127 018, Москва, Сущевский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 3.9

Инструкция по использованию СКЗИ под управлением ОС Windows

ЖТЯИ.00083-01 90 03
Листов 69

2014

Содержание

1. Инсталляция СКЗИ КриптоПро CSP 5
2. Интерфейс СКЗИ КриптоПро CSP 8
2.1. Доступ к контрольной панели СКЗИ 8
2.2. Общая настройка СКЗИ 10
2.3. Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP» 10
2.4. Настройка оборудования СКЗИ 12
2.4.1. Изменение набора устройств считывания ключевой информации 13
2.4.1.1. Добавление считывателя 13
2.4.1.2. Удаление считывателя 17
2.4.1.3. Просмотр свойств считывателя 17
2.4.2. Изменение набора устройств хранения ключевой информации 18
2.4.2.1. Добавление носителя 18
2.4.2.2. Удаление ключевого носителя 22
2.4.2.3. Просмотр свойств ключевого носителя 22
2.4.3. Настройка датчиков случайных чисел (ДСЧ) 23
2.4.3.1. Добавление ДСЧ 23
2.4.3.2. Удаление ДСЧ 26
2.4.3.3. Просмотр свойств ДСЧ 26
2.5. Работа с контейнерами и сертификатами 27
2.5.1. Тестирование, копирование и удаление контейнера закрытого ключа 28
2.5.1.1. Тестирование контейнера закрытого ключа 28
2.5.1.2. Копирование контейнера закрытого ключа 30
2.5.1.3. Удаление контейнера закрытого ключа 34
2.5.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа 35
2.5.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа 35
2.5.2.2. Установка личного сертификата, хранящегося в контейнере закрытого ключа 38
2.5.3. Установка личного сертификата, хранящегося в файле 39
2.5.4. Управление паролями доступа к закрытым ключам 43
2.5.4.1. Изменение пароля на доступ к закрытому ключу 43
2.5.4.2. Удаление запомненных паролей 44
2.6. Установка параметров безопасности 45
2.7. Дополнительные настройки 48
2.7.1. Просмотр версий используемых файлов 48
2.7.2. Установка времени ожидания ввода информации от пользователя 48
2.8. Установка параметров криптографических алгоритмов 51
2.9. Настройка аутентификации в домене Windows 51
2.10. Настройки TLS 52
3. Интерфейс генерации ключей 54
3.1. Создание ключевого контейнера 54
3.1.1. Выбор ключевого носителя 54
3.1.2. Генерация начальной последовательности ДСЧ 54
3.1.3. Ввод пароля на доступ к закрытому ключу 55
3.1.4. Выбор способа защиты доступа к закрытому ключу 55
3.1.4.1. Установка нового пароля 56
3.1.4.2. Установка мастер-ключа 56
3.1.4.3. Разделение ключа на несколько носителей 57
3.2. Открытие ключевого контейнера 58
3.2.1. Отсутствие ключевого носителя 58
3.2.2. Проверка пароля на доступ к закрытому ключу 59
3.2.2.1. Проверка текстового пароля 59
3.2.2.2. Проверка пароля при зашифровании ключа на другом ключе 59

3.2.2.3. Проверка пароля при разделении ключа между несколькими носителями..59
3.3. Генерация ключей и получение сертификата при помощи УЦ.....60
4. Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS 61
4.1. Размещение сертификата аутентификации сервера на сервере ISA.....61
4.2. Размещение сертификата клиентской аутентификации на сервере ISA 62
4.3. Настройка соединения с Web-клиентом 63
4.4. Публикация Web-сервера в сети Интернет.....66

1. Инсталляция СКЗИ КриптоПро CSP

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Для установки программного обеспечения вставьте компакт-диск в дисковод. Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы, имеющий нужный Вам уровень защищенности и удобный для Вас язык установки. Запустите выполнение установки.

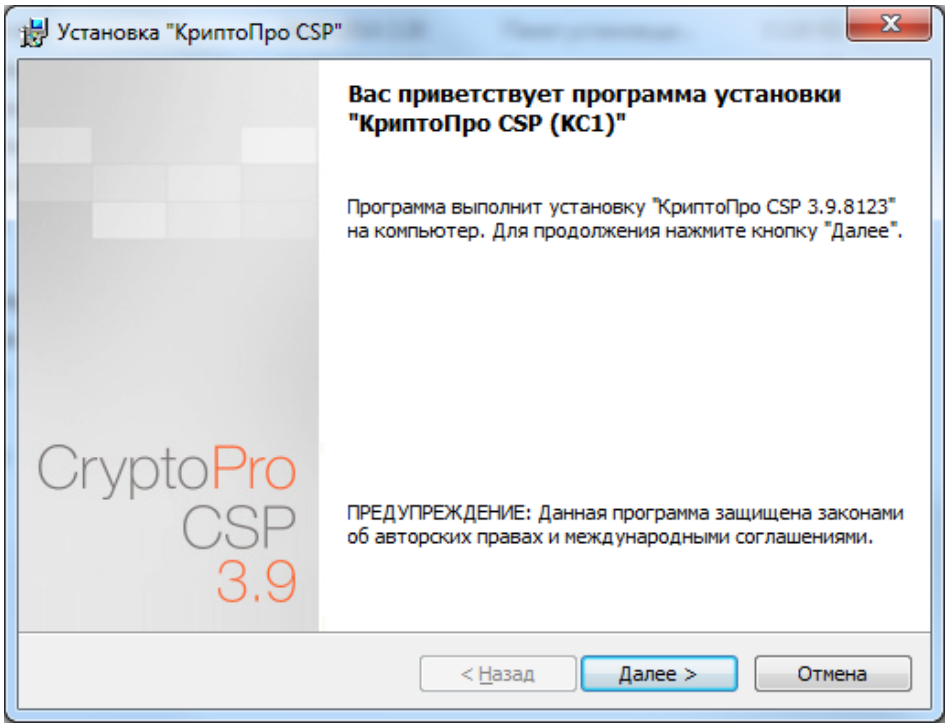


Рис. 1. Приветственное окно мастера установки.

Если мастер установки обнаружит на машине более раннюю версию СКЗИ КриптоПро CSP, то в окне появится информация о замещаемых продуктах:

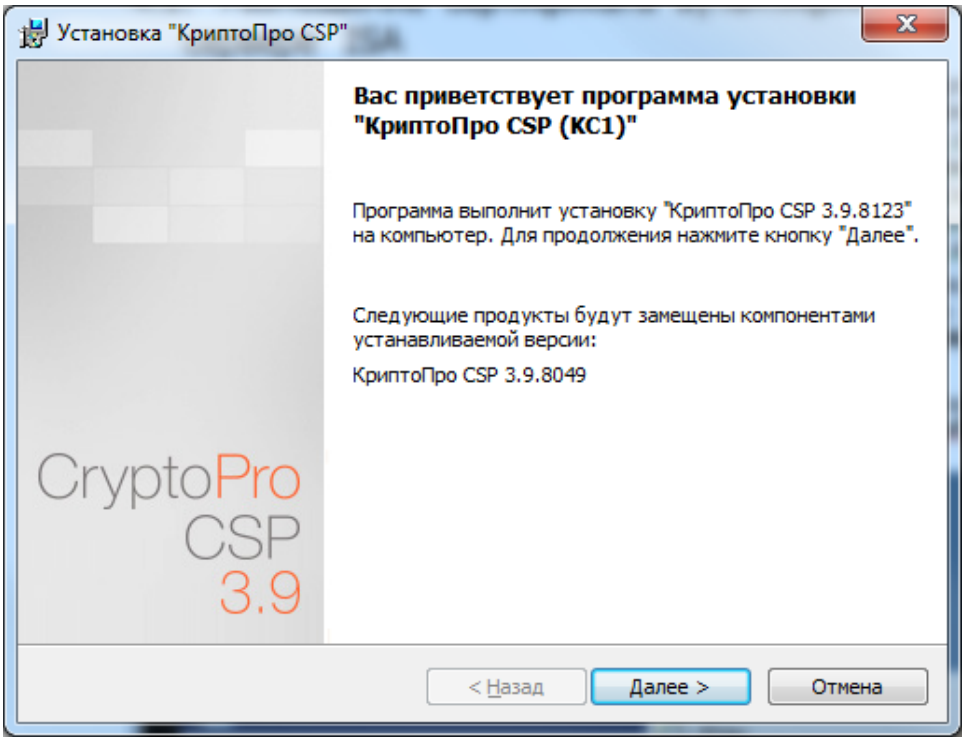
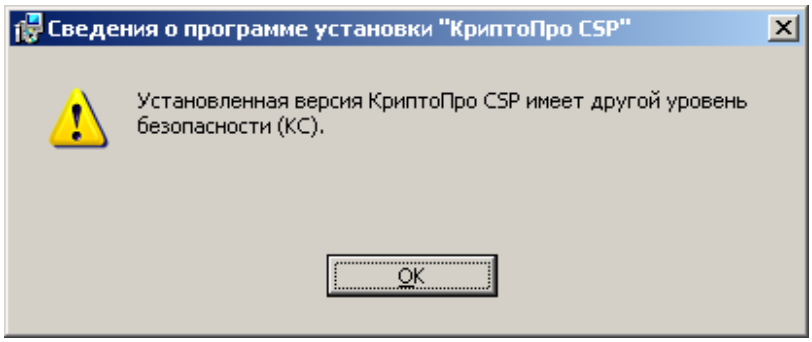


Рис. 2. Установка с замещением компонент.

Примечание: При установке в режиме замещения компонент важно, чтобы уровень защищенности установленной на компьютере версии СКЗИ КриптоПро CSP совпадал с уровнем защищенности в выбранном Вами для установки дистрибутиве. В противном случае появится сообщение об ошибке и установка завершена не будет:



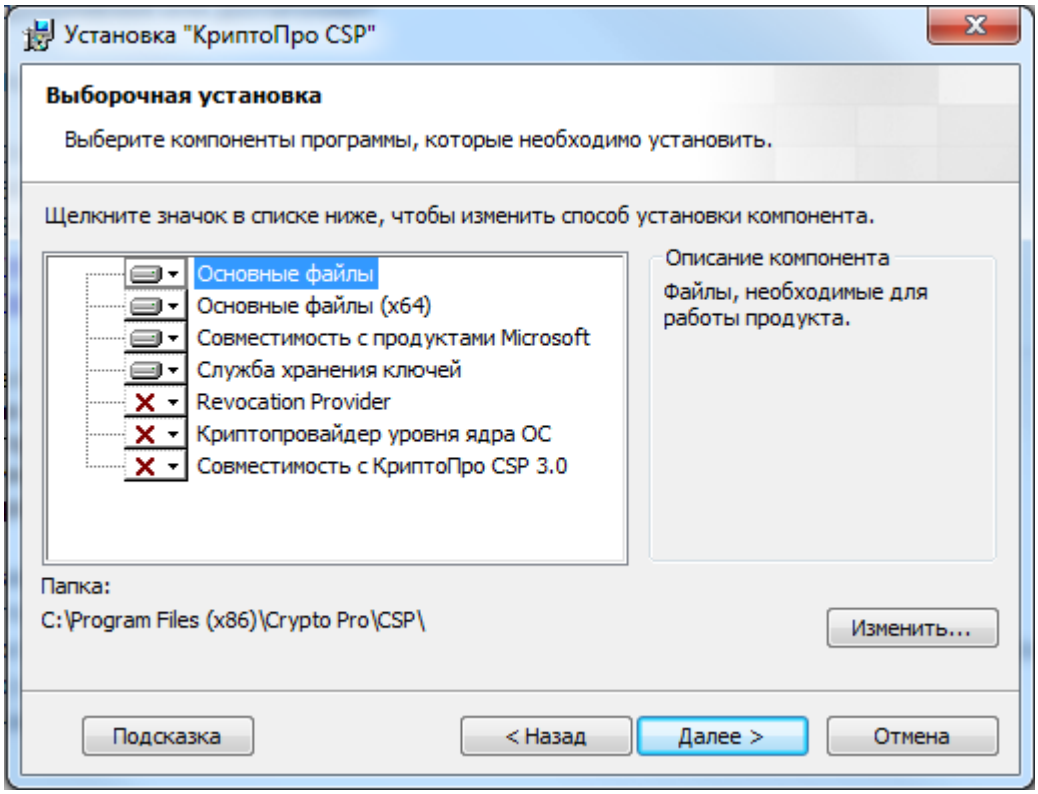
В этом случае необходимо выбрать установку с дистрибутива, имеющего соответствующий установленному уровень защищенности.

Для дальнейшей установки КриптоПро CSP нажмите **Далее**.

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел (для уровней КС2 и КС3) или настроить криптопровайдер на использование службы хранения ключей (для уровня КС1). Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств КриптоПро CSP.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

По умолчанию (вид установки «Обычная») устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). По желанию можно установить следующие дополнительные компоненты (вид установки «Выборочная»):



Revocation Provider - Механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (COC, CRL). Кроме этого предоставляет возможность использования COC, выпущенных по правилам, описанным в RFC 3280.

Служба хранения ключей – системный сервис для исполнения 2, обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ.

Криптопровайдер уровня ядра – Необходим для работы TLS в службах Windows Vista/2008/7.

Совместимость с продуктами Microsoft – Обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express. Необходим для входа в систему по смарт-картам.

Совместимость с КриптоПро CSP 3.0 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.0. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.0.

Примечание. В состав КриптоПро CSP SDK, входит описание параметров командной строки установщика Windows (**\CHM\msi-readme.txt**), которые удобно использовать для автоматического развертывания дистрибутива.

2. Интерфейс СКЗИ КриптоПро CSP

2.1. Доступ к контрольной панели СКЗИ

Данный раздел является инструкцией по использованию контрольной панели (панели настройки) средства криптографической защиты информации (СКЗИ) КриптоПро CSP. Панель настройки КриптоПро CSP доступна как отдельный пункт в группе программ «КриптоПро» (меню **Пуск ⇒ Программы**), а также из оснастки КриптоПро PKI, расположенной в той же группе программ «КриптоПро» (меню **Пуск ⇒ Программы**).

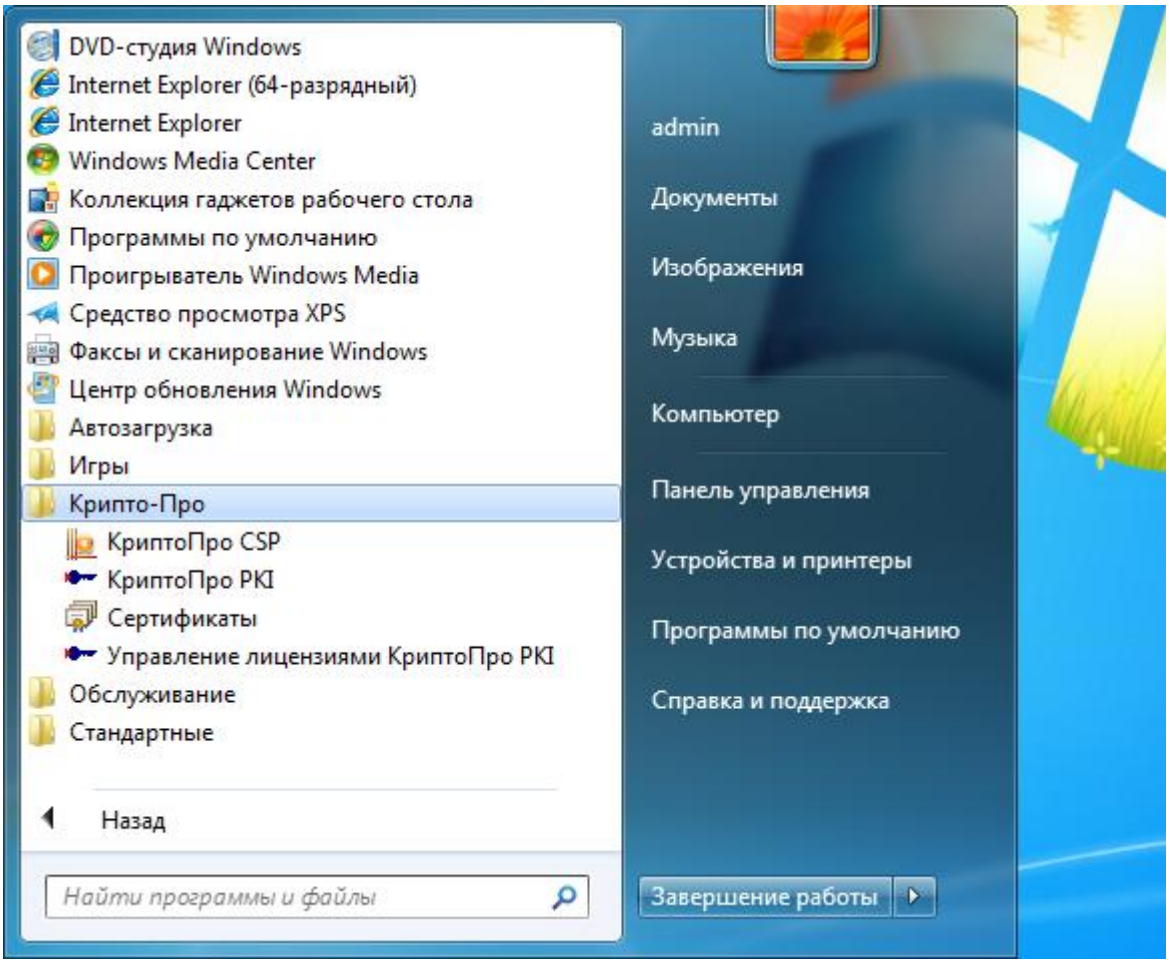


Рис. 3. Доступ к оснастке.

В оснастке «**Управление лицензиями КриптоПро PKI**», расположенной в группе программ «КриптоПро» (меню **Пуск ⇒ Программы**) осуществляется ввод лицензий и просмотр лицензионной информации обо всех установленных продуктах ООО "КРИПТО-ПРО".

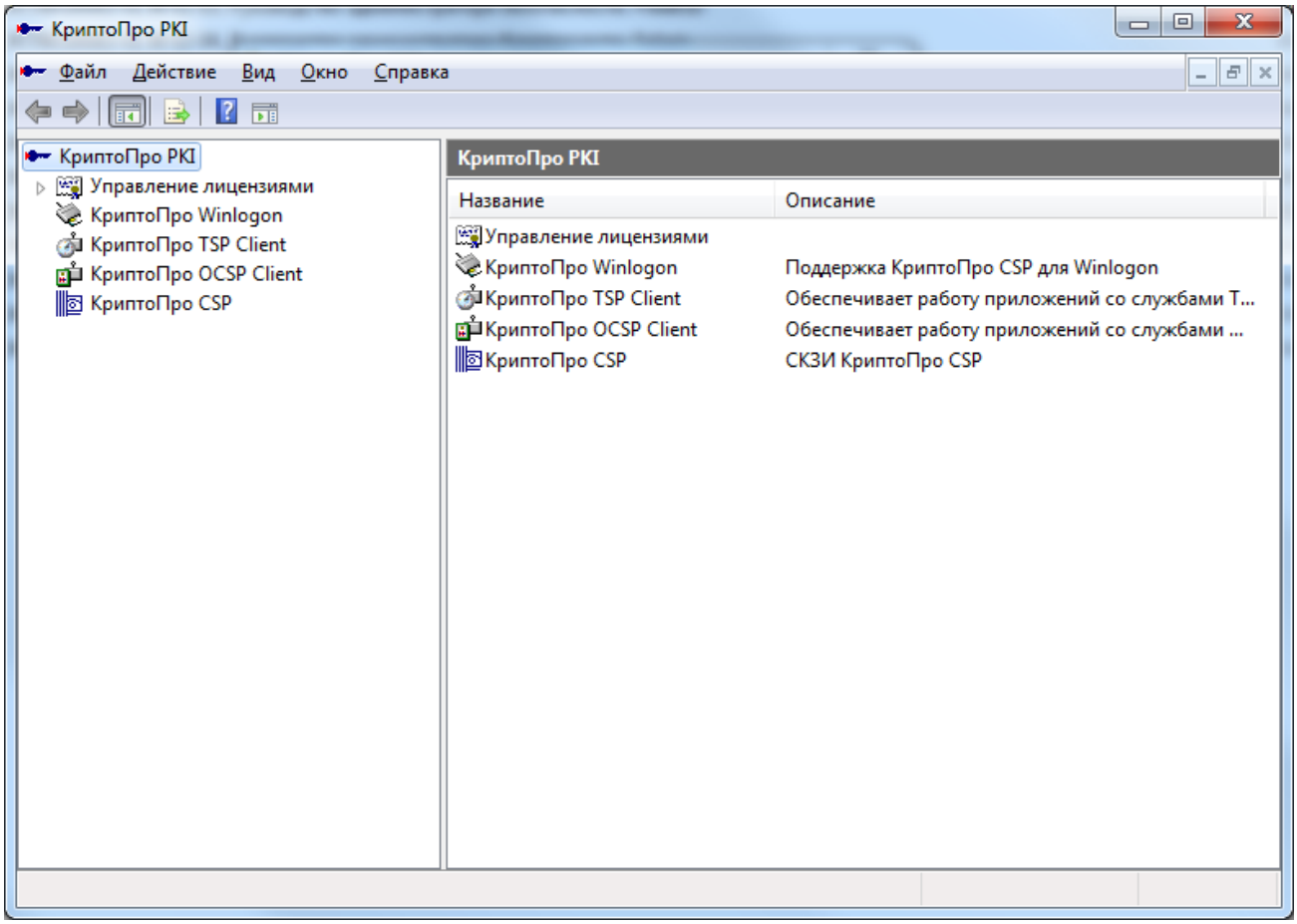


Рис. 4. Оснастка «Управление лицензиями КриптоПро PKI».

В оснастке «**КриптоПро PKI**», расположенной в группе программ «КриптоПро» (меню **Пуск ⇒ Программы**) в контекстном меню пункта **КриптоПро CSP** доступна контрольная панель СКЗИ КриптоПро CSP «**Свойства: КриптоПро CSP**» (см. Рис. 5), которая состоит из семи вкладок:

- Общие;
- Оборудование;
- Сервис;
- Безопасность;
- Дополнительно;
- Алгоритмы;
- WinLogon.

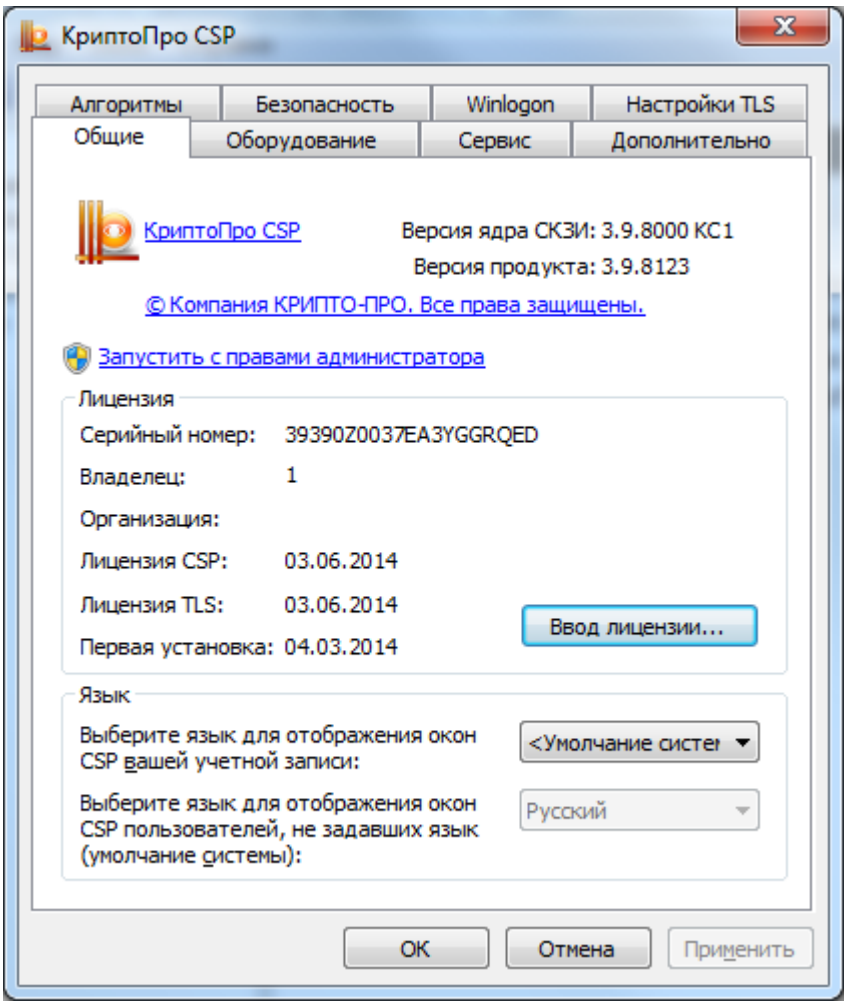


Рис. 5. Панель настройки

2.2. Общая настройка СКЗИ

Вкладка **Общие** панели свойств СКЗИ КриптоПро CSP предназначена для просмотра информации о версии установленного ПО СКЗИ КриптоПро CSP и для изменения языка отображения окон, выдаваемых криптопровайдером.

2.3. 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. 8) пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта.

Для ввода лицензии выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ Управление лицензиями КриптоПро PKI.** В оснастке Управление лицензиями КриптоПро PKI (см. Рис. 4) выберите продукт, лицензию на который Вы хотите ввести. В контекстном меню выберите **Все задачи - Ввести серийный номер.** (см. Рис. 6)

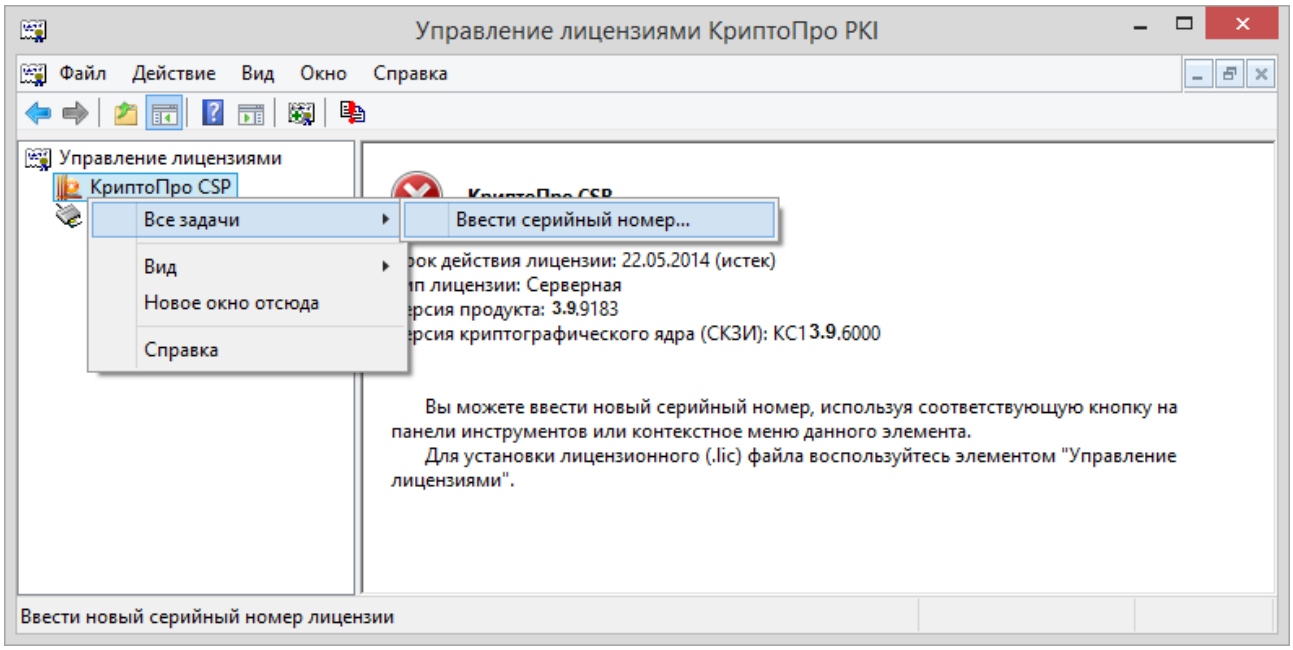


Рис. 6. Ввод серийного номера.

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. 7).

