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 JCP

Версия 2.0

Инструкция по использованию

ЖТЯИ.00091-01 91 01

Листов 50

2016 г.

Оглавление

1. Введение

Настоящее руководство содержит общее описание средства криптографической защиты информации (СКЗИ) «КриптоПро JCP» версия 2.0, его состав, ключевую систему, рекомендации по размещению технических средств, использующих СКЗИ, рекомендации по проверке целостности установленного ПО СКЗИ, по использованию СКЗИ в различных автоматизированных системах и средствах вычислительной техники.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро JCP» версия 2.0, должны разрабатываться с учетом требований настоящего Руководства.

Криптопровайдер «КриптоПро JCP» версия 2.0 является средством криптографической защиты информации (СКЗИ «КриптоПро JCP» версия 2.0), реализующим российские криптографические алгоритмы и функционирующим под управлением виртуальной машины Java 2 Runtime Environment версии 1.6 и выше.

Криптопровайдер «КриптоПро JCP» версия 2.0 должен использоваться с сертифицированными SUN Java-машинами, соответствующим требованиям безопасности SUN. Защищенность криптографических объектов, создаваемых и обрабатываемых криптопровайдером, зависит от степени защищенности и корректности Java-машины, и может быть снижена при использовании виртуальных машин, не имеющих сертификата SUN. Список сертифицированных Java-машин находится на сайте SUN по адресу: http://java.sun.com/j2se/licensees/index.html

2.Список сокращений

CRL

Список отозванных сертификатов (Certificate Revocation List)

IETF

Internet Engineering Task Force

ITU-T

Международный комитет по телекоммуникациям (International Telecommunication Union)

АС

Автоматизированная система

АРМ

Автоматизированное рабочее место

ГМД

Гибкий магнитный диск

ДСЧ

Датчик случайных чисел

HDD

Жесткий магнитный диск

КП

Конечный пользователь

НСД

Несанкционированный доступ

ОС

Операционная система

ПАК

Программно-аппаратный комплекс

ПКЗИ

Подсистема криптографической защиты информации

ПО

Программное обеспечение

Регистрация

Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту

Регламент

Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.

СВТ

Средства вычислительной техники

Сертификат

Электронный документ, подтверждающий принадлежность открытого ключа и определенных атрибутов конкретному абоненту

Сертификация

Процесс изготовления сертификата ключа проверки ЭП абонента в центре сертификации

СКЗИ

Средство криптографической защиты информации

СОС

Список отозванных сертификатов (Certificate Revocation List)

СС

Справочник сертификатов ключей проверки ЭП. Сетевой справочник.

ЦС

Центр Сертификации (Удостоверяющий Центр)

ЦР

Центр Регистрации

ЭД

Электронный документ

ЭП

Электронная подпись

3.Установка ПО СКЗИ на ПЭВМ

3.1.Способы установки

Основной способ установки «КриптоПро JCP» версия 2.0 состоит в запуске командного файла, входящего в состав дистрибутива «КриптоПро JCP» версия 2.0, имя командного файла зависит от операционной системы, на которую производится установка.

Перед установкой «КриптоПро JCP» версия 2.0 необходимо предварительно удалить предыдущую версию продукта.

Для установки «КриптоПро JCP» версия 2.0 Вы должны иметь права администратора на данной рабочей станции.

3.2.Кодировки в Java

При запуске классов «КриптоПро JCP» версия 2.0 будет выводить сообщения в кодировке принятой в Вашей java по умолчанию. В случае несовпадения кодировки, установленной в java при запуске, и кодировки окна, прочитать текст будет невозможно. Изменить кодировку при запуске java можно указав значением переменной file.encoding нужную кодировку, например

```
java -Dfile.encoding=Cp866 -version
```

Из кода программы сменить кодировку можно методом

System.setProperty("file.encoding", "UTF-8");

Если Вы хотите, чтоб «КриптоПро JCP» версия 2.0 выводил сообщения в другой кодировке, измените значение переменной. Такое возможно, например, если Вы собираетесь перенаправить вывод в файл

setup_console.bat \java >log.txt 2>&1

и анализировать его потом используя другую кодировку.

В Unix-системах java-машины используют для определения кодировки значение переменной LANG. Следите за тем, чтобы значение этой переменной совпадало с кодировкой Вашего окна.

3.2.1.Установка на Windows

Установка «КриптоПро JCP» версия 2.0 должна проводится администратором из командной строки, находясь в папке с инсталлятором:

```
setup_console.bat <путь_к_JRE>,
```

например,

```
setup_console.bat "C:\Program Files\Java\jdk1.6\jre"
```

При этом будет использоваться исполняемый файл <JRE>\bin\java.exe, а также будет произведено полное удаление файлов «КриптоПро JCP» версия 2.0, что может быть необходимо при разрешении ошибочных ситуаций. В любом случае, перед установкой автоматически осуществляется попытка деинсталляции «КриптоПро JCP» версия 2.0 на случай, если оно было ранее установлено. Если имя компании содержит пробелы, то оно должно быть заключено в кавычки. Если имя компании указывается на русском языке, то кодировка должна совпадать с указанной в <JRE>\lib\font.properties

По окончании процесса установки необходимо убедиться в корректности установки и ввести лицензию (см. «Проверка и ввод лицензии»), если она не была указана сразу, для этого запустите файл:

```
ControlPane.bat <путь_к_JRE>
```

Если установка завершилась успешно, то будет запущена контрольная панель «КриптоПро JCP» версия 2.0. При необходимости введите лицензию, как это описано

документе «ЖТЯИ.00091-01 91 02. Инструкция по использованию», раздел "Контрольная панель".

Удаление «КриптоПро JCP» версия 2.0 проводится администратором из командной строки:

```
setup_console.bat <путь_к_JRE>
```

При этом будет использоваться исполняемый файл <JRE>\bin\java.exe, а также будет произведено полное удаление файлов «КриптоПро JCP» версия 2.0.

В связи с возможностью одновременного сосуществования нескольких JRE на одной машине необходимо следить за тем, чтобы установка, удаление и использование «КриптоПро JCP» версия 2.0 проводилось одним и тем же JRE, то есть программные модули запускались одним и тем же файлом <JRE>\bin\java.exe.

Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. На Windows Vista/2008/7/2008R2/8/2012/8.1/2012R2 запуск командного файла следует выполнять как "Run as administrator".

Другой вариант установки – использование приложения setup.exe <JRE>, осуществляющего запуск графического инсталлятора.

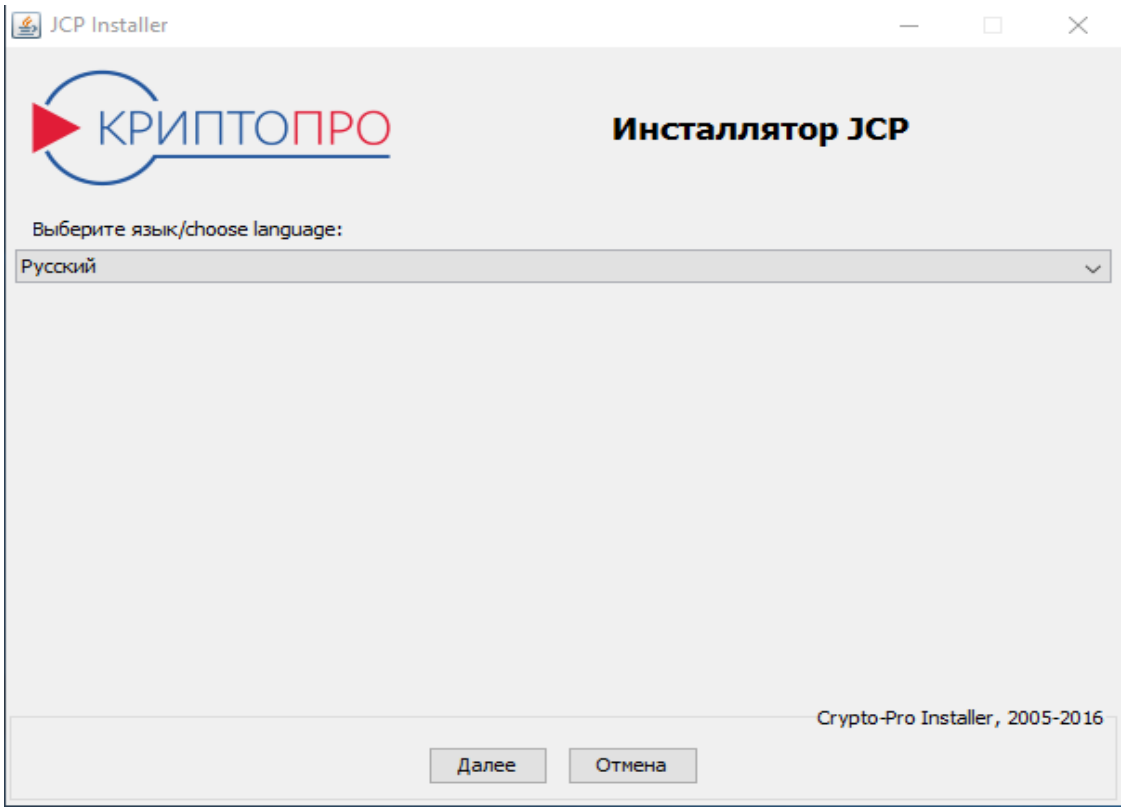

Рисунок 1. Выбор языка инсталлятора.

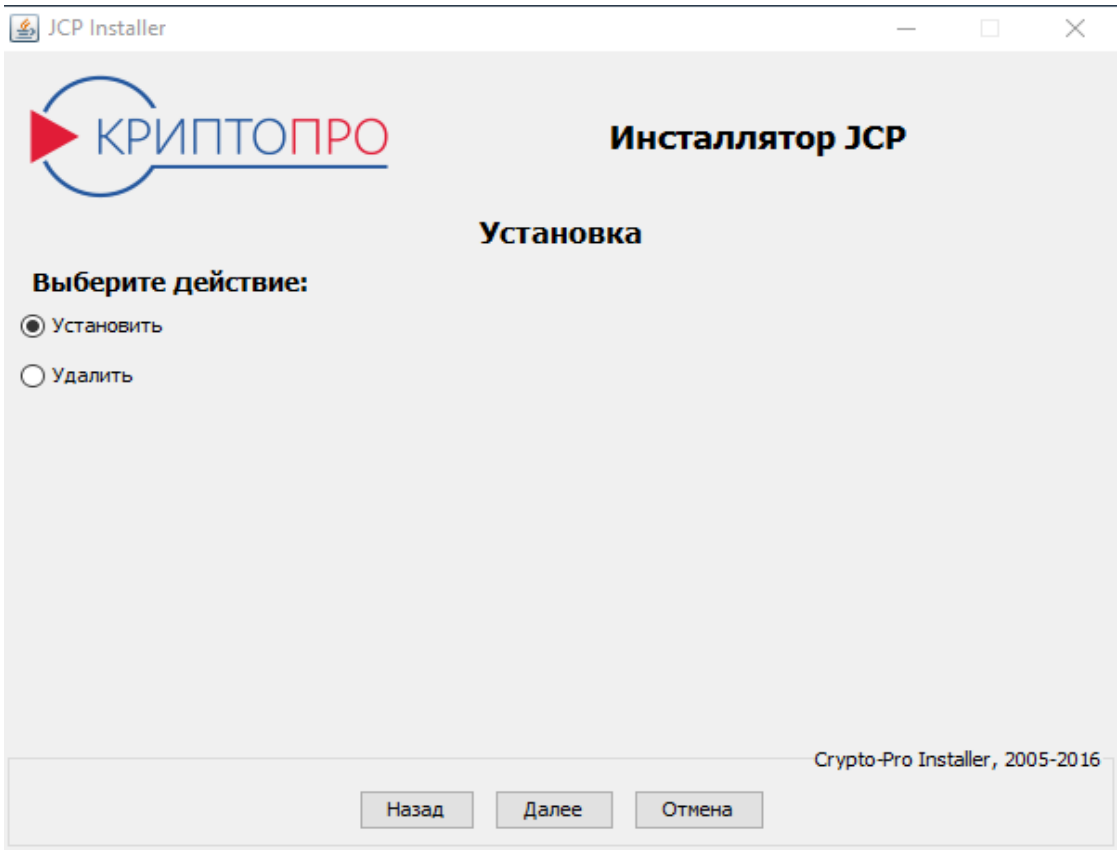

Рисунок 2. Выбор действия.

После выбора языка и действия (установка/удаление) будет предложено указать, в какой JRE будут производиться настройка, какие модули следует установить/удалить/обновить.

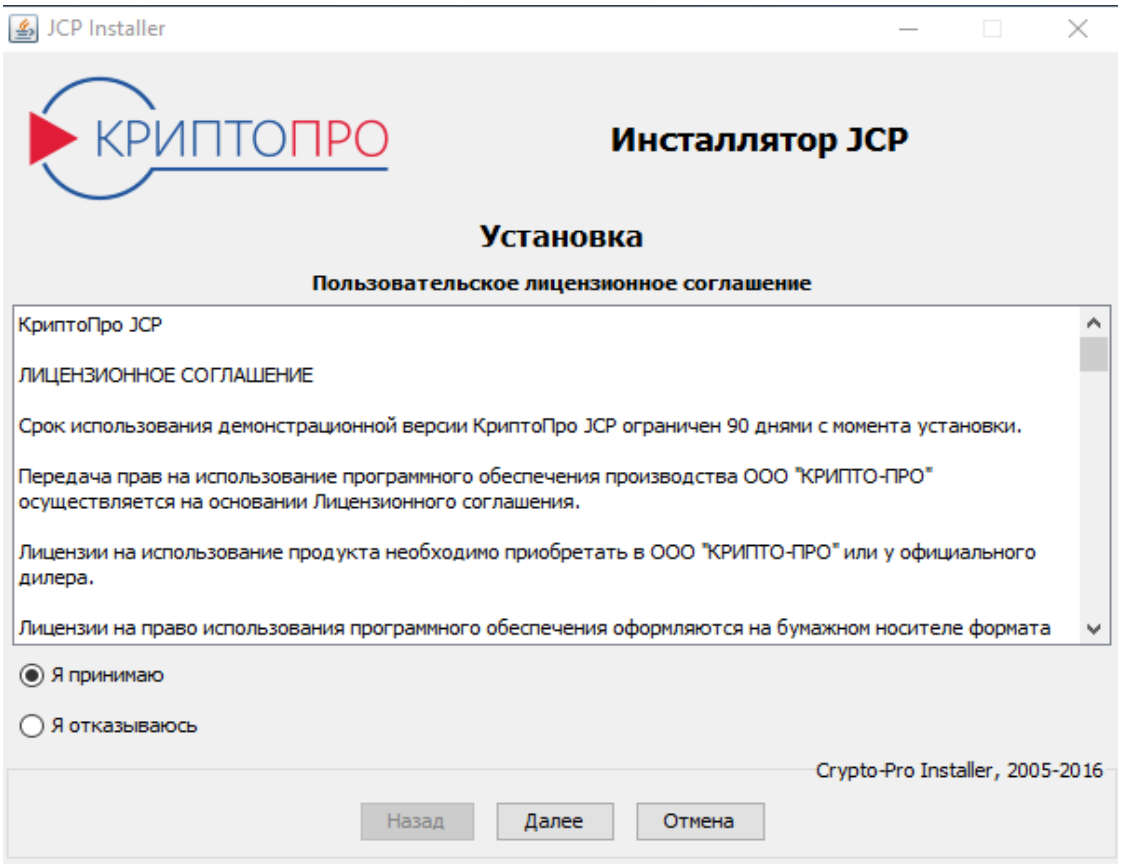

Рисунок 3. Лицензионное соглашение.

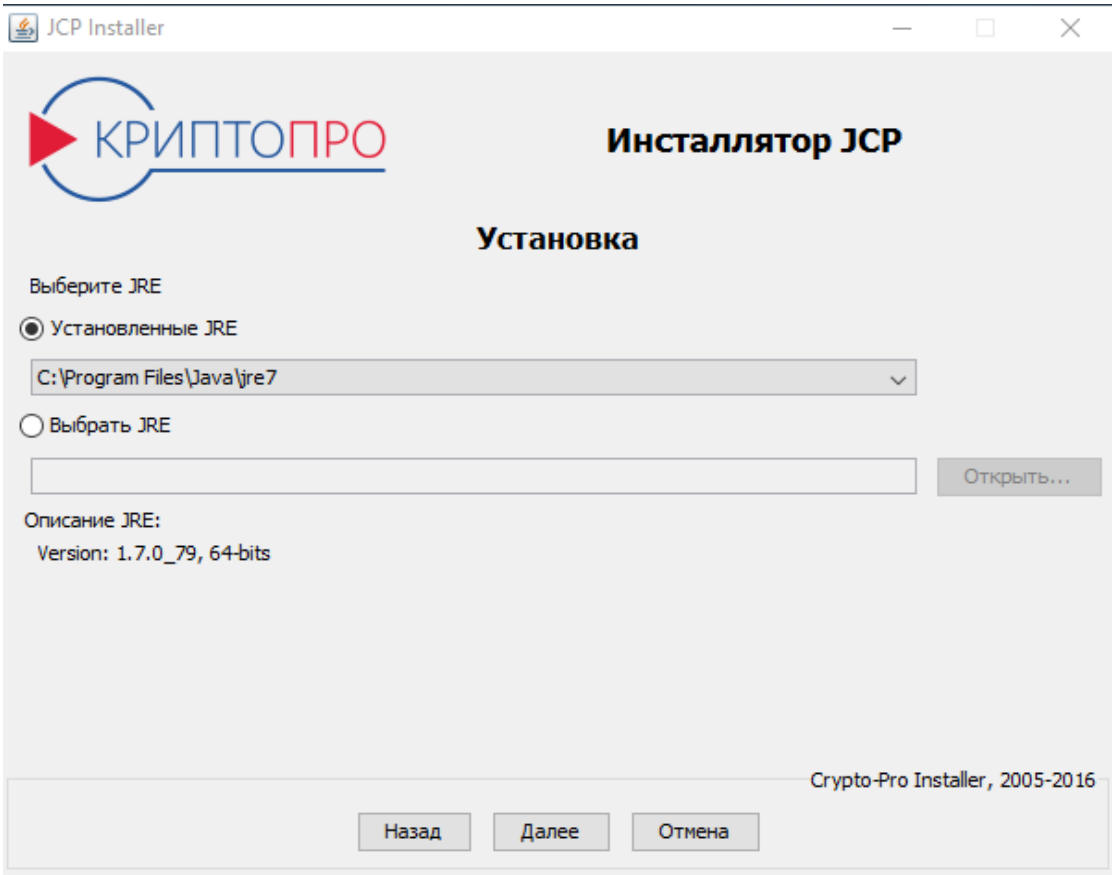

Рисунок 4. Выбор JRE.

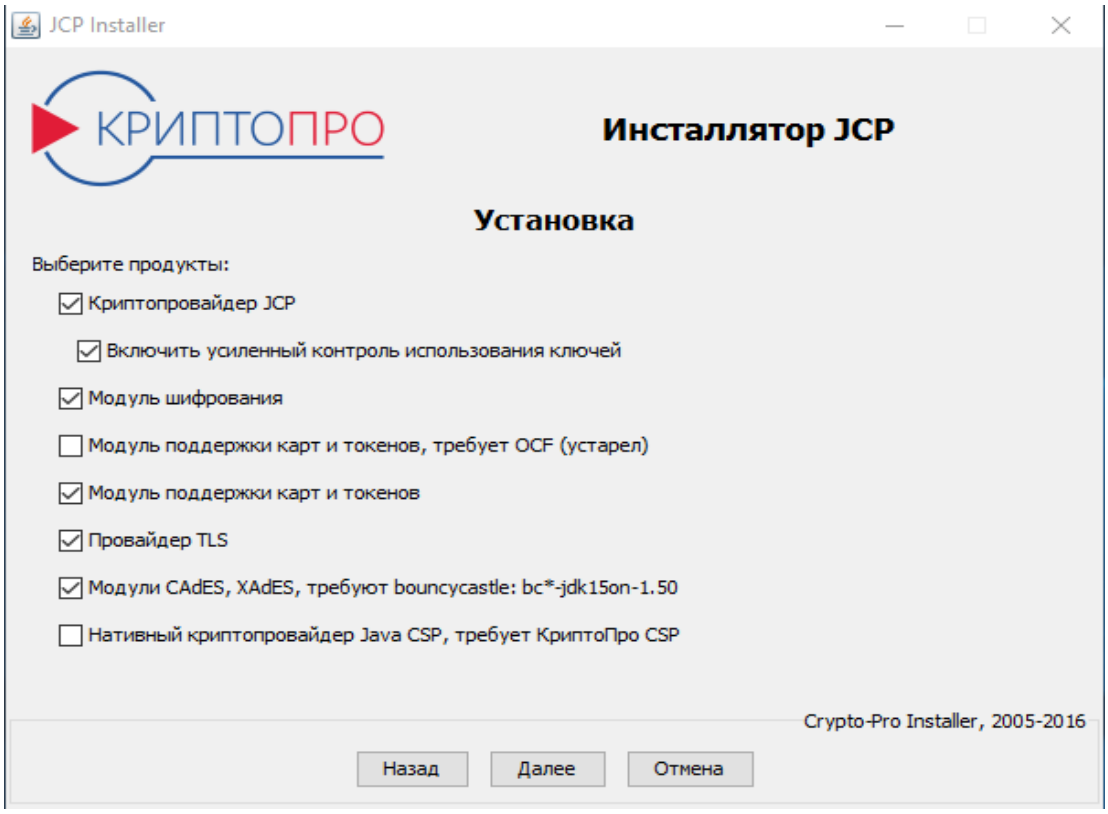

Рисунок 5. Выбор продуктов.

