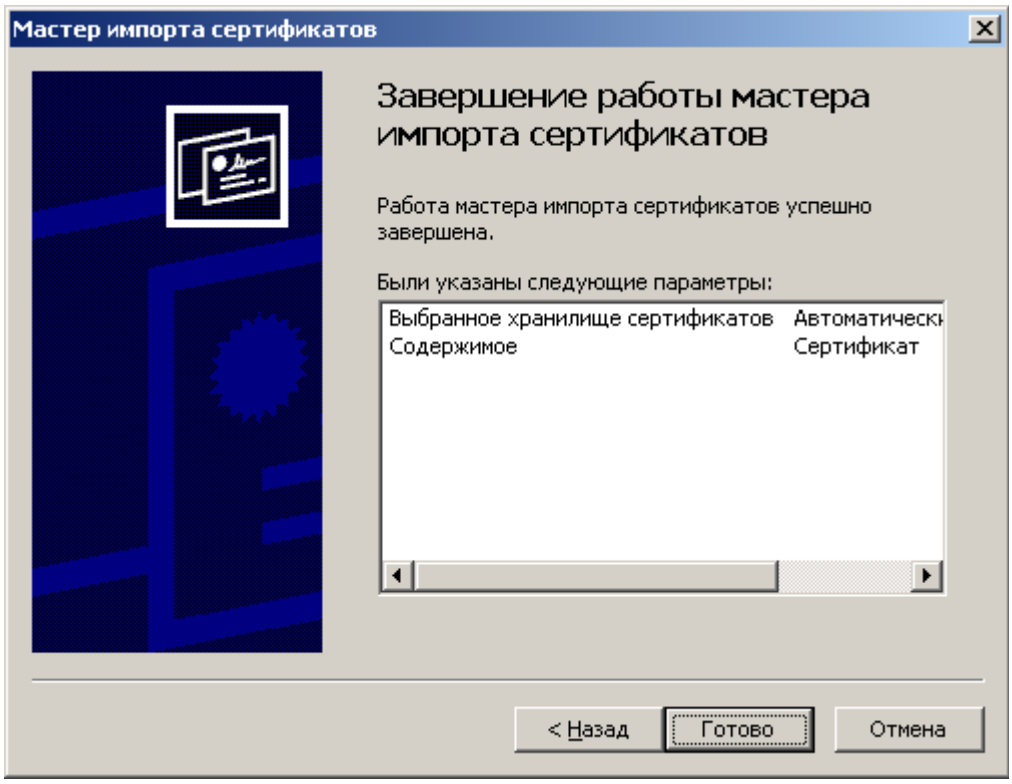


Рис. 49. Завершение мастера импорта сертификатов

Проверьте правильность выбранных параметров и нажмите кнопку **Готово.** Система отобразит окно, информирующее пользователя об успешной установке сертификата (см. Рис. 50)

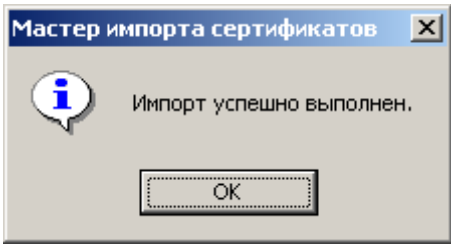


Рис. 50. Успешное выполнение импорта

2.4.3. 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 закрытый ключ, соответствующий данному сертификату.

Для того чтобы установить личный сертификат в меню, выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Сервис.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Установить личный сертификат**.

Система отобразит окно «Мастер установки личного сертификата» (см. Рис. 51). Ознакомьтесь с текстом и нажмите кнопку **Далее.**

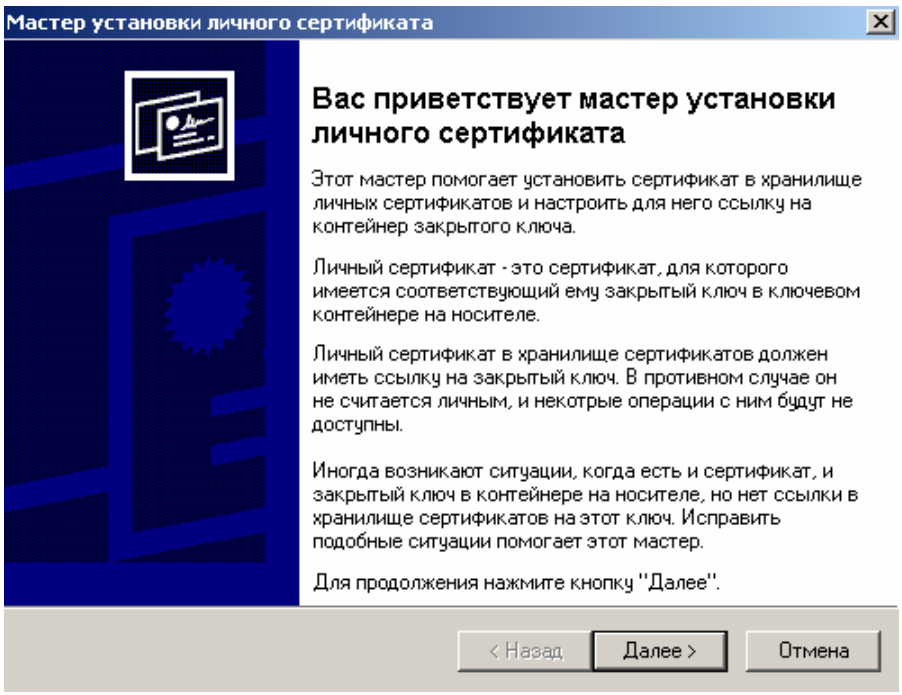


Рис. 51. Окно «Мастер установки личного сертификата»

Система отобразит окно «Расположение файла сертификата» (см. Рис. 52). В поле **Имя файла сертификата** укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее.**

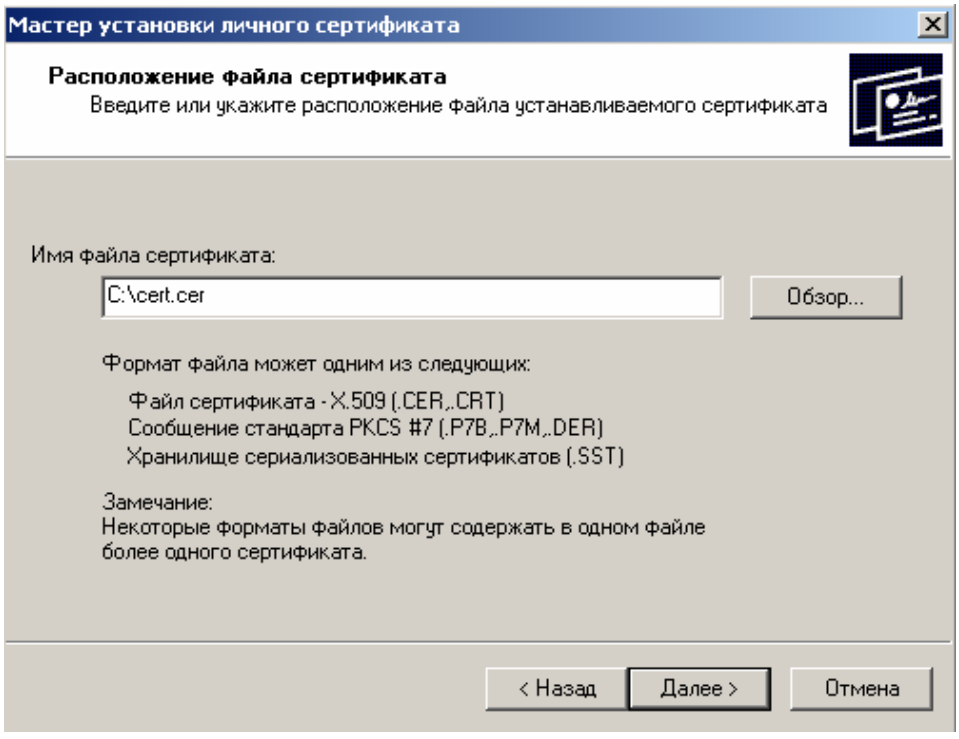


Рис. 52. Окно «Расположение файлов сертификата»

Система перейдет к окну «Сертификат для установки» (см. Рис. 53). В нем выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

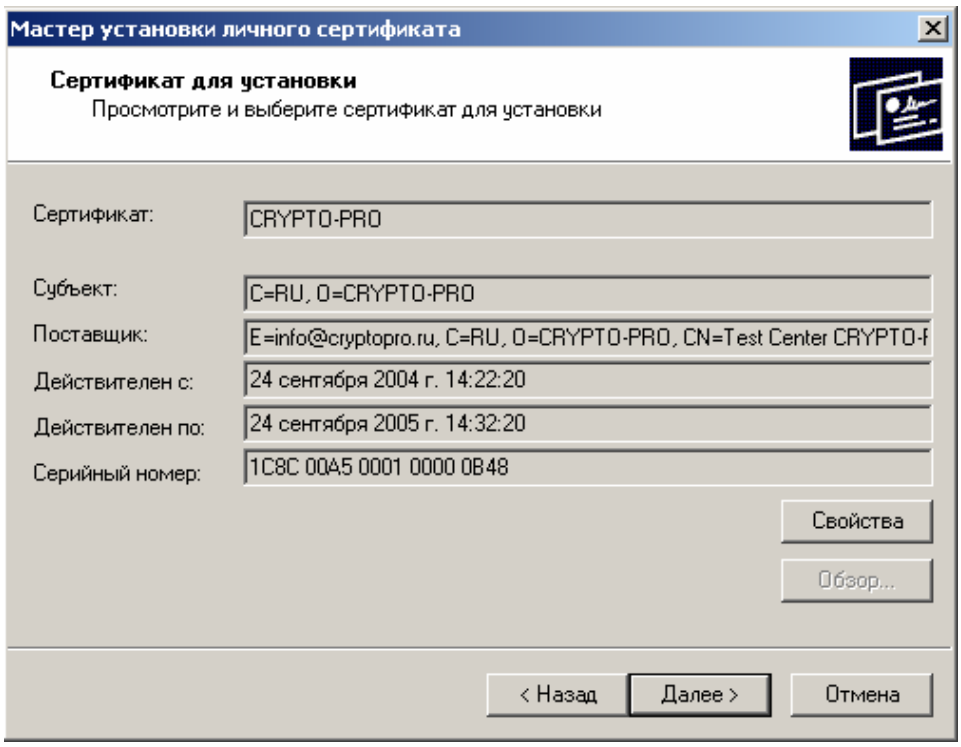


Рис. 53. Окно «Сертификат для установки»

Нажмите кнопку **Далее.**

Система отобразит окно «Контейнер закрытого ключа» (см. Рис. 54).

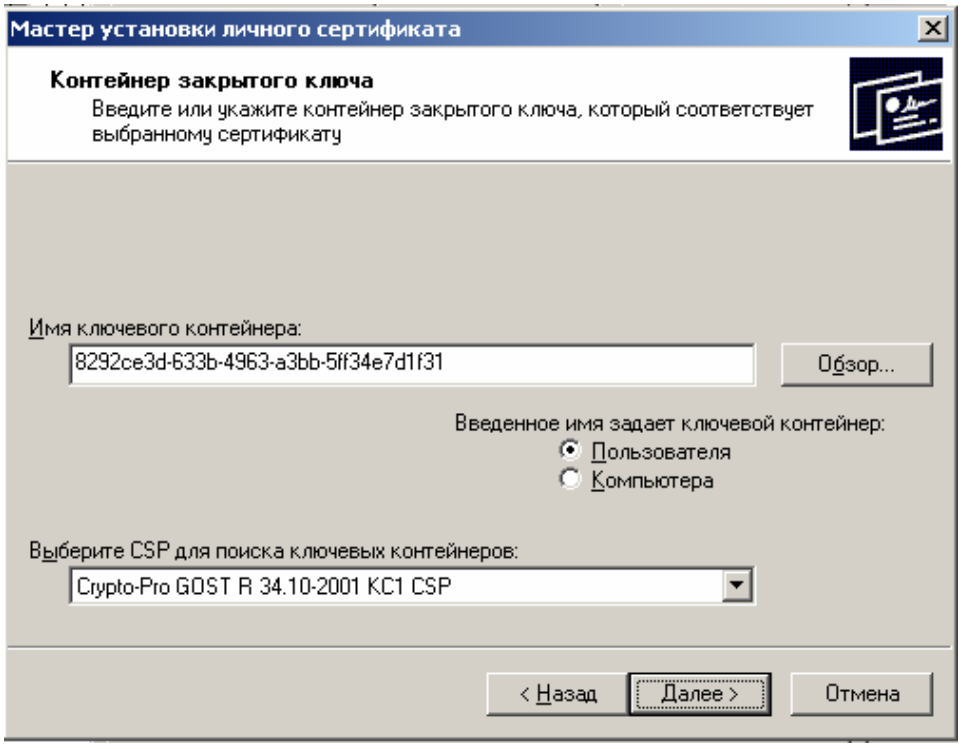


Рис. 54. Окно «Контейнер закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор**;
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер;

- **Выберите CSP для поиска ключевых контейнеров** - необходимый КриптоПровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Хранилище сертификатов» (см. Рис. 55).

