Программный комплекс «ЛИССИ-CSP» Руководство администратора

ООО «ЛИССИ-Софт»

Оглавление

1 Условия применения

Программный комплекс «ЛИССИ-CSP» (далее «ЛИССИ-CSP») устанавливается на компьютеры под управлением 32-х и 64-х разрядных операционных систем семейства MS Windows: Windows XP, Windows 7, Windows 8, Windows 8.1, Server 2003, Windows Vista, Server 2008, Server 2008 R2.

Для установки «ЛИССИ-CSP» необходимы права администратора системы.

До начала процесса установки желательно убедиться, что на компьютере не установлен криптопровайдер «КриптоПро CSP». «ЛИССИ-CSP» и «КриптоПро CSP» не совместимы между собой, поэтому наличие двух таких провайдеров в одной системе недопустимо. Если это условие не выполняется, то необходимо удалить «КриптоПро CSP», либо выбрать другую систему для установки «ЛИССИ-CSP».

2 Установка / удаление

2.1 Установка «ЛИССИ-CSP»

Для начала процесса установки необходимо загрузить последнюю версию дистрибутива с сайта - http://soft.lissi.ru/products/skzi/lissi-csp/download_lissi_csp/).

Существует 2 варианта дистрибутива «ЛИССИ-CSP»:

- **LISSI-CSP-Setup-win32.exe** - предназначен для установки только на 32-х разрядные ОС Windows.
- **LISSI-CSP-Setup-x64.exe** предназначен для установки только на 64-х разрядные ОС Windows.

Примечание: *Определение разрядности операционной системы описано в разделе 7.1.*

Выберите подходящий вам вариант и выполните его загрузку. После загрузки запустите процесс установки дважды кликнув на файл инсталлятора.

Если запущенный инсталлятор не предназначен для вашей системы, то вы увидите окно с соответствующим уведомлением:

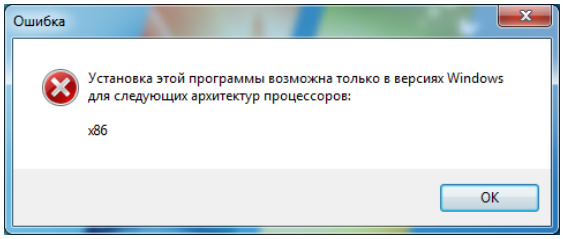

Рис. 2.1

В том случае, если на компьютере установлен «КриптоПро CSP», то на экране появится диалог с уведомлением. В этом случае до установки «ЛИССИ-CSP» необходимо удалить программный пакет «КриптоПро», либо отказаться от установки «ЛИССИ-CSP» на этой системе.

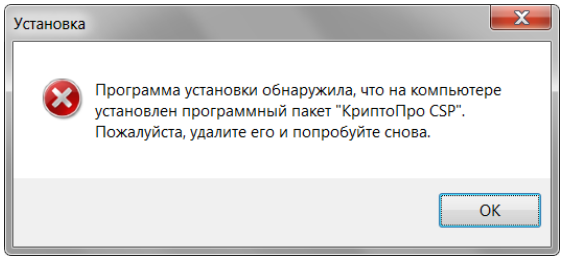

Рис. 2.2

В случае успешного прохождения всех проверок на экране появится диалог с приглашением на установку. Следует нажать кнопку «Далее».

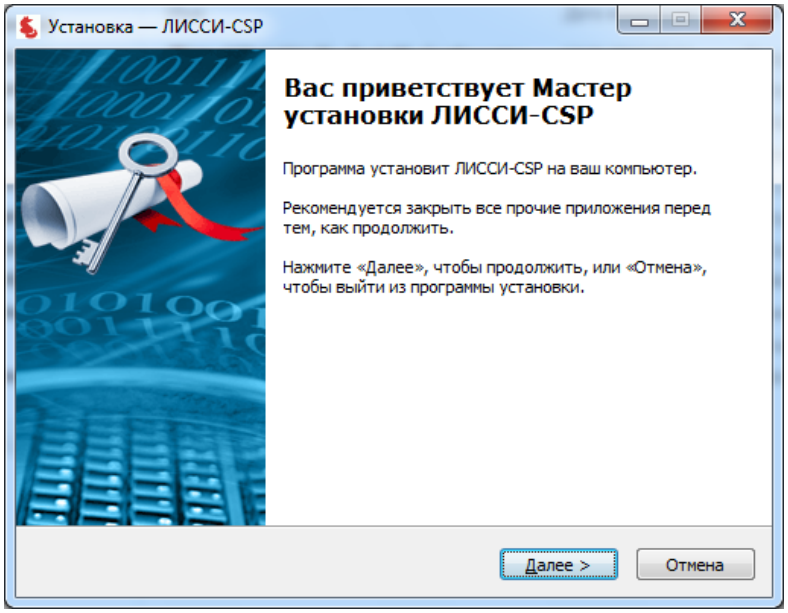

Рис. 2.3

В следующем окне необходимо выбрать вариант установки «ЛИССИ-CSP».

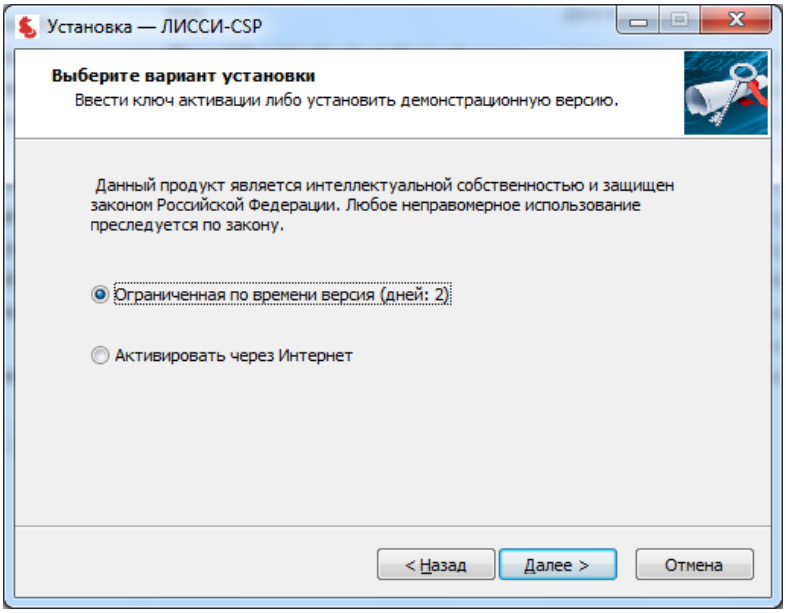

Рис. 2.4

Вариант «**Ограниченная по времени версия (2 дня)**» означает, что программа будет работать в течение 2 дней с момента установки. За это время вам потребуется активировать «ЛИССИ-CSP». Программа перестанет работать, если не произвести процедуру активации в течение 2 дней. Процедура активации описана в разделе 2.2 данного документа. Также данный вариант следует использовать, если на этом компьютере уже был ранее установлен «ЛИССИ-CSP» (ранее установленная лицензия сохраниться). Вариант «**Активировать через интернет**» означает, что «ЛИССИ-CSP» будет автоматически активирован через сеть интернет (требуется наличие доступа в сеть интернет на том компьютере, где производится установка «ЛИССИ-CSP»). Для этого потребуется ввести серийный номер «ЛИССИ-CSP», указанный в лицензионном соглашении, в соответствующем поле ввода (рис. 2.5). После ввода серийного номера нажмите кнопку «Далее» для продолжения установки.

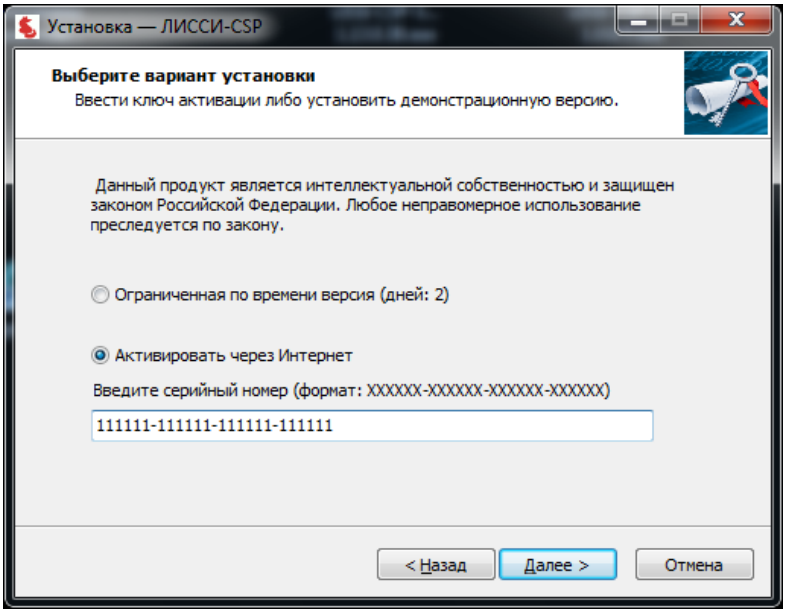

Рис. 2.5

На следующем шаге следует указать папку, в которую будет установлен пакет, либо согласиться использовать каталог, предложенный по умолчанию, и нажать кнопку «Далее».

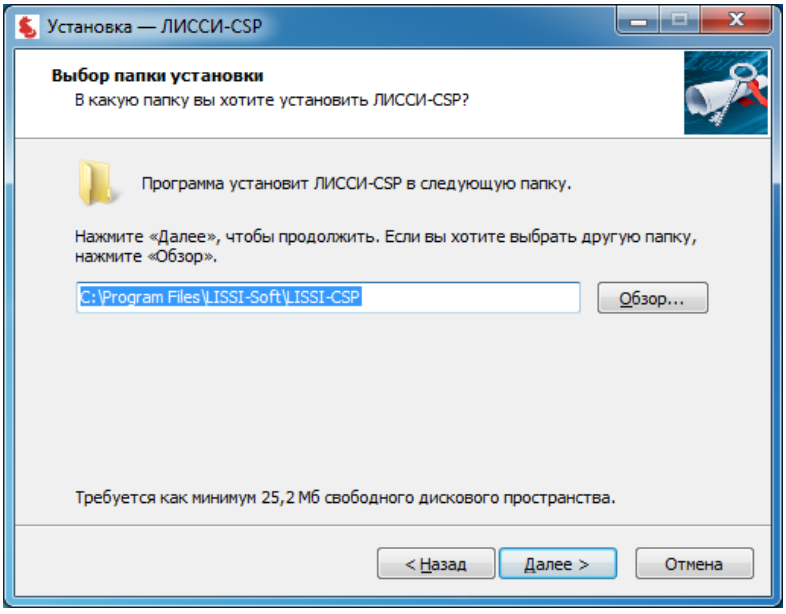

Рис. 2.6

Следующее окно информирует о готовности к началу процесса установки. Для

запуска нажмите кнопку «Установить».

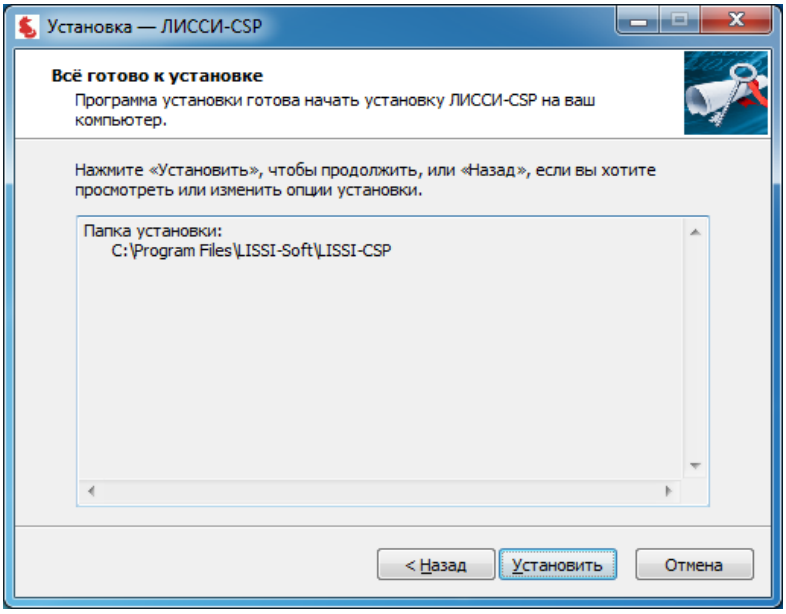

Рис. 2.7

После нажатия начнётся процесс установки следующих компонент:

- программного комплекса «ЛИССИ-CSP»
- программной библиотеки защиты информации «СКЗИ «ЛИРССЛ».

