

127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
<https://CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство

Криптографической

Защиты

Информации

КриптоПро JCP

Версия 2.0 R4

Инструкция по использованию

ЖТЯИ.00091-04 91 01
Листов 63

© ООО «КРИПТО-ПРО», 2000-2020. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро JCP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро JCP версии 2.0 R4; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

Список сокращений	5
1 Установка и удаление СКЗИ	6
1.1 Особенности установки	6
1.2 Кодировки в Java	7
1.3 Установка и удаление на Windows	7
1.3.1 Установка/удаление с помощью графического инсталлятора	8
1.3.2 Установка с помощью командной строки	14
1.4 Установка на UNIX и Mac OS	15
1.5 Локальная установка вызовом Java	16
1.6 Установка дополнительных пакетов	19
1.7 Проверка и ввод лицензии	20
1.8 Установка модулей поддержки ключевых носителей	22
1.8.1 Установка модуля поддержки JaCarta для носителей Аладдин Р.Д.	22
1.8.2 Установка/настройка модуля поддержки ESMART	23
1.8.3 Установка/настройка модуля поддержки Rutoken	26
2 Настройка СКЗИ	28
2.1 Политики безопасности	28
2.1.1 Права доступа для JCP.jar	28
2.1.2 Права доступа для администратора JCP	29
2.1.3 Права доступа для приложений	29
2.1.4 Права доступа пользователя	29
2.2 Особенности работы СКЗИ в консольном режиме	29
3 Контрольная панель КриптоПро JCP	31
3.1 Общие параметры СКЗИ (вкладка JCP)	32
3.2 Настройка параметров криптографических алгоритмов (вкладка Алгоритмы)	32
3.3 Определение путей к хранилищам ключей (вкладка Оборудование)	33
3.4 Настройка параметров безопасности (вкладка Дополнительно)	34
3.5 Контроль целостности файлов (вкладка Окружение)	35
3.6 Управление хранилищами ключевых контейнеров и сертификатов (вкладка Хранилища ключей и сертификатов)	40
3.6.1 Работа с хранилищем контейнеров	42
3.6.2 Создание контейнера. Работа с контейнером	43
3.6.3 Работа с хранилищем сертификатов	48
3.6.4 Работа с сертификатами в хранилище	50
3.6.5 Копирование, удаление объектов и смена пароля	52
4 Настройка параметров провайдера с помощью Preferences	55
5 Использование утилиты ComLine	57
5.1 Проверка установки и настроек провайдеров	57
5.2 Проверка работоспособности провайдеров	57
5.3 Работа с ключами и сертификатами	58
5.3.1 Генерация ключевой пары и соответствующего ей самоподписанного сертификата. Запись их на носитель. Генерация запроса на сертификат и запись его в файл.	58
5.3.2 Получение сертификата из запроса. Запись сертификата в хранилище и в файл	58
5.3.3 Построение цепочки сертификатов	59

5.3.4	Формирование электронной подписи	59
5.3.5	Проверка электронной подписи	60
5.4	Использование КриптоПро JavaTLS	60
5.4.1	Запуск сервера из командной строки	60
5.4.2	Запуск клиента из командной строки	61
5.4.3	Запуск клиента нагрозочного примера из командной строки	61
5.4.4	Запуск клиента на основе apache http client 4.x из командной строки	62

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
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 или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФК	Среда функционирования комплекса
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

Аннотация

Настоящая инструкция содержит описание процесса установки СКЗИ КриптоПро JCP версии 2.0 R4, интерфейса контрольной панели СКЗИ, настройки параметров провайдера, а также использования утилиты Comline.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро JCP версии 2.0 R4, должны разрабатываться с учетом требований настоящей Инструкции.

1 Установка и удаление СКЗИ

1.1 Особенности установки

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JCP в случае эксплуатации ПО в ОС Windows/*nix не требуется.

Эксплуатация осуществляется путем добавления провайдеров в список java.security:

```
security.provider.<N>=JCSP
security.provider.<N>=Crypto
security.provider.<N>=RevCheck
```

Библиотеки должны быть добавлены в classpath.

В случае использования Java-машин версии 1.7 или 1.8:

Для установки КриптоПро JCP на ПЭВМ с установленной Java-машиной версии 1.7 или 1.8 следуйте инструкции, описанной в соответствующем используемой ОС разделе.

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

Перед установкой КриптоПро JCP необходимо предварительно удалить предыдущую версию продукта.

Для установки КриптоПро JCP Вы должны иметь права администратора на данной рабочей станции.



Примечание. При работе с КриптоПро JCP в обязательном порядке должен быть включен режим усиленного контроля использования ключей.

Данный режим включается одним из способов:

- в процессе установки КриптоПро JCP, если таковая требуется (см. [рис. 5](#)). При этом после установки при первом использовании СКЗИ для инициализации встроенных в СКЗИ ПДСЧ будет произведён запуск БиоДСЧ;
- в контрольной панели КриптоПро JCP (см. [рис. 17](#)).

Использование СКЗИ с выключенным режимом усиленного контроля использования ключей допускается исключительно в тестовых целях!

1.2 Кодировки в Java

При запуске классов КриптоПро JCP сообщения будут выводиться в кодировке, принятой в Вашей виртуальной машине Java по умолчанию. Если кодировка, установленная Java при запуске, отличается от кодировки окна, текст будет отображаться некорректно. 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, чтобы КриптоПро JCP выводил сообщения в другой кодировке, измените значение переменной. Такое возможно, например, если Вы собираетесь перенаправить вывод в файл и анализировать его потом, используя другую кодировку:

```
install.bat \java >log.txt 2>&1
```

В UNIX-системах Java-машины используют для определения кодировки значение переменной `LANG`. Пожалуйста, убедитесь в том, что значение этой переменной совпадает с кодировкой Вашего окна.

1.3 Установка и удаление на Windows

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JCP в случае эксплуатации ПО в ОС Windows не требуется.

Установка КриптоПро JCP на ОС Windows с установленной Java-машиной версии 1.7 или 1.8 должна проводиться администратором с помощью командной строки из папки с инсталлятором (запуск командного файла следует выполнять с правами администратора, «Run as administrator»):

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

Например: `setup_console.bat "C:\Program Files\Java\jdk1.7\jre"`

При этом будет использоваться исполняемый файл `<JRE>\bin\java.exe`, а также будет произведено полное удаление файлов КриптоПро JCP, что может быть необходимо при разрешении ошибочных ситуаций. В любом случае, перед установкой автоматически осуществляется попытка деинсталляции КриптоПро JCP 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, необходимо запустить сценарий:

```
ControlPane.bat <путь_к_JRE>
```

Если установка завершилась успешно, то будет запущена контрольная панель. При необходимости введите лицензию, как это описано в разделе [Проверка и ввод лицензии](#).

Удаление КриптоПро JCP на ОС Windows выполняется 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.

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

1.3.1 Установка/удаление с помощью графического инсталлятора

Установка или удаление КриптоПро JCP вместе с нативной библиотекой может также может быть выполнена с помощью графического установщика setup.exe. Запуск setup.exe должен производиться под управлением учетной записи администратора.

Пошаговый процесс установки КриптоПро JCP с помощью графического установщика представлен на рис. 1 — 3. Процесс удаления аналогичен с учетом выбора соответствующего действия в окне инсталлятора (см. рис. 2).

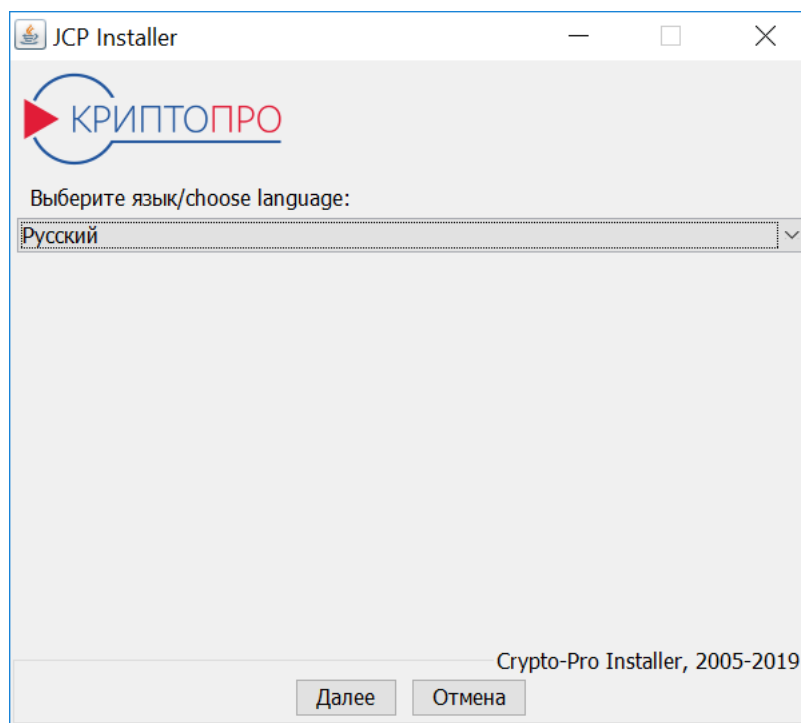


Рисунок 1. Окно выбора языка инсталлятора

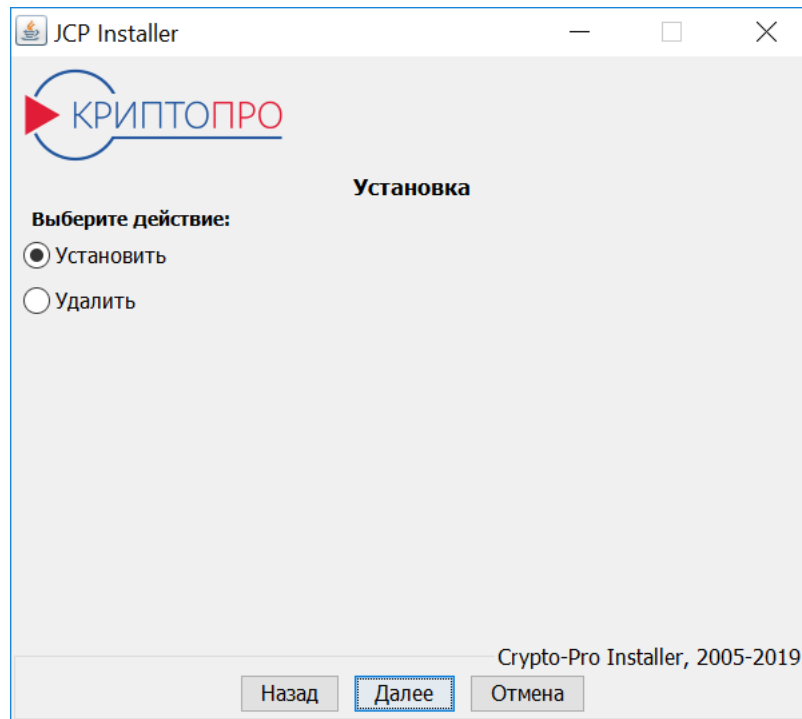


Рисунок 2. Окно выбора действия

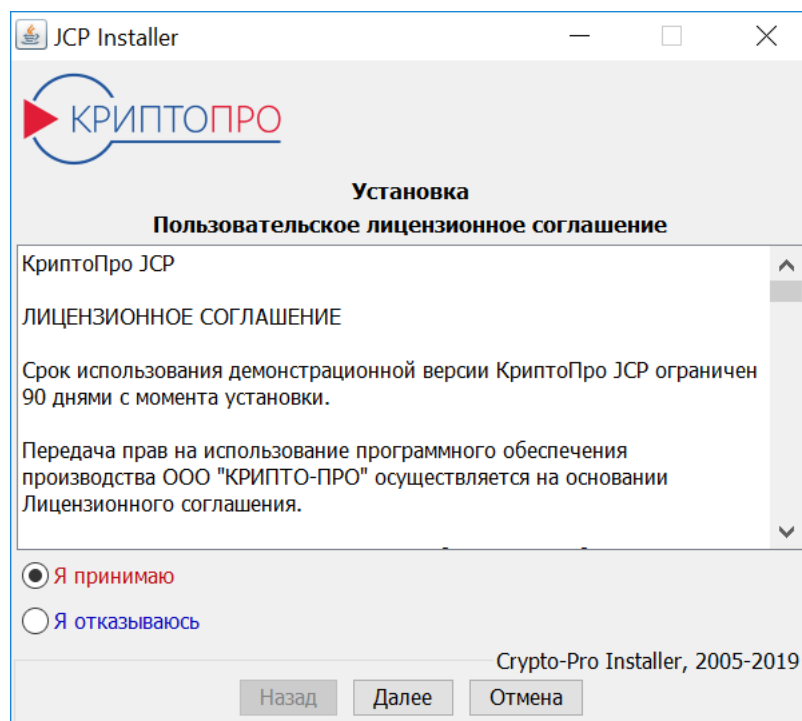


Рисунок 3. Окно с лицензионным соглашением

После выбора языка и действия (установка/удаление) мастером установки будет предложено указать, в какой JRE будут производиться настройка, какие модули следует установить/удалить/обновить (см. [рис. 4](#), [рис. 5](#)).

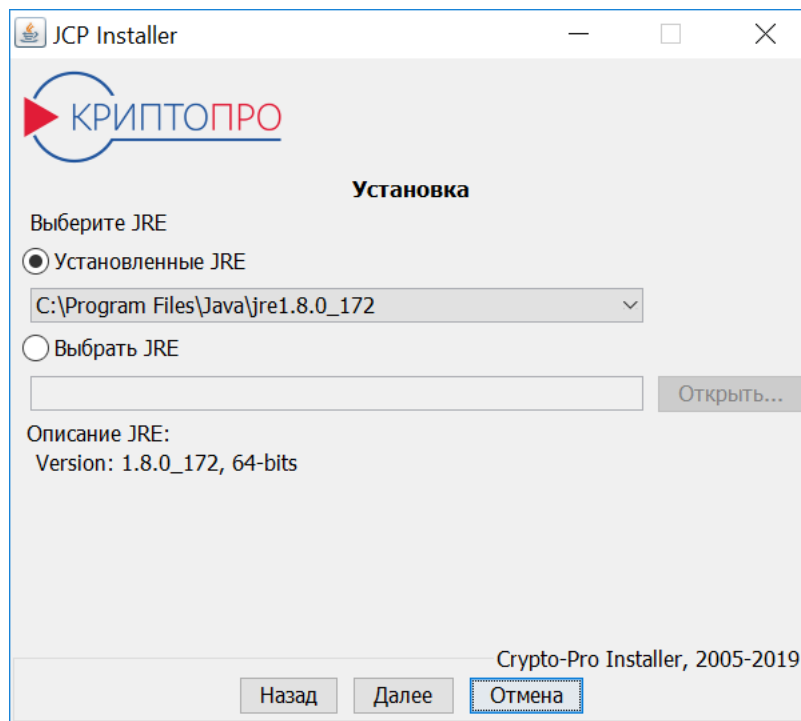


Рисунок 4. Окно выбора JRE

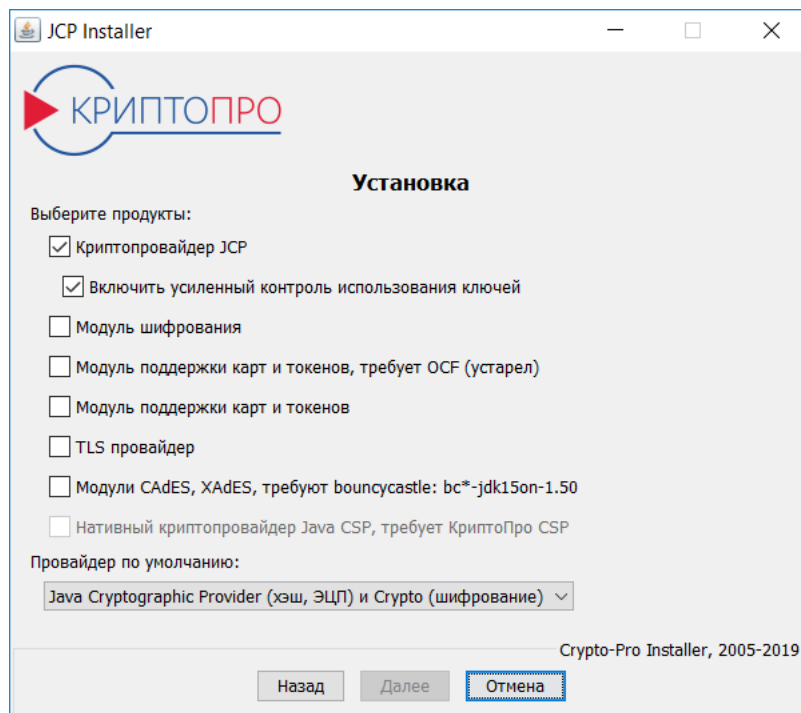


Рисунок 5. Окно выбора продукта



Примечание. При установке криптопровайдера КриптоПро JCP 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!



