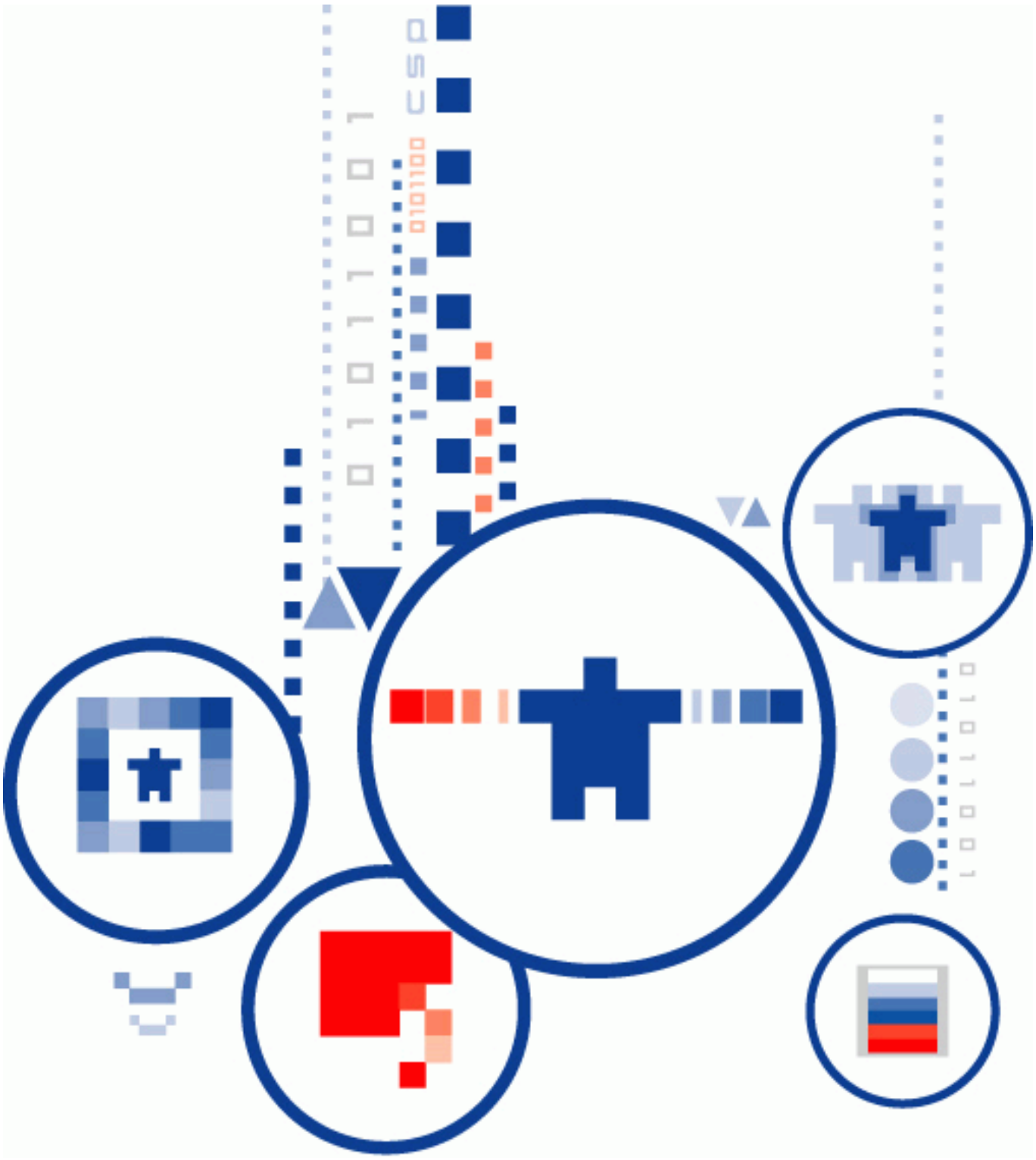
ЖТЯИ.00071-01 90 01



ПАК криптографической защиты информации «Рутокен CSP»

Инструкция по использованию

АННОТАЦИЯ

Настоящий документ содержит описание программно-аппаратного комплекса криптографической защиты информации «Рутокен CSP» (СКЗИ «Рутокен CSP»), предназначенного для защиты открытой информации в информационных системах общего пользования (вычисление и проверка электронной цифровой подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах.

Документ предназначен для пользователей как ознакомительный материал перед установкой и эксплуатацией СКЗИ «Рутокен CSP».

Информация о разработчике ПК «КриптоПро Рутокен CSP»:

ООО «Крипто-Про»
127 018, Москва, Улица Образцова, 38
Телефон: (495) 933 1168
Факс: (495) 933 1168
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

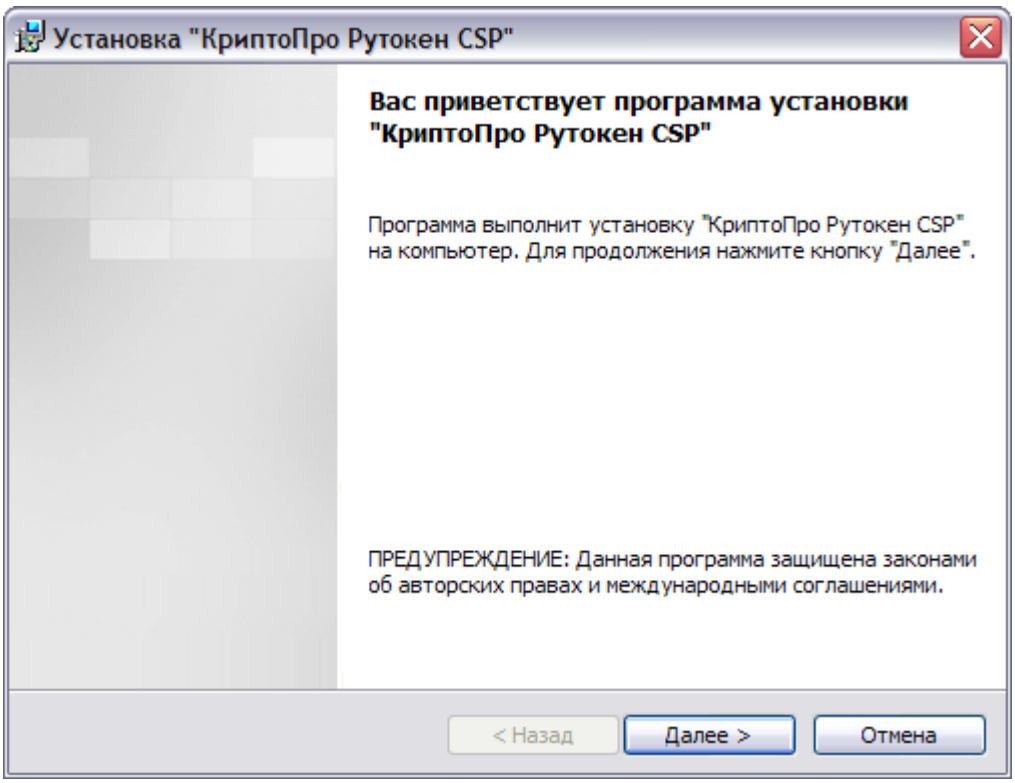
1. Инсталляция СКЗИ «Рутокен CSP»

1.1. Установка дистрибутива СКЗИ Рутокен CSP

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

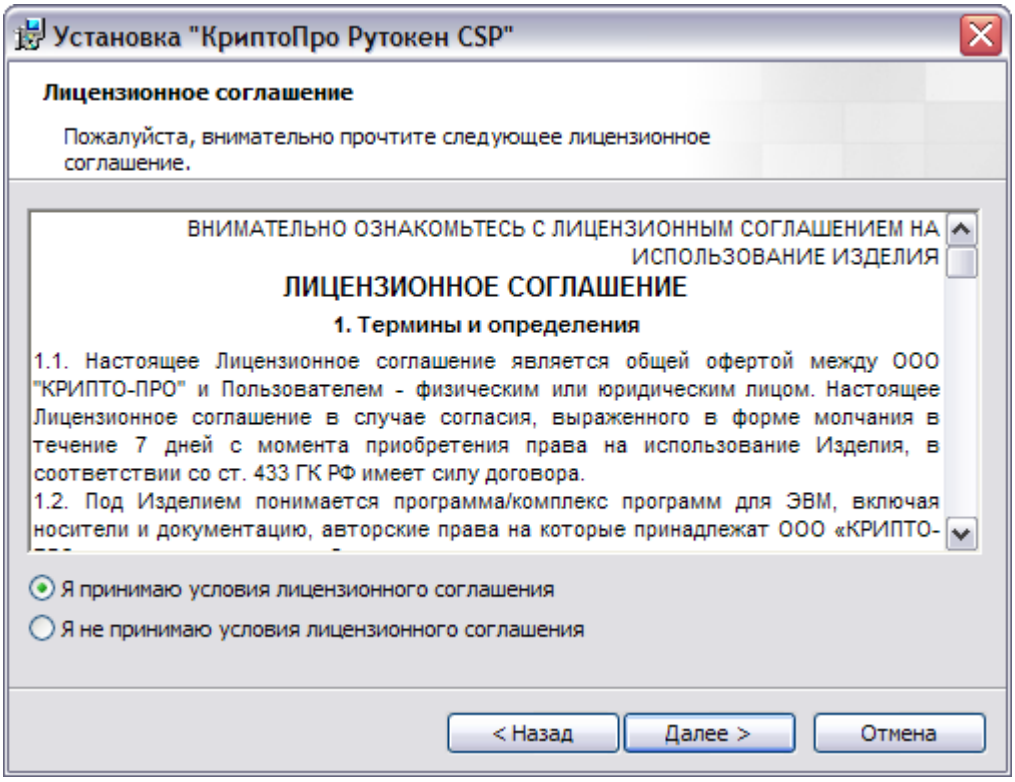
Для установки программного обеспечения вставьте компакт-диск в дисковод. Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы и удобный для Вас язык установки. Запустите выполнение установки.

Рисунок 1. Приветственное окно мастера установки.



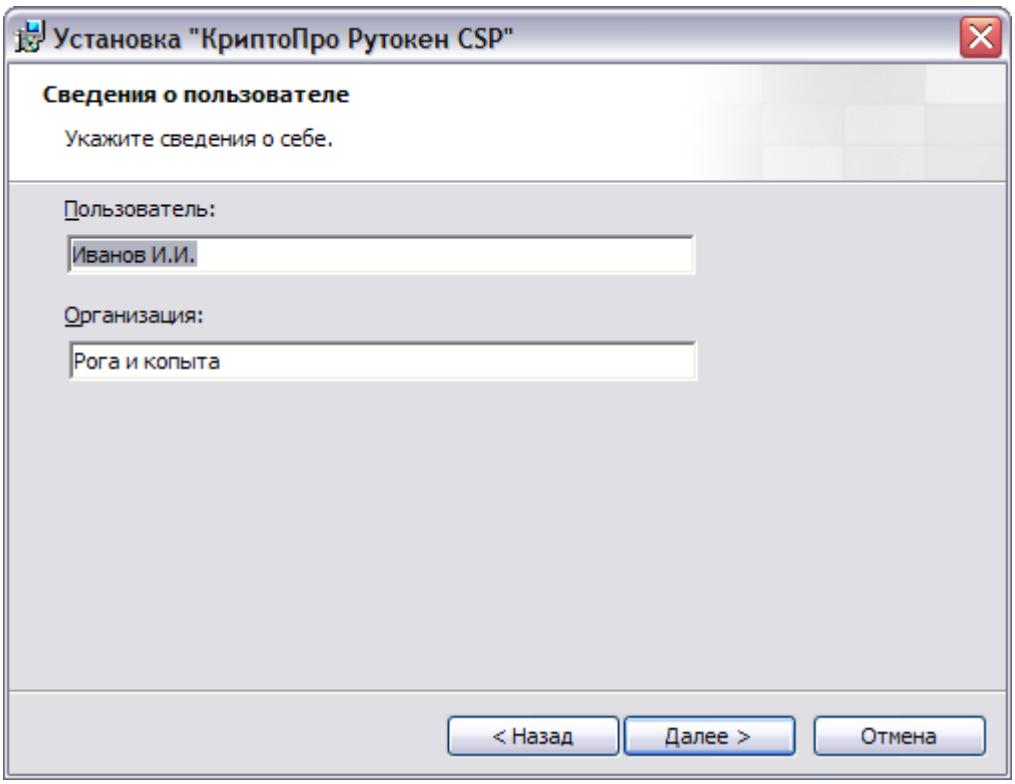
В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование СКЗИ Рутокен CSP. Если Вы согласны со всеми пунктами соглашения, выделите пункт «Я принимаю условия лицензионного соглашения», и нажмите **Далее** (см. Рисунок 2).

Рисунок 2. Лицензионное соглашение



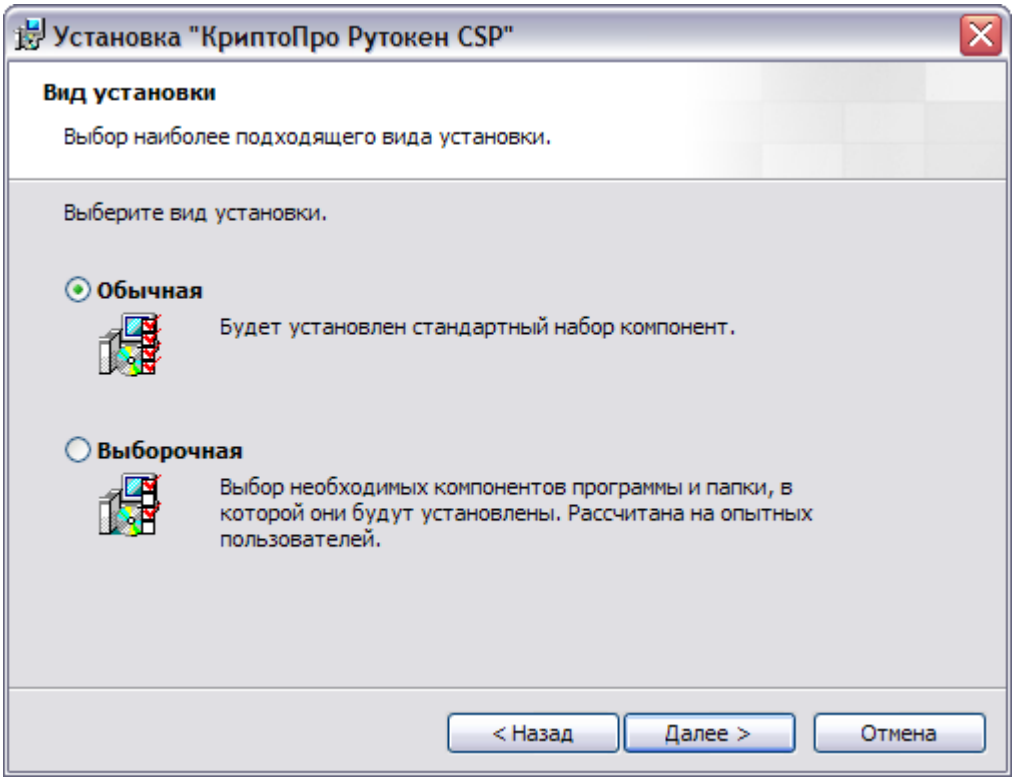
Для дальнейшей установки Рутокен CSP нажмите **Далее**. Следующим шагом необходимо ввести информацию о пользователе, производящем установку (см. Рисунок 3).