Внимание! При установке криптопровайдера «КриптоПро JCP» версия 2.0 необходимо **в обязательном порядке включить режим усиленного контроля использования ключей**. После установки при первом использовании СКЗИ для инициализации встроенных в СКЗИ ПДСЧ будет произведён запуск БиоДСЧ.

В случае, если режим усиленного контроля использования ключей не был включен при инсталляции СКЗИ, данный режим следует **в обязательном порядке** включить через контрольную панель СКЗИ. **Использование СКЗИ с выключенным режимом усиленного контроля использования ключей допускается исключительно в тестовых целях!**

С помощью пункта «Установить» может быть произведена как установка, так и обновление модулей. Если в указанной JRE уже имеется установленный «КриптоПро JCP» версия 2.0 и другие модули, то может быть предложено их обновить, если их версия устарела. Затем будет предложено указать серийные номера. Если они не указаны, то будут использованы серийные номера по умолчанию сроком действия 3 месяца. Тут же возможна проверка лицензий.

Важно! При установке модуля поддержки карт и токенов, требующего OCF, необходимо предварительно установить Open Card Framework. При установке модуля CadES необходимо скопировать в папку <JRE>/lib/ext файлы библиотек bouncycastle.

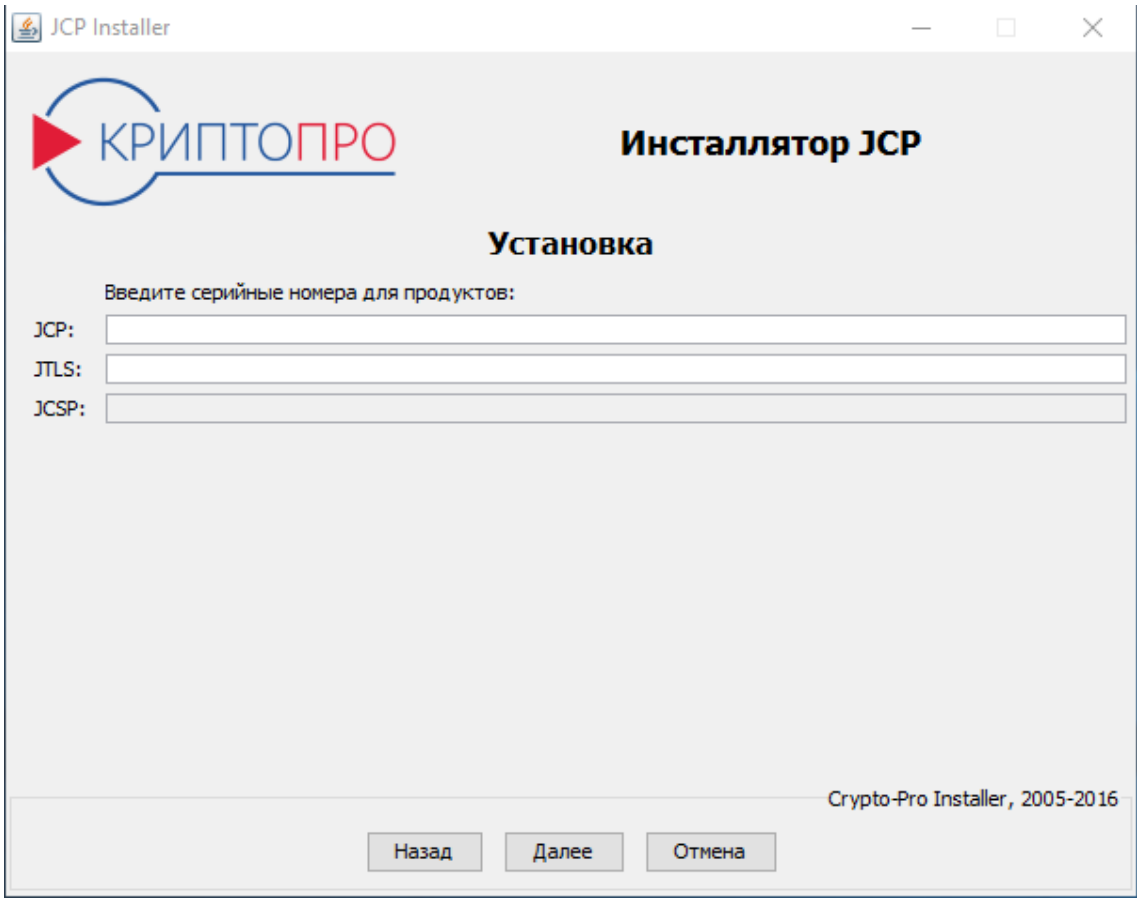

Рисунок 6. Ввод и проверка серийных номеров.

Далее будет предложено проверить корректность введенной ранее информации, удаление настроек (в случае удаления модулей).

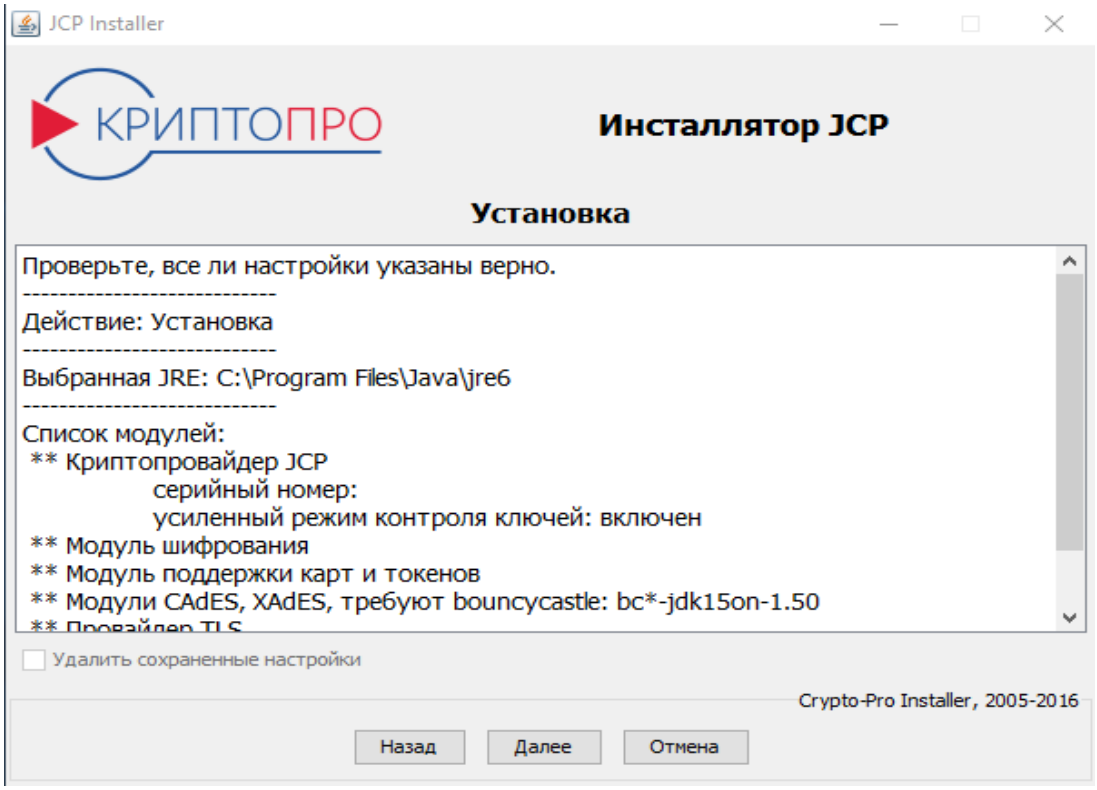

Рисунок 7. Проверка введенных данных.

Затем произойдет установка/удаление с выполнением логирования в окне установщика.

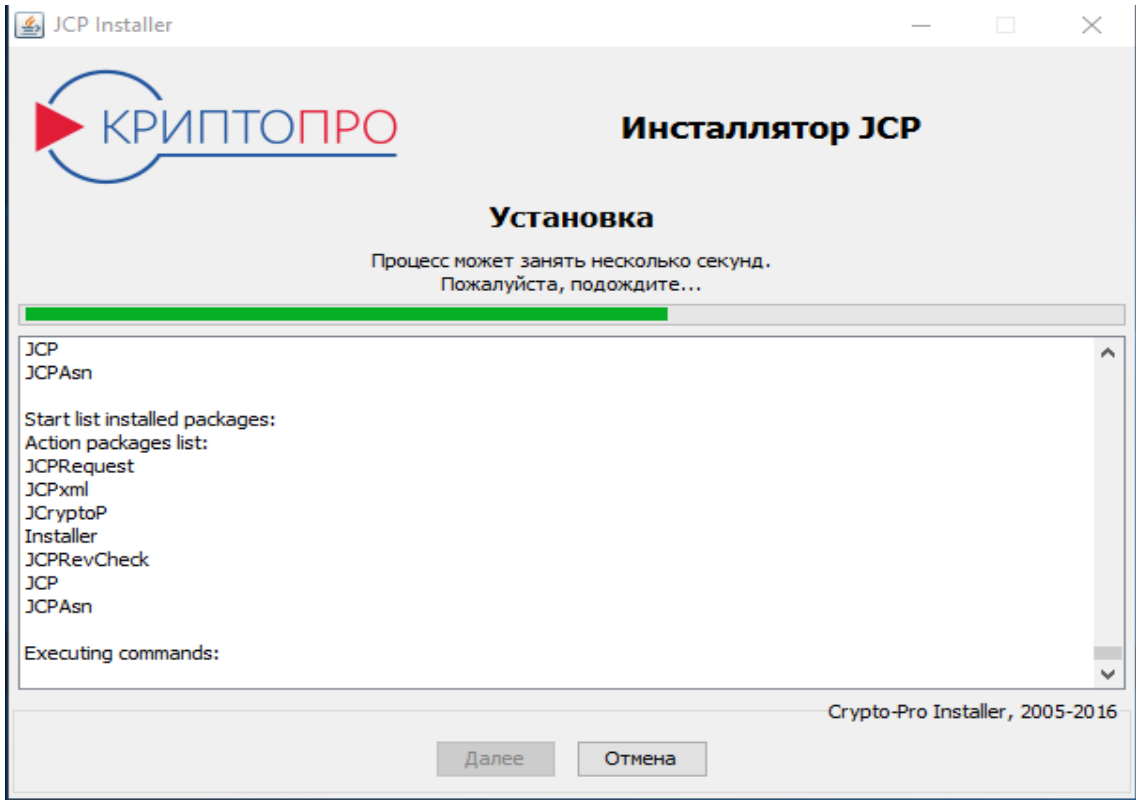

Рисунок 8. Выполнение операции.

В случае успешного выполнения будет отображено окно:

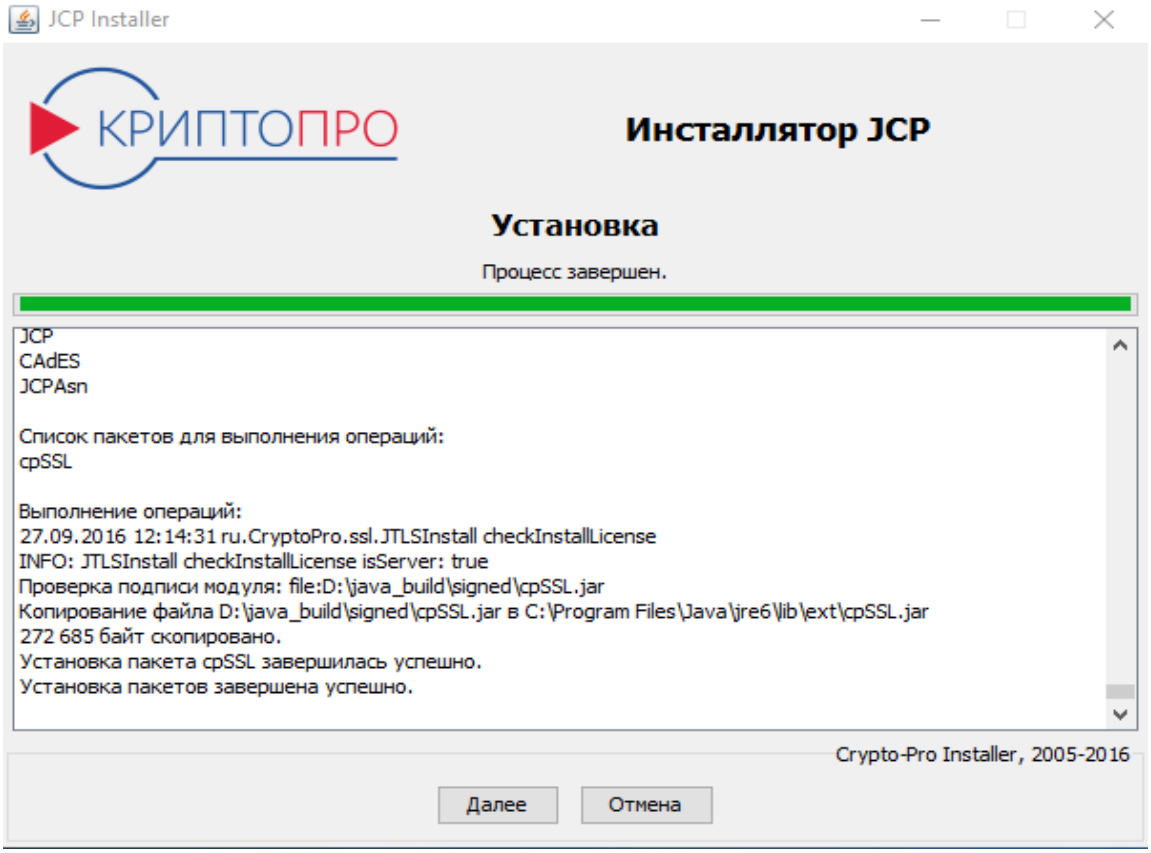

Рисунок 9. Завершение операции.

После перехода далее в случае установки может быть предложено запустить панель управления «КриптоПро JCP» версия 2.0.

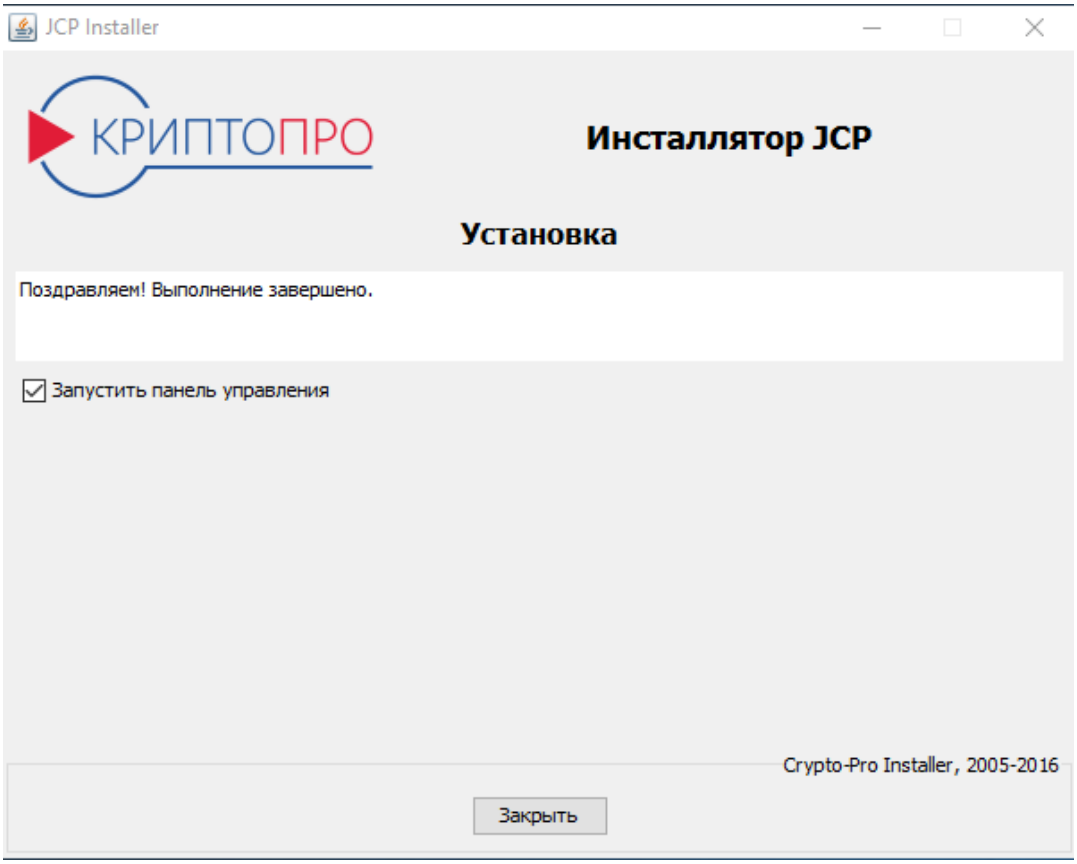

Рисунок 10. Успешное завершение и запуск панели.

Удаление отличается от установки только отсутствием некоторых шагов: лицензионное соглашение, ввод серийных номеров.

В случае ошибки соответствующее сообщение появится в ходе или при завершении операции.

Если по каким-то причинам удалить предыдущую версию «КриптоПро JCP» не удается (например, файлы заняты другим процессом), будет предложено перезапустить инсталлятор.

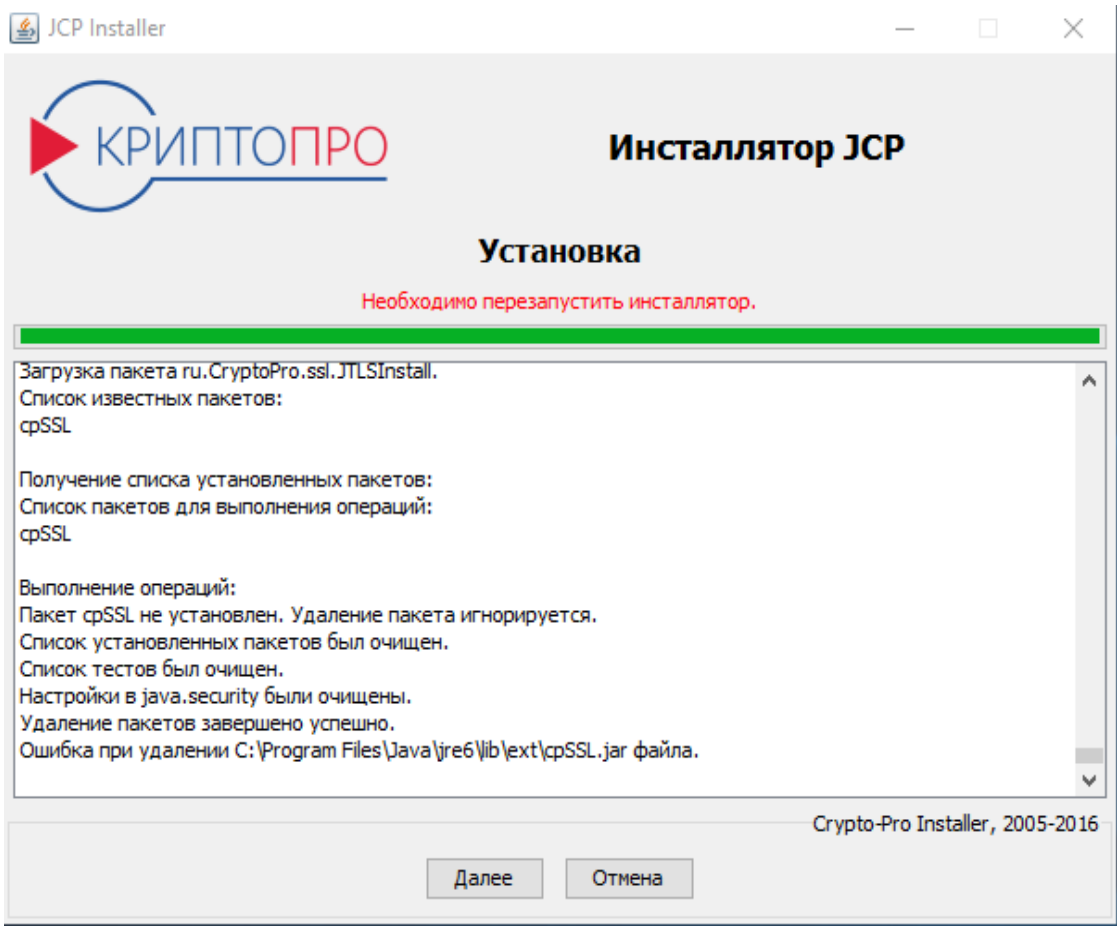

Рисунок 11. Перезапуск инсталлятора.

