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

КРИПТОПРО

# Средство Криптографической Защиты Информации

# КриптоПро CSP

## Версия 5.0 KC1

Инструкция по использованию JavaCSP

ЖТЯИ.00101-01 92 04
Листов 24

2019 г

# Содержание

**Список сокращений** . . . . . **4**

**1 Установка КриптоПро JavaCSP** . . . . . **5**
1.1 Способы установки . . . . . 5
1.2 Кодировки в Java . . . . . 5
1.3 Установка на Windows . . . . . 5
1.3.1 Установка с помощью графического инсталлятора . . . . . 6
1.3.2 Установка с помощью командной строки . . . . . 12
1.4 Установка на UNIX и Mac OS . . . . . 13
1.5 Локальная установка вызовом Java . . . . . 14
1.6 Проверка и ввод лицензии . . . . . 15
1.7 Политики безопасности . . . . . 16
1.7.1 Права доступа для JCSP.jar . . . . . 16
1.7.2 Права доступа для администратора JavaCSP . . . . . 17
1.7.3 Права доступа для приложений . . . . . 17
1.7.4 Права доступа пользователя . . . . . 17

**2 Контрольная панель** . . . . . **18**
2.1 Закладка «Java CSP» . . . . . 18
2.2 Закладка «Настройки Java CSP» . . . . . 19
2.3 Закладка «Алгоритмы» . . . . . 20
2.4 Закладка «Хранилища ключей и сертификатов» . . . . . 22

**3 Настройка параметров провайдера с помощью Preferences** . . . . . **24**

# 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 |
| 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 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 |

# 1 Установка КриптоПро JavaCSP

## 1.1 Способы установки

Перед тем, как приступить к установке КриптоПро JavaCSP, необходимо установить криптопровайдер JCP. Основной способ установки КриптоПро JavaCSP состоит в запуске командного файла, входящего в состав дистрибутива КриптоПро JCP; имя командного файла зависит от операционной системы, на которую производится установка. Другие способы — это установка отдельно модуля JavaCSP с помощью установщика JCSPInstaller или с помощью опции -jar программы java.

В системе уже может быть установлен КриптоПро JavaCSP более ранней версии. В этом случае модуль КриптоПро JavaCSP может быть обновлен согласно инструкциям, приведенным ниже. Следует учитывать, что между версиями продуктов могут быть существенные отличия, в этом случае перед установкой КриптоПро JavaCSP необходимо предварительно удалить предыдущую версию продукта.

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

## 1.2 Кодировки в Java

При запуске классов КриптоПро JavaCSP 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 JavaCSP 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 на Windows