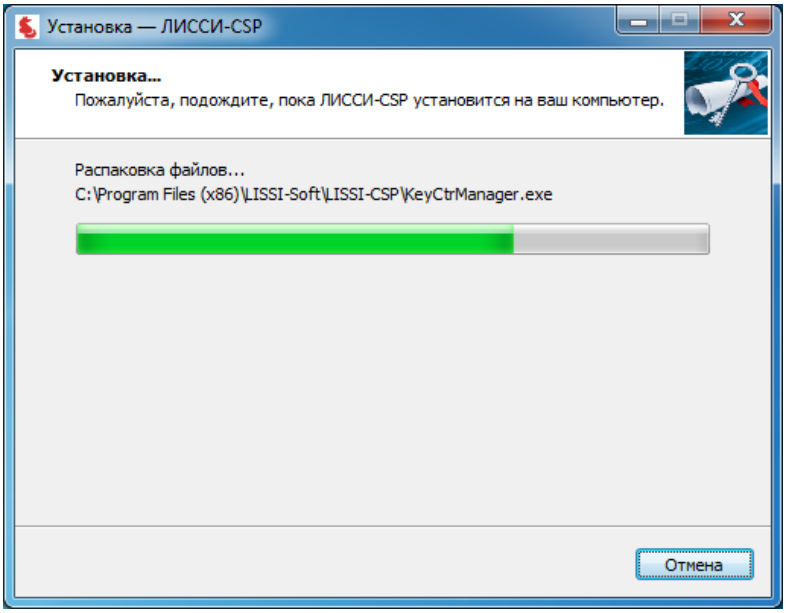

Рис. 2.8

В самом конце на экране появится диалог, информирующий о необходимости перезагрузки системы. Для немедленной перезагрузки выберите «Да, перезагрузить компьютер сейчас» и нажмите «Завершить».

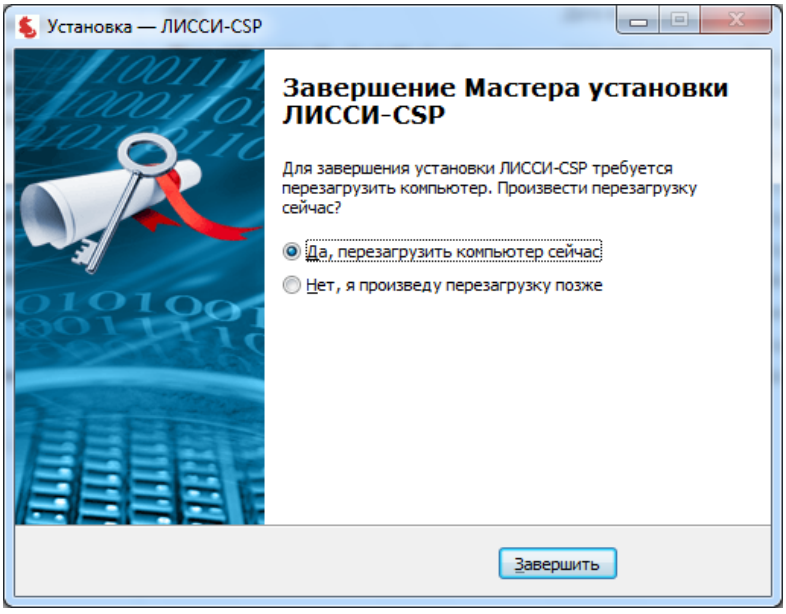

Рис. 2.9

2.2 Активация «ЛИССИ-CSP»

Для работы «ЛИССИ-CSP» после демонстрационного периода необходимо пройти процедуру активации. При покупке лицензии «ЛИССИ-CSP» вы получили серийный номер (он указан в лицензионном соглашении).

2.2.1 Активация через интернет

- Если «ЛИССИ-CSP» ещё не установлен на компьютере, то активировать «ЛИССИ-CSP» через интернет можно на этапе установки путём ввода серийного номера указанного в лицензионном соглашении (см. раздел 2.1).
- Если «ЛИССИ-CSP» уже установлен на компьютере, то необходимо запустить утилиту «Настройка ЛИССИ-CSP» («Пуск | Программы | LISSI-Soft | ЛИССИ-CSP | Настройка CSP»).

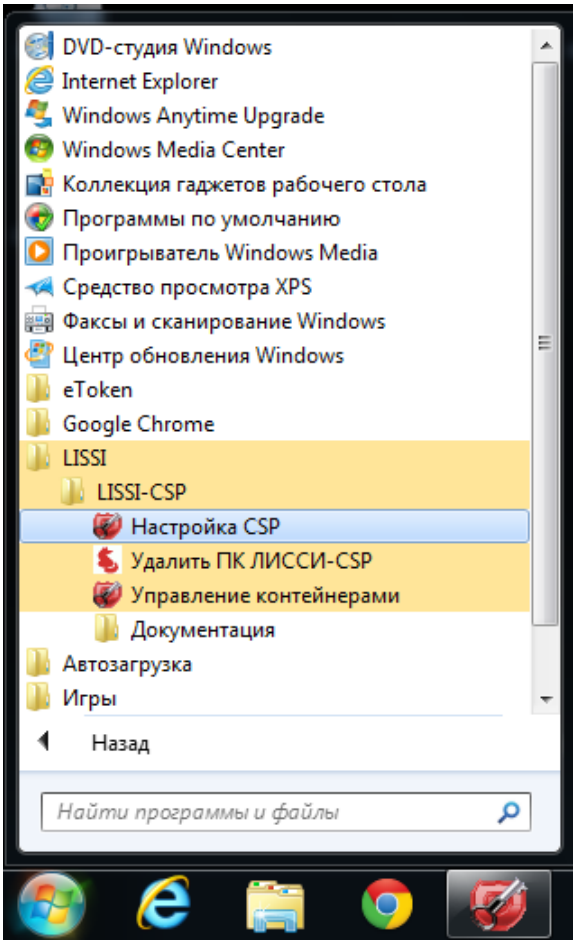

Рис. 2.10

- В появившемся диалоге с вкладками перейти на вкладку «О программе».

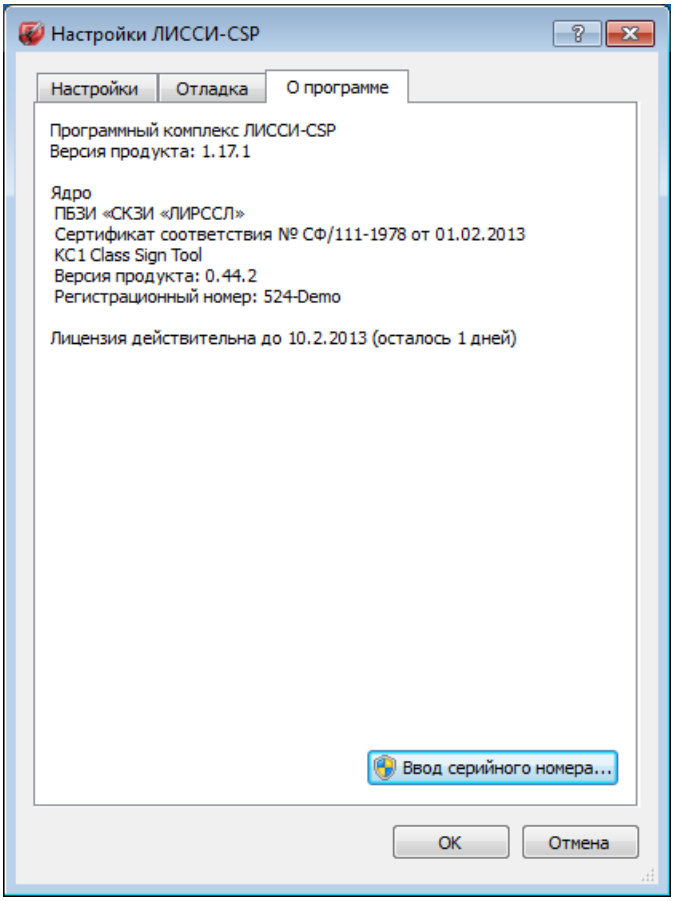

Рис. 2.11

- Нажать на кнопку «Ввод серийного номера...», в появившемся окне в поле ввода ввести серийный номер, указанный в лицензионном соглашении, и нажать кнопку «OK» (см. рисунок 2.12).

Для выполнения этой операции пользователь должен иметь права администратора системы (для ОС Vista и Windows 7 перед появлением окна потребуется подтвердить переход программы в режим администратора).

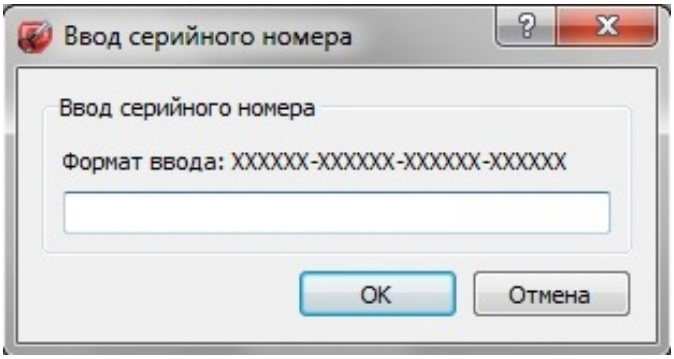

Рис. 2.12

- В случае успешного завершения процедуры активации появится диалоговое окно с уведомлением об успешной установке лицензии.

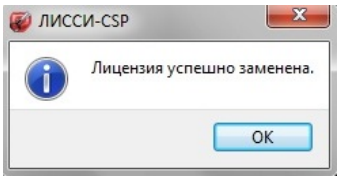

Рис. 2.13

- Если у пользователя, от имени которого запущена программа нет прав администратора, то обновить лицензию не получится.

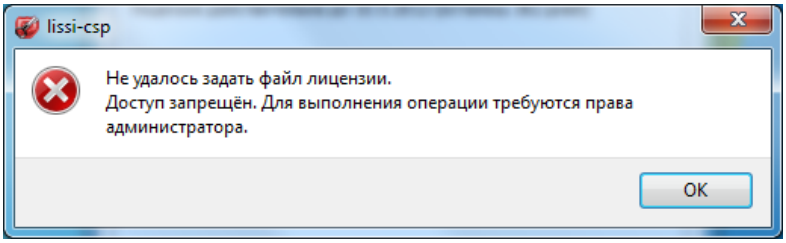

Рис. 2.14

2.3 Установка драйверов eToken компании «Aladdin»

Внимание! *Данная процедура необходима, если у Вас не установлены драйвера eToken и требуется работа с данным видом токенов.*

Для возможности использования ключевого носителя eToken в качестве хранилища ключевых контейнеров необходимо установить соответствующие драйвера. Загрузить их можно на официальном сайте компании: http://www.aladdin-rd.ru/. На момент написания документации страница загрузки драйверов находилась по ссылке: http://www.aladdin-rd.ru/support/downloads/etoken/.

2.4 Установка драйверов Rutoken компании «Актив»

Внимание! *Данная процедура необходима, если у Вас не установлены драйвера Rutoken и требуется работа с данным видом токенов.*

Для возможности использования ключевого носителя Rutoken в качестве хранилища ключевых контейнеров необходимо установить соответствующие драйвера. Загрузить их можно на официальном сайте компании: http://www.rutoken.ru/. На момент написания документации страница загрузки драйверов находилась по ссылке: http://www.rutoken.ru/support/download/drivers-for-windows/.

2.5 Установка драйверов MS_KEY K компании «Мультисофт»

Внимание! *Данная процедура необходима, если у Вас не установлены драйвера MS_KEY K и требуется работа с данным видом токенов.*

Для возможности использования ключевого носителя MS_KEY K в качестве хранилища ключевых контейнеров необходимо установить соответствующие драйвера. Загрузить их можно на официальном сайте компании. На момент написания документации страница загрузки драйверов находилась по ссылке:

http://soft.lissi.ru/docs/LSMS11/win/LCMS11_CSP_setup.exe

2.6 Установка драйверов mToken компании «ЛИССИ-Софт»

Внимание! *Данная процедура необходима, если у Вас не установлены драйвера mToken и требуется работа с данным видом токенов.*

Для возможности использования ключевого носителя mToken в качестве хранилища ключевых контейнеров необходимо установить соответствующие драйвера. Загрузить их можно на официальном сайте компании. На момент написания документации страница загрузки драйверов находилась по ссылке:

http://ca.soft.lissi.ru/docs/mToken_CSP_setup.exe

2.7 Удаление «ЛИССИ-CSP»

Для удаления «ЛИССИ-CSP» с вашего компьютера необходимо выбрать команду «Удалить ЛИССИ-CSP» из меню «Пуск | Программы | LISSI-Soft | ЛИССИ-CSP» и подтвердить ваше намерение нажатием кнопки «Да».