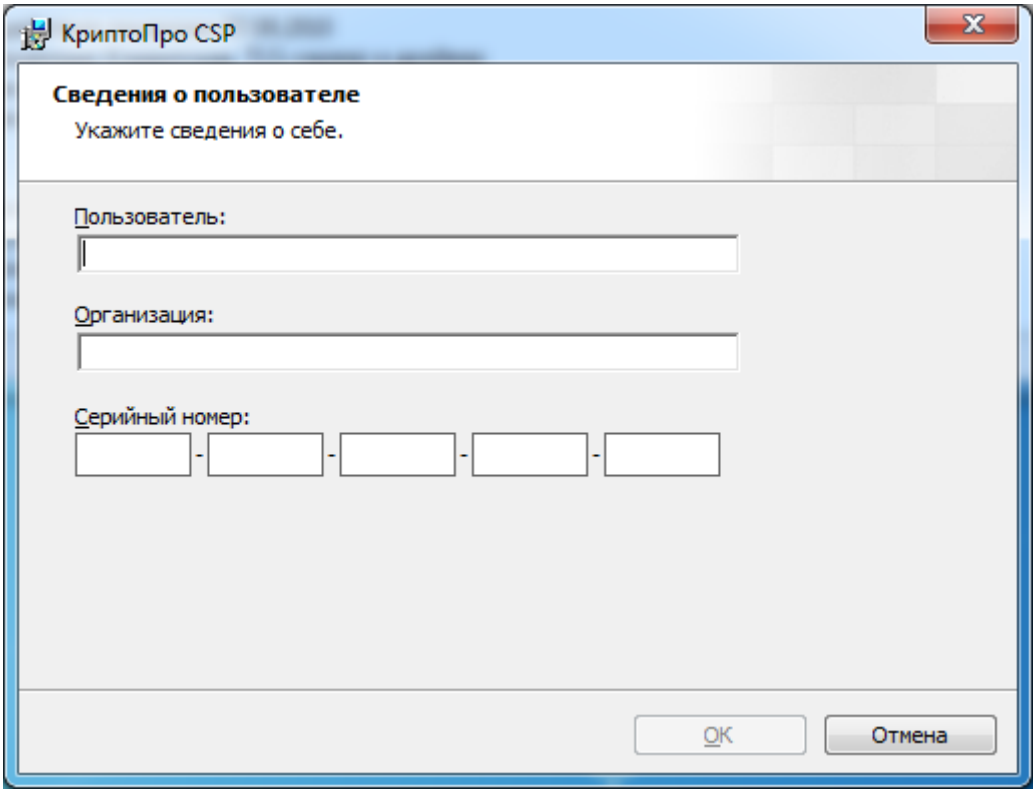


Рис. 7. Ввод данных лицензии

После ввода и нажатия клавиши OK произойдет возврат к оснастке Управление лицензиями КриптоПро PKI с указанным типом лицензии и сроком ее действия (см. Рис. 4).

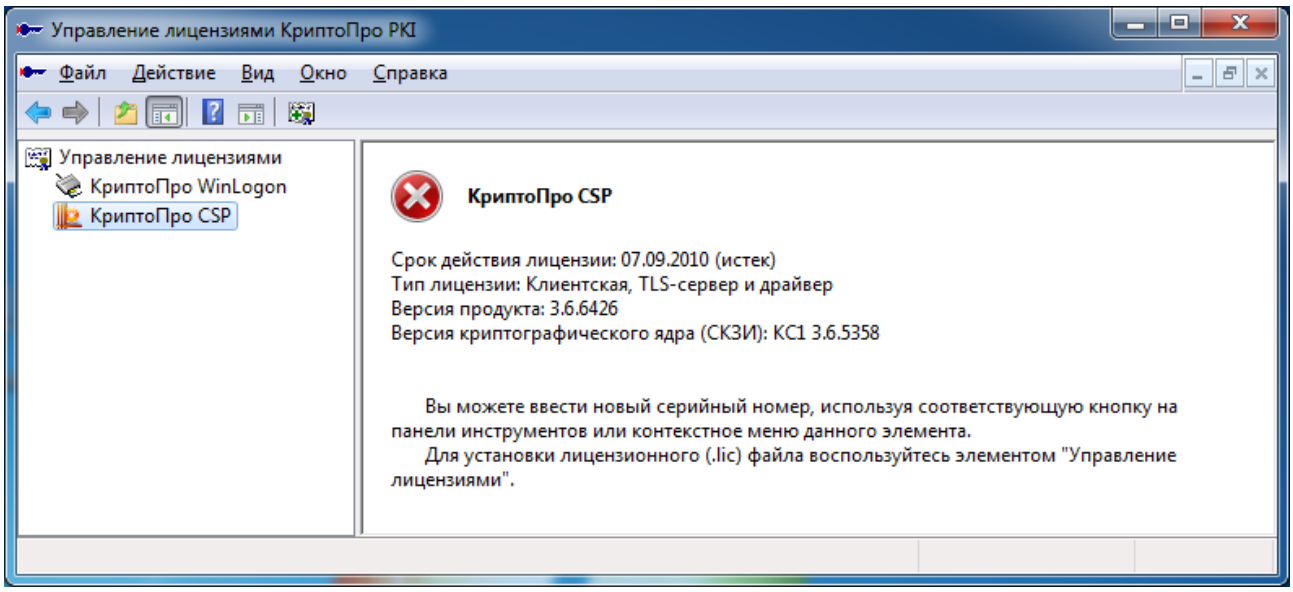
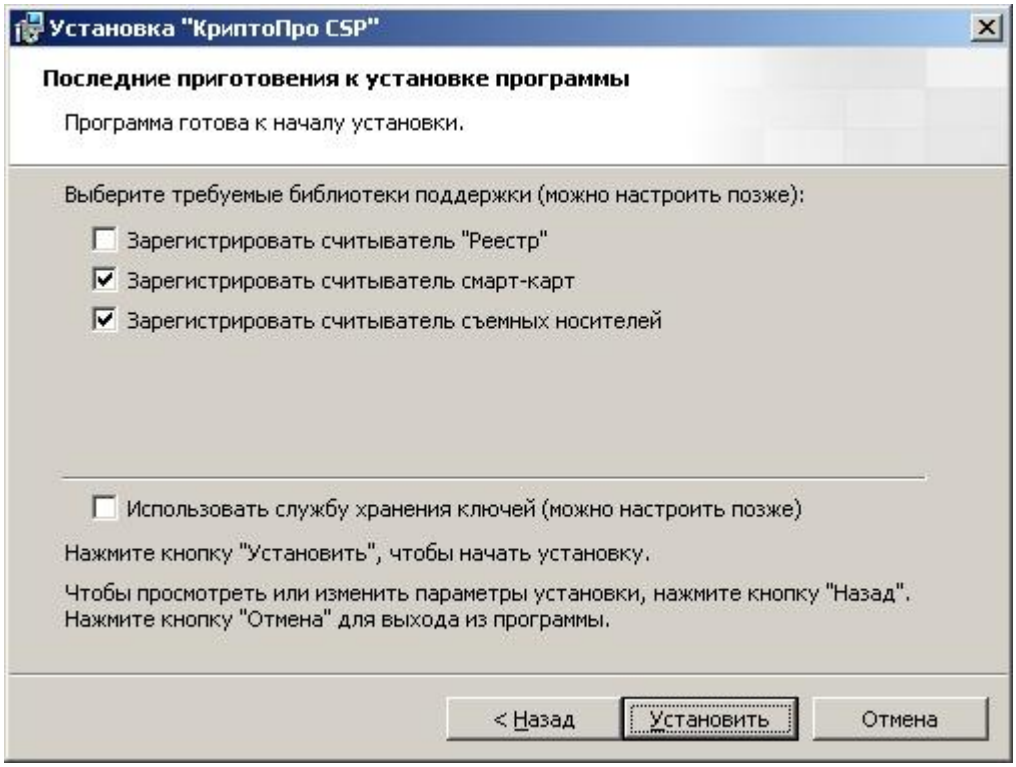


Рис. 8. Время действия лицензии истекло.

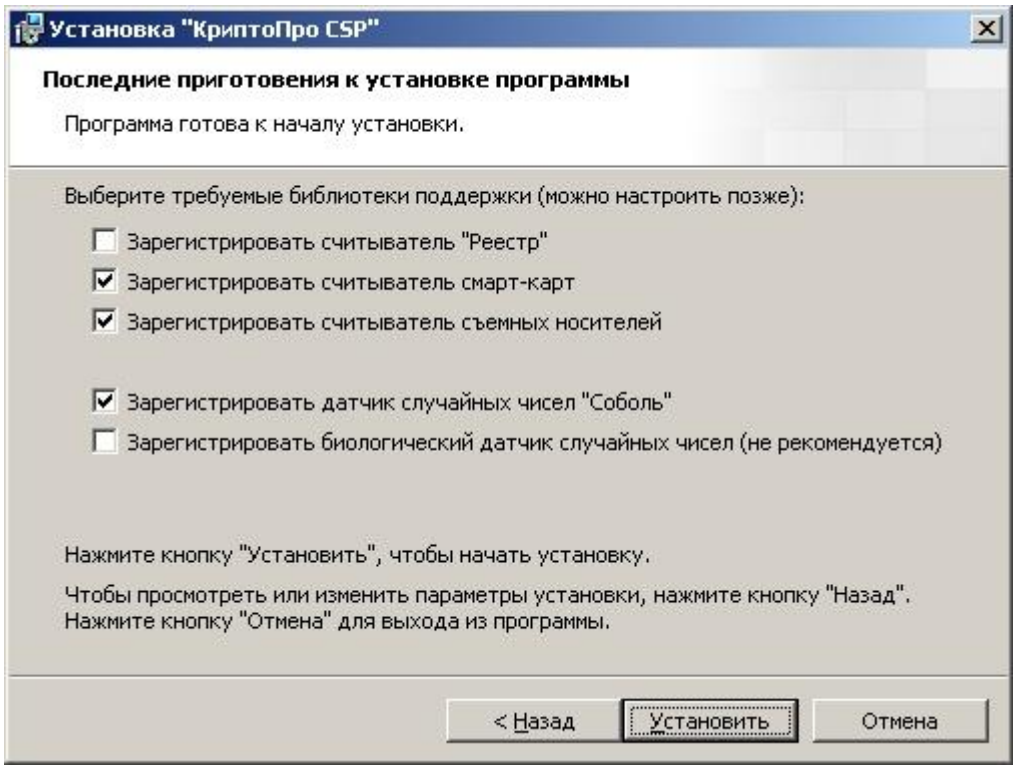
2.4. Настройка оборудования СКЗИ

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

Предустановленными являются все считыватели смарт-карт (и соответствующие им типы носителей) и все дисководы съемных дисков, в том числе flash-носители. В процессе установки криптопровайдера можно дополнительно зарегистрировать в системе считыватель «Реестр».



В исполнении по уровню защиты КС1 предустановлен Биологический ДСЧ. В исполнениях по уровням защиты КС2 и КС3 Биологический ДСЧ или аппаратный ДСЧ «Соболь» можно добавить в процессе установки криптопровайдера.



2.4.1. Изменение набора устройств считывания ключевой информации

2.4.1.1. Добавление считывателя

Для того, чтобы добавить считыватель, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить считыватели.**

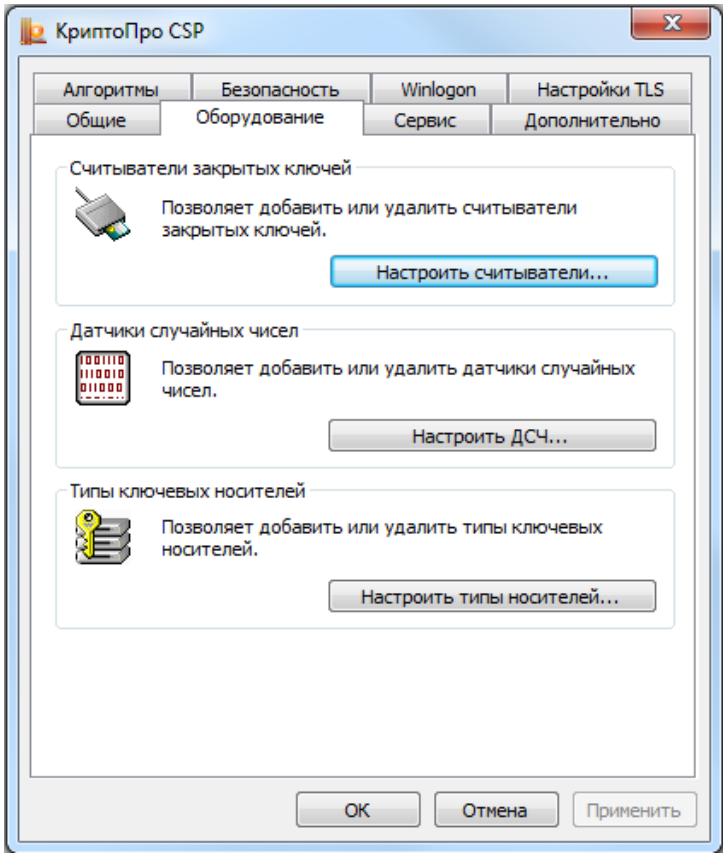


Рис. 9. Контрольная панель. Вкладка «Оборудование»

Система отобразит окно «Управление считывателями» (см. Рис. 10).

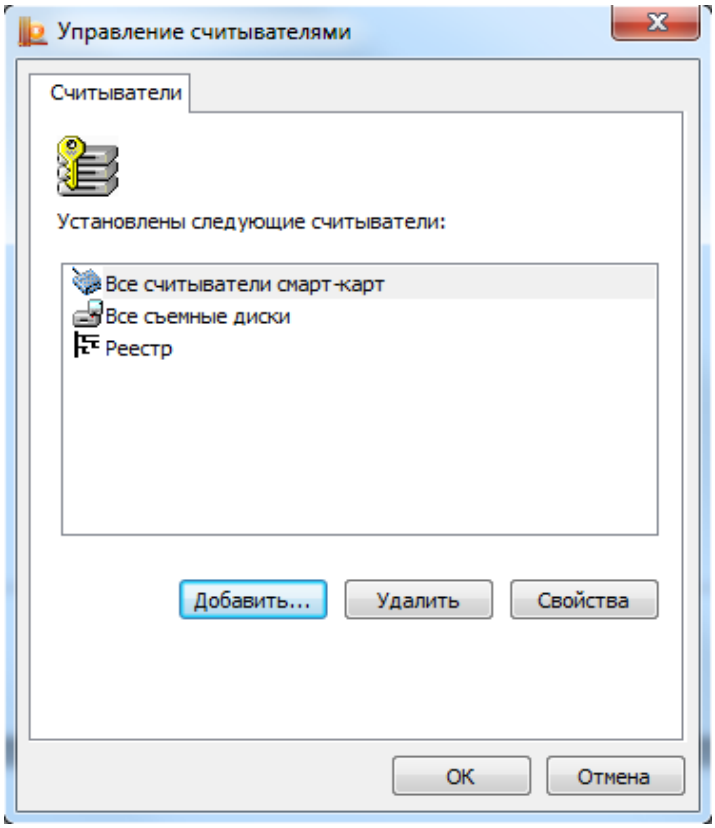


Рис. 10. Окно «Управление считывателями»

Для того чтобы КриптоПро CSP 3.9 сделало доступным использование нового считывателя, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки считывателя (см. Рис. 11). В окне мастера установки нажмите кнопку **Далее**.

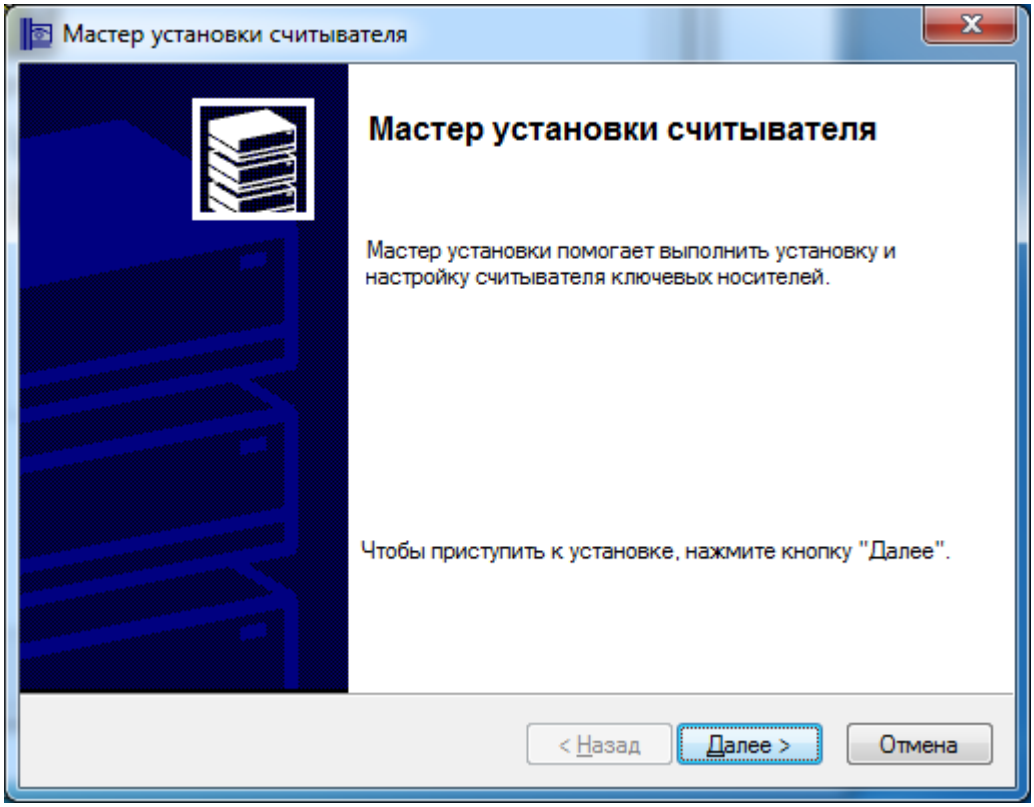


Рис. 11. Запуск мастера установки считывателя

Система отобразит окно «Выбор считывателя» (см. Рис. 12). Для того чтобы использовать считыватель, входящий в состав дистрибутива СКЗИ КриптоПро CSP, в этом окне выберите из списка считыватель, который следует добавить, и нажмите кнопку **Далее.**

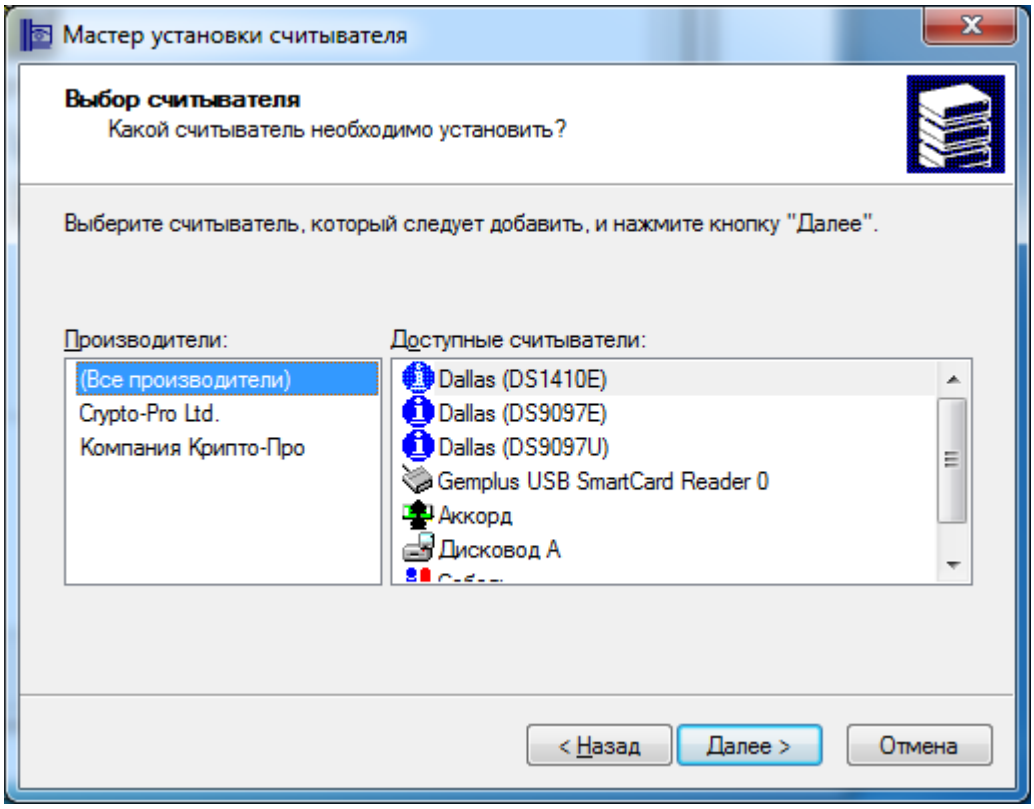


Рис. 12. Окно «Выбор считывателя»

В зависимости от выбранного считывателя может потребоваться выбор соединения для этого устройства. Тогда система отобразит окно «Выбор соединения» (см. Рис. 13). В этом окне выберите соединение для считывателя и нажмите кнопку **Далее.**

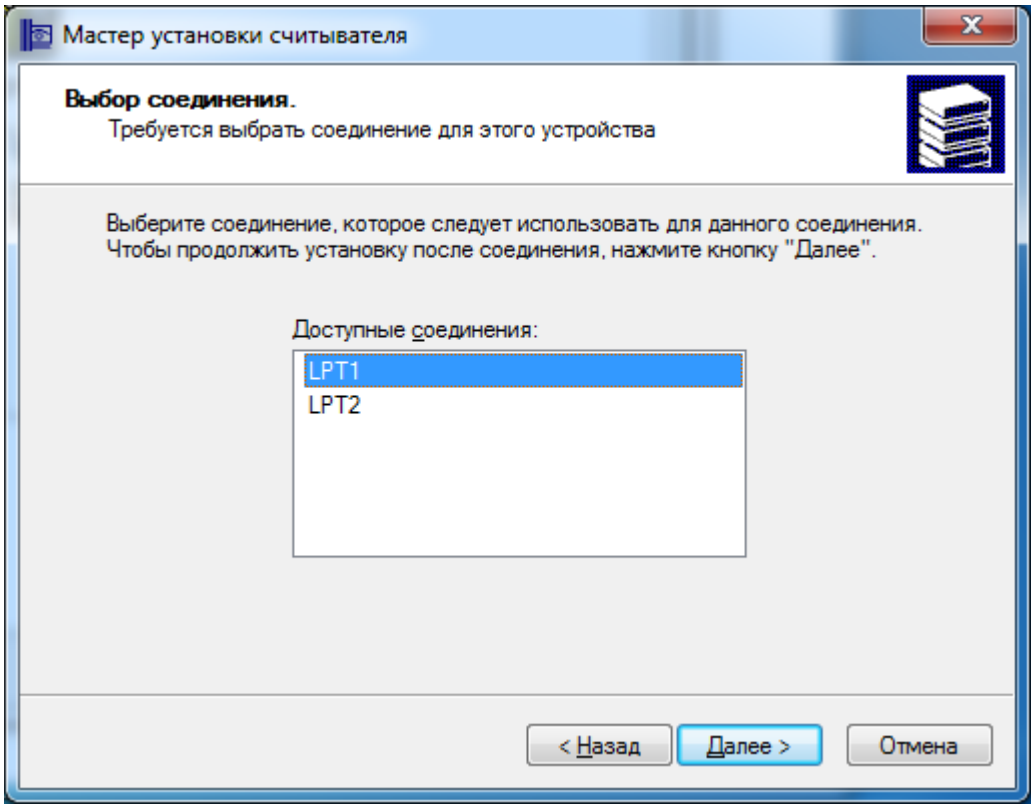


Рис. 13. Окно «Выбор считывателя»

Система отобразит окно «Имя считывателя» (см. Рис. 14). В этом окне введите имя выбранного считывателя и нажмите кнопку **Далее.**

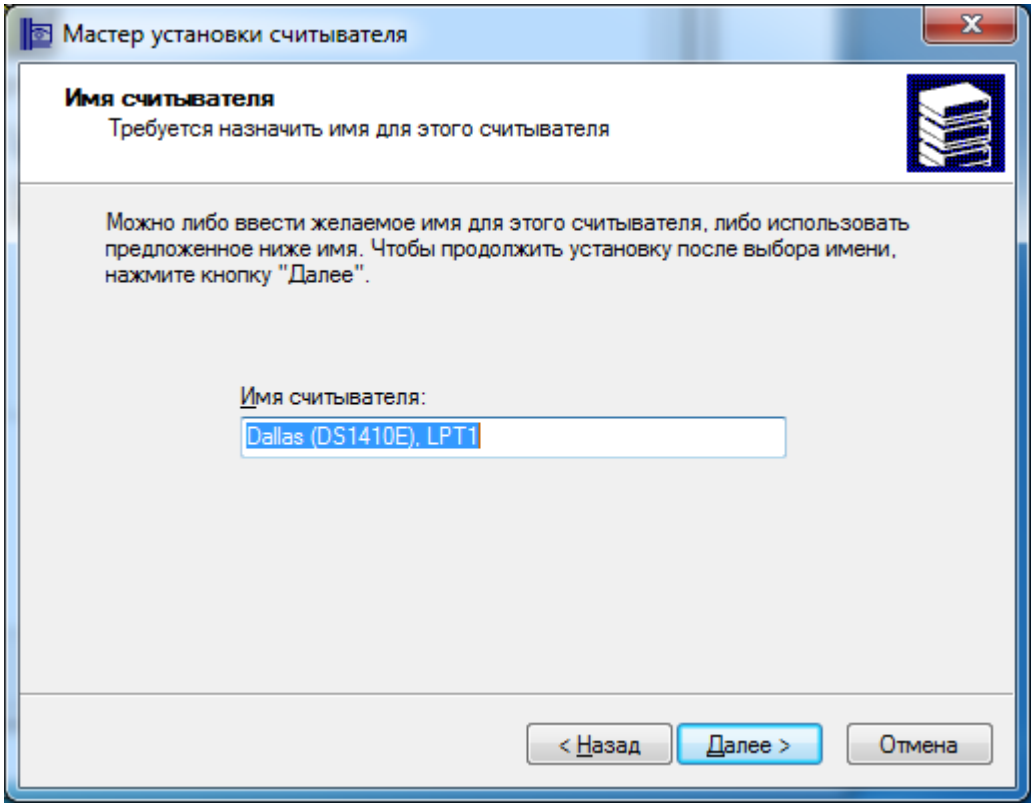


Рис. 14. Окно «Имя считывателя»

Система отобразит окно «Завершение работы мастера установки считывателя» (см. Рис. 15). Внимательно прочитайте текст в этом окне, нажмите в нем кнопку **Готово** и перезагрузите компьютер, если это требуется.

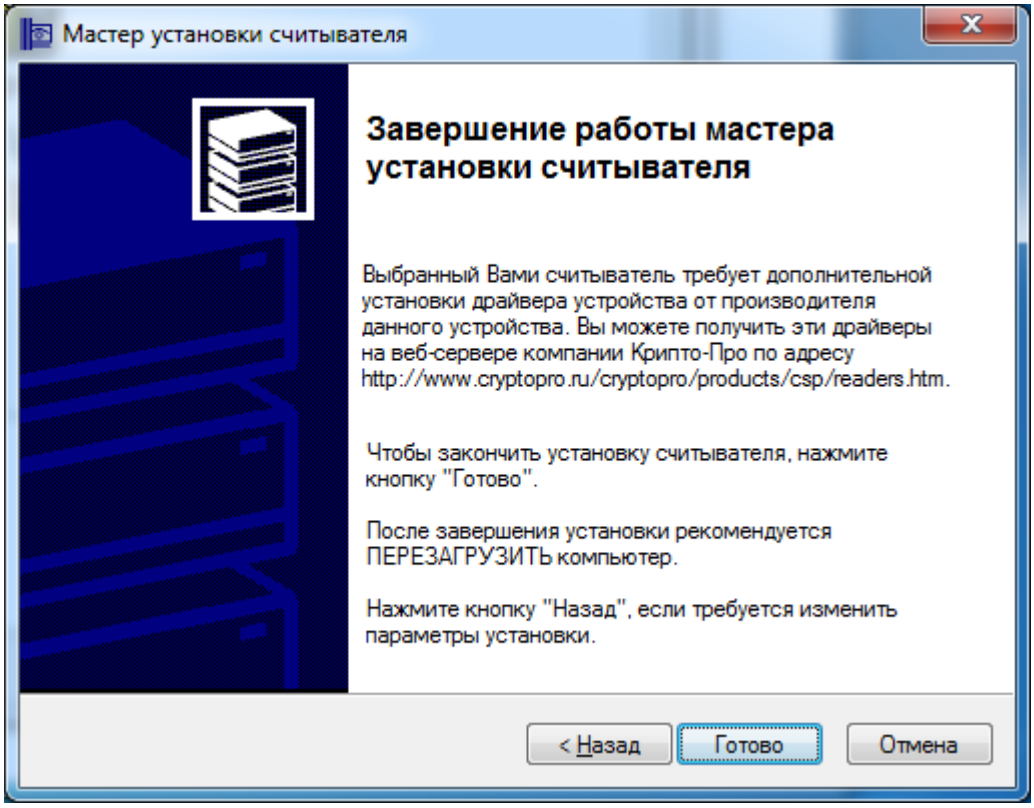


Рис. 15. Завершение мастера установки считывателя

Примечание. Имеется возможность установки драйверов сторонних производителей, обеспечивающие взаимодействие КриптоПро CSP с аппаратной частью в случае, если они не входят в состав дистрибутива СКЗИ. Для их установки следует 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.