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 закрытого ключа (см. предыдущий пункт)

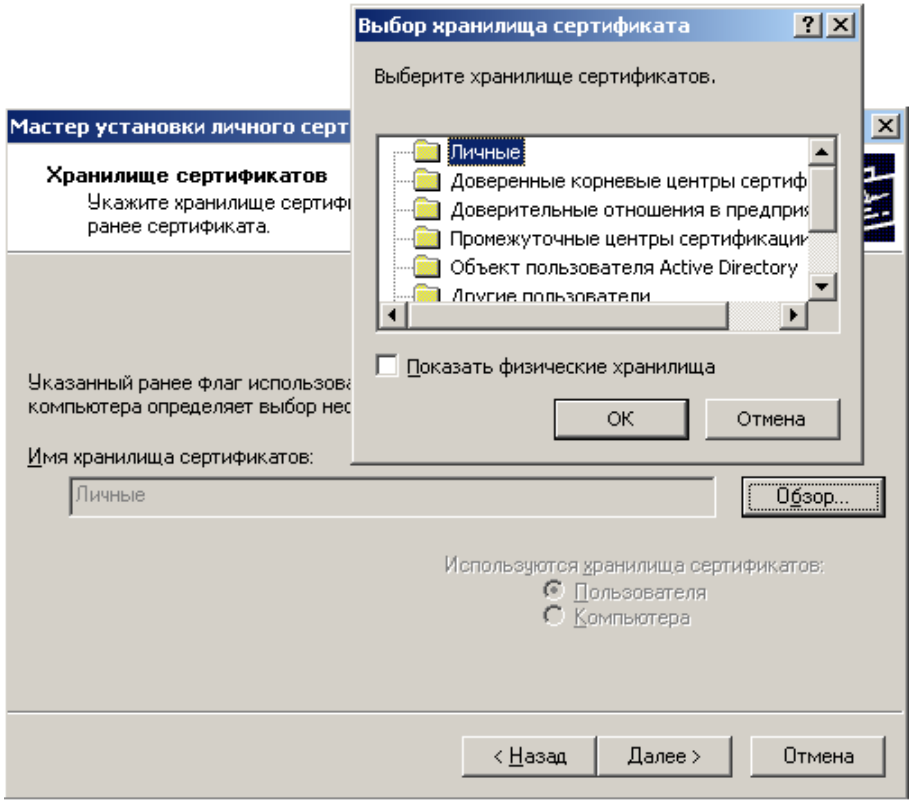


Рис. 55. Окно «Хранилище сертификатов»

После выбора хранилища система отобразит окно «Завершение работы мастера установки личного сертификата» (см. Рис. 56).

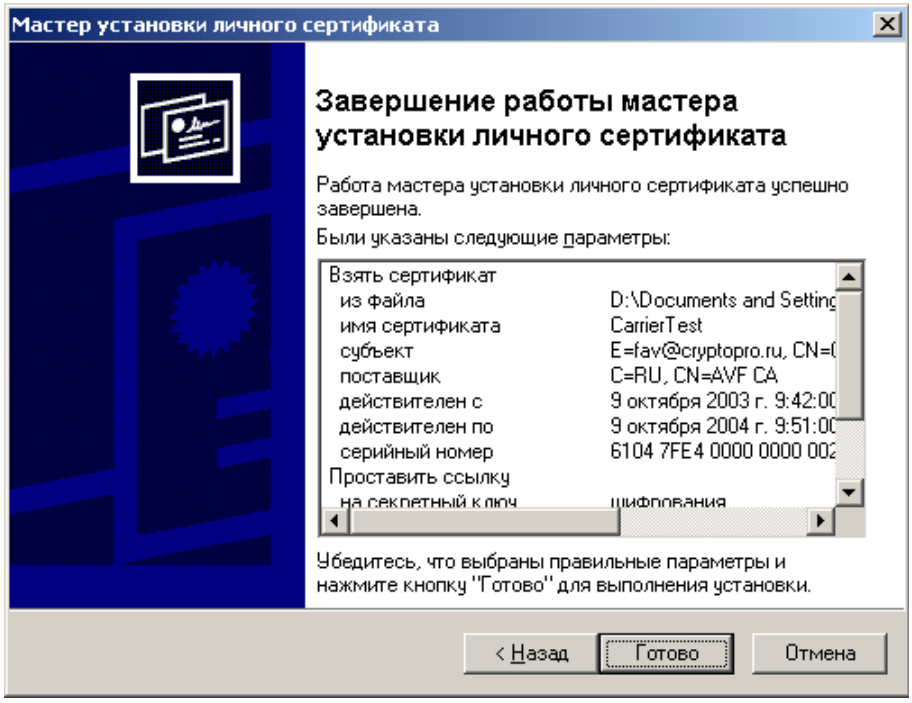


Рис. 56. Завершение работы мастера установки личного сертификата

Проверьте правильность указанных данных и нажмите кнопку **Готово.** СКЗИ «КриптоПро CSP» произведет установку сертификата.

2.4.4. Управление паролями доступа к закрытым ключам

2.4.4.1. Изменение пароля на доступ к закрытому ключу

Для того чтобы изменить пароль, в меню выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Сервис.** В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Изменить пароль**.

Система отобразит окно «Контейнер закрытого ключа» (см. Рис. 57).

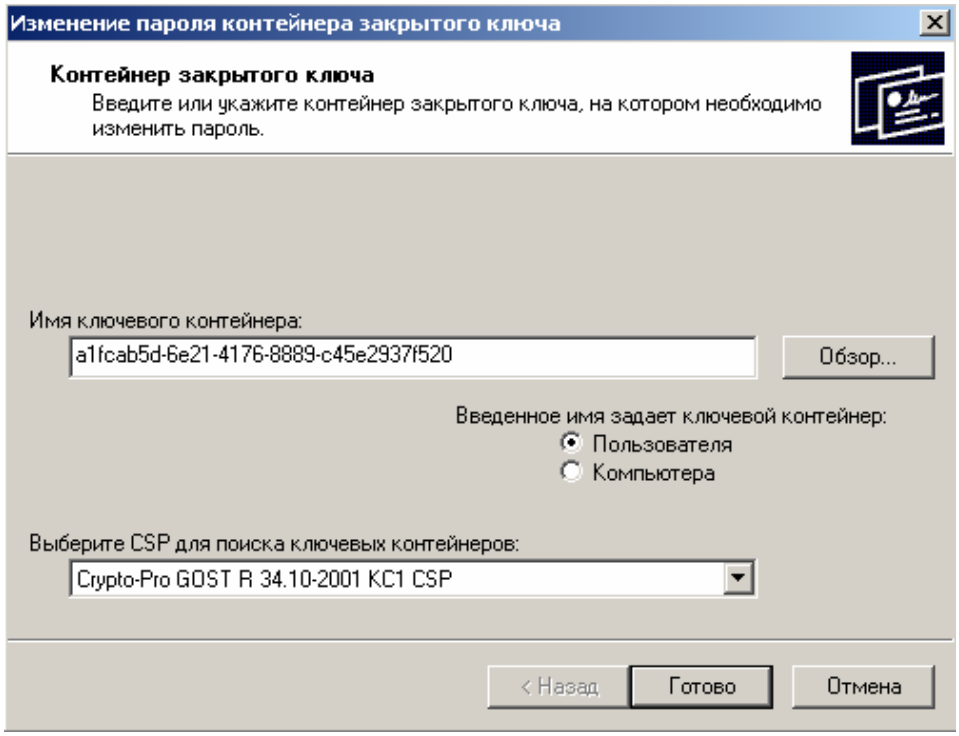


Рис. 57. Окно «Контейнер закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор**;
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище расположен контейнер;
- **Выберите CSP для поиска ключевых контейнеров** - необходимый КриптоПровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку **Готово**.

Система отобразит окно ввода пароля на доступ к закрытому ключу выбранного контейнера (см. Рис. 58). Введите указанный пароль и нажмите кнопку **ОК.**

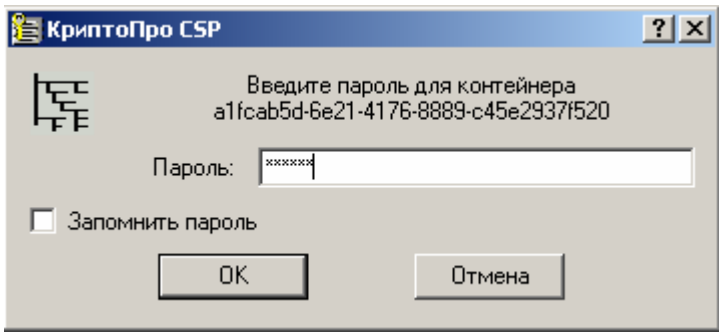


Рис. 58. Ввод пароля на доступ

Если пароль введен верно, то система отобразит окно ввода нового пароля на доступ к закрытому ключу (см. Рис. 59). Введите дважды новый пароль и нажмите кнопку **ОК.**

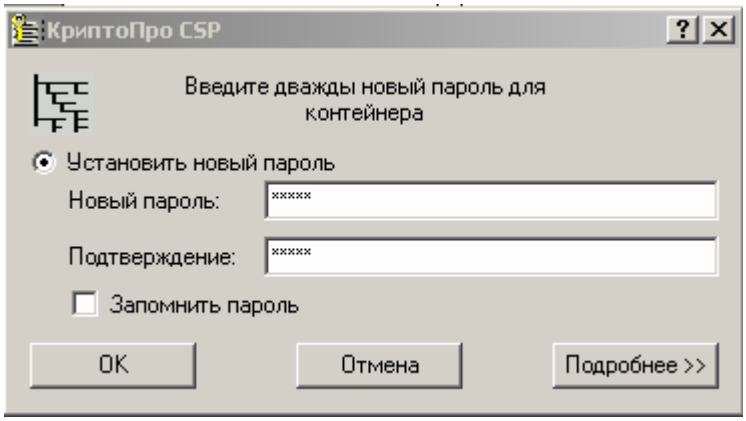


Рис. 59. Ввод нового пароля

После ввода пароля СКЗИ «КриптоПро CSP» осуществит смену пароля на доступ к закрытому ключу.

Примечание. Вместо установки пароля на доступ к закрытому ключу СКЗИ «КриптоПро CSP» позволяет зашифровать данный закрытый ключ на другом закрытом ключе, а также разделить закрытый ключ на несколько ключевых носителей. Осуществление данных операций подробно описано в пункте 3.1.4.

2.4.4.2. Удаление запомненных паролей

СКЗИ «КриптоПро CSP» позволяет сохранить в специальном хранилище локального компьютера пароли на доступ к контейнеру закрытого ключа (сохранение осуществляется установкой флага **Запомнить пароль в окне ввода пароля на доступ к закрытому ключу**). Если пароль сохранен в данном хранилище, то при обращении к закрытому ключу пароль автоматически будет

считан из контейнера без появления окна для ввода пароля. В этом же хранилище сохраняется точное нахождение ключевого контейнера (связка между именем контейнера и уникальным именем контейнера).

Для того чтобы удалить запомненный пароль в меню выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Сервис**. В панели настройки СКЗИ КриптоПро CSP (см. Рис. 35) нажмите кнопку **Удалить запомненные пароли.**

Система отобразит окно «Удаление запомненных паролей» (см. Рис. 60).

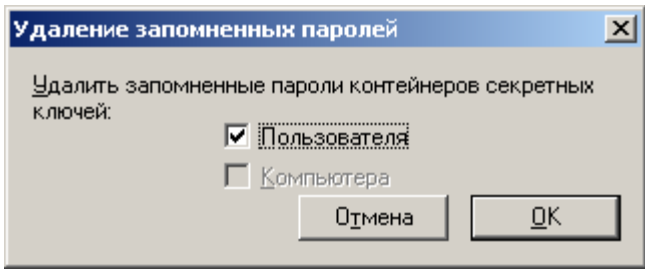


Рис. 60. Окно «Удаление запомненных паролей»

В этом окне установите флаги **Пользователя/Компьютера** для удаления сохраненных на локальном компьютере в специальном хранилище паролей и нажмите кнопку **ОК**. Если сохраненных паролей нет, то соответствующая область будет затемнена.

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

2.5. Установка параметров безопасности

Закладка **Безопасность** контрольной панели СКЗИ КриптоПро CSP предназначена для выбора параметров безопасности при работе с СКЗИ «КриптоПро CSP».

Для того чтобы установить параметры безопасности в меню выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Безопасность** (см. Рис. 61).