Рисунок 3. Сведения о пользователе.



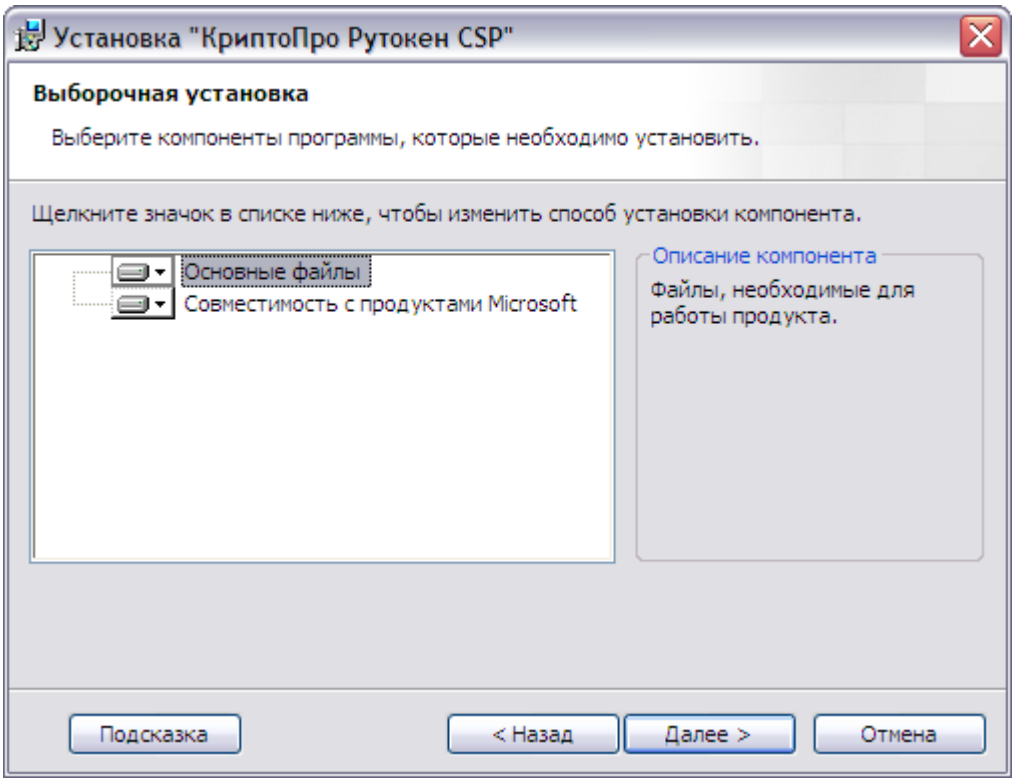
После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 4), в котором необходимо выбрать вид установки.

Рисунок 4. Вид установки



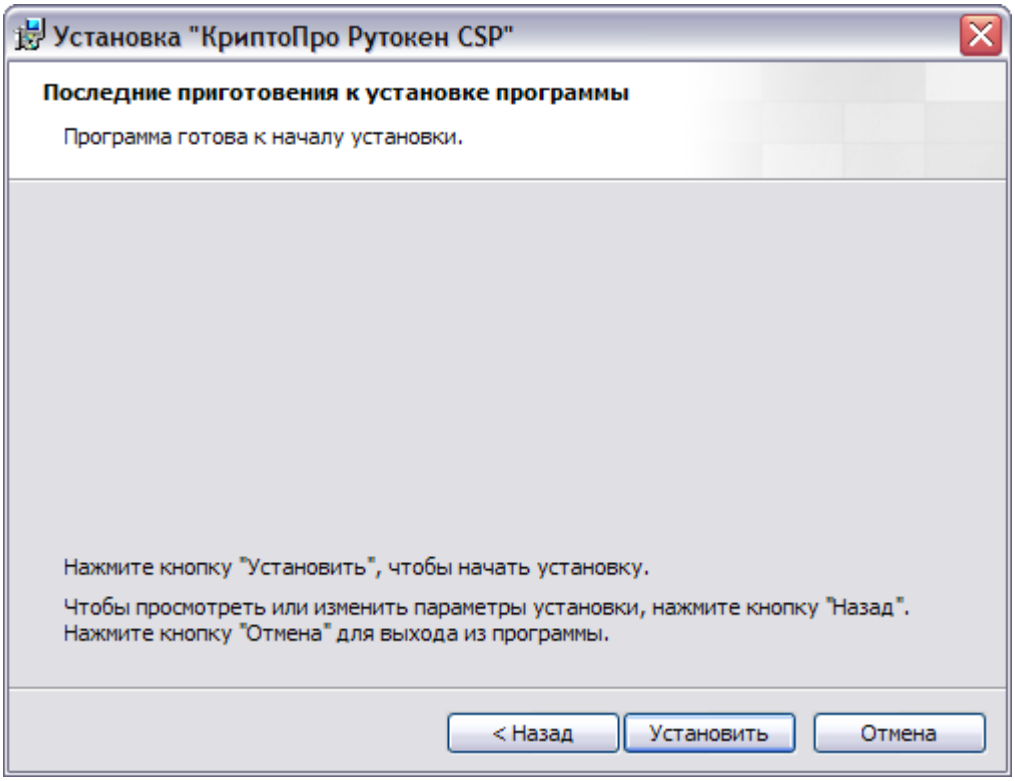
СКЗИ Рутокен CSP определяет два вида установки: обычная и выборочная. Если выбран вид установки «Обычная», то устанавливаются основные файлы для работы СКЗИ и компоненты для совместимости с продуктами Microsoft. По желанию можно не устанавливать дополнительные компоненты, в этом случае следует выбрать вид установки «Выборочная» (см. Рисунок 5).

Рисунок 5. Выборочная установка



Следующее окно мастера служит для подтверждения установки (см. Рисунок 6). При необходимости можно вернуться назад и переопределить параметры установки. Для подтверждения нажмите кнопку **Установить**.

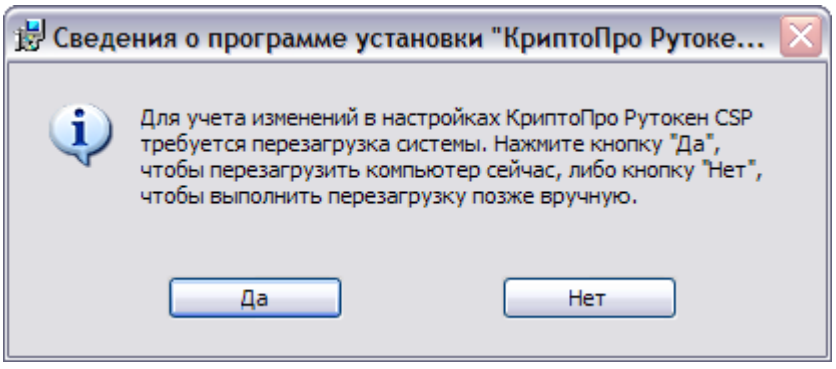
Рисунок 6. Окно подтверждения установки



После выполнения всех описанных шагов мастер устанавливает СКЗИ Рутокен CSP, сопровождая действия комментариями. По окончании установки мастер показывает окно с подтверждением успешной установки, где необходимо нажать кнопку **Готово**.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

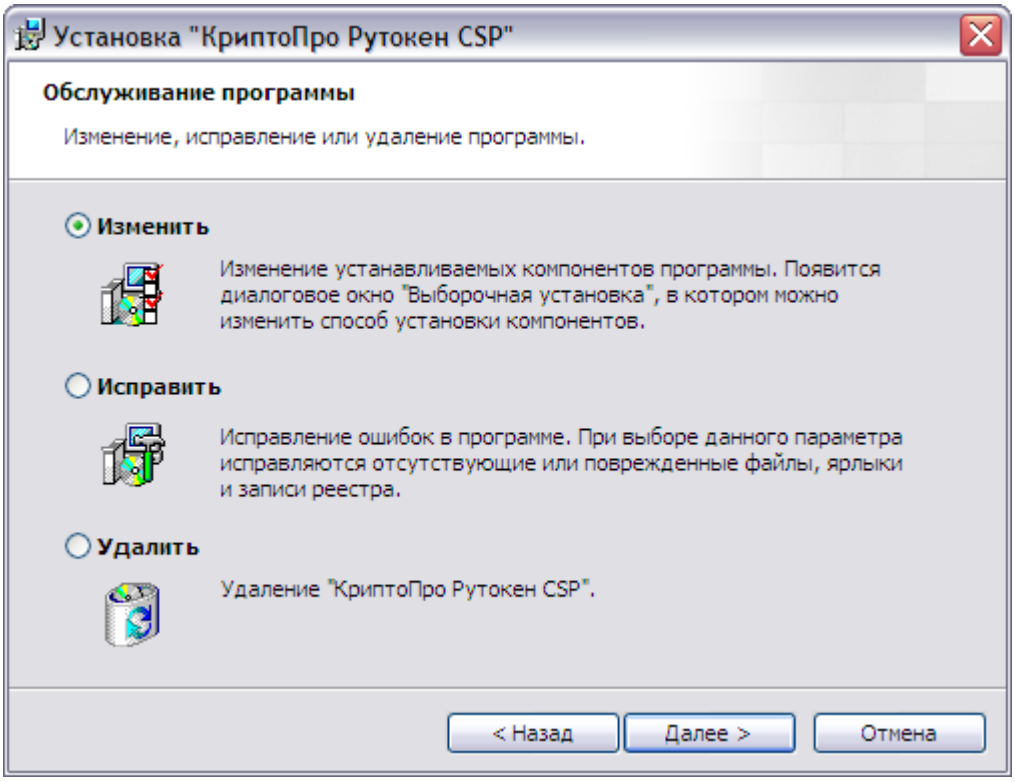
Рисунок 7. Окончание установки



1.2. Изменение, исправление или удаление программы

Если мастер установки обнаружит на машине уже установленную версию СКЗИ Рутокен CSP, то сразу после нажатия кнопки Далее в окне приветствия (см. Рисунок 1) появится соответствующая информация с предложением изменить набор установленных компонент, исправить ошибки или удалить Рутокен CSP (см. Рисунок 8).

Рисунок 8. Изменение, исправление или удаление программы

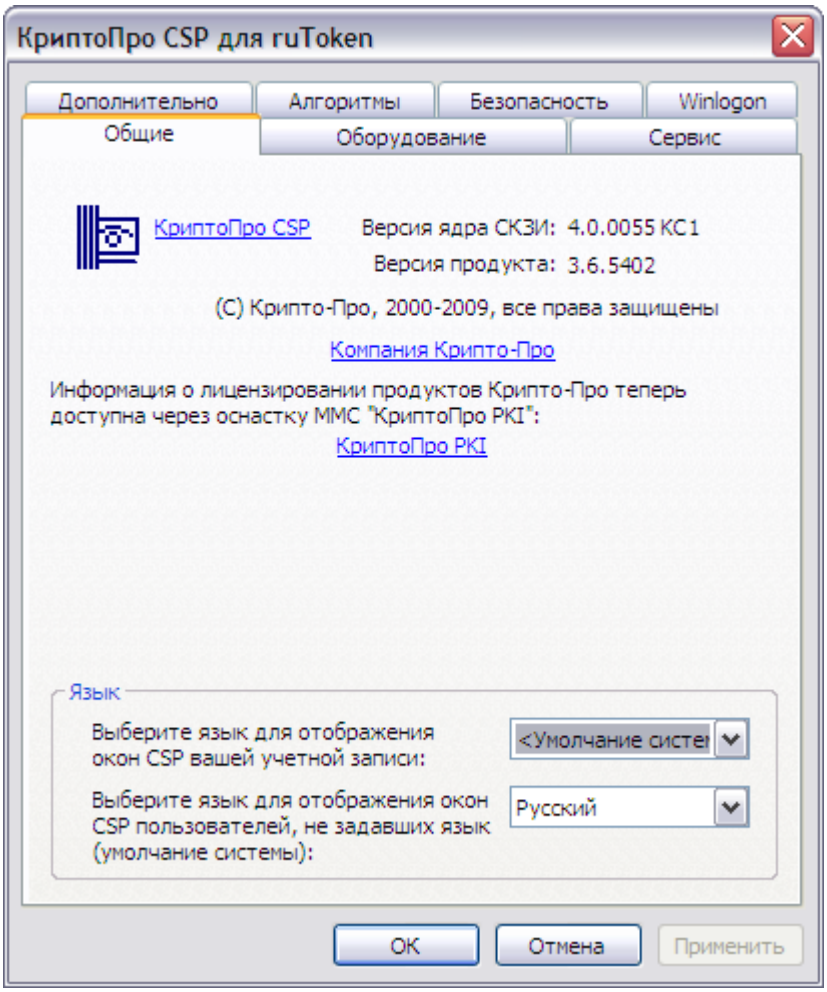


2. Интерфейс СКЗИ «Рутокен CSP»

2.1. Доступ к панели управления СКЗИ «Рутокен CSP»

Данный раздел является инструкцией по использованию панели управления программно-аппаратного комплекса криптографической защиты информации Рутокен CSP. Панель управления СКЗИ Рутокен CSP доступна из Панели управления Windows (меню **Пуск** ⇒ **Панель управления** ⇒ **Рутокен CSP**).

Рисунок 9. Панель управления Рутокен CSP



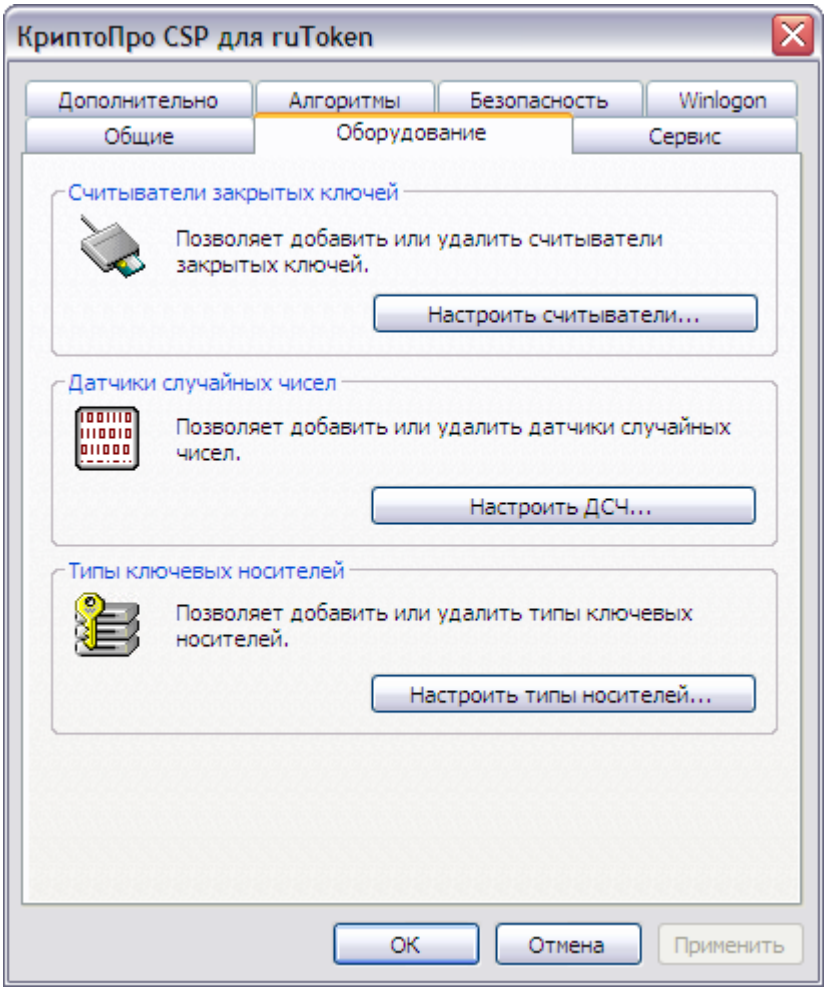
2.2. Общая настройка СКЗИ

Закладка **Общие** панели управления СКЗИ Рутокен CSP предназначена для просмотра информации о версии установленного ПАК СКЗИ Рутокен CSP и для изменения языка отображения окон, выдаваемых криптопровайдеров.