2.4.1.2. Удаление считывателя

Для того чтобы сделать недоступным использование считывателя, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить считыватели.**

Система отобразит окно «Управление считывателями» (см. Рис. 10). Выберите считыватель, который требуется сделать недоступным, и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление считывателя» (см. Рис. 16). Нажмите кнопку **Да**. Считыватель будет удален.

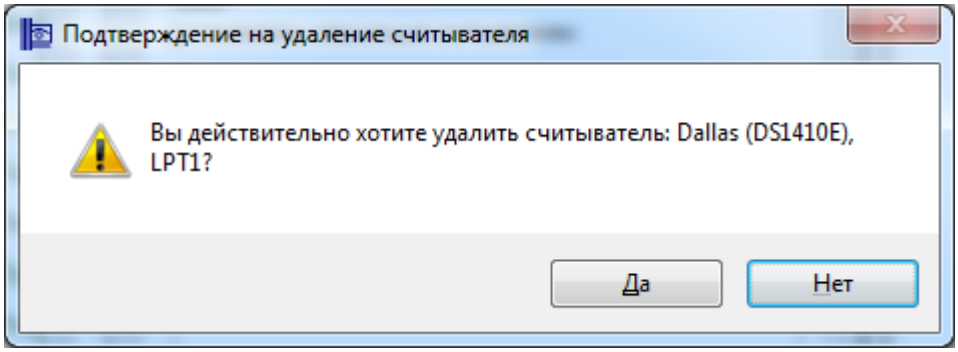


Рис. 16. Окно «Подтверждение на удаление считывателя»

2.4.1.3. Просмотр свойств считывателя

Для того, чтобы просмотреть свойства считывателя, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить считыватели.**

Система отобразит окно «Управление считывателями» (см. Рис. 10). Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя считывателя» (см. Рис. 17), в котором отображается справочная информация о выбранном считывателе, в том числе, и данные о состоянии устройства. После просмотра свойств считывателя нажмите кнопку **OK.**

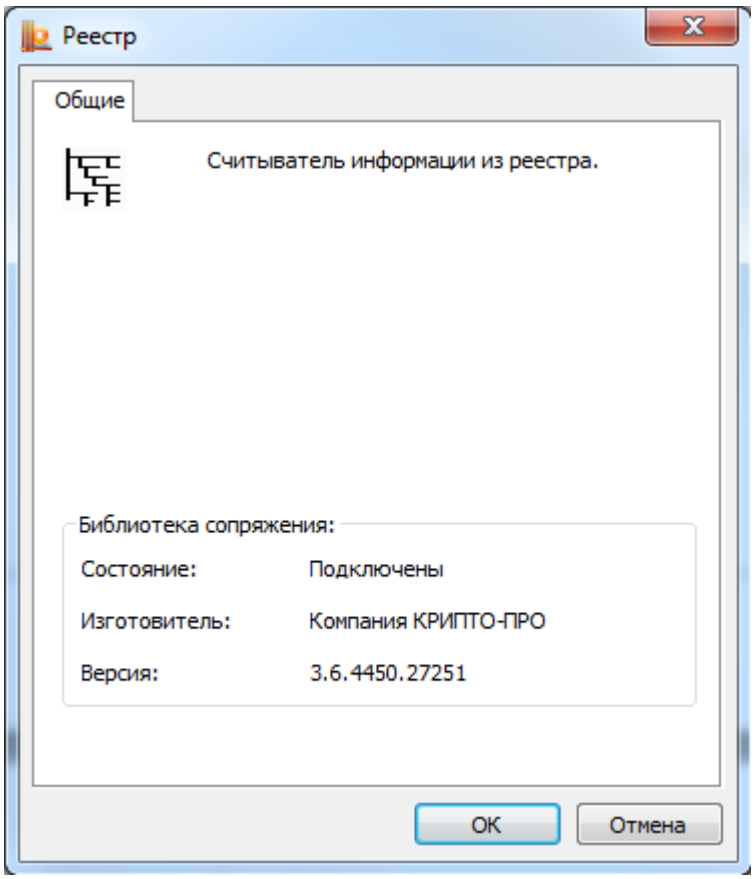


Рис. 17. Окно «Свойства: имя считывателя»

2.4.2. Изменение набора устройств хранения ключевой информации

2.4.2.1. Добавление носителя

Для того чтобы сделать доступным носитель ключевой информации, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить типы носителей.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 18).

Носители Магистра, Магистра Сбербанк/BGS, Оскар, Оскар CSP 2.0, РИК являются смарткартами. Носители типа Rutoken и eToken являются USB-ключами.

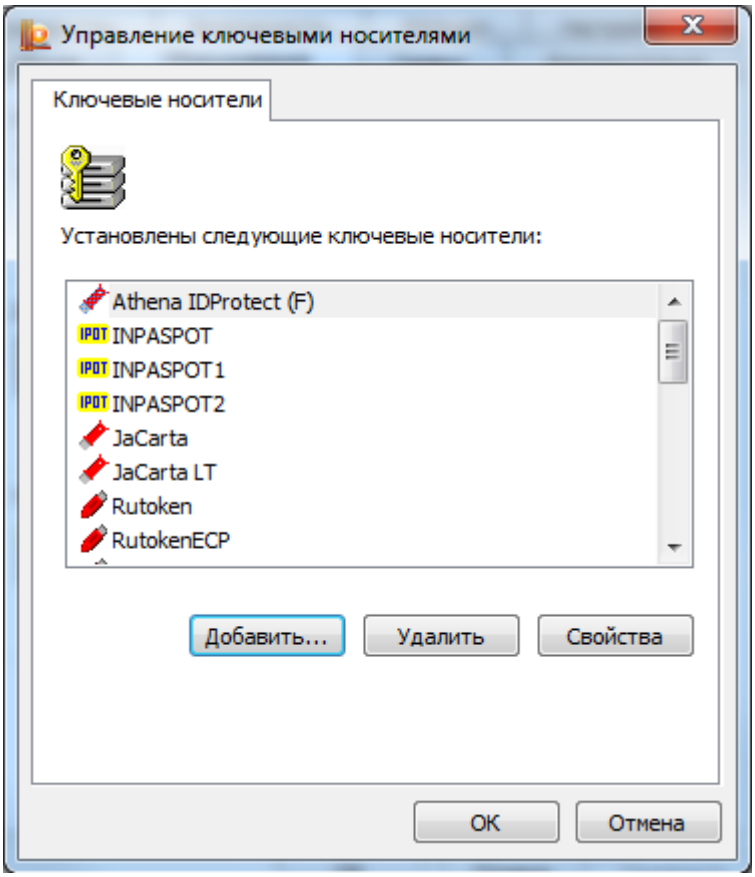


Рис. 18. Окно «Управление ключевыми носителями»

Для того чтобы сделать доступным ключевой носитель, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки ключевого носителя (см. Рис. 19). В окне мастера установки нажмите кнопку **Далее**.

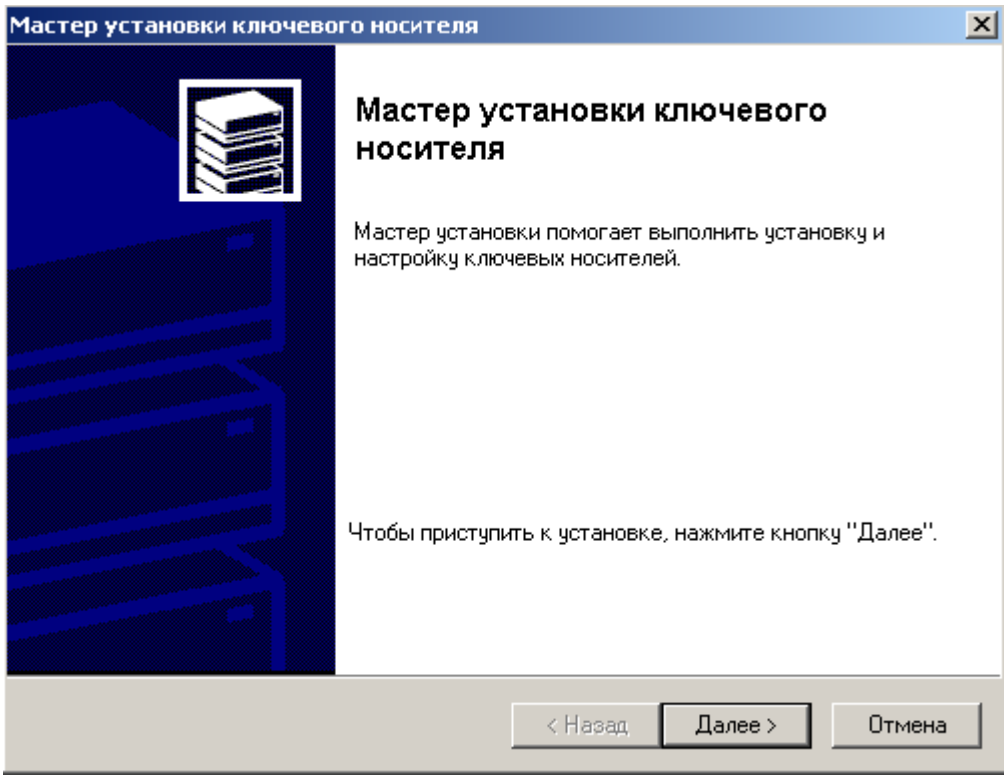


Рис. 19. Запуск мастера установки ключевого носителя

Система отобразит окно «Выбор ключевого носителя» (см. Рис. 20). В этом окне выберите ключевой носитель, который следует сделать доступным, и нажмите кнопку **Далее.**

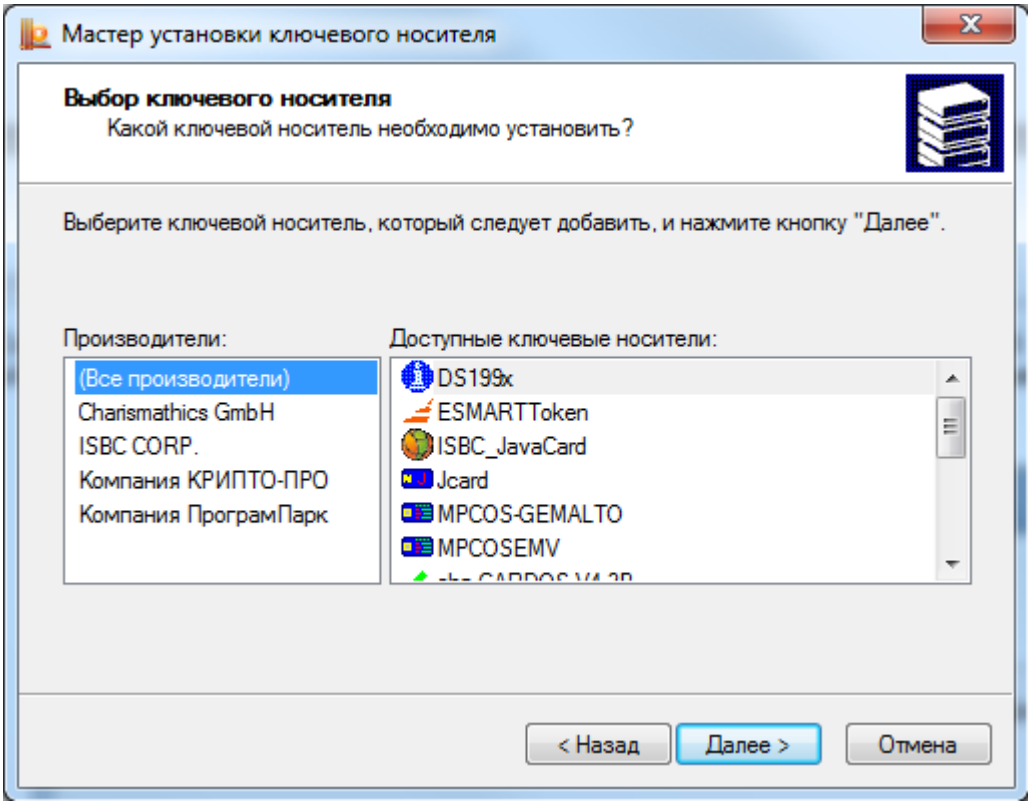


Рис. 20. Окно «Выбор ключевого носителя»

Система отобразит окно «Имя ключевого носителя» (см. Рис. 21). В этом окне введите имя выбранного носителя и нажмите кнопку **Далее.**

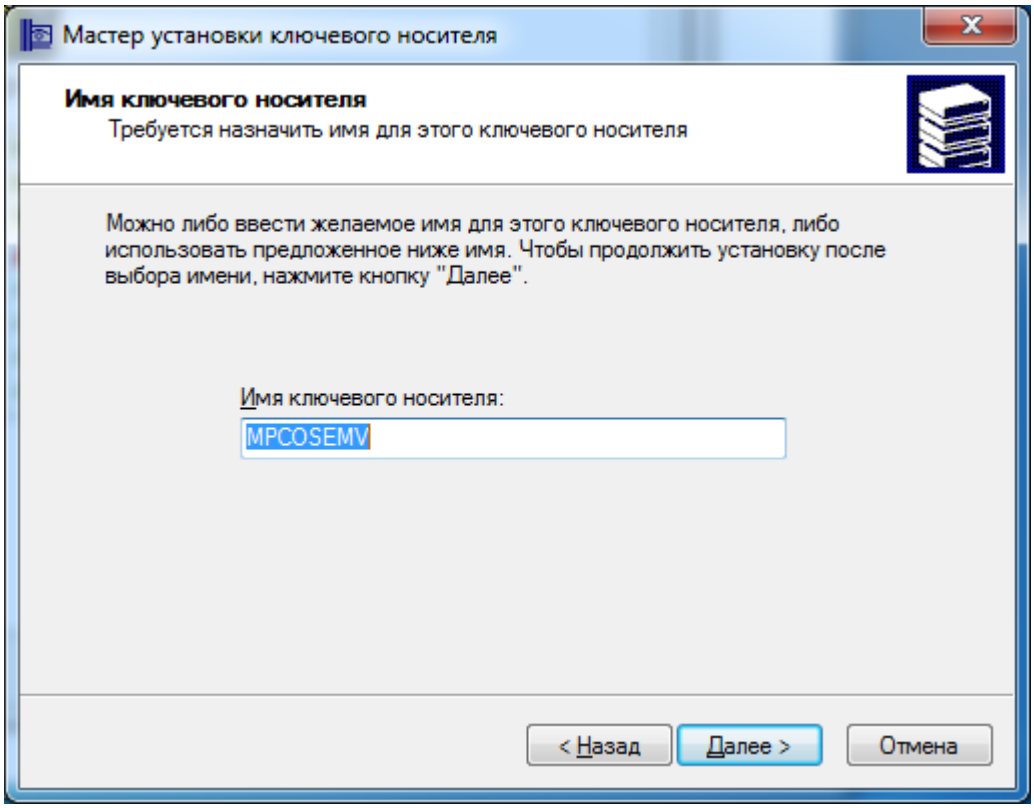


Рис. 21. Окно «Имя ключевого носителя»

Система может отобразить дополнительные окна в зависимости от типа ключевого носителя, так для MPCOS/EMV будет отображено окно «Разметка карты» (см. Рис. 22). В этом окне укажите разметку карты и нажмите кнопку **Далее.**

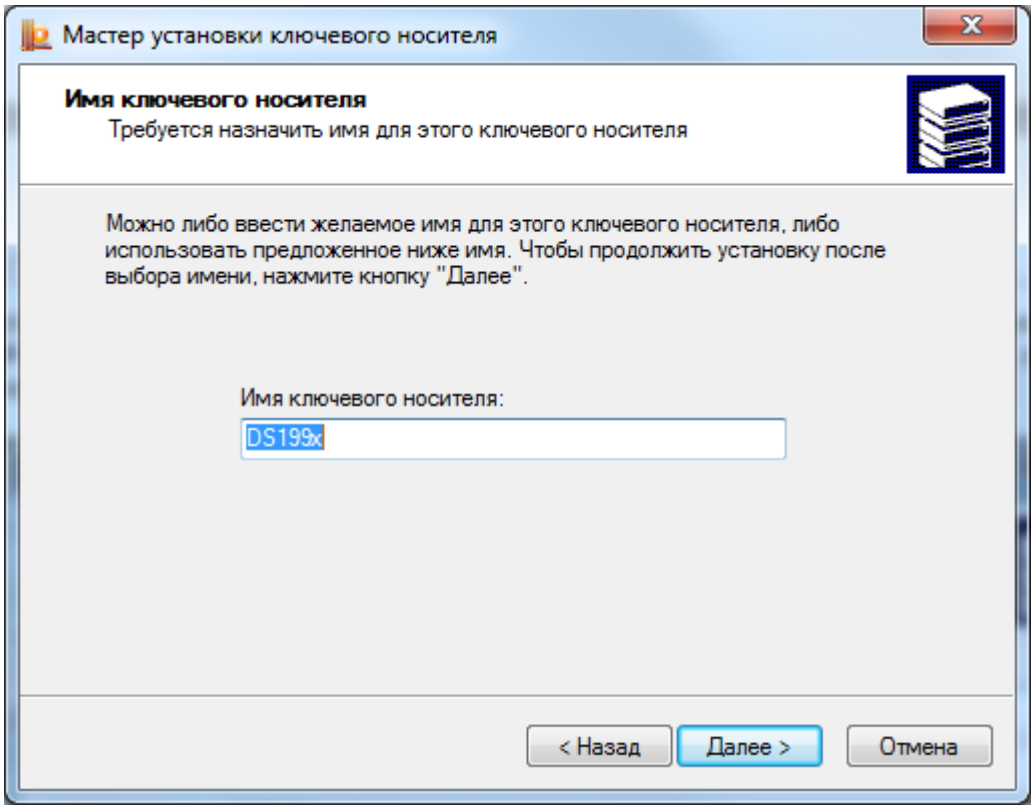


Рис. 22. Окно «Разметка карты»

Система отобразит окно «Завершение работы мастера установки ключевого носителя» (см. Рис. 23). Нажмите в нем кнопку **Готово**.

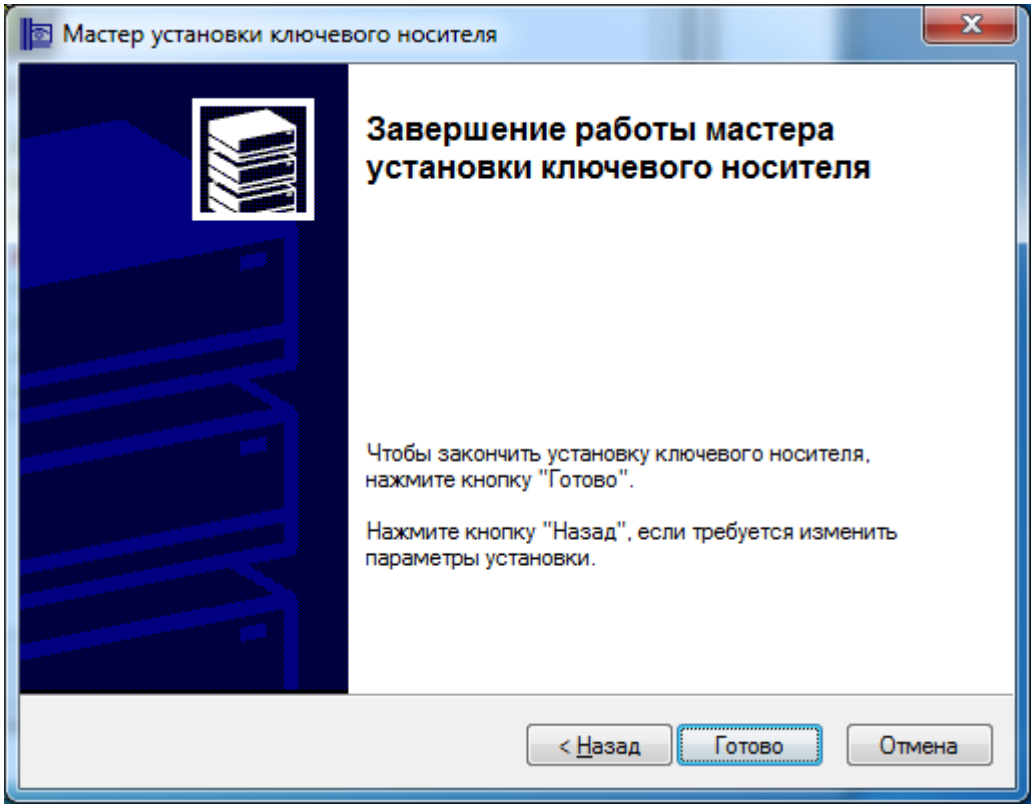


Рис. 23. Завершение мастера установки ключевого носителя

2.4.2.2. Удаление ключевого носителя

Для того чтобы сделать недоступным ключевой носитель, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование.** В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить типы носителей.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 18). Выберите ключевой носитель, который требуется удалить, и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление ключевого носителя» (см. Рис. 24). Нажмите кнопку **Да**. Ключевой станет недоступным.

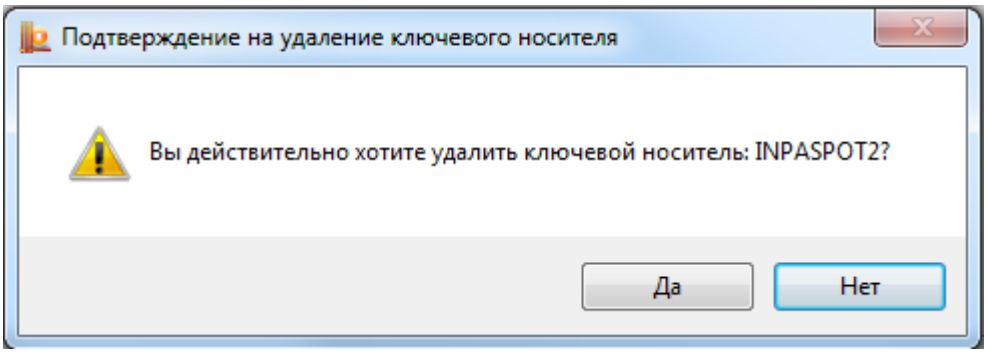


Рис. 24. Окно «Подтверждение на удаление ключевого носителя»

2.4.2.3. Просмотр свойств ключевого носителя

Для того чтобы просмотреть свойства ключевого носителя, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP** и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить носители.**

Система отобразит окно «Управление ключевыми носителями» (см. Рис. 18). Выберите ключевой носитель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя носителя» (см. Рис. 25), в котором отображается справочная информация о выбранном ключевом носителе, в том числе, и данные о состоянии устройства. После просмотра свойств ключевого носителя нажмите кнопку **ОК.**

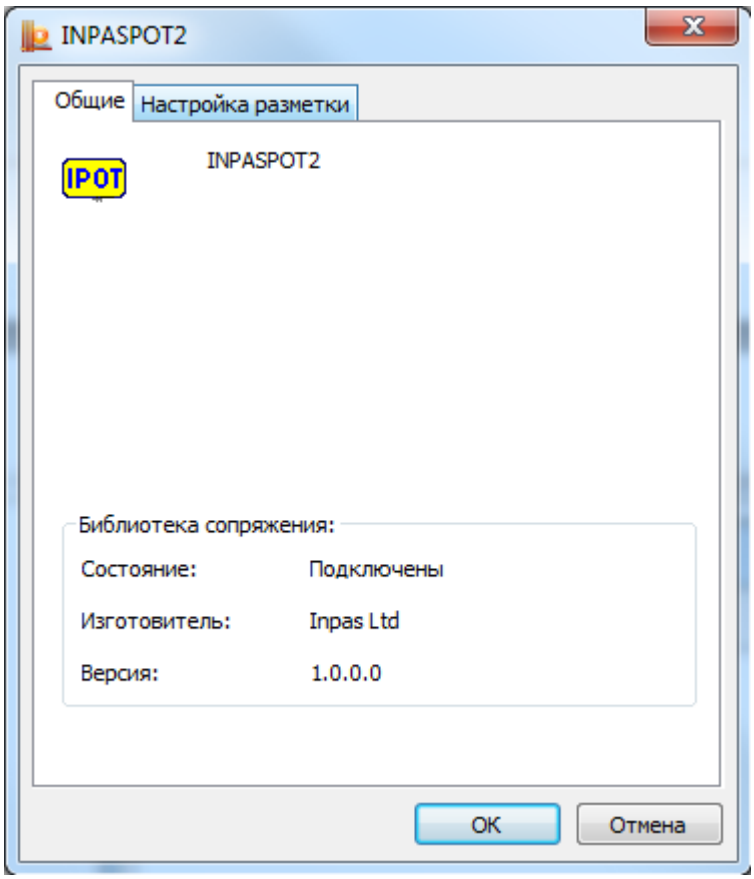


Рис. 25. Окно «Свойства: имя носителя»

2.4.3. Настройка датчиков случайных чисел (ДСЧ)

2.4.3.1. Добавление ДСЧ

При настройке ДСЧ и загрузке динамических библиотек должно быть установлено программное обеспечение, соответствующее аппаратному средству. Подключение ДСЧ должно соответствовать установкам программно-аппаратного комплекса.

Для того чтобы добавить ДСЧ, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 26).

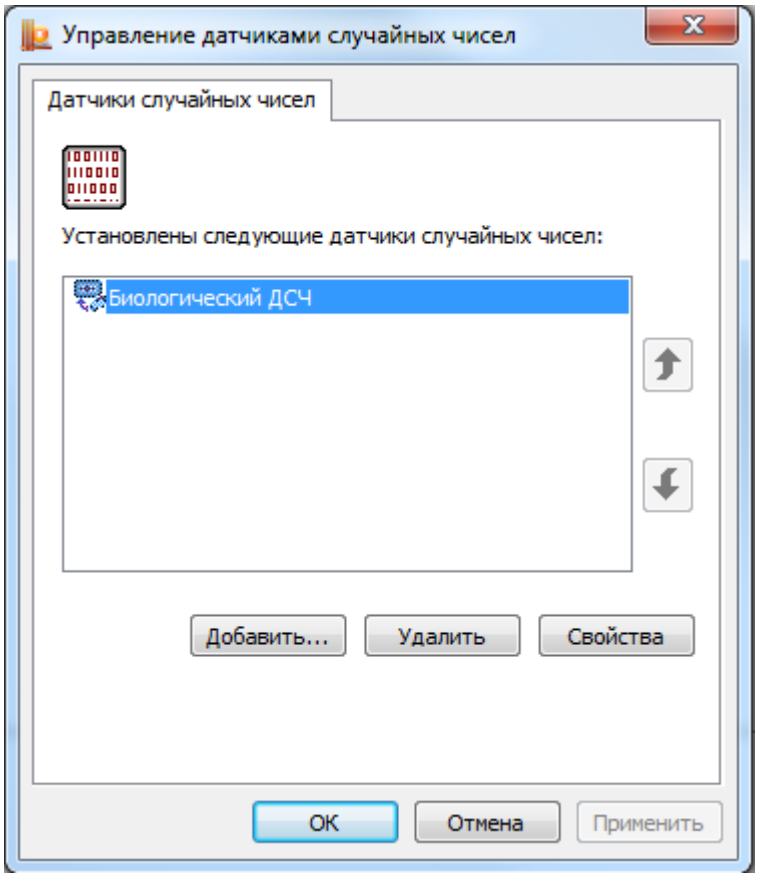


Рис. 26. Окно «Управление датчиками случайных чисел»

Для того чтобы добавить ДСЧ, нажмите кнопку **Добавить**. Произойдет запуск Мастера установки ДСЧ (см. Рис. 27). В окне мастера установки нажмите кнопку **Далее**.