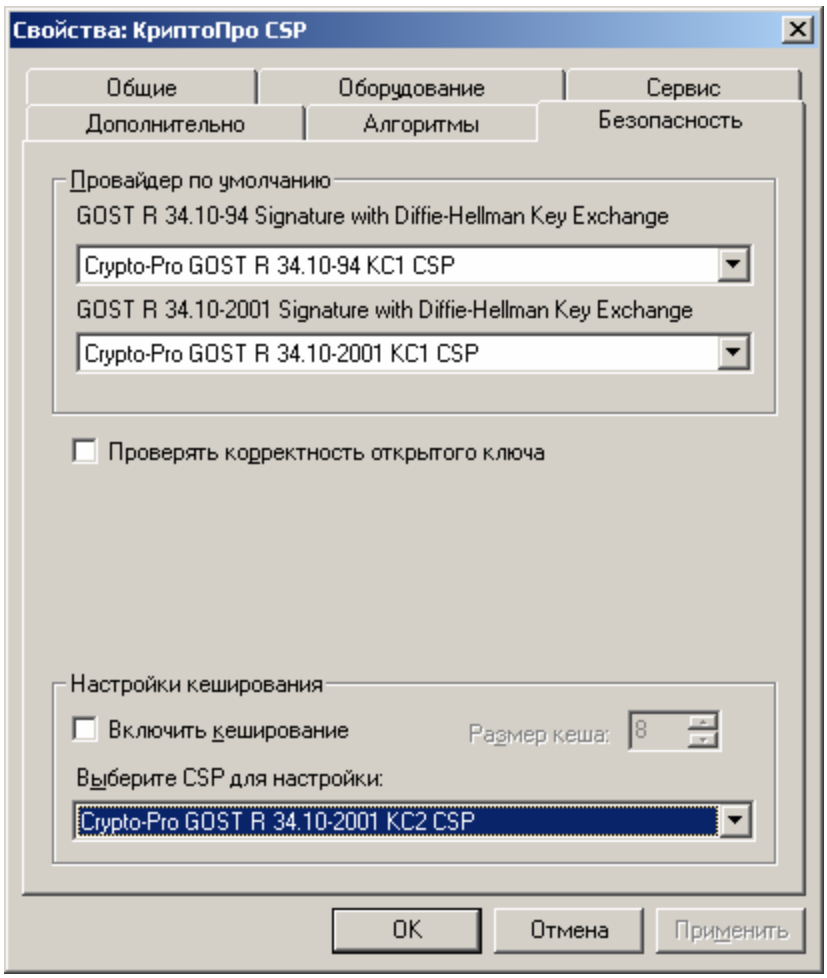


Рис. 61. Контрольная панель. Закладка «Безопасность»

СКЗИ «КриптоПро CSP» позволяет осуществлять проверку корректности устанавливаемого в контейнер открытого ключа (т.е. его соответствие государственному стандарту). Для того чтобы включить данную проверку, необходимо установить галочку в поле **Проверять корректность открытого ключа**.

СКЗИ «КриптоПро CSP» позволяет также осуществлять выбор провайдера по умолчанию для соответствующих типов провайдера.

Для типа GOST R 34.10-94 Signature with Diffie-Hellman Key Exchange:

- Не установлен;
- Crypto-Pro GOST R 34.10-94 KC1 CSP;
- Crypto-Pro GOST R 34.10-94 KC2 CSP.

Для типа GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange:

- Не установлен;
- Crypto-Pro GOST R 34.10-2001 KC1 CSP;
- Crypto-Pro GOST R 34.10-2001 KC2 CSP.

Список провайдеров может отличаться в зависимости от исполнения и установки (установка провайдеров для совместимости с предыдущими версиями).

Если СКЗИ «КриптоПро CSP» сертифицирован по уровню КС2, то возможно применение кэширования контейнеров закрытых ключей. Кэширование заключается в том, что считанные с носителя ключи остаются в памяти сервиса.

Ключи из кэша доступны любому приложению до завершения работы системы. Помимо этого ключ из кэша является доступным и после того, как он извлечен из считывателя, и даже после завершения работы загрузившего этот ключ приложения.

Кэширование контейнеров позволяет увеличить производительность приложений за счет более быстрого доступа к закрытому ключу, т.к. считывание ключа осуществляется только один раз.

Размер кэша задает количество ключей, которые одновременно могут храниться в памяти.

Для того чтобы включить кэширование, необходимо установить галочку в поле **Включить кэширование**. Необходимо также задать размер кэша в соответствующем поле ввода.



Примечание. Если на доступ к закрытому ключу установлен пароль, пароль не сохранен на локальном компьютере, закрытый ключ находится в кэше (ранее к нему уже был осуществлен доступ), то обращение к данному закрытому ключу произойдет без появления окна ввода пароля пользователя – ключ автоматически считывается из кеша.

СКЗИ «КриптоПро CSP» осуществляет кэширование закрытых ключей, связанных с сертификатами, установленными в хранилище сертификатов Локального компьютера (например, закрытых ключей Центра сертификации, Web-сервера) только для конкретного пользователя.

2.6. Дополнительные настройки

Закладка **Дополнительно** контрольной панели СКЗИ КриптоПро CSP предназначена для:

- просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов;
- установки времени ожидания ввода информации от пользователя.

2.6.1. Просмотр версий используемых файлов

Для просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов в меню выполните **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Дополнительно** (см. Рис. 62).

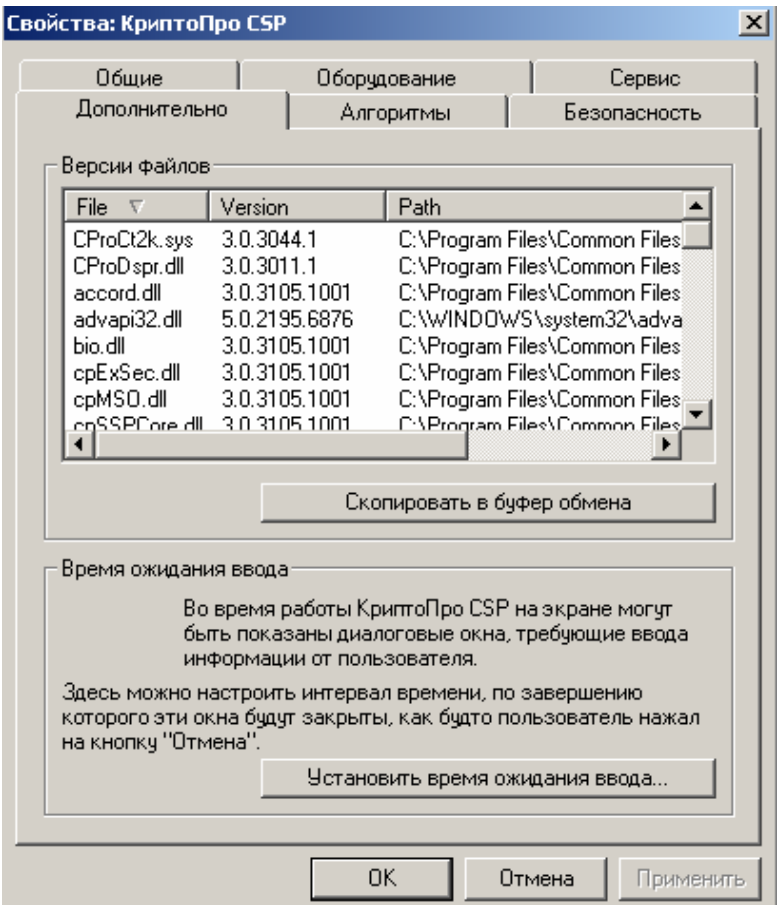


Рис. 62. Контрольная панель. Закладка «Дополнительно»

В области **Версии файлов** в табличной форме представлена информация о версиях и путях размещения использующихся СКЗИ «КриптоПро CSP» файлов.

Нажатие на кнопку **Скопировать в буфер обмена** приведет к сохранению данной информации в буфер обмена.

2.6.2. 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 закрытому ключу).

Для того чтобы установить интервал времени, по завершении которого эти окна будут автоматически закрыты (действие, эквивалентное нажатию пользователем кнопки **Отмена**), в меню выполните **Пуск ⇒ Настройка ⇒ Панель управления ⇒ КриптоПро CSP ⇒ Дополнительно** (см. Рис. 62).

В окне контрольной панели нажмите кнопку **Установить время ожидания ввода.**

Система отобразит окно «Интервал времени ожидания ввода» (см. Рис. 63). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

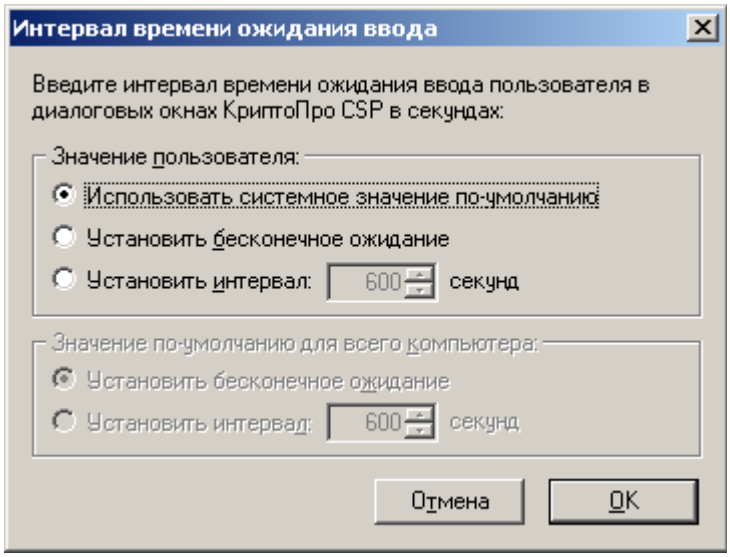


Рис. 63. Окно «Интервал времени ожидания ввода»

В этом окне 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; это значение установлено по умолчанию;
- Установить бесконечное ожидание – устанавливает бесконечное ожидание ввода данных пользователя;
- Установить интервал – определяет интервал времени, во время которого пользователь должен ввести данные.

Изменить переключатель **Значение по умолчанию для всего компьютера** может только пользователь, являющийся администратором локального компьютера (см. Рис. 64). По умолчанию установлено бесконечное ожидание ввода.

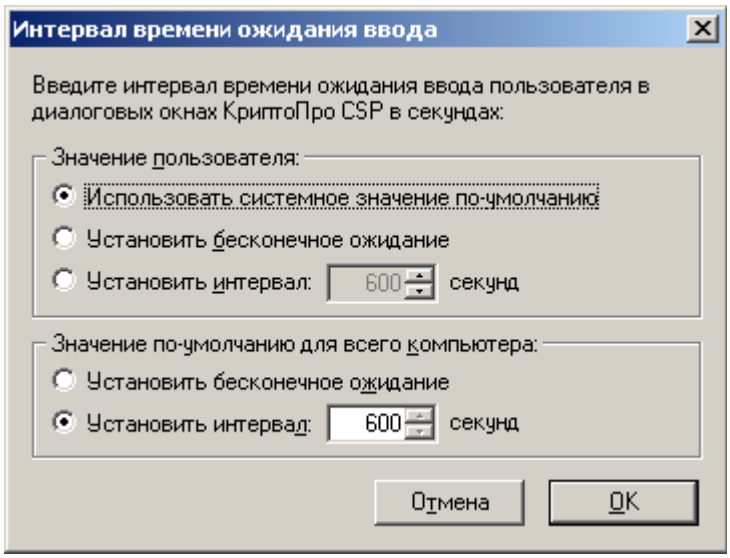


Рис. 64. Окно «Интервал времени ожидания ввода» для администратора компьютера

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).

2.7. Установка параметров криптографических алгоритмов

Закладка **Алгоритмы** контрольной панели СКЗИ КриптоПро CSP предназначена для установки различных параметров реализованных криптографических алгоритмов.