Примечание. При установке модуля CadES необходимо скопировать в папку <JRE>/lib/ext файлы библиотек bouncycastle.

При установке провайдера можно указать, какой из них будет использоваться по умолчанию. В дальнейшем это настройку можно изменить в панели на вкладке **Алгоритмы** контрольной панели. В зависимости от приоритета тот или иной провайдер будет находиться выше в списке провайдеров java.security.

С помощью пункта «Установить» может быть произведена как установка, так и обновление модулей. Если в указанной JRE уже имеется установленный JCP и другие модули, то может быть предложено их обновить, если их версия устарела.

Затем будет предложено указать серийные номера выбранных для установки продуктов (см. [рис. 6](#)). Если они не указаны, то будут использованы серийные номера по умолчанию сроком действия 3 месяца. В этом же окне возможна проверка лицензий.

Рисунок 6. Окно ввода серийных номеров продуктов

Далее будет предложено проверить корректность введенной ранее информации, удаление настроек (в

случае удаления модулей) (см. [рис. 7](#)).

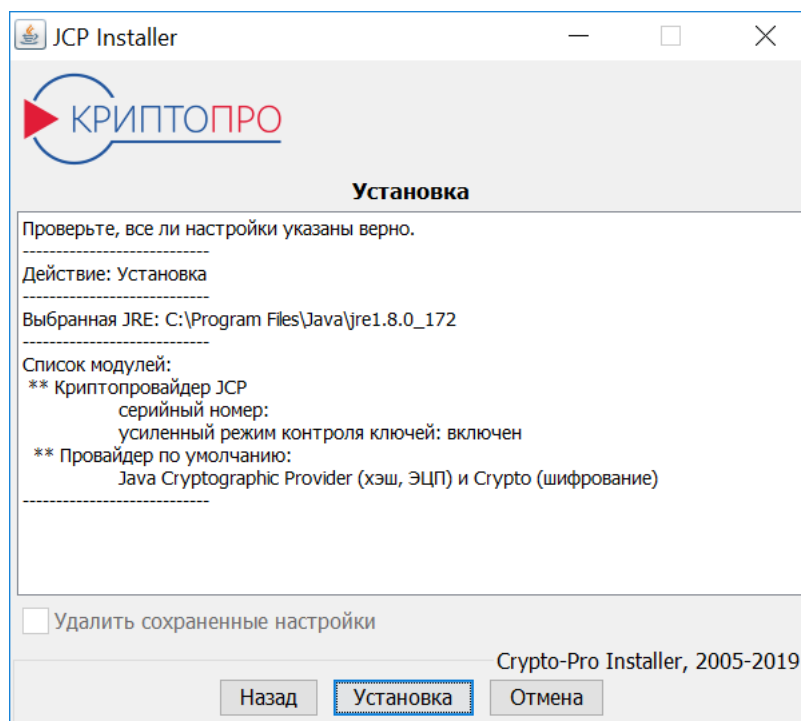


Рисунок 7. Окно проверки настроек установки/удаления

Затем произойдет установка/удаление выбранных продуктов с выполнением логирования в окне установщика (см. [рис. 8](#)).

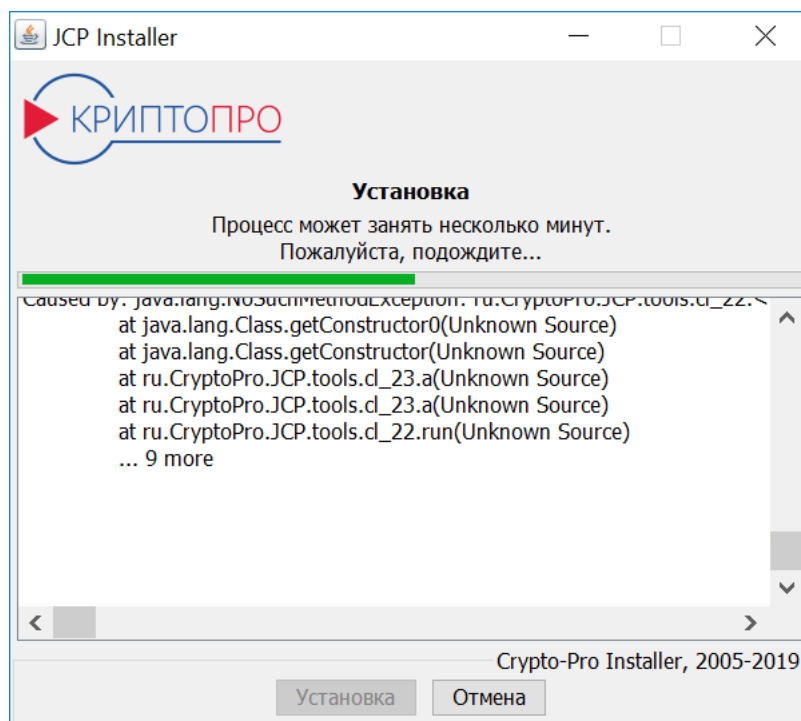


Рисунок 8. Окно процесса установки

В случае успешного выполнения установки будет отображено окно (см. [рис. 9](#)). После перехода далее

в случае установки может быть предложено запустить панель управления и создать ярлык для запуска Контрольной панели на Рабочем столе (см. [рис. 10](#)).

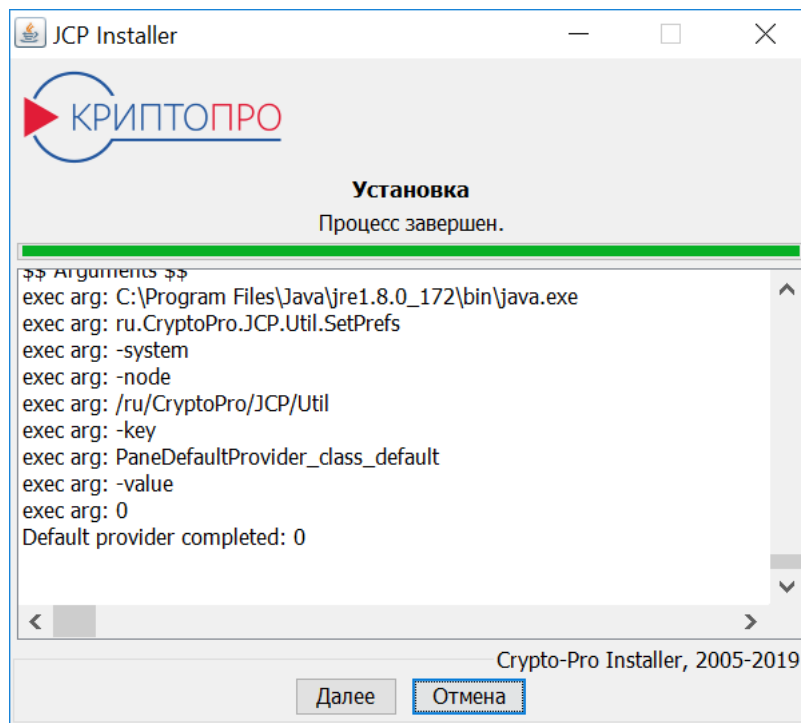


Рисунок 9. Окно с результатами установки

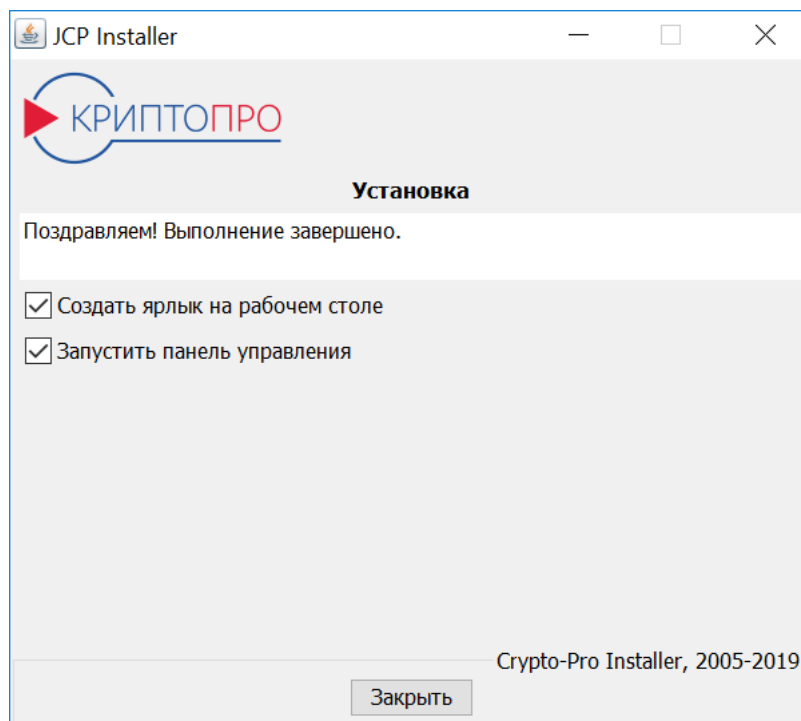


Рисунок 10. Завершение установки



Примечание. Процесс удаления отличается от установки только отсутствием некоторых шагов, таких как 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 не удастся (например, файлы заняты другим процессом), будет предложено перезапустить установщик (см. [рис. 8](#)).

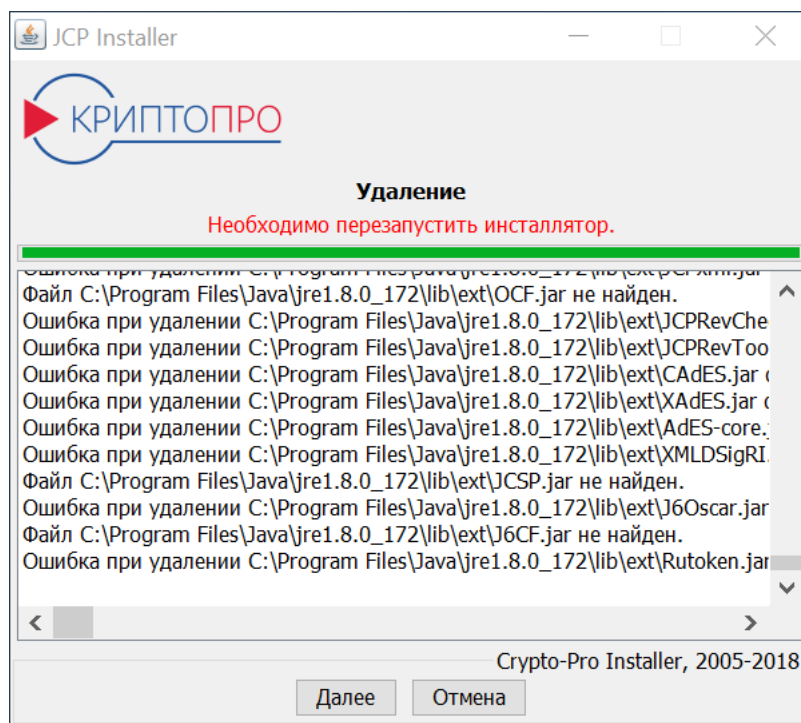


Рисунок 11. Ошибка при удалении компонентов

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

1.3.2 Установка с помощью командной строки

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

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

2) 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 | -j6cf | -cpssl | -jcsp] [-strict_mode]
[-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] [-rmsetting]
[-default_provider [0|1]]
```

- `[-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|-jbcf|-cpssl|-jcsp] — основные доступные модули (jcp и модуль шифрования jcryptop входят в состав Исполнения 2, только один jcp — Исполнения 1),
- strict_mode — включение режима усиленного контроля использования ключей (обязательно при установке, потребует работы с БюДСЧ),
- [-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] — серийные номера для выбранных продуктов,
- [-rmsetting] — удаление существующих настроек (только при удалении модулей),
- [-default_provider [0 | 1]] — провайдер по умолчанию (0 — JCP, 1 — JavaCSP).

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

Примеры команд:

1) установка КриптоПро JCP (исполнения 2 — с модулем шифрования), cpSSL и CAdES в C:\ProgramFiles\Java\jre7 с указанием серийного номера для КриптоПро JCP:

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

2) удаление КриптоПро JCP в JRE по умолчанию (текущая исполняемая JRE):

```
setup_console.bat "C:\Program Files\Java\jre7" -force -en -uninstall -jcp
```

3) доустановка к уже установленному КриптоПро JCP модуля JavaCSP в JRE по умолчанию (текущая исполняемая JRE) с указанием серийного номера для JavaCSP:

```
setup_console.bat "C:\Program Files\Java\jre7" -force -ru -install -jcsp -serial_jcsp XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

1.4 Установка на UNIX и Mac OS

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JCP в случае эксплуатации ПО в ОС *nix не требуется. В случае ОС *nix настройка СКЗИ состоит в запуске командного файла `configure.sh`, входящего в состав дистрибутива КриптоПро JCP версии 2.0 R4, для создания иерархии папок, необходимой для создания и хранения ключевых контейнеров. Запуск командного файла осуществляется под управлением учетной записи администратора.

Установка КриптоПро JCP на ОС UNIX с установленной Java-машиной версии 1.7 или 1.8 осуществляется аналогично установке КриптоПро JCP на Windows, с разницей лишь в исполняемых файлах для установки и запуска контрольной панели.

Для установки КриптоПро JCP необходимо выполнить команду:

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

Например: `setup_console.sh /usr/java/jdk1.7/jre`

Для удаления КриптоПро JCP необходимо выполнить команду:

```
setup_console.sh <путь_к_JRE>
```

Для запуска контрольной панели необходимо выполнить команду:

```
ControlPane.sh <путь_к_JRE>
```

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

Установка КриптоПро JCP должна осуществляться администратором. Права, необходимые для установки СКЗИ, можно получить одним из следующих способов:

- Войти как пользователь root;
- Выполнив команду "su";
- 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 установщике необходимо указать с помощью кнопки «Открыть...» (см. [рис. 4](#)) или вписав в специальное поле.

Графический установщик запускается с помощью скрипта `setup_gui.sh` под управлением учетной записи администратора. Работа консольного установщика описана в [разд. 1.3.2](#).

1.5 Локальная установка вызовом Java

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JCP не требуется.

При установке КриптоПро JCP на операционные системы с установленной Java-машиной версии 1.7 или 1.8, отличные от Windows и Unix, необходимо воспользоваться установкой через вызов программы Java. Этот способ установки также может использоваться при частичной установке КриптоПро JCP, 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.VariantOne
```

для установки исполнения 1 (КриптоПро JCP версии 2.0 R4 без функций шифрования)

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

для установки исполнения 2 (КриптоПро JCP версии 2.0 R4 с функциями 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 с компьютера. При обновлении версии КриптоПро JCP, 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 в одном из стандартных исполнений необходимо запустить

java -classpath JCPinst.jar ru.CryptoPro.Install.VariantOne -install — для установки Исполнения 1

java -classpath JCPinst.jar ru.CryptoPro.Install.VariantTwo -install — для установки Исполнения 2

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» версии 2.0 R3, должен быть установлен.

JCP

Провайдер для подписи, должен быть установлен.

JCPControlPane

Панель для управления настройками, должен быть установлен.

ASN1P

Расширенный ASN, должен быть установлен.

Rutoken

Библиотека (модуль) поддержки rutoken.

J6CF

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

J6Oscar

Библиотека поддержки смарт-карты Оскар, необязательный пакет, необходим для хранения секретных ключей. Требуется 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 (JTLS)»), требует установки пакетов JCP, ASN1P, JCryptoP.

При установке КриптоПро 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 необходимо запустить класс установки (для соответствующего исполнения) с опцией -uninstall, например следующим образом:

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

После завершения процесса удаления КриптоПро JCP необходимо удалить все файлы имена которых находятся в списке delfiles.lst.

Для частичного удаления КриптоПро JCP (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
```

1.6 Установка дополнительных пакетов

Для установки дополнительных пакетов, а также пакетов, входящих в состав КриптоПро JCP, 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 находиться в одной директории. Удаление пакета можно проводить любым из описанных выше способов.

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. Ниже приведен полный список классов установки для всех пакетов, входящих в КриптоПро JCP версии 2.0 R4 и КриптоПро JavaTLS, а также указано, в каких jar файлах находится пакет установщика.