2.3. Настройка оборудования

Закладка **Оборудование** панели управления СКЗИ Рутокен CSP (см. Рисунок 10) предназначена для изменения набора устройств хранения и считывания ключевой информации и датчиков случайных чисел (ДСЧ).

Рисунок 10. Закладка «Оборудование» панели управления Рутокен CSP



При установке СКЗИ Рутокен CSP все необходимые считыватели, ключевые носители и датчики случайных чисел устанавливаются автоматически. Данная закладка предназначена для работы с совместимыми устройствами.

2.4. Работа с контейнерами и сертификатами

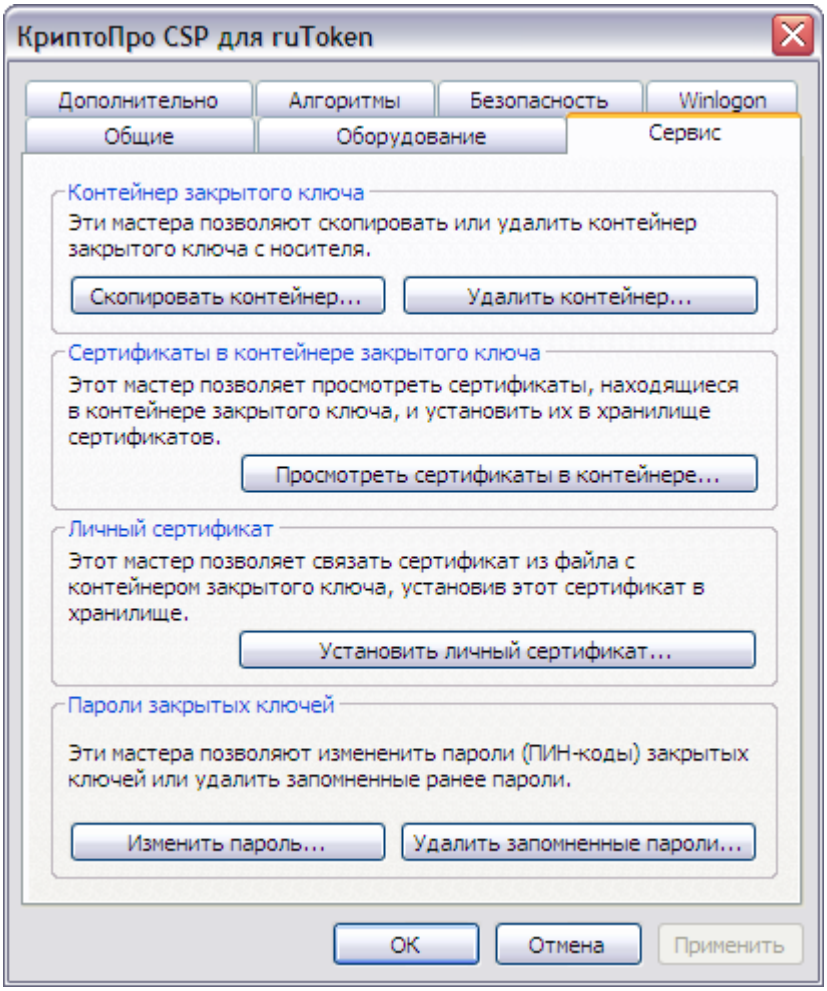
Закладка **Сервис** панели управления СКЗИ Рутокен CSP предназначена для выполнения следующих операций:

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

2.4.1. Копирование и удаление контейнера закрытого ключа

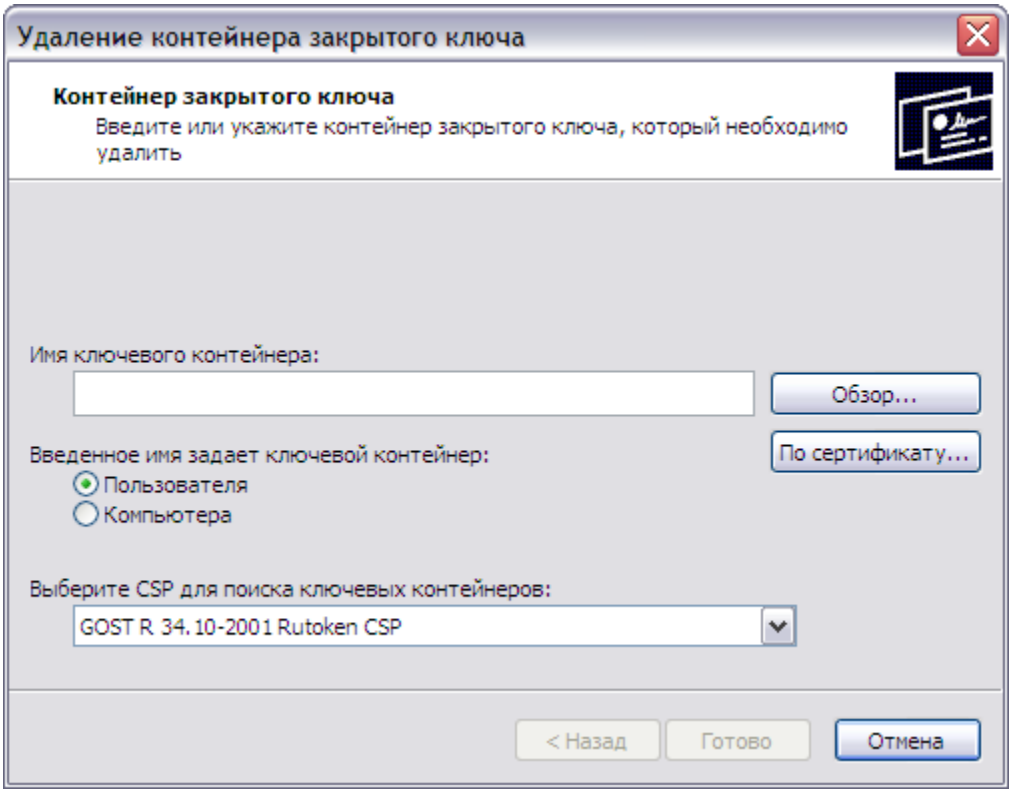
Контейнер закрытого ключа Рутокен CSP со смарткарты Магистра скопировать нельзя. Мастер копирования оставлен только для совместимых ключевых носителей. Для того, чтобы удалить контейнер, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Удалить контейнер**.

Рисунок 11. Закладка «Сервис» панели управления Рутокен CSP



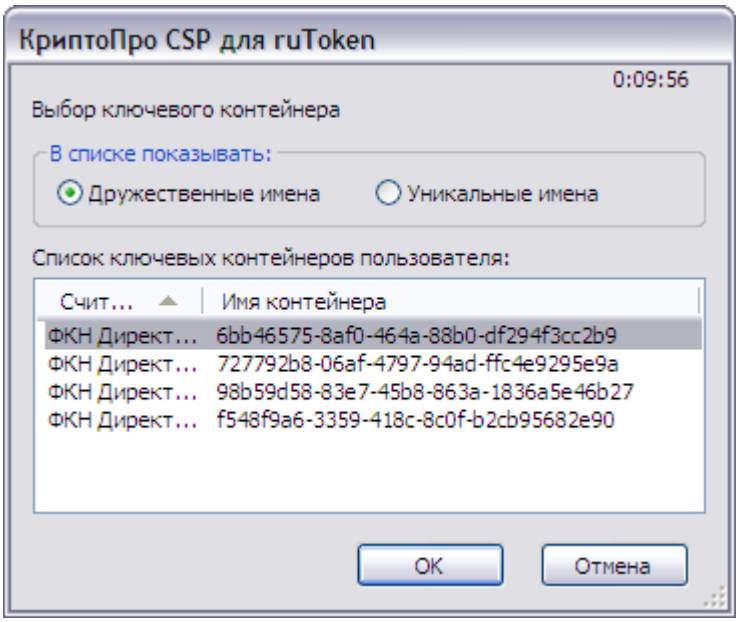
Система отобразит окно «Удаление контейнера закрытого ключа» (см. Рисунок 12).

Рисунок 12. Удаление контейнера закрытого ключа



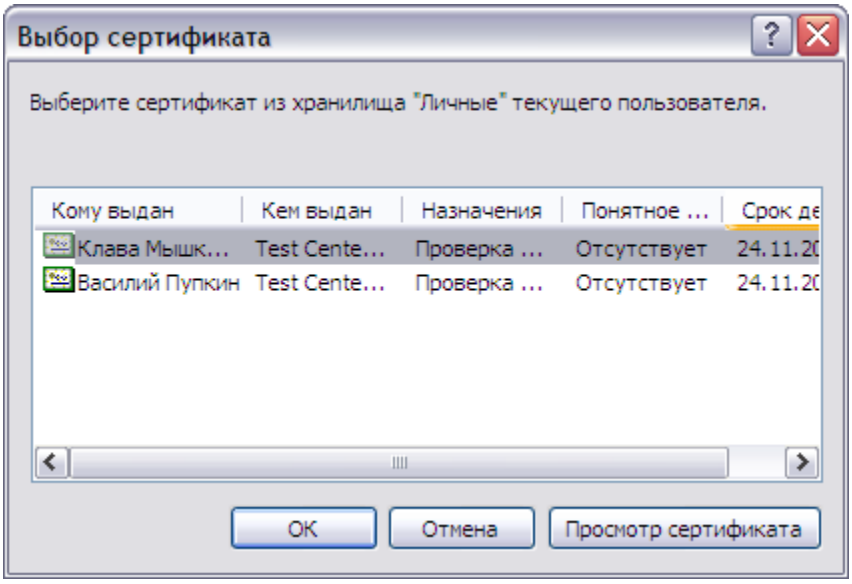
В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Рисунок 13. Выбор ключевого контейнера для копирования



Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, контейнер которого необходимо удалить (см. Рисунок 14).

Рисунок 14. Выбор сертификата для удаления контейнера



Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

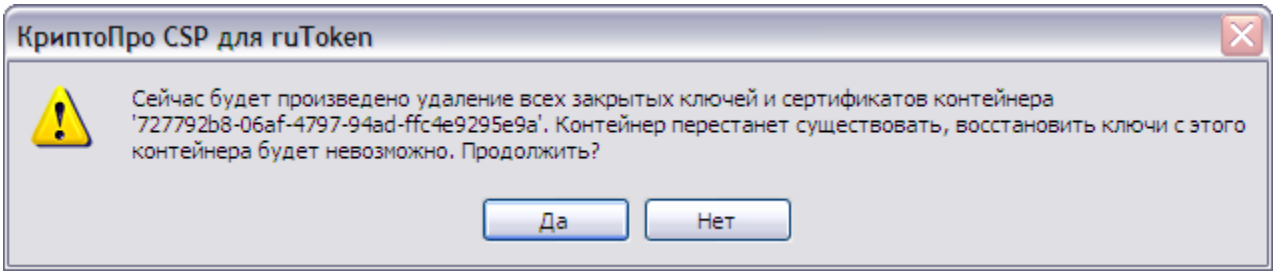
Опция **Введенное имя задает ключевой контейнер** (см. Рисунок 12) может быть установлена в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически.

Опция **Выберите CSP для поиска ключевых контейнеров** (см. Рисунок 12) позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку **Готово**.

Система отобразит окно подтверждения удаления ключевого контейнера (см. Рисунок 15). Нажмите кнопку **Да.** СКЗИ «Магистра CSP» произведет удаление ключевого контейнера.

Рисунок 15. Окно подтверждения удаления ключевого контейнера

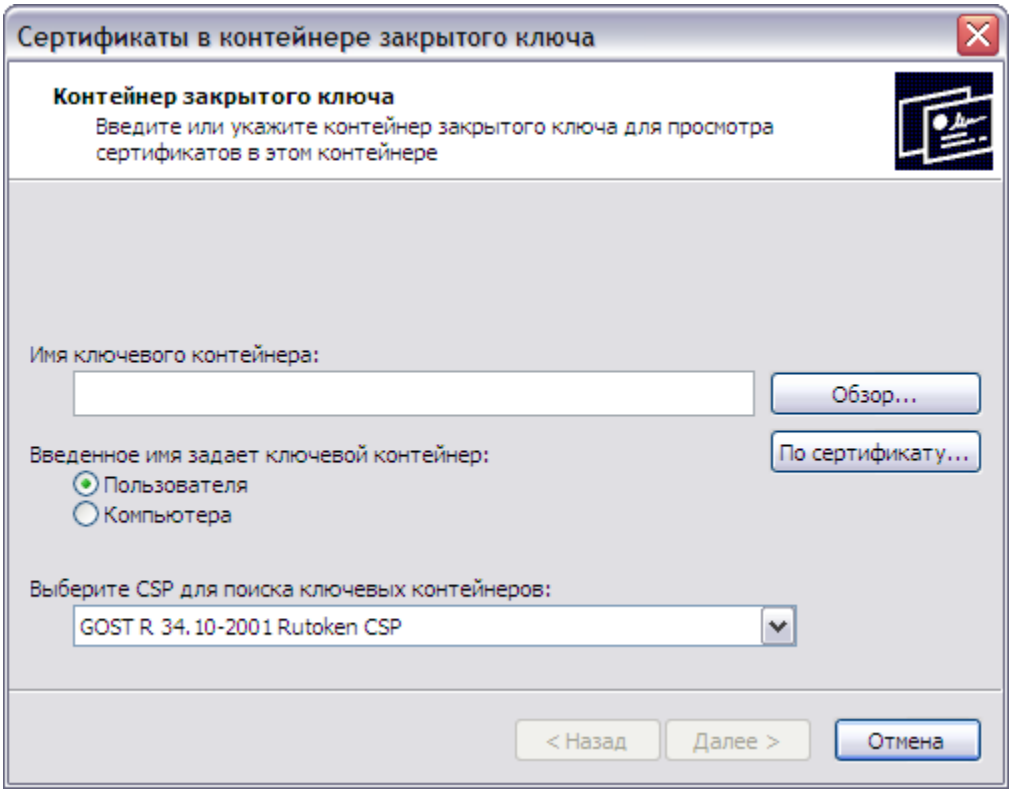


2.4.2. Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа

Для того, чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Просмотреть сертификаты в контейнере**.

Система отобразит окно «Сертификаты в контейнере закрытого ключа» (см. Рисунок 16).

Рисунок 16. Сертификаты в контейнере закрытого ключа



В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, контейнер которого необходимо удалить (см. Рисунок 14).

Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

Опция **Введенное имя задает ключевой контейнер** может быть установлена 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.