Установка КриптоПро JavaCSP должна проводиться администратором с помощью командной строки из папки с инсталлятором:

```
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 JavaCSP, что может быть необходимо при разрешении ошибочных ситуаций. В любом случае, перед установкой автоматически осуществляется попытка деинсталляции КриптоПро JavaCSP 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 КриптоПро JCP, в ней необходимо перейти на вкладку **Java CSP**. При необходимости введите лицензию, как это описано в разделе Контрольная панель.

В связи с возможностью одновременного сосуществования нескольких JRE на одном компьютере необходимо следить за тем, чтобы установка, удаление и использование КриптоПро JavaCSP 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 с помощью графического инсталлятора

Установка модуля КриптоПро JavaCSP вместе с нативной библиотекой может также может быть выполнена с помощью графического установщика `setup.exe`, как отдельного компонента КриптоПро JCP. Запуск `setup.exe` должен производиться под управлением учетной записи администратора.

Пошаговый процесс установки КриптоПро JavaCSP с помощью графического установщика представлен на рис. 1 — 3.

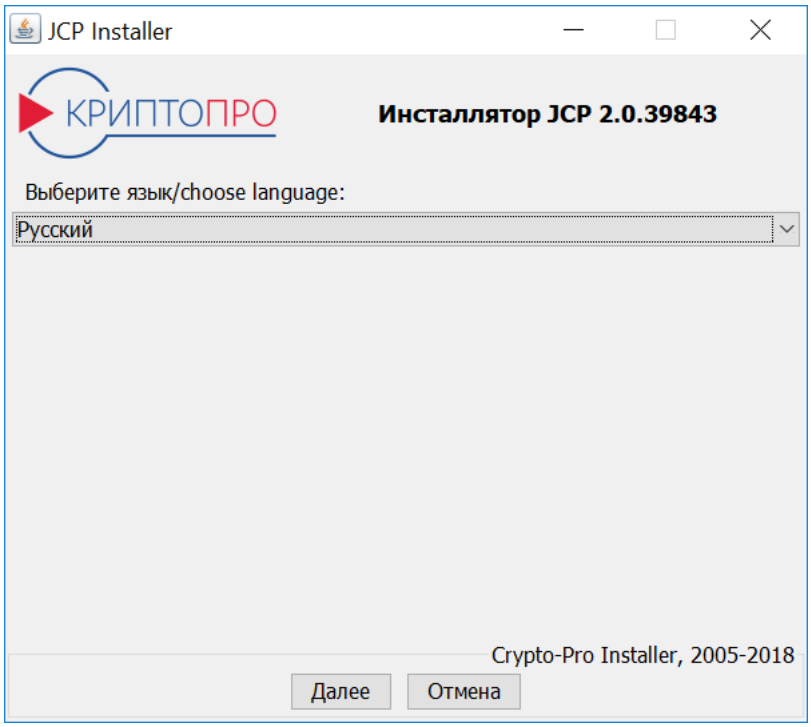


Рисунок 1. Окно выбора языка инсталлятора

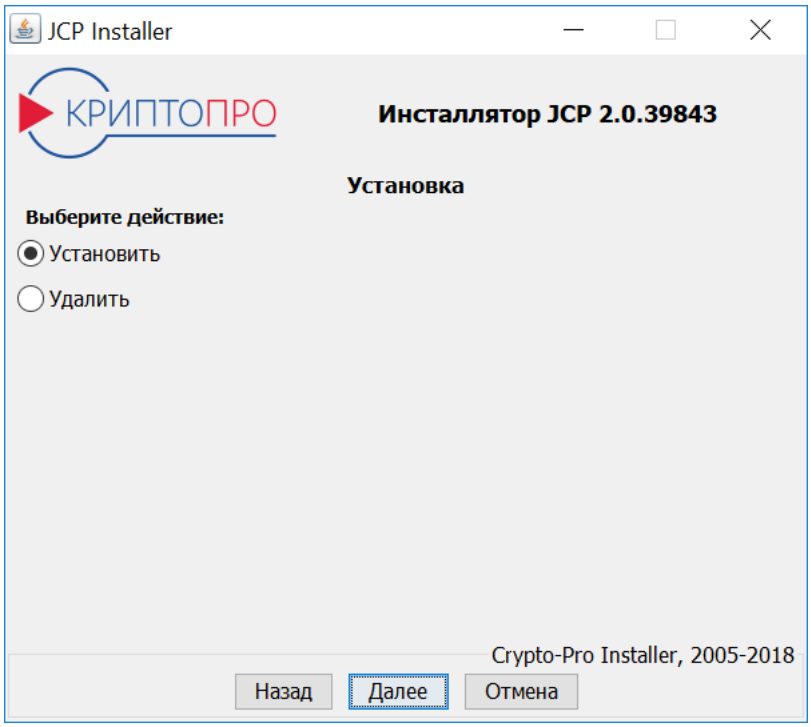


Рисунок 2. Окно выбора действия

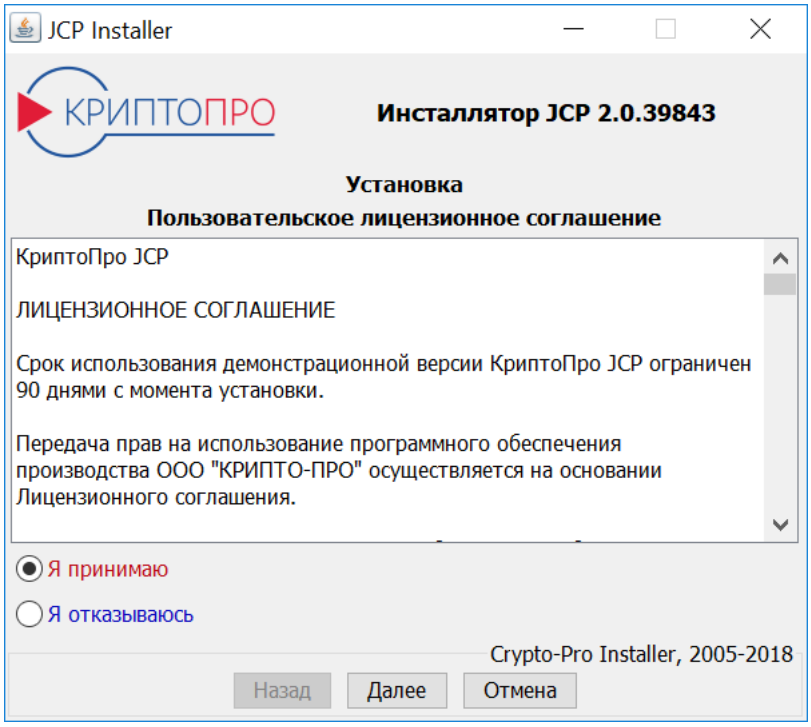


Рисунок 3. Окно с лицензионным соглашением

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).

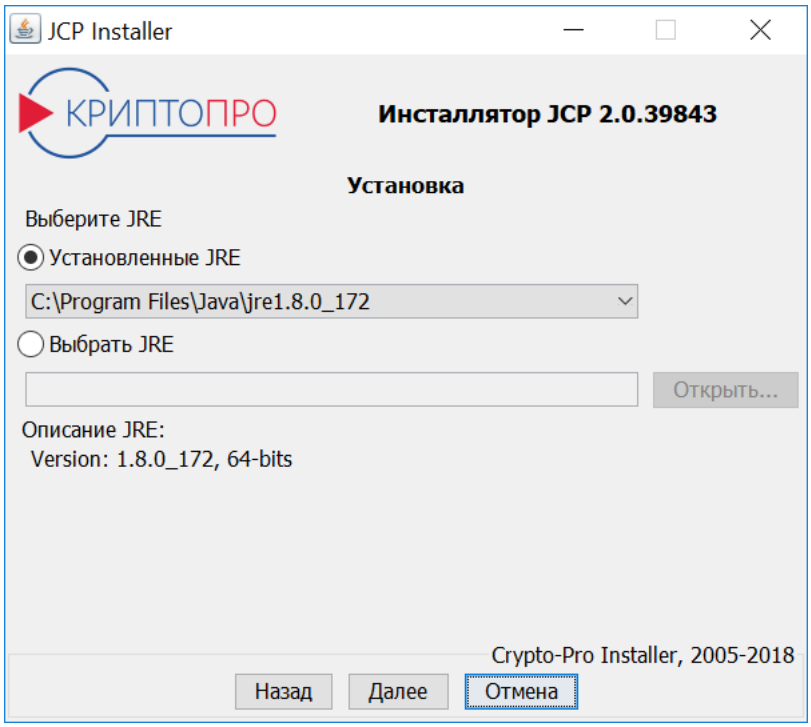


Рисунок 4. Окно выбора JRE

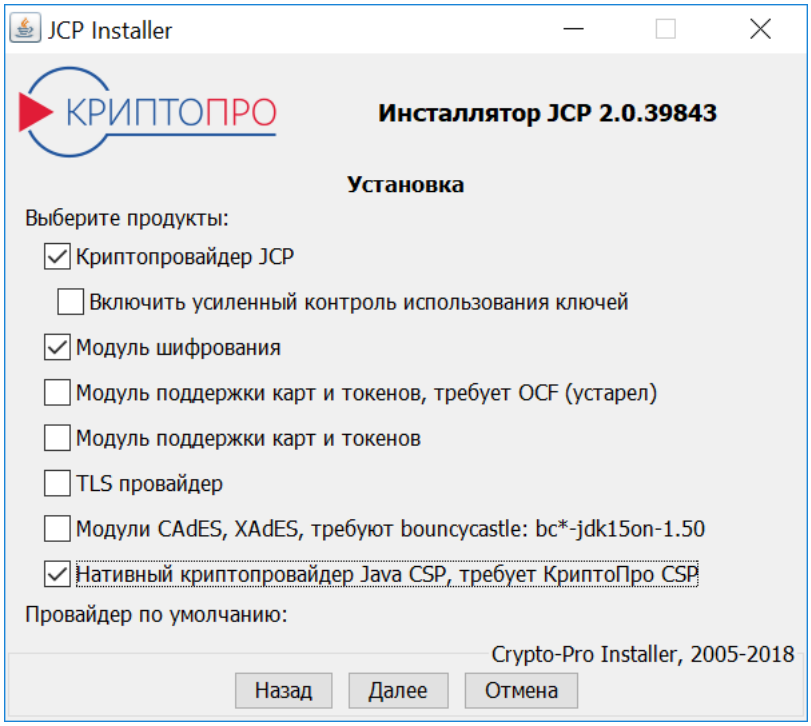


Рисунок 5. Окно выбора продукта

При установке провайдера можно указать, какой из них будет использоваться по умолчанию. В дальнейшем это настройку можно изменить в панели JCP на закладке «Алгоритмы». В зависимости от приоритета тот или иной провайдер (JCP или JavaCSP) будет находиться выше в списке провайдеров `java.security`.