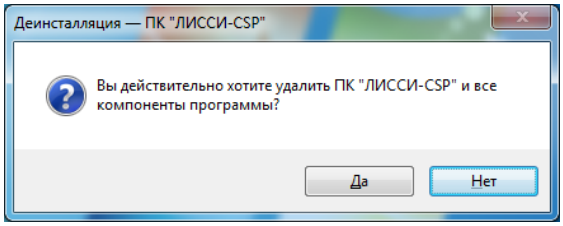

Рис. 2.15

После завершения процесса будет предложено выполнить перезагрузку компьютера. Нажмите «Да» для немедленной перезагрузки.

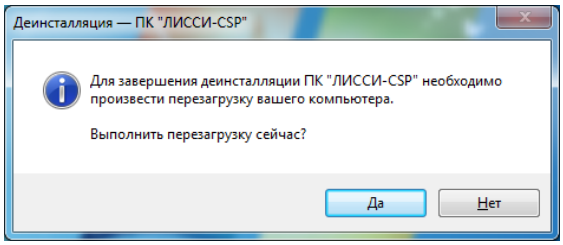

Рис. 2.16

Внимание! В процессе деинсталляции не выполняется удаление установленных ранее драйверов сторонних производителей (eToken, Rutoken и др.), т.к. они могут требоваться для работы других программных средств. В случае необходимости их удаления необходимо воспользоваться системным апплетом панели управления «Установка и удаление программ».

Например, для удаления драйверов «eToken» в списке установленных программ найти «eToken PKI Client 5.1 SP1» и нажать кнопку «Удалить», а для удаления драйверов «Rutoken» в списке установленных программ найти «Rutoken drivers» и нажать кнопку «Удалить».

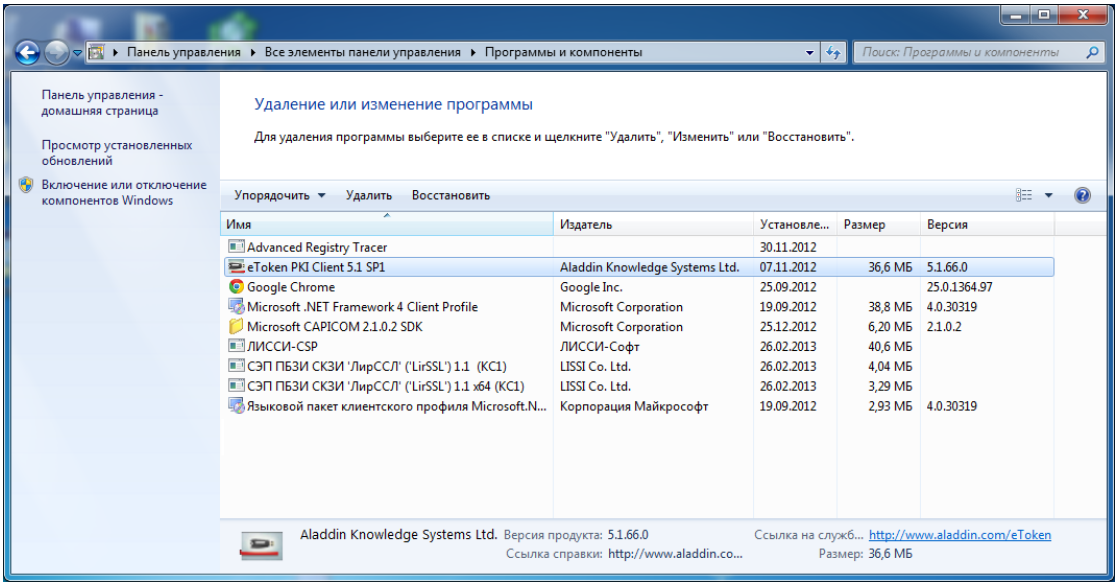

Рис. 2.17

2.8 Параметры командной строки инсталлятора «ЛИССИ-CSP»

Параметр	**Действие**
/SILENT или /VERYSILENT	Произвести установку в «тихом» режиме. От пользователя не потребуется вводить какие-либо данные. В случае указания опции */SILENT* он будет видеть ход установки. В случае указания опции */VERYSILENT* процесс установки будет скрыт от пользователя. При этом сообщения об ошибках все равно будут выводиться на экран, например, сообщение о неверном файле лицензии.
/NORESTART	Не перезагружать компьютер после установки.
/LICPATH	Путь к файлу лицензии. Параметр действует только в «тихом» режиме. Пути, содержащие знак пробела, необходимо брать в кавычки. **Пример:** */LICPATH="C:\My Documents\file.lic"*
/DIR	Директория установки программы. Пути, содержащие знак пробела, необходимо брать в кавычки. Если директория не задана, то по умолчанию используется «C:\Program Files\LISSI-Soft\LISSI-CSP». **Пример:** */DIR="C:\Program Files\LISSI-Soft\LISSI-CSP"*
/LIMITEDUSER_VERSION	Установка версии программы с ограничениями. Заставляет инсталлятор не производить копирование утилит, входящих в состав программного пакета. Кроме того в ПУСК не добавляется никакой информации об установленной программе. Данная опция предназначена для ограничения пользователей в их возможностях.

3 Управление контейнерами

3.1 Общая информация

Для управления ключевыми контейнерами «ЛИССИ-CSP» используется утилита «Управление контейнерами». Для запуска утилиты выполните команду «Пуск | Программы | LISSI-Soft | ЛИССИ-CSP | Управление контейнерами».

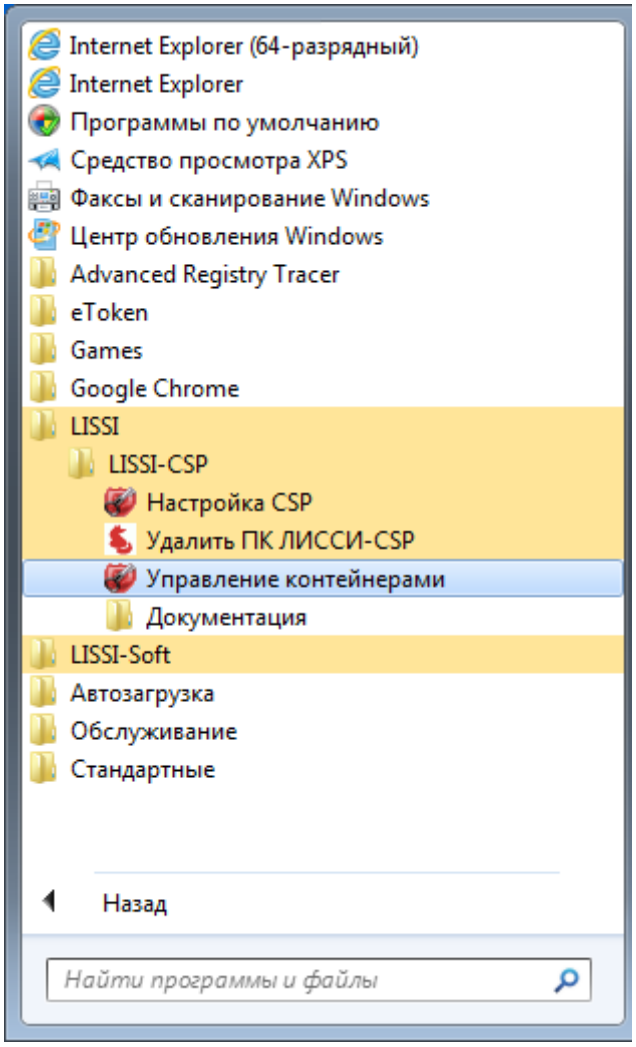

Рис. 3.1

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

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

Внимание! Утилита «Управление контейнерами» не увидит контейнеры, сформированные другими криптопровайдерами (например, «КриптоПро CSP»). Причина в том, что формат контейнера провайдера является закрытой информацией и

известен лишь производителю соответствующего провайдера.

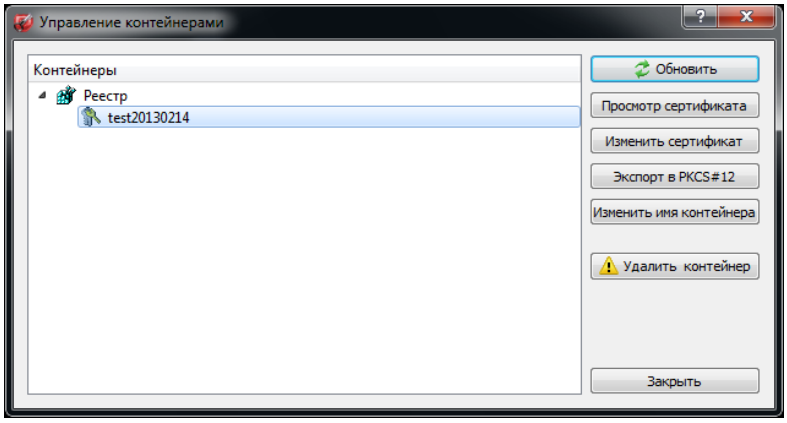

Рис. 3.2

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

Для удаления контейнера с ключевого носителя необходимо выбрать мышкой нужный контейнер в окне «Контейнеры» и нажать кнопку «Удалить контейнер». Для удаления всех контейнеров на выбранном носителе необходимо выбрать носитель и нажать кнопку «Удалить все контейнеры». Для удаления контейнеров в реестре, на флешке или дискете ввод пароля не требуется. Для удаления контейнеров на электронных USB ключах (Rutoken, eToken, и др.) необходимо ввести PIN-код.

Внимание! Если у вас нет резервной копии, то после удаления контейнера его уже невозможно будет восстановить.

3.2 Просмотр сертификата в контейнере

Для просмотра сертификата в контейнере необходимо либо выбрать мышкой нужный контейнер и нажать кнопку «Просмотр сертификата», либо навести мышкой на ключевой контейнер, нажать правую кнопку мыши и в появившемся контекстном меню выбрать «Просмотр сертификата». Если сертификат присутствует в контейнере, то на экране отобразится диалоговое окно «Сертификат» с информацией о сертификате в контейнере.

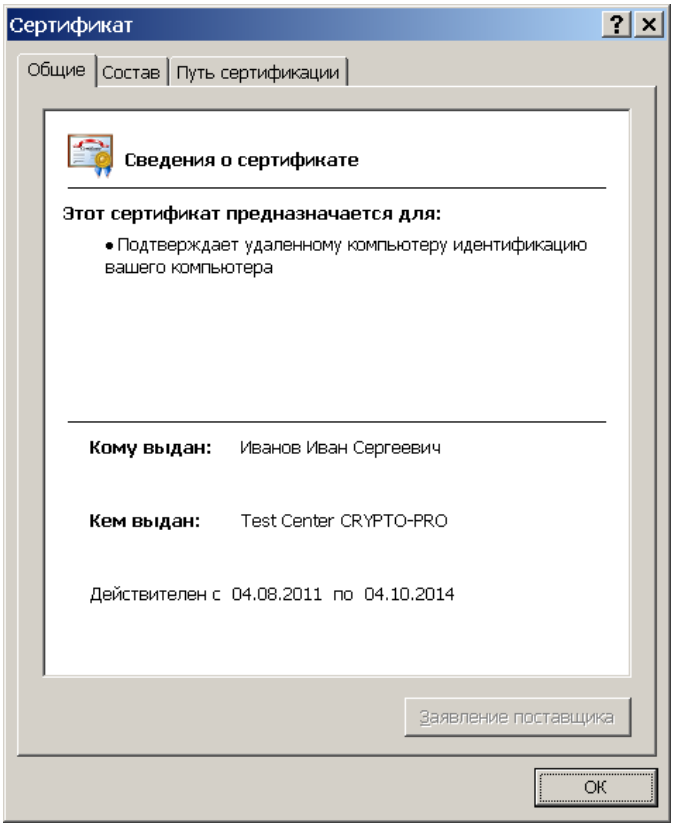

Рис. 3.3

Если контейнер не содержит сертификат, то на экране появится диалог с соответствующим уведомлением.