JCP	ru.CryptoPro.JCP.Install.JCPInstaller	JCP.jar
ASN1P	ru.CryptoPro.JCP.Install.JCPAsnInstaller	JCP.jar
J6CF	ru.CryptoPro.JCP.KeyStore.J6CF.Install	J6CF.jar
J6Oscar	ru.CryptoPro.JCP.KeyStore.J6Oscar.Install	J6Oscar.jar
Rutoken	ru.CryptoPro.JCP.KeyStore.RutokenStore.Install	Rutoken.jar
JCPxml	ru.CryptoPro.JCPxml.XMLInstall	JCPxml.jar
JCPRequest	ru.CryptoPro.JCPRequest.RequestInstall	JCPRequest.jar
JCryptoP	ru.CryptoPro.Crypto.JCryptoPInstaller	JCryptoP.jar
JCPRevCheck	ru.CryptoPro.reprov.Install	JCPRevCheck.jar (также необходим JCPRevTools.jar)
cpSSL	ru.CryptoPro.ssl.JTLSInstall	cpSSL.jar
AdES-core	ru.CryptoPro.AdES.installer.Install	adES-core.jar
CAdES	ru.CryptoPro.CAdES.installer.Install	CadES.jar
XadES	ru.CryptoPro.XAdES.installer.XAdESInstall	XadES.jar
JCSP	ru.CryptoPro.JCSP.JCSPInstaller	JCSP.jar

1.7 Проверка и ввод лицензии

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

Клиентская лицензия предусматривает количество ядер не более четырех. Если количество ядер более четырех или в дальнейшем предполагается использовать JavaTLS сервер, то необходима серверная лицензия на КриптоПро JCP версии 2.0 R4 (даже если по указанному ниже списку подходит клиентская).

Клиентские ОС:

- Windows Vista/7/8/8.1/10;
- Red Hat Enterprise Linux Desktop, Workstation (WS);
- Fedora;
- SUSE Linux Enterprise Desktop;
- OpenSUSE Linux;
- Debian GNU/Linux;
- Mandriva Corporate Desktop;
- Ubuntu Desktop Edition;
- Ubuntu Phone;
- Linux XP Enterprise Desktop 2008;
- ТД ОС АИС ФССП России (GosLinux) (x86, x64);
- Red OS (x86, x64);
- Linux Mint;
- ALT Linux Desktop, Lite;
- ROSA Desktop 2011, Enterprise Linux Desktop;

- Mac OS X.

Серверные ОС:

- Windows Server 2003/2008/2008R2/2012/2012R2/2016/2019;
- Solaris;
- FreeBSD;
- CentOS;
- AIX;
- HP-UX;
- SUSE Linux Enterprise Server;
- Red Hat Enterprise Linux Server;
- ROSA Enterprise Linux Server;
- любые ОС на архитектуре отличной от ia32/amd64.

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

Минимальные требования к лицензии для данной системы указаны на вкладке **JCP** контрольной панели, также их можно узнать из командной строки:

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

Ввод лицензии осуществляется 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 ?
```

Для ввода лицензии с помощью контрольной панели откройте вкладку **JCP** и нажмите кнопку **Ввод лицензии**. В открывшемся окне введите имя пользователя, название организации и серийный номер продукта (см. [рис. 12](#)).

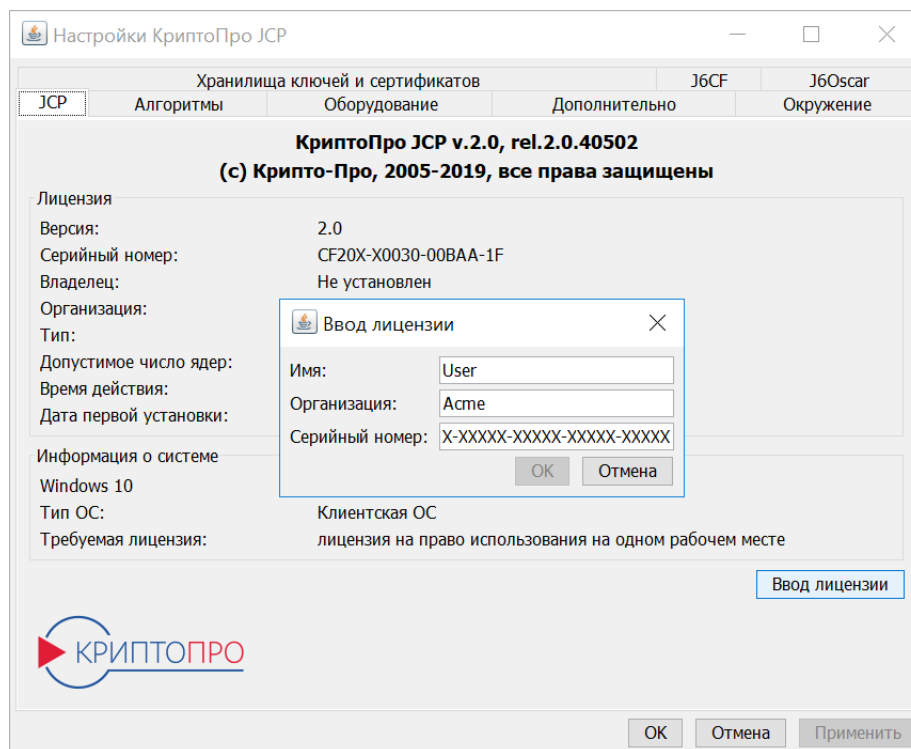


Рисунок 12. Ввод лицензии

1.8 Установка модулей поддержки ключевых носителей

1.8.1 Установка модуля поддержки JaCarta для носителей Аладдин Р.Д.

Для того чтобы использовать [носители компании Аладдин Р.Д.](#) с СКЗИ КриптоПро JCP версии 2.0 R4 (тип хранилища «J6CFStore», подробнее см. ЖТЯИ.00091-04 33 01. Руководство программиста) в исполнительной среде Java Runtime Environment, необходимо выполнить следующие подготовительные действия.

В случае использования Java-машин версии 1.7 или 1.8:

- Установить eToken RTE
Процедура установки подробно описана в руководстве пользователя eToken RTE.
- Установить исполнительную среду JRE
- Установить КриптоПро JCP версии 2.0 R4 с модулем поддержки карт и токенов J6CF (см. [Установка дополнительных пакетов](#))
Если КриптоПро JCP более ранней сборки уже был установлен, его следует переустановить. Помимо основных модулей, нужно также установить модуль поддержки карт и токенов (J6CF).
- Установить [модуль поддержки Jacarta](#) для КриптоПро JCP версии 2.0 R4

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



Примечание. Ключевые носители Jacarta и eToken, а также модуль поддержки Jacarta для КриптоПро JCP являются продуктами компании [Аладдин Р.Д.](#). По всем вопросам использования обращайтесь к компании-разработчику.

После установки или настройки необходимых модулей для корректной работы нужно определить сервис, посредством которого будет осуществляться работа модуля J6CF с данными носителями. Таким сервисом является `ru.aladdin.jacarta.cryptopro.jcp.j6cf.AladdinService`.

Задать необходимый сервис можно через контрольную панель КриптоПро JCP. Для этого на вкладке **J6CF** (см. [рис. 13](#)) нужно выбрать подходящие значения в полях «Считыватель» и «Реализация сервиса работы с картой».

Сервис, осуществляющий работу с носителем, определяется параметром `ConfigReader_class_Service` в настройках конфигурации модуля J6CF (см. [Настройка параметров провайдера с помощью Preferences](#)).

Значение этого параметра можно установить также при помощи класса `ru.CryptoPro.JCP.Util.SetPrefs` (этот класс находится в модуле JCP и предоставляет возможности для добавления и редактирования настроек):

В случае использования Java-машин версии 1.7 или 1.8:

```
java ru.CryptoPro.JCP.Util.SetPrefs -system -node ru/CryptoPro/JCP/KeyStore/J6CF -key
ConfigReader_class_Service -value ru.aladdin.jacarta.cryptopro.jcp.j6cf.AladdinService
```

1.8.2 Установка/настройка модуля поддержки ESMART

Для того чтобы использовать [ESMART](#) как носитель ключевой информации для СКЗИ КриптоПро JCP (тип хранилища «J6CFStore», подробнее см. ЖТЯИ.00091-04 33 01. Руководство программиста) в исполнительной среде Java Runtime Environment, необходимо выполнить следующие подготовительные действия.

В случае использования Java-машин версии 10 и выше:

- Скачать [модуль поддержки ESMART](#) для КриптоПро JCP версии 2.0 R4 с сайта компании-разработчика
- Распаковать архив
- Добавить библиотеку EsmartTokenJCP-1.0.2.jar из архива в classpath.

В случае использования Java-машин версии 1.7 или 1.8:

- Установить исполнительную среду JRE
- Установить КриптоПро JCP версии 2.0 R4 с модулем поддержки карт и токенов J6CF (см. [Установка дополнительных пакетов](#))
Если КриптоПро JCP более ранней сборки уже был установлен, его следует переустановить. Помимо основных модулей, нужно также установить модуль поддержки карт и токенов (J6CF).
- Установить [модуль поддержки ESMART](#) для КриптоПро JCP версии 2.0 R4
В случае, если установку не удастся выполнить средствами, входящими в пакет модуля поддержки ESMART (install.bat или install.sh), рекомендуется пользоваться следующей командой:

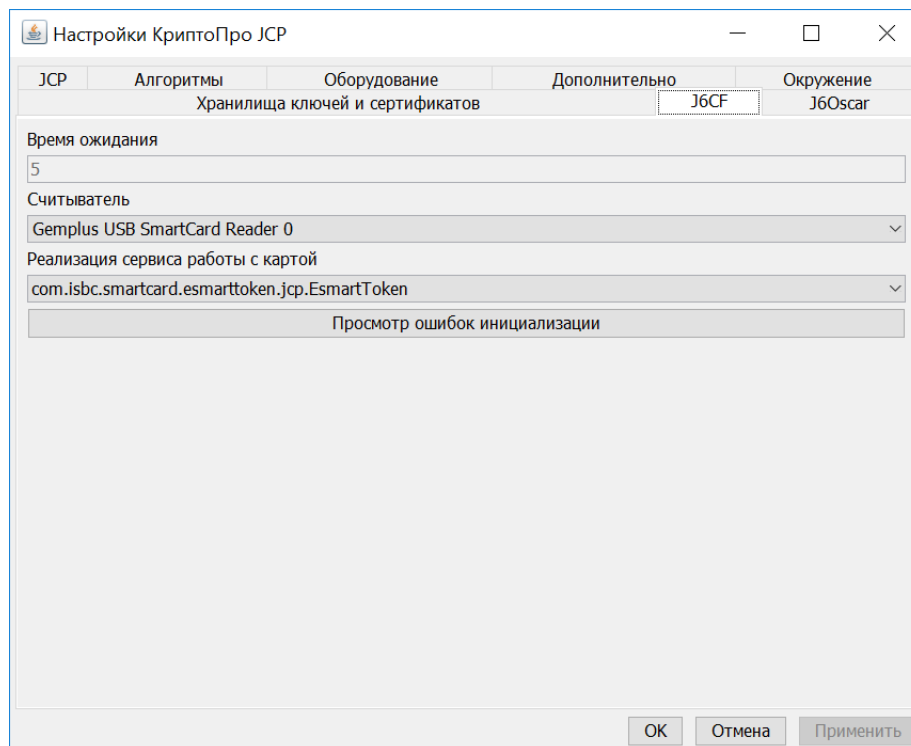
```
<JRE>/bin/java -cp EsmartTokenJCP-1.0.2.jar com.isbc.smartcard.esmarttoken.jcp.Install -install
```



Примечание. Ключевой носитель ESMART и модуль поддержки ESMART для КриптоПро JCP являются продуктами [Группы Компаний ISBC](#). По всем вопросам использования обращайтесь к компании-разработчику.

После установки или настройки необходимых модулей для корректной работы нужно определить сервис, посредством которого будет осуществляться работа модуля J6CF с носителем ESMART. Для считывателей ESMART таким сервисом является `com.isbc.smartcard.esmarttoken.jcp.EsmartToken`.

Задать необходимый сервис можно через контрольную панель КриптоПро JCP. Для этого на вкладке **J6CF** (см. [рис. 13](#)) нужно выбрать подходящие значения в полях «Считыватель» и «Реализация сервиса работы с картой».

Рисунок 13. Вкладка **J6CF**

Сервис, осуществляющий работу с носителем, определяется параметром `ConfigReader_class_Service` в настройках конфигурации модуля J6CF (см. [Настройка параметров провайдера с помощью Preferences](#)).

Значение этого параметра можно установить также при помощи класса `ru.CryptoPro.JCP.Util.SetPrefs` (этот класс находится в модуле JCP и предоставляет возможности для добавления и редактирования настроек):

В случае использования Java-машин версии 10 и выше:

```
java -cp JCP.jar ru.CryptoPro.JCP.Util.SetPrefs -user -node ru/CryptoPro/JCP/KeyStore/J6CF  
-key ConfigReader_class_Service -value com.isbc.smartcard.esmarttoken.jcp.EsmartToken
```

В случае использования Java-машин версии 1.7 или 1.8:

```
java ru.CryptoPro.JCP.Util.SetPrefs -system -node ru/CryptoPro/JCP/KeyStore/J6CF -key  
ConfigReader_class_Service -value com.isbc.smartcard.esmarttoken.jcp.EsmartToken
```

1.8.3 Установка/настройка модуля поддержки Rutoken

В случае использования Java-машин версии 1.7 или 1.8:

Для настройки работы данных носителей с КриптоПро JCP версии 2.0 R4 в исполнительной среде JRE требуется:

- Установить драйверы для носителя;
- Установить исполнительную среду JRE;
- Установить «КриптоПро JCP» версии 2.0 R3 (см. [Особенности установки](#));

Если КриптоПро JCP более ранней сборки уже был установлен, его следует переустановить.

- В состав дистрибутива КриптоПро JCP версии 2.0 R4 входит модуль Rutoken.jar, являющийся модулем поддержки носителей компании Актив(Rutoken Lite, Rutoken S, Rutoken ECP). Он устанавливается вместе с остальными библиотеками, входящими в состав дистрибутива КриптоПро JCP.



Примечание. Ключевой носитель Rutoken и модуль поддержки Rutoken для КриптоПро JCP являются продуктами компании [Актив](#). По всем вопросам использования обращайтесь к компании-разработчику.

После установки/настройки КриптоПро JCP доступ к хранилищу Rutoken можно получить программно (с помощью KeyStore) или в контрольной панели КриптоПро JCP версии 2.0 R4. При этом, если к системе подключено несколько носителей Рутокен, то для каждого носителя будет создано собственное хранилище с именем, которое формируется в формате «RutokenStore_серийныйномер».

Если к системе подключен один носитель Рутокен, то ему будет соответствовать одно хранилище с именем «RutokenStore».

Список доступных хранилищ можно получить с помощью функции `getServices()` в составе объекта провайдера КриптоПро JCP, при этом поиск следует производить среди KeyStore по имени алгоритма Rutoken.

Для работы с носителем Рутокен требуется библиотека `libpcsclite`.

В ОС Ubuntu библиотека может быть установлена в место, путь к которому не входит в список поиска Java (<https://bugs.launchpad.net/ubuntu/+source/openjdk-7/+bug/898689>). По умолчанию поиск осуществляется в папках `/usr/$platform/libpcsclite.so` или `/usr/local/$platform/libpcsclite.so`, при этом `$platform` может принимать значения `lib/64` для 64-бит. ОС SunOS, `lib` или `lib64` для ОС семейства Linux (32-бит. И 64-бит.).

Передать путь к библиотеке можно с помощью свойства `sun.security.smartcardio.library`, например, `-Dsun.security.smartcardio.library=/lib/libpcsclite.so.1`:

```
java -Dsun.security.smartcardio.library=/lib/libpcsclite.so.1
ru.CryptoPro.JCP.ControlPane.MainControlPane
```

Или создав соответствующую ссылку на библиотеку (рекомендуется).

В случае использования Java-машин версии 1.7 или 1.8:

У модуля Rutoken.jar имеются собственные классы установки/удаления:

`ru.CryptoPro.JCP.KeyStore.Rutoken.Install` — класс установки/удаления, запускается с помощью параметра `-install` или `-uninstall`;

`ru.CryptoPro.JCP.KeyStore.Rutoken.ManifestInstall` — класс установки, обычно выполняется при запуске вида `java -jar Rutoken.jar`.

2 Настройка СКЗИ

2.1 Политики безопасности

Расположение файла политик безопасности Java зависит от версии используемой Java-машины.

В случае использования Java-машин версии 10 и выше:

Файл политики Java находится в `${java.home}/conf/security/java.policy`

В случае использования Java-машин версии 1.7 или 1.8:

Файл политики Java находится в `${java.home}/lib/security/java.policy`.

2.1.1 Права доступа для JCP.jar

В случае использования Java-машин версии 10 и выше:

КриптоПро JCP версии 2.0 R4 запускается из каталога пользователя.

В случае использования Java-машин версии 1.7 или 1.8:

Необходимо настроить права доступа для файла JCP.jar согласно инструкции ниже.

КриптоПро JCP версии 2.0 R4 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";  
    permission 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. [разд. 4](#))

2.1.2 Права доступа для администратора JCP

В случае использования Java-машин версии 1.7 или 1.8:

Необходимо настроить права доступа для файла JCP.jar согласно инструкции ниже.

Администратору безопасности должны быть предоставлены следующие права доступа:

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

Кроме того, администратор безопасности должен иметь права доступа (зависят 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

2.1.3 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.

2.1.4 Права доступа пользователя

Пользователь КриптоПро JCP 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 чтение/запись файлов во временный каталог (см. [разд. 4](#));
- Права доступа, зависящие от операционной системы, на чтение/записи/создание каталогов в файлы ключей (см. [разд. 4](#))
- 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/cprosp/keysРч/var/cprosp/tmp), могут быть созданы только из-под root. Для их автоматического создания с правильными правами доступа достаточно создать контейнер из-под root.

2.2 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.

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
```

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\С\Р\tools` установить параметр `/Gost2001/Warning_class_default` в `true`.