**Примечание.** 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`.

С помощью пункта «Установить» может быть произведена как установка, так и обновление модулей. Если в указанной JRE уже имеется установленный JCP и другие модули (в том числе JavaCSP), 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.

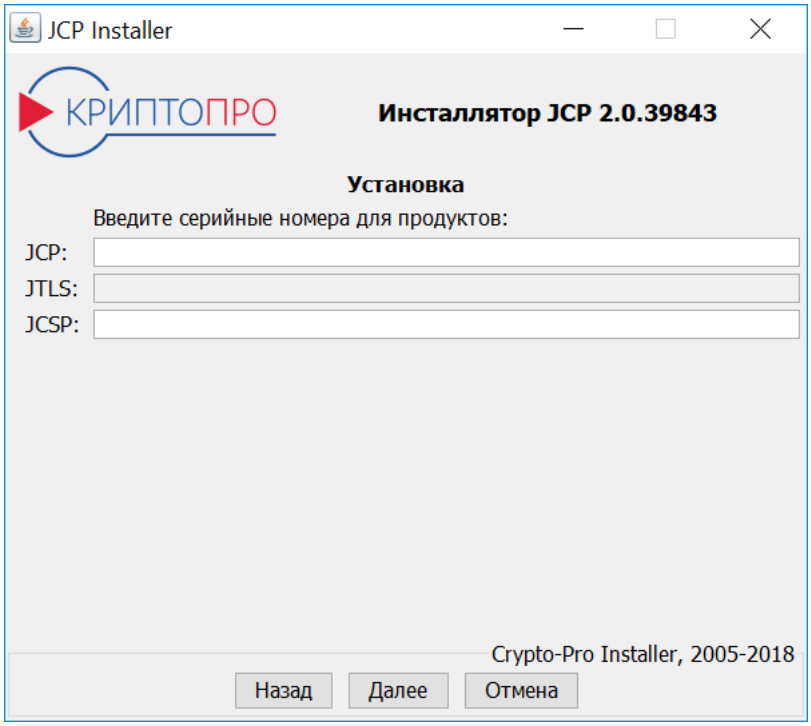


Рисунок 6. Окно ввода серийных номеров продуктов

Далее будет предложено проверить корректность введенной ранее информации, удаление настроек (в случае удаления модулей) (см. рис. 7).

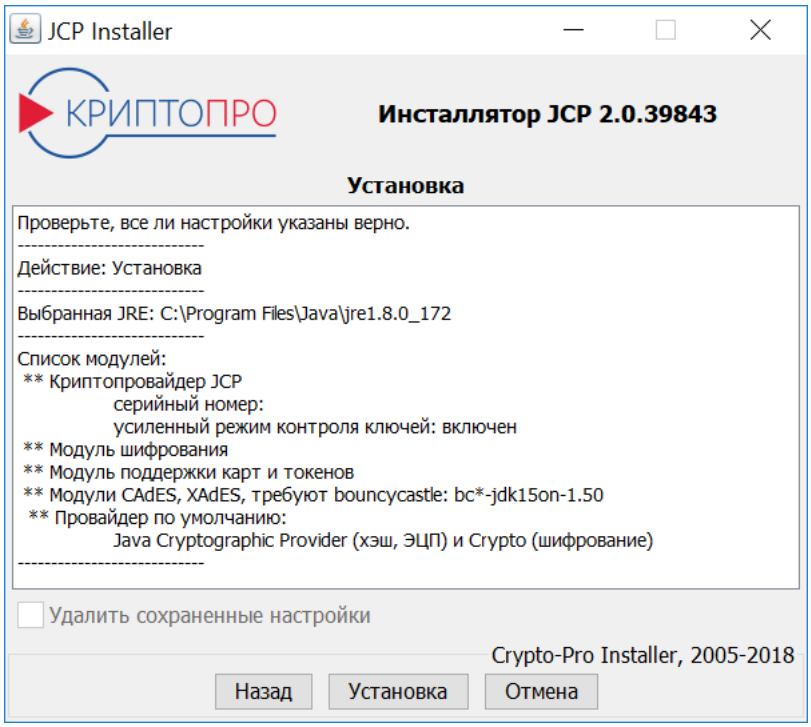


Рисунок 7. Окно проверки настроек установки/удаления

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

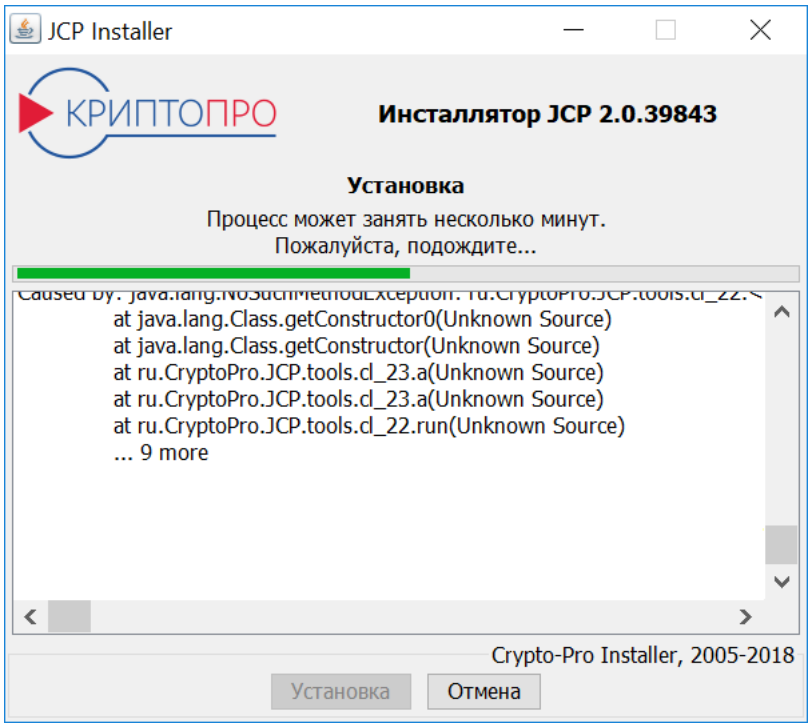


Рисунок 8. Окно процесса установки

В случае успешного выполнения установки будет отображено окно (см. рис. 9). После перехода далее в случае установки может быть предложено запустить панель управления JCP и создать ярлык для запуска Контрольной панели JCP на Рабочем столе (см. рис. 10).

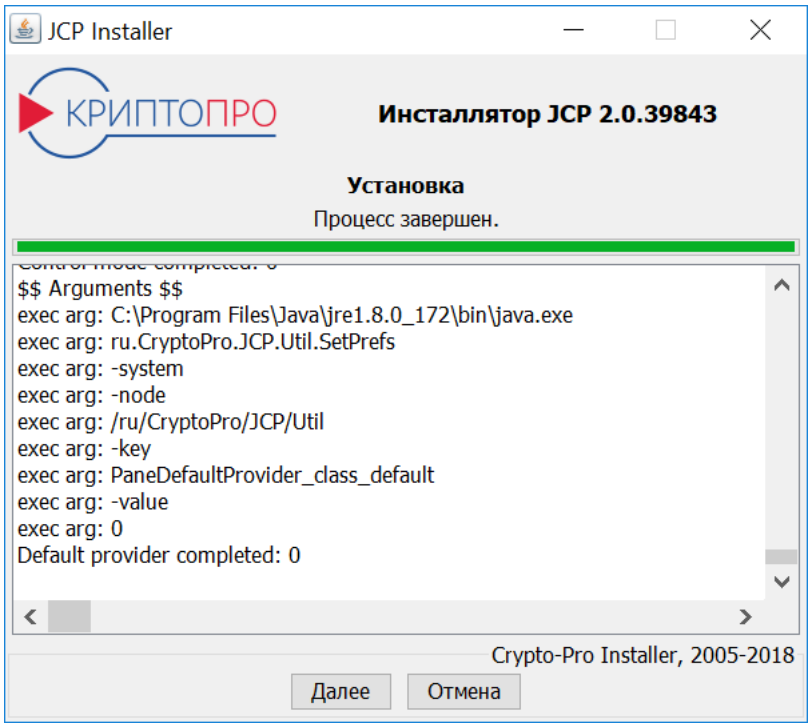


Рисунок 9. Окно с результатами установки