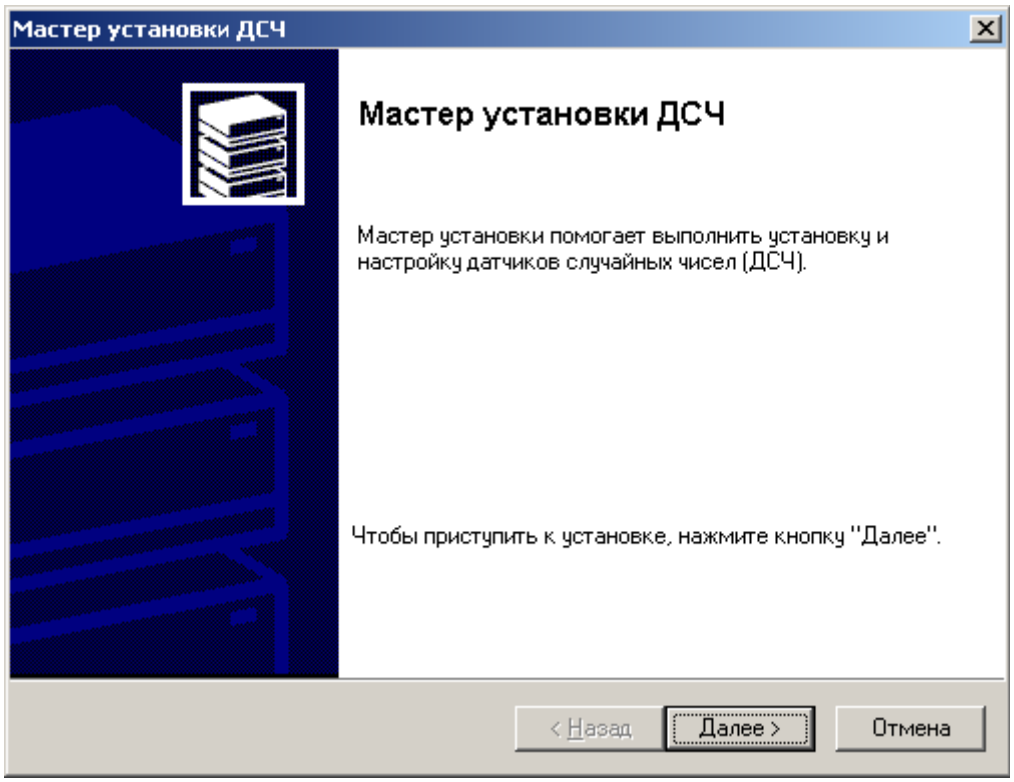


Рис. 27. Запуск мастера установки ДСЧ

Система отобразит окно «Выбор ДСЧ» (см. Рис. 28). В этом окне выберите датчик случайных чисел, который следует добавить и нажмите кнопку **Далее.**

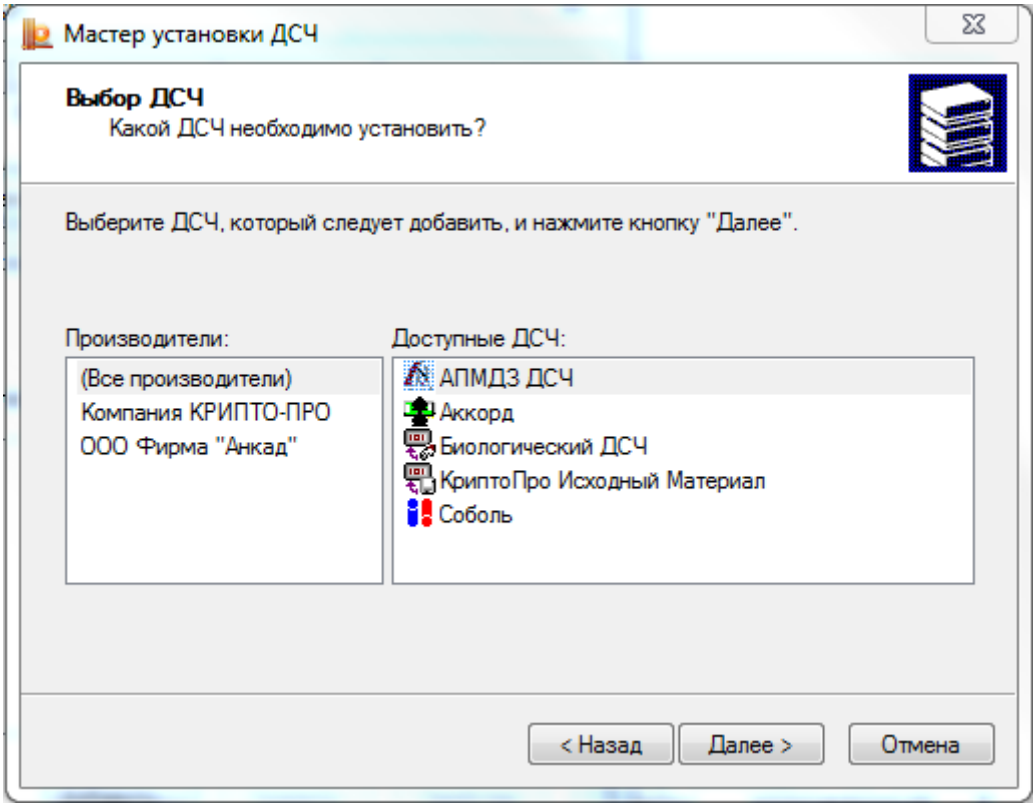


Рис. 28. Окно «Выбор ДСЧ»

Система отобразит окно «Имя ДСЧ» (см. Рис. 29). В этом окне введите имя выбранного датчика случайных чисел и нажмите кнопку **Далее.**

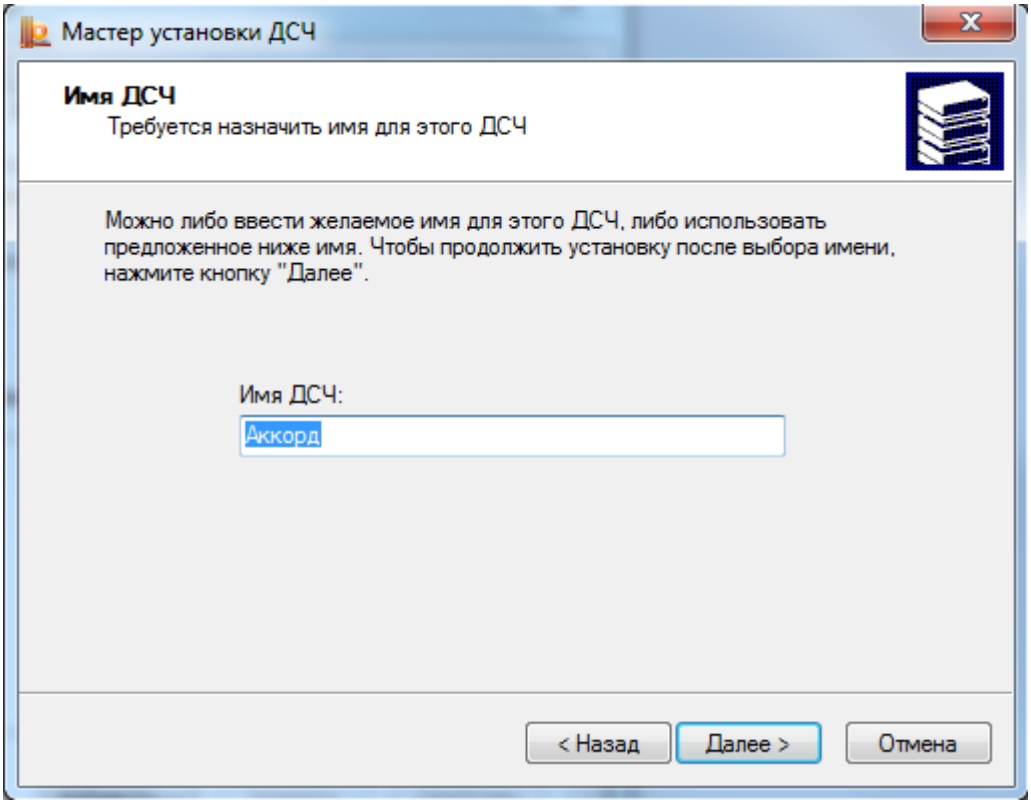


Рис. 29. Окно «Имя ДСЧ»

Система отобразит окно «Завершение работы мастера установки ДСЧ» (см. Рис. 30). Нажмите в нем кнопку **Готово** и перезагрузите компьютер**.**

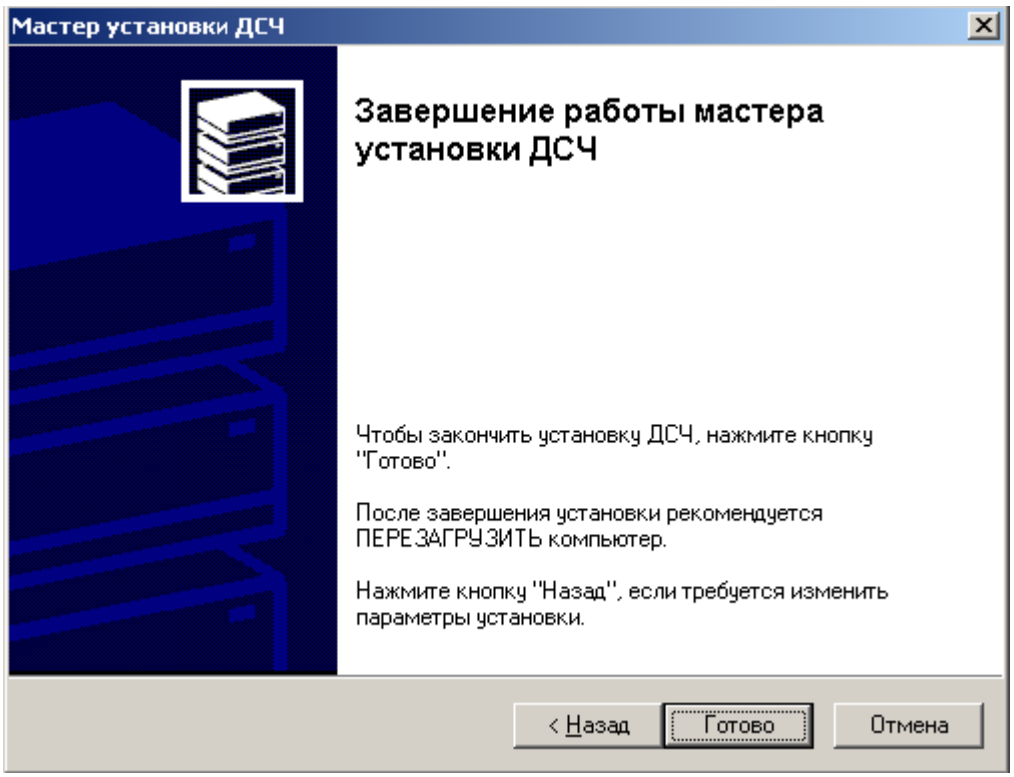


Рис. 30. Завершение мастера установки ДСЧ

2.4.3.2. Удаление ДСЧ

Для того чтобы удалить ДСЧ, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5) то нажмите её и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 26). Выберите датчик, который требуется удалить и нажмите кнопку **Удалить.**

Система отобразит окно «Подтверждение на удаление датчика случайных чисел» (см. Рис. 31). Нажмите кнопку **Да**. Датчик случайных чисел будет удален.

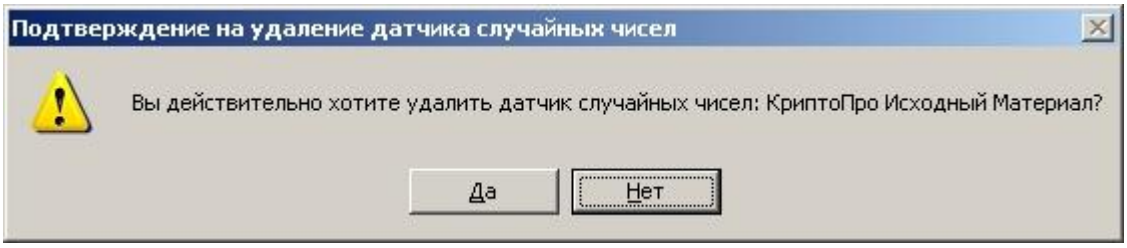


Рис. 31. Окно «Подтверждение на удаление ДСЧ»

2.4.3.3. Просмотр свойств ДСЧ

Для того чтобы просмотреть свойства ДСЧ, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP** и перейдите на вкладку Оборудование. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рис. 9) нажмите кнопку **Настроить ДСЧ.**

Система отобразит окно «Управление датчиками случайных чисел» (см. Рис. 26). Выберите датчик, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Система отобразит окно «Свойства: Имя ДСЧ» (см. Рис. 32), 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.**

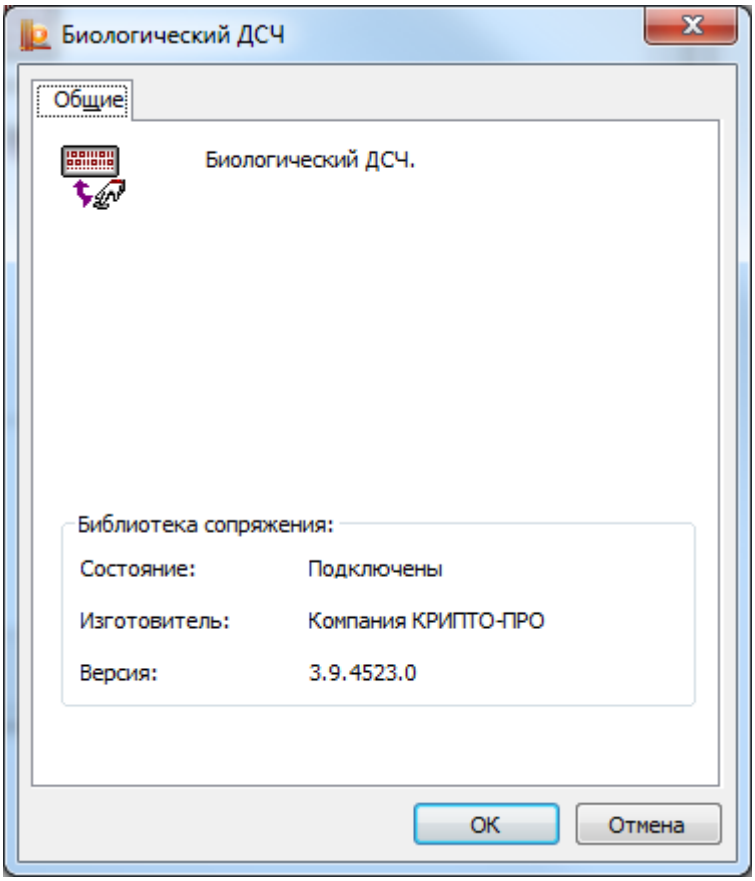


Рис. 32. Окно «Свойства: имя ДСЧ»

Примечание. Если в СКЗИ 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.

2.5. Работа с контейнерами и сертификатами

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

- Копирование и удаление закрытого ключа, находящегося в существующем контейнере;
- Тестирование (проверка работоспособности) и отображение свойств ключа (ключей) и сертификата (сертификатов) в существующем контейнере;
- Просмотр и установка сертификата, находящегося в существующем контейнере закрытого ключа на носителе;
- Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе;
- Изменение и удаление сохраненных паролей (PIN-кодов) доступа к носителям закрытых ключей;
- Очистка информации о ранее использованных съёмных носителях, на которых располагались контейнеры закрытых ключей.

2.5.1. Тестирование, копирование и удаление контейнера закрытого ключа

2.5.1.1. Тестирование контейнера закрытого ключа

Для того чтобы провести тест работоспособности контейнера закрытого ключа, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33). Нажмите кнопку **Протестировать.**

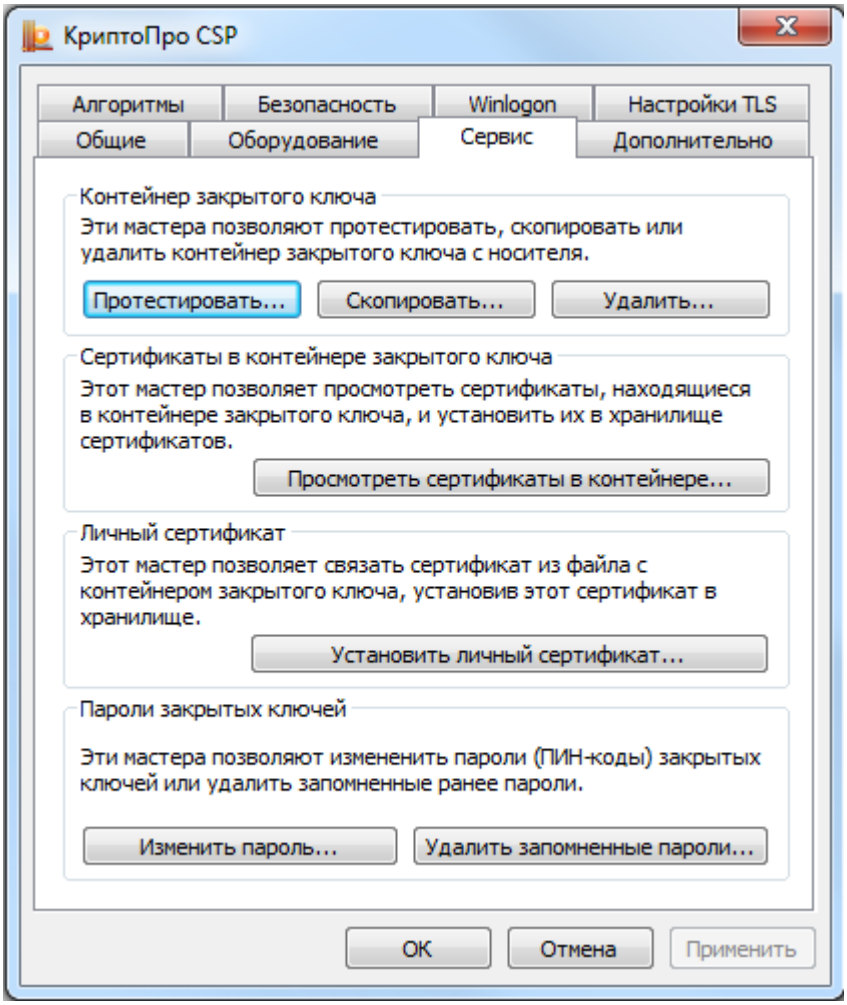


Рис. 33. Контрольная панель. Вкладка «Сервис»

Система отобразит окно «Тестирование контейнера закрытого ключа» (см. Рис. 34).

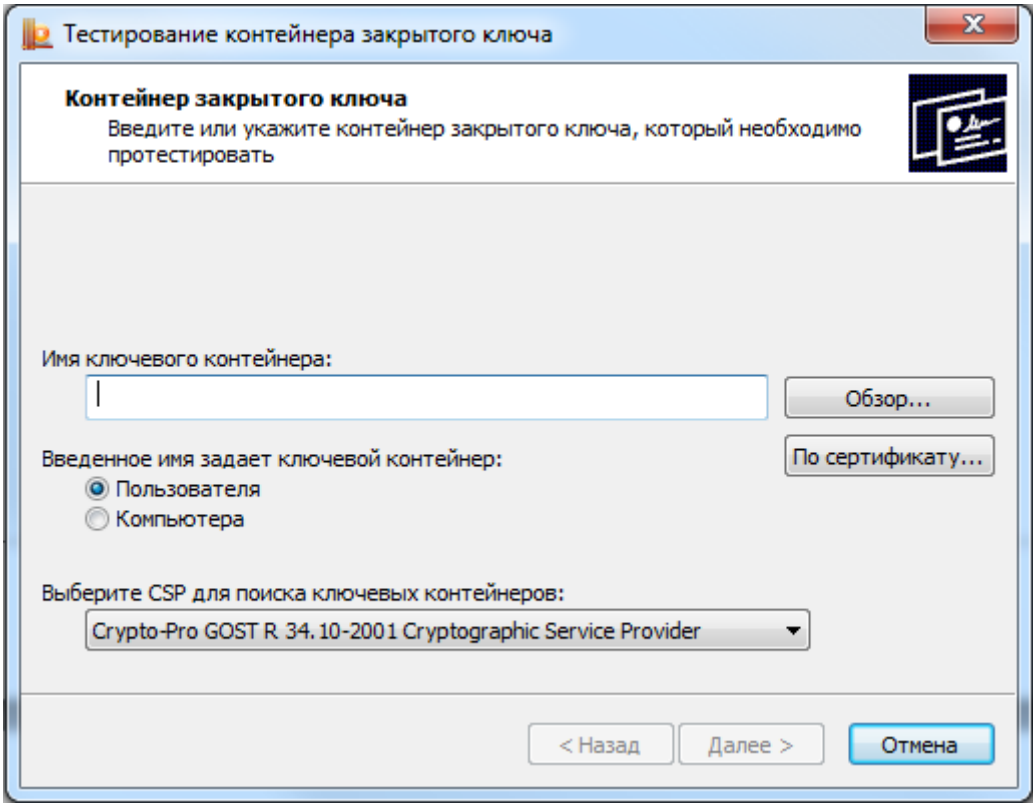


Рис. 34. Окно «Тестирование контейнера закрытого ключа»

В этом окне необходимо заполнить следующее поле ввода:

• **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор.**

Опции поиска:

- **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.

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя или, если есть права администратора, локального компьютера, тот, контейнер которого необходимо протестировать (см. Рис. 38);

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 итоговое окно мастера «Тестирование контейнера закрытого ключа» (см. Рис. 35), в котором будет выведена информация о данном контейнере и результат теста.

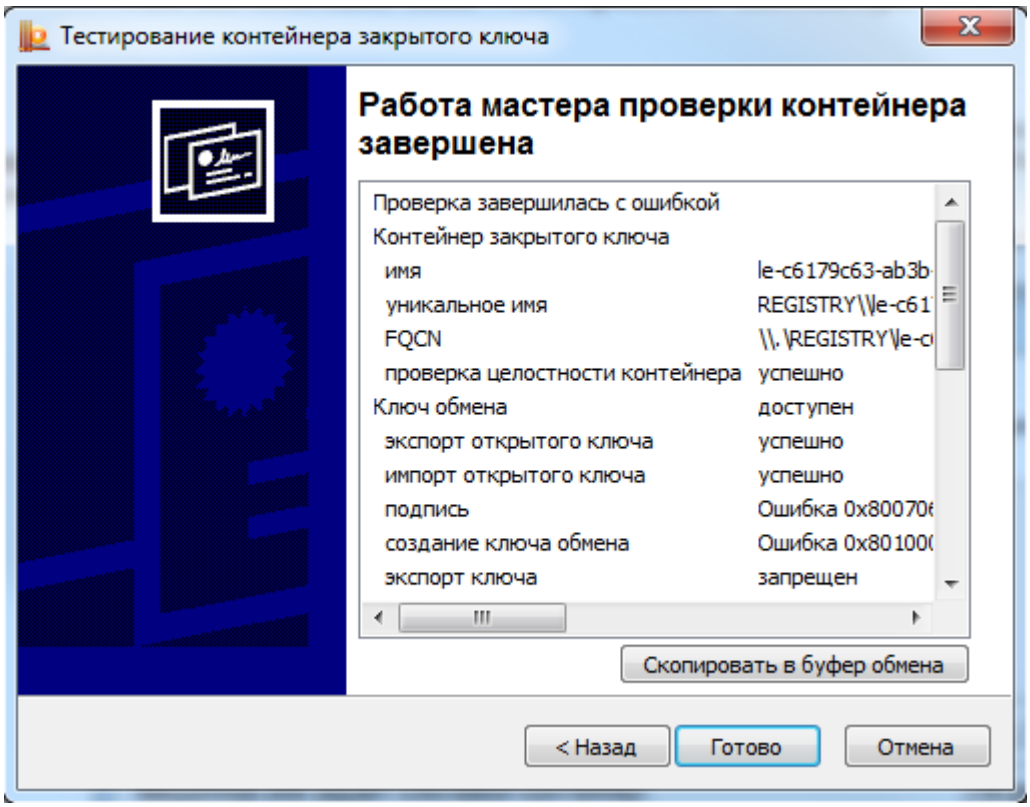


Рис. 35. Итоговое окно «Тестирование контейнера закрытого ключа»

2.5.1.2. Копирование контейнера закрытого ключа

Для того чтобы скопировать контейнер закрытого ключа, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33). Нажмите кнопку **Скопировать**.

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

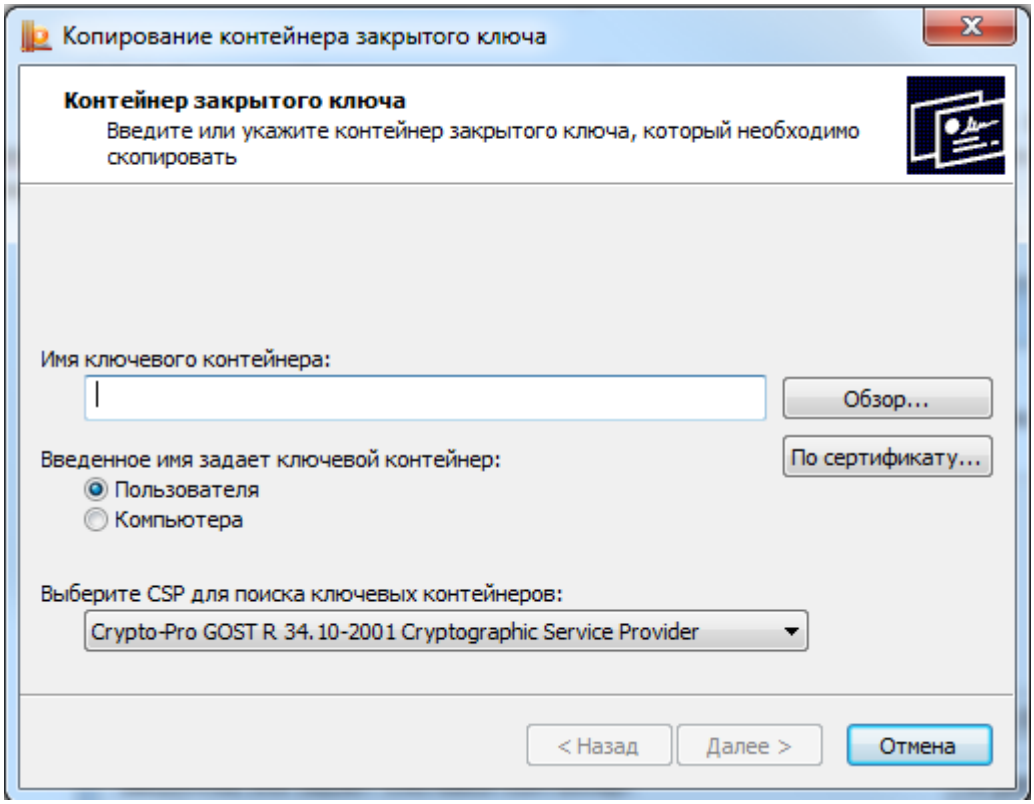


Рис. 36. Окно «Копирование контейнера закрытого ключа»

В этом окне необходимо заполнить следующее поле ввода:

• **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор.**

Опции поиска:

- **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.

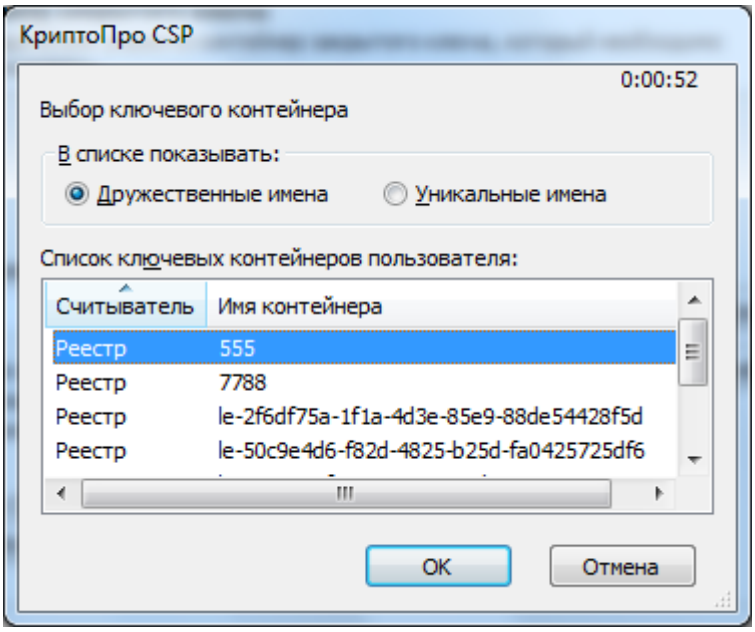


Рис. 37. Выбор ключевого контейнера

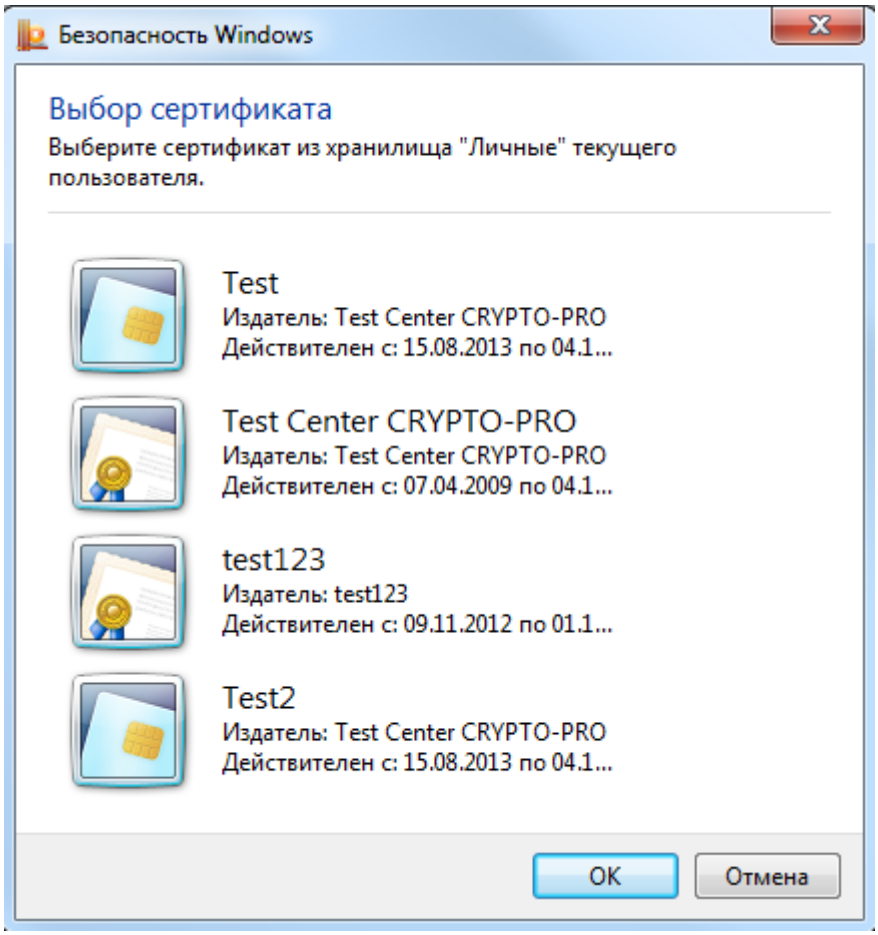


Рис. 38. Выбор сертификата

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя или, если есть права администратора, локального компьютера, тот, контейнер которого необходимо скопировать (см. Рис. 38);

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. 39), 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.