После нажатия на кнопку «Далее» инсталлятор будет перезапущен и перейдет к стадии проверки введенной информации (рис. 7), после чего ранее прерванная операция установки/удаления может быть возобновлена и завершена.

Консольная версия инсталлятора setup_console.bat при запуске требует указать JRE. Она мало отличается от графической версии. Возможны 2 варианта использования консольного инсталлятора:

а) пошагово указывать язык инсталлятора, JRE и вводить данные аналогично тому, как это делается в графическом инсталляторе; при этом можно использовать клавишу Enter для сохранения значения по умолчанию на каждом шаге.

б) выполнить установку/удаление без взаимодействия с пользователем. Обязательно необходимо указывать аргумент -force! Это возможно при использовании дополнительных параметров командной строки, например (setup_console.bat -help):

setup_console.bat <JRE> -force [-ru | -en] [-install | -uninstall] [-jre <value>] [-jcp | -jcryptop | -cpssl | -cades | -ocf | -j6cf | -cpssl | -jcsp] [-strict_mode] [-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] [-rmsetting]

где

•[-ru | -en] — язык инсталлятора,

•[-install | -uninstall] - выбранное действие (установка или удаление),

•[-jre <value>] - путь к JRE (по умолчанию, если параметр не задан, будет использоваться текущая исполняемая JRE),

•[-jcp | -jcryptop | -cpssl | -cades | -ocf | -j6cf | -cpssl | -jcsp] — основные доступные модули (jcp и модуль шифрования jcryptop образуют “Исполнение 2”, только один jcp – “Исполнение 1”),

•[-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] - серийные номера для выбранных продуктов,

• [-strict_mode] – включение режима усиленного контроля использования ключей (обязательно при инсталляции, потребует работы с БиоДСЧ),

•[-rmsetting] – удаление существующих настроек (только при удалении модулей).

Большинство аргументов может быть опущено. Так, отсутствие -jre приведет к использованию текущей исполняемой JRE, заданной в <JRE>.

Примеры команд:

1) установка «КриптоПро JCP» версия 2.0 (Вариант исполнения 2 — с модулем шифрования), cpSSL и CAdES в "C:\Program Files\Java\jre7" с указанием серийного номера для «КриптоПро JCP» версия 2.0.

setup_console.bat "C:\Program Files\Java\jre6" -force -ru -install -jre "C:\Program Files\Java\jre7" -jcp -jcryptop -cpssl -cades -serial_jcp XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

2) удаление «КриптоПро JCP» версия 2.0 в JRE по умолчанию (текущая исполняемая JRE) "C:\Program Files\Java\jre6".

setup_console.bat "C:\Program Files\Java\jre6" -force -en -uninstall -jcp

3) доустановка к уже установленному «КриптоПро JCP» версия 2.0 модуля Java CSP в JRE по умолчанию (текущая исполняемая JRE) с указанием серийного номера для Java CSP.

setup_console.bat "C:\Program Files\Java\jre6" -force -ru -install -jcsp -serial_jcsp XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

3.2.2.Установка на Unix и Mac OS

Установка «КриптоПро JCP» версия 2.0 на Unix осуществляется аналогично установке «КриптоПро JCP» версия 2.0 на Windows, с разницей лишь в исполняемых файлах для установки «КриптоПро JCP» версия 2.0, удаления «КриптоПро JCP» версия 2.0 и запуска контрольной панели «КриптоПро JCP» версия 2.0:

для установки «КриптоПро JCP» версия 2.0:

```
./setup_console .sh <путь_к_JRE> ,
```

например,

```
setup_console.sh /usr/java/jdk1.6/jre
```

для удаления «КриптоПро JCP» версия 2.0:

```
setup_console.sh <путь_к_JRE>
```

для запуска контрольной панели:

```
ControlPane.sh <путь_к_JRE>
```

При этом будет использоваться исполняемый файл <JRE>/bin/java.

Установка «КриптоПро JCP» версия 2.0 должна осуществляться администратором. Права, необходимые для установки «КриптоПро JCP» версия 2.0, можно получить:

1. Войти как пользователь root;
2. Выполнив команду "su";
3. Выполнив команду "sudo -s" (единственный штатный способ для Mac OS).

Другой вариант установки с помощью графического setup_gui.sh в системах Unix и Mac OS аналогичны Windows, за исключением одного отличия: JRE для установки/удаления в графическом инсталляторе необходимо указать с помощью кнопки «Открыть…» (рис. 4) или вписав в поле.

Графический инсталлятор запускается с помощью скрипта setup_gui.sh <JRE> под управлением учетной записи администратора.

3.2.3.Локальная установка вызовом Java

При установке «КриптоПро JCP» версия 2.0 на операционные системы отличные от Windows и Unix необходимо воспользоваться установкой через вызов программы java. Этот способ установки также может использоваться при частичной установке «КриптоПро JCP» версия 2.0, а также при установке из других программ.

Перед запуском установки необходимо убедиться в том, что:

•все файлы для установки находятся в одном каталоге;

•в переменной окружения PATH первым встречается каталог <JRE>/bin/ именно той java-машины, в которую планируется проводиться установка, либо при каждом выполнении команд указывается полный путь к исполняемому файлу java;

•установка производится администратором.

Для запуска программы установки необходимо вызвать java с именем jar файла, например:

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantTwo
```

для установки Варианта 2 («КриптоПро JCP» версия 2.0 с функциями шифрования)

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne
```

для установки Варианта 1 («КриптоПро JCP» версия 2.0 без функций шифрования)

Программа установки поддерживает следующие команды:

-install

Установка пакета или нескольких пакетов.

-uninstall

Удаление одного или нескольких пакетов.

-installed

Получение списка установленных пакетов.

-help

Получение справки.

При выполнении команды могут быть указаны дополнительные опции:

-skipFiles

Запретить копировать или удалять JAR-файлы.

-rmsetting

Удалить все настройки. При задании этой опции будут удалены все пользовательские и административные настройки. Рекомендуется использовать эту опцию только при полном удалении «КриптоПро JCP» версия 2.0 с компьютера. При переустановке «КриптоПро JCP» на новую версию, эту опцию использовать не рекомендуется.

-verbose [<file>]

Детализированный вывод протокола на экран или в файл <file>.

-dest [<folder>]

Установить в каталог <folder>.

-force

Отключить проверку наличия ранее установленного/удаленного пакета.

Для полной установки «КриптоПро JCP» версия 2.0 в одном из стандартных исполнений необходимо запустить

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantTwo -install
```

для установки Исполнения 2

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne -install
```

для установки Исполнения 1.

Для выборочной первоначальной установки нескольких пакетов необходимо задать список устанавливаемых пакетов для опции install, например:

```
java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne -install Installer,JCP
```

Список возможных пакетов:

JCPinst

Пакет установки всех пакетов входящих в «КриптоПро JCP» версия 2.0 и «КриптоПро JTLS» версия 2.0, должен быть установлен.

JCP

Провайдер для подписи, должен быть установлен.

JCPControlPane

Панель для управления настройками, должен быть установлен.

ASN1P

Расширенный ASN, должен быть установлен.

OCF

Store для хранения ключей на смарт-картах, необязательный пакет, требует установки OpenCard Framework.

Oscar

Библиотека поддержки смарт-карты Оскар, необязательный пакет, необходим для хранения секретных ключей. Требует установки пакета OCF.

J6CF

Store для хранения ключей на смарт-картах, необязательный пакет, требует SUN java 1.6 (работа через пакет javax.smartcardio).

J6Oscar

Библиотека поддержки смарт-карты Оскар, необязательный пакет, необходим для хранения секретных ключей. Требует установки пакета J6CF.

JCPRequest

Пакет формирования запроса на сертификат, необязательный пакет, требует установки пакета ASN1P.

JCPxml

Пакет поддержки подписи xml в формате xmldsig, необязательный пакет.

JCryptoP

Криптопровайдер с функциями шифрования, необязательный пакет, входит только в Исполнение 2.

JCPRevCheck

Пакет поддержки совместимости с КриптоПро УЦ при проверке цепочки сертификатов, необязательный пакет, требует установки пакета ASN1P.

JCPRevCheck

Пакет со служебными классами для поддержки JCPRevCheck и JCPRequest, требует установки JCPRevCheck и JCPRequest.

cpSSL

Пакет реализующий протоколы SSL и TLS в соответствии с российскими криптографическими алгоритмами, необязательный пакет, не входит ни в одно из исполнений (устанавливается отдельно, см. «Руководство программиста» КриптоПро JTLS), требует установки пакетов JCP, ASN1P, JCryptoP.

При установке пакета JCP могут быть указаны дополнительные опции:

-serial XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Установка серийного номера XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

-company "Your Company"

Установка компании владельца серийного номера, используется только совместно с -serial. Если имя компании содержит пробелы, то оно должно быть заключено в кавычки.

Для удаления «КриптоПро JCP» версия 2.0 необходимо запустить класс вариант установки с опцией -uninstall, например следующим образом:

```
java ru.CryptoPro.Install.VariantTwo -uninstall -skipfiles delfiles.lst
```

После завершения процесса удаления «КриптоПро JCP» версия 2.0, необходимо удалить все файлы имена которых находятся в списке delfiles.lst.

Для частичного удаления «КриптоПро JCP» версия 2.0 (удаления нескольких пакетов) опции -uninstall можно задавать имена удаляемых пакетов аналогично опции -install. Так же при удалении можно задавать и другие опции, описанные выше.

Для получения списка установленных пакетов можно воспользоваться командной строкой:

```
java ru.CryptoPro.Install.VariantTwo –installed
```

3.2.4.Установка дополнительных пакетов

Установка дополнительных пакетов осуществляется другим способом. Для установки дополнительных пакетов, а так же пакетов входящих в состав «КриптоПро JCP» версия 2.0, но не установленных при начальной установке, необходимо использовать установщик входящий в состав дополнительного пакета или воспользоваться установкой пакета по умолчанию.

Установка дополнительного пакета с настройками по умолчанию, осуществляется вызовом java:

```
java -jar <имя jar>
```

Если пакет состоит из нескольких jar файлов, то все файлы пакета должны находится в одной директории. Удаление пакета можно проводить любым из способов описанных выше.

Установка дополнительного пакета с заданием опций, производится вызовом программы установки из этого пакета. Например:

```
java -classpath JCPxml.jar ru.CryptoPro.JCPxml.XMLInstall -install
```

Список опций класса установки совпадает со списком опций при установке из программы установки «КриптоПро JCP» версия 2.0. Ниже приведен полный список классов установки для всех пакетов входящих в «КриптоПро JCP» версия 2.0 и «КриптоПро JTLS» версия 2.0.

JCP

ru.CryptoPro.JCP.Install.JCPInstaller; установщик пакета находится в файле JCP.jar

ASN1P

ru.CryptoPro.JCP.Install.JCPAsnInstaller; установщик пакета находится в файле JCP.jar

OCF

ru.CryptoPro.JCP.KeyStore.OCF.Install; установщик пакета находится в файле OCF.jar

Oscar

ru.CryptoPro.JCP.KeyStore.Oscar.Installer; установщик пакета находится в файле Oscar.jar

J6CF

ru.CryptoPro.JCP.KeyStore.J6CF.Install; установщик пакета находится в файле J6CF.jar

J6Oscar

ru.CryptoPro.JCP.KeyStore.J6Oscar.Install; установщик пакета находится в файле J6Oscar.jar

JCPxml

ru.CryptoPro.JCPxml.XMLInstall; установщик пакета находится в файле JCPxml.jar

JCPRequest

ru.CryptoPro.JCPRequest.RequestInstall; установщик пакета находится в файле JCPRequest.jar

JCryptoP

ru.CryptoPro.Crypto.JCryptoPInstaller; установщик пакета находится в файле JCryptoP.jar

JCPRevCheck

ru.CryptoPro.reprov.Install; установщик пакета находится в файле JCPRevCheck.jar (также необходим JCPRevTools.jar)

cpSSL

ru.CryptoPro.ssl.JTLSInstall; установщик пакета находится в файле cpSSL.jar

AdES-core

ru.CryptoPro.AdES.installer.Install; установщик пакета находится в файле adES-core.jar

CAdES

ru.CryptoPro.CAdES.installer.Install; установщик пакета находится в файле CadES.jar

XadES

ru.CryptoPro.XAdES.installer.XAdESInstall; установщик пакета находится в файле XadES.jar

JCSP

ru.CryptoPro.JCSP.JCSPInstaller; установщик пакета находится в файле JCSP.jar

3.2.5.Проверка и ввод лицензии

Криптопровайдер «КриптоПро JCP» версия 2.0 имеет два типа лицензий: клиентские и серверные. Тип лицензии зависит от платформы, операционной системы и дальнейшего применения провайдера.

Клиентские ОС:

- Windows 2000 Proffesional;
- Windows Vista;
- Windows 7/8/8.1;
- Red Hat Enterprise Linux X.X Desktop;
- Red Hat Enterprise Linux X.X Workstation; (WS)
- Fedora X;
- SUSE Linux Enterprise Desktop XX;
- OpenSUSE Linux XX.X;
- Debian GNU/Linux X.X;
- Mandriva Corporate Desktop X;
- Ubuntu X.XX Desktop Edition;
- Linux XP Enterprise Desktop 2008;
- ALT Linux X.X Desktop;
- ALT Linux X.X Lite.

Серверные ОС:

- Windows 2000 Server;
- Windows 2003;
- Windows 2008;
- Windows 2008R2;
- Windows 2012;
- Windows 2012R2;
- Solaris;
- FreeBSD;
- AIX;
- HP-UX;
- любые ОС на архитектуре отличной от ia32/amd64;

Клиентская лицензия предусматривает количество ядер не более четырех. Если количество ядер более четырех или в дальнейшем предполагается использовать JTLS сервер, то необходима серверная лицензия «КриптоПро JCP» версия 2.0 (даже если по вышеуказанному списку подходит клиентская).

Для работы с лицензией можно использовать контрольную панель или командную строку (класс `ru.CryptoPro.JCP.tools.License`).

Минимальные требования к лицензии для данной системы указаны на контрольной панели (закладка "Общие"), также их можно узнать из командной строки:

```
ru.CryptoPro.JCP.tools.License -required
```

Ввод лицензии осуществляется через контрольную панель или вызовом класса `ru.CryptoPro.JCP.tools.License` с параметрами:

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -company "company_name" -store
```

или

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -combase "company_name_in_base64" -store
```

Также можно проверить заданную лицензию без ее установки:

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -company "company_name"
```

или

```
ru.CryptoPro.JCP.tools.License -serial "serial_number" -combase "company_name_in_base64"
```

При использовании параметра "-combase" имя компании вводится в base64 кодировке.

Вызов класса `ru.CryptoPro.JCP.tools.License` без параметров проверит установленную лицензию.

Дату первой установки можно узнать с помощью команды:

```
ru.CryptoPro.JCP.tools.License -first
```

Для вывода справки:

```
ru.CryptoPro.JCP.tools.License ?
```

Начало формы

Конец формы

3.3.Установка модуля поддержки eToken

Для того чтобы использовать eToken как носитель ключевой информации для СКЗИ «КриптоПро JCP» версия 2.0 (тип хранилища "OCFStore" см. «Руководство программиста») в исполнительной среде Java Runtime Environment, необходимо выполнить следующие подготовительные действия:

- **Установить eToken RTE**;

  Процедура установки подробно описана в руководстве пользователя eToken RTE

- **Установить исполнительную среду JRE**;
- **Установить OpenCard Framework** ;

  OpenCard Framework (OCF) – это открытый стандарт, который обеспечивает поддержку смарт-карт на Java-платформе. eToken для «КриптоПро JCP» версия 2.0 использует OCF, поэтому следующим шагом будет установка библиотеки OCF.

  Загрузите OCFbase и скопируйте все *.jar файлы в папку ${java.home}/jre/lib/ext, файлы *.properties в папку ${java.home}/jre/lib.

- **Установить «КриптоПро JCP» версия 2.0** (см. «Способы установки»);

  Если «КриптоПро JCP» версия 2.0 уже был установлен его следует переустановить.

- **Установить модуль поддержки eToken для «КриптоПро JCP» версия 2.0**.

  Модуль поддержки eToken для «КриптоПро JCP» версия 2.0 (также как и сам электронный ключ eToken) является продуктом компании Aladdin. По всем вопросам использования обращаться к компании-разработчику.

Для установки программного обеспечения вы должны иметь права администратора на данной рабочей станции.

3.4.Политики безопасности

${java.home}/lib/security/java.policy

3.4.1.Права доступа для JCP.jar

«КриптоПро JCP» версия 2.0 устанавливается в каталог `${java.home}\lib\ext`. Обычно этот каталог имеет права доступа разрешающие всем jar файлам, содержащимся в этом каталоге, получить все права доступа

```
grant codeBase "file:${java.home}/lib/ext/*" {
    permission java.security.AllPermission;
};
```

Если этот каталог имеет права доступа отличные от приведенных выше необходимо настроить права доступа для JCP.jar. Примерный вид этого файла приведен ниже.

```
grant codeBase "file:${java.home}/lib/ext/jcp.jar" {
    permission java.lang.RuntimePermission "preferences", "read";
    permission java.util.PropertyPermission "os.name", "read";
    java.util.PropertyPermission "<usedProperty>", "read";
    permission java.io.FilePermission "<pathToLocalMutex>/*" "read, write";
};
```

где:

- **<usedProperty>** - Property используемые при настройке, каких-либо путей.
- **<pathToLocalMutex>** Путь к UnixMutex для пользователя (подробнее см. «Настройки контрольной панели»)

3.4.2.Права доступа для администратора JCP

Администратору безопасности должны быть предоставлены следующие права доступа:

```
grant {
    permission java.lang.RuntimePermission "preferences", "read";
}
```

Кроме того, администратор безопасности должен иметь:

- права доступа зависящие от операционной системы для доступа к настройкам Preferences. Например, для Windows администратор безопасности должен иметь права доступа для чтения/записи в ключ реестра `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\ru\/Crypto/Pro\/J/C/P`

3.4.3.Права доступа для приложений

Установленные на JAVA машину приложения не должны осуществлять доступ к ключам. Для этого все приложения установленные на Java машину должны быть или получены от производителей доверенным способом или иметь права доступа запрещающие доступ к ключам.

Обычно каталог `${java.home}\lib\ext` разрешает всем приложениям для всех пользователям все права доступа. Необходимо или ограничить эти права доступа, запретив доступ в каталоги содержащие ключи (а так же к смарт-карте и дискете) или устанавливать в этот каталог только приложения производителей полученные доверенным способом.

3.4.4.Права доступа пользователя

Пользователь «КриптоПро JCP» версия 2.0 должен обладать следующими правами доступа:

•Права доступа, зависящие от операционной системы, для доступа к настройкам Preferences. Например, для Windows пользователь должен иметь права доступа для чтения из ключа реестра
`HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\ru\/Crypto/Pro\/J/C/P;`

•Права доступа, зависящие от операционной системы, на чтения/запись файлов во временный каталог (см. настройки контрольной панели);

•Права доступа, зависящие от операционной системы, на чтение/записи/создание каталогов в файлы ключей (см. настройки контрольной панели)

•Права доступа, зависящие от операционной системы, на чтение/запись/создание каталогов на дискету (при использовании носителя дискета)

Примечание: для Unix платформ папки `keys` и `tmp`, заданные по умолчанию (`/var/cprocsp/keys` и `/var/cprocsp/tmp`), могут быть созданы только из под root. Для их автоматического создания с правильными правами доступа достаточно создать контейнер из под root.

3.5.Особенности работы СКЗИ в консольном режиме

Для обеспечения работы СКЗИ в системах, где невозможно отображение графических окон, необходимо переключить часть функционала на использование в консольном режиме.

1. По умолчанию в СКЗИ используется графический БиоДСЧ. Для переключения на консольный БиоДСЧ необходимо запустить метод main() класса BioRandomConsole():

```
java -cp JCP.jar ru.CryptoPro.JCP.Random.BioRandomConsole
```

При необходимости графический БиоДСЧ можно включить, вызвав метод main() класса BioRandomFrame():