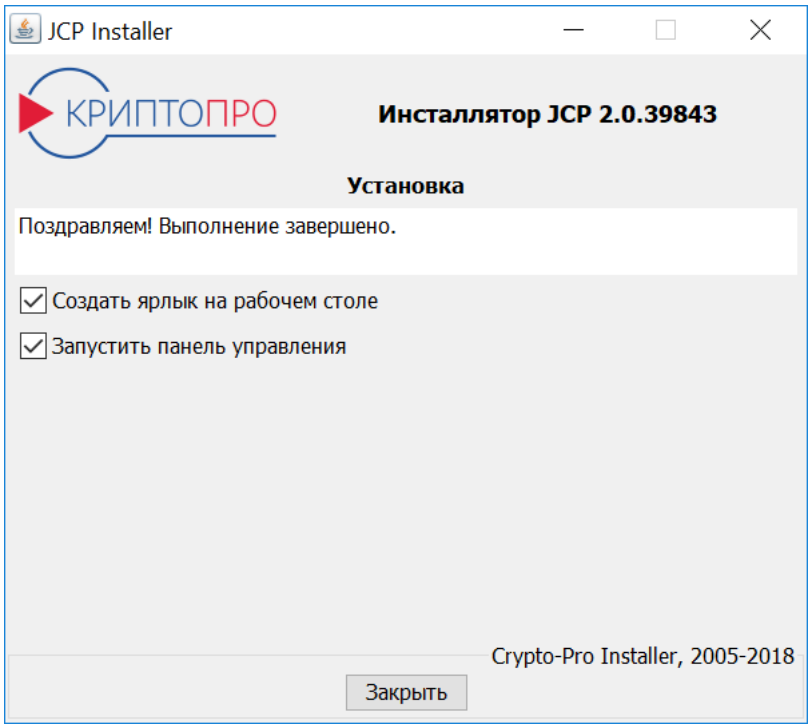


Рисунок 10. Завершение установки

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 JCP не удается (например, файлы заняты другим процессом), будет предложено перезапустить установщик (см. рис. 8).

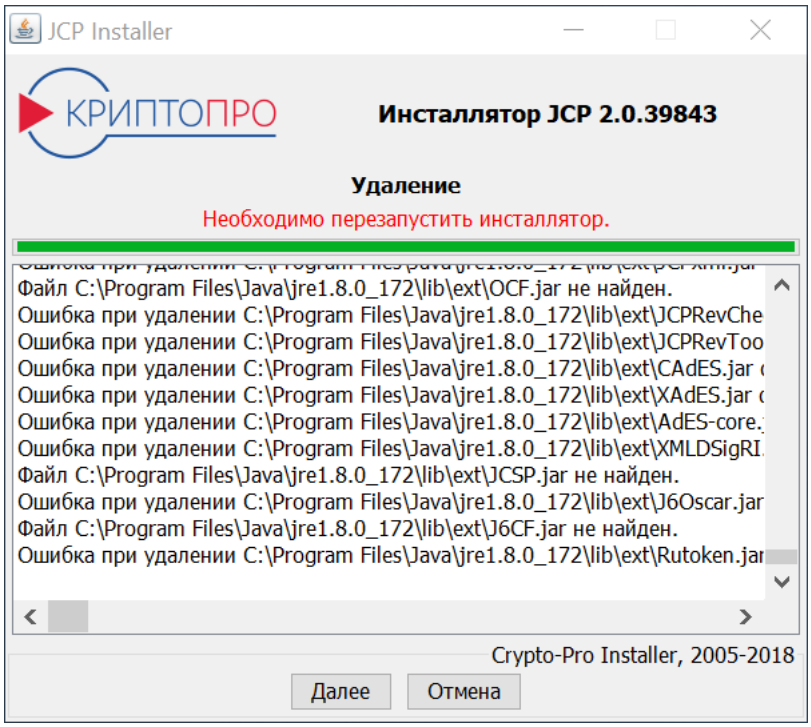


Рисунок 11. Ошибка при удалении компонентов

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

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,
- [-serial_jcp <value> -serial_cpssl <value> -serial_jcsp <value>] — серийные номера для выбранных продуктов,
- [-default_provider [0 | 1]] — провайдер по умолчанию (0 — JCP, 1 – JavaCSP),
- [-rmsetting] — удаление существующих настроек (только при удалении модулей).

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

**Примеры команд:**

1) установка JCP (с модулем шифрования), cpSSL и CAdES в `C:\Program Files\Java\jre7` с указанием серийного номера для JCP:

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

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

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

3) дополнительная установка к уже установленному 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

Установка КриптоПро JavaCSP на UNIX осуществляется аналогично установке КриптоПро JavaCSP на Windows, с разницей лишь в исполняемых файлах для установки и запуска контрольной панели КриптоПро JCP.

Для **установки** КриптоПро JavaCSP необходимо выполнить команду:

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

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

**Удаление** КриптоПро JavaCSP осуществляется одновременно с удалением КриптоПро JCP, для чего 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 JavaCSP должна осуществляться администратором. Права, необходимые для установки JCP, 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

При установке КриптоПро JavaCSP 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, 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 JCSP.jar ru.CryptoPro.JCSP.JCSPInstaller
```