Опция **Выберите CSP для поиска ключевых контейнеров** позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

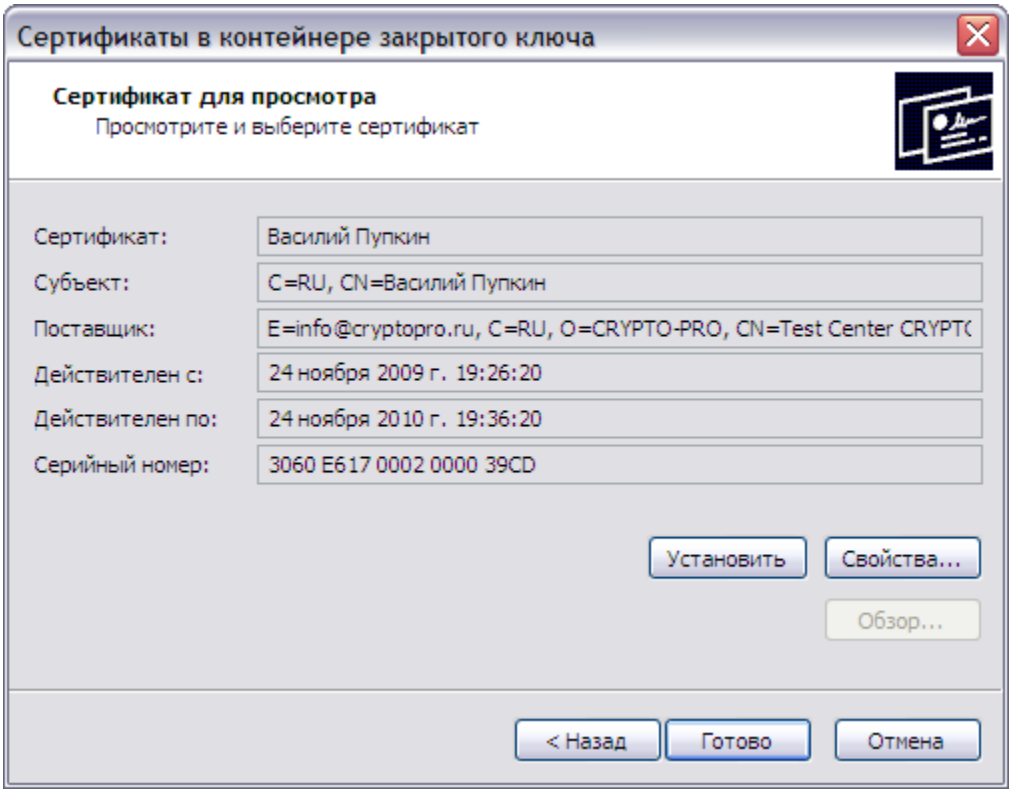
После того, как все поля заполнены, следует нажать на кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Сертификат для просмотра» (см. Рисунок 17).

Если в контейнере закрытого ключа сертификат отсутствует, то будет отображено окно с соответствующей информацией.

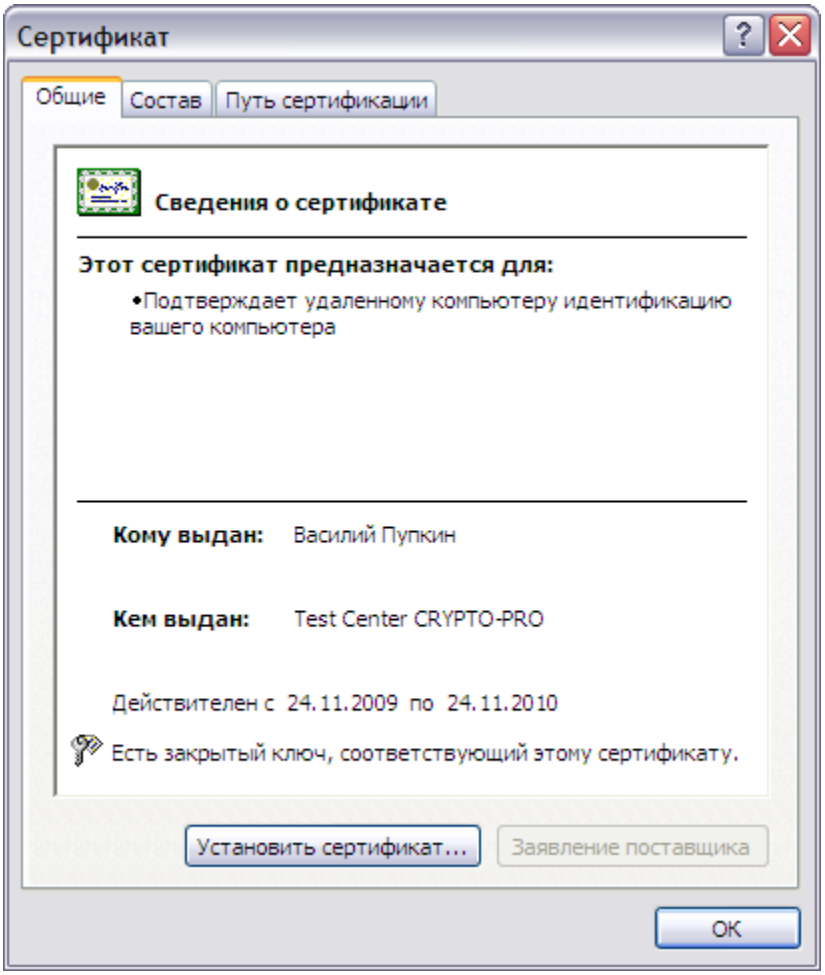
В этом случае просмотр сертификата будет недоступен.

Рисунок 17. Окно «Сертификат для просмотра»



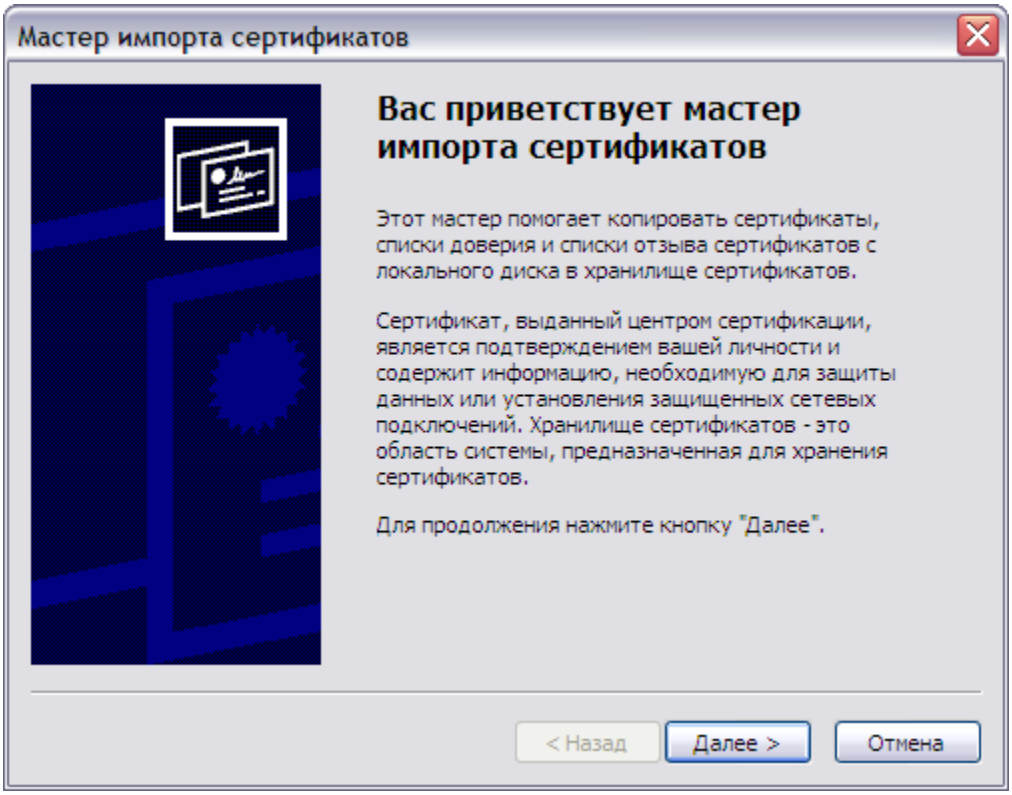
Для просмотра основных свойств сертификата нажмите кнопку **Свойства**. Система отобразит окно «Сертификат», со свойствами выбранного сертификата (см. Рисунок 18).

Рисунок 18. Окно просмотра свойств сертификата



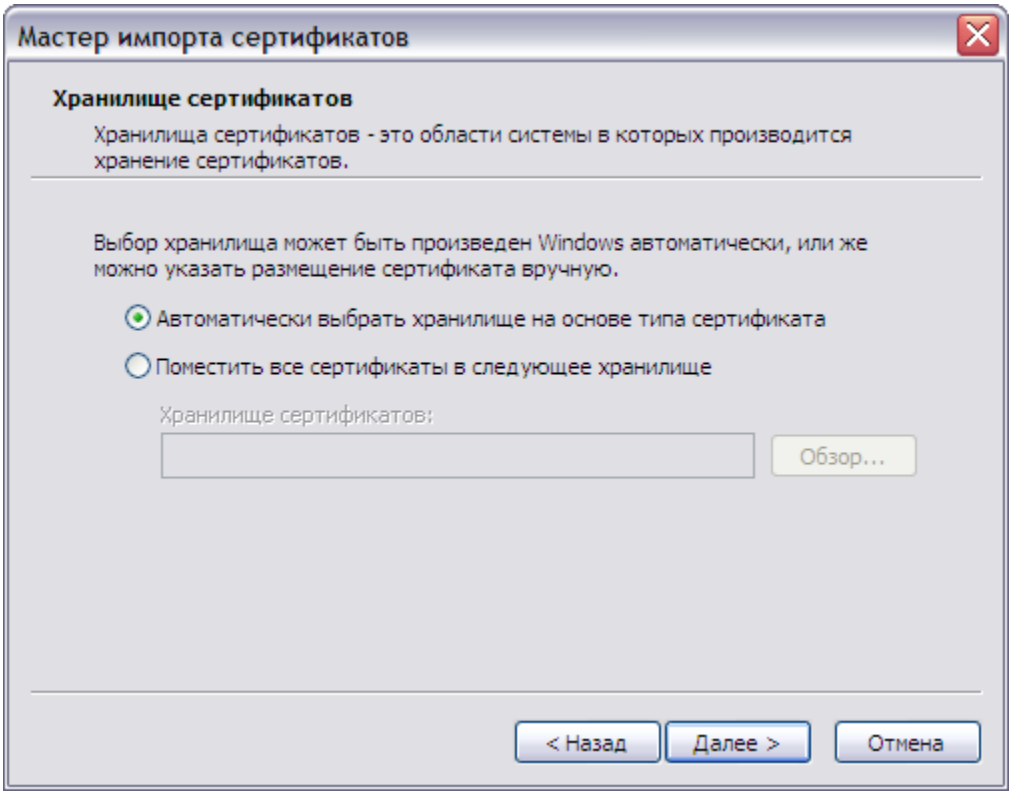
Если требуется установить сертификат, находящийся в контейнере, в хранилище сертификатов, то следует в окне просмотра свойств сертификата нажать на кнопку **Установить сертификат**. Будет запущен **Мастера импорта сертификатов** (см. Рисунок 19).

Рисунок 19. Мастер импорта сертификатов



Нажмите кнопку **Далее**. Система отобразит окно «Хранилище сертификатов», в котором необходимо указать, в какое хранилище требуется поместить сертификат (см. Рисунок 20).

Рисунок 20. Выбор хранилища

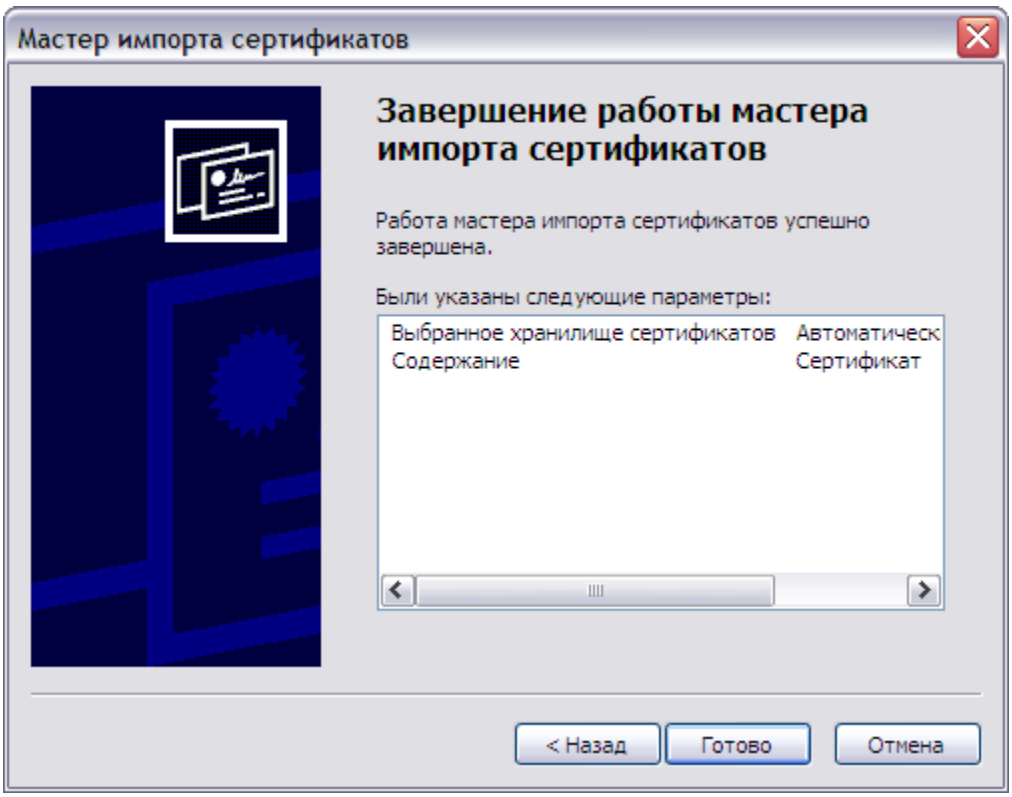


Установите переключатель **Автоматически выбрать хранилище на основе типа сертификата**, если Вы хотите, чтобы сертификат из контейнера закрытого ключа был установлен в хранилище «Личные» текущего пользователя. Так же есть возможность указать размещение сертификата вручную, для этого следует выбрать опцию **Поместить все сертификаты в следующее хранилище** и в появившемся окне выбрать нужное хранилище.

При необходимости установки сертификата в хранилище «Личные» локального компьютера следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Установить личный сертификат**.

После выполненных действий нажмите кнопку **Далее**. Система отобразит окно «Завершение работы мастера импорта сертификатов» (см. Рисунок 21).