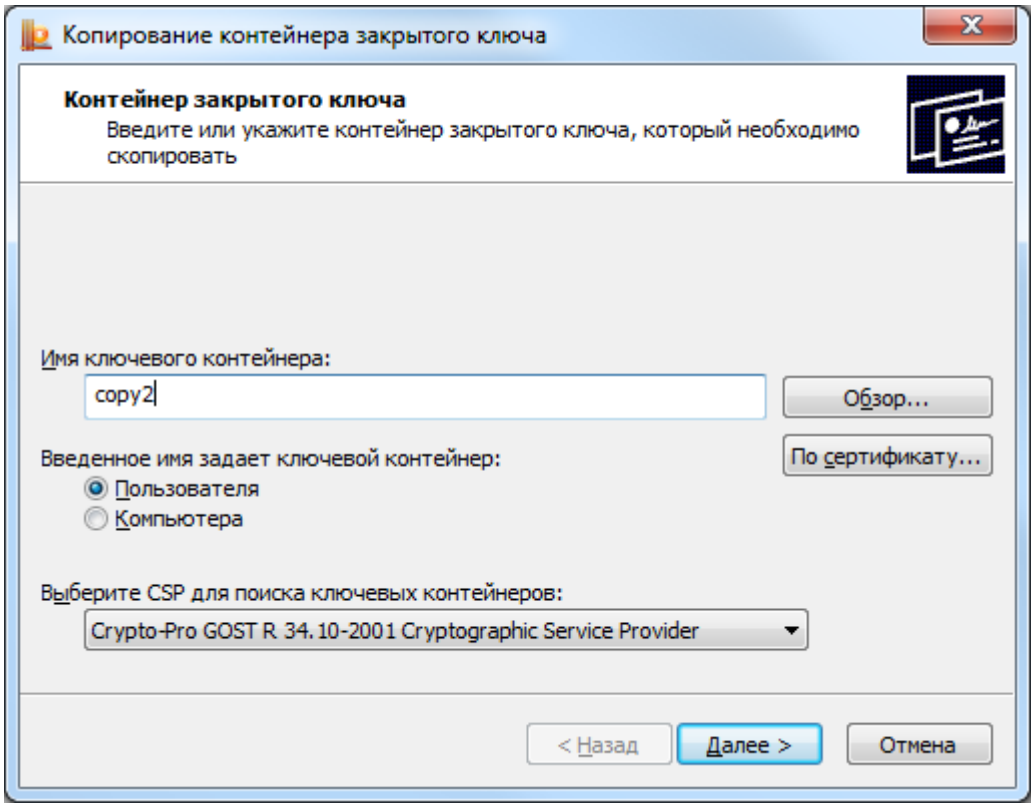


Рис. 39. Окно «Копирование контейнера закрытого ключа»

После ввода нажмите кнопку **Готово**. Система отобразит окно, в котором необходимо выбрать носитель для скопированного контейнера (см. Рис. 40).

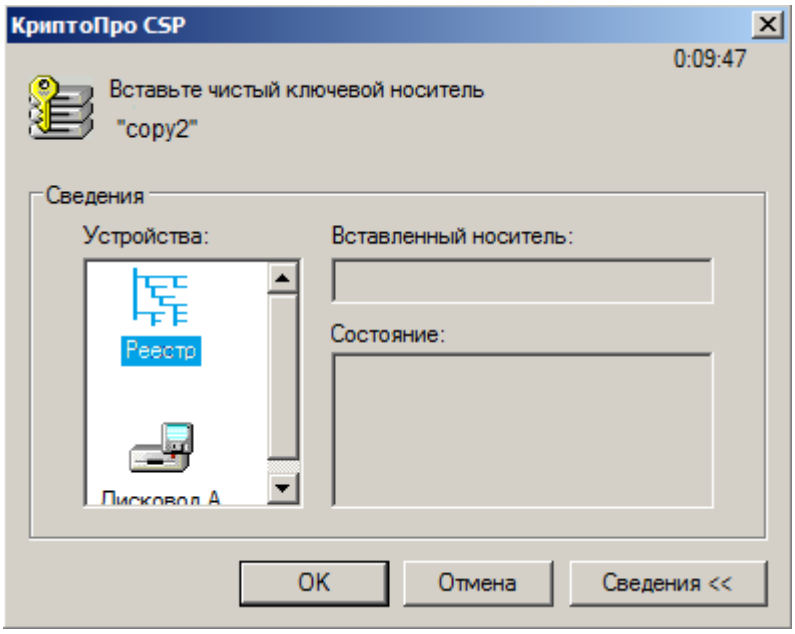


Рис. 40. Окно выбора носителя

Вставьте носитель в считыватель и нажмите кнопку **ОК**. Система отобразит окно установки пароля на доступ к закрытому ключу (см. Рис. 41). Введите пароль, подтвердите его, при необходимости установите флаг **Сохранить 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).

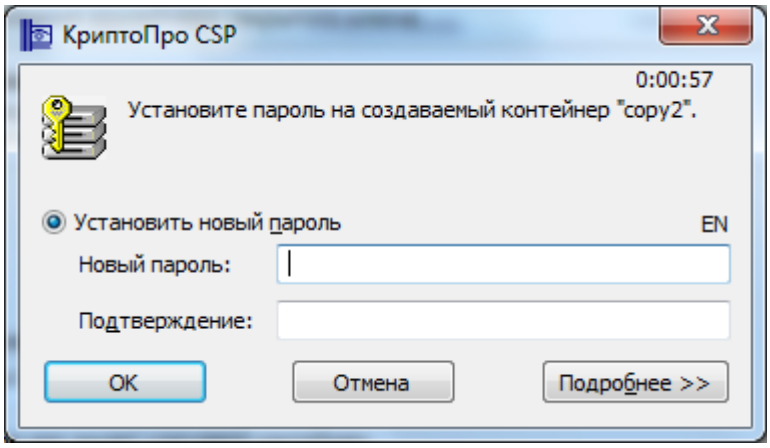


Рис. 41. Окно ввода пароля

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

2.5.1.3. Удаление контейнера закрытого ключа

Для того чтобы удалить контейнер закрытого ключа выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33), нажмите кнопку **Удалить контейнер**.

Система отобразит окно «Удаление контейнера закрытого ключа» (см. Рис. 42).

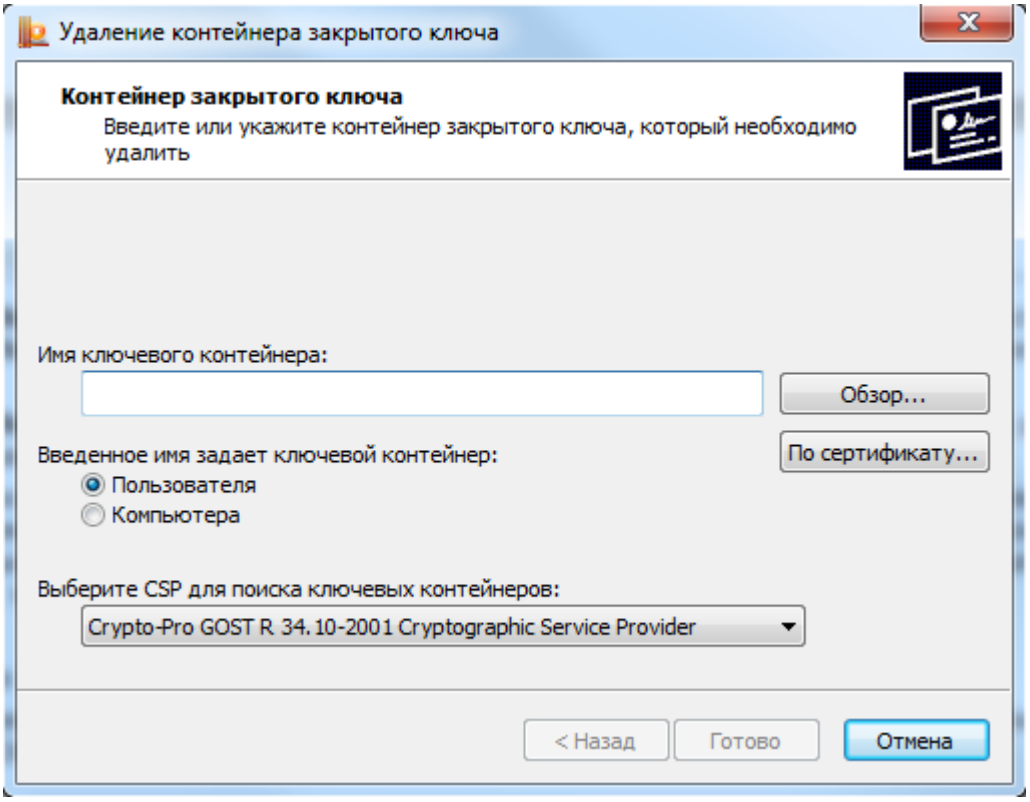


Рис. 42. Окно «Удаление контейнера закрытого ключа»

В этом окне необходимо заполнить следующее поле ввода:

• **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор.**

Опции поиска:

- **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.

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя или, если есть права администратора, локального компьютера, тот, контейнер которого необходимо скопировать (см. Рис. 38);

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

Система отобразит окно подтверждения удаления ключевого контейнера (см. Рис. 43). Нажмите кнопку **Да.** СКЗИ «КриптоПро CSP» произведет удаление ключевого контейнера.

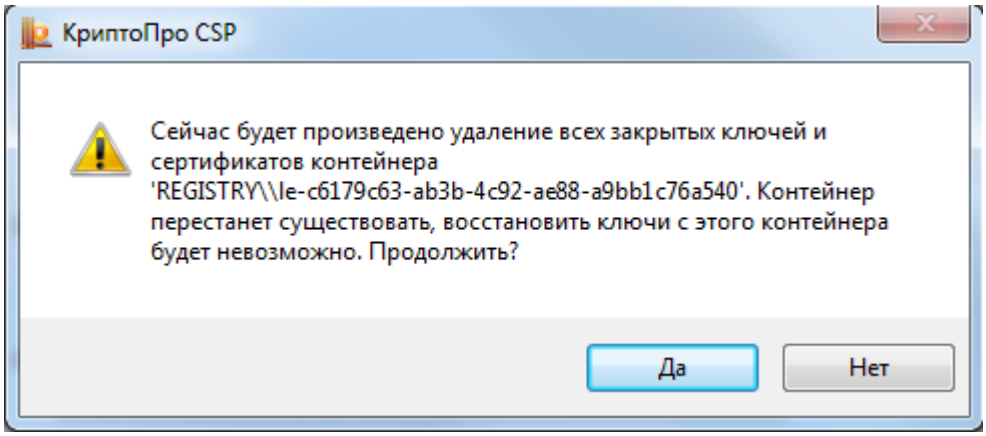


Рис. 43. Окно подтверждения удаления ключевого контейнера

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

2.5.2.1. Просмотр сертификата, хранящегося в контейнере закрытого ключа

Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33), нажмите кнопку **Просмотреть сертификаты в контейнере**.

Система отобразит окно «Сертификаты в контейнере закрытого ключа» (см. Рис. 44).

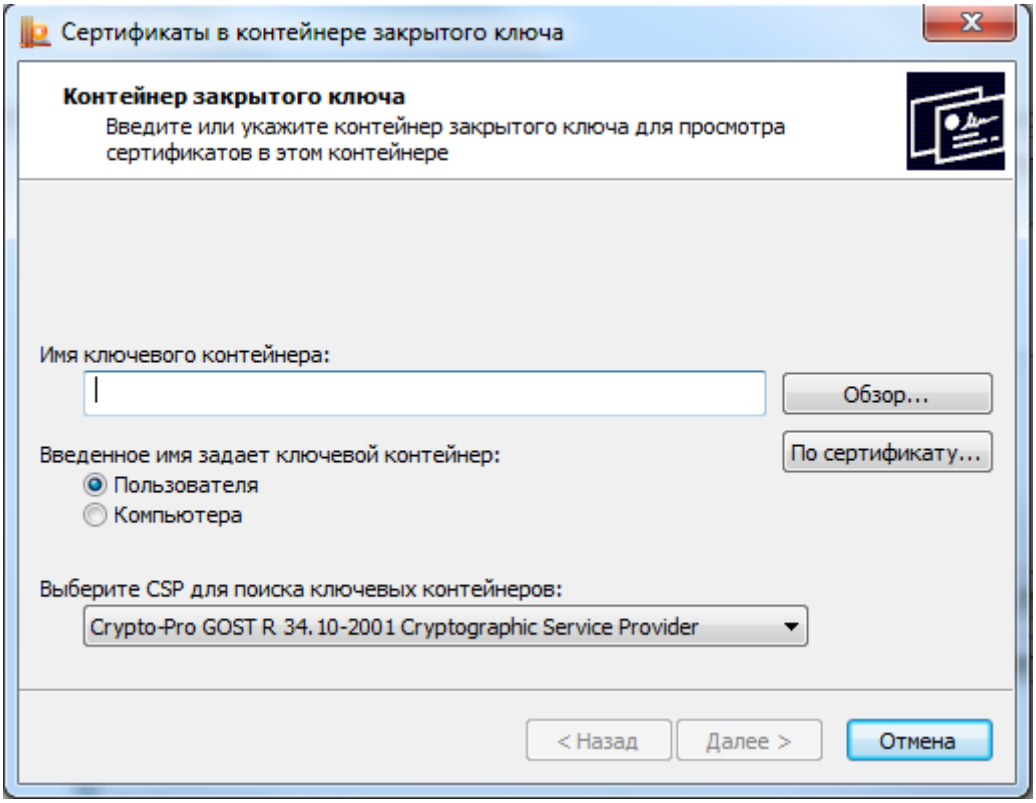


Рис. 44. Окно «Сертификаты в контейнере закрытого ключа»

В нем необходимо заполнить следующее поле ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор.**

Опции поиска:

- **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.

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя и локального компьютера, тот, контейнер которого нужно просмотреть (см. Рис. 36);

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

Если контейнер был сделан на компьютере с КриптоПро CSP версии 3.9 и на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Если сертификата в контейнере закрытого ключа нет, то система отобразит окно, информирующее пользователя об отсутствии сертификата в контейнере (см. Рис. 45).

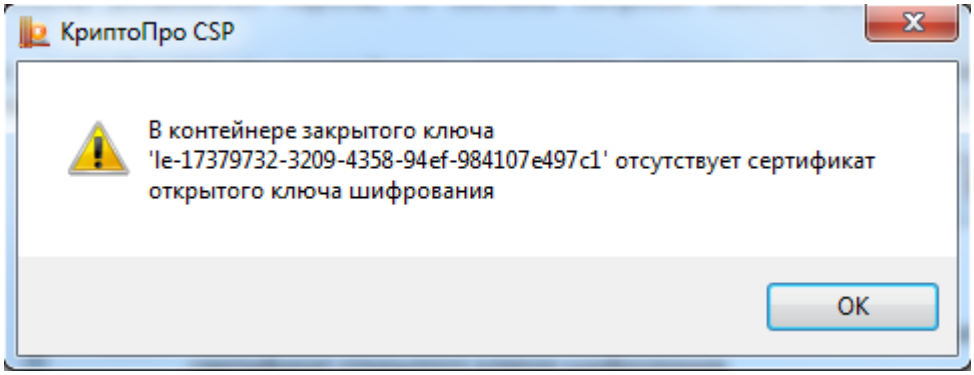


Рис. 45. Окно, информирующее об отсутствии сертификата

Если сертификат в выбранном контейнере имеется, то система отобразит окно «Сертификат для просмотра» (см. Рис. 46).

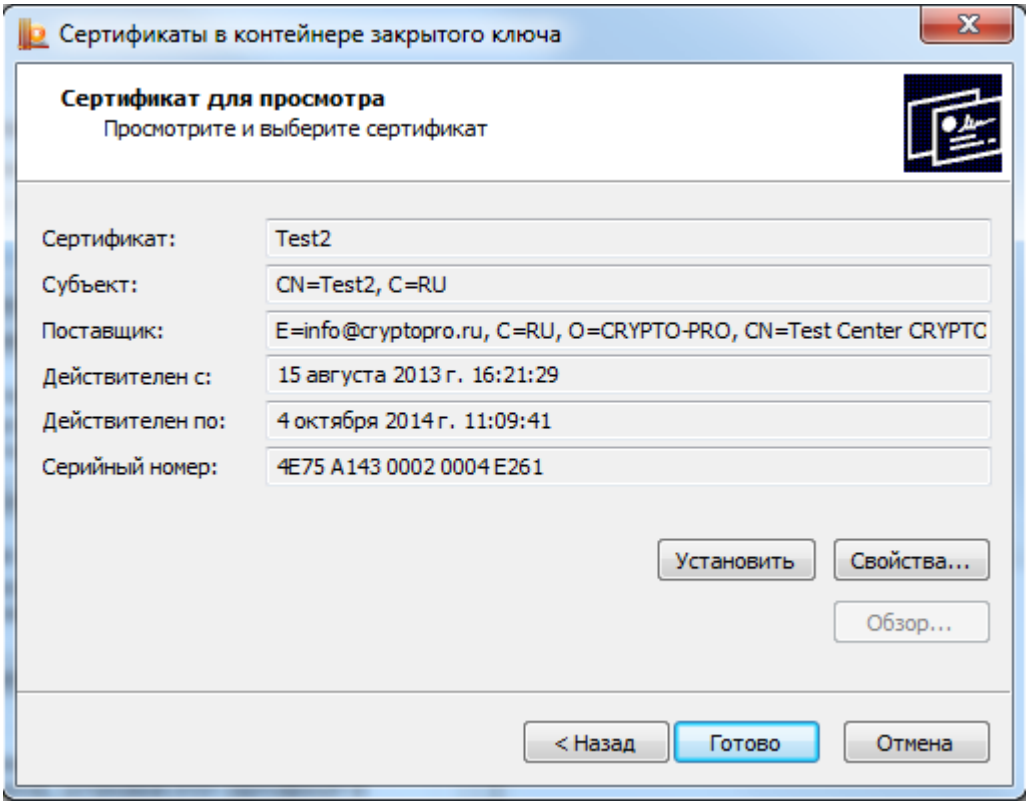


Рис. 46. Окно «Сертификаты в контейнере закрытого ключа»

Для просмотра основных свойств сертификата нажмите кнопку **Свойства** в окне «Сертификаты в контейнере закрытого ключа» (см. Рис. 46). Система отобразит свойства сертификата (см. Рис. 47).

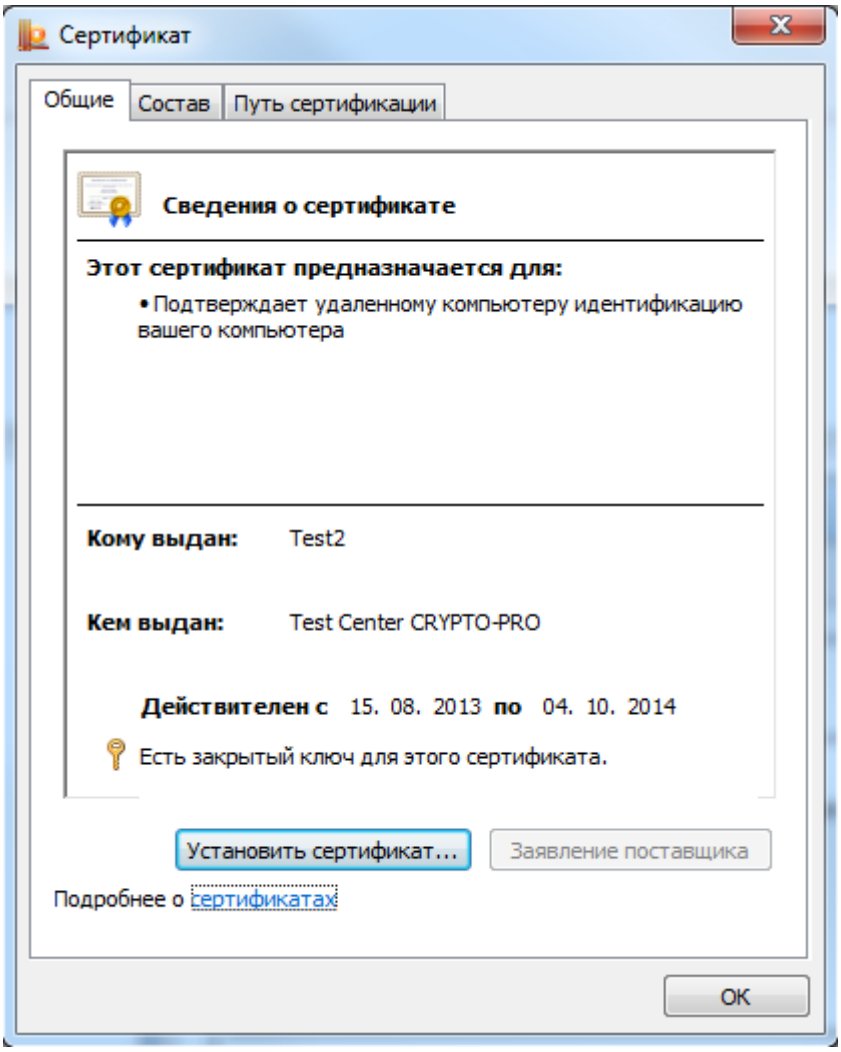


Рис. 47. Окно просмотра свойств сертификата

2.5.2.2. 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 также 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 2.5.2.1.

В окне «Сертификаты в контейнере закрытого ключа» (см. Рис. 46) нажмите кнопку **Установить**.

Сертификат будет установлен в хранилище «Личные» текущего пользователя или компьютера, в зависимости от опции, выбранной при поиске контейнера.

Если сертификат уже есть в хранилище, будет выдано предупреждение о перезаписи прежнего сертификата (см. Рис. 48).

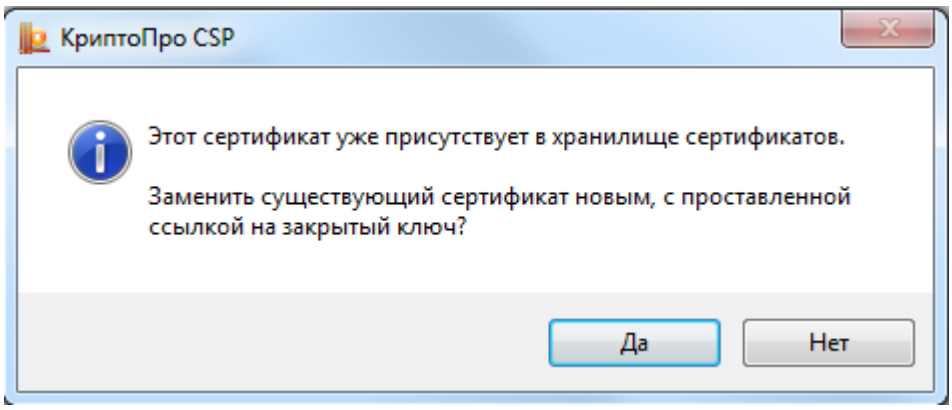


Рис. 48. Предупреждение о перезаписи сертификата

В случае успеха будет выдано окно о завершении операции (см. Рис. 49).

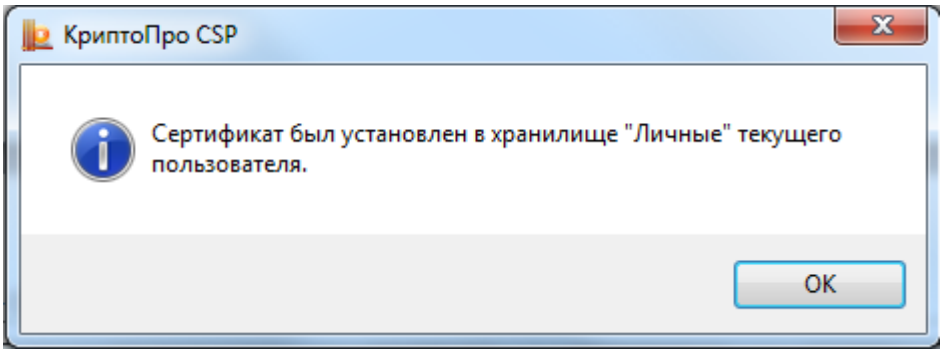


Рис. 49. Окно завершения установки сертификата

2.5.3. Установка личного сертификата, хранящегося в файле

Примечание. В данном разделе инструкции 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 выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33), нажмите кнопку **Установить личный сертификат**.

Система отобразит окно «Расположение файла сертификата» (см. Рис. 50). В поле **Имя файла сертификата** укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее.**

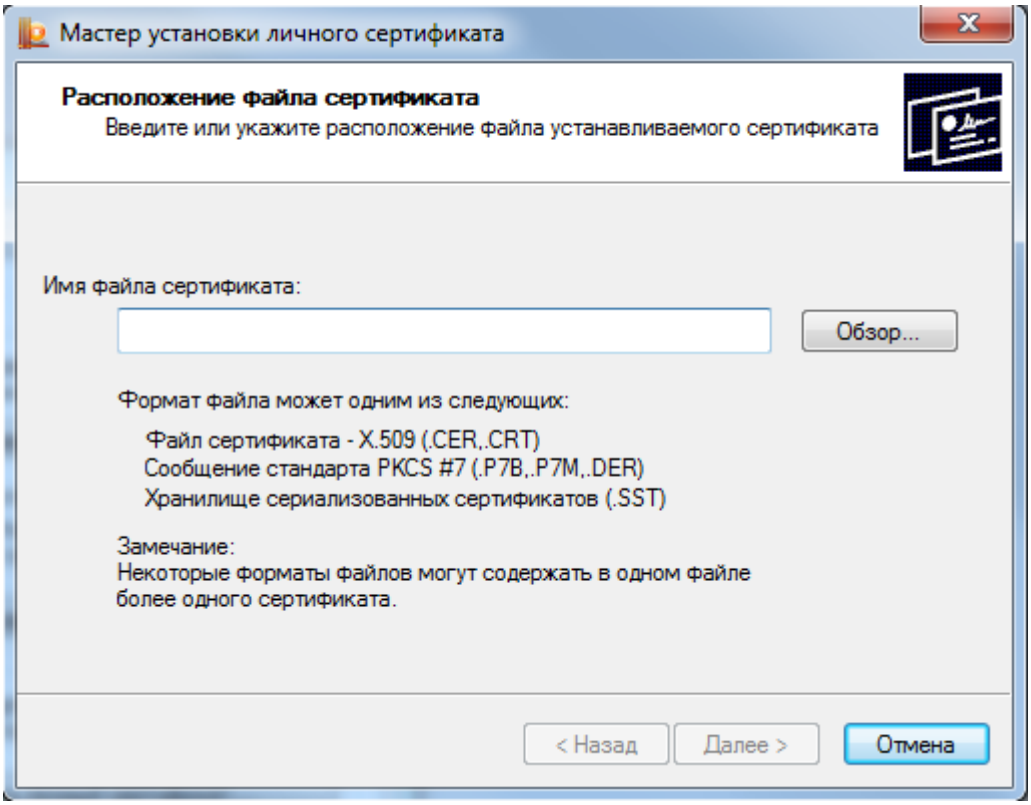


Рис. 50. Окно «Расположение файлов сертификата»

Система перейдет к окну «Сертификат для установки» (см. Рис. 51). В нем выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

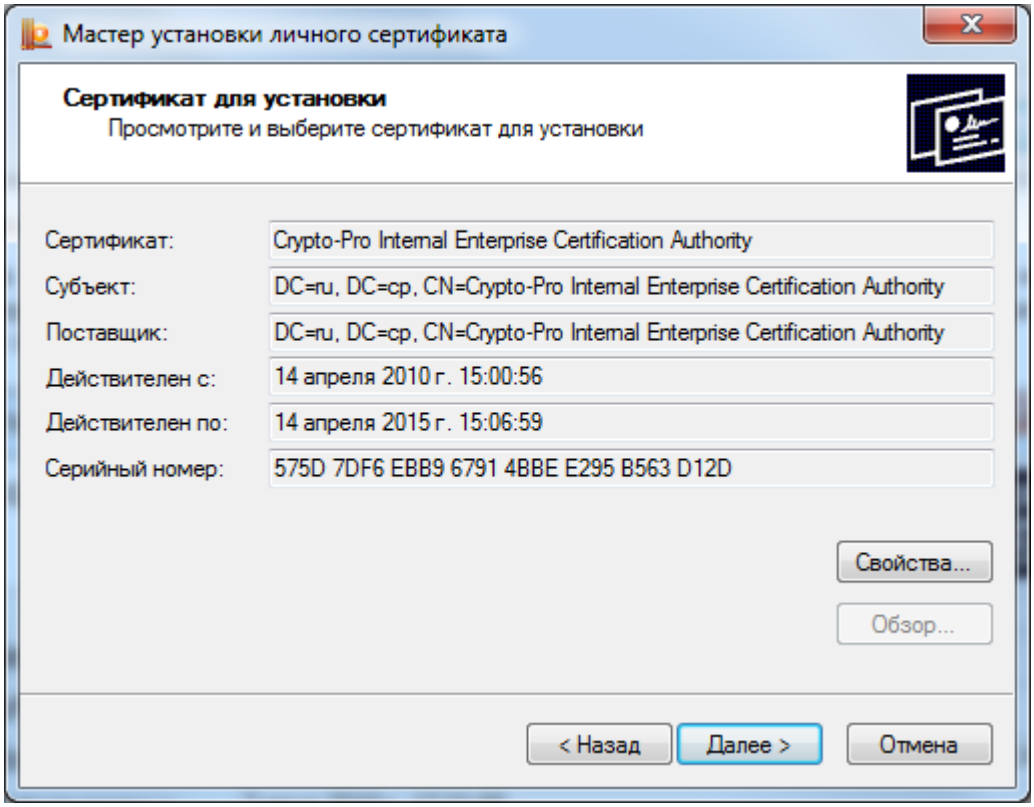


Рис. 51. Окно «Сертификат для установки»

Нажмите кнопку Далее. Система отобразит окно «Контейнер закрытого ключа» (см. Рис. 52).