```
java -cp JCP.jar ru.CryptoPro.JCP.Random.BioRandomFrame
```

2. Для отключения окон, предупреждающих об окончании срока разрешения на использование ключей ГОСТ Р 34.10-2001 для выработки электронной подписи, необходимо в Java Preferences в разделе ru\/Crypto/Pro\/J/C/P\tools установить параметр /Gost2001/Warning_class_default в true.

4.Контрольная панель

В данном разделе приводится описание контрольной панели «КриптоПро JCP» версия 2.0, которая является инструментом, позволяющим устанавливать и изменять наиболее важные настройки криптопровайдера «КриптоПро JCP» версия 2.0, такие как:

- лицензия на использование криптопровайдера;
- используемые параметры криптографических алгоритмов;
- пути к хранилищам закрытых ключей и ключей ЭП;
- настройки безопасности при работе с криптопровайдером;
- файлы, контроль целостности которых необходим.

Для запуска контрольной панели в Windows можно использовать

```
ControlPane.bat <путь_к_JRE>
```

Для запуска контрольной панели в Unix используйте

```
ControlPane.sh <путь_к_JRE>
```

Запуск контрольной панели в других операционных системах осуществляется запуском класса ru.CryptoPro.JCP.ControlPane.MainControlPane принятым в Вашей системе способом.

4.1.Введение

Контрольная панель «КриптоПро JCP» версия 2.0 предназначена для работы с настройками криптопровайдера «КриптоПро JCP» версия 2.0 при помощи следующих обеспечиваемых ею операций:

- просмотр информации о существующей лицензии на использование «КриптоПро JCP» версия 2.0, а также установка новой лицензии;
- определение параметров реализованных криптографических алгоритмов;
- определение путей к хранилищам закрытых ключей и ключей ЭП(дисковод и жесткий диск);
- выбор параметров безопасности при работе с криптопровайдером «КриптоПро JCP» версия 2.0;
- контроль целостности требуемых файлов;
- управление хранилищами контейнеров и сертификатов.

Панель состоит из шести закладок ("Общие", "Алгоритмы", "Оборудование", "Дополнительно" и "Окружение", "Хранилища ключей и сертификатов"), каждая из которых обеспечивает выполнение одной из перечисленных операций. При установке дополнительных компонентов криптопровайдера «КриптоПро JCP» версия 2.0 количество закладок контрольной панели может быть увеличено.

Изменение всех настроек криптопровайдера разрешено только для пользователя, обладающего всеми правами (т.е. для администратора).Все поля контрольной панели для администратора доступны для редактирования. Для остальных пользователей часть полей панели, в зависимости от установленных для пользователей прав, будет доступна только для чтения.

Также следует обратить внимание на то, что внешний вид контрольной панели может отличаться от изображений, приведенных в данной документации. Внешний вид панели зависит от настроек, операционной системы, установленной Java машины и т.д.

4.2.Закладка "Общие" (панель "Лицензия")

Панель "Лицензия" предназначена для просмотра информации о текущей лицензии на использование криптопровайдера «КриптоПро JCP» версия 2.0, а также для установки новой лицензии, если это необходимо.

При установке криптопровайдера «КриптоПро JCP» версия 2.0 без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования «КриптоПро JCP» версия 2.0 после окончания этого срока пользователь

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

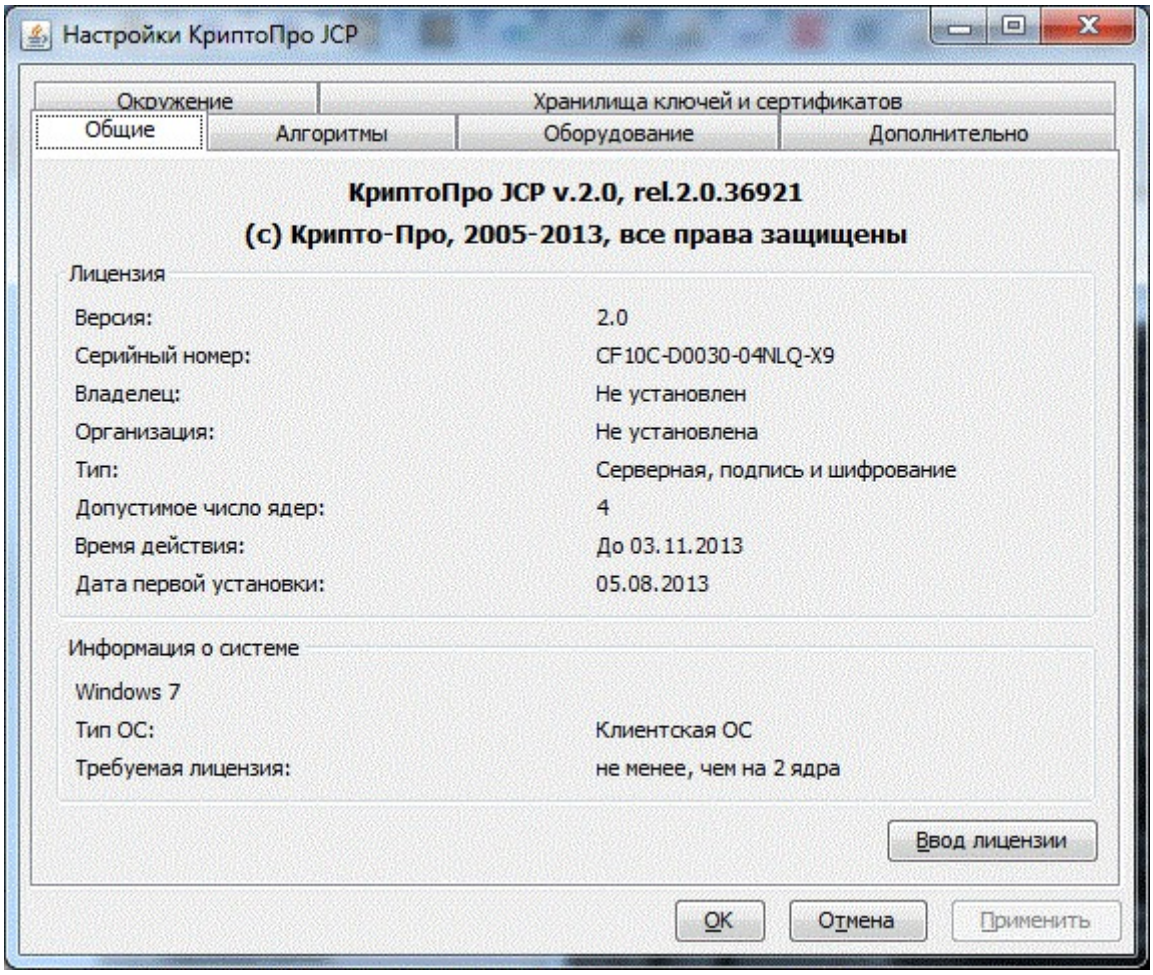

Рисунок 12. Внешний вид панели "Лицензия" (временная лицензия)

Панель включает в себя следующую информацию:

- версия криптопровайдера «КриптоПро JCP» версия 2.0;
- серийный номер лицензии на использование криптопровайдера «КриптоПро JCP» версия 2.0;
- имя владельца лицензии;
- организация, к которой относится владелец;
- тип лицензии;
- допустимое число процессоров для данной лицензии;
- время действия лицензии;
- дату первой установки провайдера.

Также указывается информация об операционной системе пользователя.

Помимо этого, в панель включена кнопка "Ввод лицензии", позволяющая по истечению срока действия предыдущей лицензии устанавливать серийный номер новой лицензии, а также информацию о ее владельце.

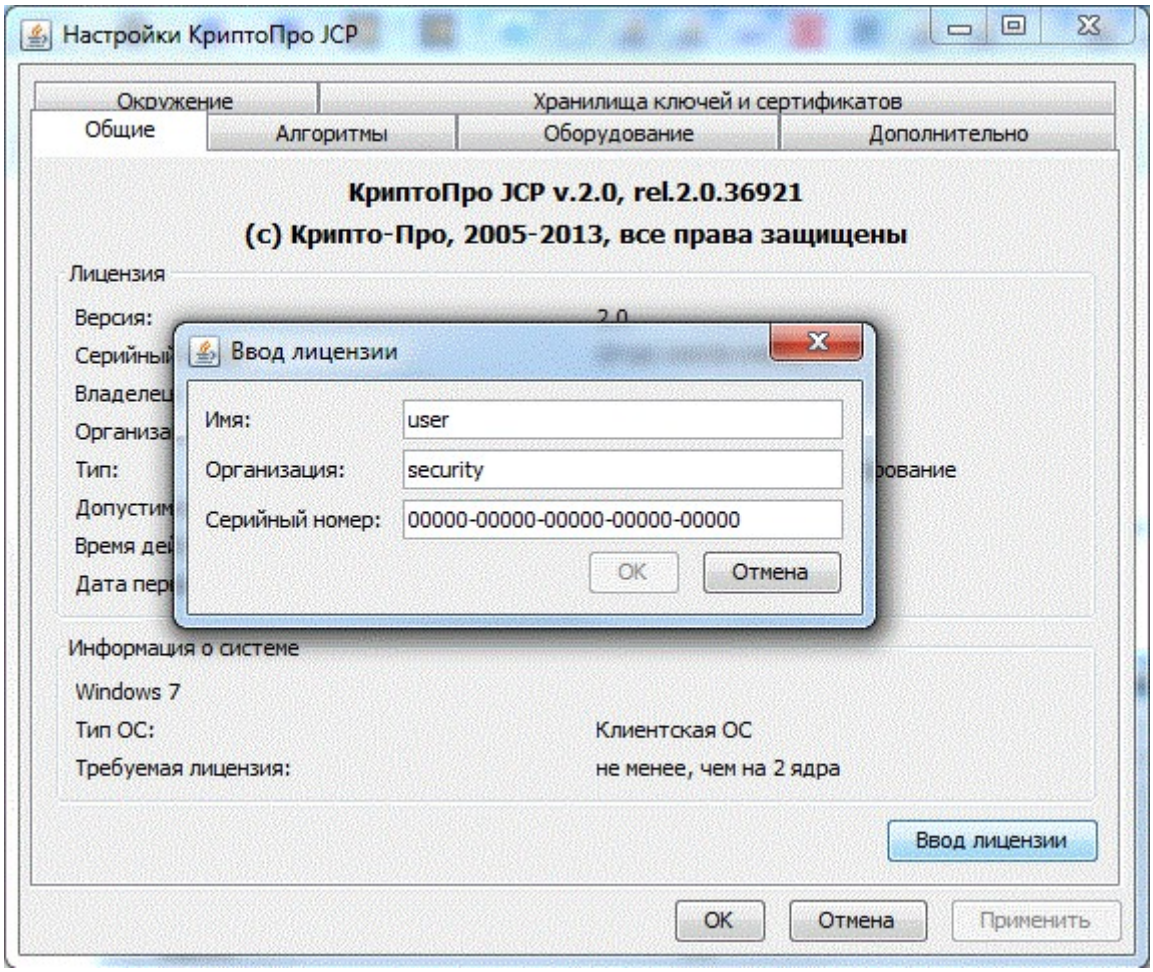

Рисунок 13. Ввод серийного номера лицензии

После ввода серийного номера новой лицензии, а также информации о владельце устанавливаемой лицензии, на панели "Лицензия" будет отображена введенная информация.

ВАЖНО: лицензия будет сохранена только после нажатия кнопок "OK" или "Применить"

4.3.Закладка "Алгоритмы" (панель "Параметры")

Панель "Алгоритмы" предназначена для просмотра используемых параметров реализованных криптографических алгоритмов. Помимо этого допускается изменение текущих параметров на любые другие, допустимые соответствующими алгоритмами.

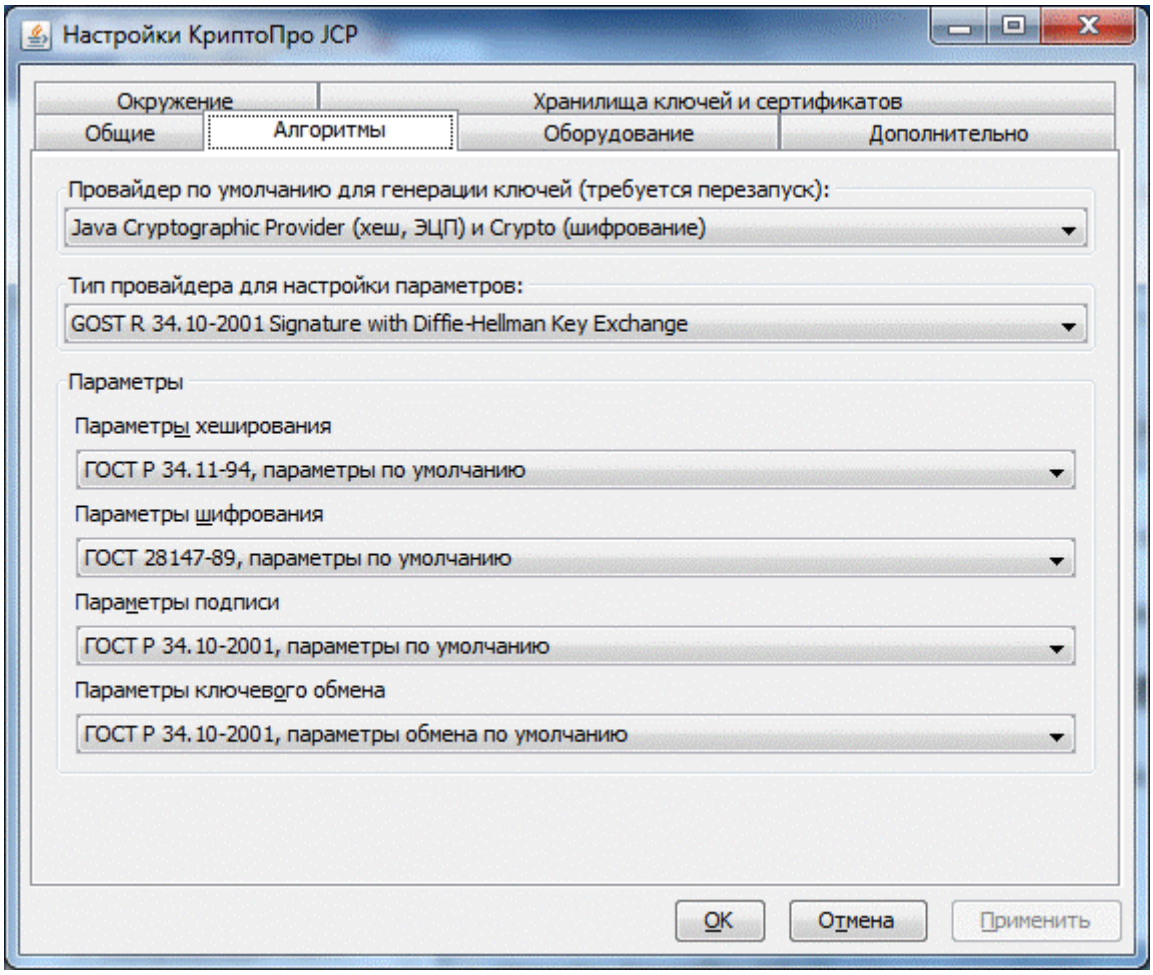

Рисунок 14. Внешний вид панели "Алгоритмы"

По умолчанию в панели "Алгоритмы" определены настройки:

•Провайдер по умолчанию для генерации ключей (требуется перезапуск)

•Тип провайдера для настройки параметров.

По умолчанию в панели "Алгоритмы" определен следующий набор параметров, которые можно настраивать в зависимости от выбранного типа провайдера:

•параметры алгоритма хэширования: ГОСТ Р 34.11-94 (параметры по умолчанию для провайдера ГОСТ Р 34.10-2001), ГОСТ Р 34.11-2012 (256) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 256 бит) и ГОСТ Р 34.11-2012 (512) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 512 бит);

•параметры алгоритма шифрования: ГОСТ 28147-89 (параметры по умолчанию для провайдера ГОСТ Р 34.10-2001) и ТК26 Z (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012);

•параметры алгоритма выработки и проверки электронной подписи: ГОСТ Р 34.10-2001 (параметры по умолчанию для провайдеров ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, 256 бит) и ГОСТ Р 34.10-2012 (512) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 512 бит);

•параметры алгоритма Диффи-Хеллмана: ГОСТ Р 34.10-2001 (параметры обмена по умолчанию для провайдеров ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, 256 бит) и ГОСТ Р 34.10-2012 (512) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 512 бит).

Панель позволяет задать провайдер по умолчанию для работы на вкладке "Хранилища ключей и сертификатов" (после сохранения изменения потребуется перезапуск панели, чтобы зафиксировать изменения на вкладке "Хранилища ключей и сертификатов"), а также устанавливать следующие параметры:

•параметры алгоритма хэширования: ГОСТ Р 34.11-94 (параметры по умолчанию для провайдера ГОСТ Р 34.10-2001), ГОСТ Р 34.11-2012 (256) (параметры по умолчанию

для провайдера ГОСТ Р 34.10-2012, 256 бит) и ГОСТ Р 34.11-2012 (512) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 512 бит);