3 Контрольная панель КриптоПро JCP

В данном разделе приводится описание контрольной панели КриптоПро JCP версии 2.0 R4, которая является инструментом, позволяющим устанавливать и изменять настройки криптопровайдера с помощью следующих функций:

- просмотр информации о существующей лицензии на использование КриптоПро JCP, а также установка новой лицензии;
- определение параметров реализованных криптографических алгоритмов;
- определение путей к хранилищам закрытых ключей и ключей ЭП;
- выбор параметров безопасности при работе с криптопровайдером;
- контроль целостности файлов;
- управление хранилищами ключевых контейнеров и сертификатов.

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.

Управление основными настройками СКЗИ осуществляется с помощью 6 вкладок контрольной панели:

- [Общие](#);
- [Алгоритмы](#);
- [Оборудование](#);
- [Дополнительно](#);
- [Окружение](#);
- [Хранилища ключей и сертификатов](#);

При установке дополнительных компонентов криптопровайдера КриптоПро JCP (например, КриптоПро JavaTLS) количество закладок контрольной панели может быть увеличено.

В случае использования Java-машин версии 10 и выше:

Изменение всех настроек криптопровайдера разрешено для пользователя, запустившего панель. Все поля контрольной панели доступны для редактирования. В случае изменения настройки будут сохранены для данного пользователя.

В случае использования Java-машин версии 1.7 или 1.8:

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.



Примечание. Внешний вид контрольной панели может отличаться от изображений, приведенных в данном документе. Внешний вид панели зависит от текущих настроек, операционной системы, установленной Java-машины и т.д.

3.1 Общие параметры СКЗИ (вкладка JCP)

Вкладка **JCP** содержит информацию о версии установленного СКЗИ, системе, текущей лицензии на использование криптопровайдера, а также используется для установки новой лицензии, если это необходимо.

При установке криптопровайдера КриптоПро JCP версии 2.0 R4 без ввода лицензии пользователю предоставляется временная лицензия с ограниченным сроком действия. Для использования СКЗИ после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для ввода серийного номера новой лицензии, а также информации о ее владельце, используйте кнопку «Ввод лицензии». **ВАЖНО:** лицензия будет сохранена только после нажатия кнопок «ОК» или «Применить». Обновленная информация о лицензии будет отражена в секции «Лицензия».

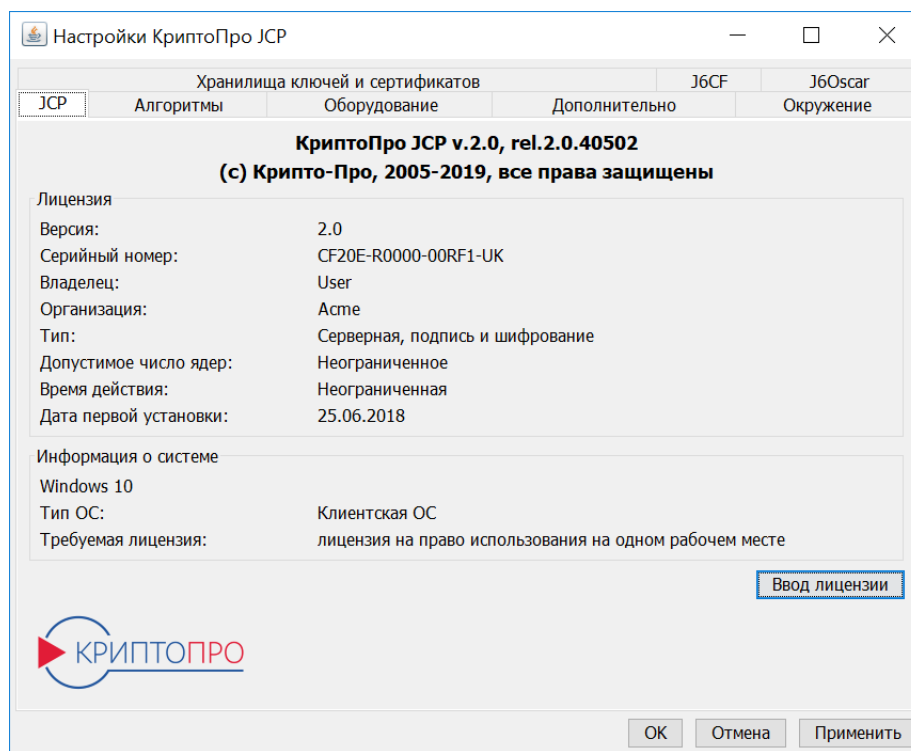


Рисунок 14. Вкладка JCP

3.2 Настройка параметров криптографических алгоритмов (вкладка Алгоритмы)

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

Для настройки доступны следующие параметры:

- выбор провайдера по умолчанию;

- параметры хэширования, шифрования, подписи и ключевого обмена для каждого доступного типа провайдера.

В случае использования Java-машин версии 10 и выше:

На вкладке **Алгоритмы** отсутствует поле «Провайдер по умолчанию для генерации ключей». Для выбора провайдера используется поле «Выберите провайдер» вкладки **Хранилища ключей и сертификатов** (подробнее см. [рис. 23.](#))

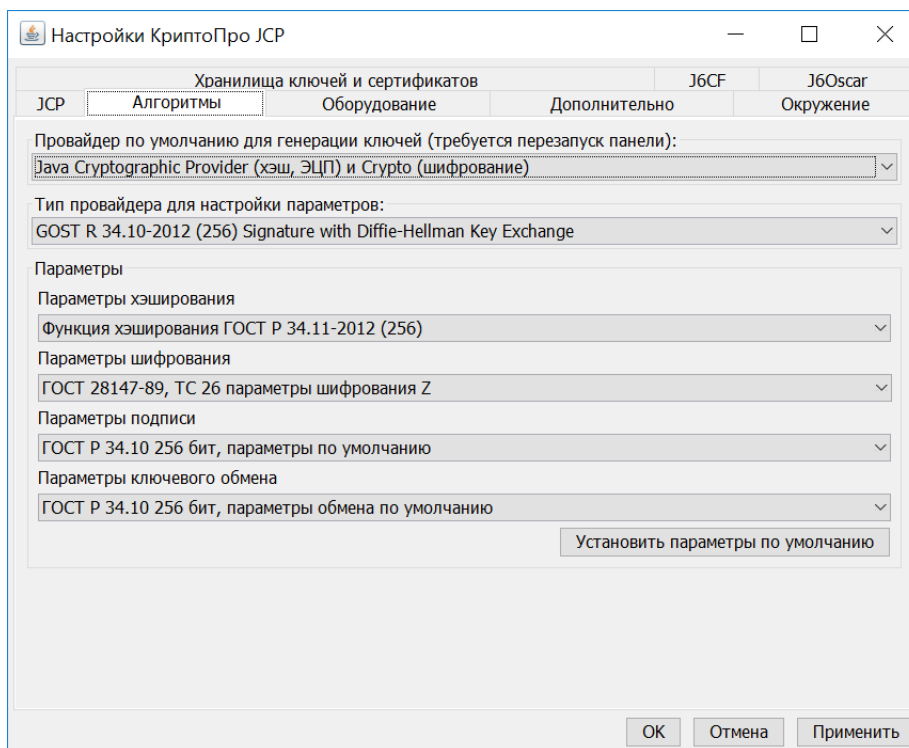


Рисунок 15. Вкладка JCP

3.3 Определение путей к хранилищам ключей (вкладка Оборудование)

Вкладка содержит 2 поля настройки — «Путь к хранилищу Floppy» для определения пути к дисководу и «Путь к хранилищу HDImage» 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 — `${user.home}\LocalSettings\ApplicationData\CryptoPro`
- Для Unix-платформ:
 - путь к дисководу — `/var/cprocsp/mnt/0;`
 - путь к жесткому диску — `/var/cprocsp/keys/${user.name};`

Предполагается, что системные настройки `${...}` установлены также в значения по умолчанию, т.е. значение `${user.name}` - это имя текущего пользователя, а `${user.home}` установлено в директорию `DocumentsandSettings\${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.

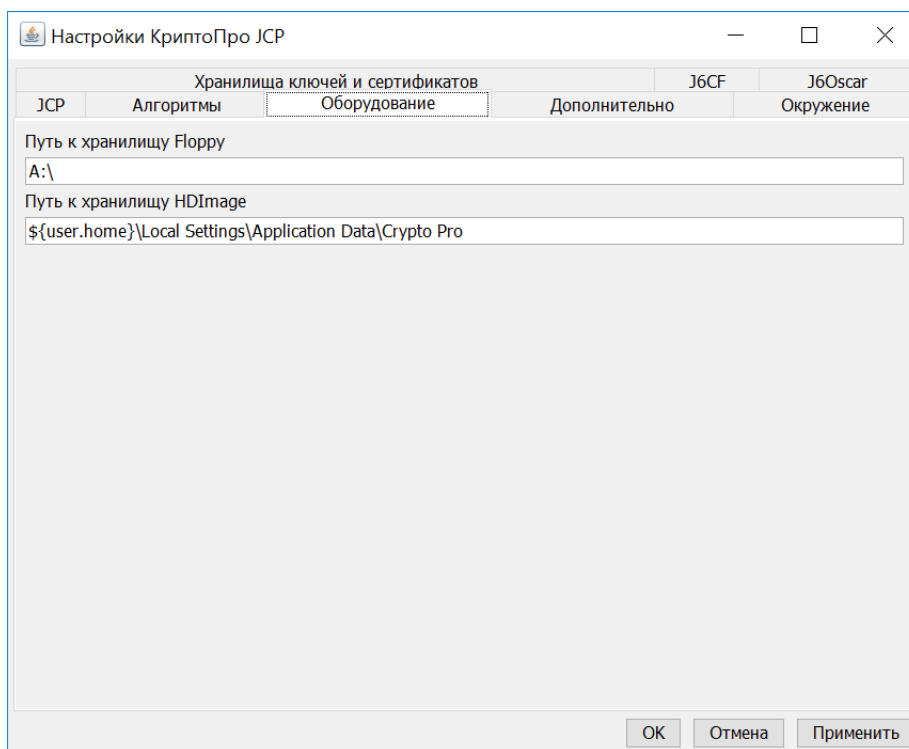


Рисунок 16. Вкладка Оборудование

3.4 Настройка параметров безопасности (вкладка Дополнительно)

Вкладка **Дополнительно** предоставляет интерфейс управления следующими настройками:

- **Путь Unix Mutex для пользователей** — путь к файлам, используемым для синхронизации работы с общими ресурсами пользователями криптопровайдера КриптоПро JCP версии 2.0 R4, а также для синхронизации между криптопровайдерами КриптоПро JCP и КриптоПро CSP);

По умолчанию установлены значения:

- Для Windows-платформ: `${java.io.tmpdir}\${user.name}`
- Для Unix-платформ - `/var/cprocp/tmp`

- **Проверять срок действия закрытого ключа** — определяет необходимость проверки срока действия долговременных закрытых ключей. По умолчанию опция включена.

- **Не отображать предупреждения об использовании ключей ГОСТ Р 34.10-2001** — определяет необходимость отображения предупреждений о невозможности использования ключей ГОСТ Р 34.10-2001 для выработки электронной подписи после 31 декабря 2019 года.

- **Усиленный контроль использования ключей** — включение режима усиленного контроля использования ключей. Режим должен быть в обязательном порядке включён при использовании СКЗИ. Использование СКЗИ при выключенном режиме разрешено исключительно в тестовых целях.

- **Скрипт для смены прав на папку ключей пользователя** — определение 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.

По умолчанию установлены значения:

– По умолчанию для Windows-платформ скрипт отсутствует, поскольку по умолчанию путем к закрытым ключам обмена и ключам электронной подписи пользователя является `${user.home}\LocalSettings\ApplicationData\CryptoPro`, где `${user.name}` — имя текущего пользователя, а `${user.home}` установлено в директорию `DocumentsandSettings\${user.name}`. При такой настройке `${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 `${user.home}` в отличную от `DocumentsandSettings\${user.name}` (где `${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.

– Значение по умолчанию для Unix-платформ — `chmod a-rwx,u+rwx`.

• **Время ожидания ввода, в сек** — задает 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 истечении указанного периода оно закрывается.

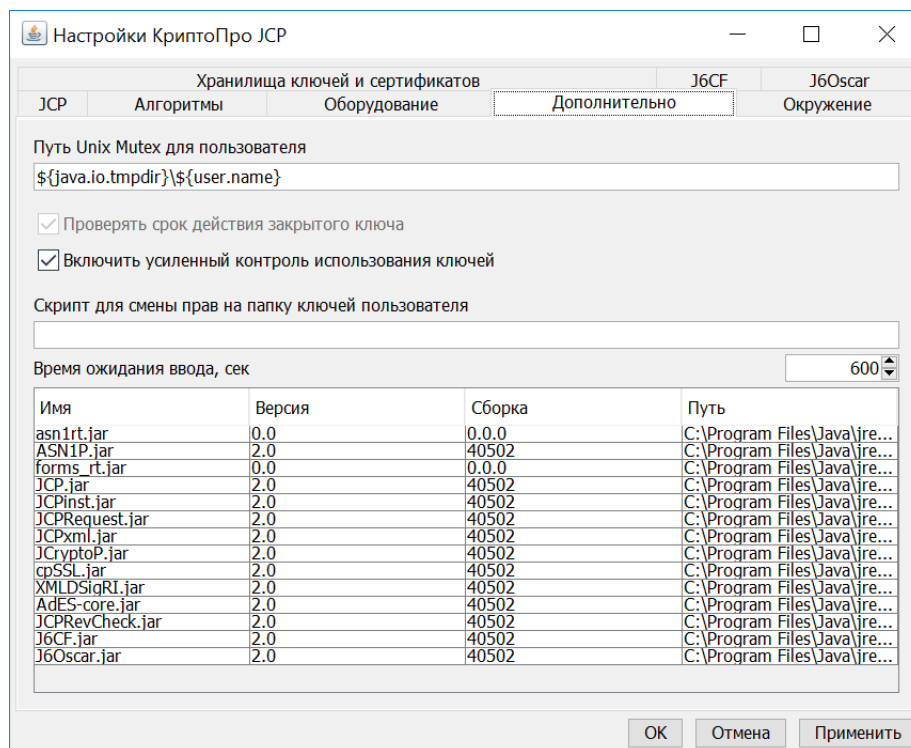
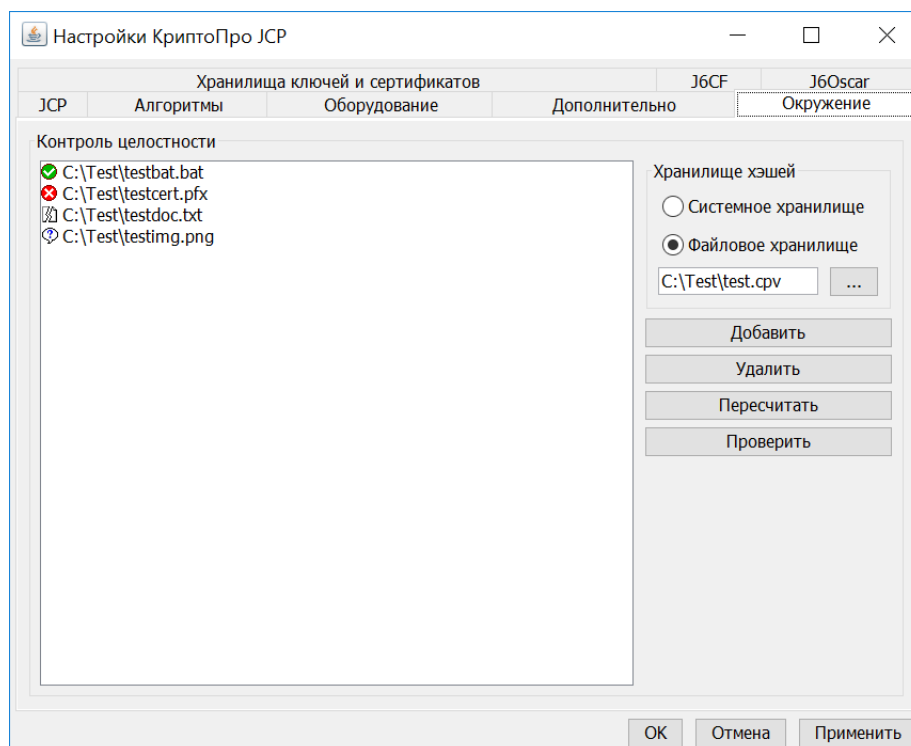


Рисунок 17. Вкладка **Дополнительно**

3.5 Контроль целостности файлов (вкладка **Окружение**)

Секция «Контроль целостности» вкладки **Окружение** предназначена для контроля целостности файлов ОС средствами КриптоПро JCP. 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;
- выбирать хранилище, по которому будет осуществляться контроль всех файлов.