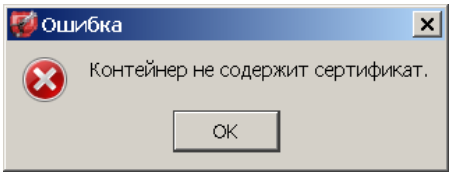

Рис. 3.4

Сертификат в контейнере носителя можно просмотреть не только с помощью утилиты «Управление контейнерами». Средства системы, например, «Internet Explorer» также видят этот сертификат без дополнительных действий по импорту сертификата в систему.

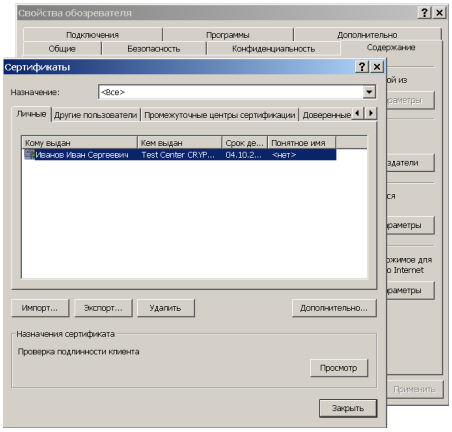

Рис. 3.5

Это обеспечивается специальным компонентом провайдера, предоставляющим системе информацию о всех сертификатах в контейнерах. Удалить такой сертификат средствами системы не получится. Сертификат исчезнет автоматически, если извлечь из компьютера носитель с контейнером или удалить контейнер средствами утилиты «Управление контейнерами».

3.3 Изменение сертификата в контейнере

Кнопка «Изменить сертификат» предназначена для обновления сертификата контейнера, а также для возможности положить сертификат в контейнер, в том случае, если он в нём отсутствует. Обновление сертификата может потребоваться в случае продления срока его действия.

Изменить сертификат контейнера можно только в случае точного соответствия открытого ключа сертификата открытому ключу в контейнере.

Для изменения сертификата контейнера либо выберете нужный контейнер в окне «Контейнеры» и нажмите кнопку «Изменить сертификат», либо наведите мышкой на контейнер, сертификат которого вы хотите изменить, нажмите правую кнопку мыши и в появившемся контекстном меню выберите вкладку «Изменить сертификат». Потребуется ввести пароль (PIN-код) для доступа к контейнеру.

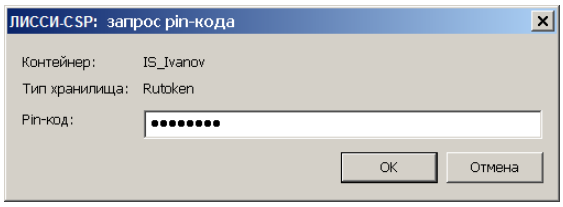

Рис. 3.6

Если сертификат уже присутствует в контейнере, то утилита сообщит об этом с требованием подтверждения запрошенной операции. Нажмите кнопку «Да» для продолжения.

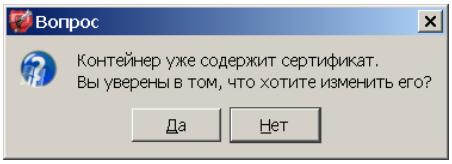

Рис. 3.7

В следующем окне потребуется выбрать файл с сертификатом, который будет помещён в выбранный контейнер, и нажать «Открыть».

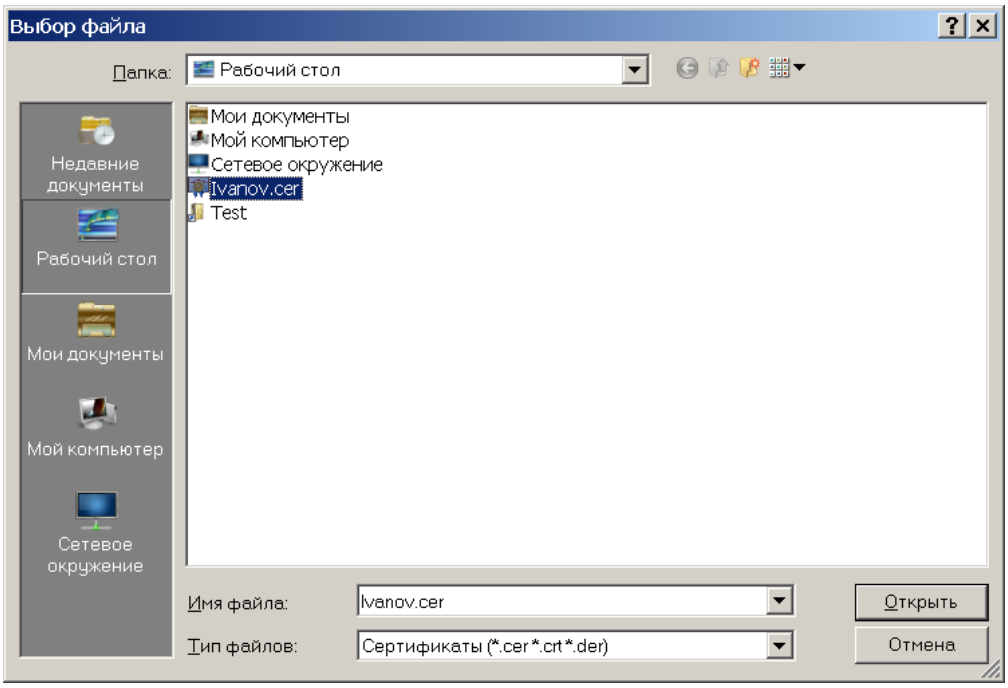

Рис. 3.8

В случае успеха вы увидите окно с соответствующим сообщением. Оно информирует о том, что новый сертификат был успешно положен в контейнер на место старого.

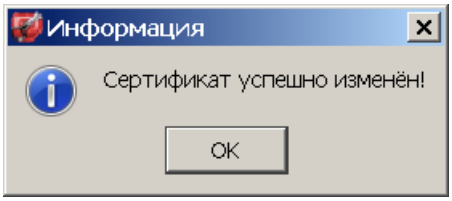

Рис. 3.9

3.4 Установка сертификата центра сертификации

Для установки сертификата центра сертификации необходимо двойным щелчком мыши щёлкнуть по файлу с нужным сертификатом. Результатом на это действие будет отображение на экране диалога «Сертификат». Нажмите кнопку «Установить сертификат...» в нижней части вкладки «Общие» диалога.

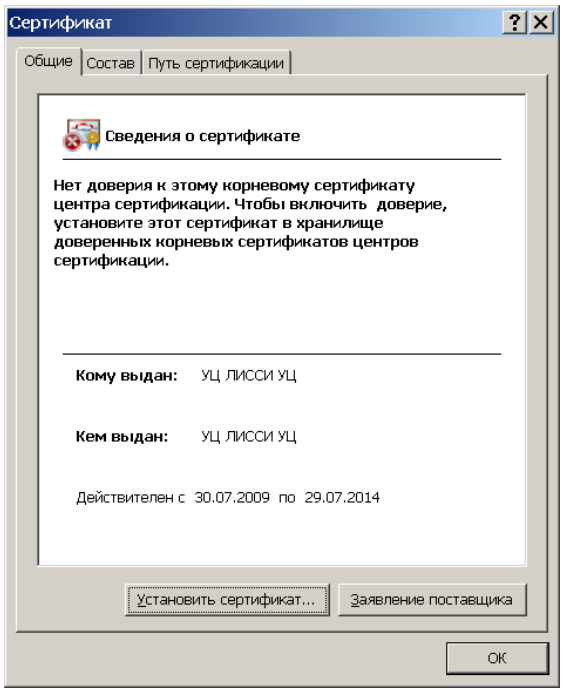

Рис. 3.10

На экране появится диалог мастера импорта сертификатов. Нажмите в нём кнопку «Далее» для начала процедуры импорта.

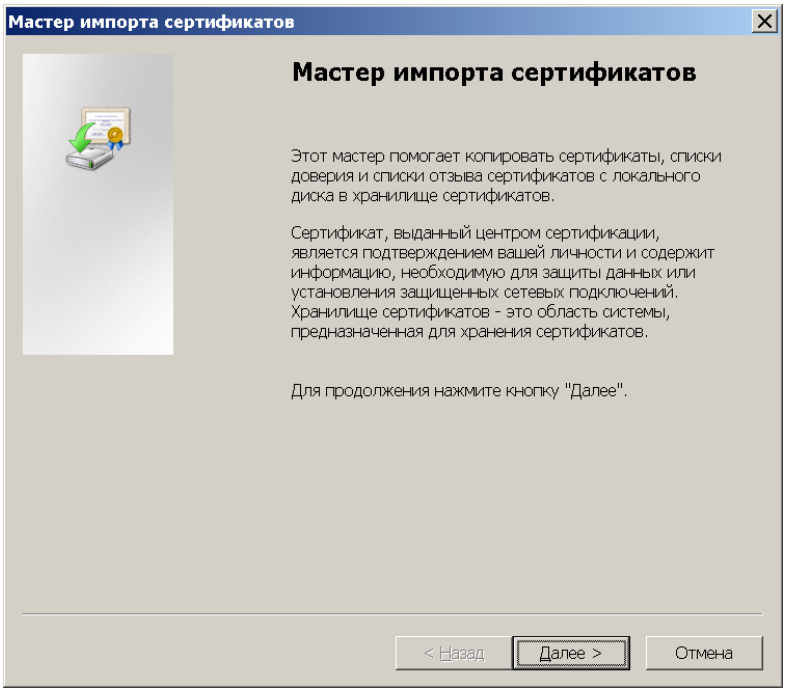

Рис. 3.11

На экране появится диалог выбора типа хранилища, в которое будет установлен сертификат центра сертификации. Установите переключатель в положение «Поместить все сертификаты в следующее хранилище» и нажмите кнопку «Обзор...».

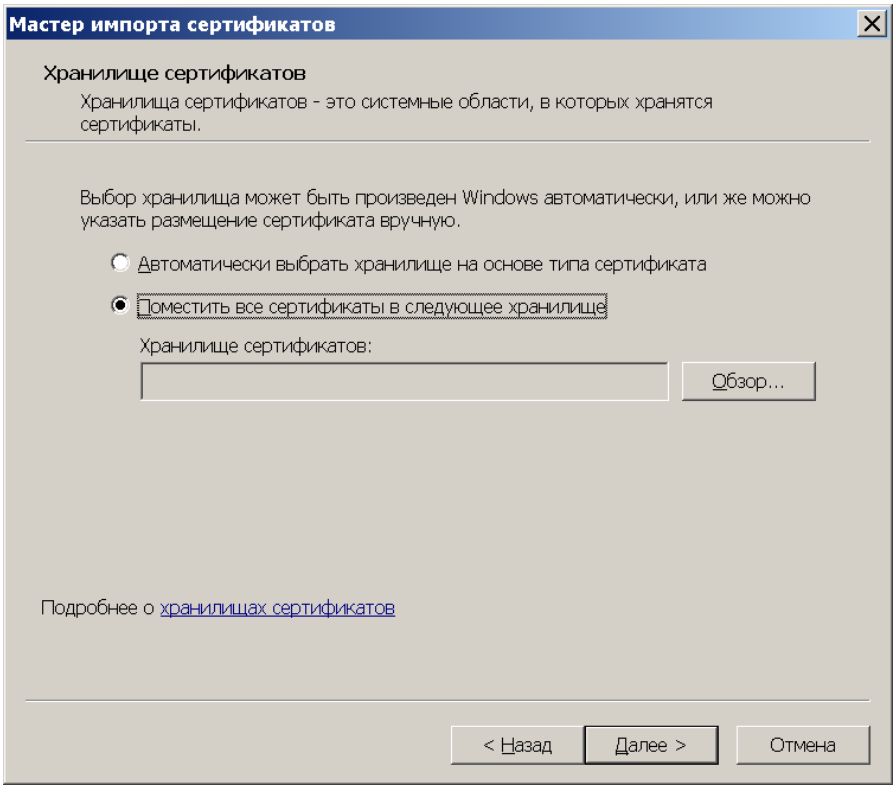

Рис. 3.12

На экране появится диалог выбора хранилища сертификатов. Если вы устанавливаете корневой сертификат (самоподписанный), то выберете в дереве папку «**Доверенные корневые центры сертификации**», если же вы устанавливаете промежуточный сертификат (подписанный другим центром сертификации), то выберете в дереве папку «**Промежуточные центры сертификации**», и нажмите «OK».