•параметры алгоритма шифрования: ГОСТ 28147-89 (параметры по умолчанию для провайдера ГОСТ Р 34.10-2001) и ТК26 Z (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012), а также параметры шифрования 1, параметры шифрования 2, параметры шифрования 3, параметры Оскар 1.1, параметры Оскар 1.0, параметры РИК1, ТК26 2, ТК26 1, ТК26 3, ТК26 4, ТК26 5, ТК26 6;

•параметры алгоритма выработки и проверки электронной подписи: ГОСТ Р 34.10-2001 (параметры по умолчанию для провайдеров ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, 256 бит) и ГОСТ Р 34.10-2012 (512) (параметры по умолчанию для провайдера ГОСТ Р 34.10-2012, 512 бит) , а также параметры Оскар 2.x, параметры подписи 1 для провайдеров ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (256) и параметры ТК26 2 для провайдера ГОСТ Р 34.10-2012 (512);

•параметры алгоритма Диффи-Хеллмана - ГОСТ Р 34.10-2001 (параметры обмена по умолчанию, параметры обмена 1 для провайдеров ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, 256 бит) и и параметры ТК26 2 для провайдера ГОСТ Р 34.10-2012 (512).

4.4.Закладка "Оборудование"

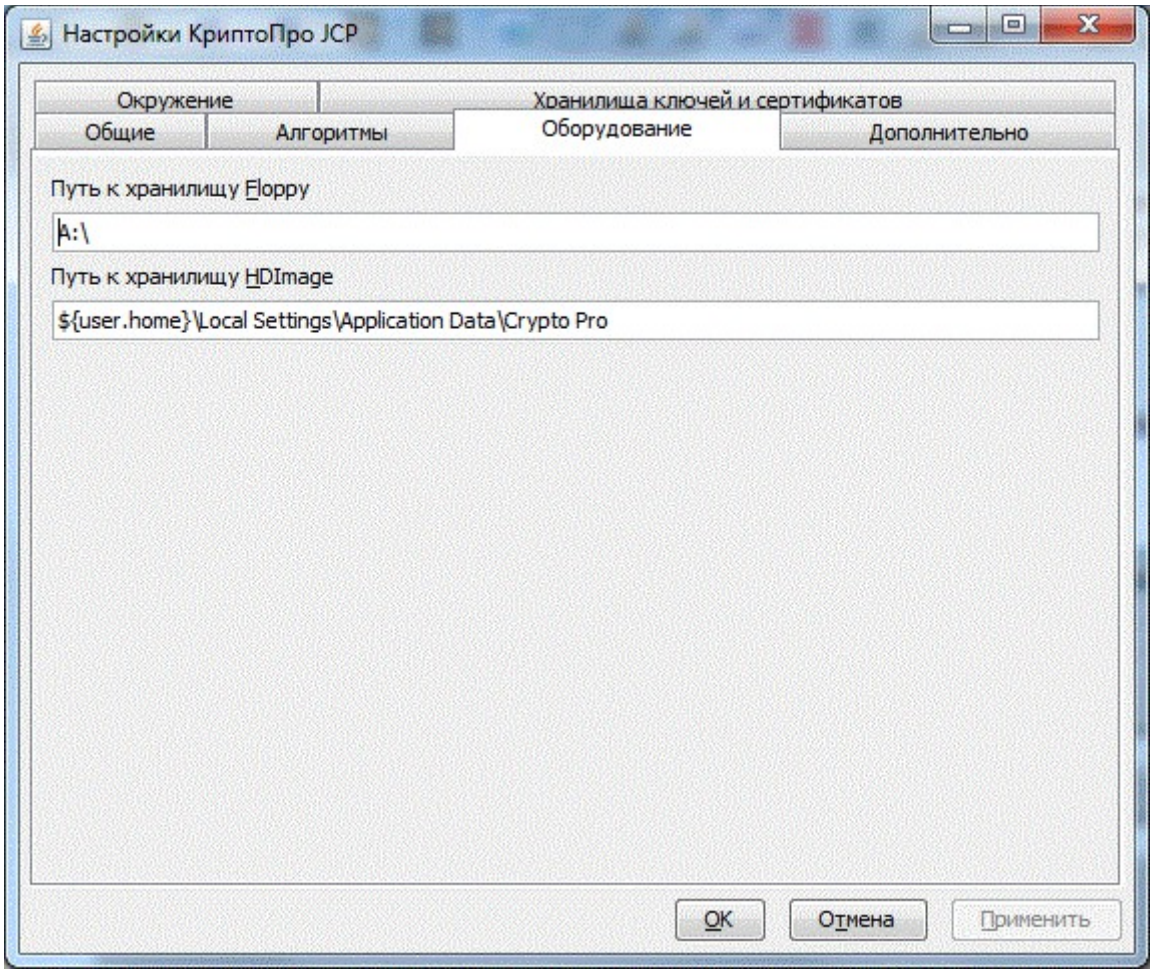

Рисунок 15. Внешний вид закладки "Оборудование"

Закладка состоит из двух полей:

•"Путь к хранилищу Floppy" - это поле предназначено для определения пути к дисководу;

•"Путь к хранилищу HDImage" - это поле предназначено для определения пути к жесткому диску.

По умолчанию в панели установлены следующие пути к носителям:

•Для Windows-платформ:

- путь к дисководу - "A:\";
- путь к жесткому диску - "${user.home}\Local Settings\Application Data\Crypto Pro";

•Для Unix-платформ:

- путь к дисководу - "/var/cprocsp/mnt/0";
- путь к жесткому диску - "/var/cprocsp/keys/${user.name}";

Предполагается, что системные настройки ${...} установлены также в значения по умолчанию, т.е. значение ${user.name} - есть имя текущего пользователя, а ${user.home} установлено в директорию "Documents and Settings\${user.name}". Следует обратить внимание на то, что при изменении текущих настроек криптопровайдера, новые пути к носителям могут содержать любые допустимые системные настройки вида "${...}". Следует учитывать, что значение переменной может быть изменено при запуске Java-машины.

4.5.Закладка "Дополнительно"

Закладка "Дополнительно" предназначена для выбора параметров безопасности при работе с криптопровайдером «КриптоПро JCP» версия 2.0.

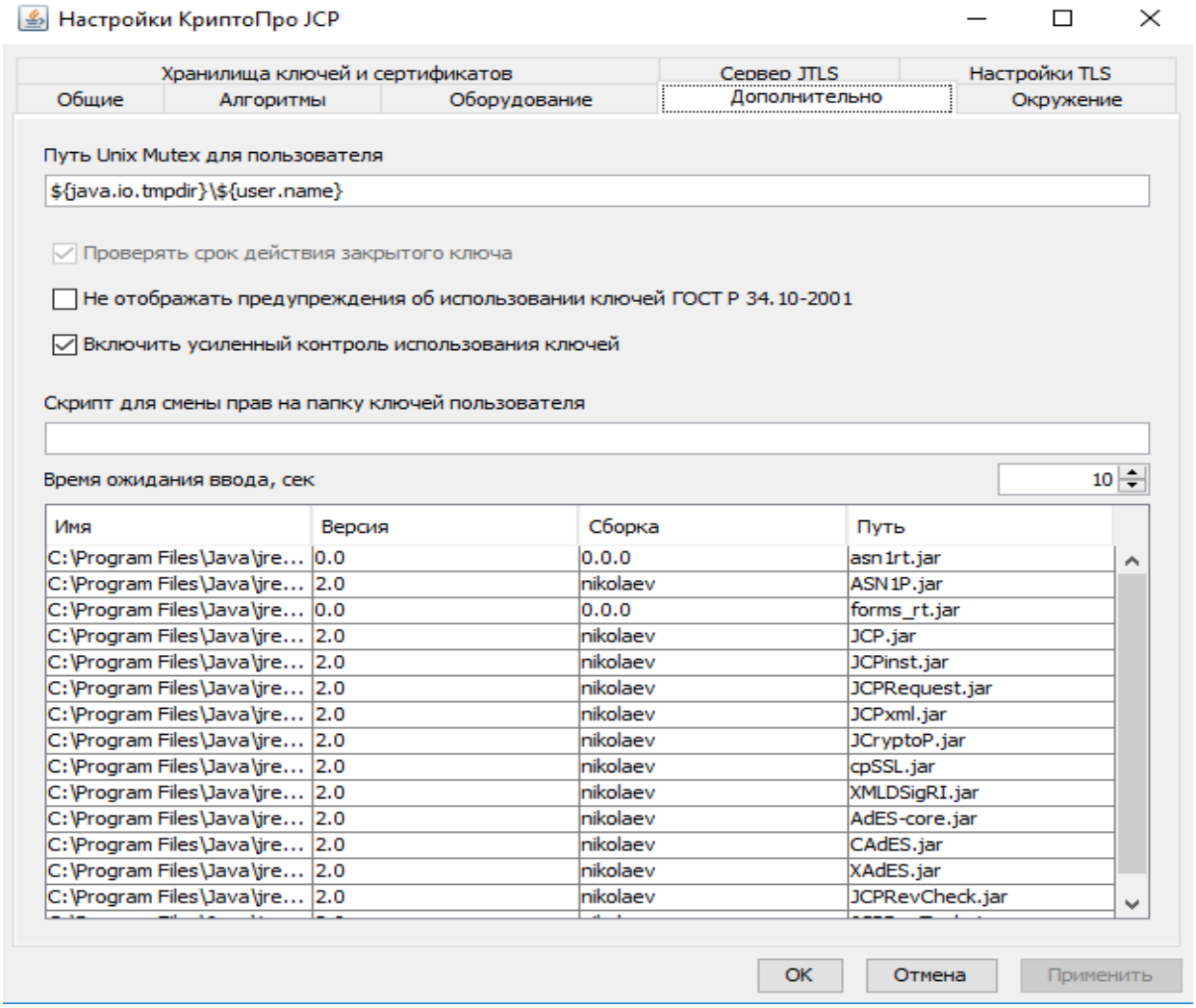

Рисунок 16. Внешний вид закладки "Дополнительно"

Закладка состоит из следующих компонентов:

•"Путь Unix Mutex для пользователей" - это поле предназначено для определения пути к файлам, используемых для синхронизации работы с общими ресурсами пользователями криптопровайдера «КриптоПро JCP» версия 2.0, а также для синхронизации между криптопровайдерами «КриптоПро JCP» версия 2.0 и КриптоПро CSP);

•"Проверять срок действия закрытого ключа" – это поле предназначено для определения необходимости проверки срока действия долговременных закрытых ключей.

•"Не отображать предупреждения об использовании ключей ГОСТ Р 34.10-2001" - это поле предназначено для определения необходимости отображения предупреждений о невозможности использования ключей ГОСТ Р 34.10-2001 для выработки электронной подписи после 31.12.2018 года.

•"Усиленный контроль использования ключей" – это поле предназначено для включения режима усиленного контроля использования ключей. **Режим должен быть в обязательном порядке включён после инсталляции СКЗИ. Использование СКЗИ при выключенном режиме разрешено исключительно в тестовых целях.**

•Скрипт для смены прав на папку ключей пользователя - это поле предназначено для определения имени скрипта, обеспечивающего пользователей конкретными правами. Необходимость данного скрипта обуславливается тем, что созданные одним пользователем закрытые ключи и ключи ЭП могут быть доступны для чтения другим пользователям (а значит, и для копирования). Ввиду требований безопасности администратор при помощи скрипта обязан запретить доступ всех пользователей к ключам электронной подписи и закрытым ключам обмена данного пользователя. При указании имени скрипта ограничения прав, к нему автоматически добавляется путь к ключам электронной подписи и закрытым ключам обмена данного пользователя.

•Время ожидания ввода, в сек - означает период отображения окна с уведомлением о чтении секретной информации с ключевого носителя в случае обращения программы к закрытому ключу с битом "user protected". По умолчанию окно отображается поверх других окон в течение 10 минут, но может быть закрыто пользователем. По истечение указанного периода оно закроется.

•Версии файлов провайдера

По умолчанию для каждого из полей определены следующие значения:

•"Путь Unix Mutex для пользователей":

○для Windows-платформ - "${java.io.tmpdir}\${user.name}";

○для Unix-платформ - "/var/cprocsp/tmp";

•"Проверять открытый ключ" - установлено;

•"Скрипт для смены прав на папку ключей пользователя"

○для Windows-платформ - скрипт отсутствует, поскольку по умолчанию путем к закрытым ключам обмена и ключам электронной подписи пользователя является "${user.home}\Local Settings\Application Data\Crypto Pro", где ${user.name} - имя текущего пользователя, а ${user.home} установлено в директорию "Documents and Settings\${user.name}". При такой настройке ${user.home}, любая подпапка этой директории ограничивает права пользователей нужным образом. Если же путь к носителю изменяется таким образом, что происходит выход за рамки этой директории, либо производится переопределение ${user.home} в отличную от "Documents and Settings\${user.name}" (где ${user.name} - имя текущего пользователя) директорию, то в этом случае в новой директории не гарантируется обеспечение необходимых прав пользователя. Поэтому при таком изменении пути к носителям в данном поле необходимо указать имя скрипта ограничения прав;

○для Unix-платформ - "chmod a-rwx,u+rwx".

4.6.Закладка "Окружение" (панель "Контроль целостности")

Панель "Контроль целостности" предназначена для контроля целостности файлов ОС средствами «КриптоПро JCP» версия 2.0. Панель оперирует "хранилищами" контрольных сумм, с ее помощью можно:

•добавлять в хранилище файлы, ставя их таким образом на контроль;

•рассчитывать для них контрольные суммы (хэши);

•проверять хэши;

•удалять файлы из хранилища, снимая их с контроля.

Кроме того, можно выбирать хранилище, по которому будет осуществляться контроль.

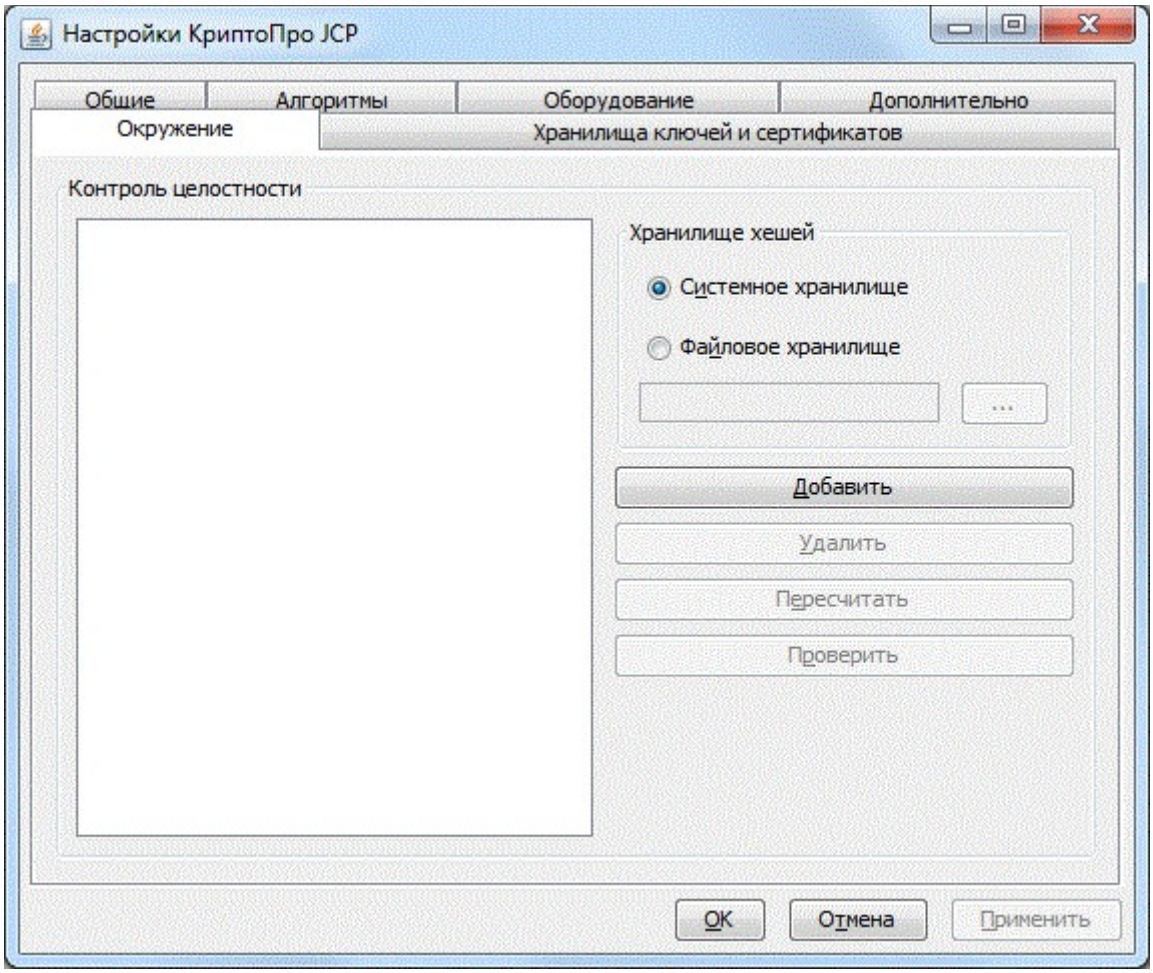

Рисунок 17. Внешний вид панели "Контроль целостности"

Панель состоит из окна, в котором отображаются контролируемые файлы, панели "Хранилище хэшей", и кнопок "Проверить", "Пересчитать", "Добавить", "Удалить".