Рисунок 18. Вкладка **Окружение**

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.

Типы хранилищ

Хэши файлов могут храниться:

- в системных настройках (системное хранилище)

В случае хранения их в системных настройках не нужен никакой дополнительный выбор, система автоматически определяет их месторасположение.

- в файле (файловое хранилище)

В случае хранения хэшей в файле, следует определить хранилище, указав имя файла, в котором будет организовано хранилище. Файл хранилища должен иметь расширение .srv. 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 .srv, то оно будет заменено на .srv. 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.

Начальные установки

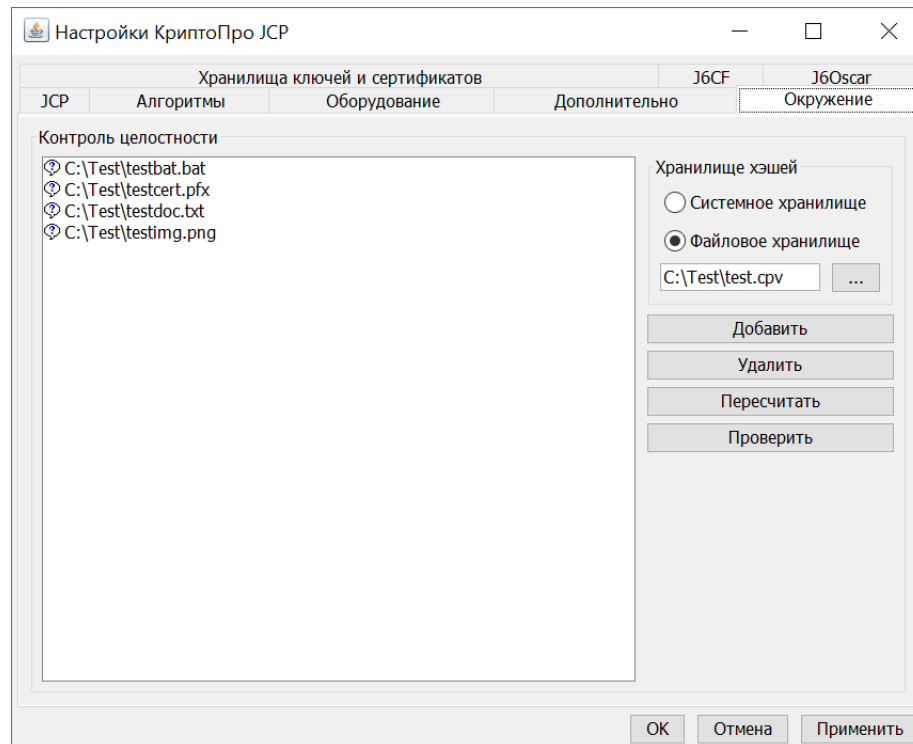
Изначально установлено хранилище в системных настройках, список файлов в нем пуст. При открытии файлового диалога для выбора нового хранилища или для добавления файлов, они откроются в домашнем каталоге пользователя.

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».

Работа с хранилищем

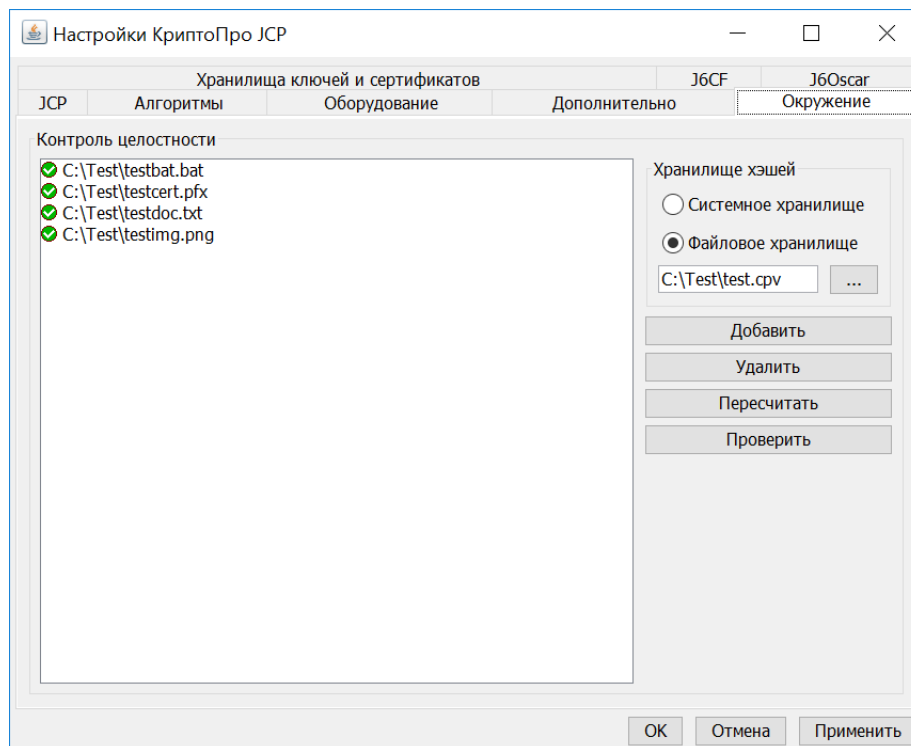
- Добавление файлов

При нажатии кнопки «Добавить» в раскрывшемся диалоге необходимо 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 19. Вкладка **Окружение**, добавление файлов

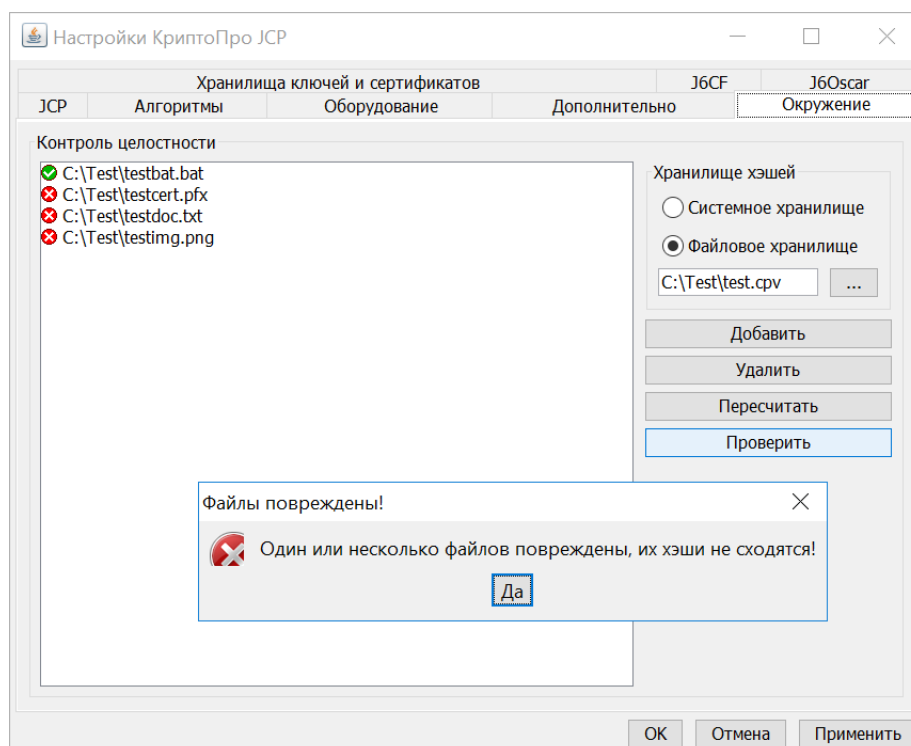
- Вычисление хэшей

Для вычисления значений хэшей выделите файлы, лежащие в хранилище и отображенные в окне, и нажмите 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».

Рисунок 20. Вкладка **Окружение**, успешное вычисление/пересчет значений хэшей

- Проверка целостности файлов

Выделите необходимые файлы, лежащие в хранилище и отображенные в окне и нажмите кнопку «Проверить». Будут проверены все выделенные файлы, а если не был выделен ни один, будут проверены все файлы, находящиеся в хранилище.

Рисунок 21. Вкладка **Окружение**, ошибка при проверке целостности файлов

- Удаление файлов

Выделите файлы, лежащие в хранилище и отображенные в окне, и нажмите 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. Исключения составляют текущие каталоги для диалогов добавления файлов в хранилище и выбора хранилища, которые сохраняются после каждого закрытия соответствующего диалога.

Права доступа к функциям

Установки вкладки, 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.

3.6 Управление хранилищами ключевых контейнеров и сертификатов (вкладка Хранилища ключей и сертификатов)

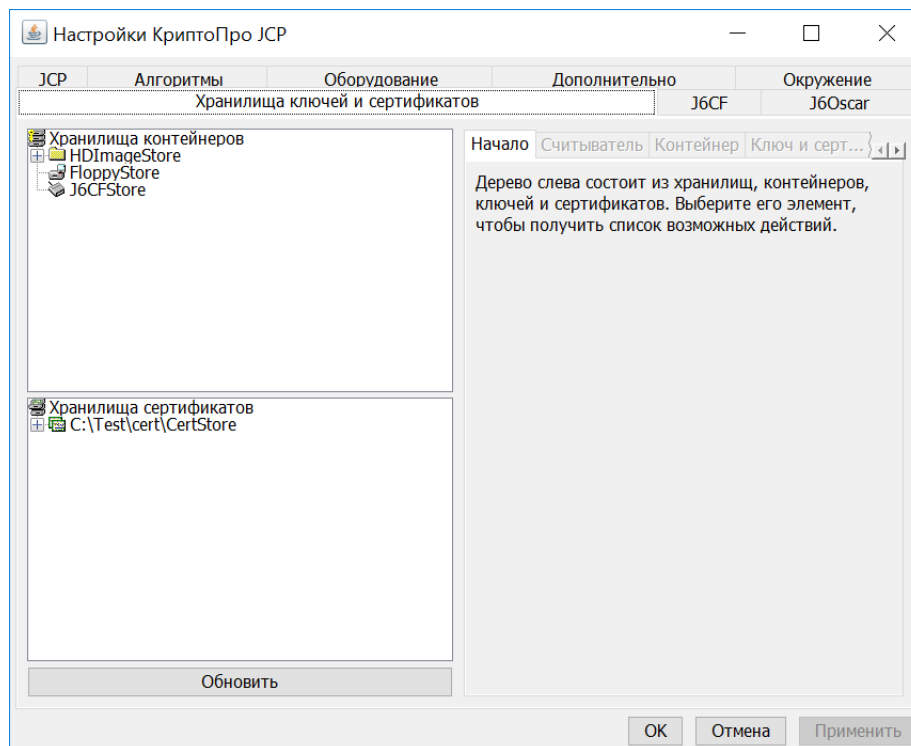
Вкладка **Хранилища ключей и сертификатов** предназначена для просмотра хранилищ ключей, установленных в системе, просмотра и управления контейнерами в хранилищах.

Вкладка предоставляет доступ к следующим функциям:

- создание, копирование, просмотр и удаление контейнеров в хранилище;
- копирование и просмотр сертификатов в хранилищах и в контейнерах,
- добавление сертификатов из файлов и контейнеров в хранилище сертификатов и удаление сертификатов из хранилища;
- установка и изменение паролей на хранилищах и контейнерах.

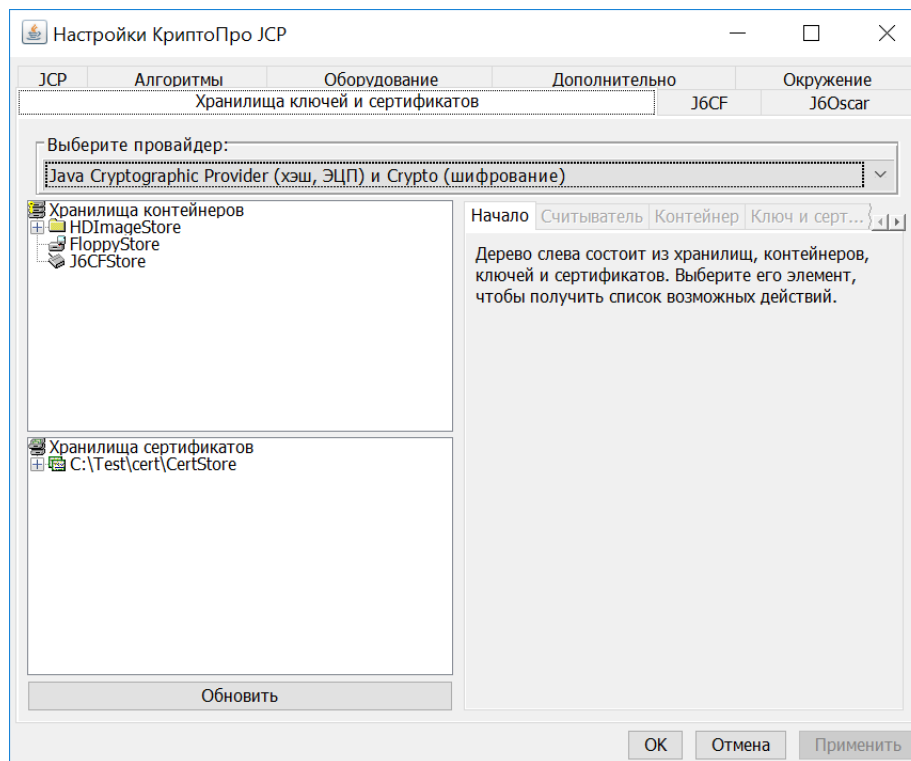
Вкладка содержит окно просмотра дерева хранилищ контейнеров, окно просмотра дерева хранилищ сертификатов, кнопки управления хранилищами и кнопки управления объектами в хранилищах.

При выборе любого элемента дерева автоматически будет выбрана закладка с соответствующими кнопками для выполнения операций над данным объектом.

Рисунок 22. Вкладка **Хранилища ключей и сертификатов**

В случае использования Java-машин версии 10 и выше:

По кнопке «Выберите провайдер» можно выбрать один из установленных провайдеров, для которого будут отображаться контейнеры (см. [рис. 23](#)). Для возможности выбора провайдера JCSP необходимо передать его при запуске в classpath контрольной панели.