Для установки параметров криптографических алгоритмов необходимо в меню выполнить **Пуск** ⇒ **Настройка** ⇒ **Панель управления** ⇒ **КриптоПро CSP** ⇒ **Алгоритмы** (см. Рис. 65):

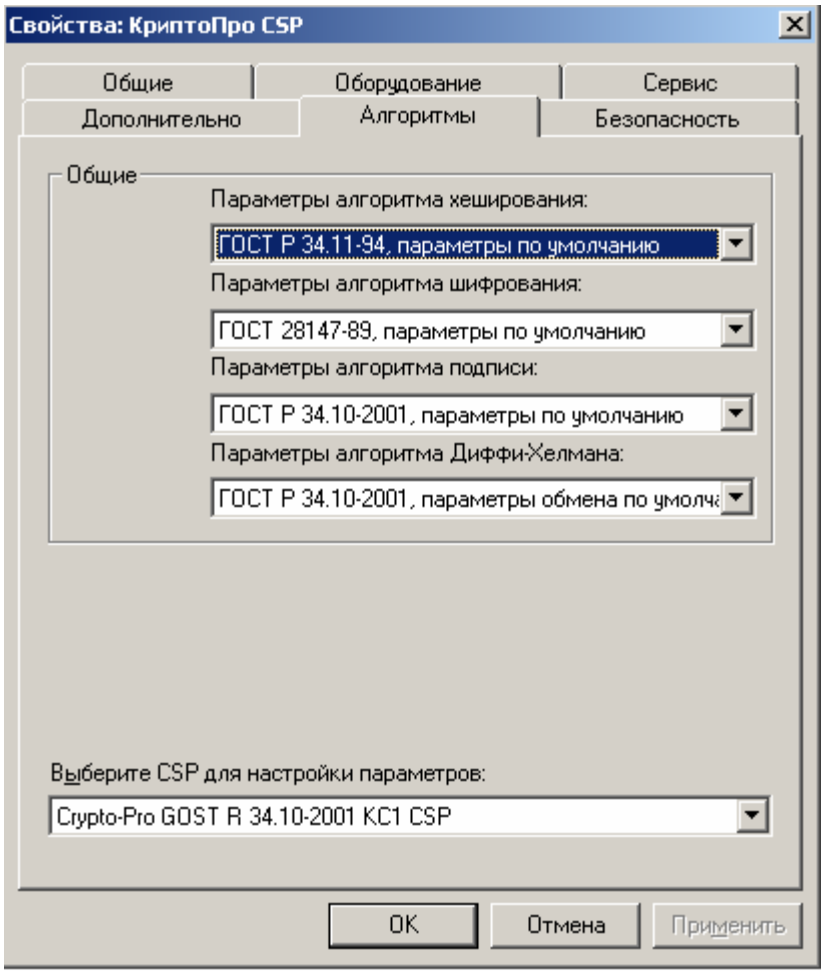


Рис. 65. Контрольная панель. Закладка «Алгоритмы»

Закладка **Алгоритмы** содержит две области, в каждой из которых для соответствующих криптографических алгоритмов реализована возможность установки параметров:

в области **Общие**

- осуществляется установка параметров алгоритма хеширования – ГОСТ Р 34.11-94 (параметры по умолчанию);
- осуществляется установка параметров алгоритма шифрования – ГОСТ 28147-89 (параметры по умолчанию, параметры Оскар 1.0, параметры Оскар 1.0,

параметры РИК1, параметры шифрования 1, параметры шифрования 2, параметры шифрования 3).

- установка параметров алгоритма выработки и проверки электронной цифровой подписи:
    - для Crypto-Pro GOST R 34.10-2001 - ГОСТ Р 34.10-2001 (параметры по умолчанию, параметры Оскар 2.x, параметры подписи 1);
    - для Crypto-Pro GOST R 34.10-94 - ГОСТ Р 34.10-94 (параметры по умолчанию, параметры подписи 1, параметры подписи 2, параметры подписи 3)
- установка параметров алгоритма Диффи-Хеллмана:
    - для Crypto-Pro GOST R 34.10-2001 - ГОСТ Р 34.10-2001 (параметры обмена по умолчанию, параметры обмена 1);
    - для Crypto-Pro GOST R 34.10-94 - ГОСТ Р 34.10-94 (параметры по умолчанию, параметры обмена 1, параметры обмена 2, параметры обмена 3).

В области **Выберите CSP для настройки параметров**.

3. Интерфейс генерации ключей

3.1. Создание ключевого контейнера

3.1.1. Выбор ключевого носителя

При создании ключевого контейнера система отобразит окно выбора ключевого носителя (Рис. 66).

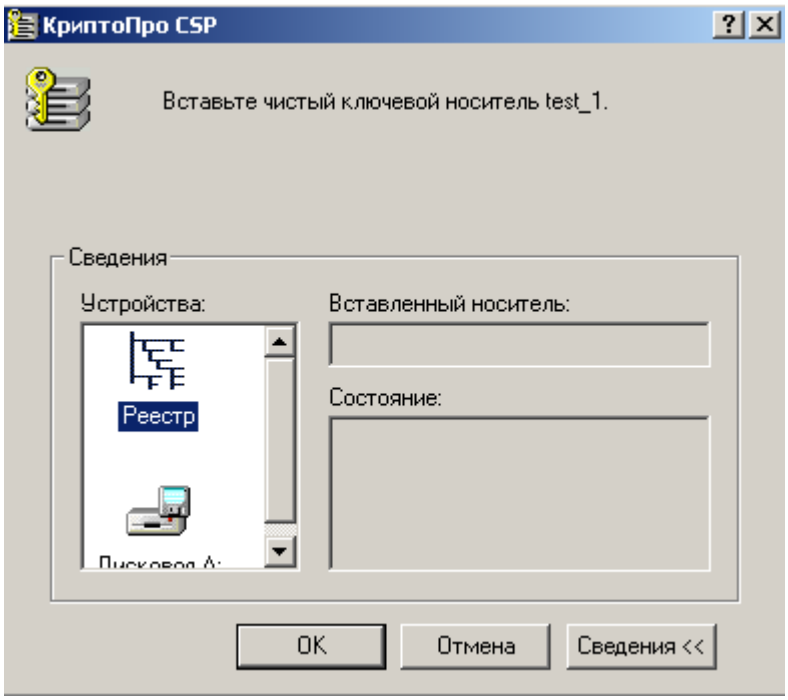


Рис. 66. Выбор ключевого носителя

Это окно отображается в том случае, когда пользователь имеет несколько устройств, служащих ключевыми считывателями. В случае, когда ключевой считыватель только один, он выбирается автоматически, и это окно не отображается.

После того, как ключевой считыватель выбран, нажмите кнопку **OK**.

3.1.2. Генерация начальной последовательности ДСЧ

После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, система отобразит окно «Биологический датчик случайных чисел» (см. Рис. 67).

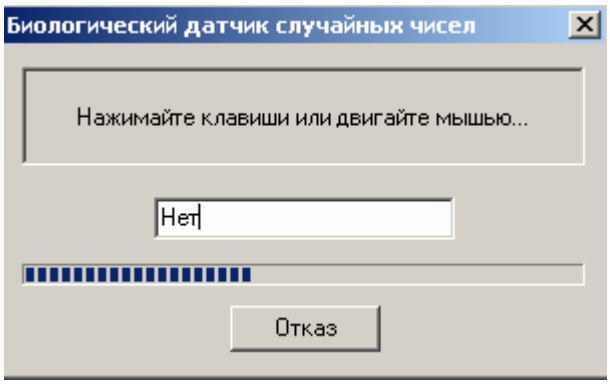


Рис. 67. Биологический датчик случайных чисел

Биологический датчик случайных чисел предназначен для генерации начальной последовательности датчика случайных чисел.

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.1.3. Ввод пароля на доступ к закрытому ключу

После завершения работы биологического датчика случайных чисел система отобразит окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рис. 68).

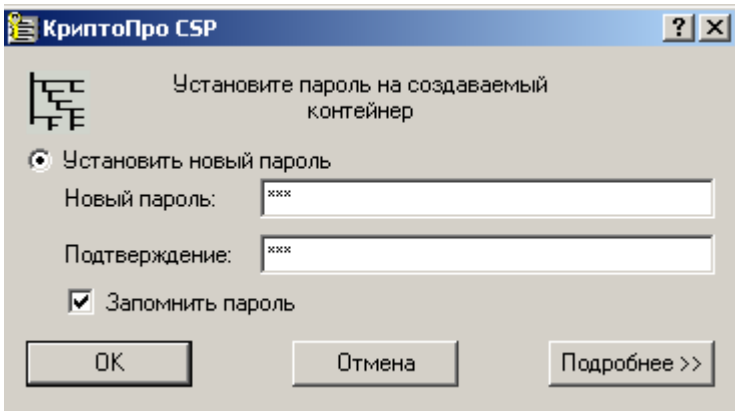


Рис. 68. Ввод пароля на доступ к закрытому ключу

В этом окне существует возможность ввода текстового пароля на доступ к закрытому ключу создаваемого контейнера (один и тот же пароль необходимо ввести в поля **Новый пароль** и **Подтверждение**). При установке галочки напротив поля **Запомнить пароль,** он будет сохранен в реестре.

После ввода пароля нажмите кнопку **ОК**.

Если ключ генерируется на носитель, поддерживающий аппаратный пароль или пин-код, то необходимо ввести тот пароль (пин-код), который установлен на этот ключевой носитель.

3.1.4. Выбор способа защиты доступа к закрытому ключу

Помимо ввода пароля в СКЗИ «КриптоПро CSP» существуют другие средства защиты доступа к закрытому ключу. Для выбора подходящего средства защиты в окне ввода пароля на доступ к закрытому ключу создаваемого контейнер (см. Рис. 68) нажмите кнопку **Подробнее**. Система отобразит окно выбора способа защиты доступа к закрытому ключу создаваемого контейнера (см. Рис. 69). Защита носителей поддерживающих аппаратный пароль (пин-код) возможна только на этом пароле (пин-коде).

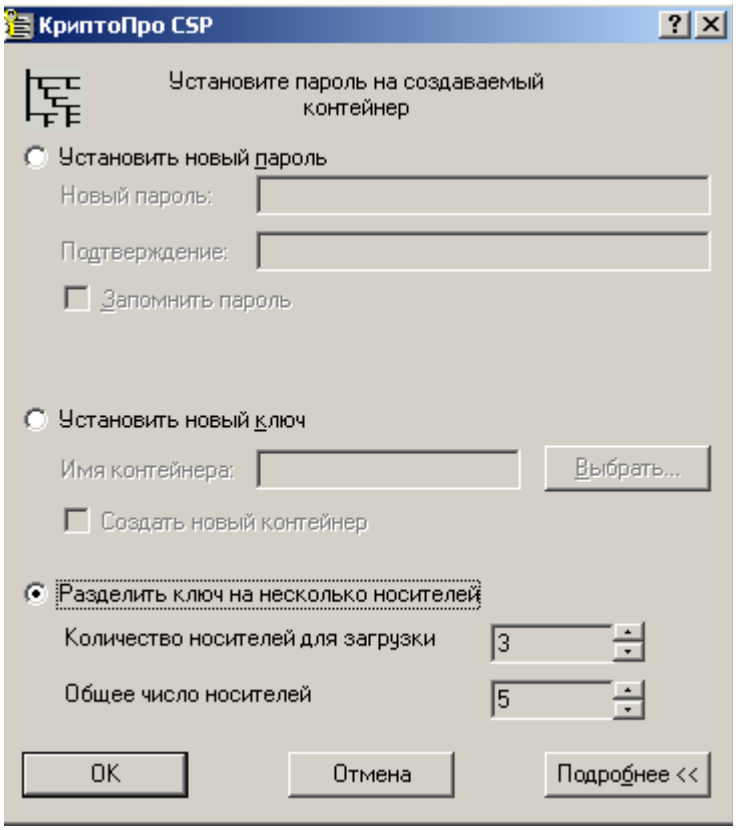


Рис. 69. Выбор средства защиты доступа к закрытому ключу

В этом окне содержатся следующие поля:

- **Установить новый пароль** – ввод текстового пароля;
- **Установить новый ключ** – зашифрование данного закрытого ключа на другом закрытом ключе;
- **Разделить ключ на несколько носителей** – разделение данного закрытого ключа на несколько носителей для обеспечения доступа к нему.

Для возврата из окна выбора способа защиты доступа к закрытому ключу (см. Рис. 69) к окну ввода пароля на доступ (см. Рис. 68) повторно нажмите кнопку **Подробнее**.

3.1.4.1. Установка нового пароля

Если переключатель установлен в поле **Установить новый пароль** (см. Рис. 69), то СКЗИ «КриптоПро CSP» осуществит защиту ключа при помощи пароля на доступ, введенного с клавиатуры. Необходимо осуществить действия, описанные в пункте 3.1.3.

3.1.4.2. Установка нового ключа

Если переключатель установлен в поле **Установить новый ключ** (см. Рис. 69), то СКЗИ «КриптоПро CSP» осуществит защиту ключа при помощи зашифрования данного закрытого ключа на другом закрытом ключе.

Для этого необходимо ввести имя контейнера (или выбрать контейнер из списка с помощью кнопки **Выбрать**), содержащего закрытый ключ, на котором будет осуществлено зашифрование исходного закрытого ключа. При нажатии кнопки **Выбрать** система отобразит список существующих контейнеров (см. Рис. 70).