Панель "Хранилище хэшей" состоит, в свою очередь, из переключателя между системным и файловым хранилищами.

4.6.1.Типы хранилища

Хэши файлов могут храниться в системных настройках (системное хранилище), или в файле (файловое хранилище). В случае хранения их в системных настройках не нужен никакой дополнительный выбор, система автоматически определяет их месторасположение. В случае хранения хэшей в файле, следует определить хранилище, указав имя файла, в котором будет организовано хранилище. Файл хранилища должен иметь расширение "cpv". Его можно задать, переключившись в режим файла в панели "Хранилище хэшей", и введя его имя в строке ввода, или выбрав его в раскрывающемся файловом меню. Если расширение выбранного или вновь создаваемого файла не "cpv", то оно будет заменено на "cpv". Если файл изначально не является файлом хранилища, то он будет открыт как пустое хранилище (как хранилище, у которого не сошлась контрольная сумма), но при нажатии кнопки "Применить", если были какие-то изменения, будет перезаписан, и все прежние данные в нем будут утеряны. Вновь создаваемый файл открывается как пустое хранилище.

4.6.2.Работа с хранилищем

Любое хранилище - список файлов с их контрольными суммами, в свою очередь контролируемый. Это означает, что любое хранилище может формально находиться в

одном из трех состояний: "не существовать", "существовать, но быть испорченным", и "существовать и быть исправным". Открытие хранилища происходит при старте панели или при смене хранилища внутри контрольной панели. Если хранилище, которое в настоящий момент выбрано, не существует, то в него можно только добавлять файлы (соответственно, сначала доступна только кнопка "Добавить"). После того, как в несуществующее хранилище добавлен хотя бы один файл, также становятся доступными кнопки "Пересчитать", "Проверить", "Удалить". Все они выполняют лишь виртуальные операции, и результат действий не сохраняется. Однако если после любых изменений сохранить хранилище, то будет выполнена стандартная проверка на возможность сохранения, и, в случае успеха, хранилище будет сохранено, а в противном случае будет выдано сообщение об ошибке. Если хранилище существует и повреждено, то будет выдано сообщение об ошибке, и хранилище будет открыто как несуществующее. Если хранилище исправно, то при его открытии произойдет считывание списка файлов.

Все операции с файлами в хранилище буферизуются. Это значит, что пока не нажата кнопка "Применить", хранилище изменено не будет. При нажатии кнопки "Применить" фиксируется текущее состояние текущего открытого хранилища. Состояние любых других хранилищ, в том числе и открытых раньше, не сохраняется.

•Состояние файла в хранилище

Файл в открытом хранилище может быть в одном из четырех состояний:

 - не проверялся

 - проверен, хэш сходится

 - проверялся, хэш не сходится

 - поврежден или удален

Файлы сохраняются в хранилище только в том случае, если все они находятся в состоянии "Проверен, хэш сходится".

При открытии исправного хранилища из него читаются все содержащиеся в нем файлы. Все они автоматически переходят в состояние "Не проверялся". После открытия хранилища с файлами разумно выполнить проверку целостности для всего списка файлов.

•Добавление файлов

При нажатии кнопки "Добавить" в раскрывшемся диалоге выбрать нужные файлы, и они будут добавлены в текущее хранилище. Изначально окно открывается в домашнем каталоге пользователя, но после успешного сохранения настроек в Контрольной Панели сохраняется последний каталог, из которого брались файлы, и в следующий раз диалог откроется в этом каталоге. Файлы могут быть добавлены по одному и списком.

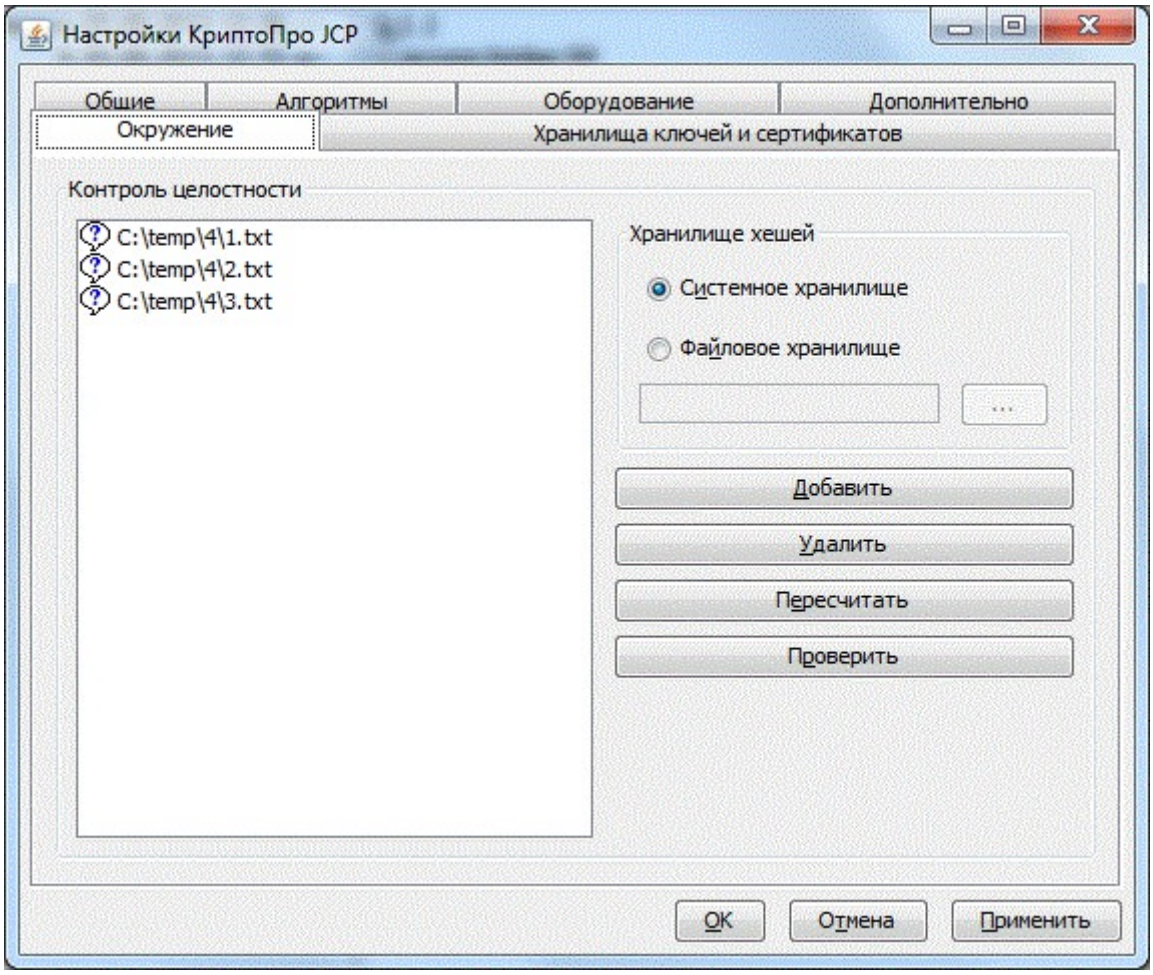

Рисунок 18. Панель "Контроль целостности". Добавление файлов

•Вычисление хэшей

Выделить файлы, лежащие в хранилище и отображенные в окне. Нажать кнопку "Пересчитать". Хэши для всех выделенных файлов будут пересчитаны. Если не выделен ни один файл, хэши будут пересчитаны для всех файлов в хранилище. После вывода сообщения об успешном пересчете хэшей все файлы, для которых хэши были подсчитаны заново, изменят свое состояние на " Проверен, хэш сходится ".

•Проверка целостности

Выделить файлы, лежащие в хранилище и отображенные в окне. Нажать кнопку "Проверить". Будут проверены все выделенные файлы, а если не был выделен ни один, будут проверены все файлы, находящиеся в хранилище.

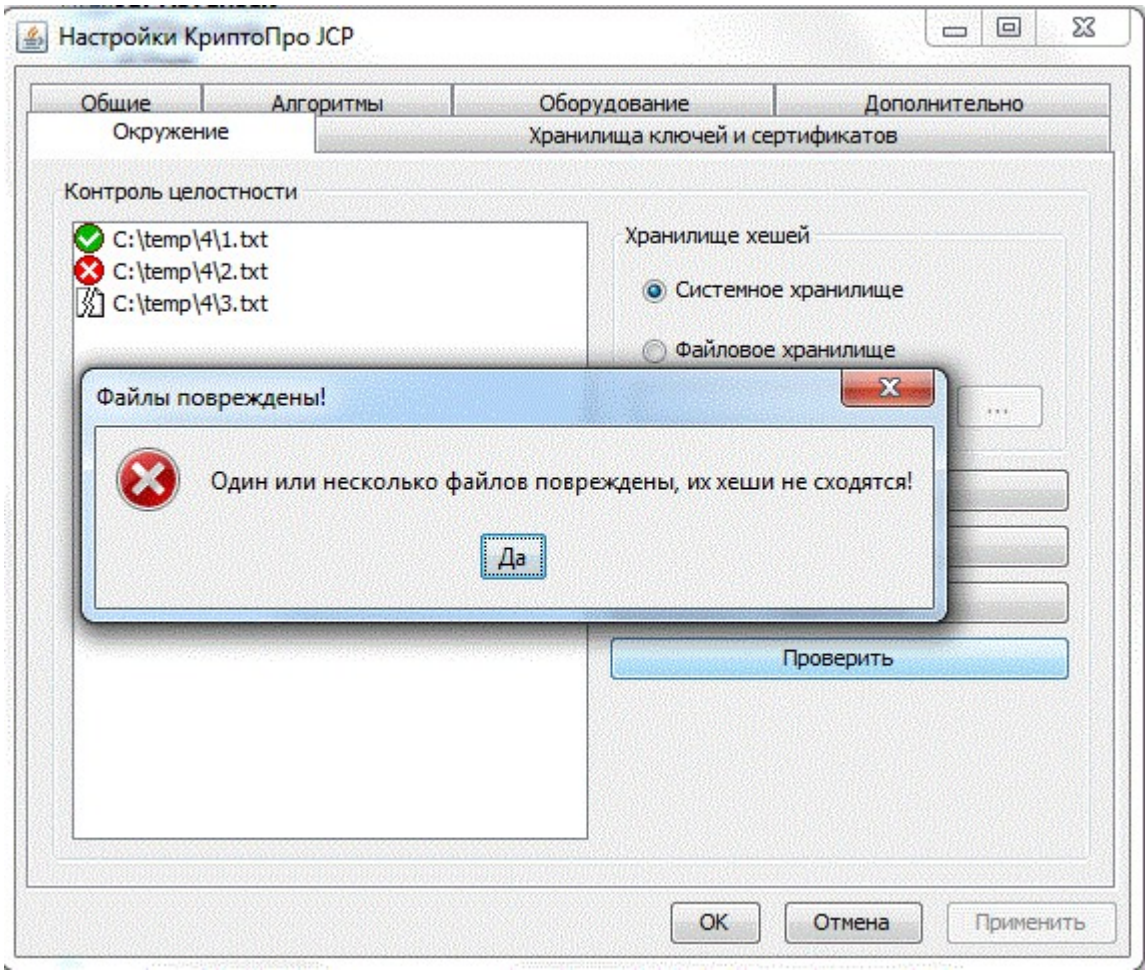

Рисунок 19. Панель "Контроль целостности". Нарушение целостности файлов

•Удаление файлов

Выделить файлы, лежащие в хранилище и отображенные в окне. Нажать кнопку "Удалить". Выделенные файлы будут удалены из хранилища.

•Сохранение состояния

Сохранение состояние панели (сохранение хранилища, и сохранения текущего хранилища, при наличии изменений) происходит при нажатии кнопки "Применить" или кнопки "ОК". В любом другом случае сохранения состояния панели не происходит. Исключение составляют текущие каталоги для диалогов добавления файлов в хранилище и выбора хранилища, которые сохраняются после каждого закрытия соответствующего диалога.

4.6.3.Права на работы с панелью "Контроль целостности"

Установки панели, такие как текущие каталоги для добавляемых в хранилище файлов и для файловых хранилищ, сохраняются в настройках пользователя. Выбранное в настоящий момент на данном компьютере хранилище описано в системных настройках. Прочитать выбранное хранилище может пользователь, которому системные настройки доступны для чтения. Изменить выбор хранилища может пользователь, которому системные настройки доступны для записи. Если пользователь не может задать хранилище, соответствующий переключатель погашен.

У любого хранилища также есть права на чтение и запись для каждого пользователя. Они совпадают с правами пользователя для файла хранилища, или для системных настроек, если в качестве хранилища выбраны они. Создав хранилище из-под одного пользователя, следует также установить возможность чтения этого хранилища для всех других пользователей, кто может работать с контрольной панелью.

В случае, если пользователь не может ни писать в текущее (существующее) хранилище, ни читать из него, погашены кнопки "Добавить", "Удалить", "Проверить",

"Пересчитать" (то же, если текущим оказалось несуществующее хранилище). Если пользователь имеет права на чтение хранилища, погашены все кнопки, кроме "Проверить". Если пользователь имеет права на запись в хранилище, все четыре кнопки доступны.

4.6.4.Начальные установки

Изначально установлено хранилище в системных настройках, список файлов в нем пуст. При открытии файлового диалога для выбора нового хранилища или для добавления файлов, они откроются в домашнем каталоге пользователя.