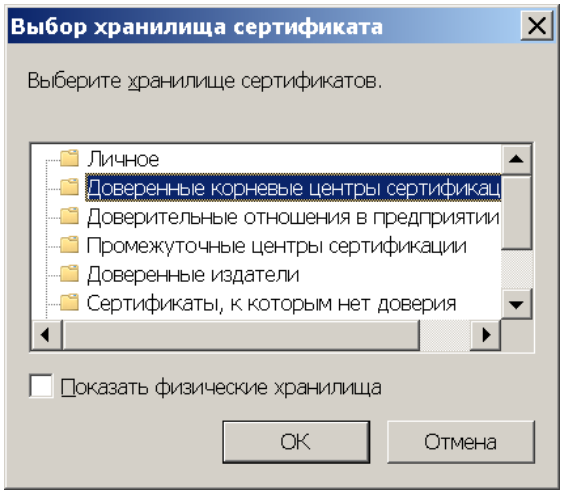

Рис. 3.13

Нажмите кнопку «Далее».

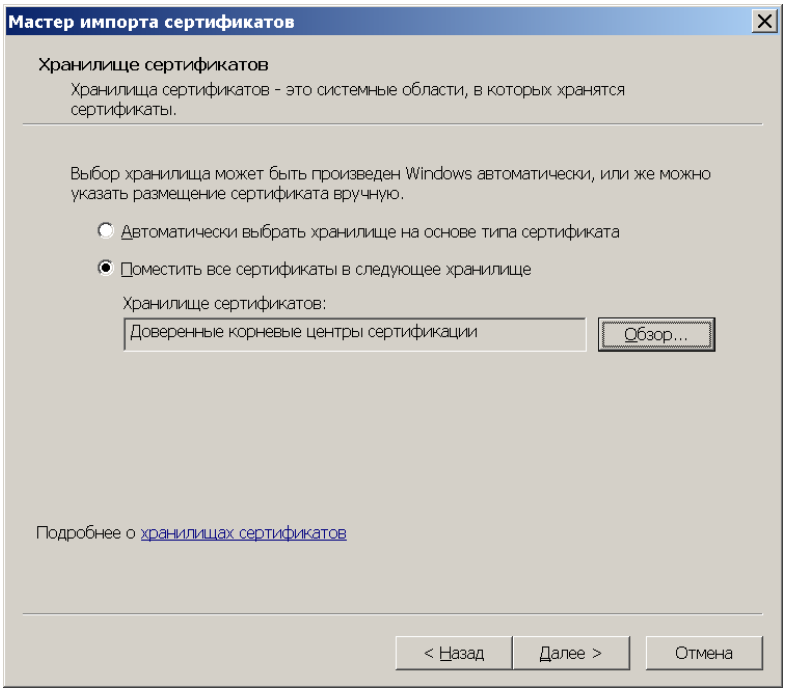

Рис. 3.14

На следующем шаге нажмите «Готово».

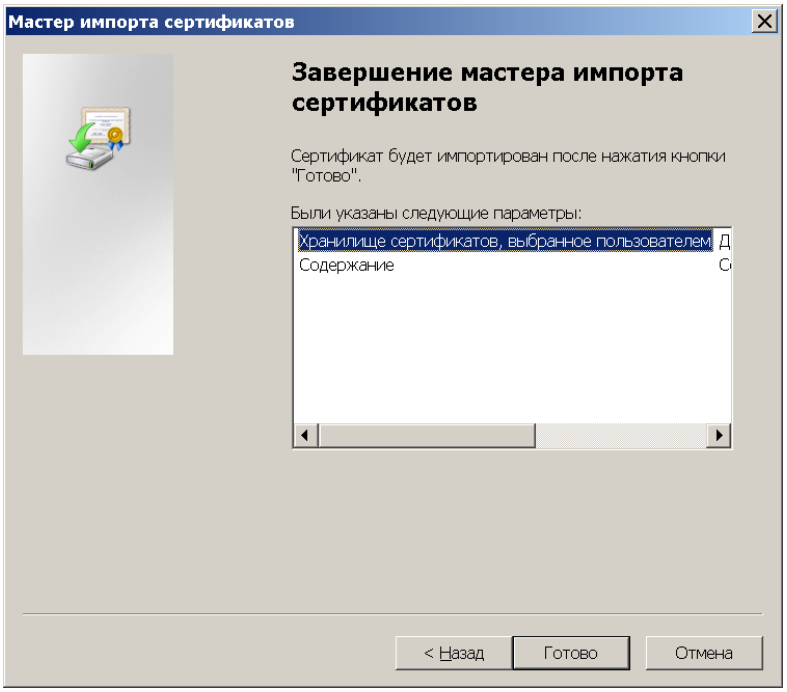

Рис. 3.15

На экране появится диалог «Предупреждение о безопасности». Нажмите кнопку «Да» для начала импорта сертификата.

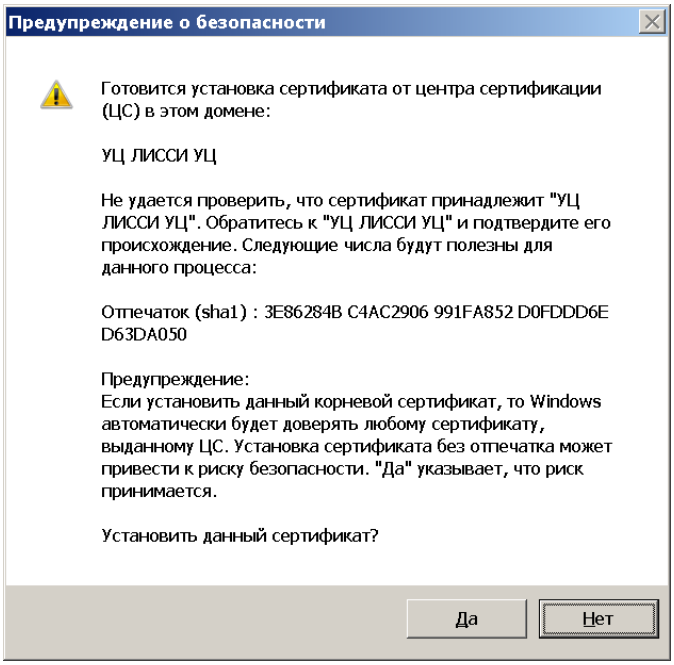

Рис. 3.16

Нажмите «ОК» для завершения процесса импорта.

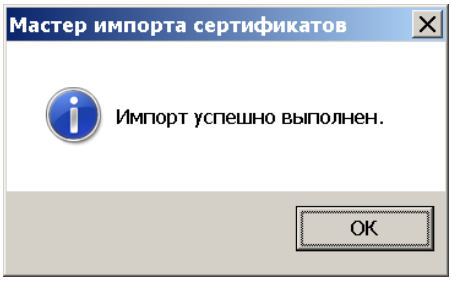

Рис. 3.17

4 Настройки CSP

Для запуска утилиты «Настройка CSP» выполните команду «Пуск | Программы | LISSI-Soft | ЛИССИ-CSP | Настройка CSP». На экране появится диалоговое окно с вкладками.

4.1 Поддерживаемые ключевые носители

Ключевой носитель – это хранилище, использующееся для хранения ключевых контейнеров с ключевыми парами. Таким хранилищем может быть как отчуждаемый носитель (флешка, дискета, eToken и др.), так и реестр Windows.

«ЛИССИ-CSP» поддерживает следующие основные типы ключевых носителей:

- Реестр
- Дискета
- Съёмное устройство (флешка)
- eToken
- eToken ГОСТ
- Rutoken
- Rutoken ЭЦП
- MS_Key
- Java card

Во вкладке «Настройки» в разделе «Доступные типы ключевых носителей» перечислены все поддерживаемые типы ключевых носителей. При этом галочками отмечены те их них, которые доступны для использования на данный момент без установки дополнительных программных средств.

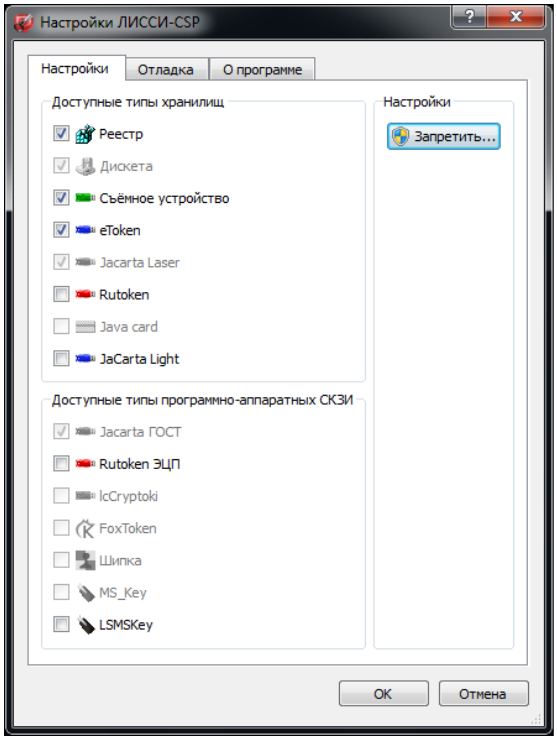

Рис. 4.1

Если тип ключевого носителя в списке не отмечен галочкой, значит, для возможности его использования необходимо установить соответствующие драйвера. Если вы щёлкните по этому элементу списка, то вы увидите информационное сообщение.

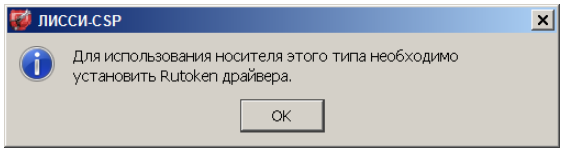

Рис. 4.2

Реестр, дискета и съёмное устройство доступны сразу после установки «ЛИССИ-CSP». Для возможности использования других типов носителей необходимо установить соответствующие драйвера. После установки драйверов элементы, ранее не отмеченные галочками, автоматически отметятся. Об установке драйверов читайте в разделе 2.1 данного документа.

Внимание! Для возможности использования ключевых носителей eToken ГОСТ не требуется установка драйверов. Библиотека поддержки JaCarta ГОСТ включает в себя поддержку eToken ГОСТ.

Кнопка «Запретить...» предназначена для возможности выборочного отключения поддерживаемых типов носителей. Отключение типа носителя означает, что носи-

тели (устройства) данного типа не будут распознаваться программными модулями «ЛИССИ-CSP», при этом они также не будут видны в «Утилите управления контейнерами». Для запрета необходимы права Администратора системы. Рекомендуется запрещать все неиспользуемые типы носителей, это позволит ускорить работу «ЛИССИ-CSP» при обнаружении устройств, используемых для хранения ключевых пар.

Для отключения заданных типов носителей нажмите кнопку «Запретить» и в специальном диалоговом окне отметьте те типы носителей, которые не должны распознаваться «ЛИССИ-CSP» *(для ОС Vista и Windows 7 перед появлением диалога потребуется подтвердить переход программы в режим администратора)*.

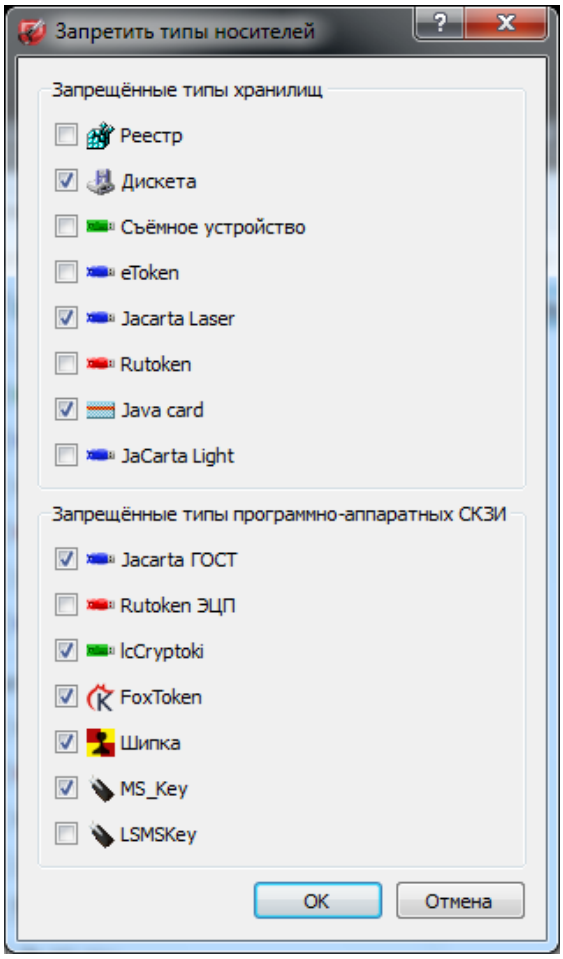

Рис. 4.3

После нажатия кнопки «OK» выбранные носители будут отмечены, как запрещённые, и не будут доступны для использования в «ЛИССИ-CSP».