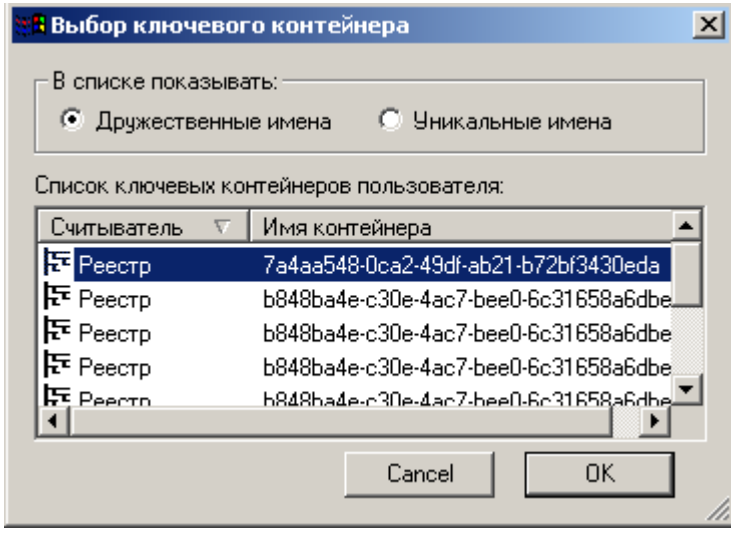


Рис. 70. Список существующих контейнеров

После выбора необходимого контейнера нажмите кнопку **ОК**. При этом произойдет зашифрование данного закрытого ключа на ключе выбранного контейнера.

СКЗИ «КриптоПро CSP» позволяет осуществлять зашифрование данного ключа не только на существующем закрытом ключе. При установке галочки напротив поля **Создать новый контейнер** (см. Рис. 69) система аналогично создаст новый контейнер и на его ключе осуществит зашифрование закрытого ключа данного контейнера.

3.1.4.3. Разделение ключа на несколько носителей

Если переключатель установлен в поле **Разделить ключ на несколько носителей** (см. Рис. 69), то СКЗИ «КриптоПро CSP» осуществит защиту ключа при помощи разделения доступа к нему между несколькими ключевыми носителями. Каждый из этих носителей является самостоятельным контейнером с собственным паролем на доступ к закрытому ключу.

Необходимо заполнить следующие поля:

- **Количество носителей для загрузки** – число носителей, необходимых для доступа к закрытому ключу.
- **Общее количество носителей** – общее количество носителей, между которыми ключ будет разделен.

После заполнения этих полей система перейдет к процессу создания новых контейнеров, участвующих в разделении исходного ключа. Количество создаваемых контейнеров равно значению, указанному в поле **Общее количество носителей:**

1. Для каждого создаваемого контейнера система отобразит окно выбора ключевого носителя (см. Рис. 66). В этом окне необходимо выбрать носитель, который будет участвовать в разделении ключа.
2. После того, как для всех контейнеров выбраны носители, система отобразит окно «Биологический датчик случайных чисел» (см. Рис. 67), в котором произойдет генерация начальной последовательности датчика случайных чисел. Если установлен физический датчик случайных чисел, то генерация произведена будет им. В этом случае окно «Биологический датчик случайных чисел» отображаться не будет.
3. После завершения генерации система отобразит окно ввода пароля на доступ к закрытому ключу для каждого создаваемого контейнера (см. Рис. 68). В этом окне необходимо ввести пароль либо выбрать другое средство защиты доступа к закрытому ключу при помощи кнопки **Подробнее** (см. Рис. 69).

После того, как все контейнеры, участвующие в разделении ключа, будут созданы, произойдет процесс обеспечения защиты доступа к закрытому ключу.

3.2. Открытие ключевого контейнера

3.2.1. Отсутствие ключевого носителя

В случае отсутствия ключевого носителя при открытии ключевого контейнера система отобразит окно, сообщающее об отсутствии носителя (см. Рис. 71).

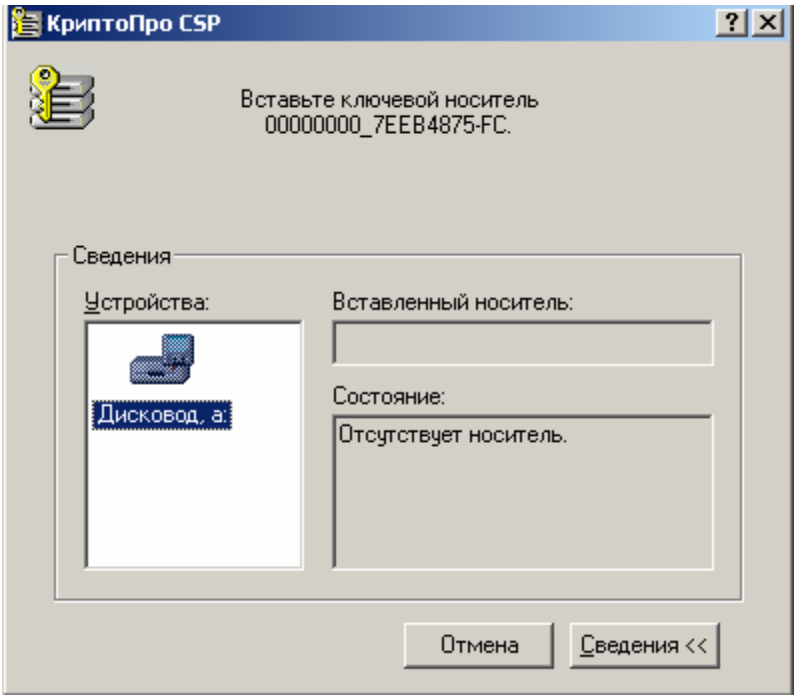


Рис. 71. Отсутствие необходимого носителя

После того, как носитель будет подключен, система перейдет к следующему окну (см. Рис. 72).

Если требуемый носитель установить не удается, нажмите кнопку **Отмена**. В этом случае процесс открытия контейнера прекратится.

В случае, когда необходимый ключевой носитель подключен, окно, сообщающее об отсутствии ключевого носителя, отображаться не будет.

3.2.2. Проверка пароля на доступ к закрытому ключу

После того, как необходимый носитель установлен, система потребует подтверждение пароля на доступ к закрытому ключу открываемого контейнера.

3.2.2.1. Проверка текстового пароля

Если защита доступа к закрытому ключу была осуществлена при помощи ввода текстового пароля (см. пункт 3.1.4.1), то будет отображено окно проверки пароля для доступа к закрытому ключу открываемого контейнера (см. Рис. 72).

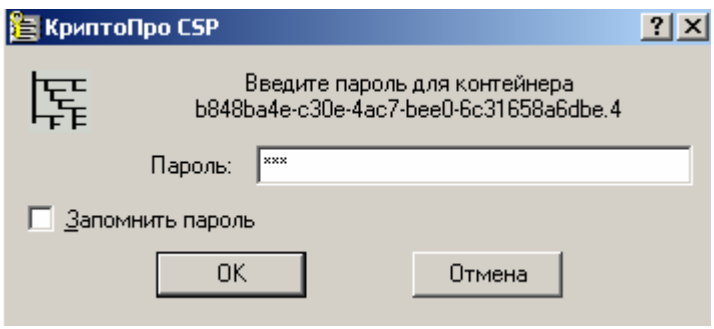


Рис. 72. Проверка пароля на доступ к закрытому ключу

Если при создании открываемого ключевого контейнера во время ввода пароля на доступ к закрытому ключу галочка напротив поля **Запомнить пароль** была установлена (см. пункт 3.1.3), то пароль был сохранен в реестре. Повторный ввод (проверка) этого пароля не требуется, поэтому окно проверки пароля отображено не будет.

Если пароль введен неверно, система попросит повторно ввести пароль.

После того, как пароль указан верно, система предложит ввести новый пароль на доступ к закрытому ключу этого контейнера (см. Рис. 73).

Примечание. Носители, имеющие аппаратный пин-код, могут иметь ограничение на количество неудачных попыток ввода пароля. Превышение этого предела приводит к блокированию носителя или контейнера.

3.2.2.2. Проверка пароля при зашифровании ключа на другом ключе

Если защита доступа к закрытому ключу была осуществлена при помощи зашифрования данного закрытого ключа на другом закрытом ключе (см. пункт 3.1.4.2), то будет отображено окно проверки пароля для доступа к закрытому ключу контейнера, на ключе которого проводилось зашифрование (см. Рис. 72).

После того, как был получен доступ к ключу расшифрования, произойдет расшифрование ключа открываемого контейнера. Система предложит ввести новый пароль на доступ к закрытому ключу этого контейнера (см. Рис. 73).

3.2.2.3. Проверка пароля при разделении ключа между несколькими носителями

Если защита доступа к закрытому ключу осуществлялась при помощи разделения ключа между носителями (см. пункт 3.1.4.3), то проверку требуется осуществить для такого количества носителей, какое было указано в поле **Количество носителей для загрузки** при создании контейнера. При нахождении одного из ключа система осуществит стандартную проверку пароля для ключа-части.

При открытии одного из носителей, участвующего в разделении ключа некоторого контейнера (а все они в свою очередь также являются носителями), проверка пароля на доступ к закрытому ключу проводится в соответствии со способом защиты доступа к ключу, примененным к данному носителю. В общем случае, для разных носителей, участвующих в разделении закрытого ключа одного и того же контейнера, могут быть применены разные способы защиты доступа к ключу.

3.2.3. Ввод нового пароля на доступ к закрытому ключу

Если при создании контейнера пароль сохранялся, то в окне ввода нового пароля по умолчанию напротив поля **Запомнить пароль** будет стоять галочка.

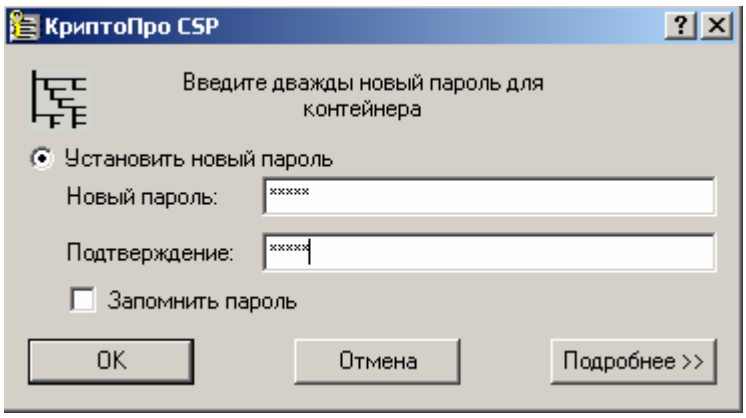


Рис. 73. Ввод нового пароля на доступ к закрытому ключу

В этом окне необходимо дважды ввести новый пароль либо при помощи нажатия кнопки **Подробнее** перейти к окну выбора способа защиты доступа к закрытому ключу (см. Рис. 69). Все действия по выбору способы защиты доступа описаны в пункте 3.1.4.

После выполненных действий нажмите кнопку **OK**.

Если смена пароля не требуется, нажмите кнопку **Отмена**.

3.3. Генерация ключей и получение сертификата при помощи УЦ

Для формирования личных ключей и получения сертификатов можно воспользоваться тестовым Центром Сертификации http://www.CryptoPro.ru/CertSrv.