При открытии ранее уже использованной панели, будет выведено последнее установленное хранилище, и в окне файлов будут отображены все содержащиеся в хранилище файлы со знаком "Не проверялся".

4.7.Закладка "Хранилища ключей и сертификатов"

Панель "Хранилища ключей и сертификатов" предназначена для просмотра хранилищ ключей, установленных в системе, просмотра и управления контейнерами в хранилищах.

С помощью панели можно:

•копировать, просматривать, создавать и удалять контейнеры в хранилище;

•копировать и просматривать сертификаты в хранилищах и в контейнерах, добавлять сертификаты из файлов и контейнеров в хранилище сертификатов и удалять их из него;

•изменять пароли на хранилищах и контейнерах.

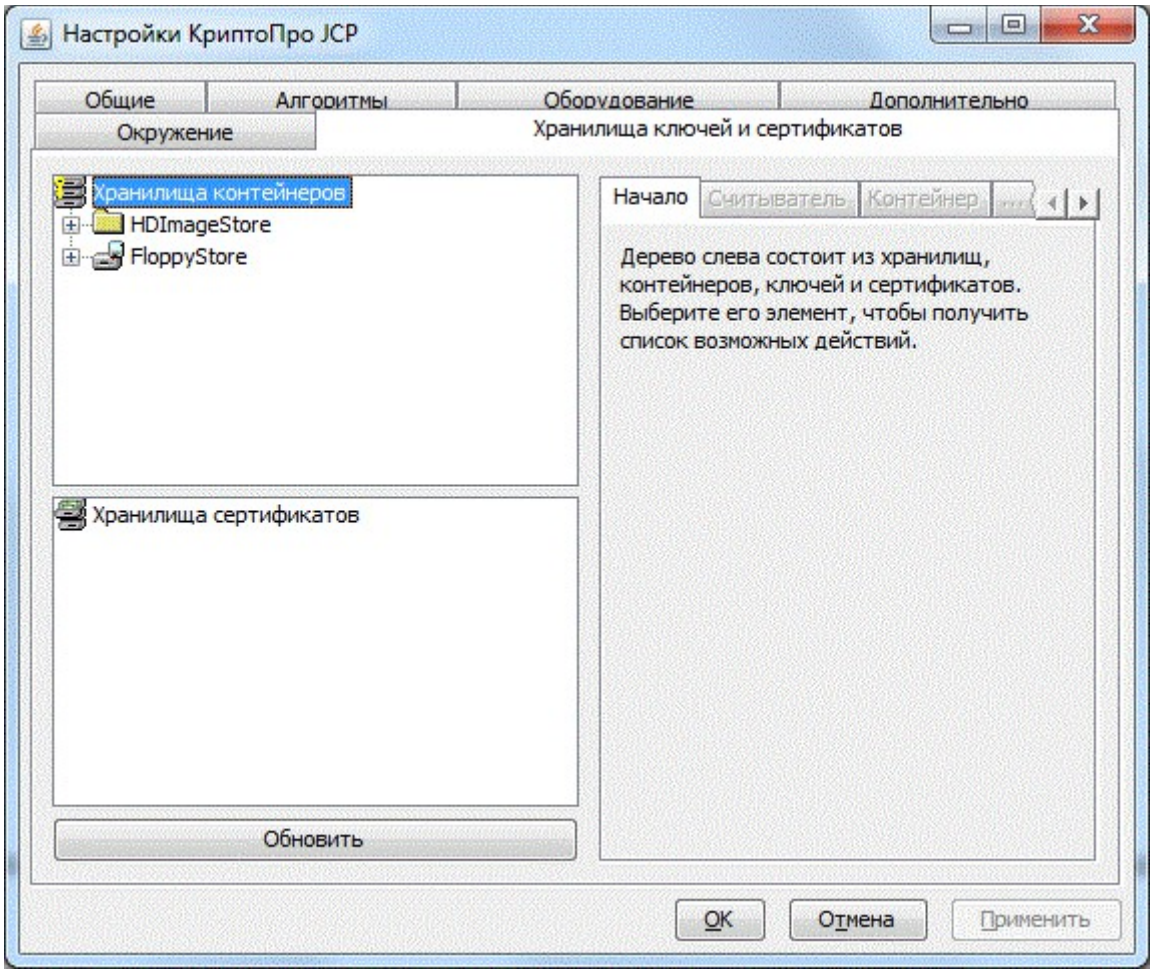

Рисунок 20. Внешний вид панели "Хранилища ключей и сертификатов"

Панель состоит из окна просмотра дерева хранилищ контейнеров, окна просмотра дерева хранилищ сертификатов, кнопок управления хранилищами и кнопок управления объектами в хранилищах.

4.7.1.Работа с хранилищами

При открытии панели дерево хранилищ и контейнеров находится в свернутом состоянии, показаны только хранилища, установленные в системе. Двойной щелчок мыши или нажатие "Ввод" на любом их хранилищ проинициализирует попытку открытия данного хранилища. В этом случае:

•если выбрано хранилище контейнеров, на котором не может быть установлен пароль, хранилище будет открыто;

•если выбрано хранилище сертификатов появится окно ввода пароля для хранилища.

Если во время открытия хранилища произошла ошибка, сообщение о ней будет выдано на экран.

При установке курсора на любой элемент дерева, автоматически переключающиеся закладки справа, покажет закладку с соответствующими кнопками для выполнения операций над данным объектом.

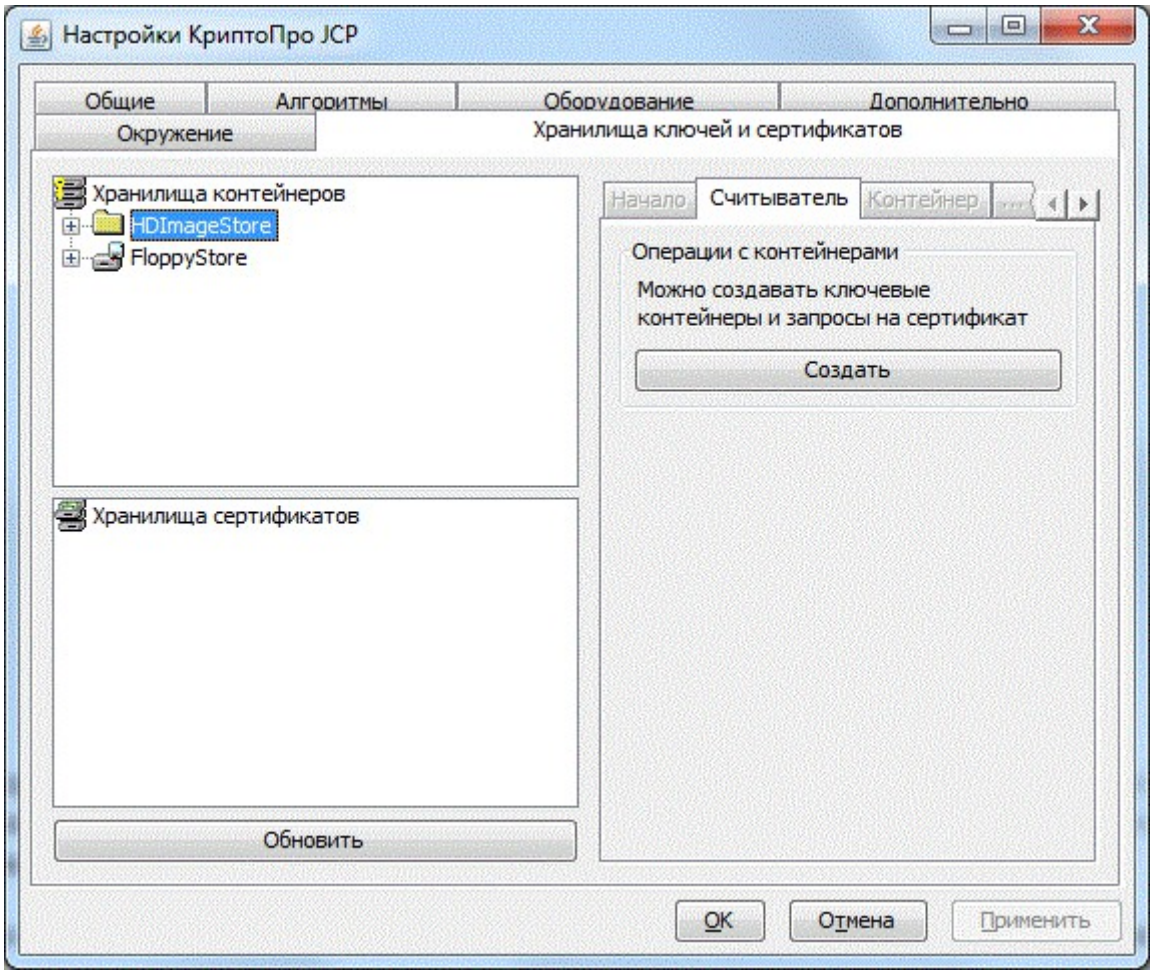

Рисунок 21. Панель "Хранилища ключей и сертификатов". Выбор хранилища контейнеров

В хранилище в общем случае хранятся алиасы - контейнеры (в хранилищах контейнеров) либо сертификаты (в хранилищах сертификатов). Содержимое любого контейнера можно просмотреть, с помощью двойного клика мыши и нажатия "Ввод" на нем. При этом раскроется окно ввода пароля для контейнера. Если введен правильный пароль, контейнер будет раскрыт и его содержимое (набор сертификатов и ключ) будет отображено как листья в дереве. Если же пароль неправильный, или произошла какая-то ошибка чтения контейнера, будет выведен единственный лист: "Контейнер не открывался".

Будь то контейнер или хранилище, в случае, если для него выведен лист "... не открывался", после схлопывания дерева в его ветке и повторного двойного клика на листе будет произведена очередная попытка открытия.

Успешно открытое хранилище или контейнер не надо открывать заново в случае схлопывания ветки дерева. Также и после успешно завершенных операций, требующих открытия хранилища или контейнера (изменение пароля, копирование), заново их открывать не нужно.

4.7.2.Создание контейнера. Работа с контейнером.

При установке указателя на одно из хранилищ контейнеров доступно действие "Создать" контейнер.

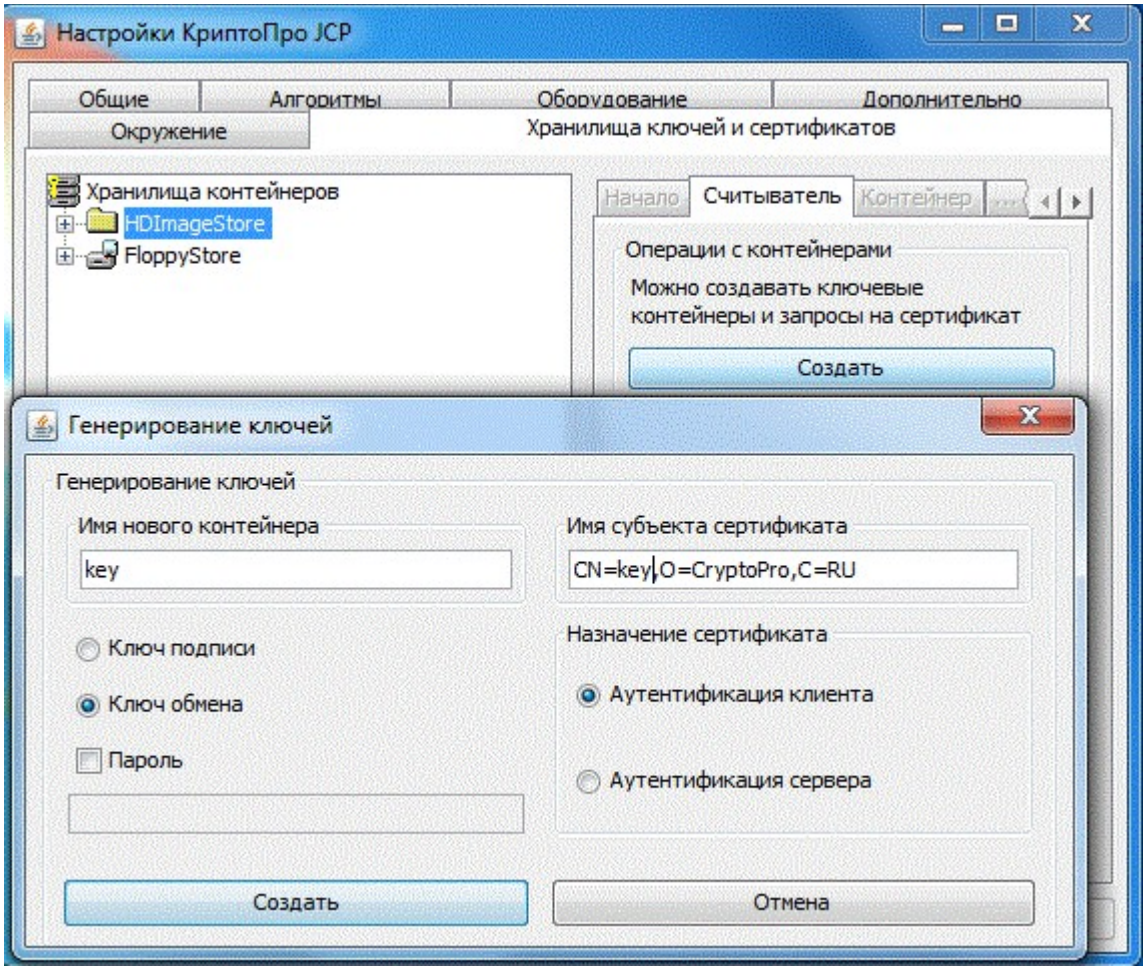

Рисунок 22. Панель "Хранилища ключей и сертификатов". Создание контейнера

Данная реализация позволяет получить ключ электронной подписи или обмена с самоподписанным сертификатом (для аутентификации сервера или клиента (выбор справа)). Также указываются имя нового контейнера и имя субъекта сертификата. При совпадении имени создаваемого контейнера с именем уже существующего в хранилище контейнера будет выведено сообщение о перезаписи или отмене. Ключ можно сохранить без пароля или с паролем. Для сохранения ключа с паролем необходимо выбрать флаг "Пароль" и в соответствующее поле ввести пароль. Дополнительно можно выбрать тип провайдера. При нажатии кнопки "Создать" будет сгенерирован ключ и сертификат, и контейнер с указанным именем и паролем будет записан в текущее хранилище.

Если создается ключ обмена, то перед созданием контейнера убедитесь, что провайдер Crypto установлен, т.к. для данного случая генерации ключа происходит по алгоритму Диффи-Хелмана (ключ подходит как для обмена, так и для подписи). Если провайдер Crypto не установлен, появится сообщение об ошибке "Провайдер Crypto не найден".

После данных операций появится окно диалога сохранения запроса на сертификат.

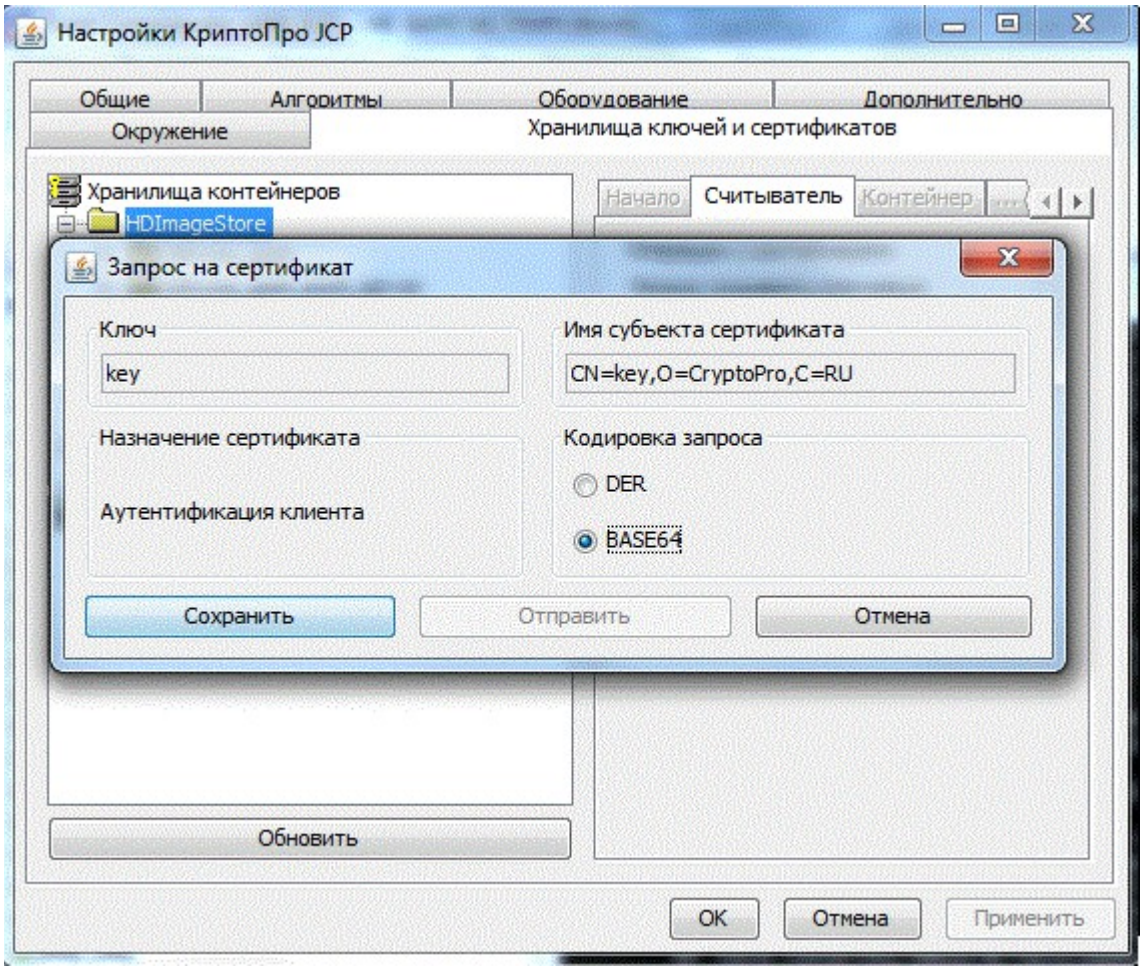

Рисунок 23. Панель "Хранилища ключей и сертификатов". Сохранение запроса на сертификат после генерации ключа

Сохраненный запрос можно использовать для получения сертификата на УЦ.

Полученный на УЦ и сохраненный в файл сертификат можно уложить в соответствующий контейнер установив на нем указатель и нажав кнопку "Добавить", в появившейся закладке операций для объекта контейнер). При выполнении данного действия осуществляется перезапись сертификата в контейнере. В контейнер можно также добавлять цепочку сертификатов (из файла *.p7b).

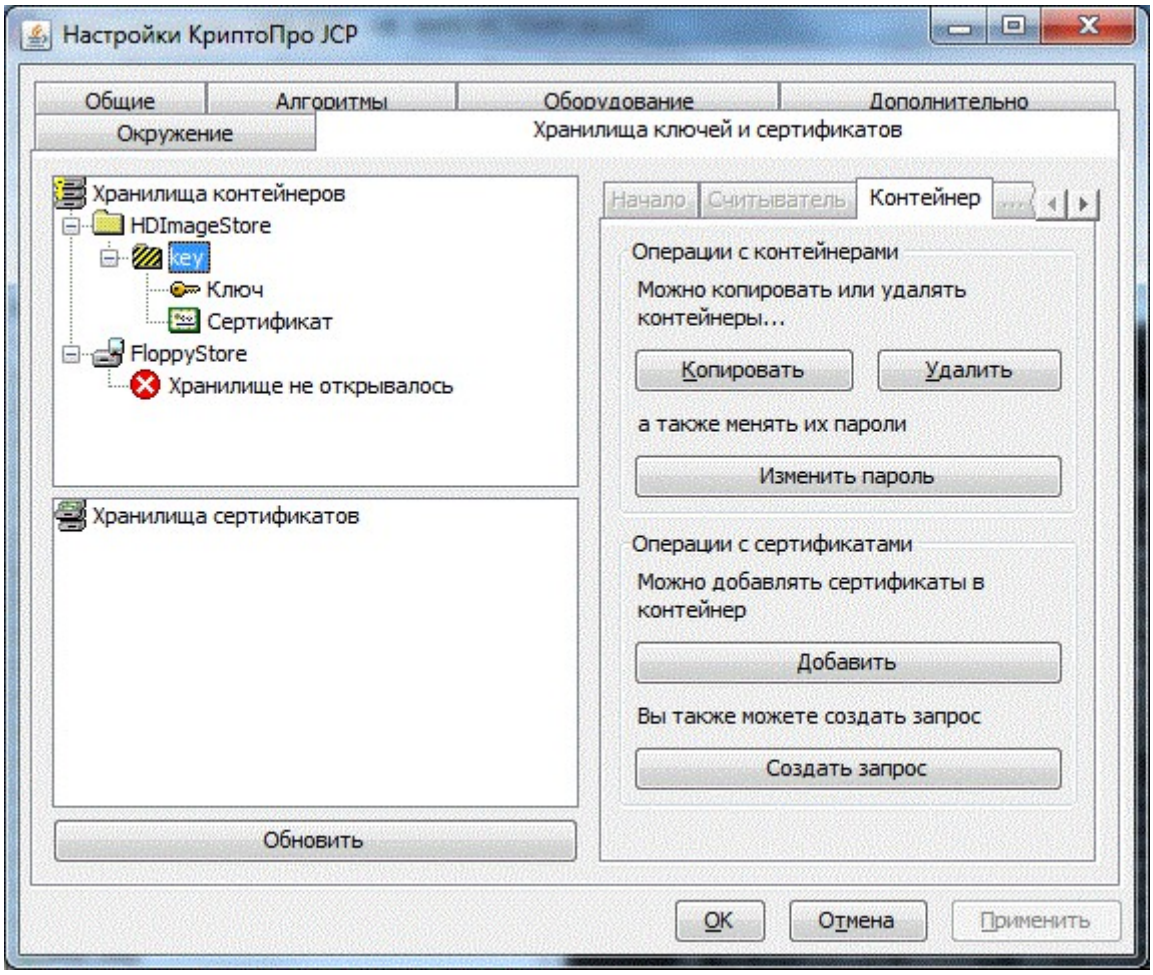

Рисунок 24. Панель "Хранилища ключей и сертификатов". Открытие контейнера

Также становятся доступны следующие операции с контейнером:

- копирование;
- удаление;
- изменение пароля;
- установка сертификата (-ов) в контейнер;
- создание в контейнере нового запроса на сертификат взамен имеющегося внутри сертификата (-ов).

При установке указателя на ключ в контейнере, будет выведена информация о ключе.

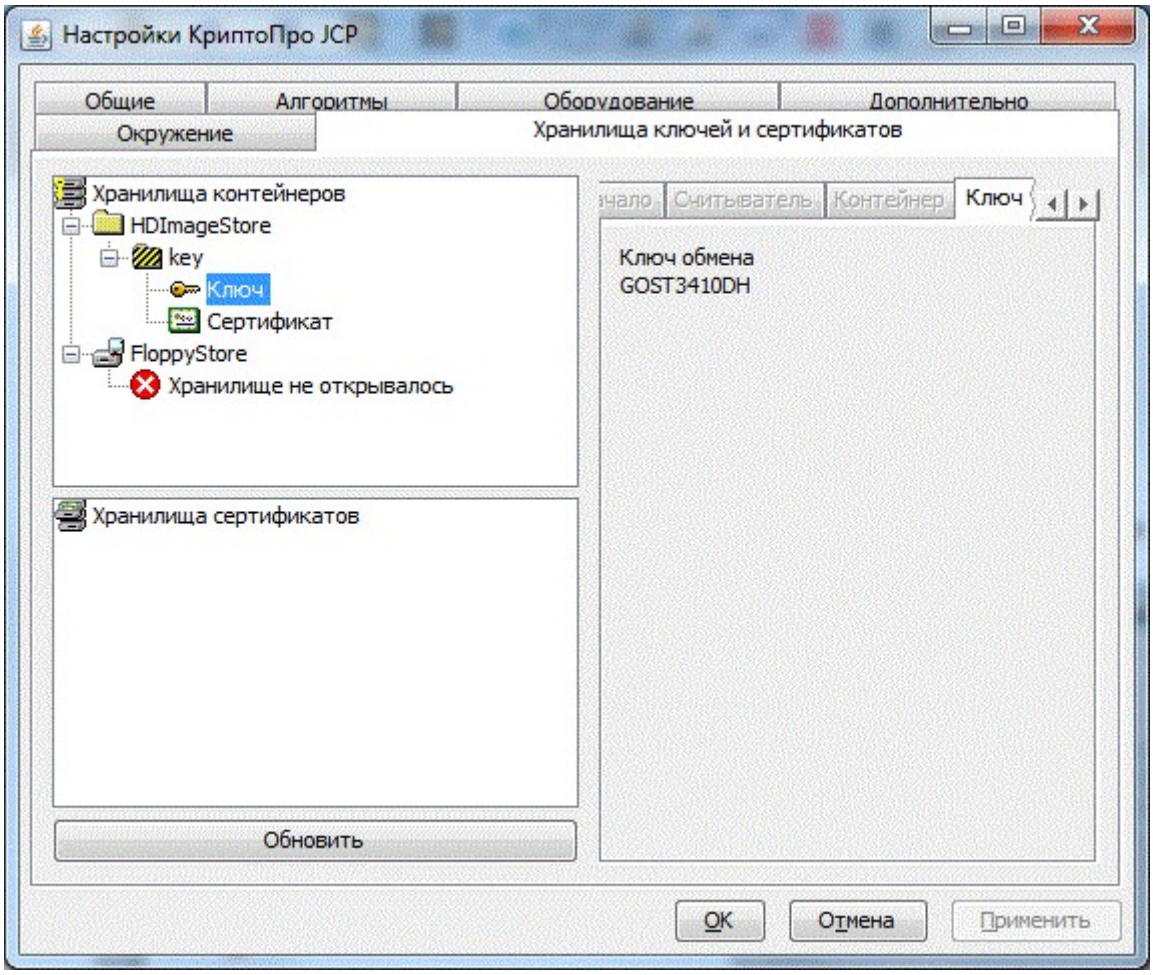

Рисунок 25. Панель "Хранилища ключей и сертификатов". Выбор ключа

При установке указателя на сертификат в контейнере будут доступны операции просмотра и копирования. Кнопка "Построить" позволяет осуществить поиск цепочки для данного сертификата (в выбранном хранилище сертификатов).

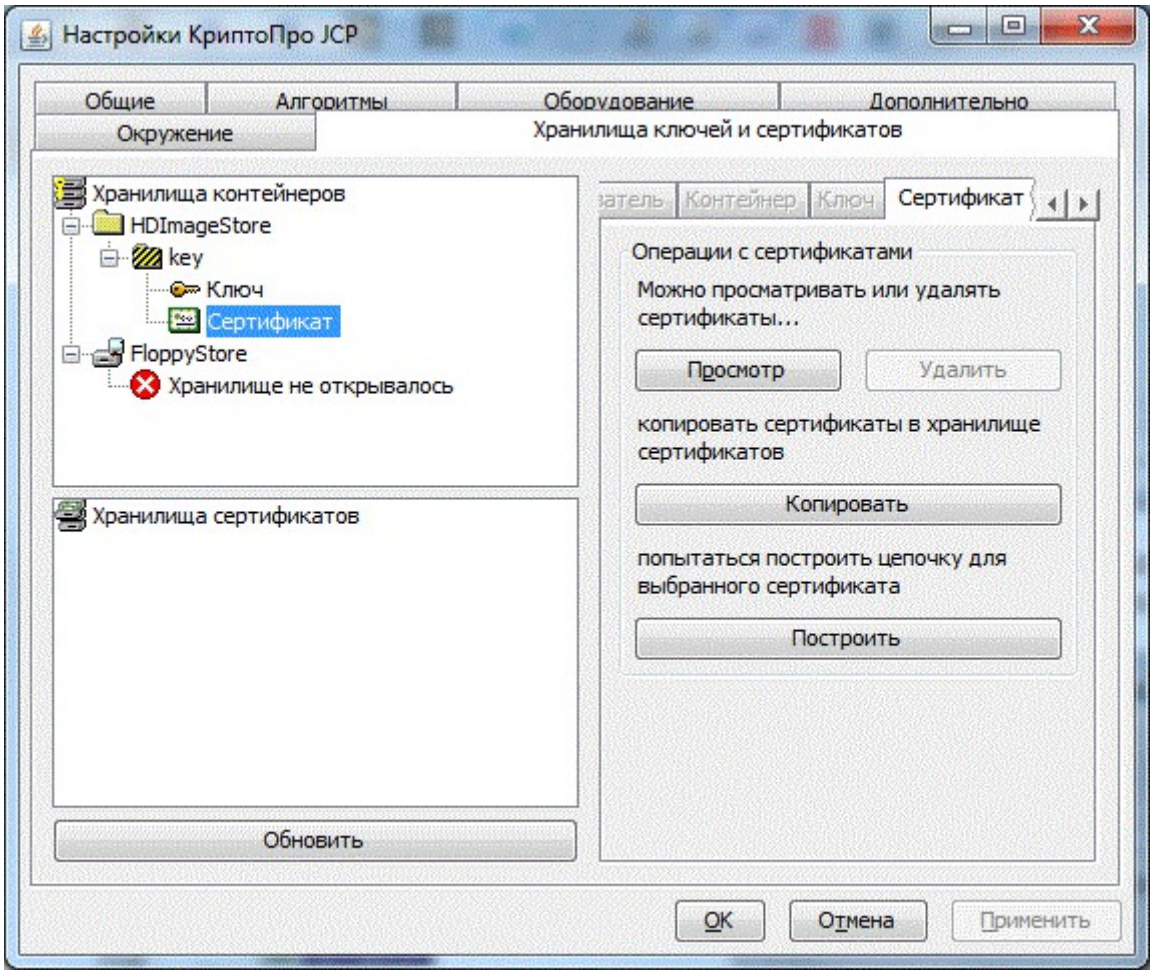

Рисунок 26. Панель "Хранилища ключей и сертификатов". Выбор сертификата

Чтобы открыть или создать новое хранилище сертификатов следует установить указатель на корневой элемент дерева хранилищ сертификатов. После нажатия кнопки "Найти / Создать" появится окно диалога открытия (создания) хранилища.

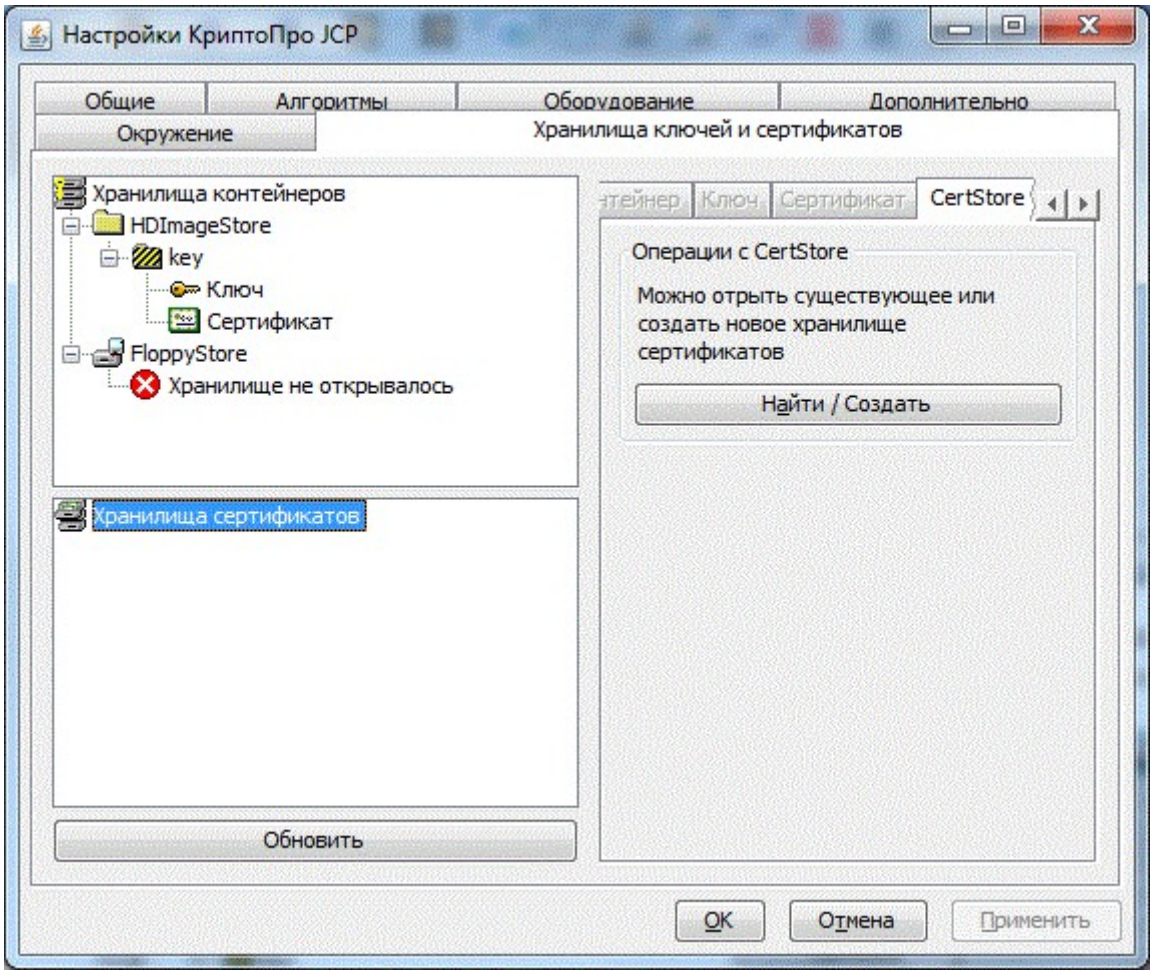

Рисунок 27. Панель "Хранилища ключей и сертификатов". Выбор хранилищ сертификатов

После открытия(создания) хранилища сертификатов в дереве появится соответствующий лист.

При установлении указателя на хранилище сертификатов становятся доступны следующие операции:

•Добавить

добавление сертификатов в хранилище из файлов

•Изменить пароль

•Убрать

удаление данного хранилище из списка отображения (файл хранилища не удаляется)

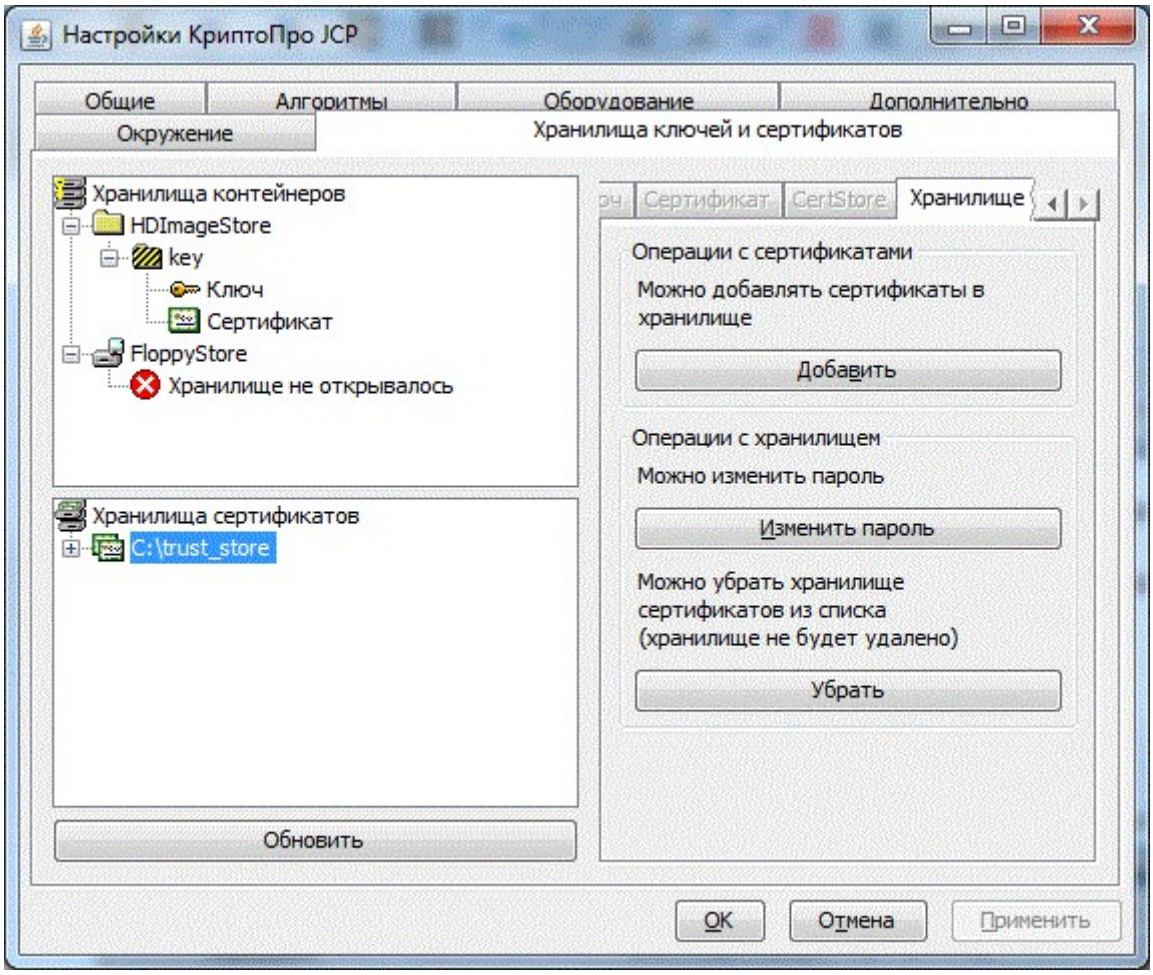

Рисунок 28. Панель "Хранилища ключей и сертификатов". Выбор хранилища сертификатов