Рисунок 21. Завершение мастера импорта сертификатов



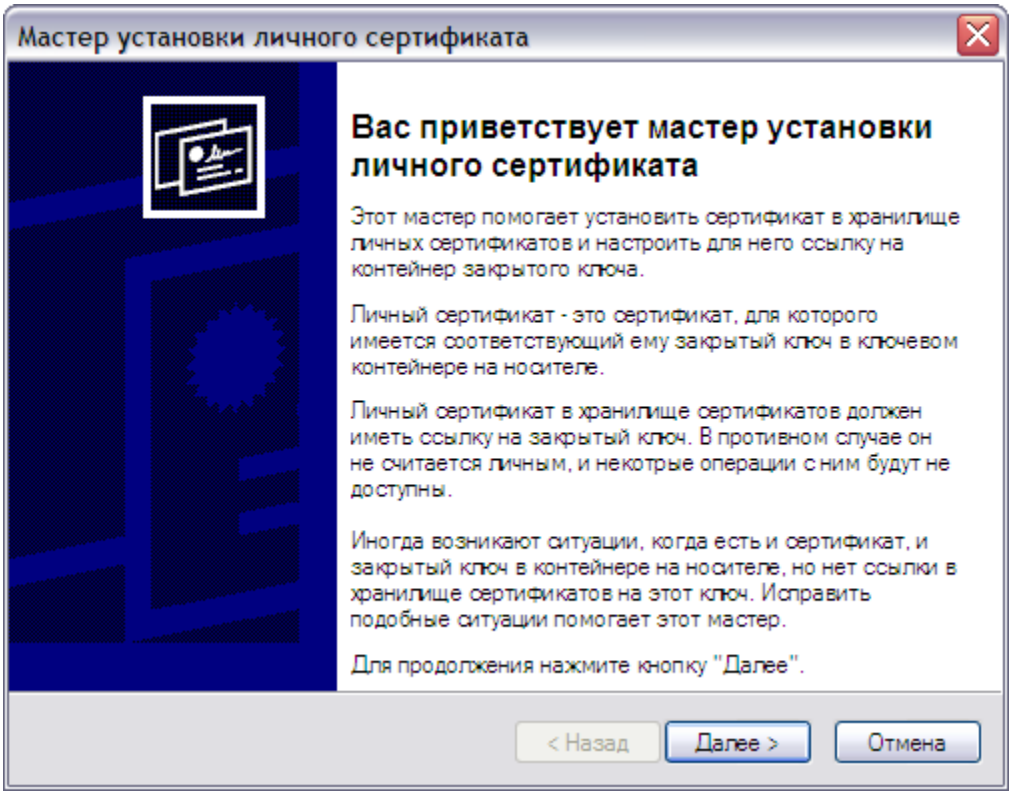
Проверьте правильность выбранных параметров и нажмите кнопку **Готово.** Будет отображено окно, информирующее пользователя об успешной установке сертификата.

2.4.3. Установка личного сертификата, хранящегося в файле

Для того, чтобы связать личный сертификат, хранящийся в файле с контейнером закрытого ключа, установив сертификат в хранилище «Личные» следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать кнопку **Установить личный сертификат**.

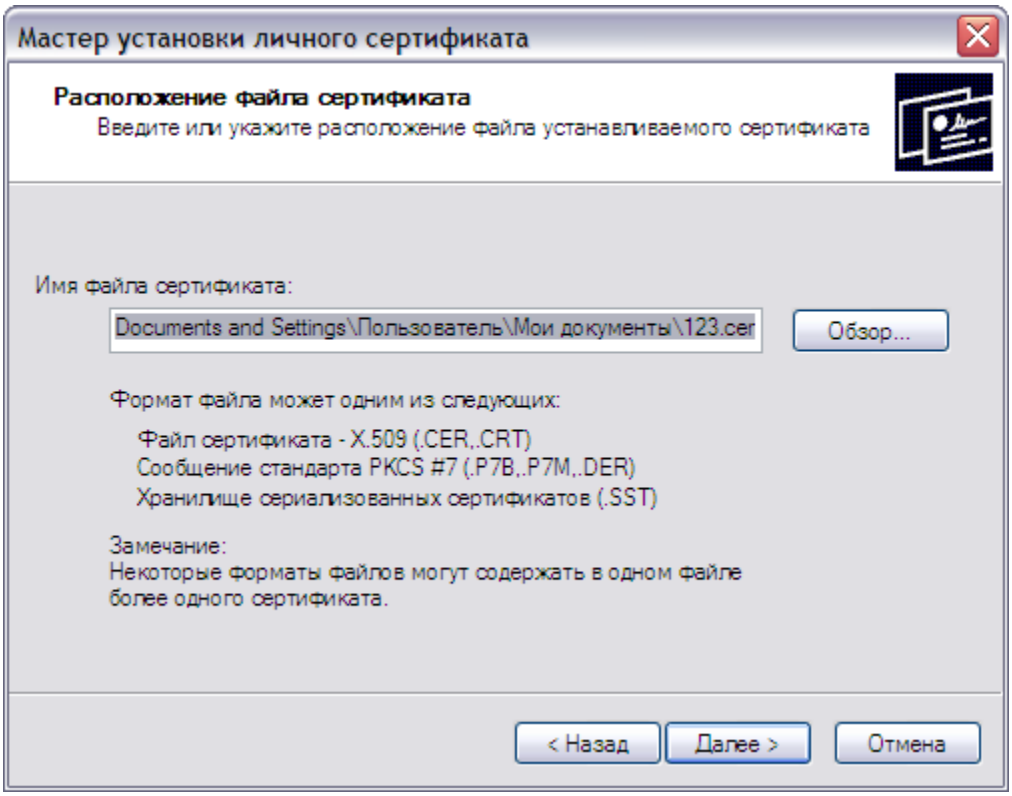
Будет запущен Мастер установки личного сертификата (см. Рисунок 22). Ознакомьтесь с текстом и нажмите кнопку **Далее.**

Рисунок 22. Мастер установки личного сертификата



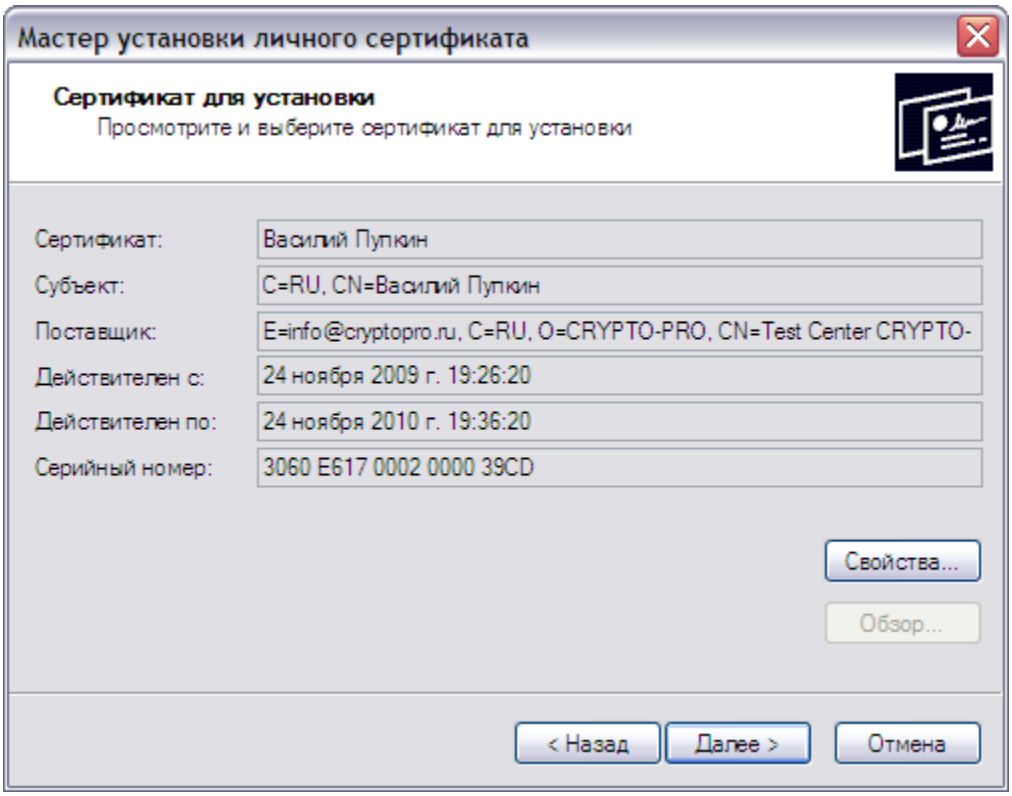
Система отобразит окно «Расположение файла сертификата» (см. Рисунок 23). В поле **Имя файла сертификата** укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее.**

Рисунок 23. Окно «Расположение файлов сертификата»



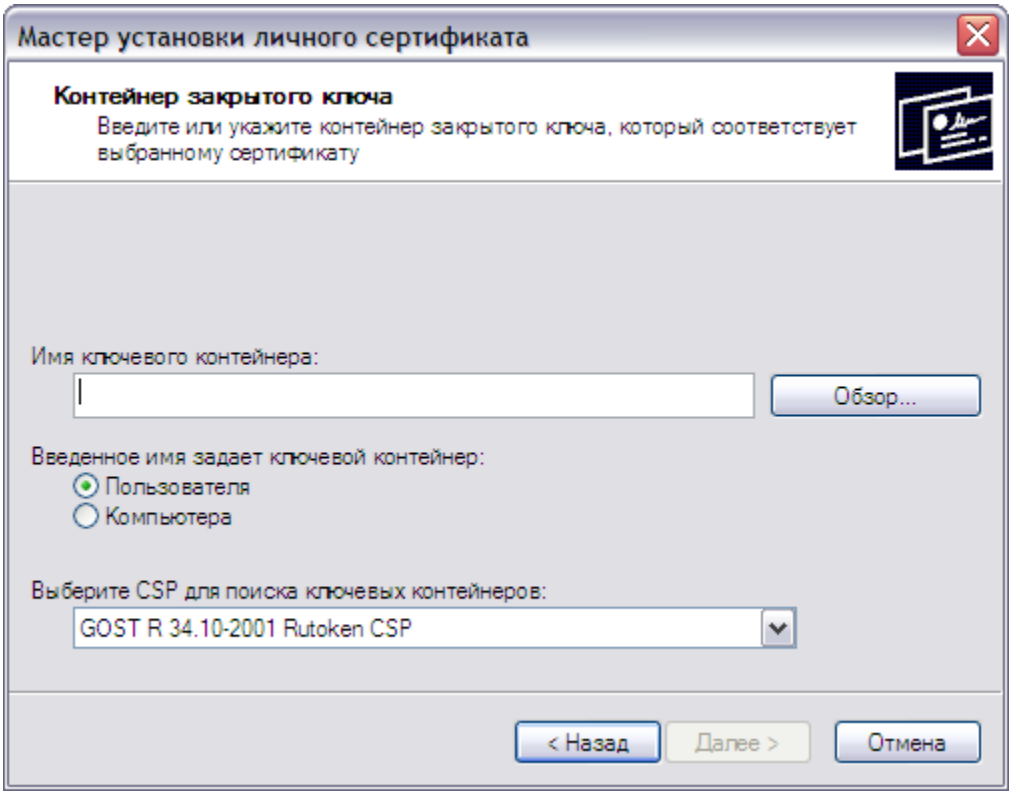
Система перейдет к окну «Сертификат для установки» (см. Рисунок 24). В нем выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

Рисунок 24. Окно «Сертификат для установки»



Нажмите кнопку **Далее**. Система отобразит окно «Контейнер закрытого ключа» (см. Рисунок 25).

Рисунок 25. Окно «Контейнер закрытого ключа»



В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка (см. Рисунок 13) посредством нажатия кнопки **Обзор.**

Опция «Введенное имя задает ключевой контейнер» может быть установлена в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер.

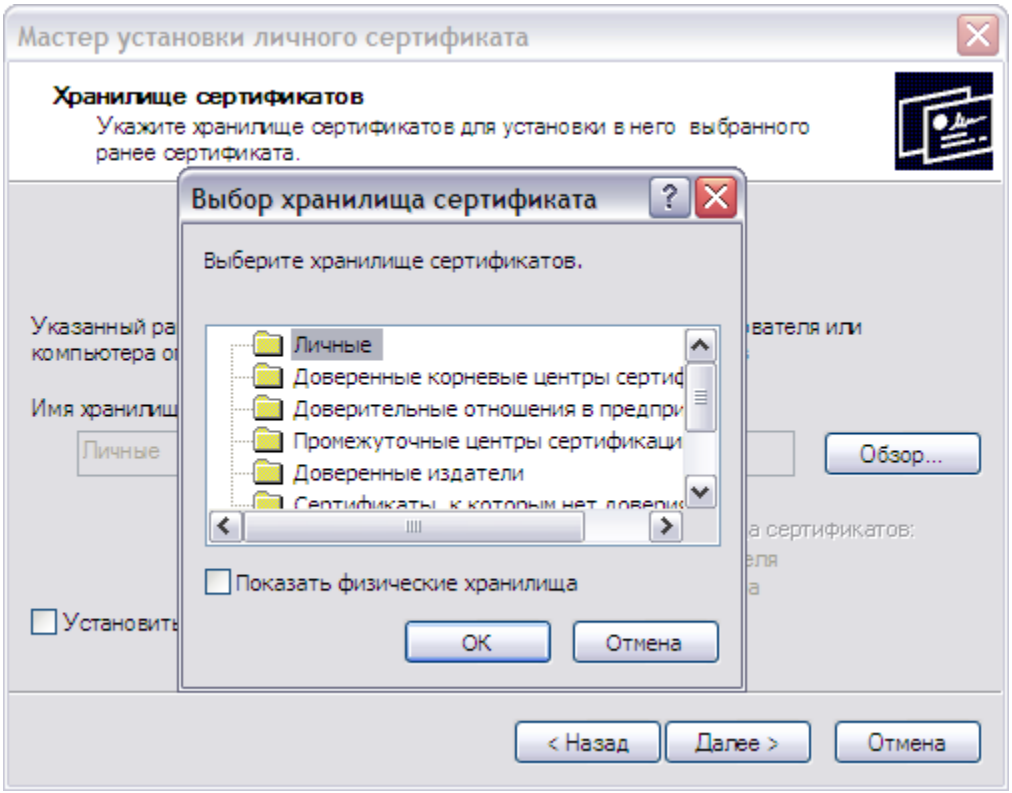
Опция «Выберите CSP для поиска ключевых контейнеров» позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на 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. Рисунок 26).