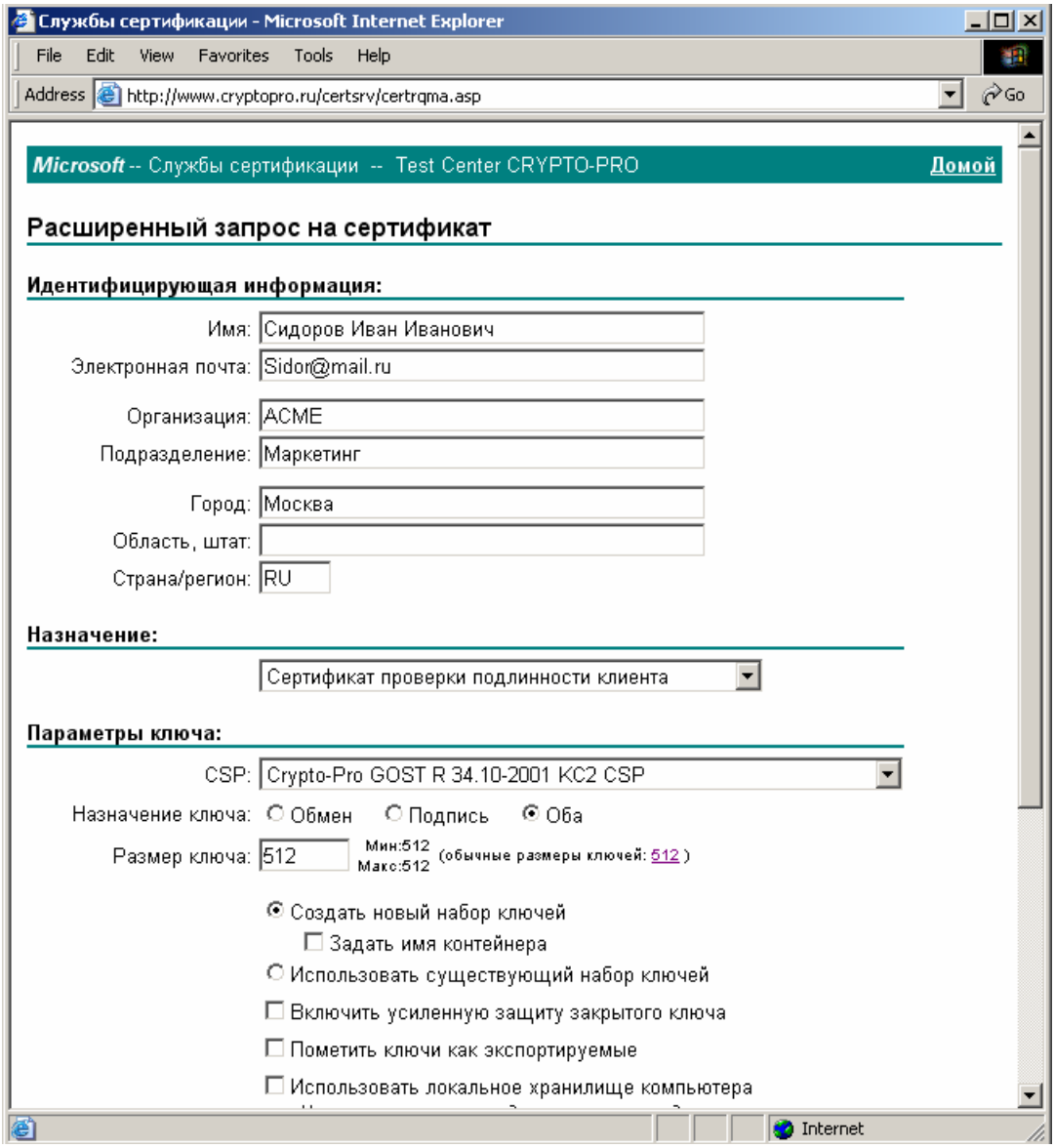


Рис. 74. Генерация ключа при помощи УЦ

В диалоге создания ключа и формирования запроса на сертификат задайте "Имя Владельца" сертификата и введите свой адрес электронной почты "Адрес E-Mail".

Если запрашиваемый сертификат предполагается использовать в электронной почте, выберите **Защищенная электронная почта** в разделе **Область применения ключа**.

Если запрашиваемый сертификат предполагается использовать в протоколе TLS, выберите **Сертификат аутентификации клиента** в разделе **Область применения ключа**.

Примечание. Если введенный адрес почты не совпадает с зарегистрированным адресом в Outlook Express (Outlook), использовать криптографические функции в электронной почте будет невозможно.

4. Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS

4.1. Размещение сертификата на сервере ISA

На компьютере с сервером ISA сертификат должен быть размещен в Local Computer certificate store. Для этого необходимо после установки сертификата через mmc консоль скопировать сертификат из хранилища учетной записи пользователя в хранилище учетной записи компьютера. Для этого необходимо:

Запустить консоль MMC

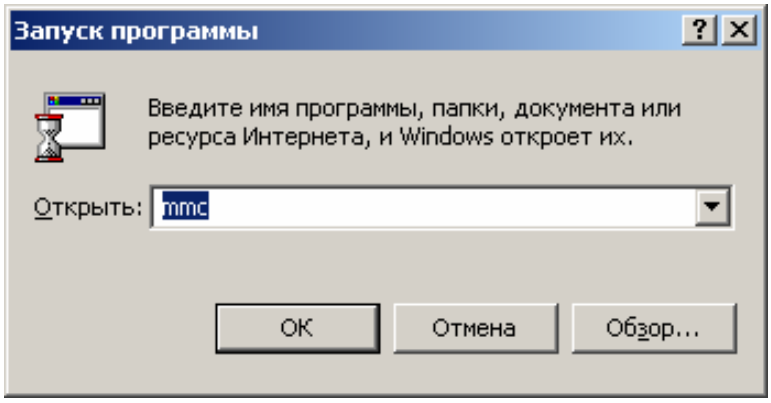


Рис. 75. Запуск консоли MMC

В корень консоли MMC установить две изолированные оснастки диспетчера сертификатов:

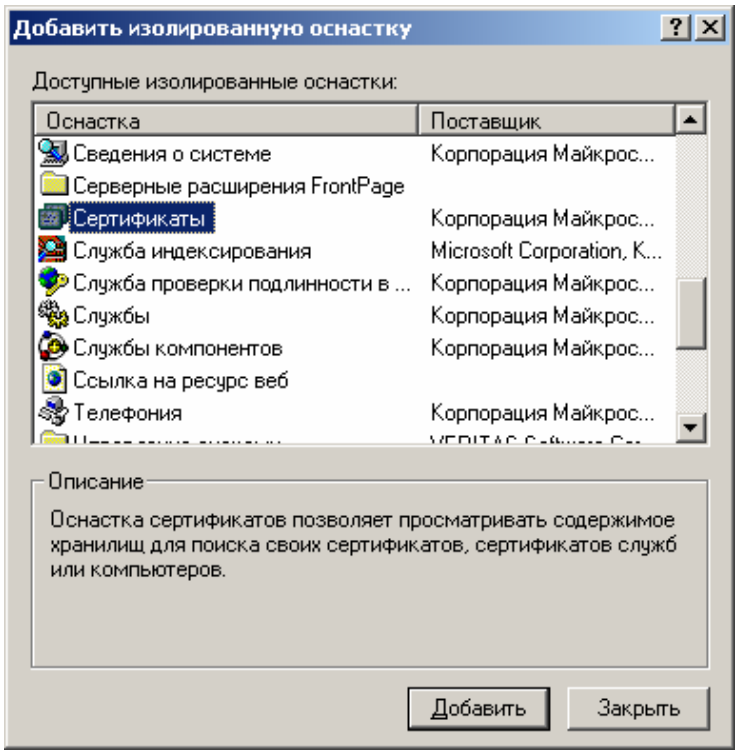


Рис. 76. Добавление изолированной оснастки

Установить одну оснастку для управления сертификатами учетной записи пользователя:

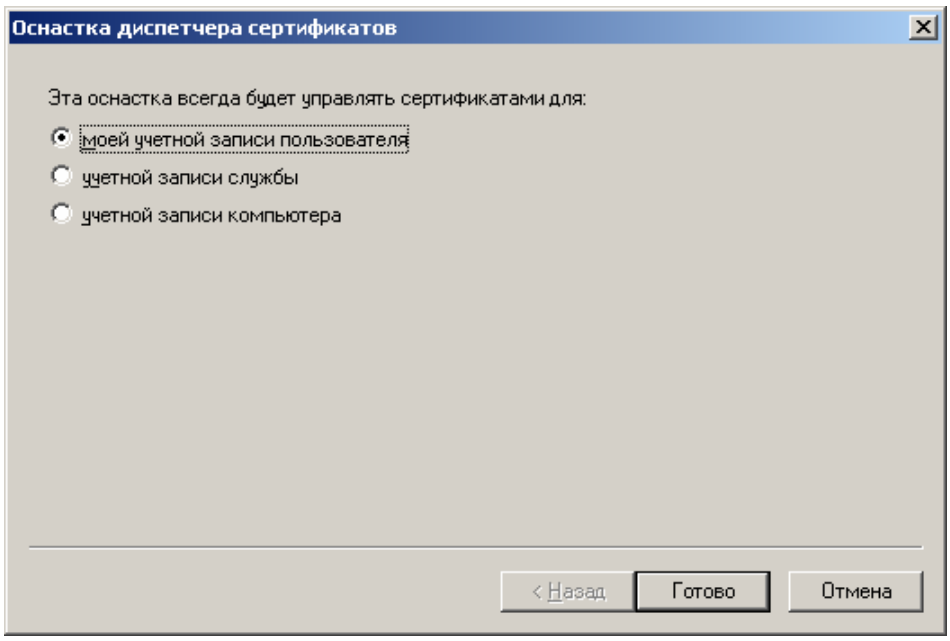


Рис. 77. Оснастка диспетчера сертификатов (1)

Установить вторую оснастку для управления учетной записи компьютера:

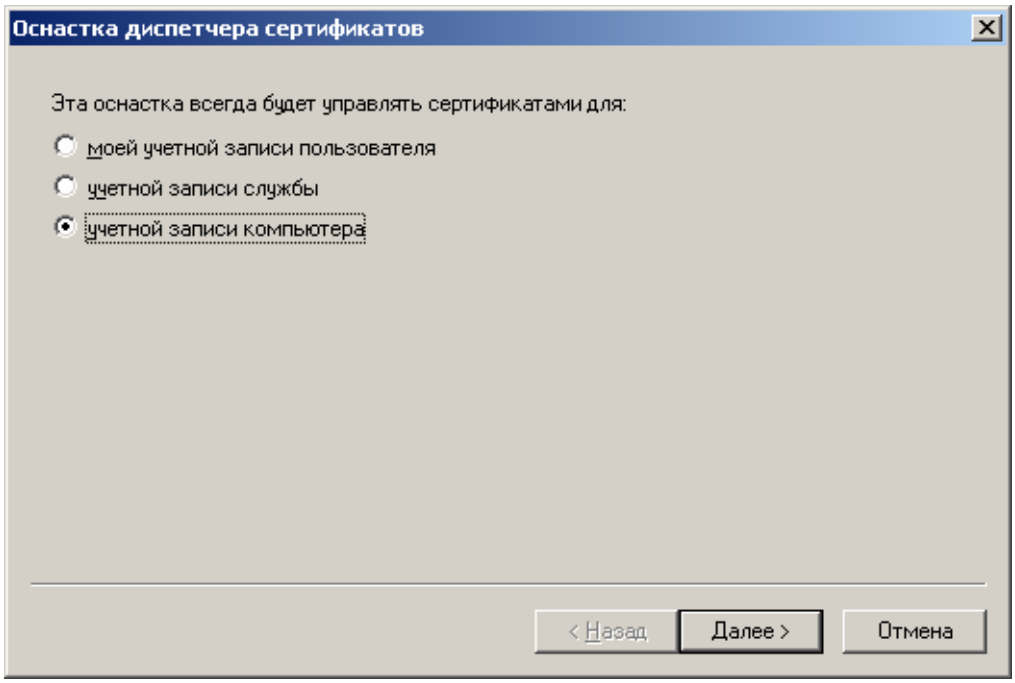


Рис. 78. Оснастка диспетчера сертификатов (2)

После выбора этих оснасток корень консоли должен выглядеть приблизительно:

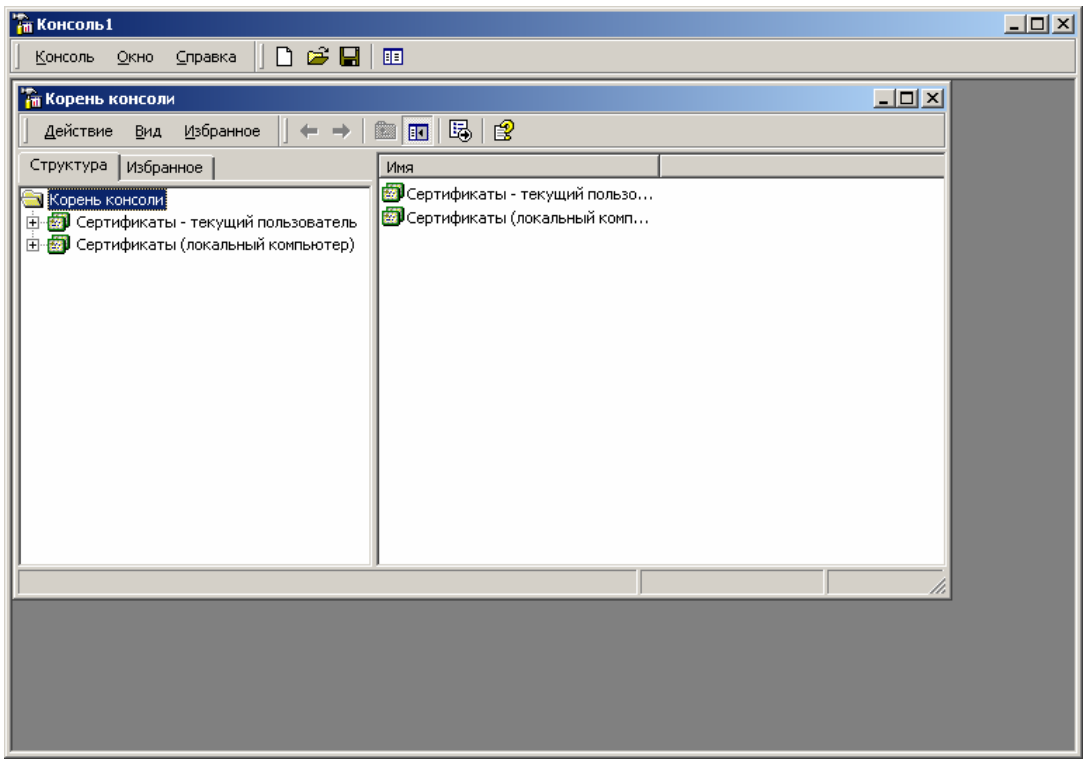


Рис. 79. Консоль MMC

Установите курсор на сертификат сервера ISA:

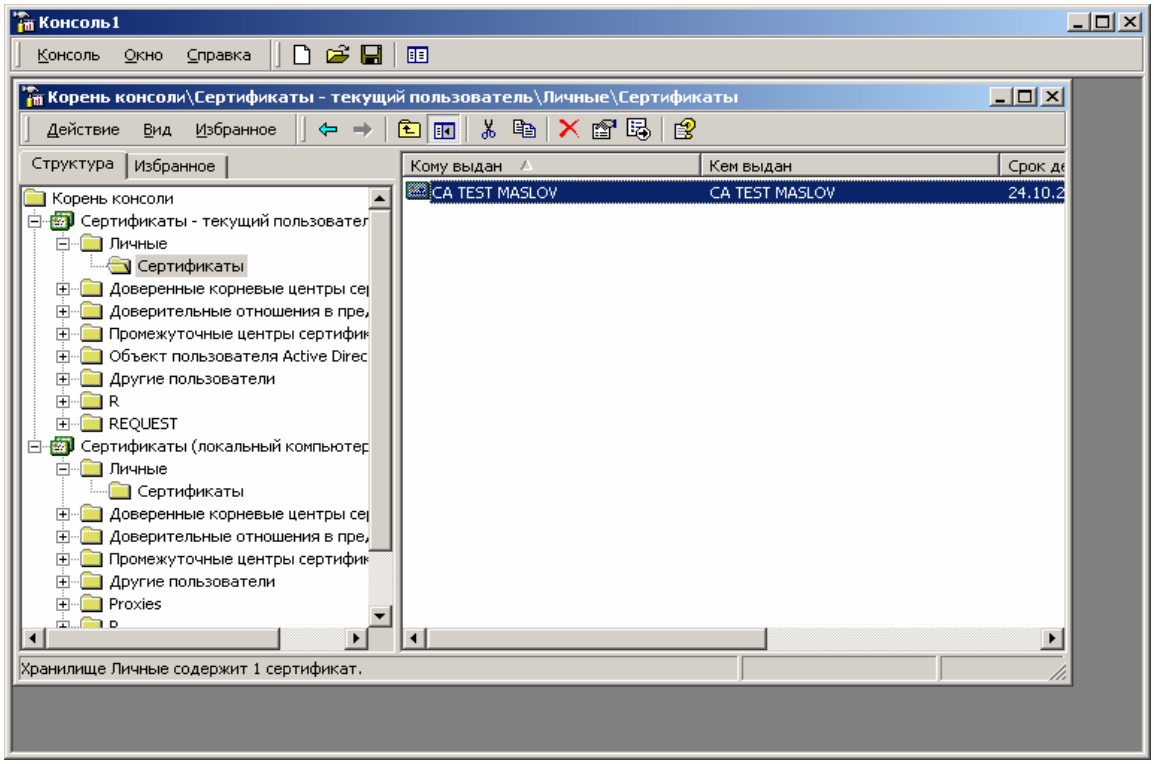


Рис. 80. Корень консоли MMC

С использованием функции Copy, занесите сертификат в буфер Clipboard

После этого установите курсор на разделе «личные» сертификатов локального компьютера и выполните функцию Paste

После установки сертификата серверной аутентификации ISA, таким же образом установите сертификат центра сертификации в раздел «Доверенные корневые центры сертификации» хранилища локального компьютера.

4.2. Настройка соединения с Web-клиентом

После установки сертификатов открытых ключей, необходимо установить и настроить Слушателя для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется на вкладке Incoming Web Requests окна свойств ISA сервера (рис. 69):

В окне ISA Management установить курсор на имя сервера и нажать правую кнопку мыши.

В появившемся меню выбрать пункт Properties.

В окне свойств сервера выбрать закладку Incoming Web Requests.

Выберите режим индивидуального Слушателя для каждого IP адреса в поле Identification.

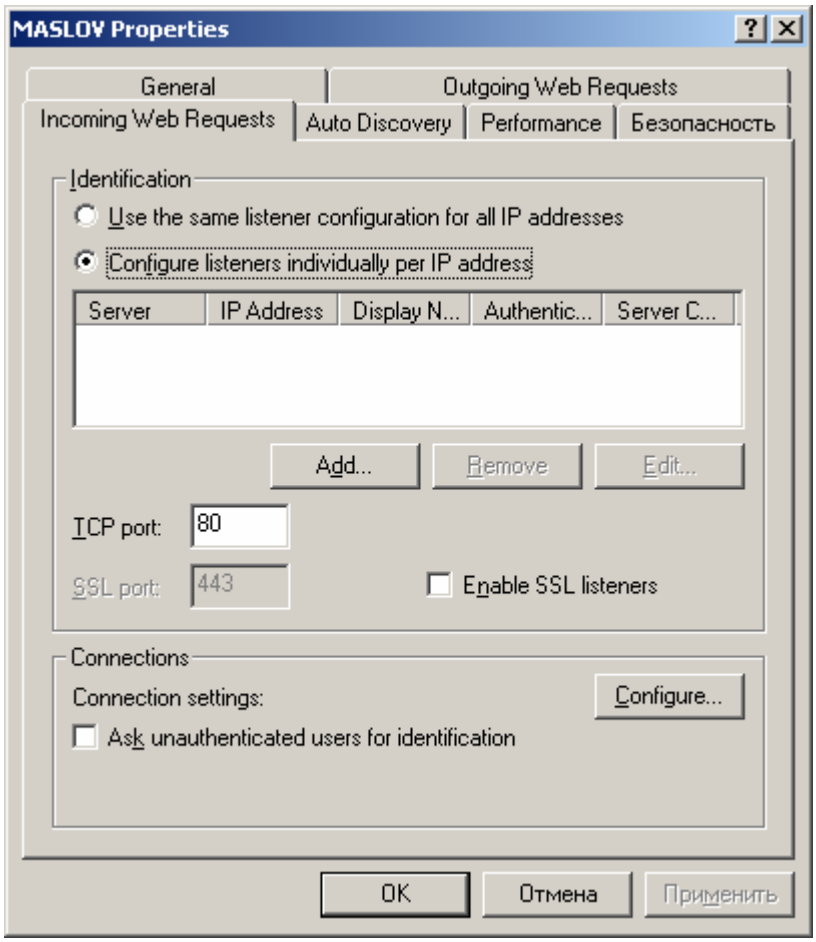


Рис. 81. Установка и настройка Слушателей

Добавьте нового Слушателя в список слушателей ISA сервера.

Установите имя сервера.

Установите внешний IP-адрес, на который будет настроен Слушатель.

Введите имя, с которым будет отображаться данный Слушатель в дальнейшем (опционально).

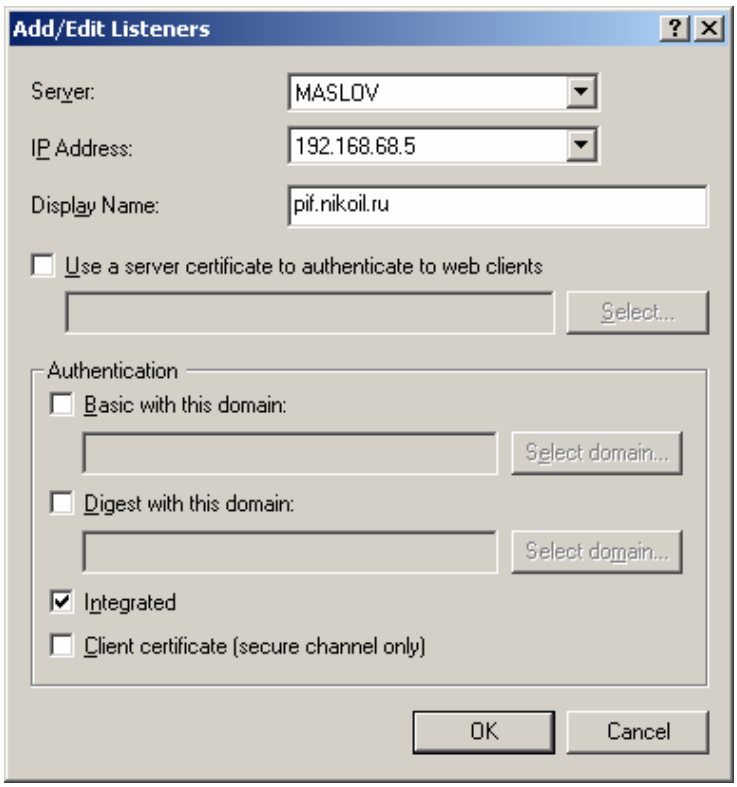


Рис. 82. Добавление Слушателя/редактирование свойств Слушателя(1)

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификации сервера ISA необходимо:

В окне добавления Слушателя или в окне редактировании свойств Слушателя, указать на использование сертификата сервера при аутентификации с Web-клиентом.

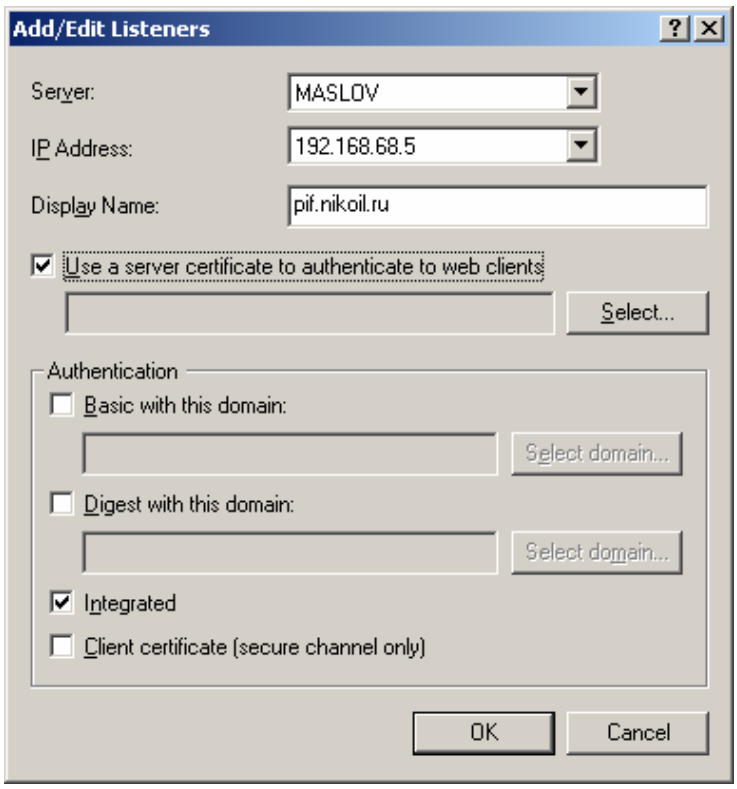


Рис. 83. Добавление Слушателя/редактирование свойств Слушателя(2)

Выбрать сертификат сервера, который будет использоваться для аутентификации.

Нажать кнопку Select.

В появившемся окне выбрать из списка сертификат открытого ключа сервера:

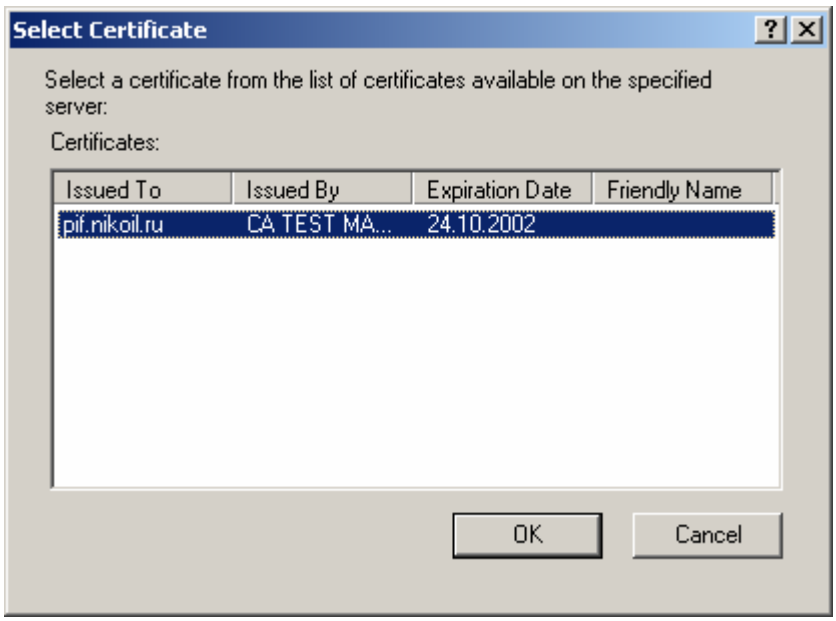


Рис. 84. Выбор сертификата открытого ключа сервера

Указать на использование сертификата клиента (опция Client certificate (secure channel only)).