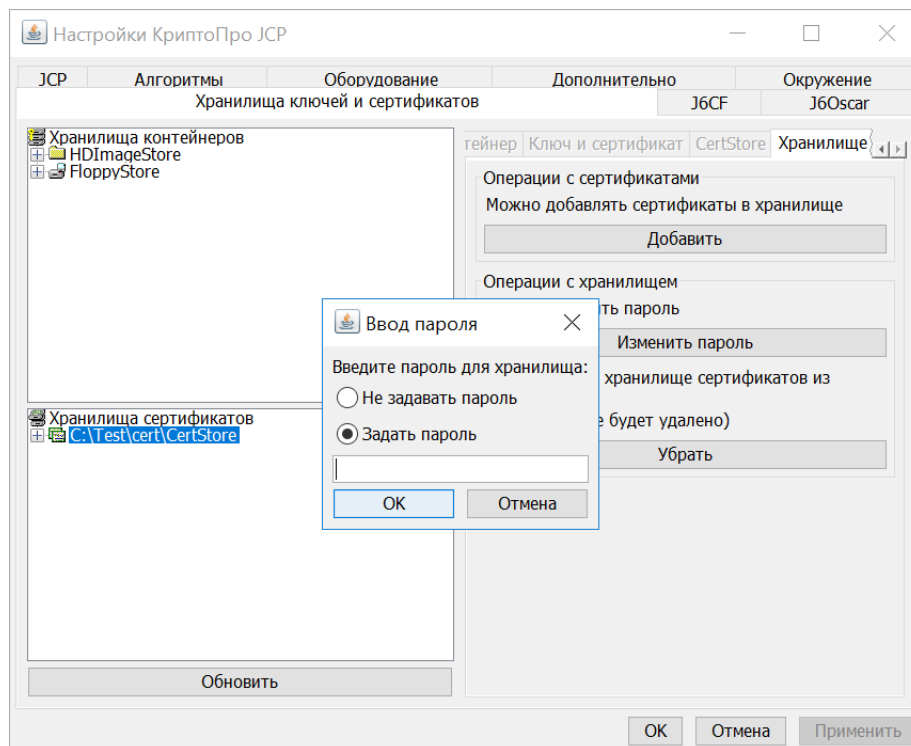
Рисунок 23. Вкладка **Хранилища ключей и сертификатов**

3.6.1 Работа с хранилищем контейнеров

При открытии панели дерева хранилищ и контейнеров находятся в свернутом состоянии, показаны только хранилища, установленные в системе. Двойной щелчок мыши или нажатие кнопки «Ввод» на любом из 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 (см. [рис. 24](#)).

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

Рисунок 24. Вкладка **Хранилища ключей и сертификатов**

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 или нажатия кнопки «Ввод». 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».

Если для контейнера или хранилища 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.

3.6.2 Создание контейнера. Работа с контейнером

При установке указателя на одно из хранилищ контейнеров доступно действие «Создать» контейнер (см. [рис. 25](#)).

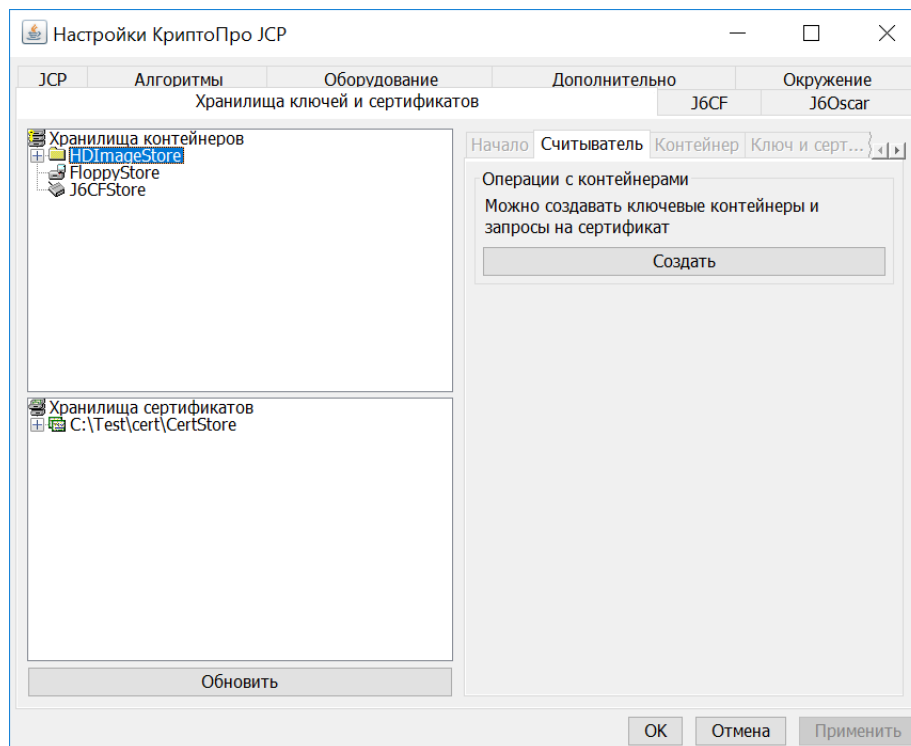
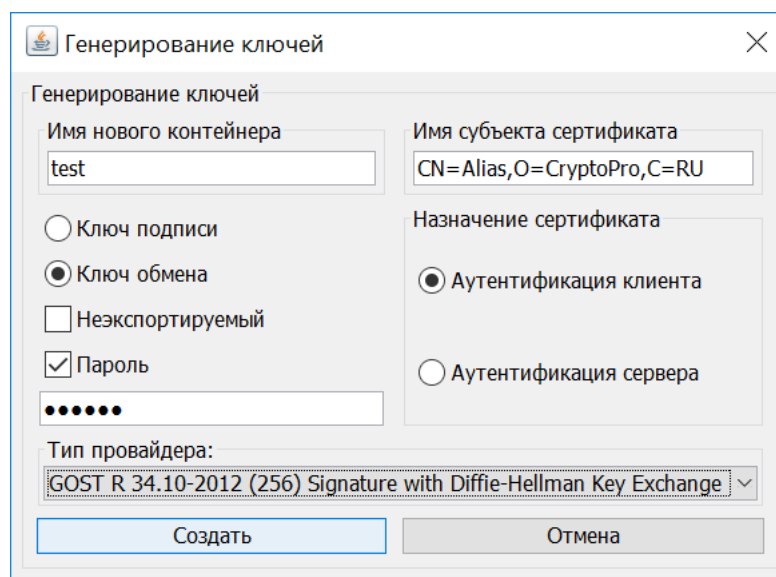
Рисунок 25. Вкладка **Хранилища ключей и сертификатов**, создание контейнера

Рисунок 26. Генерирование ключей и создание контейнера

Данная реализация позволяет получить ключ электронной подписи или обмена с самоподписанным сертификатом для аутентификации сервера или клиента.

В окне «Генерирование ключей» установите параметры создаваемых контейнера, ключей и сертификата:

- Укажите имя нового контейнера и имя субъекта сертификата. При совпадении имени создаваемого контейнера с именем уже существующего в хранилище контейнера будет выведено сообщение об ошибке.
- Выберите тип генерируемого ключа — Ключ подписи или Ключ обмена.



Примечание. Если создается ключ обмена, то перед созданием контейнера убедитесь, что провайдер Crypto установлен (имеется в папке запуска скрипта контрольной панели и передан в classpath), 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».

- При необходимости ключ может быть помечен как неэкспортируемый.
- Ключ можно сохранить без пароля или с паролем. Для сохранения ключа с паролем необходимо выбрать флаг «Пароль» и в соответствующее поле ввести пароль.
- Укажите имя субъекта и назначение сертификата.
- Выберите тип провайдера.

При нажатии кнопки «Создать» будет сгенерирован ключ и сертификат, и контейнер с указанным именем и паролем будет записан в текущее хранилище.

После этого появится окно диалога сохранения запроса на сертификат (см. [рис. 27](#)).

Сохраненный запрос можно использовать для получения сертификата на УЦ. Полученный на УЦ и сохраненный в файл сертификат можно в дальнейшем добавить в соответствующий контейнер (см. [рис. 29](#)). При выполнении данного действия осуществляется перезапись сертификата в контейнере. В контейнер можно также добавлять цепочку сертификатов (из файла *.p7b).

Рисунок 27. Запрос на сертификат

После создания контейнер будет добавлен в дерево хранилища контейнеров. При установке указателя на контейнер откроется вкладка объекта «Контейнер», в которой будут доступны следующие операции (см. [рис. 28](#)):

- копирование;
- удаление;
- изменение пароля;
- добавление ключа (доступна после открытия контейнера и ввода пароля в случае, когда в контейнере лежит один ключ).



Примечание. При добавлении нового ключа в существующий контейнер будет выведено окно «Генерирование ключей» (см. [рис. 25](#)), но с заполненным именем контейнера, типом ключа (подписи или обмена), паролем.

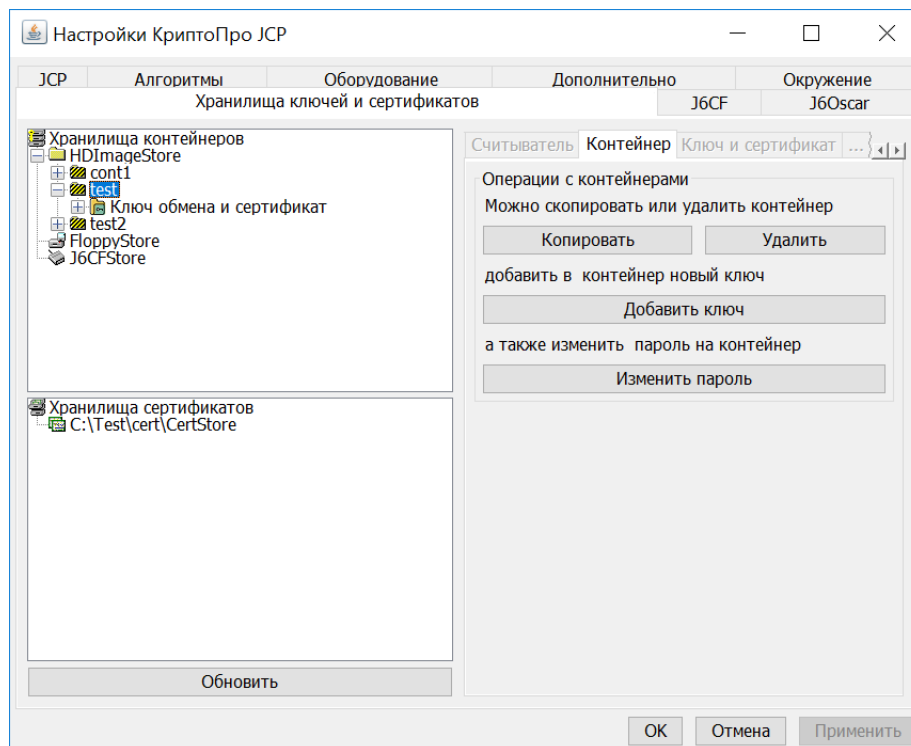


Рисунок 28. Вкладка **Хранилища ключей и сертификатов**, управление контейнером

В контейнере содержится один или два объекта «Ключ и сертификат». При этом в названии объекта указывается, какой ключ в нем содержится (ключ подписи или ключ обмена).

При установке указателя на объект «Ключ и сертификат» откроется вкладка, в которой будут доступны следующие операции (см. [рис. 29](#)):

- просмотр сертификата;
- копирование сертификата в хранилище сертификатов;
- построение цепочки (в выбранном хранилище сертификатов);
- добавление сертификата (или цепочки сертификатов);
- создание запроса на сертификат;
- просмотр информации о ключе в контейнере.

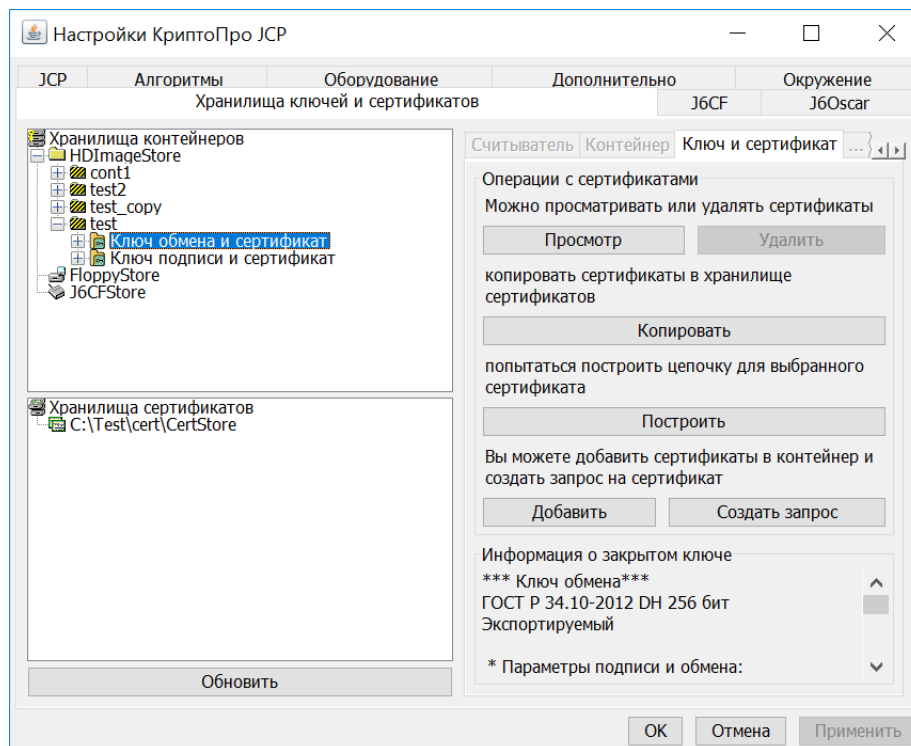


Рисунок 29. Вкладка **Хранилища ключей и сертификатов**, операции с сертификатом и ключом

При установке указателя на ключ в контейнере будет выведена информация о ключе (см. [рис. 30](#)). При установке указателя на сертификат в контейнере (см. [рис. 31](#)) доступны соответствующие операции с сертификатом, описанные выше.

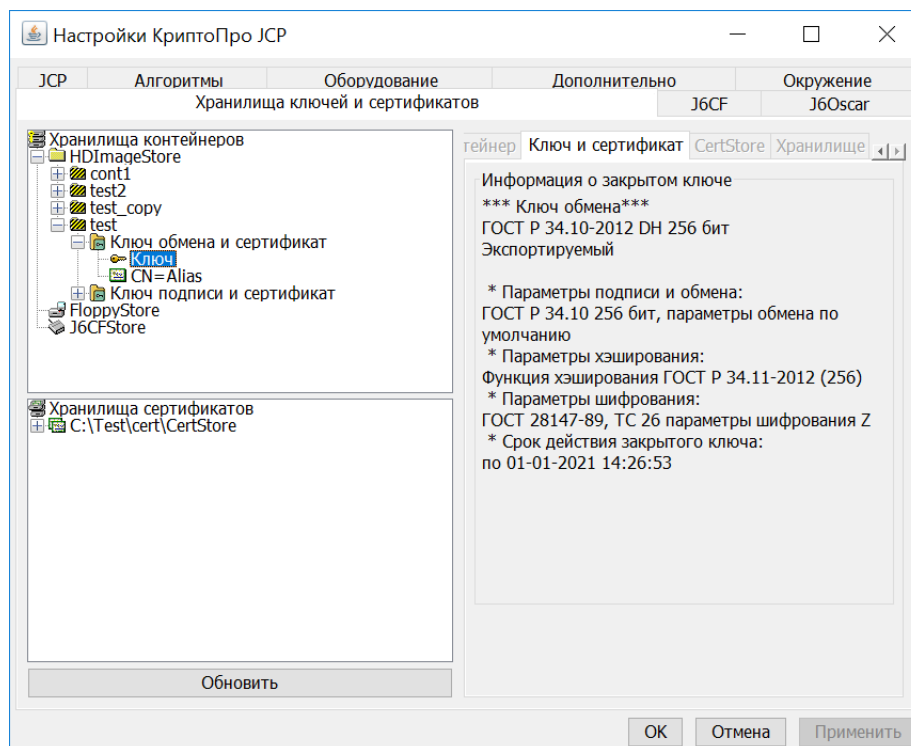


Рисунок 30. Вкладка **Хранилища ключей и сертификатов**, информация о ключе в контейнере

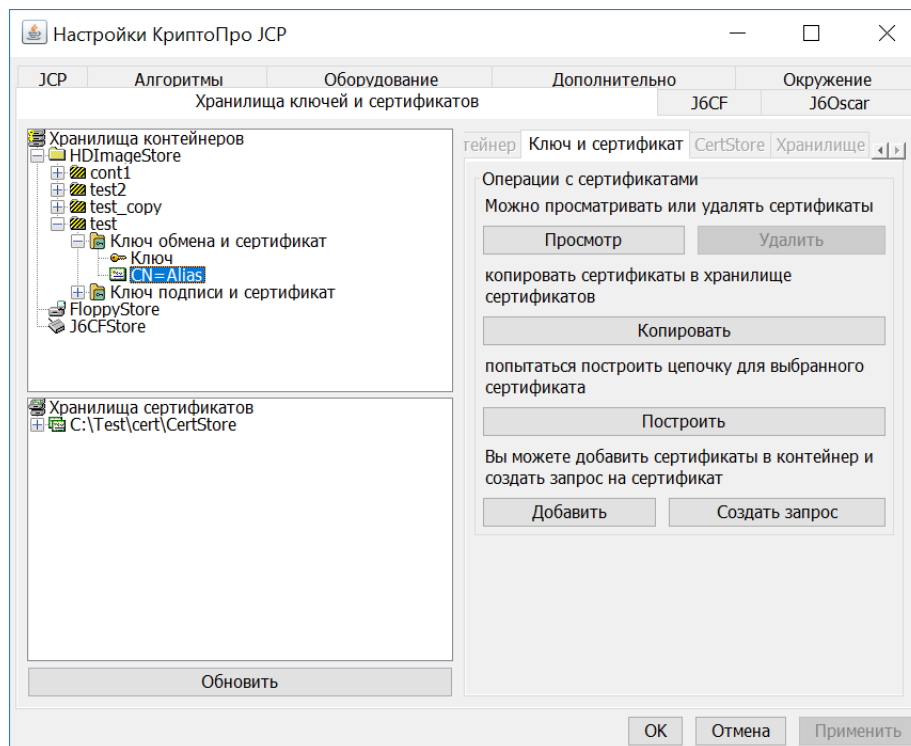


Рисунок 31. Вкладка **Хранилища ключей и сертификатов**, операции с сертификатом в контейнере

Сертификаты могут храниться в контейнерах (подробнее см. [рис. 31](#)) и в файловой части хранилища — хранилище сертификатов. Подробнее операции с сертификатом описаны в [Работа с сертификатами в хранилище](#).