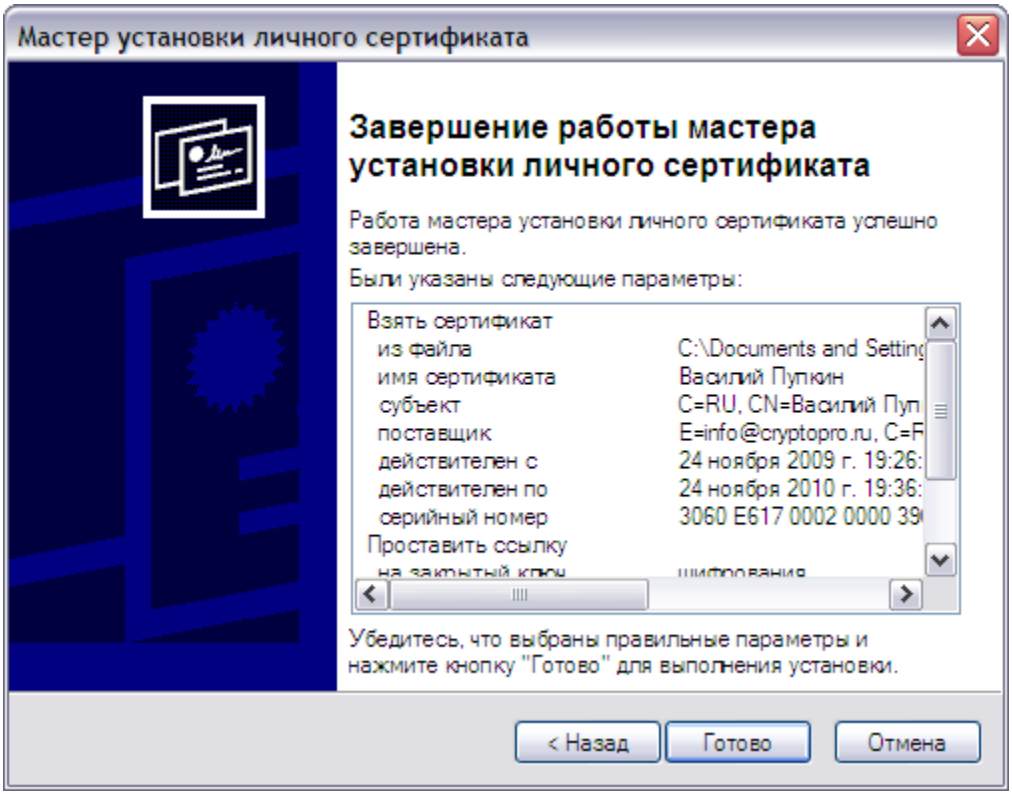
С помощью кнопки **Обзор** выберите хранилище «Личные». Сертификат будет установлен в хранилище «Личные» текущего пользователя или в хранилище «Личные» локального компьютера, в зависимости от значения переключателя опции «Введенное имя задает ключевой контейнер», заданной на предыдущем шаге. Изменить значение данной опции нельзя; оно определяется расположением контейнера закрытого ключа.

Рисунок 26. Окно «Хранилище сертификатов»



После выбора хранилища система отобразит окно «Завершение работы мастера установки личного сертификата» (см. Рисунок 27).

Рисунок 27. Завершение работы мастера установки личного сертификата



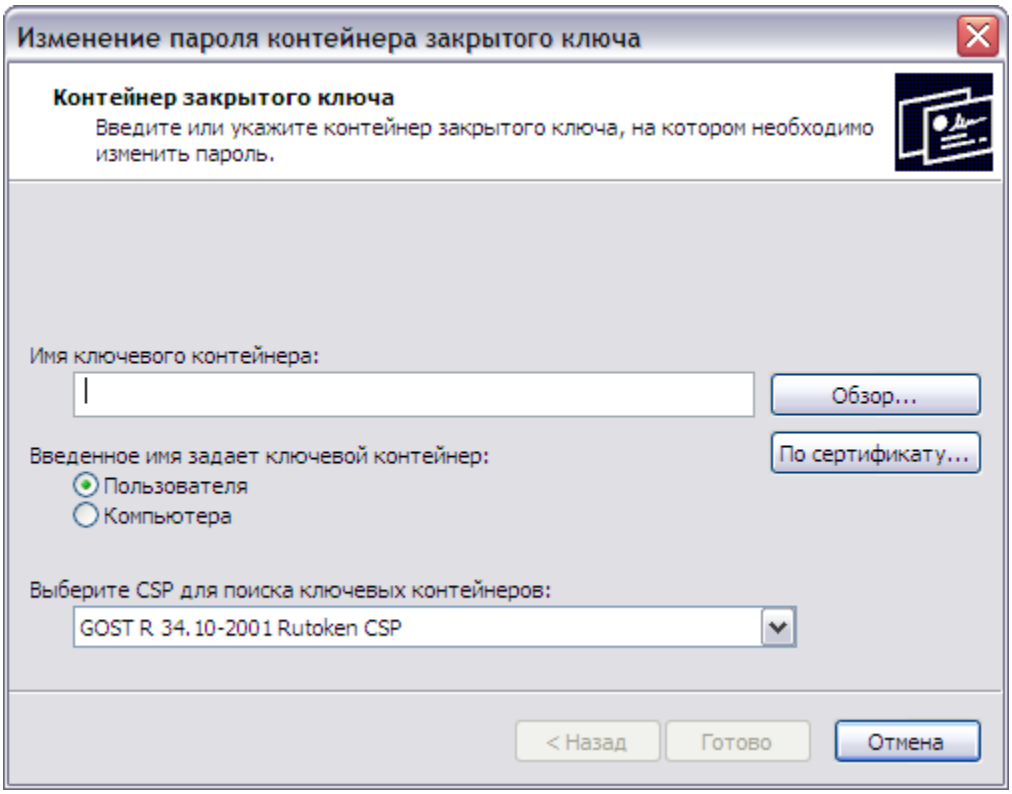
Проверьте правильность указанных данных и нажмите кнопку **Готово.** СКЗИ «Магистра CSP» произведет установку сертификата.

2.5. Управление паролями доступа к закрытым ключам

Для того чтобы изменить пароль на доступ к закрытому ключу, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать на кнопку **Изменить пароль**.

Система отобразит окно «Изменение пароля контейнера закрытого ключа» (см. Рисунок 28).

Рисунок 28. Изменение пароля контейнера закрытого ключа



В этом окне необходимо заполнить **Имя ключевого контейнера** – его можно ввести вручную или выбрать из списка посредством нажатия кнопки **Обзор.**

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** следует нажать кнопку **По сертификату** и выбрать сертификат, на доступ к контейнеру закрытого ключа которого необходимо изменить пароль.

Выбор сертификата производится из хранилища «Личные» текущего пользователя. Если у пользователя есть права администратора, то выбор будет производиться из хранилища «Личные» локального компьютера.

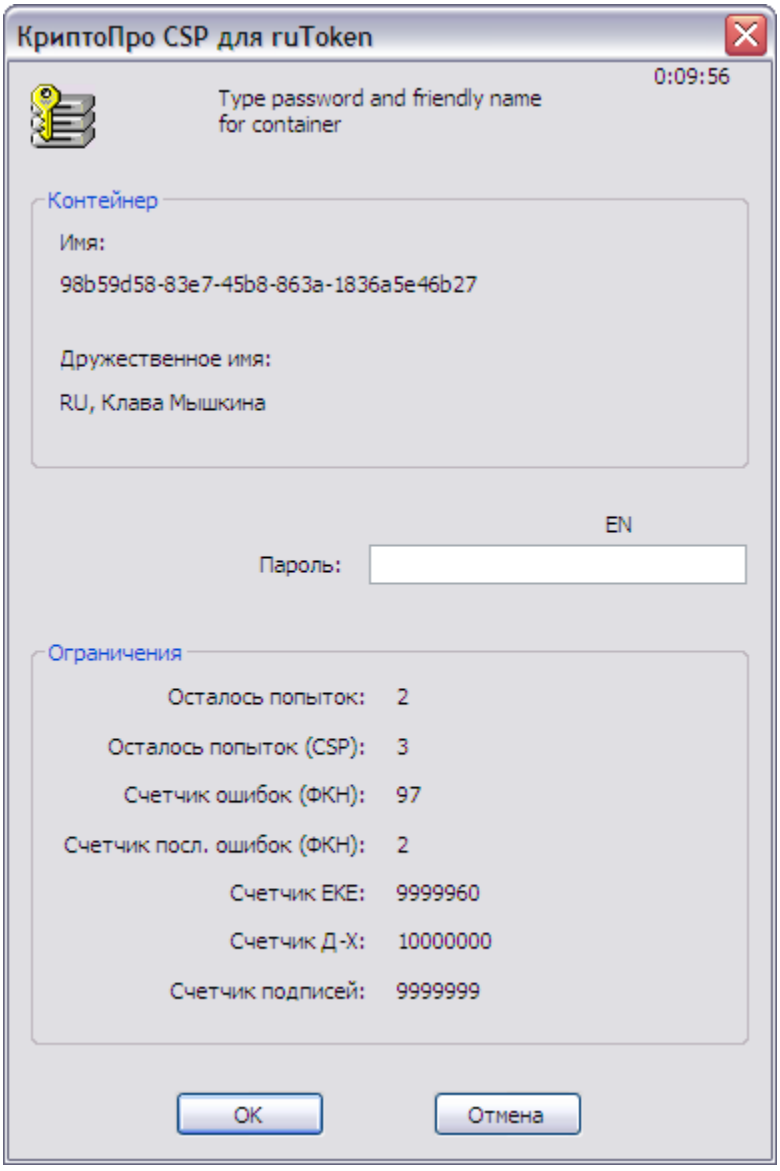
Опция **Введенное имя задает ключевой контейнер** может быть установлена в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер. При выборе контейнера по сертификату переключатель будет установлен в нужное положение автоматически.

Опция **Выберите CSP для поиска ключевых контейнеров** позволяет выбрать криптопровайдер (CSP) из предлагаемого списка.

После того, как все поля заполнены, следует нажать на кнопку **Готово**. Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его (см. Рисунок 29). Введите пароль и нажмите кнопку **ОК**. Если пароль введен неверно, система попросит повторно ввести пароль.

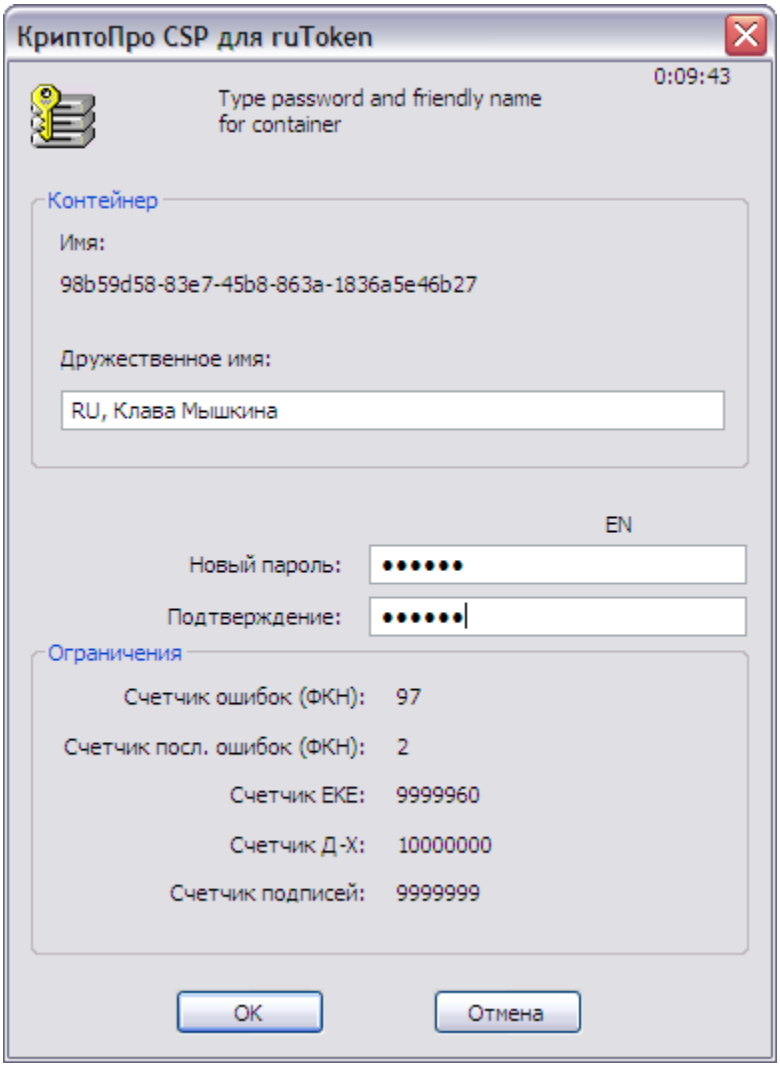
В СКЗИ Рутокен CSP установлено ограничение числа попыток ввода пароля. Превышение этого числа приведет к блокированию контейнера (см. раздел 4).

Рисунок 29. Ввод пароля на доступ к закрытому ключу



Система отобразит окно ввода нового пароля на доступ к закрытому ключу (см. Рисунок 30). Введите дважды новый пароль и нажмите кнопку **ОК**.

Рисунок 30. Ввод нового пароля на доступ к закрытому ключу



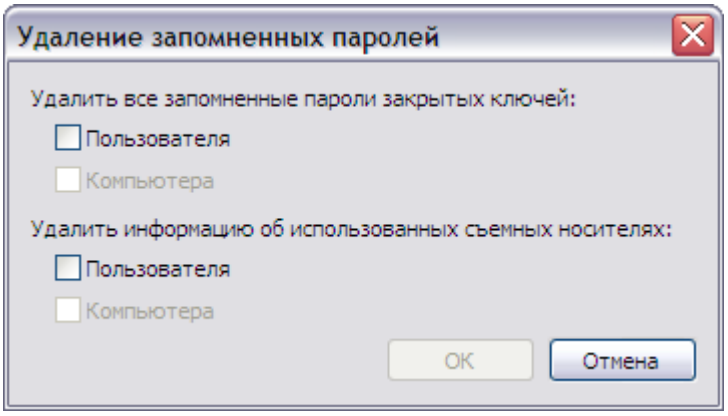
После ввода пароля СКЗИ «Рутокен CSP» осуществит смену пароля на доступ к закрытому ключу.

СКЗИ «Рутокен CSP» позволяет удалить запомненные пароли доступа к контейнерам закрытых ключей и информацию об использованных съемных носителях.

Для того чтобы удалить запомненный пароль, следует выбрать вкладку **Сервис** панели управления Рутокен CSP (см. Рисунок 11) и нажать на кнопку **Удалить запомненные пароли.**

Система отобразит окно «Удаление запомненных паролей» (см. Рисунок 31).

Рисунок 31. Окно «Удаление запомненных паролей»



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

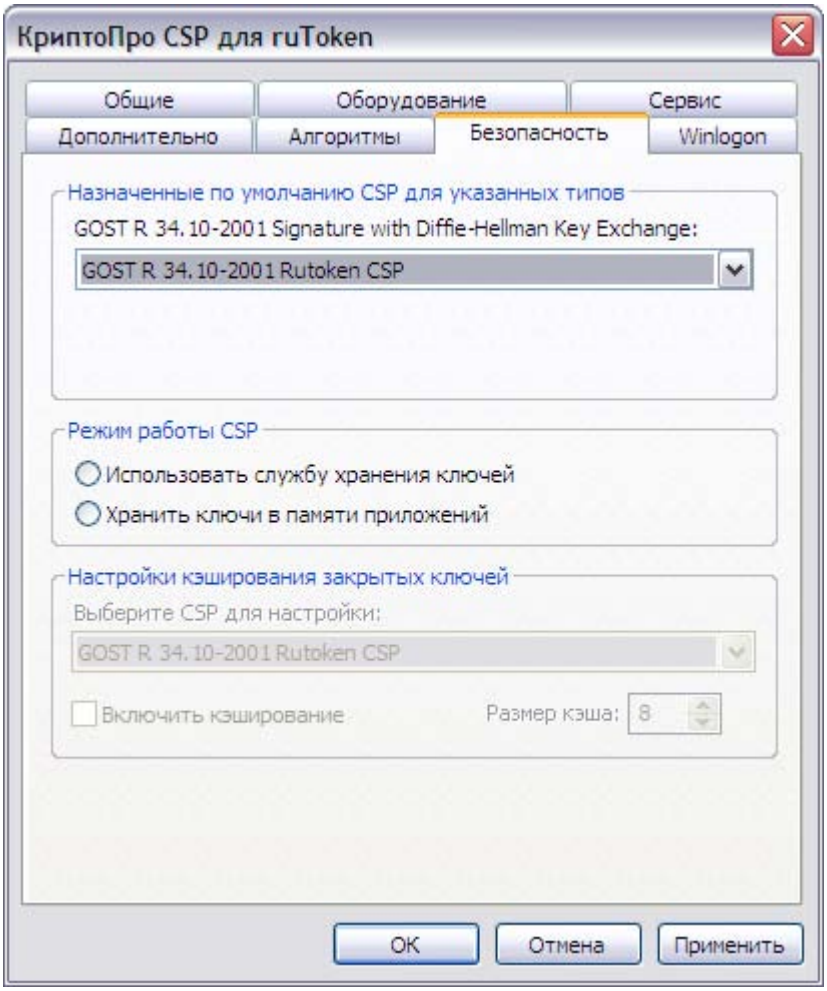
СКЗИ «Рутокен CSP» осуществит удаление сохраненных паролей только из специального хранилища на локальном компьютере, пароль на доступ к закрытому ключу не удаляется.