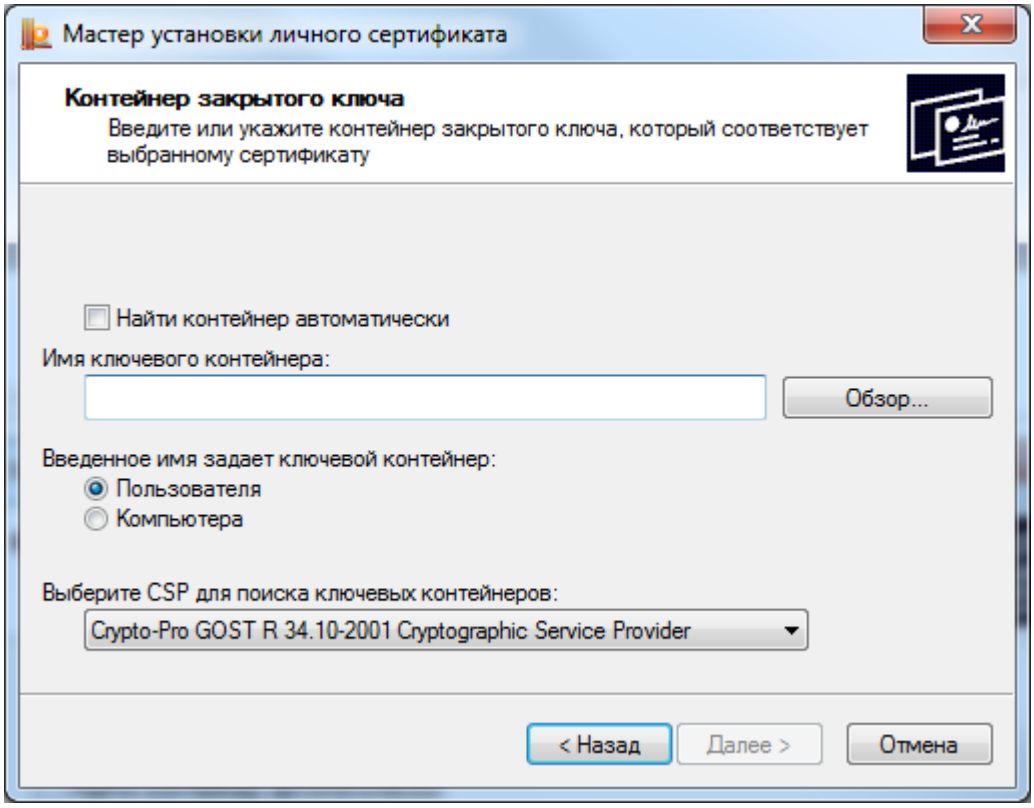


Рис. 52. Окно «Контейнер закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Найти контейнер автоматически** – проводит поиск подходящего контейнера среди доступных контейнеров, если контейнер найден, то его имя будет подставлено сразу;
- **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. 53).

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)

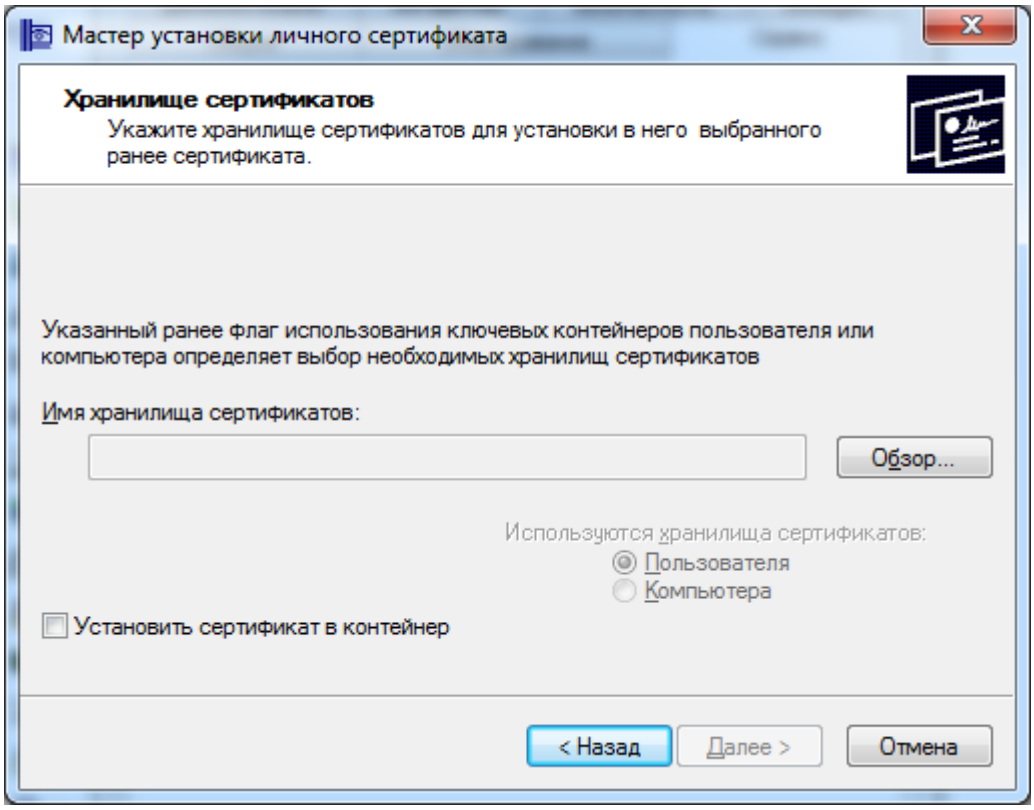


Рис. 53. Окно «Хранилище сертификатов»

Одновременно сертификат можно записать в ключевой контейнер для удобства поиска сертификата при переносе контейнера на другой компьютер. Для этого служит опция «Установить сертификат в контейнер» (см. Рис. 53).

После выбора хранилища система отобразит окно «Завершение работы мастера установки личного сертификата» (см. Рис. 54).

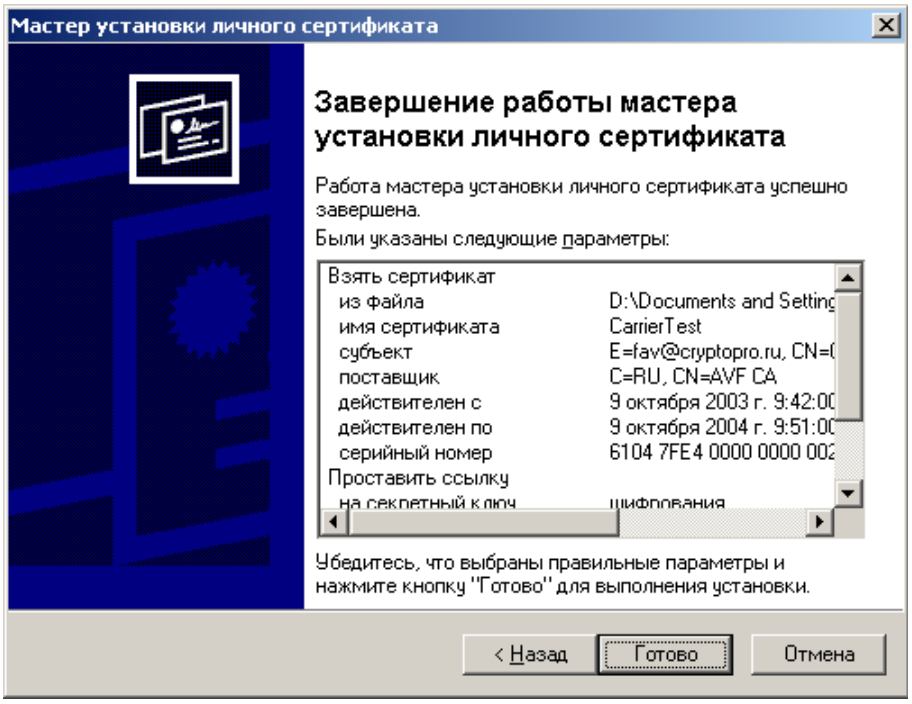


Рис. 54. Завершение работы мастера установки личного сертификата

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

2.5.4. Управление паролями доступа к закрытым ключам

2.5.4.1. Изменение пароля на доступ к закрытому ключу

Для того чтобы изменить пароль на контейнер, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33), нажмите кнопку **Изменить пароль**.

Система отобразит окно «Контейнер закрытого ключа» (см. Рис. 55).

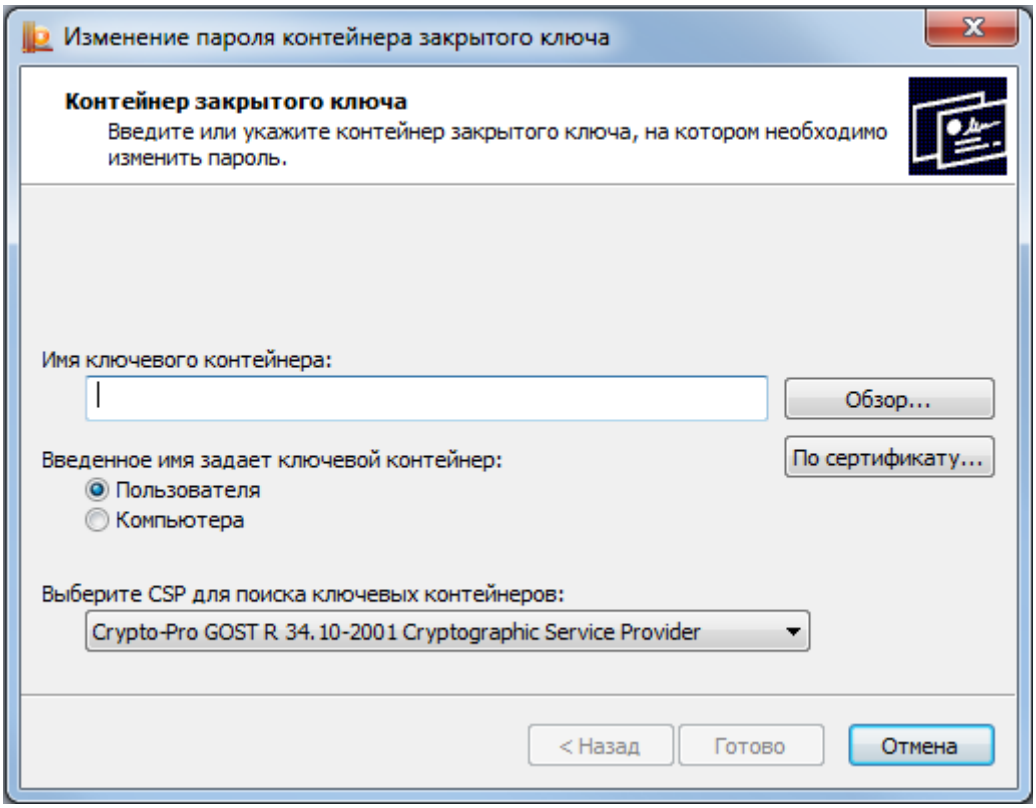


Рис. 55. Окно «Контейнер закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

- **Имя ключевого контейнера** – вводится вручную или выбирается из списка (см. Рис. 37) посредством нажатия кнопки **Обзор.** Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя и локального компьютера, тот, контейнер которого нужно просмотреть (см. Рис. 38);
- **Введенное имя задает ключевой контейнер** – переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически;
- **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. 56). Введите указанный пароль и нажмите кнопку **ОК.**

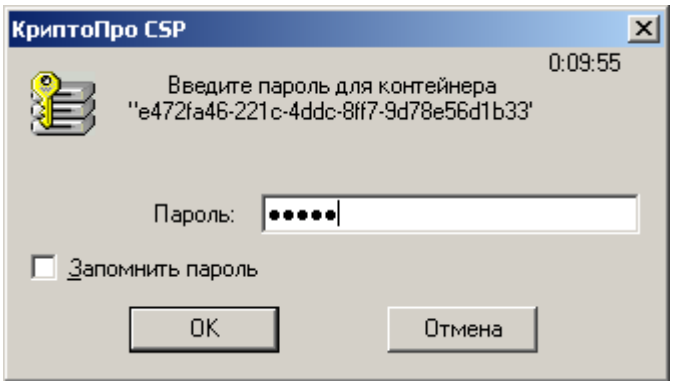


Рис. 56. Ввод пароля на доступ

Если пароль введен верно, то система отобразит окно ввода нового пароля на доступ к закрытому ключу (см. Рис. 57). Введите дважды новый пароль и нажмите кнопку **ОК.**

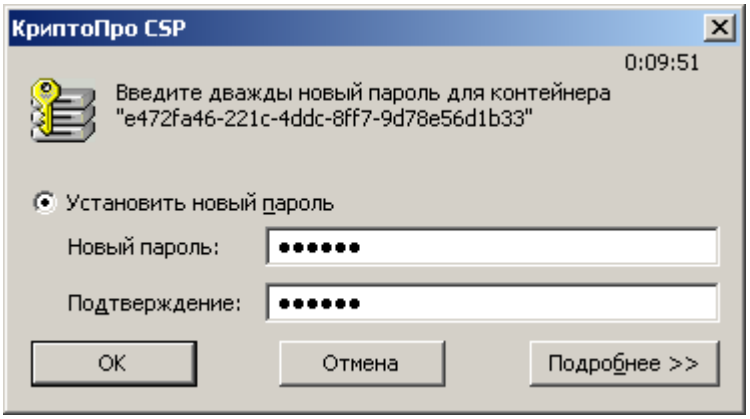


Рис. 57. Ввод нового пароля

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 описано в пункте 3.1.5.

2.5.4.2. 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 выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 33), нажмите кнопку **Удалить запомненные пароли.**

Система отобразит окно «Удаление запомненных паролей» (см. Рис. 58).

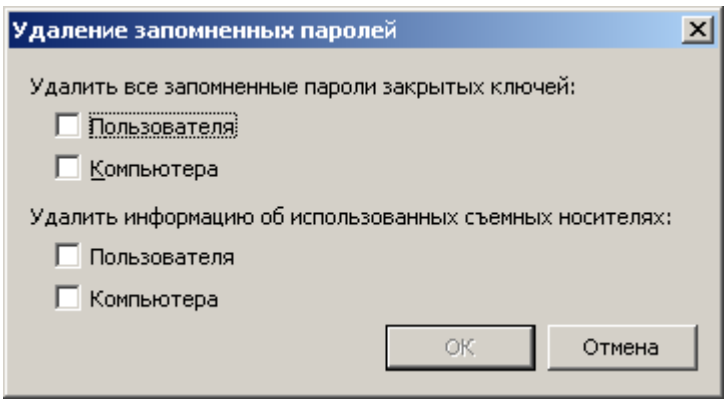


Рис. 58. Окно «Удаление запомненных паролей»

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.

Кроме того, в этом же окне можно отдельно удалить информацию о физических характеристиках носителей, на которых расположены ключевые контейнеры, использовавшиеся ранее на данном компьютере. Это полезно, если ключевой контейнер на новом носителе имеет то же имя, что один из ранее использовавшихся на данном компьютере контейнеров.

2.6. Установка параметров безопасности

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

Для того чтобы установить параметры безопасности, выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP.** Если активна ссылка «Запустить с правами администратора» (см. Рис. 5), то нажмите её и перейдите на вкладку **Безопасность** (см. Рис. 59).

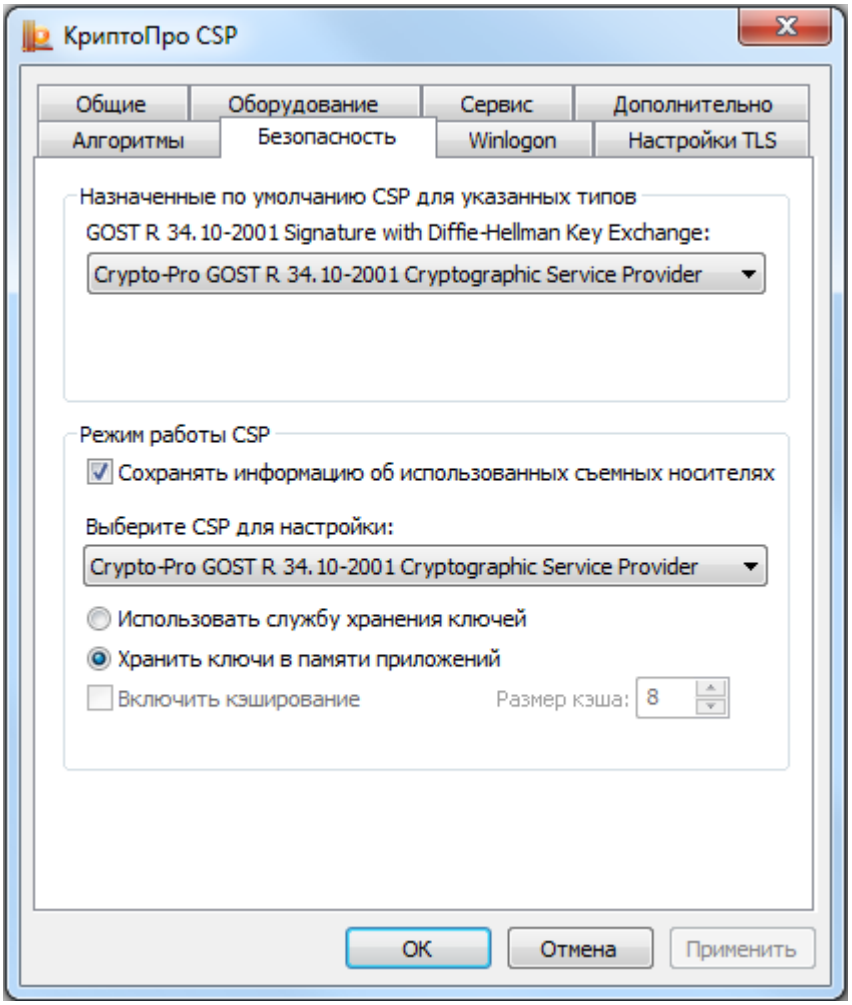


Рис. 59. Контрольная панель. Вкладка «Безопасность»

Если СКЗИ «КриптоПро CSP» сертифицирован по уровню КС1, то на вкладке Безопасность можно выбрать режим работы: с хранением ключей в памяти приложений либо с хранением ключей в службе хранения ключей. При хранении ключей в службе хранения ключей все операции с закрытым ключом производятся внутри службы, внешнему приложению выдается только результат, что более безопасно, чем хранить ключи непосредственно в памяти приложений. В исполнениях СКЗИ, сертифицированных по уровню КС2 или КС3, режим работы с хранением ключей в службе является единственным доступным (см. Рис. 60).

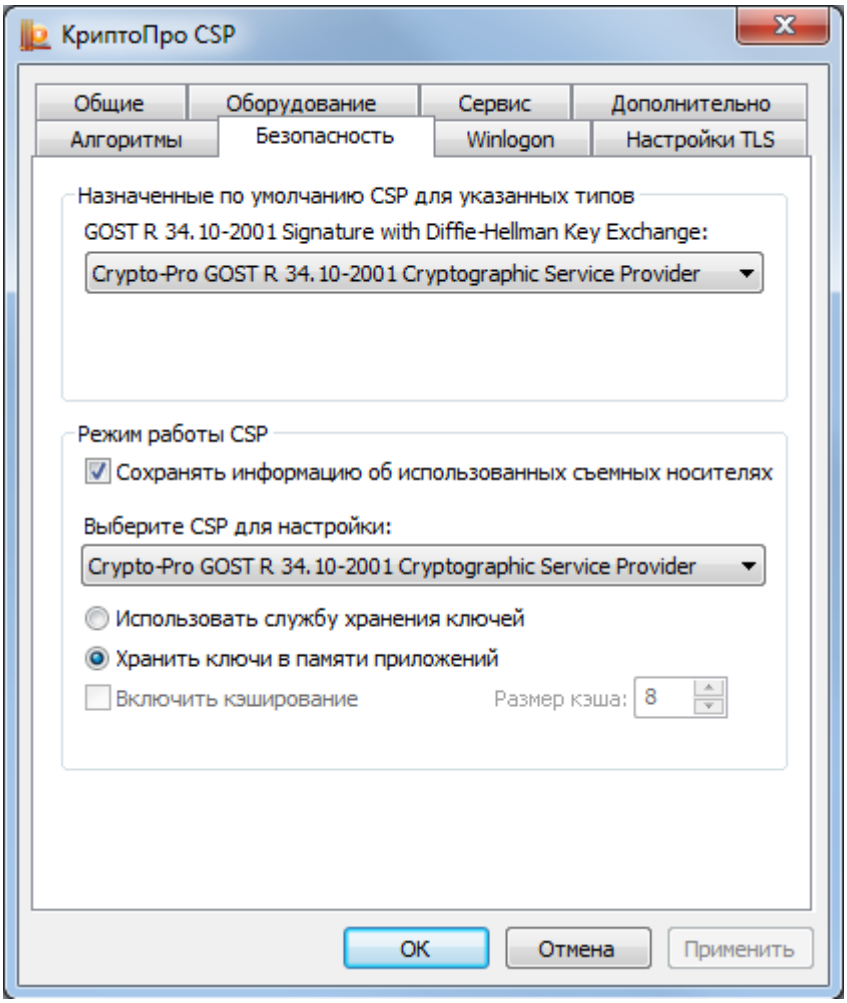


Рис. 60. Вкладка Безопасность, уровень защиты КС2 или КС3.

При хранении ключей в службе хранения ключей возможно применение кэширования контейнеров закрытых ключей. Кэширование заключается в том, что считанные с носителя ключи остаются в памяти сервиса.

Ключ из кэша является доступным и после извлечения ключевого носителя из считывателя, а также после завершения работы загрузившего этот ключ приложения. Каждый ключ из кэша доступен любому приложению, которое работает под той же учётной записью, что и приложение, поместившее этот ключ в кэш. Все ключи из кэша доступны до завершения работы службы хранения ключей. При переполнении кэша очередной ключ записывается на место самого раннего ключа, помещённого в кэш.

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 флаг 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.

2.7. Дополнительные настройки

Вкладка **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.

2.7.1. Просмотр версий используемых файлов

Для просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Дополнительно** (см. Рис. 61).

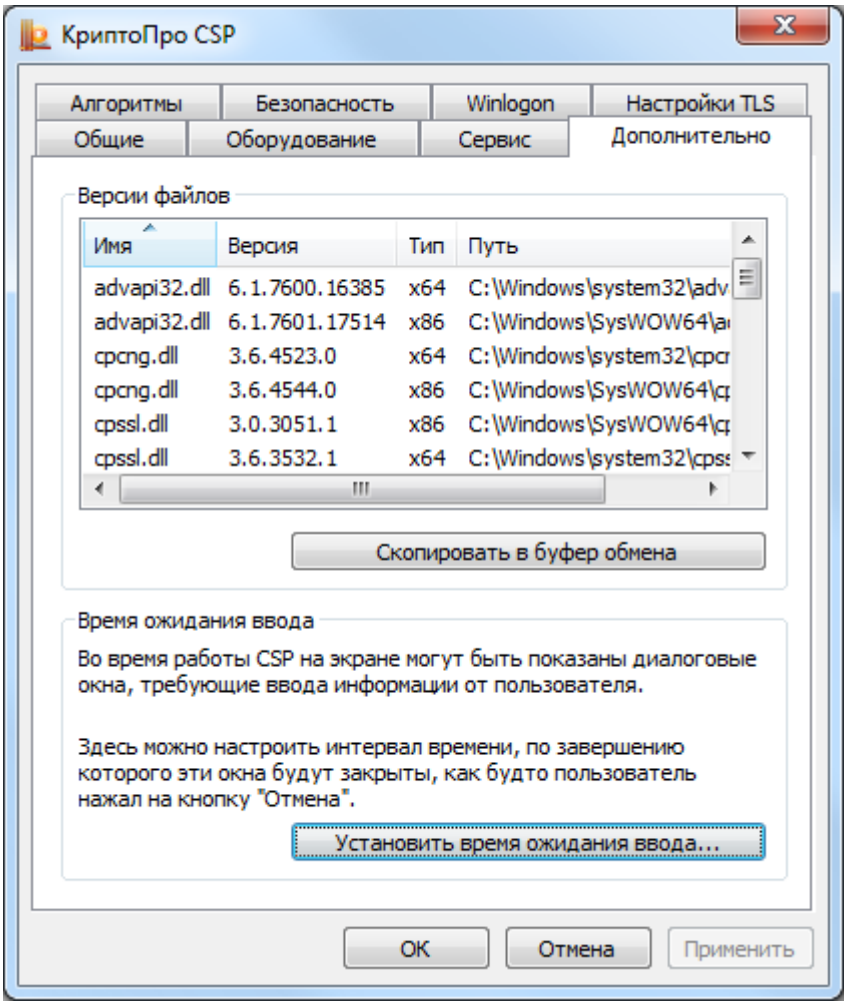


Рис. 61. Контрольная панель. Вкладка «Дополнительно»

В разделе **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.

2.7.2. 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**), выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Дополнительно** (см. Рис. 61).

Нажмите кнопку **Установить время ожидания ввода.**

Система отобразит окно «Интервал времени ожидания ввода» (см. Рис. 62). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

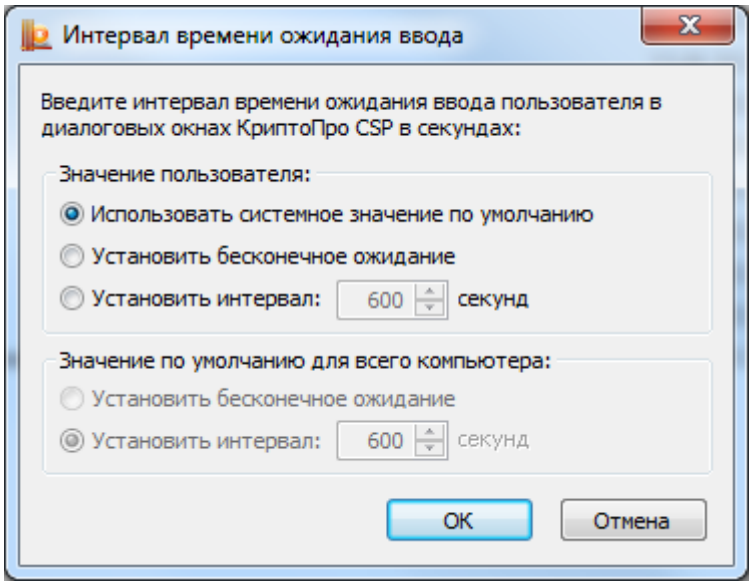


Рис. 62. Окно «Интервал времени ожидания ввода»

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 администратор локального компьютера (см. Рис. 63). При этом, если в панели КриптоПро CSP активна ссылка «Запустить с правами администратора» (см. Рис. 5), то её нужно нажать.