При установке указателя на сертификат в хранилище сертификатов доступны операции просмотра, копирования и удаления сертификата из данного хранилища. Кнопка "Построить" позволяет осуществить поиск цепочки для данного сертификата (в выбранном хранилище сертификатов).

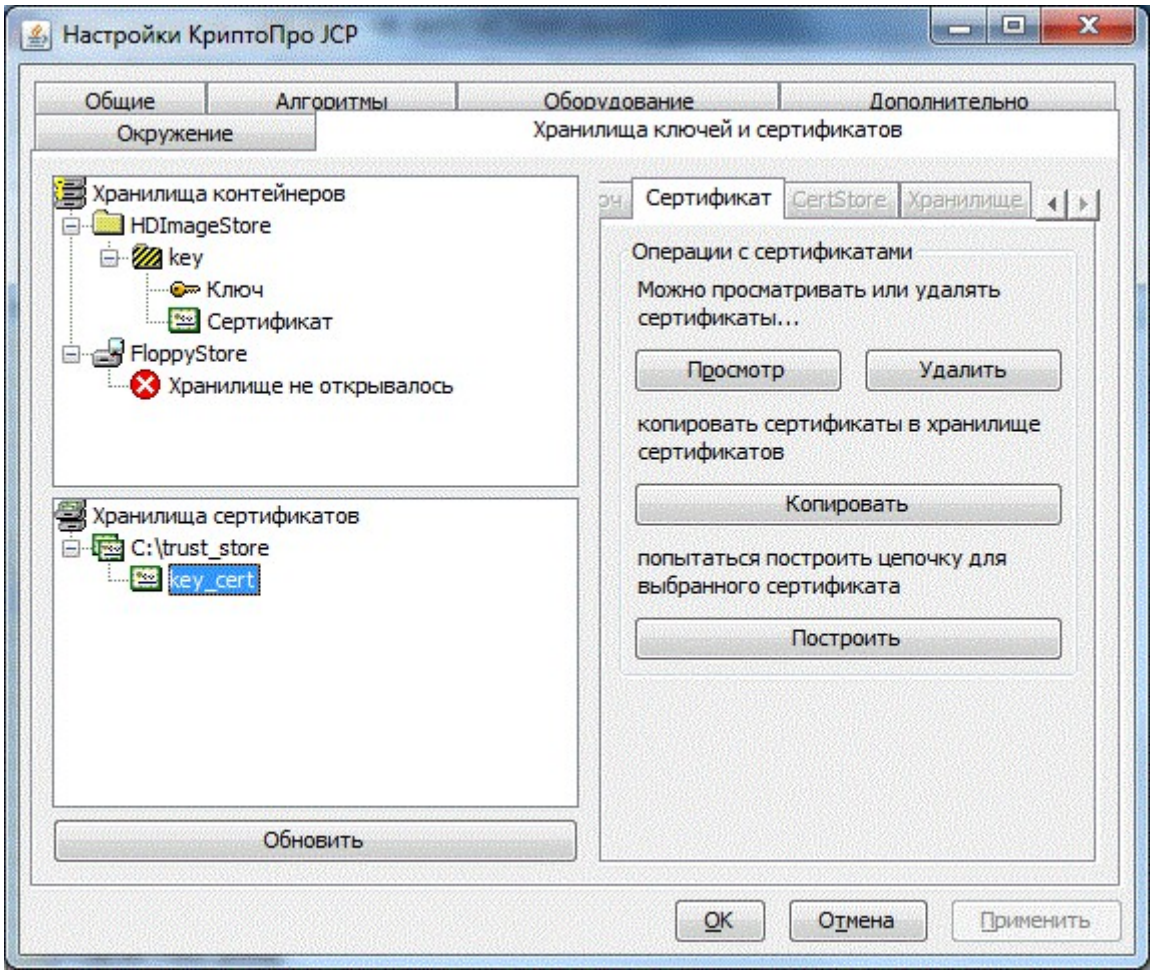

Рисунок 29. Панель "Хранилища ключей и сертификатов". Просмотр сертификата

4.7.3.Просмотр сертификатов

Сертификаты могут хранится в контейнерах и в файловой части хранилища - хранилище сертификатов. В любом случае к ним может быть применена операция "просмотреть сертификат" (кнопка "Просмотр"). Для сертификата будет выведено окно просмотра с тремя закладками: "Общая информация", "Подробно" и "Путь". Первая закладка содержит общую информацию о сертификате: действителен ли он, срок его действия, имя издателя и владельца.

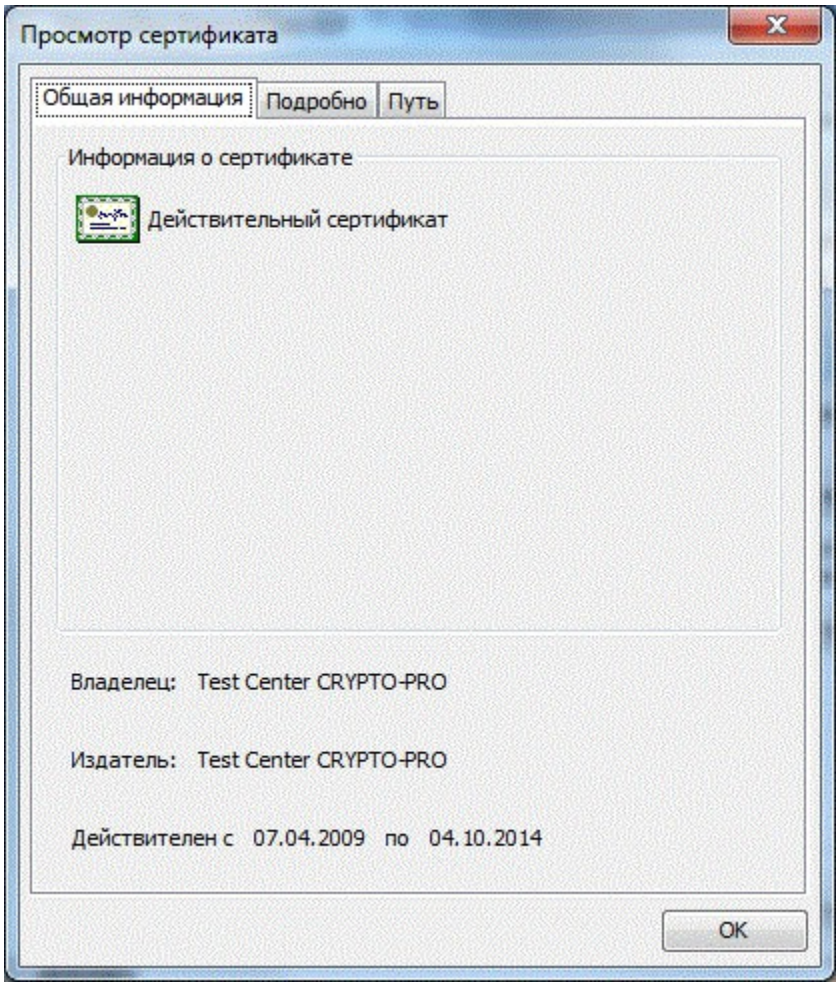

Рисунок 30. Внешний вид окна "Просмотр сертификата"

Вторая закладка содержит информацию о большинстве полей сертификата, представленных в виде списка, каждая строка которого - пара "Имя поля":"Значение поля".

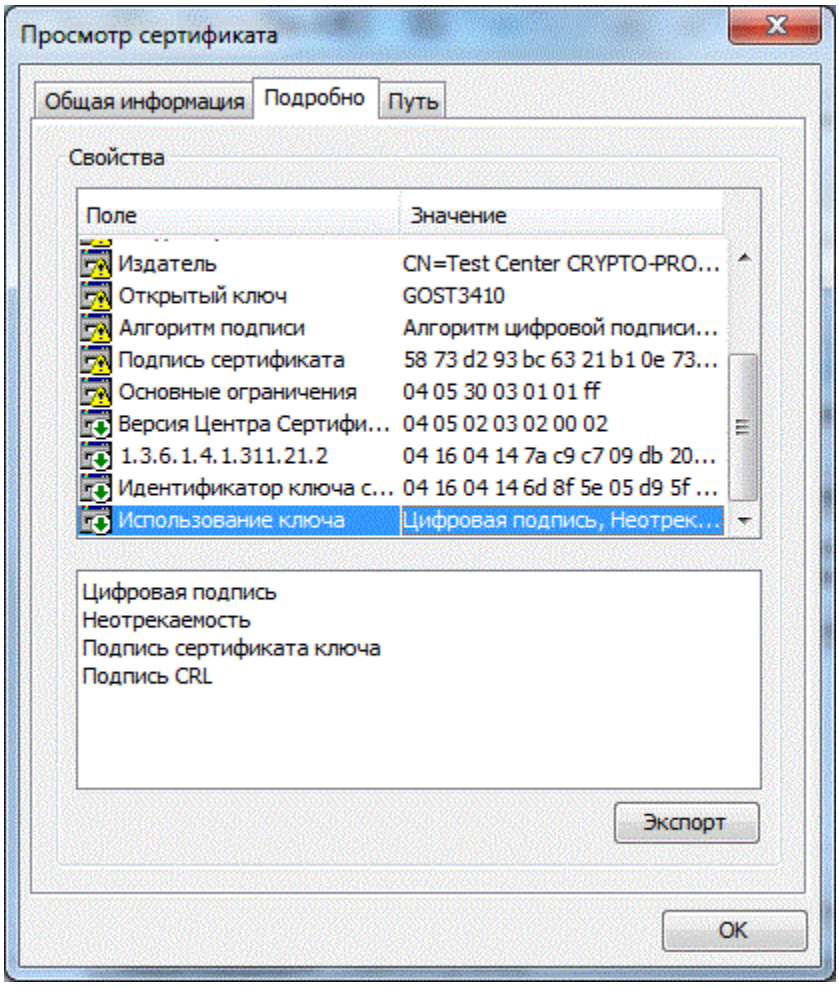

Рисунок 31. Окно "Просмотр сертификата". Подробное описание сертификата

С помощью кнопки "Просмотр" можно также просматривать цепочки и наборы сертификатов, хранящиеся вместе с ключами в контейнерах. Перед просмотром производится попытка построить цепочку из набора сертификатов контейнера, и, если это удалось, набор сертификатов выводится в третьей вкладке окна просмотра в виде дерева. В противном случае в третьей вкладке выводится набор сертификатов в виде списка. В любом случае в первых двух вкладках отображается информация для конечного сертификата (сертификата ключа). На третьей же вкладке есть возможно просмотреть полную информацию о любом из сертификатов в наборе, кроме конечного, выбрав его в окне и нажав кнопку "Просмотр".

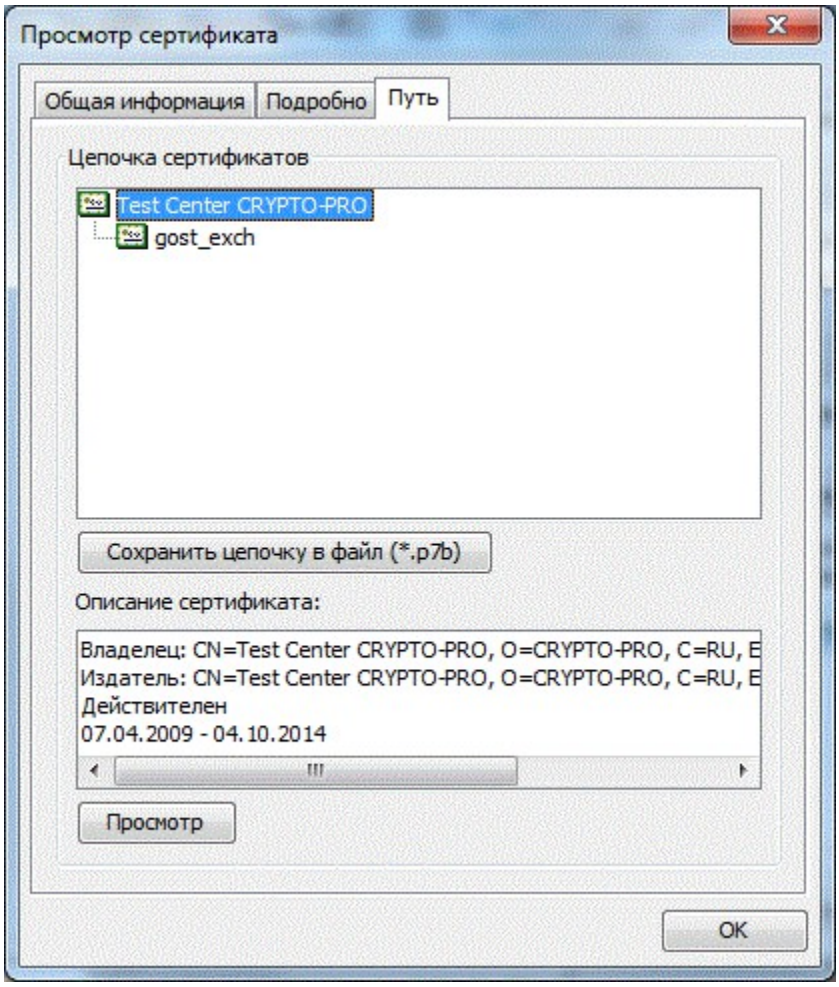

Рисунок 32. Окно "Просмотр сертификата". Цепочка сертификатов

Цепочку можно сохранить в файл формата CMS (*.p7b). Закрывается окно просмотра сертификатов по кнопке "Ок", или при нажатии "Esc", или при нажатии на кнопку закрытия в углу окна.

4.7.4.Копирование, удаление объектов и смена пароля

Операция копирования применима к контейнерам и сертификатам. Контейнеры, содержащие экспортируемый ключ, можно копировать из одного хранилища в другое, а также копировать в то же хранилище (переименование). Сертификаты можно копировать только в файловое хранилище (хранилище сертификатов), но безразлично - из контейнера или из хранилища сертификатов. При нажатии кнопки "копировать", когда выбран контейнер, сначала производится его открытие, потом выводится окно "Выбор хранилища", после выбора хранилища назначения задаются новое имя контейнера в хранилище и его пароль. Затем производится копирование.

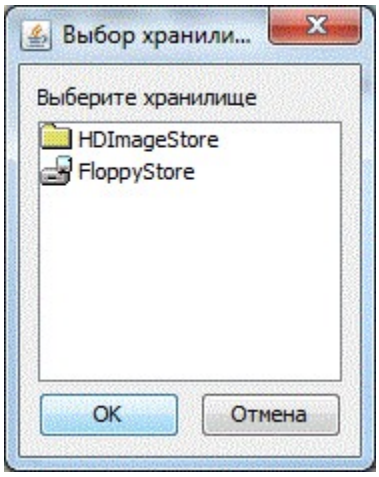

Рисунок 33. Внешний вид окна "Выбор хранилища контейнеров" при копировании контейнера

Для сертификата копирование осуществляется в том же порядке, что и для контейнера, однако не запрашиваются старый и новый пароль.

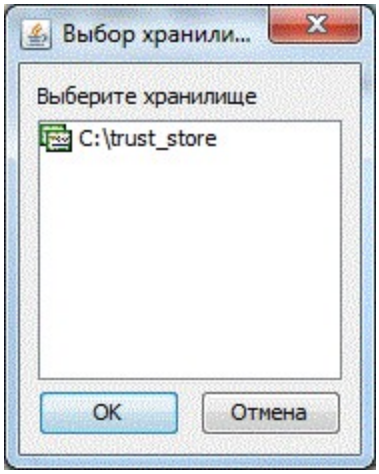

Рисунок 34. Внешний вид окна "Выбор хранилища сертификатов" при построении цепочки

Операция удаления объекта применима к любому алиасу - сертификату или контейнеру в хранилище. Выполняется по кнопке "Удалить".

Операция изменения пароля применима к файловой части хранилища - хранилищу сертификатов, и к контейнерам. При смене пароля происходит перезапись объекта с тем же именем, но с другим паролем, соответственно, чтобы изменить пароль на контейнере, необходимо, чтобы он содержал экспортируемый ключ.

Операция смены пароля состоит из открытия объекта (для этого потребуется старый пароль) и ввода нового пароля с подтверждением.

5.Литература

1.[РФ.Защита]. Закон РФ № 24-ФЗ от 20.02.95 г. "Об информации, информатизации и защите информации".

2.[РФ.ГосТайна]. Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне".

3.[РФ.Безопасность]. Закон РФ № 2446-1 от 05.03.92 г. "О безопасности".

4.[РФ.Связь]. Закон РФ № 15-ФЗ от 16.02.95 г. "О связи".

5.[РФ.Серификация]. Закон РФ № 5151-1 от 10.06.93 г. "О сертификации продукции и услуг".

6.[РФ.Стандартизация]. Закон РФ № 5154-1, 1993 г. "О стандартизации".

7.[РФ.Изменения]. Закон РФ № 4871-1, 1993 г. "Об обеспечении единства измерений".

8.[РФ.Органы связи]. Закон РФ № 4524-1 от 19.02.93 г. "О федеральных органах правительственной связи и информации".

9.[РФ.ГК]. Гражданский кодекс Российской Федерации. Ч. 1. Принят Государственной Думой 21 октября 1994 г. Одобрен Советом Федерации.

10.[ГОСТ 34003]. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

11.[ГОСТ 28147]. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

12.[ГОСТ 341001]. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

13.[ГОСТ 3411]. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

14.[ГОСТ 50739]. ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

15.[ГОСТ 1]. ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.

16.[ГОСТ 16487]. ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.

17.[ГОСТ 50922]. ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.

18.[Лицензирование]. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г.

19.[ГТК Термины]. Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.

20.[ГТК защита]. Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.

21.[ГТК НСД]. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Москва, 1992 г.

22.[ГТК Классификация]. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.

23.[ГТК Показатели]. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.

24.[Халянин]. Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.

25.[Бияшев]. Бияшев Р.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации / Зарубежная радиоэлектроника. 1989. № 12. С. 76-91.

26.[Словарь]. Толковый словарь по информатике. - М.: Финансы и статистика, 1991.

27.[Терминология]. Терминология в области защиты информации: Справочник / ВНИИстандарт, 1993.

28.[Формуляр]. ЖТЯИ.00091-01 30 01. КриптоПро JCP. Формуляр.

29.ЖТЯИ.00091-01 33 01. КриптоПро JCP. Руководство программиста.

30.ЖТЯИ.00009-01 30 01. Удостоверяющий центр "КриптоПро УЦ". Формуляр.

31.[X.680-X.699]. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)

32.[X.509]. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

33.[PKIX]. RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

34.[ПКЗ-2005]. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

35.Джим Яворски, Пол Дж. Перроун. "Система безопасности Java 2 Руководство разработчика." М. Издательский дом "Вильямс", 2001 ISBN 5-8459-0165-0 (рус)