4.2 Поддержка носителей с неизвлекаемым ключом

В качестве ключевых носителей в «ЛИССИ-CSP» могут также использоваться токены с аппаратной реализацией российских криптоалгоритмов (прежде всего, алгоритма ГОСТ Р 34.10-2001 (ЭЦП)).

Важным аспектом использования токенов с аппаратной реализацией российских криптоалгоритмов является то, что ключевая пара формируется внутри такого токена, и все операции с использованием закрытого ключа также выполняются самим токеном (закрытый ключ никогда не покидает пределы токена, т.е. является неизвлекаемым).

В качестве ключевых носителей с неизвлекаемым ключом в «ЛИССИ-CSP» могут использоваться eToken ГОСТ, Rutoken ЭЦП и MS_Key K. Для выполнения криптографических операций с закрытым ключом на таких носителях «ЛИССИ-CSP» обращается к соответствующему токену через специальный программный интерфейс. Для всех остальных криптографических операций «ЛИССИ-CSP» использует собственное криптоядро.

Внимание! Для токенов с неизвлекаемым ключом не поддерживаются операции импорта/экспорта в формате PKCS#12.

4.3 Версия CSP

Во вкладке «О программе»»можно посмотреть информацию о версии продукта.

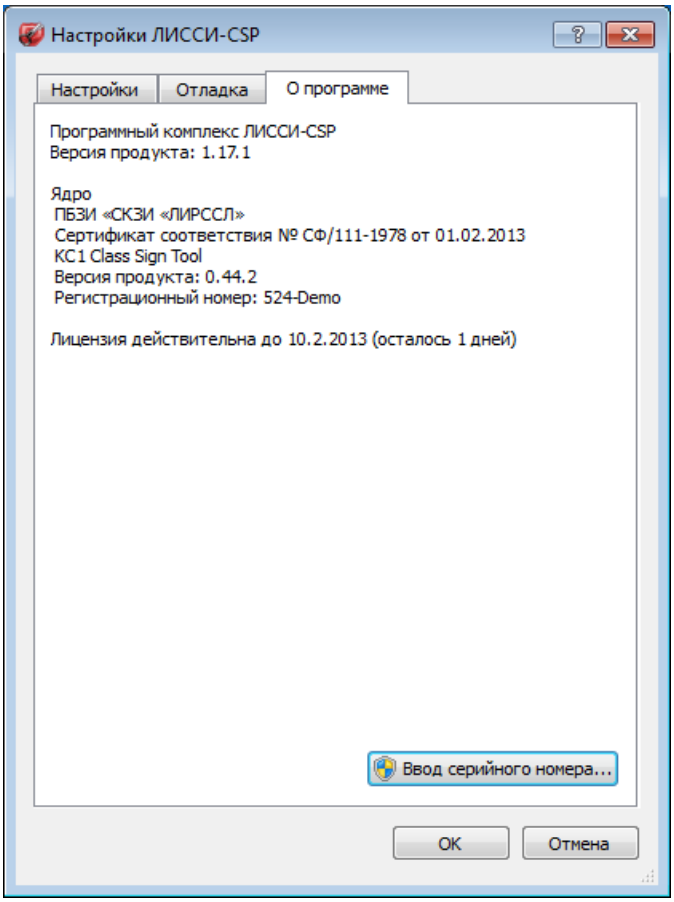
Настройки ЛИССИ-CSP
Настройки
Отладка
О программе
Программный комплекс ЛИССИ-CSP
Версия продукта: 1.17.1
Ядро
ПБЗИ «СКЗИ «ЛИРССЛ»
Сертификат соответствия № СФ/111-1978 от 01.02.2013
KC1 Class Sign Tool
Версия продукта: 0.44.2
Регистрационный номер: 524-Demo
Лицензия действительна до 10.2.2013 (осталось 1 дней)
Ввод серийного номера...
OK
Отмена

Рис. 4.4

5 Работа с PKCS#12

PKCS#12 – это стандарт семейства «Public-Key Cryptography Standards (PKCS)», опубликованный «RSA Laboratories». Он определяет формат файла, используемого для хранения закрытых ключей с сертификатами. Файл PKCS#12 защищается при помощи основанного на пароле симметричного ключа.

«ЛИССИ-CSP» позволяет осуществлять экспорт содержимого ключевых контейнеров в файл в формате PKCS#12, а также проводить обратную операцию импорта файла PKCS#12 в ключевой контейнер. Такой функционал может использоваться для переноса ключевых пар между различными компьютерами с «ЛИССИ-CSP», для переноса ключевых пар в другие программные системы, поддерживающие стандарт PKCS#12 и работающие на различных платформах, а также для резервного копирования ключевых пар.

5.1 Экспорт ключевого контейнера в файл PKCS#12

Экспорт ключевого контейнера в PKCS#12 выполняется по личному сертификату. В группу «Личные» попадают те сертификаты, у которых есть соответствующий закрытый ключ. Для выполнения операции экспорта необходимо выполнить команду «Пуск | Программы | LISSI-Soft | ЛИССИ-CSP | Управление контейнерами». На экране появится диалоговое окно со списком доступных носителей и контейнеров. Чтобы осуществить экспорт сертификата какого-либо контейнера, необходимо либо выбрать контейнер и нажать кнопку «Экспорт в PKCS#12», либо навести курсор на контейнер, сертификат которого вы хотите экспортировать, нажать правую кнопку мыши и в появившемся контекстном меню выбрать вкладку «Экспорт в PKCS#12». На экране появится диалог для выбора имени файла в формате PKCS#12. Выберете нужный каталог, задайте имя и нажмите кнопку «Сохранить».

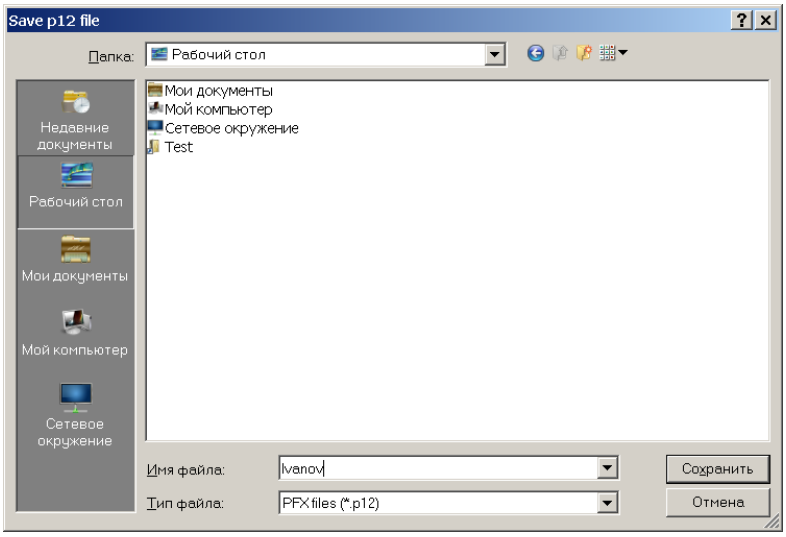

Рис. 5.1

На экране появится диалог запроса PIN-кода (пароля) для доступа к контейнеру, привязанного к выбранному сертификату. Введите его и нажмите «OK».

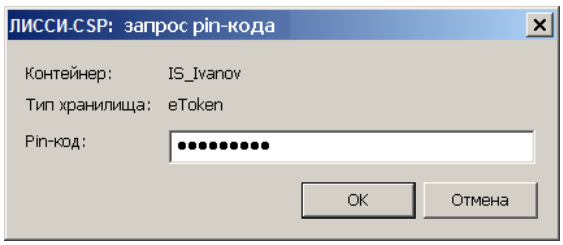

Рис. 5.2

На экране появится запрос пароля для защиты файла в формате PKCS#12. Этот пароль потребуется при выполнении обратной операции импорта. Дважды введите пароль и нажмите «OK».

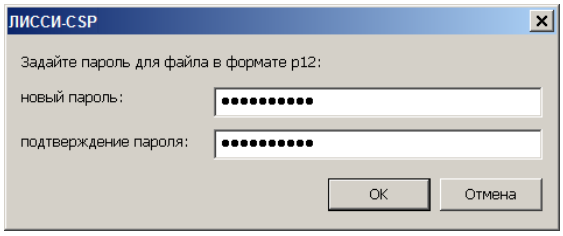

Рис. 5.3

На экране появится диалог, подтверждающий успешное завершение операции экспорта, а в выбранном каталоге появится созданный файл с расширением «p12».

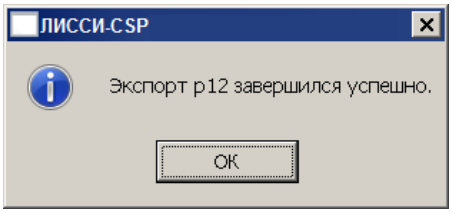

Рис. 5.4

5.2 Импорт файла PKCS#12 в ключевой контейнер

Операция импорта файла в формате PKCS#12 выполняется средствами системы. Для начала импорта дважды щёлкните мышью по файлу в формате PKCS#12. На экране появится диалог мастера импорта сертификатов. Нажмите кнопку «Далее».

На экране появится диалог мастера импорта сертификатов. Нажмите кнопку «Далее».

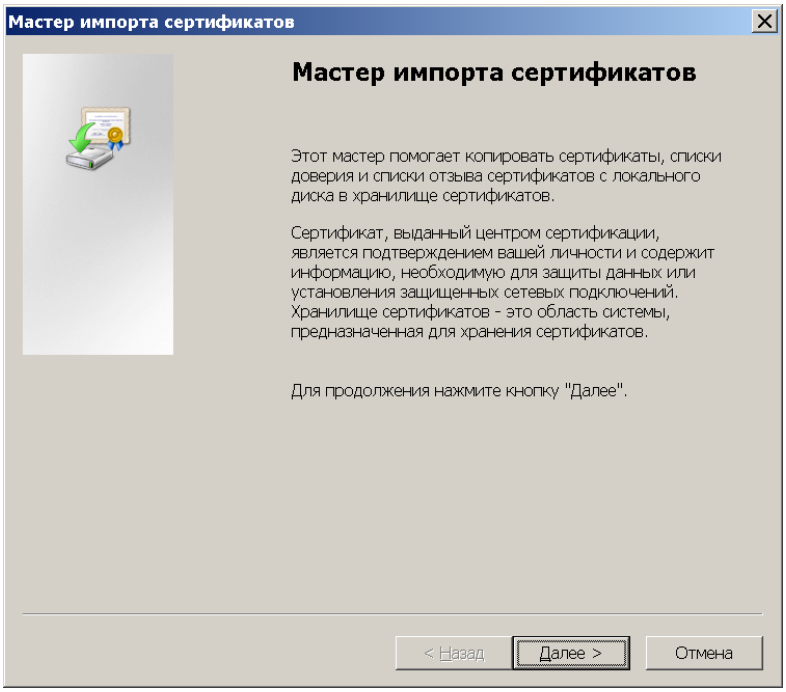

Рис. 5.5

В следующем диалоге в поле ввода необходимо указать путь к импортируемому файлу PKCS#12 (используйте кнопку «Обзор...» для вызова диалога выбора файла). Нажмите кнопку «Далее».