По умолчанию установлено ожидание ввода в течение 600 секунд.

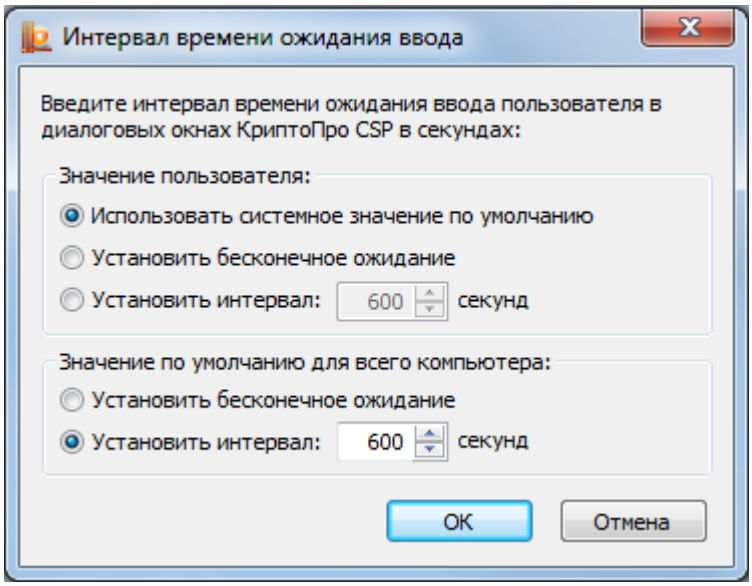


Рис. 63. Окно «Интервал времени ожидания ввода» для администратора компьютера

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).

2.8. Установка параметров криптографических алгоритмов

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

Для установки параметров криптографических алгоритмов необходимо выполнить **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Алгоритмы** (см. Рис. 64):

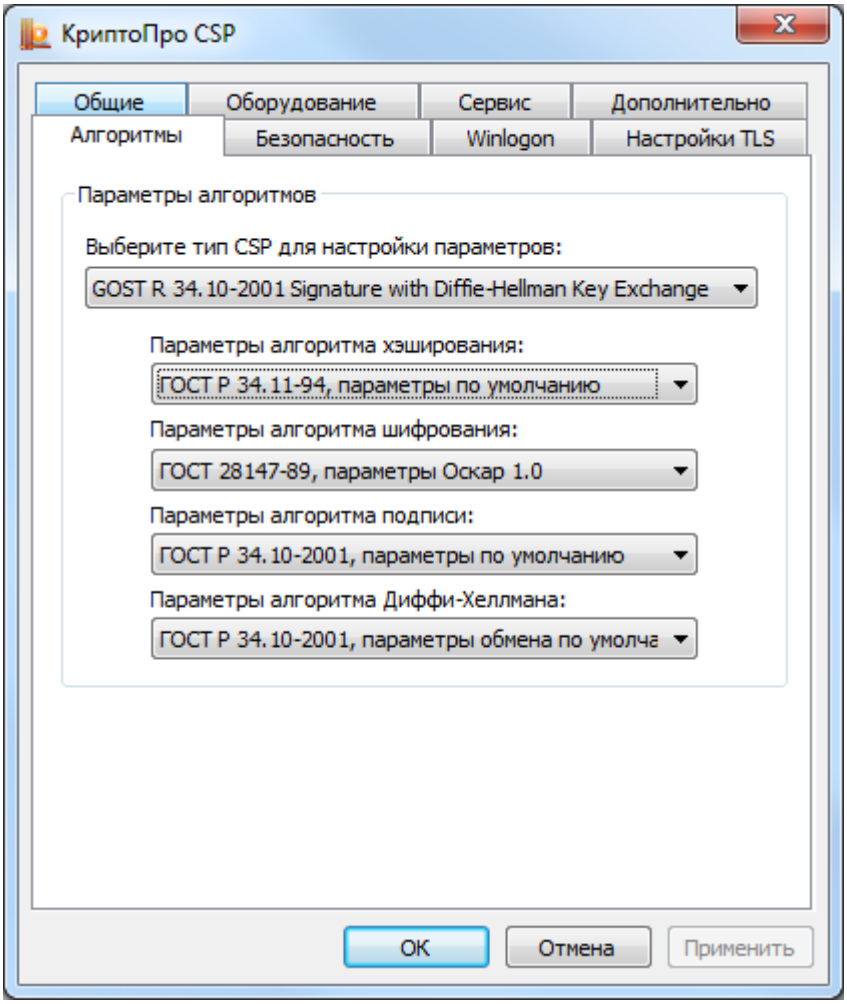


Рис. 64. Контрольная панель. Вкладка «Алгоритмы»

На закладке **Алгоритмы** можно выбрать тип криптопровайдера, для которого будет осуществляться настройка (в версии КриптоПро CSP 3.9 доступен единственный тип криптопровайдера: GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange), после чего для соответствующих криптографических алгоритмов реализована возможность установки параметров:

- 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 1.1, параметры РИК1, параметры шифрования 1, параметры шифрования 2, параметры шифрования 3).
- установка параметров алгоритма выработки и проверки электронной цифровой подписи - ГОСТ Р 34.10-2001 (параметры по умолчанию, параметры Оскар 2.x, параметры подписи 1);
- установка параметров алгоритма Диффи-Хеллмана - ГОСТ Р 34.10-2001 (параметры обмена по умолчанию, параметры обмена 1).

2.9. Настройка аутентификации в домене Windows.

Вкладка **Winlogon** контрольной панели СКЗИ КриптоПро CSP предназначена для настройки аутентификации в домене с использованием алгоритмов ГОСТ.

Для настройки Winlogon выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Winlogon** (см. Рис. 65):

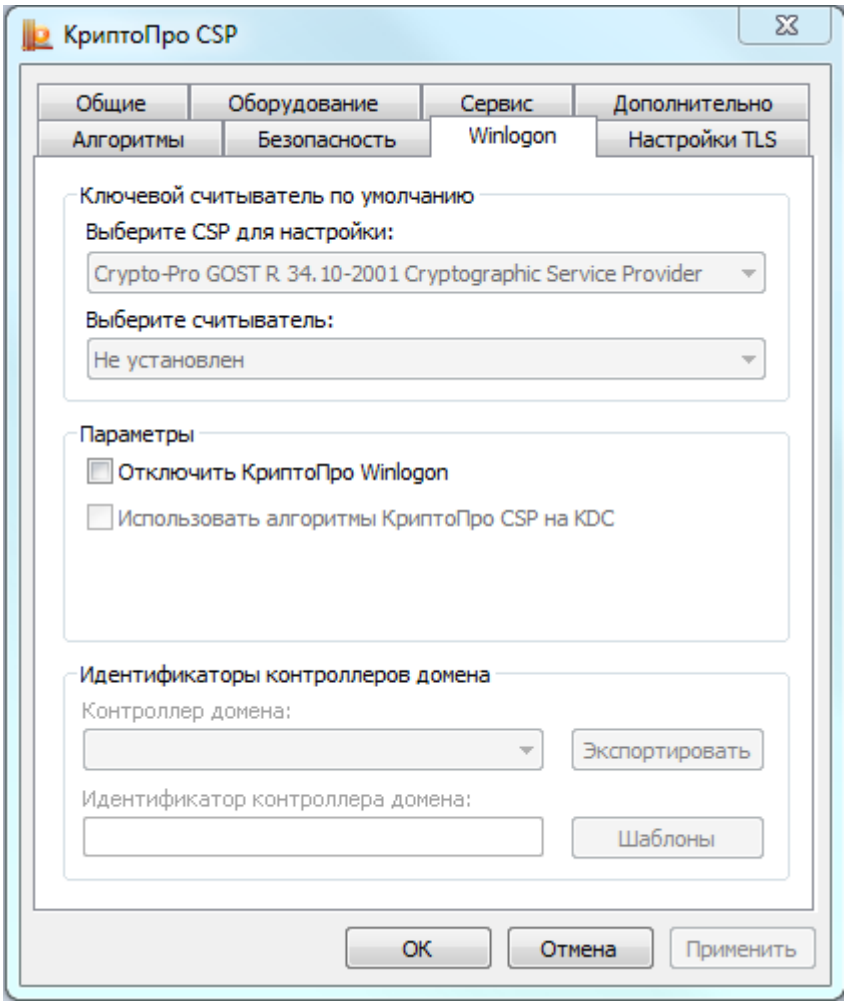


Рис. 65. Контрольная панель, вкладка Winlogon.

При установке на контроллер домена будет доступна для выбора опция **Использовать алгоритмы КриптоПро CSP на KDC** и будут заполнены поля идентификаторов контроллера домена. Подробно о настройке Winlogon см. соответствующую документацию.

При необходимости можно полностью отключить использование алгоритмов ГОСТ при аутентификации в домене. Для этого предназначена опция **Отключить КриптоПро Winlogon**.

2.10. Настройки TLS.

Вкладка **Настройка TLS** на контрольной панели СКЗИ КриптоПро CSP предназначена для настройки протокола TLS, обеспечивающем аутентификацию связывающихся сторон, конфиденциальность и целостность пересылаемой информации.

Для настройки TLS выполните **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP** и перейдите на вкладку **Настройка TLS** (см. Рис. 65).

При установлении флага в поле клиента **Использовать протокол OCSP**, клиентом осуществляется протокол проверки сертификата по базе сервера OCSP Responder.

При установлении флага в поле клиента **Не проверять сертификат сервера на отзыв**, клиентом не производится проверка сертификатов на принадлежность списку отозванных сертификатов (CRL).

При установлении флага в поле клиента **Не использовать устаревшие cipher suite-ы** отключается возможность использования cipher suite, в которых были обнаружены уязвимости.

При установлении флага в поле сервера **Использовать протокол OCSP**, сервером осуществляется протокол проверки сертификата по базе сервера OCSP Responder.

Путем установления соответствующих флагов в полях сервера достигается отключение сервером проверки сертификата клиента на наличие в списке отозванных сертификатов, проверки назначения собственного сертификата, использование cipher suite, в которых были обнаружены уязвимости,

Посредством установления/снятия флагов, связанных с расширением Renegotiation Indication, контролируется требование безопасного связывания нескольких фаз handshake (см. RFC 5746).

В соответствующих полях настраивается размер кэша сессий и максимальное число центров сертификации в запросе сертификата.

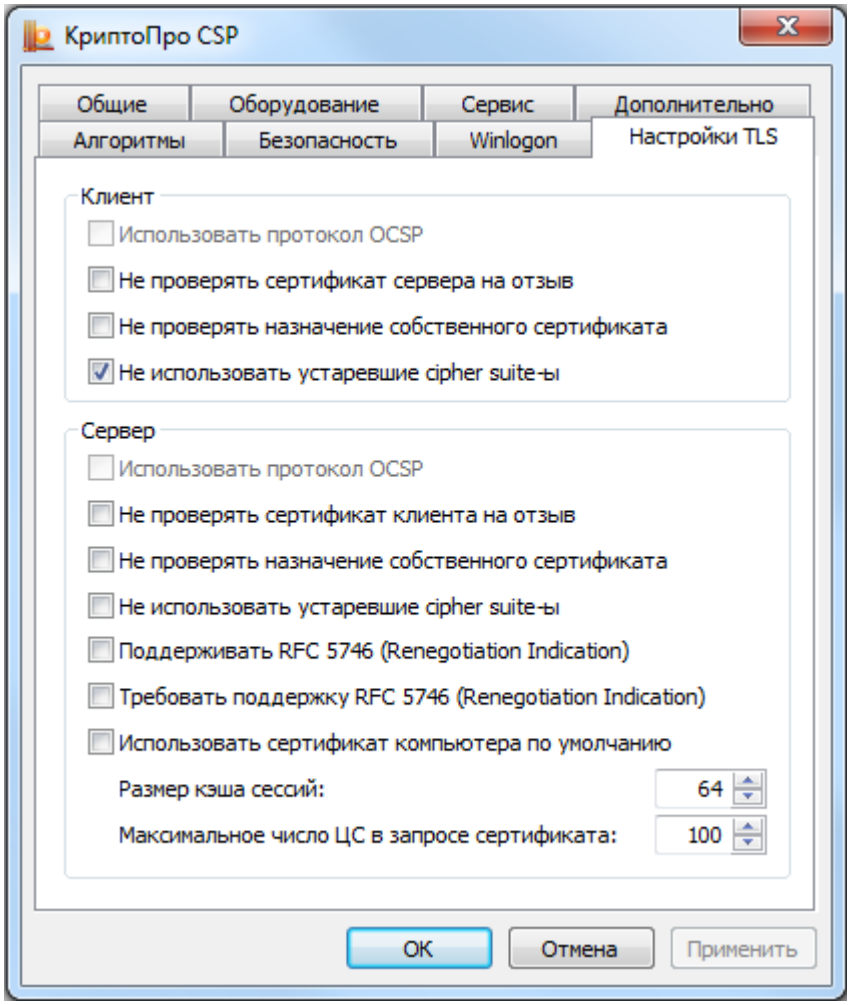


Рис.66. Контрольная панель, вкладка Настройка TLS

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 (см. Рис.).

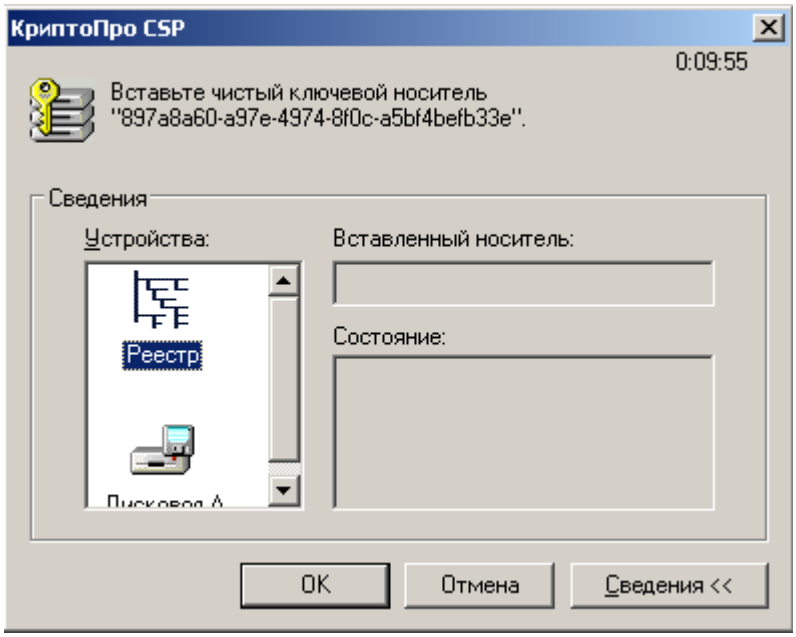


Рис. 67. Выбор ключевого носителя

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.).

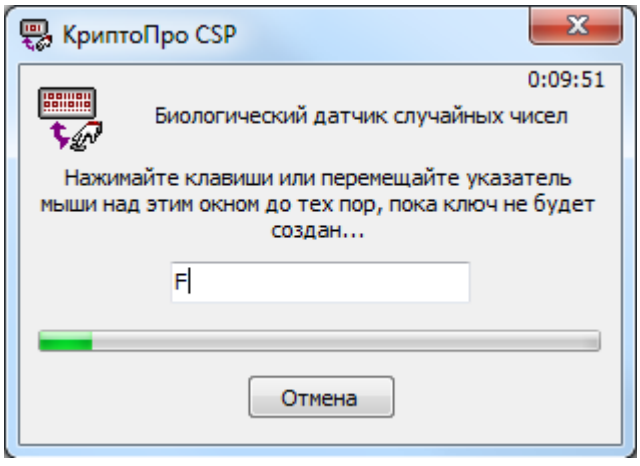


Рис. 68. Биологический датчик случайных чисел

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

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.1.3. Использованием сервисного десктопа

В операционных системах Windows Vista/2008/7/2008R2/8/2012 в случае использования службы хранения ключей для уровня КС1 или использования датчиков случайных чисел для уровней КС2/КС3 (Биологический ДСЧ) диалоги выбора считывателя и генерации ключа появляются на сервисном десктопе.

3.1.4. 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.).

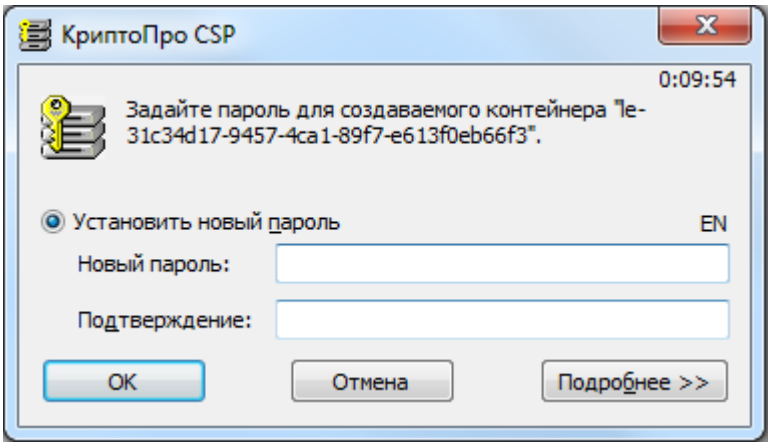


Рис. 71. Ввод пароля на доступ к закрытому ключу

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**).

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.

3.1.5. 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.) нажмите кнопку **Подробнее**. Система отобразит окно выбора способа защиты доступа к закрытому ключу создаваемого контейнера (см. Рис.). Защита носителей поддерживающих аппаратный пароль (пин-код) возможна только на этом пароле (пин-коде).

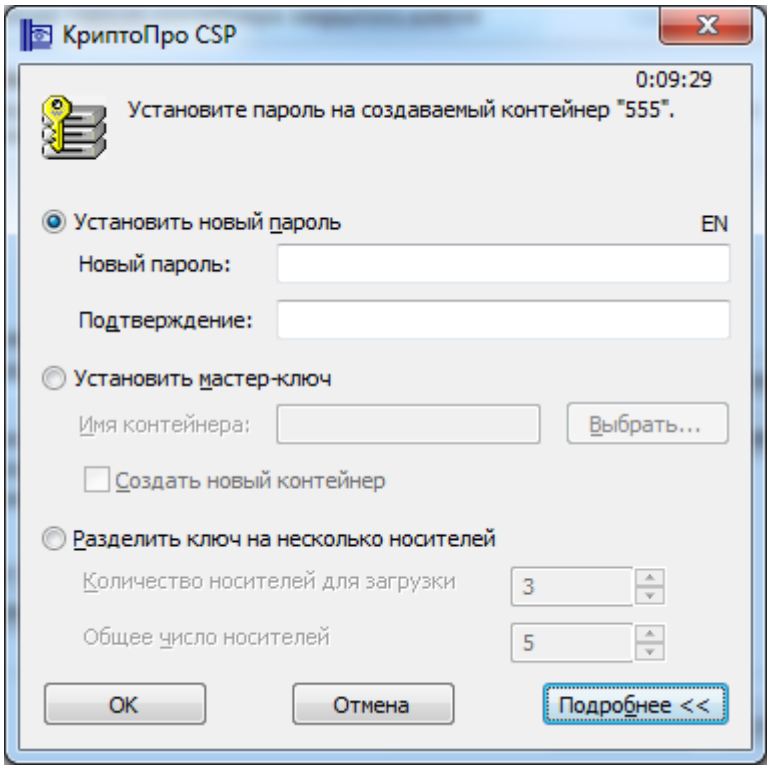


Рис. 72. Выбор средства защиты доступа к закрытому ключу

В этом окне содержатся следующие поля:

- **Установить новый пароль** – ввод текстового пароля;
- **Установить мастер-ключ** – зашифрование данного закрытого ключа на другом закрытом ключе (из другого ключевого контейнера);
- **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.) к окну ввода пароля на доступ (см. Рис.) повторно нажмите кнопку **Подробнее**.

3.1.5.1. Установка нового пароля

Если переключатель установлен в поле **Установить новый пароль** (см. Рис.), то СКЗИ «КриптоПро CSP» осуществит защиту ключа при помощи пароля на доступ, введенного с клавиатуры. Необходимо осуществить действия, описанные в пункте 3.1.4.

3.1.5.2. Установка мастер-ключа

Если переключатель установлен в поле **Установить мастер-ключ** (см. Рис.), 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.).

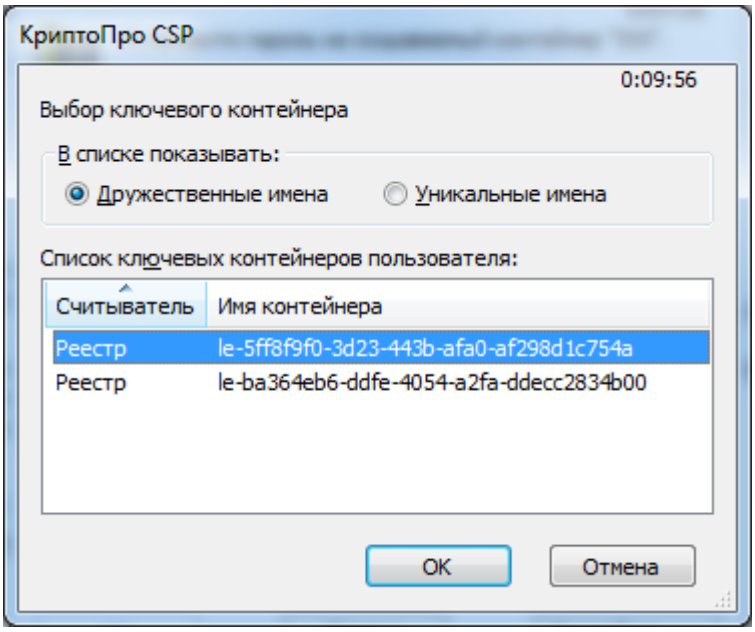


Рис. 66. Список существующих контейнеров

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 флага напротив поля **Создать новый контейнер** (см. Рис.) система аналогично создаст новый контейнер и на его ключе осуществит зашифрование закрытого ключа данного контейнера.

3.1.5.3. Разделение ключа на несколько носителей

Если переключатель установлен в поле **Разделить ключ на несколько носителей** (см. Рис.), 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.). 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.), 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.). В этом окне необходимо ввести пароль либо выбрать другое средство защиты доступа к закрытому ключу при помощи кнопки **Подробнее** (см. Рис.).

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.).

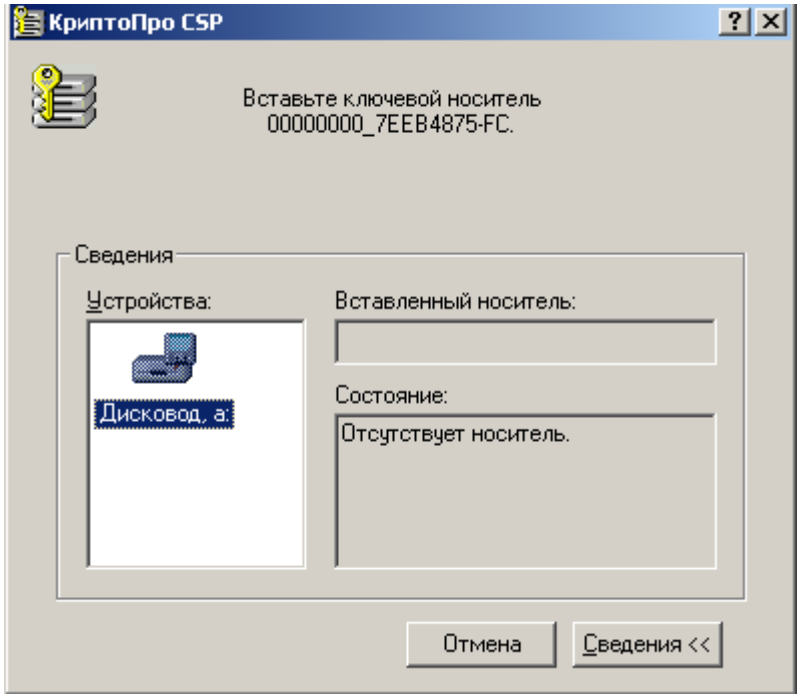


Рис. 67. Отсутствие необходимого носителя

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

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 3.1.5.1), то будет отображено окно проверки пароля для доступа к закрытому ключу открываемого контейнера (см. Рис.).

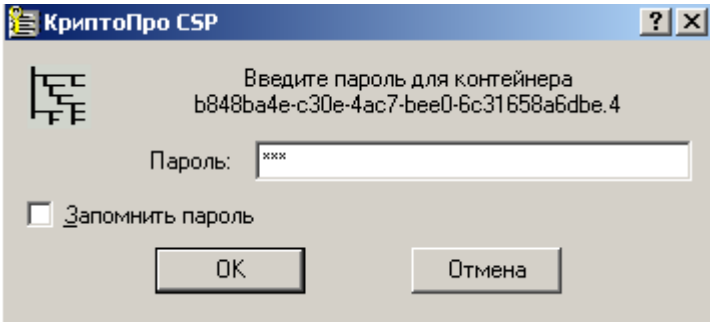


Рис. 68. Проверка пароля на доступ к закрытому ключу

Если ранее во время ввода пароля на доступ к закрытому ключу флаг напротив поля **Сохранить пароль** был установлен, 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.

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 3.1.5.2), то будет отображено окно проверки пароля для доступа к закрытому ключу контейнера, на ключе которого проводилось зашифрование (см. Рис.).

После того, как был получен доступ к ключу расшифрования, произойдет расшифрование ключа открываемого контейнера.

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 3.1.5.3), 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.

3.3. 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.