3.6.3 Работа с хранилищем сертификатов

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.

При необходимости при открытии/создании хранилища возможно указать/установить пароль в соответствующем окне.

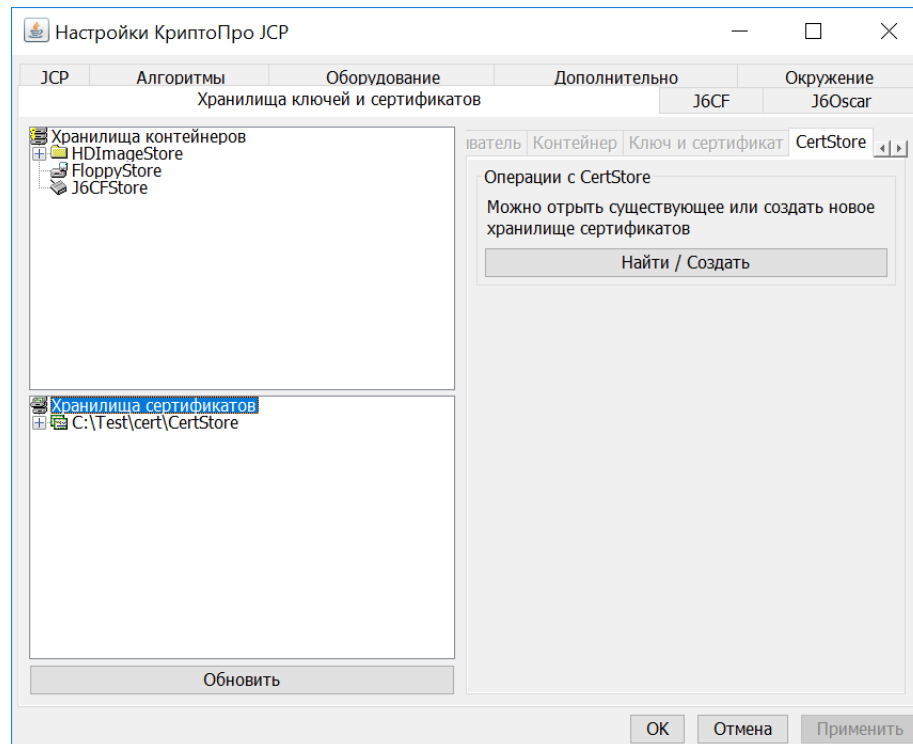


Рисунок 32. Вкладка **Хранилища ключей и сертификатов**, открытие/создание хранилища

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

При установлении указателя на хранилище сертификатов становятся доступны следующие операции (см. [рис. 33](#)):

- **Добавить** — добавление сертификатов в хранилище из файлов;
- **Изменить пароль** — изменение пароля хранилища;
- **Убрать** — удаление данного хранилища из списка отображения (файл хранилища не удаляется).

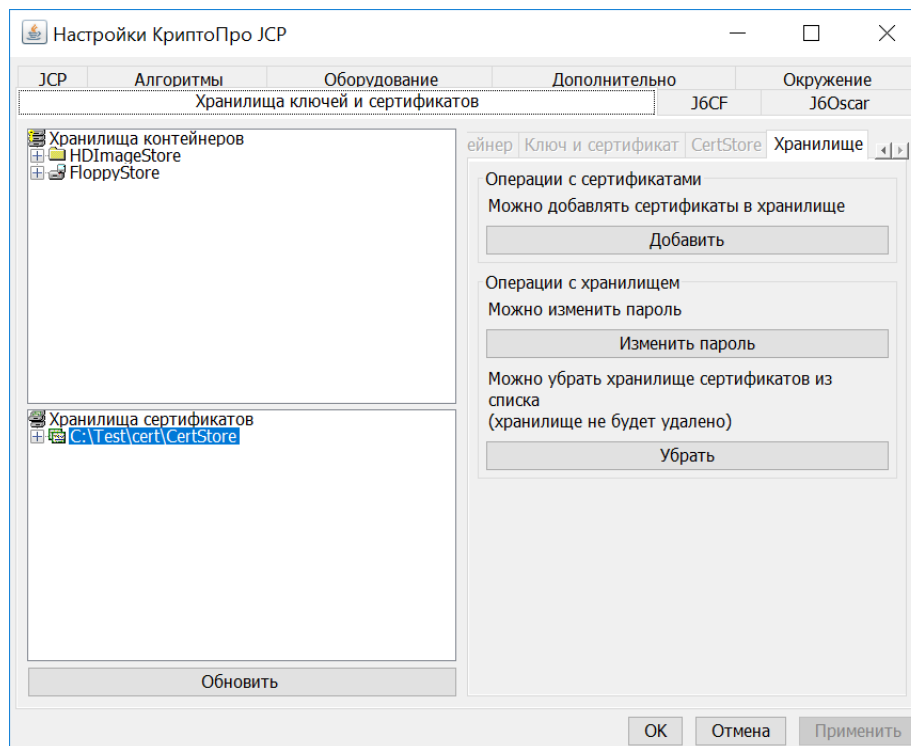


Рисунок 33. Вкладка **Хранилища ключей и сертификатов**, операции с хранилищем сертификатов

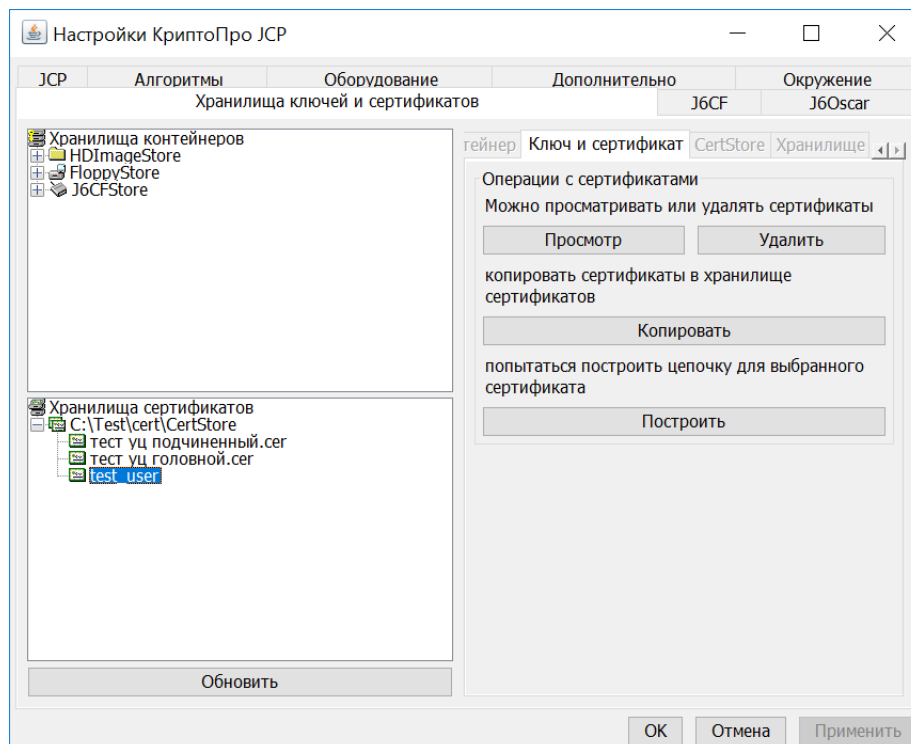
3.6.4 Работа с сертификатами в хранилище

При установке указателя на сертификат в хранилище сертификатов доступны операции (см. [рис. 34](#)):

- просмотр сертификата;
- удаления сертификата из хранилища;
- копирование сертификата в хранилище сертификатов;
- построение цепочки (в выбранном хранилище сертификатов).



Примечание. Операции удаления и копирования сертификата требуют ввода пароля на хранилище сертификатов.

Рисунок 34. Вкладка **Хранилища ключей и сертификатов**, операции с сертификатом

Сертификаты могут храниться в контейнерах (подробнее см. [рис. 31](#)) и в файловой части хранилища — хранилище сертификатов. В любом случае к ним может быть применена операция просмотра сертификата (кнопка «Просмотр»). Для сертификата будет выведено окно просмотра с тремя закладками: «Общая информация», «Подробно» и «Путь» (см. [рис. 35 — 37](#)).

Первая закладка содержит общую информацию о сертификате: действителен ли он, срок его действия, имя издателя и владельца. Вторая закладка содержит информацию о большинстве полей сертификата, представленных в виде списка, каждая строка которого — пара «Имя поля : Значение поля».

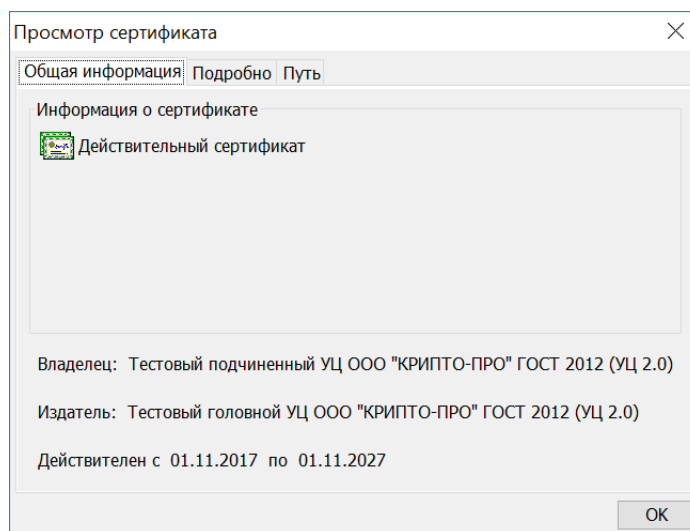


Рисунок 35. Общая информация о сертификате

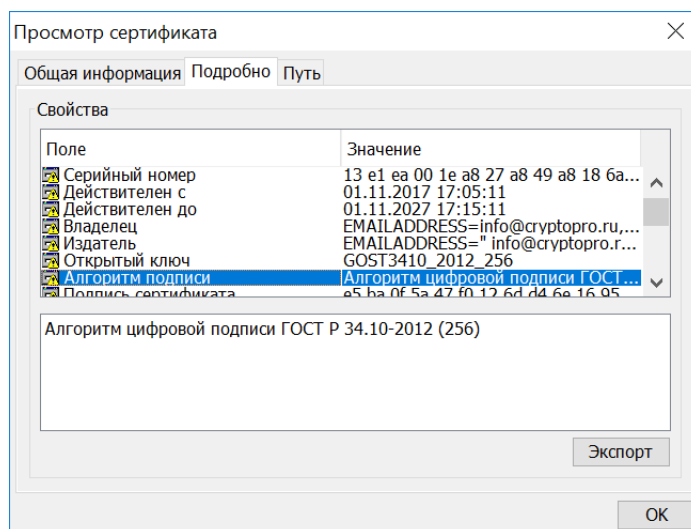


Рисунок 36. Поля сертификата

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 (см. [рис. 37](#)). 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 вкладке также есть возможно просмотреть полную информацию о любом из сертификатов в наборе, кроме конечного, выбрав его в окне и нажав кнопку «Просмотр». По кнопке «Сохранить цепочку в файл» можно сохранить цепочку сертификатов в файл формата CMS (*.p7b).

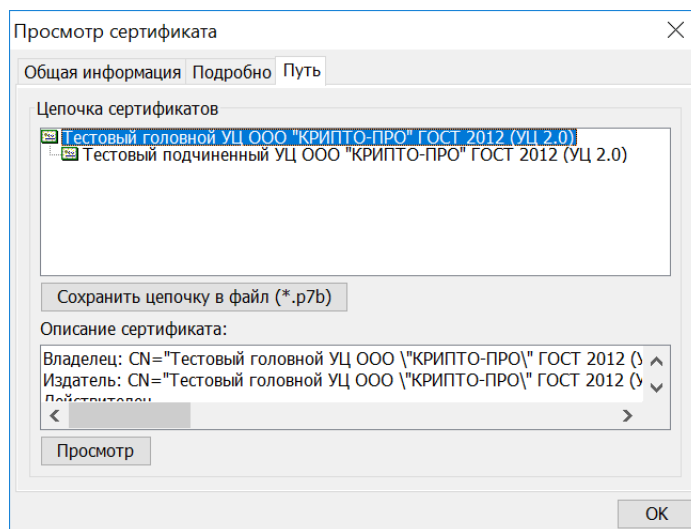


Рисунок 37. Цепочка сертификатов

3.6.5 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 (см. [рис. 38](#)). Затем производится копирование.

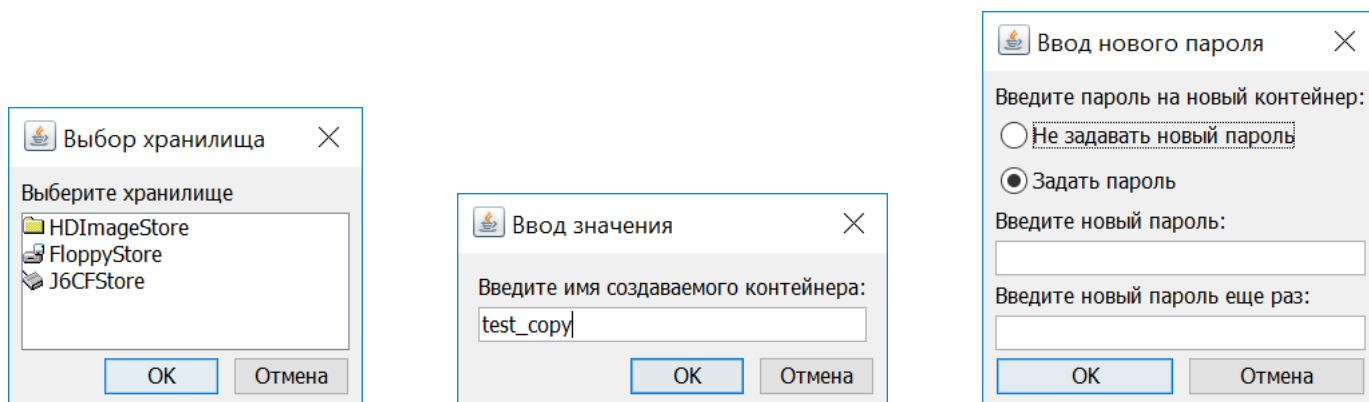


Рисунок 38. Копирование контейнера

Для сертификата копирование осуществляется в том же порядке, что и для контейнера, однако не запрашиваются старый и новый пароль (см. [рис. 39](#)).

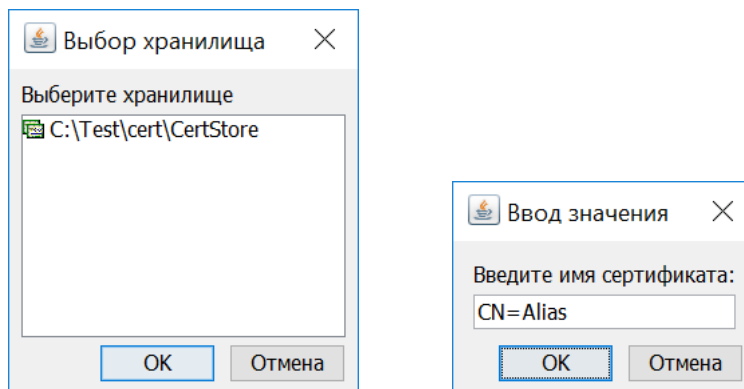


Рисунок 39. Копирование сертификата

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 (см. [рис. 40](#)). 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.