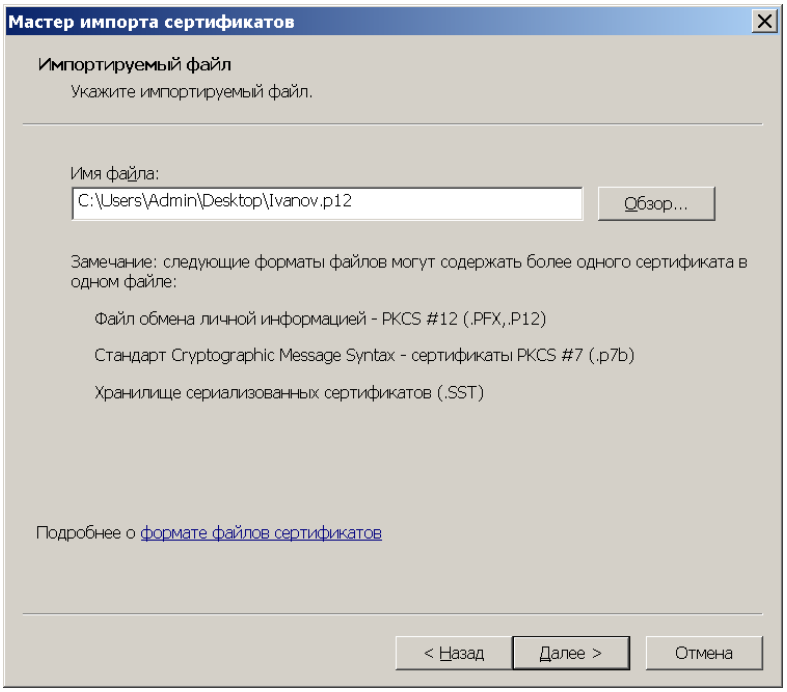

Рис. 5.6

В появившемся диалоге в поле ввода «Пароль» задайте пароль к файлу PKCS#12 и нажмите кнопку «Далее».

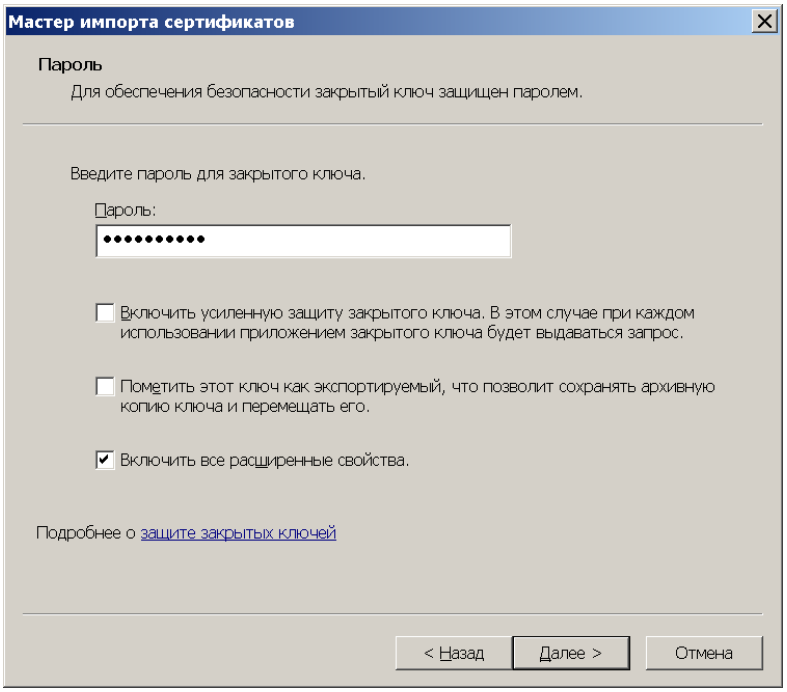

Рис. 5.7

В следующем диалоге установите переключатель в положение «Автоматически выбрать хранилище на основе типа сертификата» и нажмите кнопку «Далее».

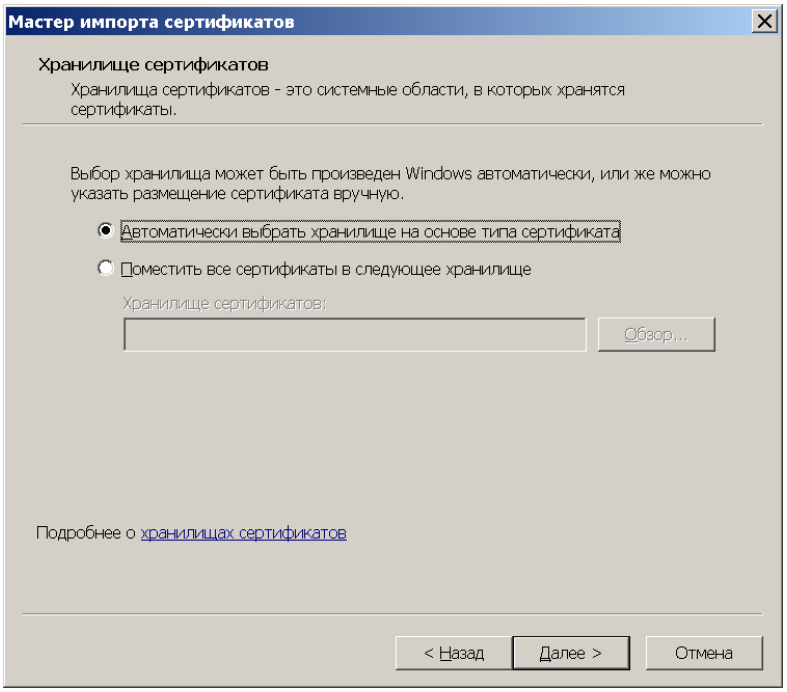

Рис. 5.8

В появившемся диалоге нажмите кнопку «Готово» для начала операции импорта.

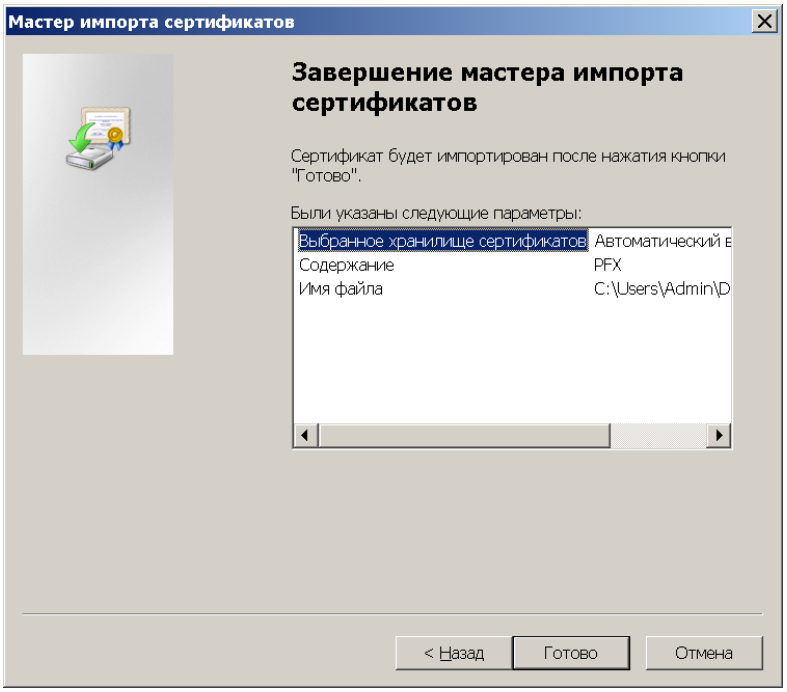

Рис. 5.9

Далее появится диалог выбора носителя, на который будет помещён новый ключевой контейнер. В этом диалоге отображаются все доступные на данный момент носители с указанием их типа и серийного номера (в скобках). Установка флажка «Показать ключевые контейнеры» позволяет отобразить также ключевые контейнеры на носителях, если такие имеются. Если носитель ещё не вставлен в компьютер, то необходимо его вставить и нажать кнопку «Обновить».

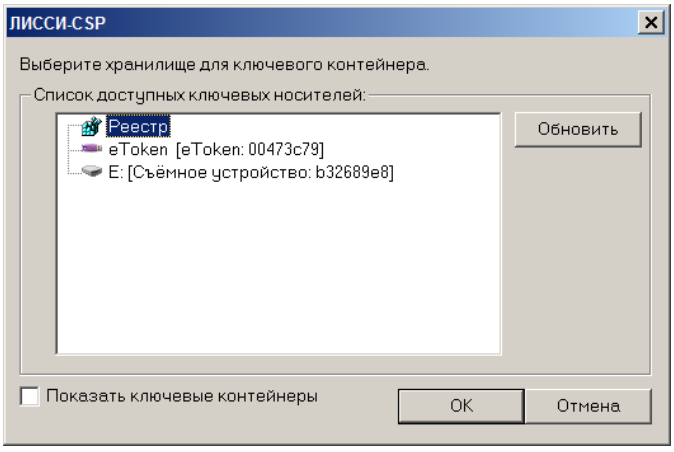

Рис. 5.10

Уникальное имя нового контейнера генерируется автоматически и не может быть задано пользователем.

Выберете нужный носитель из списка доступных и нажмите кнопку «OK».

Задайте PIN-код (пароль) для доступа к носителю (новому контейнеру) и нажмите кнопку «OK».

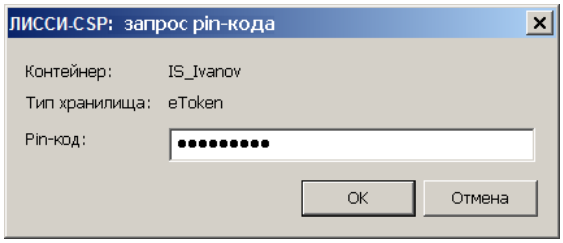

Рис. 5.11

В случае успеха появится диалог, информирующий о том, что импорт был успешно завершён.

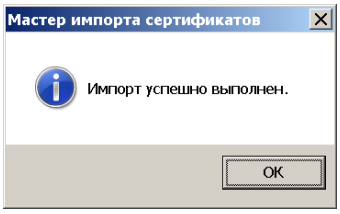

Рис. 5.12

6 Изменение PIN-кода электронного ключа

6.1 Изменение PIN-кода eToken

Вставьте ваш электронный ключ eToken (если он ещё не вставлен) в USB порт компьютера и выполните команду «Пуск | Программы | eToken | eToken PKI Client | eToken Properties».

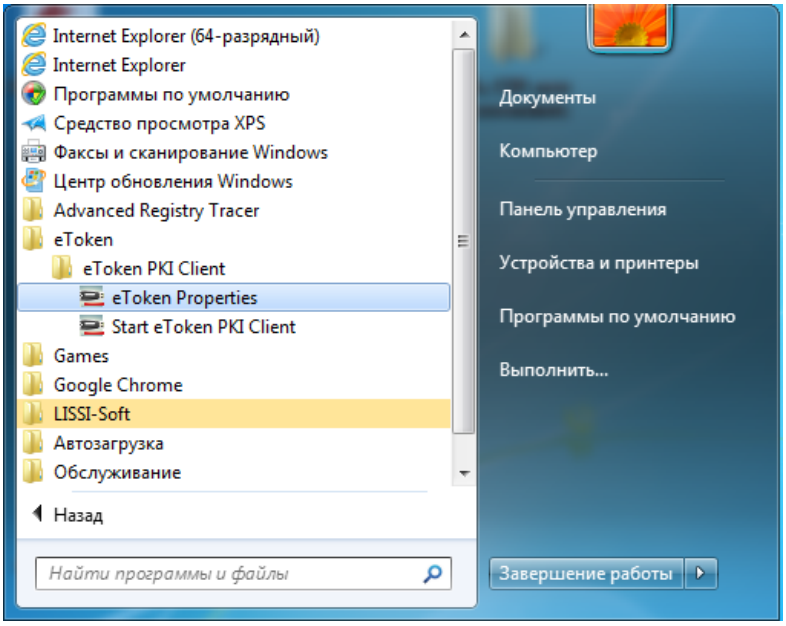

Рис. 6.1

В появившемся окне щелчком левой клавиши мышки выберите команду «Изменить пароль eToken».