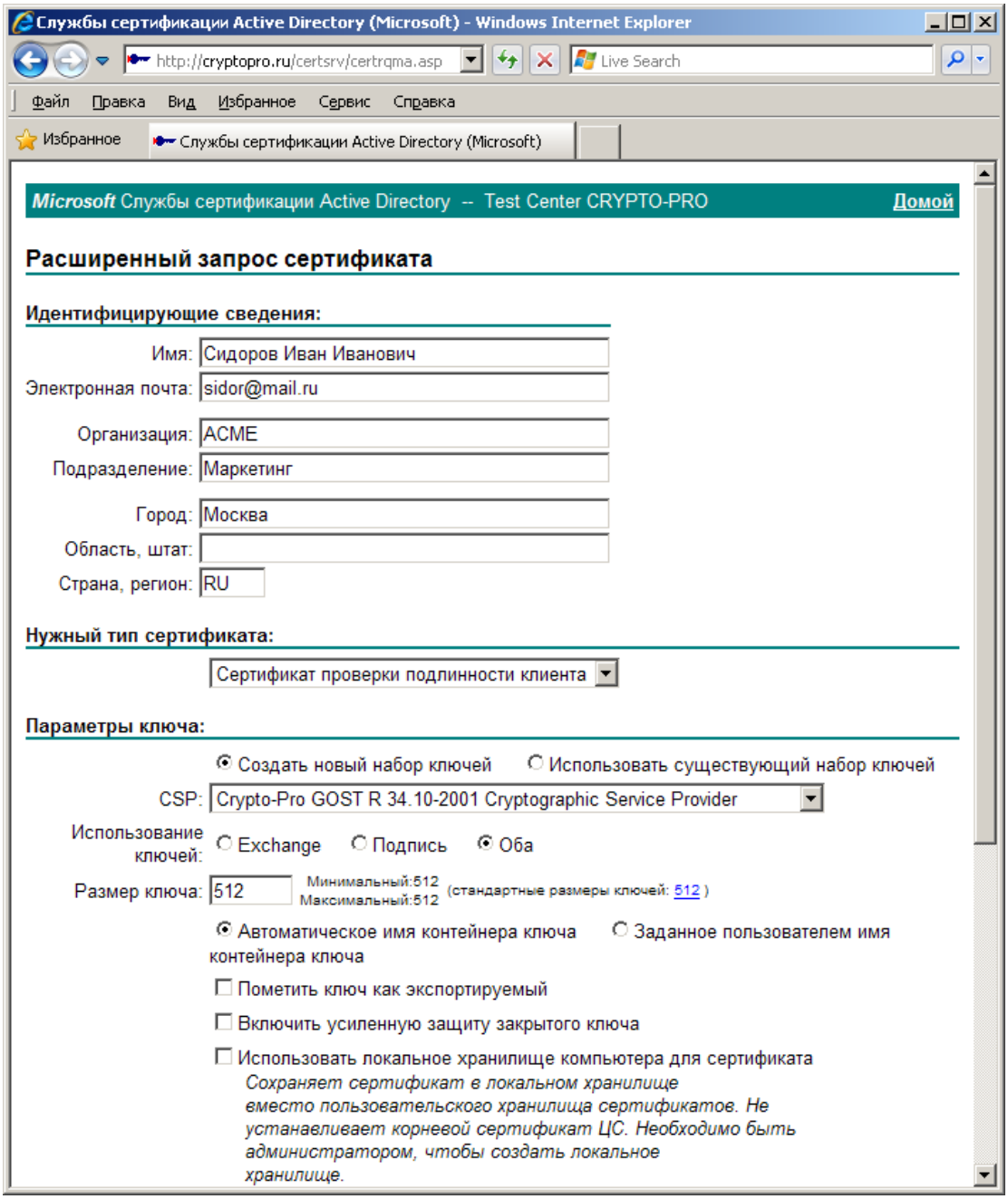


Рис. 69. Генерация ключа при помощи УЦ

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 аутентификации сервера на сервере ISA/TMG

На компьютере с сервером ISA сертификат аутентификации сервера должен быть размещен в хранилище **Локальный компьютер\Личные** с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра сертификации, выдавшего этот сертификат - в хранилище **Локальный компьютер\Доверенные корневые Центры Сертификации** (если этот ЦС корневой) или **Локальный компьютер\Промежуточные Центры Сертификации** (если этот ЦС подчинённый. В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network Service** на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

Проверить наличие необходимых сертификатов можно с помощью оснастки "Сертификаты". Для запуска консоли нужно выполнить **Пуск ⇒ Программы ⇒ КриптоПро ⇒ Сертификаты**

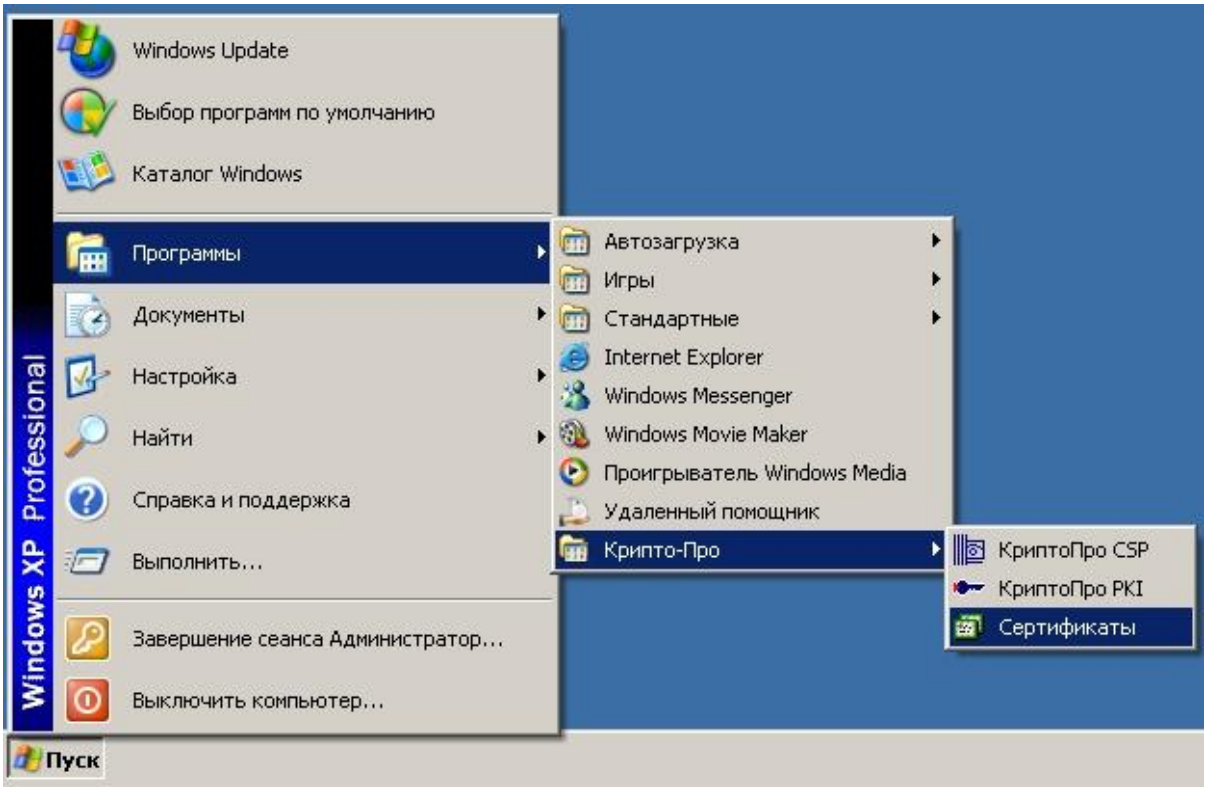


Рис. 70. Запуск консоли Сертификаты

После запуска корень консоли должен выглядеть приблизительно:

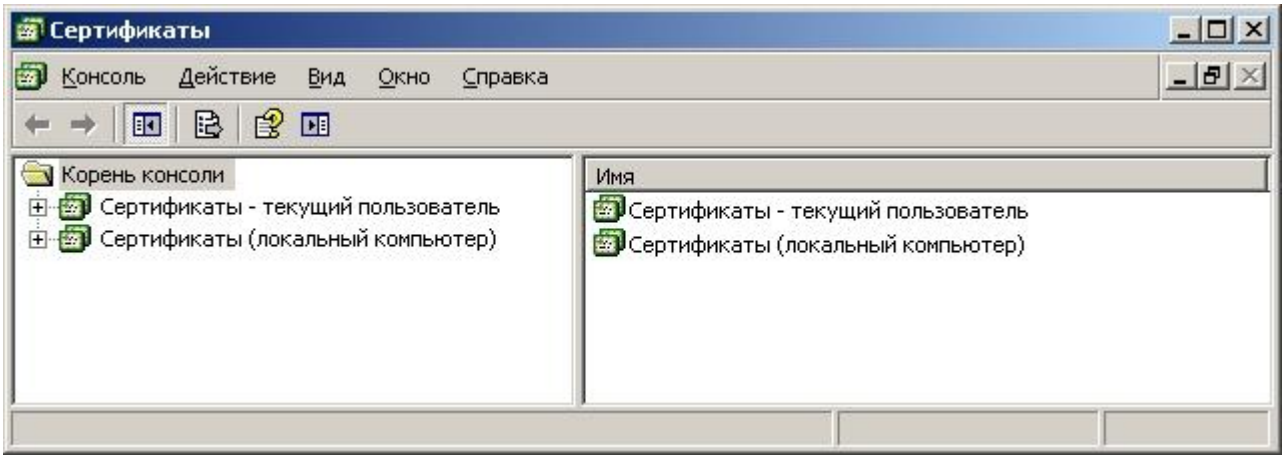


Рис. 71. Корень консоли Сертификаты

Установите курсор на сертификат сервера ISA:

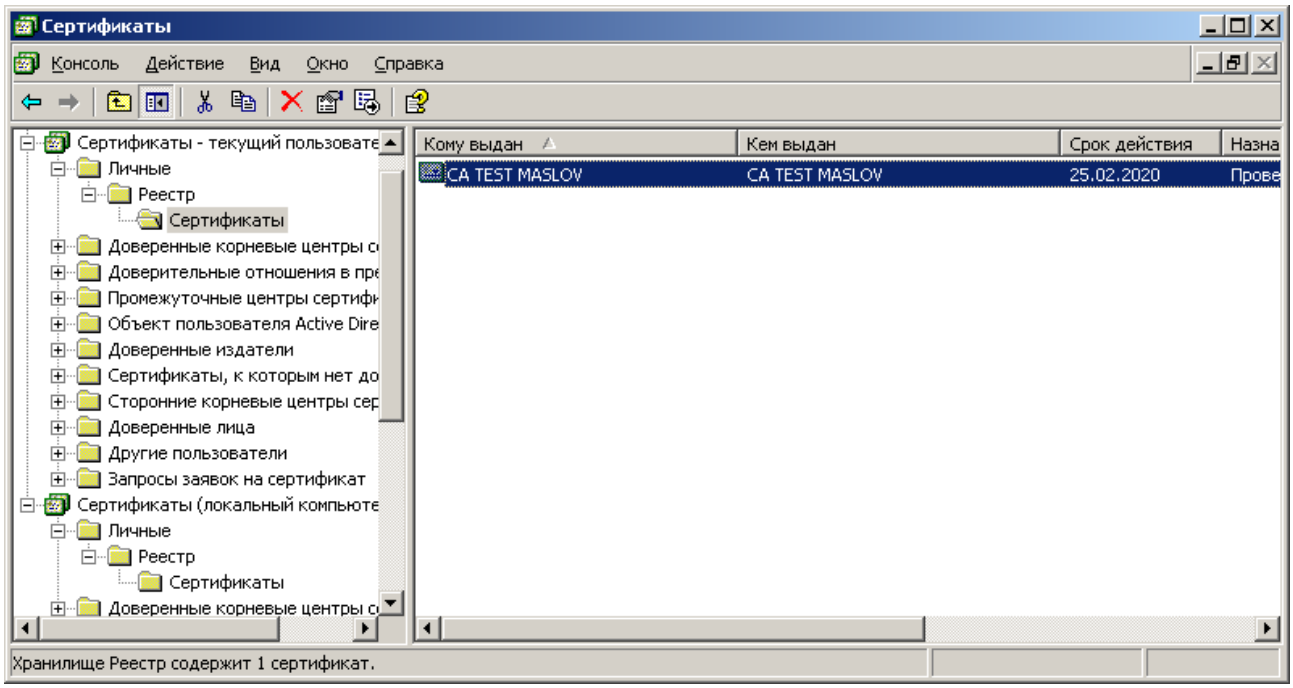


Рис. 72. Корень консоли MMC

С использованием функции «Копировать», занесите сертификат в буфер Clipboard

После этого установите курсор на разделе «Личные» сертификатов локального компьютера и выполните функцию «Вставить»

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

4.2. Размещение сертификата клиентской аутентификации на сервере ISA/TMG

Если между сервером ISA и конечным веб-сервером требуется шифрование трафика по TLS с аутентификацией по сертификату клиента, то выпускается сертификат клиентской аутентификации. На компьютере с сервером ISA этот сертификат должен быть размещен в хранилище **Локальный компьютер\Личные** с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра сертификации, выдавшего этот сертификат - в хранилище **Локальный компьютер\Доверенные корневые Центры Сертификации** (если этот ЦС корневой) или **Локальный компьютер\Промежуточные Центры Сертификации** (если этот ЦС подчинённый.

В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network Service** на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

4.3. 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.):

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.

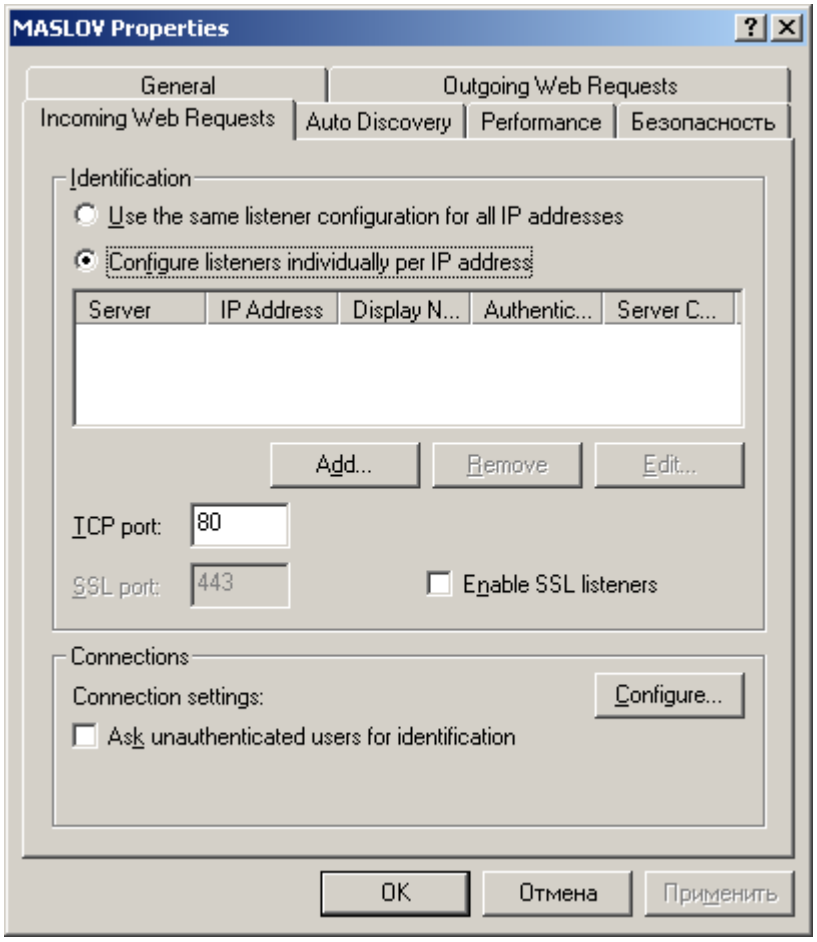


Рис. 80. Установка и настройка Слушателей

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).

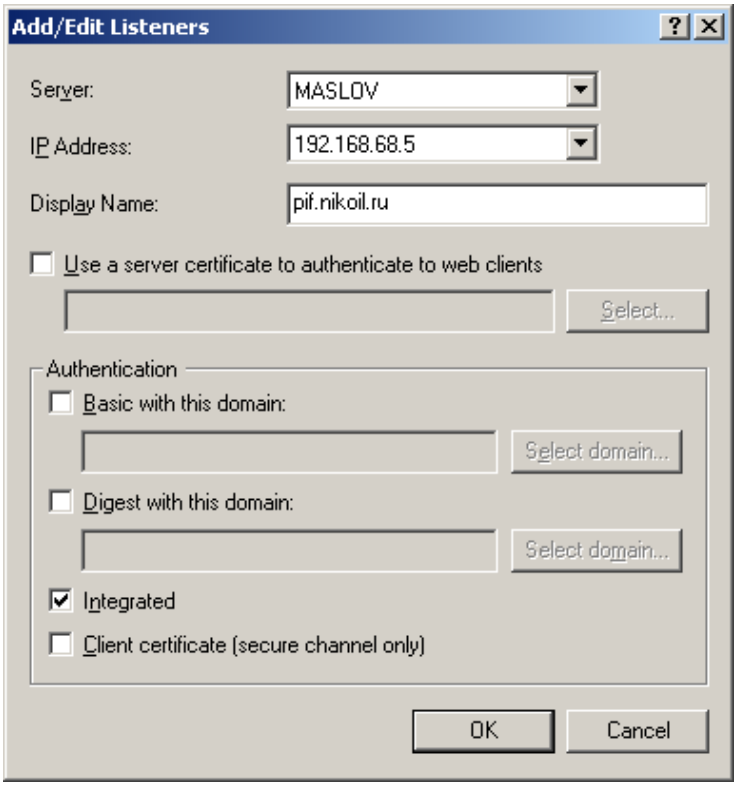


Рис. 81. Добавление Слушателя/редактирование свойств Слушателя(1)

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.

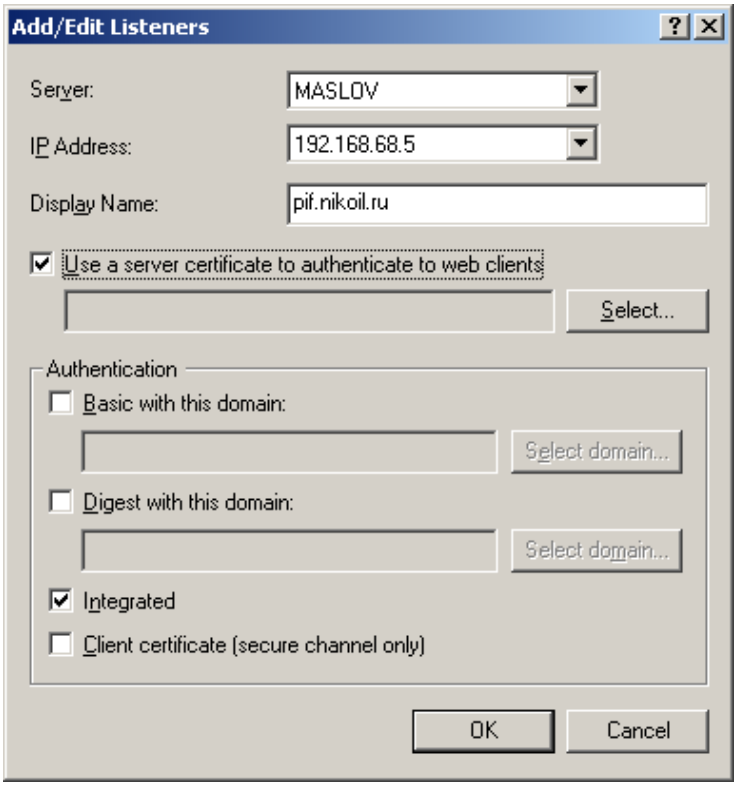


Рис. 82. Добавление Слушателя/редактирование свойств Слушателя(2)

Выбрать сертификат сервера, который будет использоваться для аутентификации.

Нажать кнопку Select.

В появившемся окне выбрать из списка сертификат открытого ключа сервера:

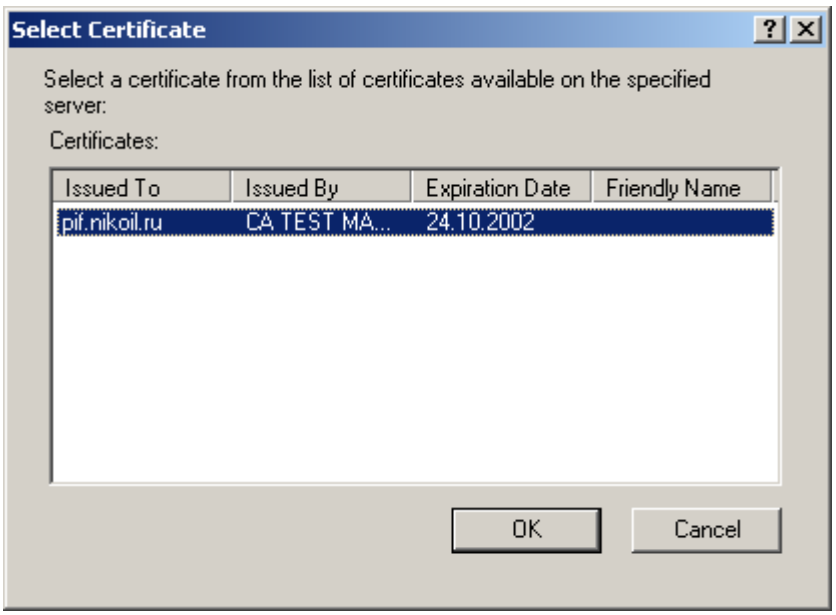


Рис. 733. Выбор сертификата открытого ключа сервера

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

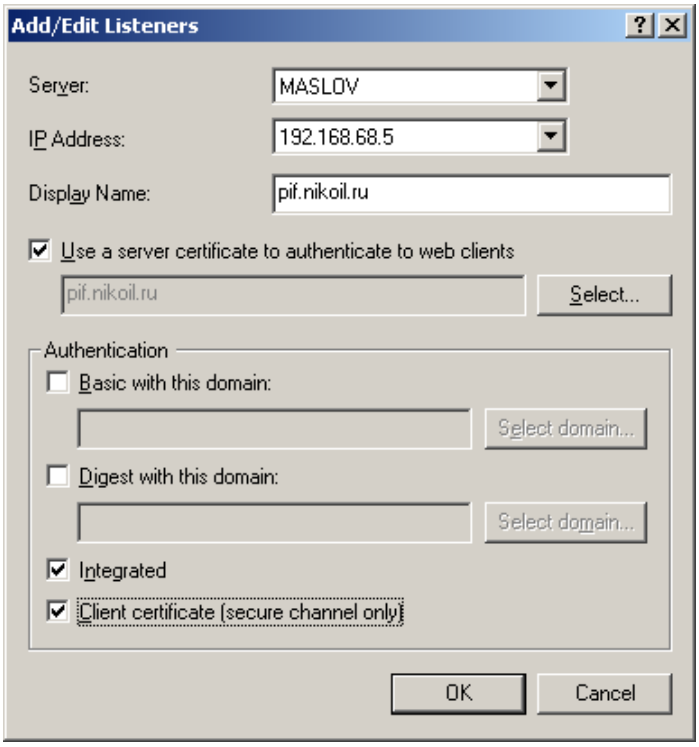


Рис. 74. Добавление Слушателя/редактирование свойств Слушателя(3)

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

Установка и настройка Слушателей осуществляется по документации на ISA сервер.

В окне добавления Слушателя или в окне редактировании свойств Слушателя необходимо указать на использование сертификата сервера при аутентификации с Web-клиентом и выбрать настроенный в п. 4.1. сертификат сервера, который будет использоваться для аутентификации.

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификацией необходимо дополнительно указать на требование сертификата клиента.

4.4. 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 (вкладка **Action** окна свойств правила Web публикации).

область использования ключа должна содержать «Аутентификация Сервера»

Установить сертификат корневого ЦС в цепочке сертификатов Web-сервера на сервере ISA, в хранилище **Локальный компьютер\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. 755. Окно Мастера создания Правила Web

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

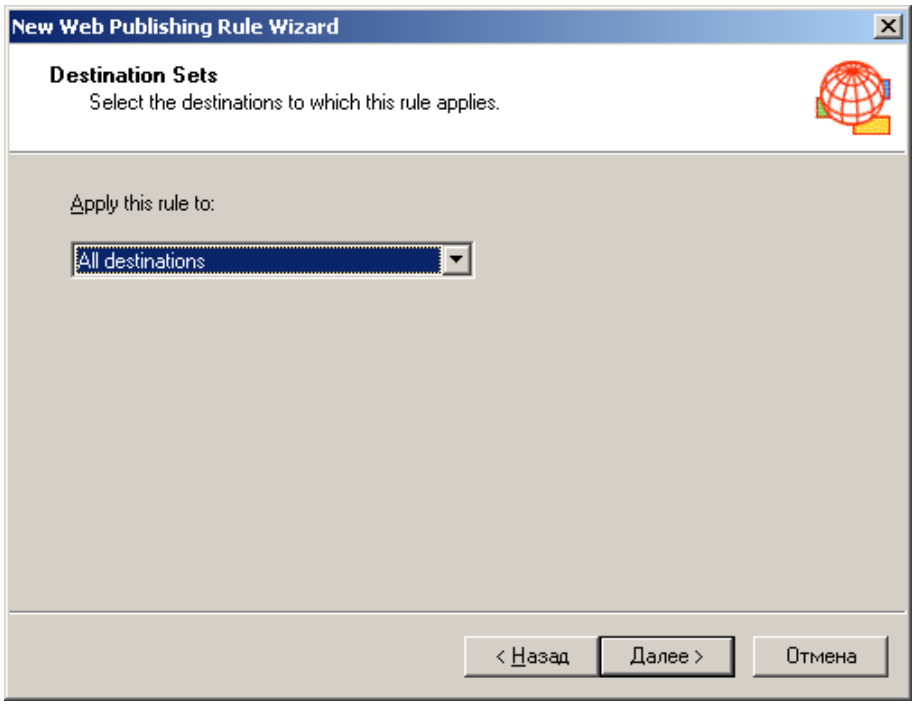


Рис. 76. Окно установки назначения

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»

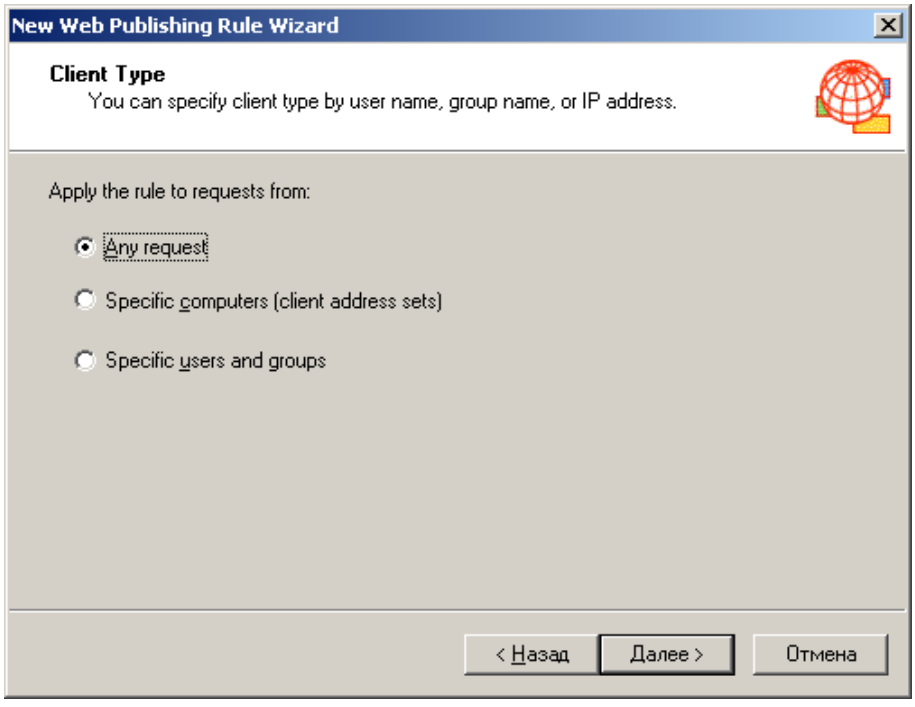


Рис. 77. Окно типа клиента

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»

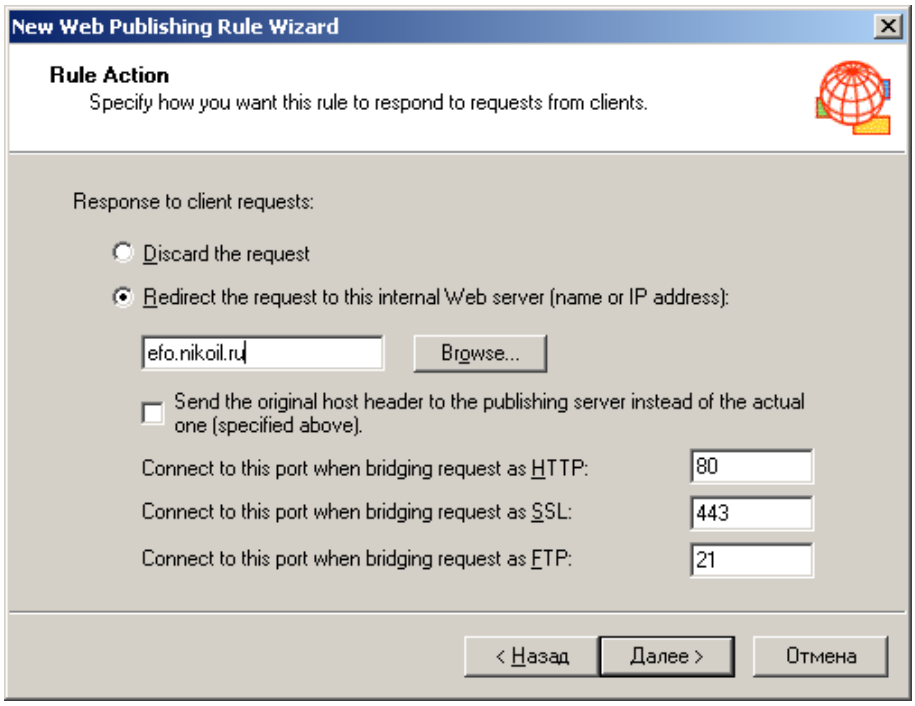


Рис. 788. Окно ввода доменного имени

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.

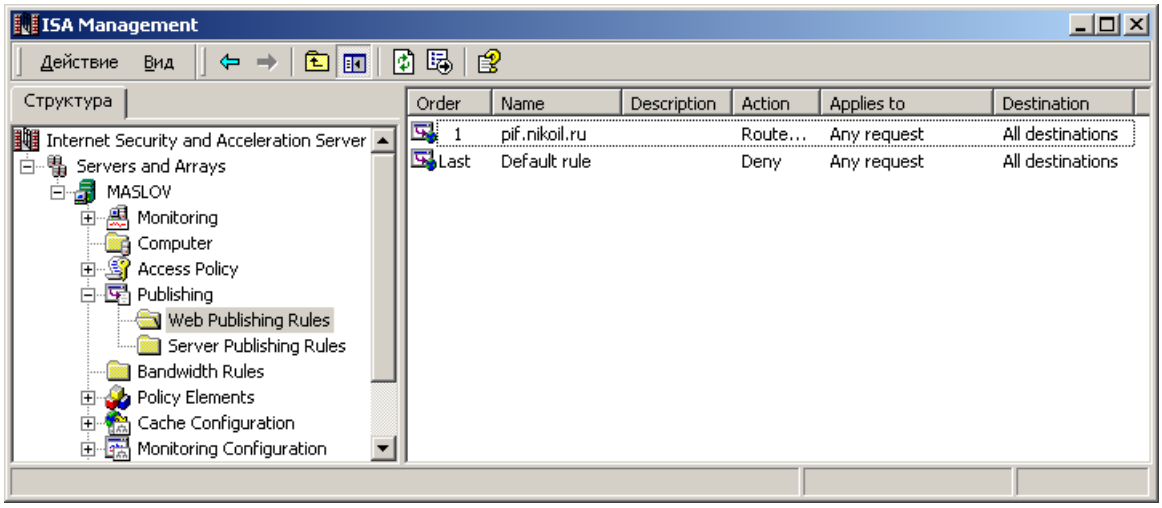


Рис. 799. Список правил Web-публикации