Кроме того, в этом же окне можно отдельно удалить информацию о физических характеристиках носителей, на которых расположены ключевые контейнеры, использовавшиеся раньше 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

Закладка **Безопасность** (см. Рисунок 32) панели управления СКЗИ Рутокен CSP предназначена для выбора параметров безопасности при работе с СКЗИ «Рутокен CSP».

Рисунок 32. Закладка «Безопасность» панели управления СКЗИ Рутокен CSP



В данном окне можно назначить криптопровайдер, используемый по умолчанию.

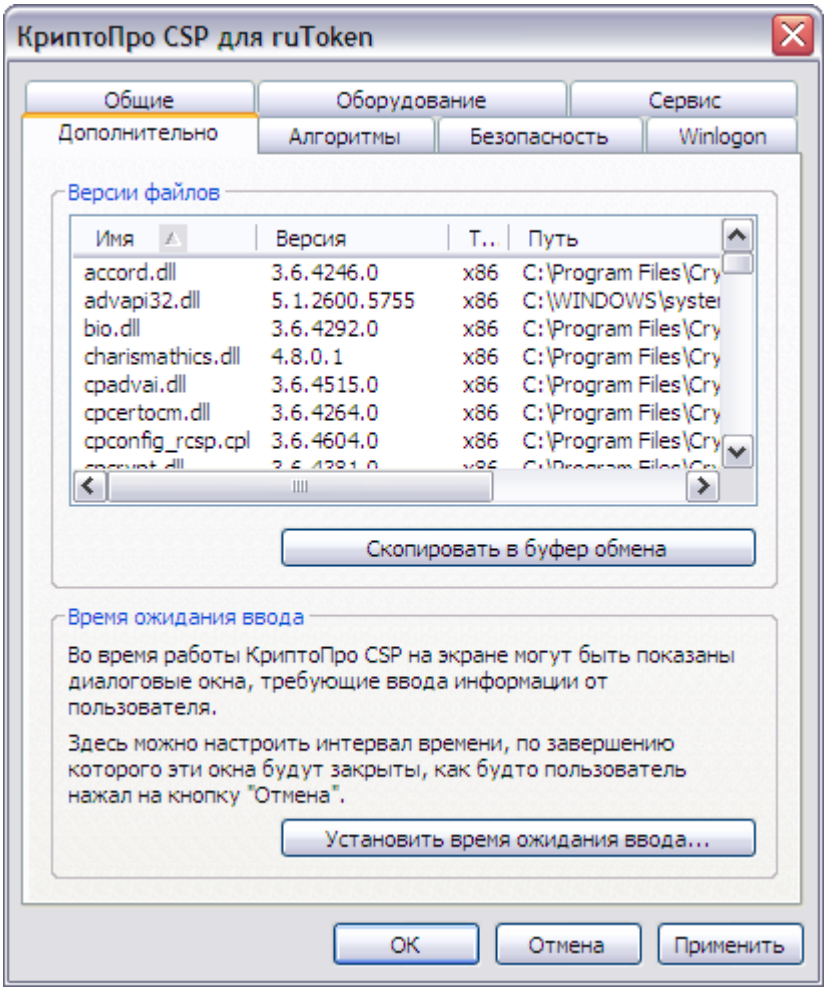
В СКЗИ «Рутокен CSP» хранение ключей (в памяти приложений и в службе хранения ключей) запрещено, все ключи хранятся только на ключевых носителях. Также в СКЗИ «Рутокен CSP» не используется кэширование контейнеров закрытых ключей - ключи не покидают пределов носителя.

2.7. Дополнительные настройки

Закладка **Дополнительно** (см. Рисунок 33) панели управления СКЗИ Рутокен CSP предназначена для выбора параметров безопасности при работе с СКЗИ «Рутокен CSP».

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

Рисунок 33. Закладка «Дополнительно» панели управления СКЗИ Рутокен CSP



2.7.1. Просмотр версий используемых файлов

Для того чтобы удалить запомненный пароль, следует выбрать вкладку **Дополнительно** панели управления Рутокен CSP (см. Рисунок 33). В области **Версии файлов** в табличной форме представлена информация о версиях и путях размещения использующихся СКЗИ «Рутокен CSP» файлов.

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

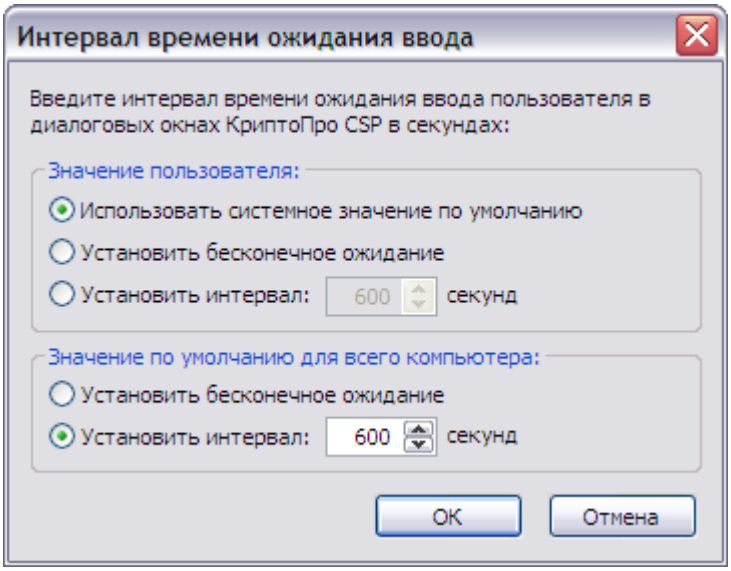
2.7.2. Установка времени ожидания ввода информации от пользователя

Во время работы СКЗИ «Рутокен 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**), следует выбрать вкладку **Дополнительно** панели управления Рутокен CSP (см. Рисунок 33)и нажать на кнопку **Установить время ожидания ввода.**

Система отобразит окно «Интервал времени ожидания ввода» (см. Рисунок 34). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

Рисунок 34. 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**;
- Установить бесконечное ожидание – устанавливает бесконечное ожидание ввода данных от пользователя;
- Установить интервал – определяет интервал времени, во время которого пользователь должен ввести данные.

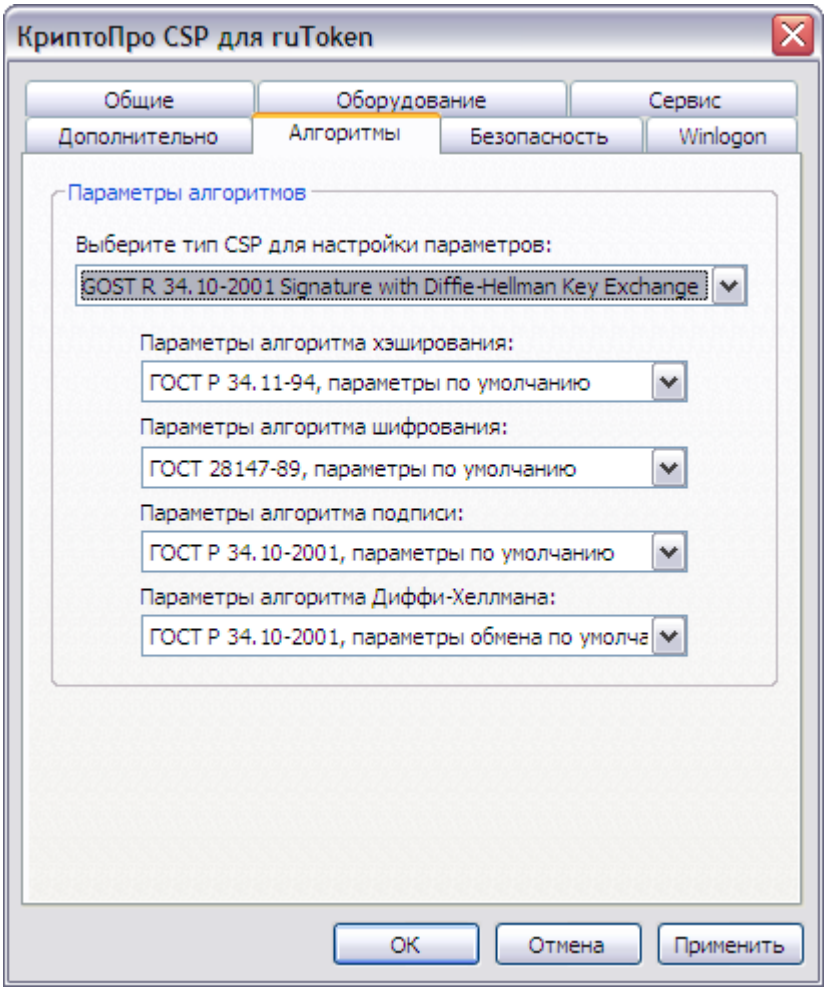
Изменить значение переключателя **Значение по умолчанию для всего компьютера** может только пользователь, являющийся администратором локального компьютера. По умолчанию установлено ожидание ввода в течение 600 секунд.

Значение интервала времени ожидания ввода от пользователя имеет больший приоритет по отношению к значению, заданному 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

Закладка **Алгоритмы** (см. Рисунок 35) панели управления СКЗИ Рутокен CSP предназначена для установки различных параметров реализованных криптографических алгоритмов.

Рисунок 35. Закладка «Алгоритмы» панели управления СКЗИ Рутокен CSP



На закладке **Алгоритмы** можно выбрать тип криптопровайдера, для которого будет осуществляться настройка. В СКЗИ «Рутокен CSP» доступен единственный тип криптопровайдера - GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange.

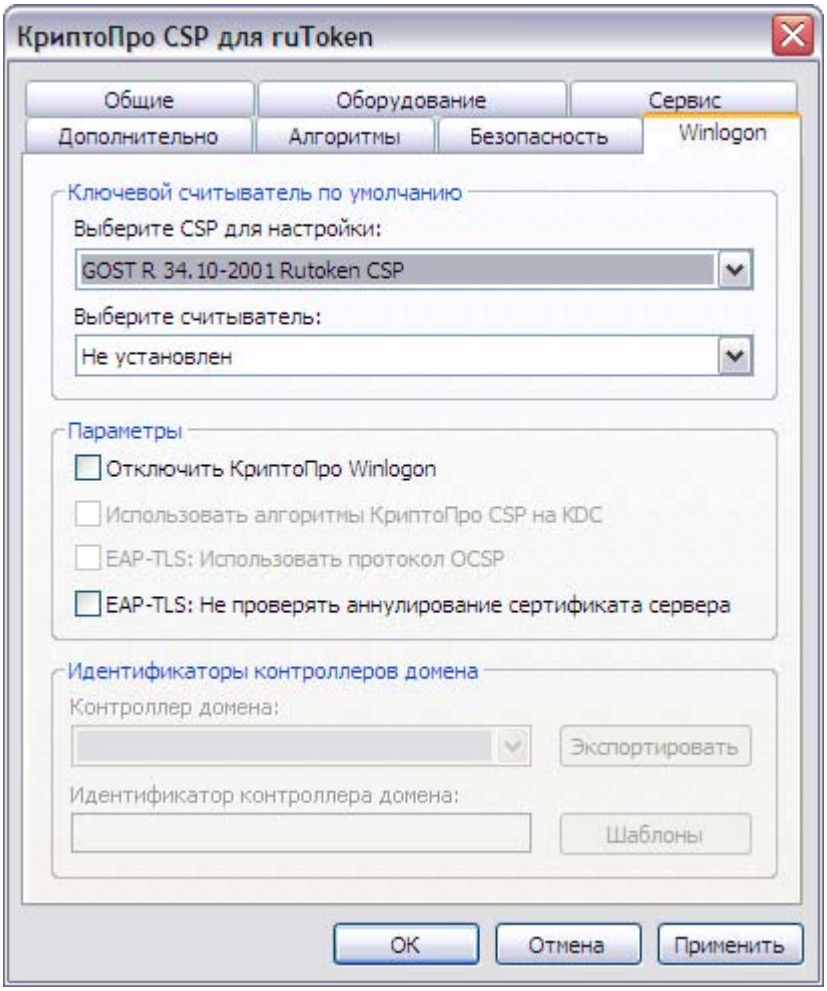
Настройка параметров реализована для следующих криптографических алгоритмов:

- алгоритм хеширования – ГОСТ Р 34.11-94 (параметры по умолчанию);
- алгоритм 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);
- алгоритм выработки и проверки электронной цифровой подписи - ГОСТ Р 34.10-2001 (параметры по умолчанию, параметры Оскар 2.x, параметры подписи 1);
- алгоритм Диффи-Хеллмана - ГОСТ Р 34.10-2001 (параметры обмена по умолчанию, параметры обмена 1).

2.9. Настройка аутентификации в домене Windows

Закладка **Winlogon** (см. Рисунок 36) панели управления СКЗИ Рутокен CSP предназначена для настройки аутентификации в домене с использованием алгоритмов ГОСТ.

Рисунок 36. Закладка «Winlogon» панели управления СКЗИ Рутокен CSP



Подробно настройка КриптоПро Winlogon рассматривается в сопроводительной документации, поставляемой вместе с продуктом КриптоПро Winlogon.

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

3. Интерфейс генерации ключей

3.1. Создание ключевого контейнера

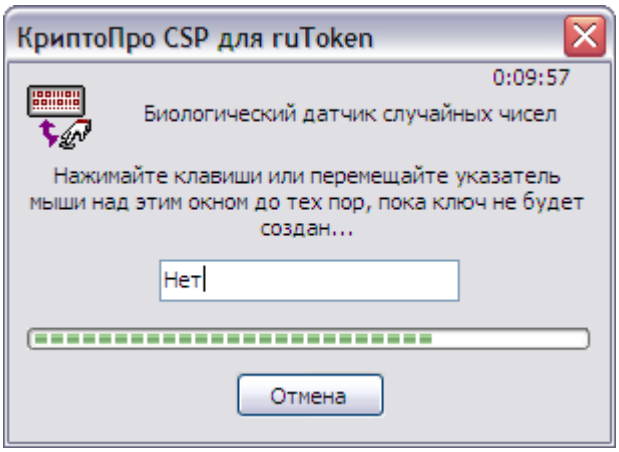
3.1.1. Выбор ключевого носителя

Окно выбора ключевого носителя отображается в том случае, когда пользователь имеет несколько устройств, служащих ключевыми считывателями. В СКЗИ Рутокен CSP изначально установлен только один ключевой считыватель, который выбирается автоматически, и окно выбора ключевого носителя не отображается.

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. Рисунок 37).