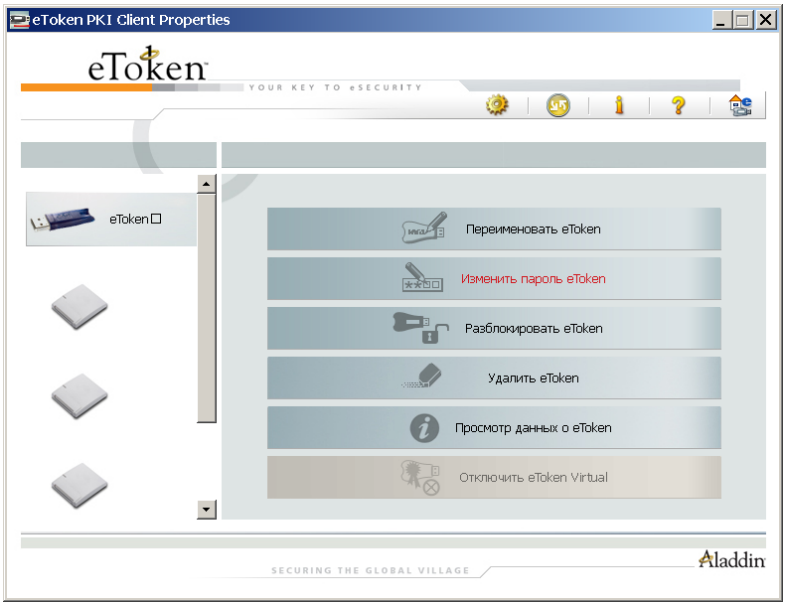

Рис. 6.2

В появившемся диалоге в поле ввода «Текущий пароль для eToken» введите текущий PIN-код. В полях ввода «Новый пароль для eToken» и «Подтверждение» введите новый PIN-код. Для возможности изменения текущего PIN-кода на новый он должен удовлетворять требованиям к сложности. Если «поле прогресса» не заполнено на 100%, то сменить PIN-код не удастся. Для усложнения пароля используйте буквы в большом и малом регистре, а также цифры.

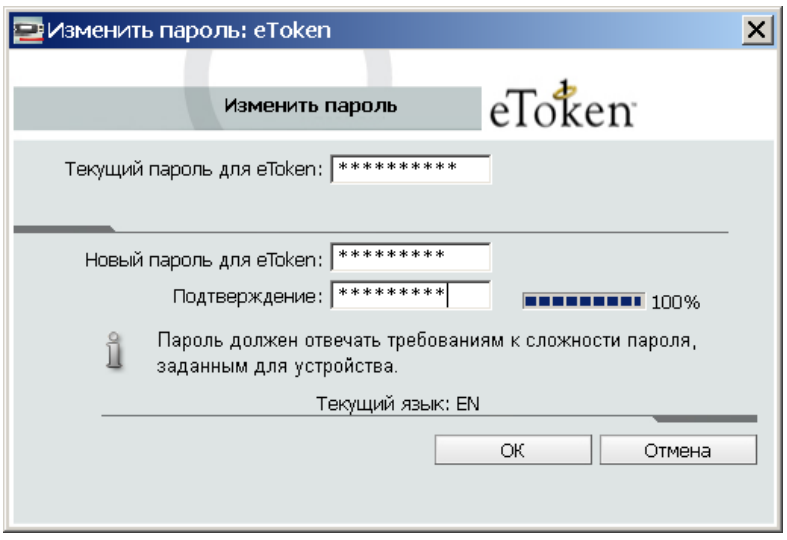

Рис. 6.3

Если сложность пароля удовлетворительная, то нажмите «OK» для смены PIN-кода.

В случае успеха на экране появится диалог с соответствующим уведомлением.

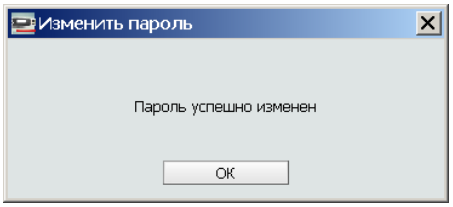

Рис. 6.4

Нажмите «OK» и закройте программу щелчком левой клавиши мыши по крестику в правом верхнем углу.

6.2 Изменение PIN-кода Rutoken

Вставьте ваш электронный ключ Rutoken (если он ещё не вставлен) в USB порт компьютера и выполните команду «Пуск | Настройка | Панель управления». В появившемся окне найдите иконку «Панель Управления Рутокен» и щёлкните по ней двойным щелчком мыши.

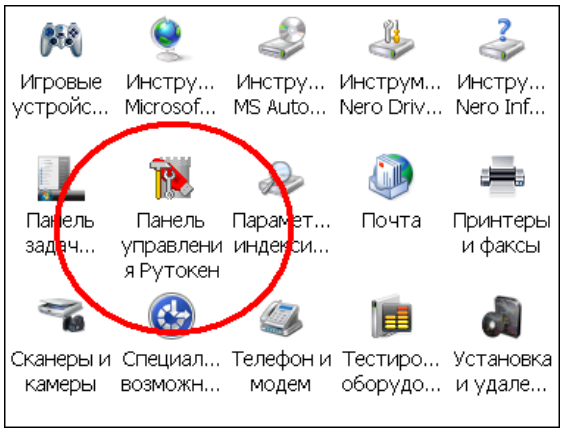

Рис. 6.5

Убедитесь, что в появившемся диалоге во вкладке «Администрирование» в разделе «Считыватели Rutoken» выбран нужный Rutoken и нажмите кнопку «Login...».

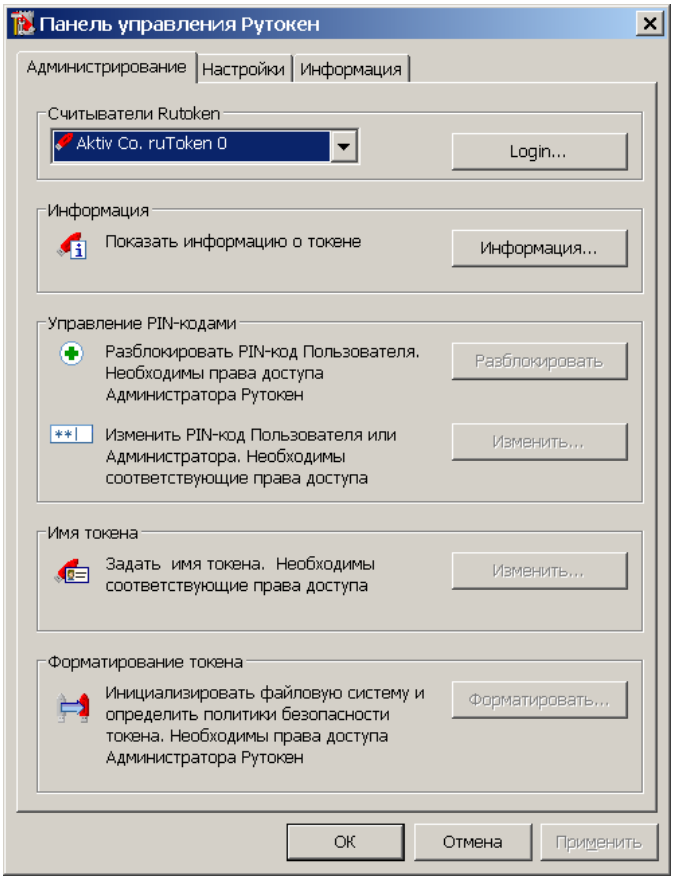

Рис. 6.6

В появившемся диалоге введите текущий PIN-код для Rutoken и нажмите «OK».

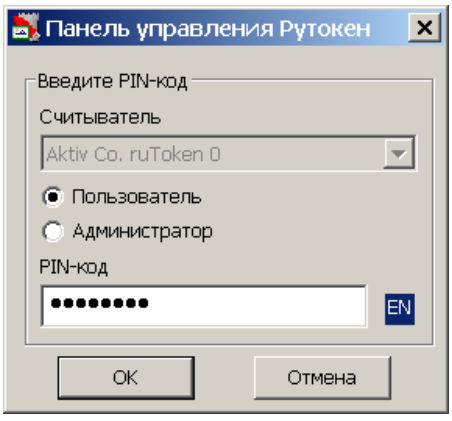

Рис. 6.7

В разделе «Управление PIN-кодами» нажмите копку «Изменить». В появившемся

диалоге введите новый PIN-код и его подтверждение в соответствующих полях ввода и нажмите кнопку «OK».

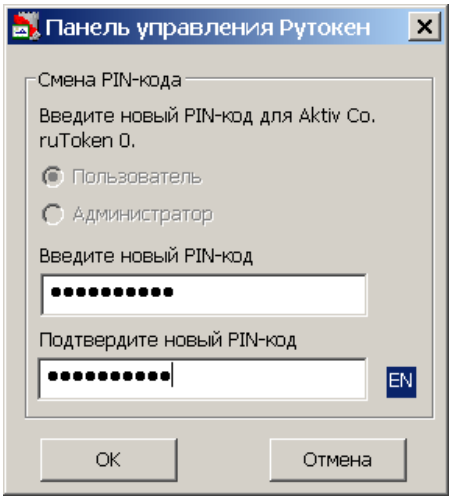

Рис. 6.8

PIN-код успешно изменён. Нажмите «OK» для выхода из программы.

7 Дополнительная информация

7.1 Определение разрядности операционной системы

В случае если у вас установлена ОС Windows XP, 2003 с большой вероятностью у вас 32-х рязрядная ОС.

В случае если у вас установлена ОС Windows Vista, 7, 2008 разрядность можно узнать выполнив следующие действия:

- Выполнить щелчок правой клавишей мыши на пункте «Компьютер» в главном меню (Пуск) и выбрать в появившемся контекстном меню пункт «Свойства»;
- В появившемся окне в строчке «Тип системы» будет указана разрядность вашей ОС.

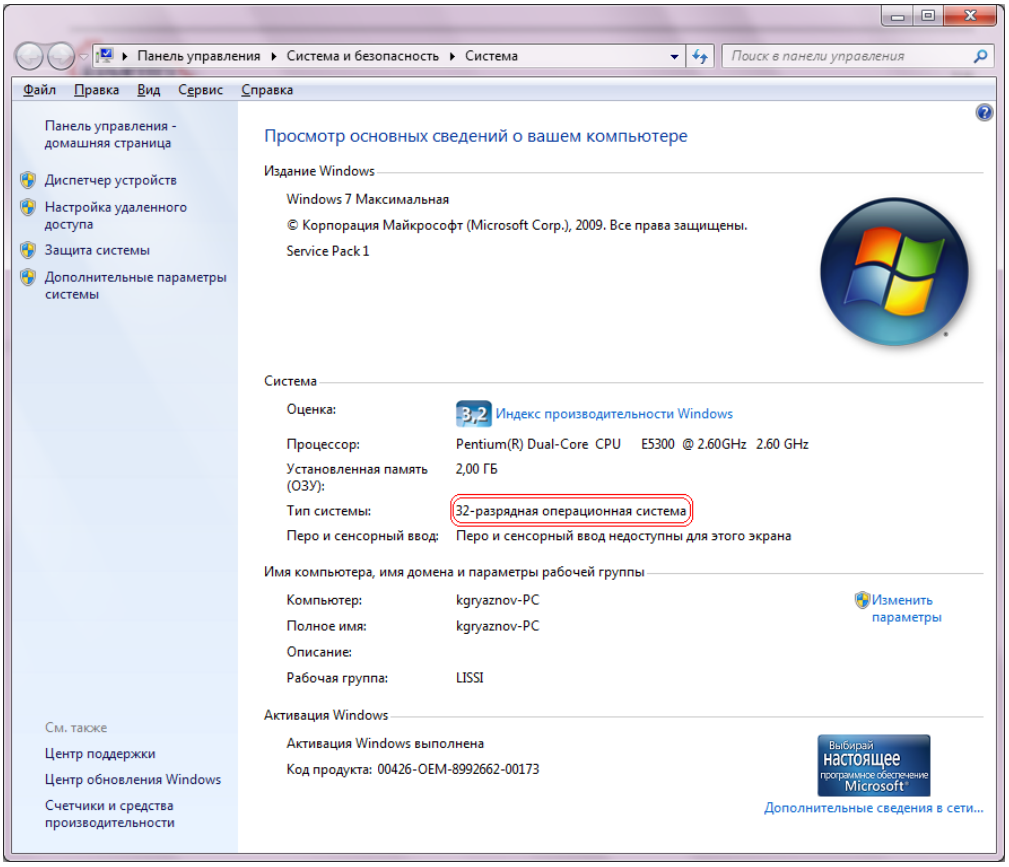

Рис. 7.1

7.2 Определение типа токена

Определить какой у вас тип токена можно сравнив внешний вид и обозначение вашего токена с моделями представленными на сайте производителей.

- http://www.aladdin-rd.ru/catalog/etoken/models.php - электронные ключи eToken компании «Aladdin»
- http://www.rutoken.ru/products/ - электронные ключи Rutoken компании «Актив».
- http://www.multisoft.ru/katalog/zawita_informacii/skzi_ms_key_k/ms_key_k_isp5/ - электронные ключи MS_Key K компании «Мультисофт».