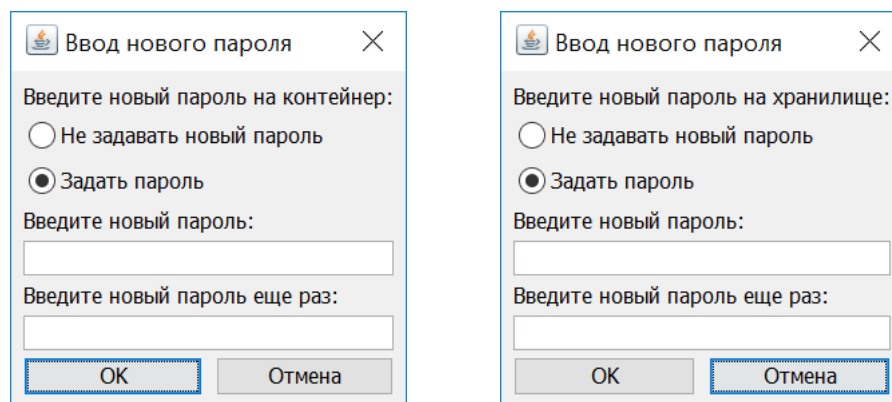


Рисунок 40. Изменение пароля контейнера/хранилища сертификатов

4 Настройка параметров провайдера с помощью Preferences

В некоторых случаях может потребоваться настройка КриптоПро JCP путем редактирования параметров провайдера, хранящихся в Preferences.

Доступ к ним преимущественно можно получить тремя способами:

1) программно, с помощью `Preferences.systemRoot()` или `Preferences.userRoot()`, перечисления путей к узлам и задания новых значений;

2) вручную, редактируя параметры в соответствующих разделах (`SOFTWARE\JavaSoft\Prefs\ru` или `SOFTWARE\Wow6432Node\JavaSoft\Prefs\ru` компьютера `HKEY_LOCAL_MACHINE` или пользователя `HKEY_CURRENT_USER`) реестра ОС Windows или файлы вида `prefs.xml` в соответствующих папках `.systemPrefs/ru` (например, `/etc/.java/.systemPrefs/ru`) или `.userPrefs (/home/user/.userPrefs/ru)` ОС *nix;

3) с помощью класса `ru.CryptoPro.JCP.Util.SetPrefs`, находящегося в модуле JCP и предоставляющего возможности для добавления и редактирования, например:

```
java ru.CryptoPro.JCP.Util.SetPrefs -user -node ru/CryptoPro/JCP -key JCP_any_param -value any_value
```

```
java u.CryptoPro.JCP.Util.SetPrefs -system -node ru/CryptoPro/JCP/Key -key JCP_any_param -value any_value
```



Примечание. Отмеченные параметры доступны только при использовании Java-машин версии 1.7 или 1.8.

Таблица 1. Основные параметры JCP

Описание	Путь	Ключ	Соответствует
Список установленных пакетов	<code>ru/CryptoPro</code>	<code>AbstractInstaller_class_Uninstall</code>	
Список закладок панели управления	<code>ru/CryptoPro/JCP/ControlPane</code>	<code>MainControlPaneConfig_class_Pages</code>	
Время ожидания закрытия окна с предупреждением о доступе к ключу, число секунд	<code>ru/CryptoPro/JCP/Key</code>	<code>userInputTimeout</code>	Закладка «Дополнительно», время ожидания ввода
Список классов доступных типов хранилищ (внутри пути — доступ к настройкам отдельных хранилищ)	<code>ru/CryptoPro/JCP/KeyStore</code>	<code>StoreConfig_class_Store</code>	
Номер провайдера по умолчанию, число (0 — JCP, 1 — Java CSP)	<code>ru/CryptoPro/JCP/Util</code>	<code>PaneDefaultProvider_class_default</code>	Закладка «Алгоритмы», провайдер по умолчанию
Управление усиленным контролем использования ключа, true или false	<code>ru/CryptoPro/JCP/tools/Control</code>	<code>StrengthenedKeyUsageControl</code>	Закладка «Дополнительно», включение усиленного контроля использования ключей
Параметры хеширования, шифрования, подписи	<code>ru/CryptoPro/JCP/params</code>		Закладка «Алгоритмы», параметры хеширования, шифрования, подписи

Путь к хранилищу Floppy	ru/CryptoPro/JCP/KeyStore/HDImage	FloppyStore_class_default	Закладка «Оборудование», путь к хранилищу Floppy
Путь к хранилищу HDImage	ru/CryptoPro/JCP/KeyStore/HDImage	HDImageStore_class_default	Закладка «Оборудование», путь к хранилищу HDImage
Скрипт для смены прав на папку ключей пользователя	ru/CryptoPro/JCP/KeyStore/HDImage	HDImageReader_Chmod_default	Закладка «Оборудование», скрипт для смены прав на папку ключей пользователя
Запрет отображения об использовании ключей ГОСТ Р 34.10-2001, true или false	ru/CryptoPro/JCP/tools	Gost2001Warning_class_default	Закладка «Оборудование», запрет отображения об использовании ключей ГОСТ Р 34.10-2001
Путь Unix Mutex для пользователя	ru/CryptoPro/JCP/tools	UnixMutex_class_pathToLocks	Закладка «Оборудование», путь Unix Mutex для пользователя
Поддерживаемые службы работы с носителями	ru/CryptoPro/JCP/KeyStore/J6CF	ConfigReader_class_Services	Закладка "J6CF", список поддерживаемых служб
Служба работы с носителями по умолчанию	ru/CryptoPro/JCP/KeyStore/J6CF	ConfigReader_class_Service	Закладка "J6CF", служба по умолчанию
Носитель, используемый по умолчанию	ru/CryptoPro/JCP/KeyStore/J6CF	ConfigReader_class_Reader	Закладка "J6CF", носитель, используемый по умолчанию
Время ожидания при работе с носителем	ru/CryptoPro/JCP/KeyStore/J6CF	ConfigReader_class_Timeout	Закладка "J6CF", время ожидания

5 Использование утилиты ComLine

Функциями провайдера можно воспользоваться с помощью готовых классов пакета **ComLine** из модуля Samples, входящего в состав КриптоПро JCP.

Запустите **ComLine** с вызовом нужного класса либо сам класс, используя следующие параметры командной строки.

В случае использования Java-машин версии 10 и выше:

```
java -cp * ComLine NameofClass args или java NameofClass args

например:

java -cp * ComLine KeyPairGen -alias name_of_key -dname CN=autor,OU=Security,O=CryptoPro,C=RU
-reqCertpath C:/req.txt

или

java -cp * KeyPairGen -alias name_of_key -dname CN=autor,OU=Security,O=CryptoPro,C=RU
-reqCertpath C:/req.txt
```

В случае использования Java-машин версии 1.7 или 1.8:

```
java ComLine NameofClass args или java NameofClass args

например:

java ComLine KeyPairGen -alias name_of_key -dname CN=autor,OU=Security,O=CryptoPro,C=RU
-reqCertpath C:/req.txt

или

java KeyPairGen -alias name_of_key -dname CN=autor,OU=Security,O=CryptoPro,C=RU -reqCertpath
C:/req.txt
```

5.1 Проверка установки и настроек провайдеров

Проверку установки и основных настроек провайдера можно осуществить запуском:

CheckConf (без параметров)

5.2 Проверка работоспособности провайдеров

Работоспособность провайдера можно проверить запуском:

CheckConfFull [-servDir C:/*.*)]

-servDir

рабочая директория (по умолчанию текущая)

Выполняются тесты на генерацию ключей, генерацию и проверку подписи, а также тесты на создание ssl-соединения (если установлен/настроен КриптоПро JavaTLS). (Запуск возможен при условии, что КриптоПро JCP версии 2.0 R4 был установлен/передан в classpath успешно).

5.3 Работа с ключами и сертификатами

5.3.1 Генерация ключевой пары и соответствующего ей самоподписанного сертификата. Запись их на носитель. Генерация запроса на сертификат и запись его в файл.

```
KeyPairGen -alias name_of_key [-alg GOST3410EL] [-storetype HDImageStore] [-storepath null]
[-storepass null] [-keypass password] [-isServer true] -dname CN=autor,OU=Security,O=CryptoPro,C=RU
-reqCertpath C:/*.* -encoding der
```

-alias	уникальное имя записываемого ключа
-alg	алгоритм для генерации (по умолчанию GOST3410EL)
-storetype	имя ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-storepath	путь к хранилищу доверенных сертификатов (по умолчанию null)
-storepass	пароль на хранилище доверенных сертификатов (по умолчанию null)
-keypass	пароль на записываемый ключ (по умолчанию null)
-isServer	если ключ серверный, то значение true (по умолчанию false)
-dname	имя субъекта для генерации самоподписанного сертификата
-encoding	кодировка (DER/BASE64) (по умолчанию DER)
-reqCertpath	путь для записи запроса

Полученные таким образом ключи можно использовать как для генерации ЭП, так и для обмена.

5.3.2 Получение сертификата из запроса. Запись сертификата в хранилище и в файл

```
getCert -alias name_of_key [-storetype HDImageStore] [-storepath null] [-storepass null] -http
http://www.cryptopro.ru/certsrv/ -certpath C:/*.* -reqCertpath C:/*.*
```

-alias	уникальное имя ключа
-storetype	имя ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-storepath	путь к хранилищу доверенных сертификатов (по умолчанию null)
-storepass	пароль на хранилище доверенных сертификатов (по умолчанию null)
-http	путь к центру сертификации

-reqCertpath	путь к файлу с запросом
-encoding	кодировка запроса (DER/BASE64) (по умолчанию DER)
-certpath	путь к файлу для записи сертификата

5.3.3 Построение цепочки сертификатов

```
Certs -alias name_of_key [-storetype HDImageStore] [-storepath null] [-storepass null] [keypass password] -certs C:/my.cer,C:/*.*cer,...,C:/root.cer
```

-alias	уникальное имя ключа
-keypass	пароль на ключ (по умолчанию null)
-storetype	имя ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-storepath	путь к хранилищу доверенных сертификатов (по умолчанию null)
-storepass	пароль на хранилище доверенных сертификатов (по умолчанию null)
-certs	пути к сертификатам

5.3.4 Формирование электронной подписи

```
Signature -alias name_of_key [-storetype HDImageStore] [-storepath null] [-storepass null] [-keypass password] -signpath C:/*.* -filepath C:/*.*
```

-alias	уникальное имя ключа
-keypass	пароль на записываемый ключ (по умолчанию null)
-storetype	имя ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-storepath	путь к хранилищу доверенных сертификатов (по умолчанию null)
-storepass	пароль на хранилище доверенных сертификатов (по умолчанию null)
-signpath	путь к файлу подписи
-filepath	путь к подписываемому файлу

5.3.5 Проверка электронной подписи

```
SignatureVerif -alias name_of_key [-storetype HDImageStore] [-storepath null] [-storepass null]  
-signpath C:/*.* -filepath C:/*.*
```

-alias	уникальное имя ключа
-keypass	пароль на записываемый ключ (по умолчанию null)
-storetype	имя ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-storepath	путь к хранилищу доверенных сертификатов (по умолчанию null)
-storepass	пароль на хранилище доверенных сертификатов (по умолчанию null)
-signpath	путь к файлу подписи
-filepath	путь к подписываемому файлу

5.4 Использование КриптоПро JavaTLS

5.4.1 Запуск сервера из командной строки

```
Server [-port port] [-auth true] [-keyStoreType HDImageStore] [-trustStoreType HDImageStore]  
-trustStorePath C:/*.* -trustStorePassword trust_pass -keyStorePassword key_pass
```

-port	порт сервера (по умолчанию 443)
-auth	нужна ли аутентификация клиента (по умолчанию false)
-keyStoreType	тип ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-trustStoreType	тип носителя для хранилища доверенных сертификатов HDImageStore (жесткий диск), FloppyStore (дискета) (по умолчанию HDImageStore)
-trustStorePath	путь к хранилищу доверенных сертификатов
-trustStorePassword	пароль на хранилище доверенных сертификатов
-keyStorePassword	пароль на ключ
-servDir	рабочая директория сервера (по умолчанию текущая)

При запросе ресурса shutdown сервер останавливается, предварительно послав клиенту ответ, который содержит сообщение об остановке сервера по окончании сессии.

5.4.2 Запуск клиента из командной строки

```
Client [-port port] [-server serverName] [-keyStoreType HDImageStore] [-trustStoreType  
HDImageStore] -trustStorePath C:/*.* -trustStorePassword trust_pass -keyStorePassword key_pass  
[-fileget gettingFileName] [-fileout outputFilePath]
```

-port	порт сервера (по умолчанию 443)
-server	имя сервера (по умолчанию localhost)
-keyStoreType	тип ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-trustStoreType	тип носителя для хранилища доверенных сертификатов HDImageStore (жесткий диск), FloppyStore (дискета) (по умолчанию HDImageStore)
-trustStorePath	путь к хранилищу доверенных сертификатов
-trustStorePassword	пароль на хранилище доверенных сертификатов
-keyStorePassword	пароль на ключ
-fileget	имя ресурса (по умолчанию index.html)
-fileout	путь к файлу вывода (по умолчанию out.html)

5.4.3 Запуск клиента нагрузочного примера из командной строки

Нагрузочный пример содержится в samples.jar/JTLS_samples/HighLoadExample.

```
JTLS_samples.HighLoadExample -client [-port hostPort] [-host hostName] [-get sourcePage] [-t T]  
[-n N] -source sourceDir -store tempDir -trustStorePath C:/*.* [-trustStoreType trust_type]  
-trustStorePassword trust_pass [-keyStoreType keystoreType] [-keyStorePassword key_pass] [-ct X]  
[-external] [-apache4] [-trace] [-help]
```

При выполнении команды, возможно, потребуется указать параметры -Dcom.sun.security.enableCRLDP=true и -Dcom.ibm.security.enableCRLDP=true для осуществления проверки цепочки сертификатов online.

-port	порт сервера (по умолчанию 443)
-host	имя сервера (по умолчанию 127.0.0.1)
-get	имя загружаемого ресурса (по умолчанию default.htm)
-t	количество потоков (подключений) (по умолчанию 2)
-n	количество запросов на поток (подключение) (по умолчанию 2)
-source	папка с ресурсами для передачи сервером клиенту (пока не используется)

-store	папка для сохранения загружаемого ресурса
-trustStorePath	путь к хранилищу доверенных сертификатов
-trustStoreType	тип носителя для хранилища доверенных сертификатов HDImageStore (жесткий диск), FloppyStore (дискета) (по умолчанию HDImageStore)
-trustStorePassword	пароль на хранилище доверенных сертификатов
-keyStoreType	тип ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-keyStorePassword	пароль на ключ
-ct	таймаут работы потока клиента (сек.) (по умолчанию 5 мин.)
-external	означает подключение к "внешнему"(не созданному в этом же примере) серверу
-apache4	означает использование Apache HttpClient 4.x вместо внутреннего класса Client. Библиотеки apache должны быть в каталоге lib/ext (classpath)
-trace	означает подробный вывод в консоль
-help	информация о том, какие команды можно использовать

5.4.4 Запуск клиента на основе apache http client 4.x из командной строки

Пример содержится в samples.jar/JTLS_samples/ApacheHttpClient4XExample.

```
JTLS_samples.ApacheHttpClient4XExample [-port hostPort] [-host hostName] [-get sourcePage]
[-allow] [-auth] [-save path] -trustStorePath C:/*. * [-trustStoreType trust_type]
-trustStorePassword trust_pass [-keyStoreType keystoreType] [-keyStorePassword key_pass] [-help]
```

При выполнении команды, возможно, потребуется указать параметры -Dcom.sun.security.enableCRLDP=true и -Dcom.ibm.security.enableCRLDP=true для осуществления проверки цепочки сертификатов online.

-port	порт сервера (по умолчанию 443)
-host	имя сервера (по умолчанию 127.0.0.1)
-get	имя загружаемого ресурса (по умолчанию default.htm)
-save	полный путь для сохранения загруженного ресурса
-allow	для отключения проверки соответствия адреса ресурса и CN серверного сертификата
-auth	указывает на необходимость клиентской аутентификации

-trustStorePath	путь к хранилищу доверенных сертификатов
-trustStoreType	тип носителя для хранилища доверенных сертификатов HDImageStore (жесткий диск), FloppyStore (дискета) (по умолчанию HDImageStore)
-trustStorePassword	пароль на хранилище доверенных сертификатов
-keyStoreType	тип ключевого носителя HDImageStore (жесткий диск), FloppyStore (дискета), RutokenStore или J6CFStore (смарт-карты и токены) (по умолчанию HDImageStore)
-keyStorePassword	пароль на ключ
-help	информация о том, какие команды можно использовать