Рисунок 37. Биологический датчик случайных чисел



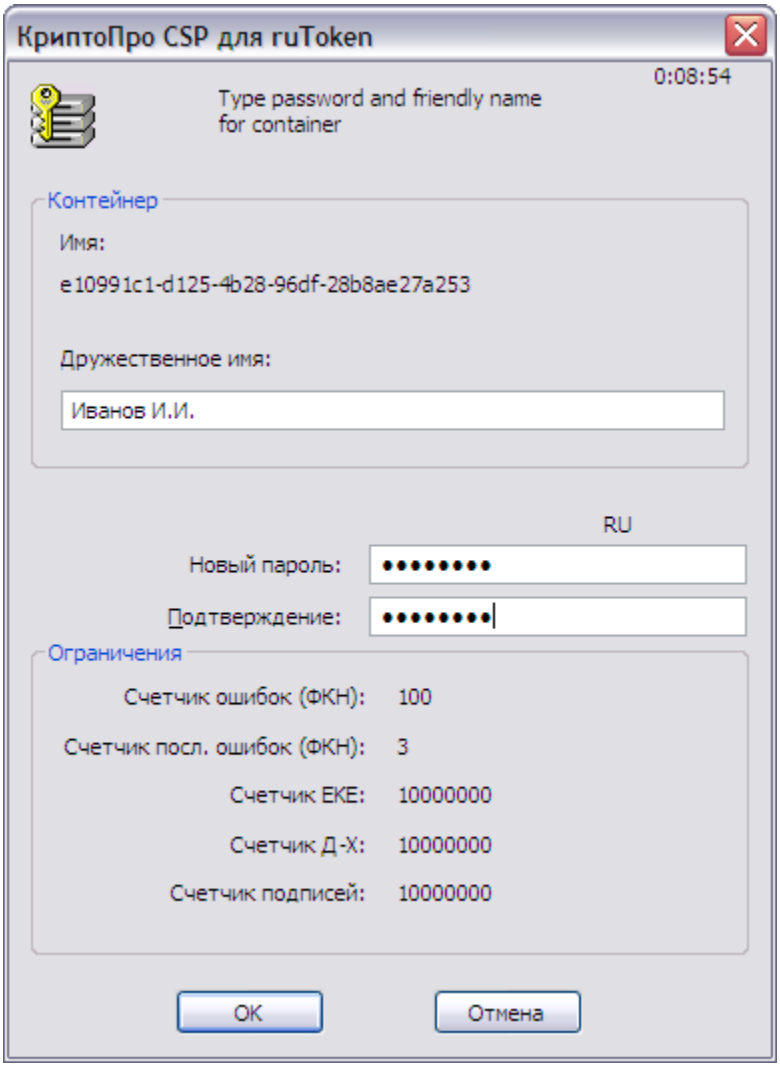
Биологический датчик случайных чисел предназначен для генерации начальной последовательности датчика случайных чисел.

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.1.3. Ввод пароля на доступ к закрытому ключу

После завершения работы биологического датчика случайных чисел система отобразит окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 38).

Рисунок 38. 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**.

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. После того, как носитель будет подключен, система перейдет к окну ввода пароля на доступ к закрытому ключу открываемого контейнера (см. Рисунок 39).

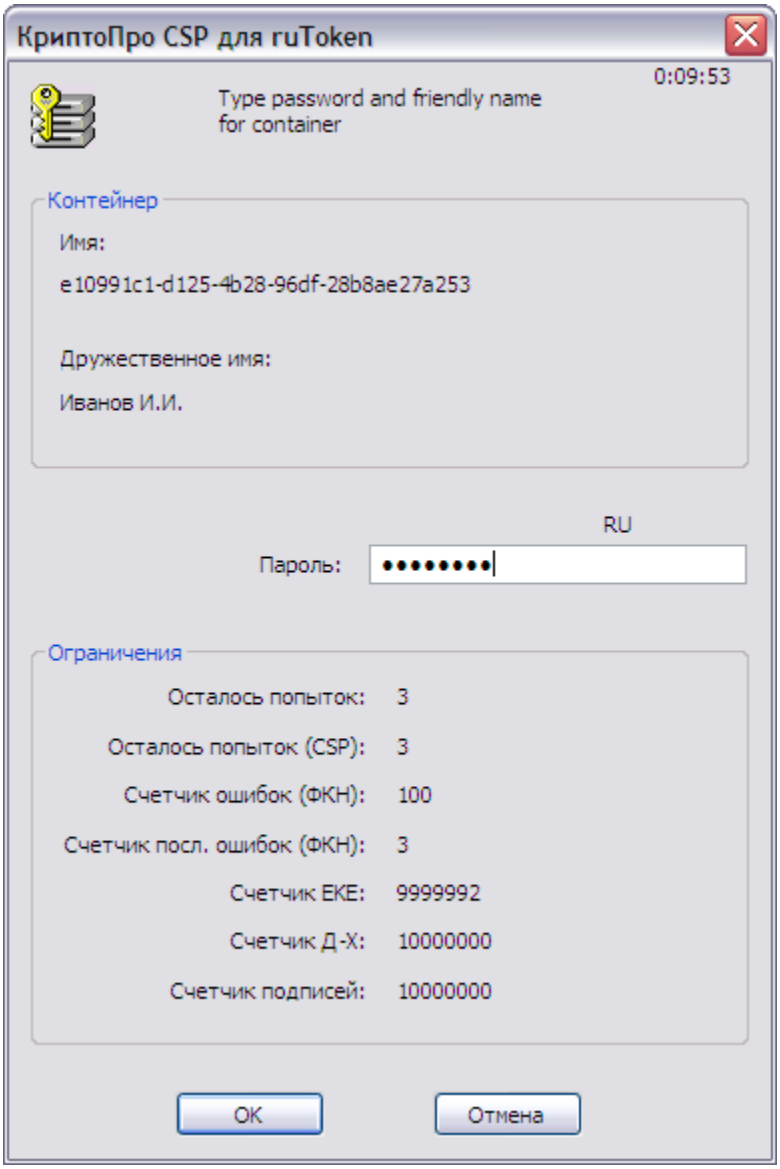
Если требуемый носитель установить не удается, нажмите кнопку **Отмена**. В этом случае процесс открытия контейнера прекратится.

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 (см. Рисунок 39).

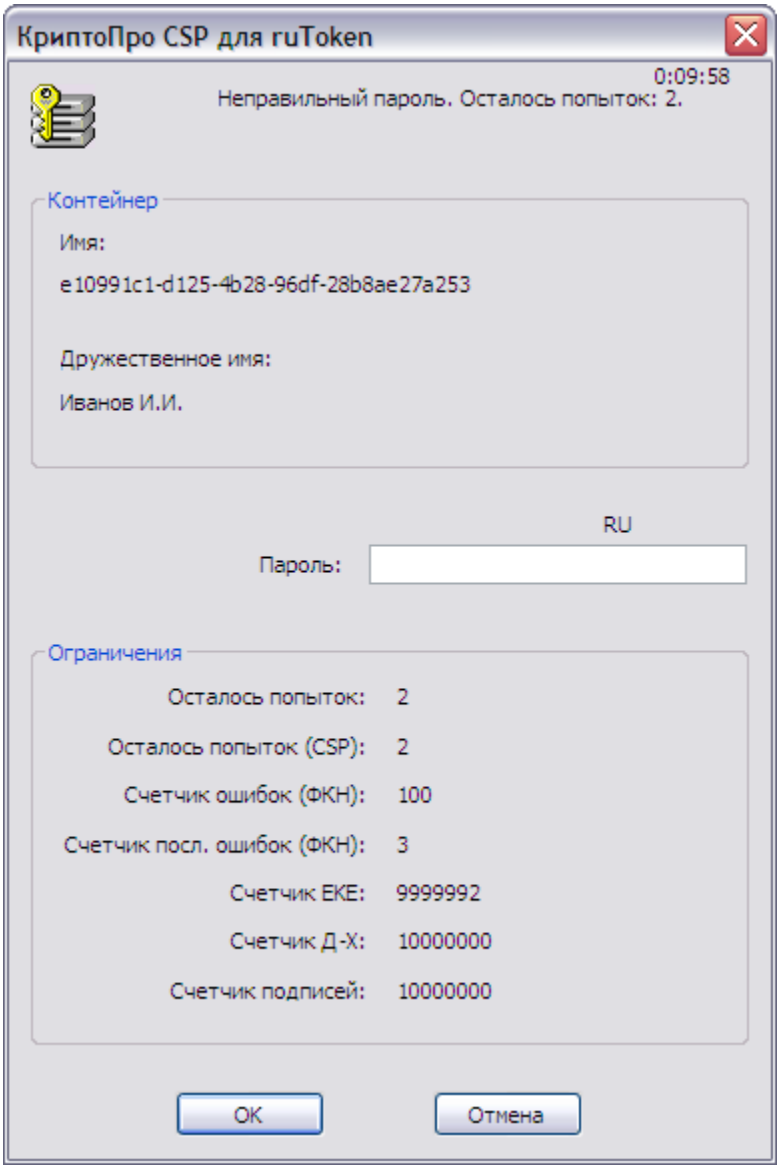
Рисунок 39. Проверка пароля на доступ к закрытому ключу



Если пароль введен неверно, система попросит повторно ввести пароль (см. Рисунок 40).

В СКЗИ Рутокен CSP установлено ограничение числа попыток ввода пароля. Превышение этого числа приведет к блокированию контейнера (см. раздел 4).

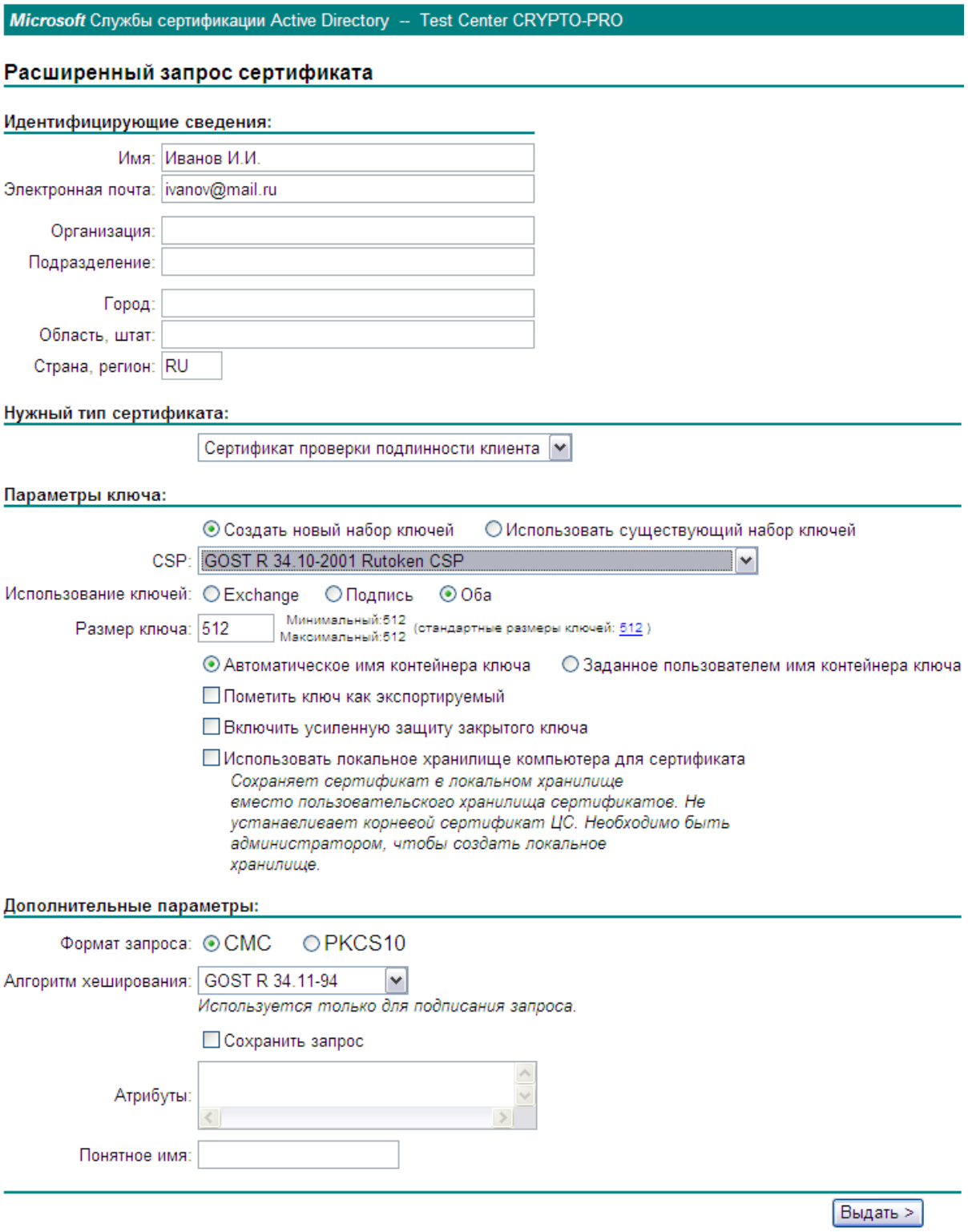
Рисунок 40. Повторный ввод пароля на доступ к закрытому ключу



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 (см. Рисунок 41) либо http://www.CryptoPro.ru/CertSrv_vista для ОС Windows Vista и Windows 2008.

Рисунок 41. Генерация ключа при помощи УЦ



В диалоге создания ключа и формирования запроса на сертификат задайте имя владельца сертификата и введите адрес электронной почты.

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

Выберите нужный тип сертификата в зависимости от его назначения.

В поле **Параметры ключа** выберите тип криптопровайдера Magistra CSP. Задайте остальные параметры ключа и дополнительные параметры, исходя из своих требований к создаваемому ключу.

Нажмите на кнопку **Выдать**.

4. Счетчики и ограничения

В СКЗИ Рутокен CSP поддерживается набор счетчиков на выполнение криптографических операций, количество попыток ввода пароля и количество ошибок. Обнуление любого из данных счетчиков приведет к блокировке контейнера.

Описание счетчиков приведено в таблице:

Таблица 1. Счетчики, используемые в СКЗИ Рутокен CSP

Счетчик	Максимальное значение	Описание
Счетчик попыток ввода пароля	3	Минимальное значение среди всех счетчиков.
Счетчик попыток ввода пароля (CSP)	3	Число попыток ввода пароля через диалог СКЗИ Рутокен CSP. При правильном вводе пароля значение счетчика восстанавливается.
Счетчик ошибок (ФКН)	100 – 256*	Число ошибок аутентификации в протоколе взаимодействия с ФКН.
Счетчик последовательных ошибок (ФКН)	3 - 5*	Число ошибок аутентификации идущих подряд в протоколе взаимодействия с ФКН.
Счетчик EKE	10 000 000*	Количество внутренних криптографических операций ФНК.
Счетчик Диффи-Хеллмана	10 000 000*	Количество операций Диффи-Хеллмана.
Счетчик подписей	10 000 000*	Количество подписей, которое может быть создано с использованием закрытого ключа из данного контейнера.

* Значение определяется ключевым носителем.

5. Перечень сокращений

CSP	Криптопровайдер (Cryptographic Service Provider)
EKE	Протокол электронного обмена ключами (Electronic Key Exchange)
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
СКЗИ	Средство криптографической защиты информации
ФКН	Функциональный ключевой носитель

6. Перечень рисунков