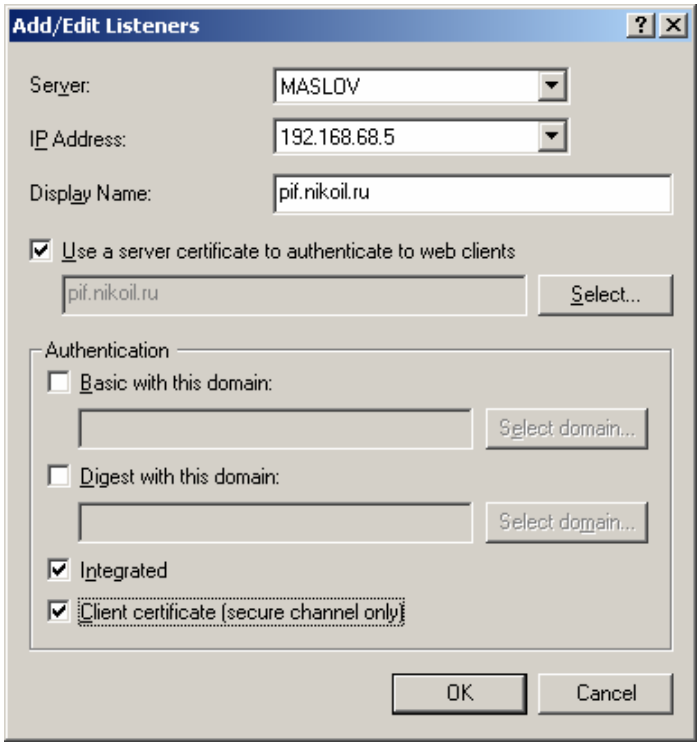


Рис. 85. Добавление Слушателя/редактирование свойств Слушателя(3)

4.3. Публикация Web-сервера в сети Интернет

В этом разделе рассматривается порядок действий при опубликовании Web-сервера, расположенного во внутренней сети. При этом соединение сервера ISA и Web-сервера будет установлено по протоколу SSL.

Для публикации Web-сервера во внешнюю сеть необходимо:

Получить и установить на публикуемый Web-сервер сертификат открытого ключа, который будет использоваться для серверной аутентификации.

Требования к сертификату:

Имя сертификата (Common name) должно совпадать с доменным именем Web-сервера, указываемого для редиректа поступающих запросов (закладка **Action** окна свойств правила Web публикации). Например: epif.big.nikoil.ru

область использования ключа должна содержать «Аутентификация Сервера»

Установить сертификат Web-сервера на сервере ISA, в хранилище локального компьютера (**Local Computer certificate stor**), раздел «Доверенные корневые центры сертификации»

Настроить Web-сервер для поддержки SSL соединения

Настройка Web-сервера производится в соответствии с документацией соответствующего Web-сервера.

Создать и настроить правила публикации на сервере ISA.

В окне **ISA Management** установить курсор на **Web Publishing Rules,** находящийся в группе **Publishing**

Нажать правую кнопку мыши и в появившемся меню выбрать последовательно **New** и **Rule**

В открывшемся окне, с помощью Мастера создания Правила Web публикации, создать правило.

Ввести имя публикации (произвольное имя) и нажать «Далее»



Рис. 86. Окно Мастера создания Правила Web

В окне **Destination Sets** оставить значение, предлагаемое по умолчанию (любые назначения) и нажать «Далее».

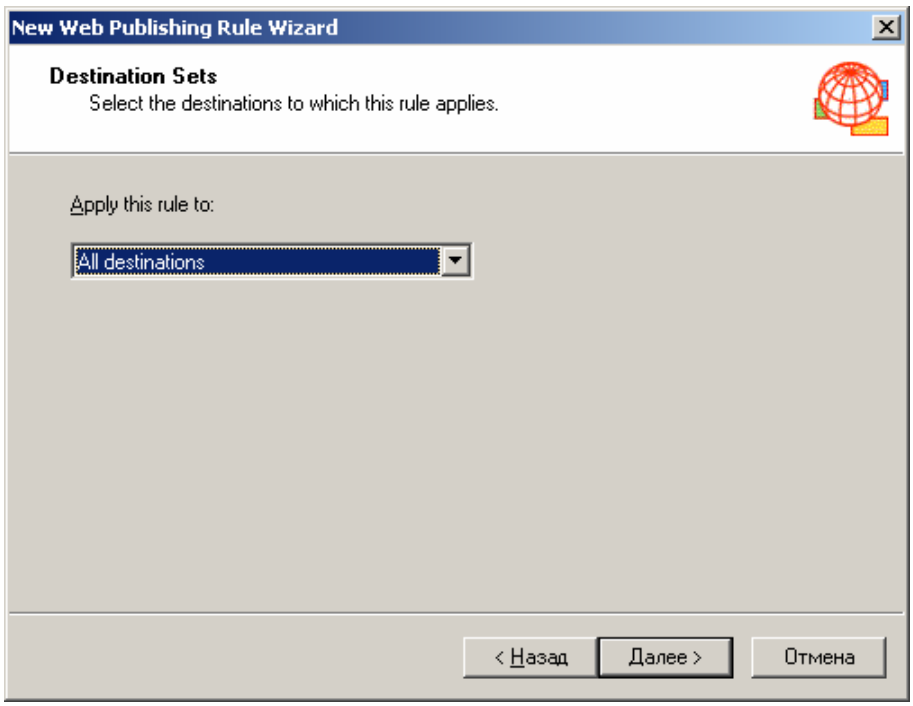


Рис. 87. Окно установки назначения

Этой установкой определяется, что данное правило публикации (фактически редирект) будет применяться ко всем Web-запросам, прошедшим через Слушателей, вне зависимости от того, какой ресурс из внутренней сети они запросили. В случае публикации нескольких Web-серверов, необходимо создать и применять в правилах публикации назначения.

В окне Client Type оставить значение, предлагаемое по умолчанию (любые запросы) и нажать «Далее»

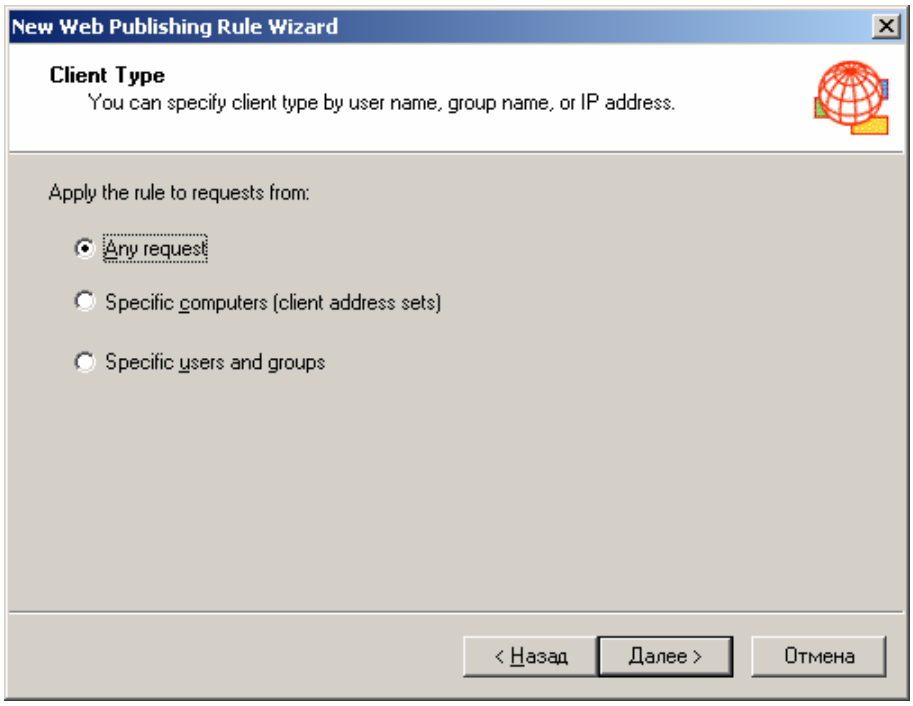


Рис. 88. Окно типа клиента

В этом окне мы указываем, что правило применяется ко всем Web-запросам, вне зависимости от того клиента, кто сформировал запрос.

В окне **Rule Action** выбрать редирект запросов во внутренний Web-сервер (**Redirect the request to this ...**)

Ввести доменное имя публикуемого Web-сервера и нажать «Далее»

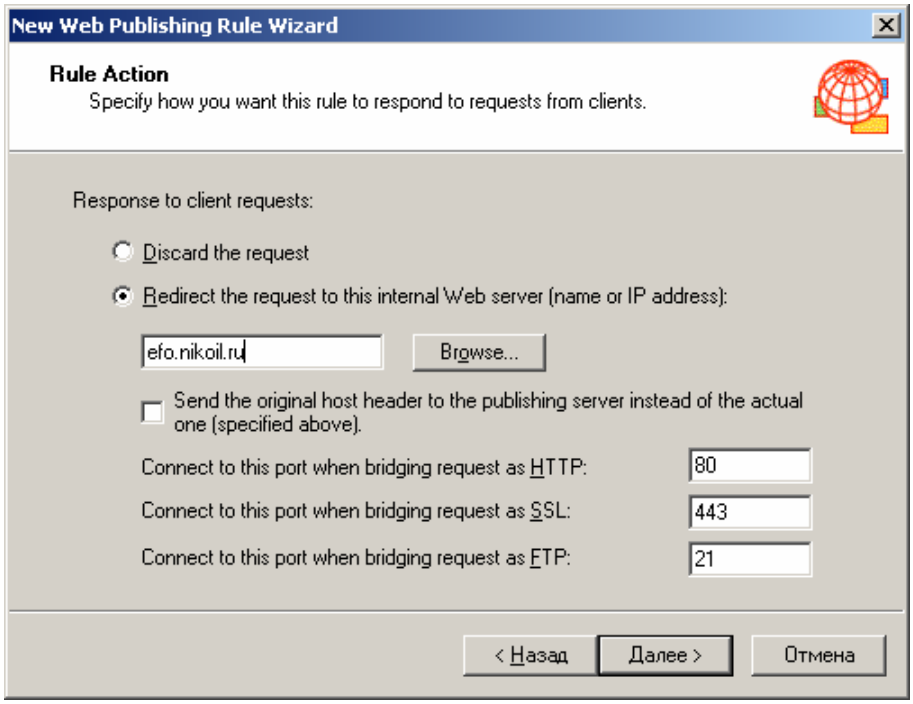


Рис. 89. Окно ввода доменного имени

Установив правило редиректа таким образом, все запросы, пришедшие к Слушателю на 80 порт, будут редиректироваться на 80 порт Web-сервера. Тоже самое будет происходить с запросами, поступившими на 443 порт (по протоколу TLS).

Завершить работу Мастера, нажав «Готово».

В списке правил Web-публикации появиться новая строка, соответствующая созданному нами правилу.

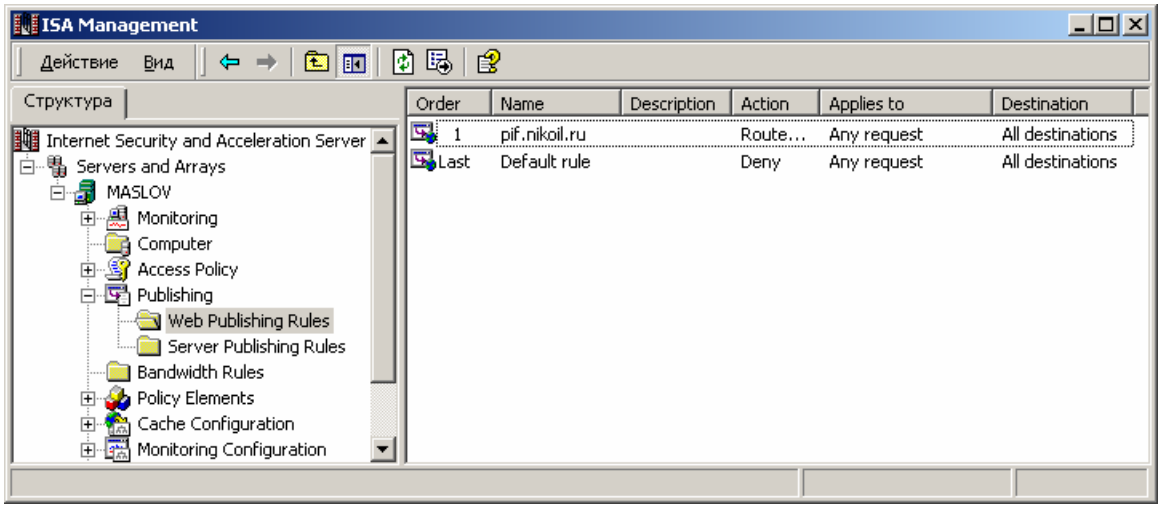


Рис. 90. Список правил Web-публикации