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 JavaCSP с компьютера. При обновлении версии КриптоПро JavaCSP, 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 JavaCSP необходимо запустить:

```
java -classpath JCSP.jar ru.CryptoPro.JCSP.JCSPInstaller -install
```

При установке пакета JavaCSP 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 JavaCSP необходимо запустить класс вариант установки с опцией -uninstall, например следующим образом:

```
java ru.CryptoPro.JCSP.JCSPInstaller -uninstall -skipfiles delfiles.lst
```

После завершения процесса удаления JavaCSP, необходимо удалить все файлы имена которых находятся в списке `delfiles.lst`. Также необходимо удалить библиотеку `cspjni`.

## 1.6 Проверка и ввод лицензии

Для работы с лицензией можно использовать контрольную панель (закладка **Java CSP**) или командную строку (класс `ru.CryptoPro.JCSP.JCSPLicense`).

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

```
ru.CryptoPro.JCSP.JCSPLicense -required
```

Ввод лицензии осуществляется вызовом класса `ru.CryptoPro.JCSP.JCSPLicense` с параметрами:

```
ru.CryptoPro.JCSP.JCSPLicense -serial "serial_number" -company "company_name" -store
```

Также можно проверить заданную лицензию без ее установки:

```
ru.CryptoPro.JCSP.JCSPLicense -serial "serial_number" -company "company_name"
```

Вызов класса `ru.CryptoPro.JCSP.JCSPLicense` без параметров проверит установленную лицензию.

Дату первой установки можно узнать с помощью команды:

```
ru.CryptoPro.JCSP.JCSPLicense -first
```

Для вывода справки:

`ru.CryptoPro.JCSP.JCSPLicense ?`

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

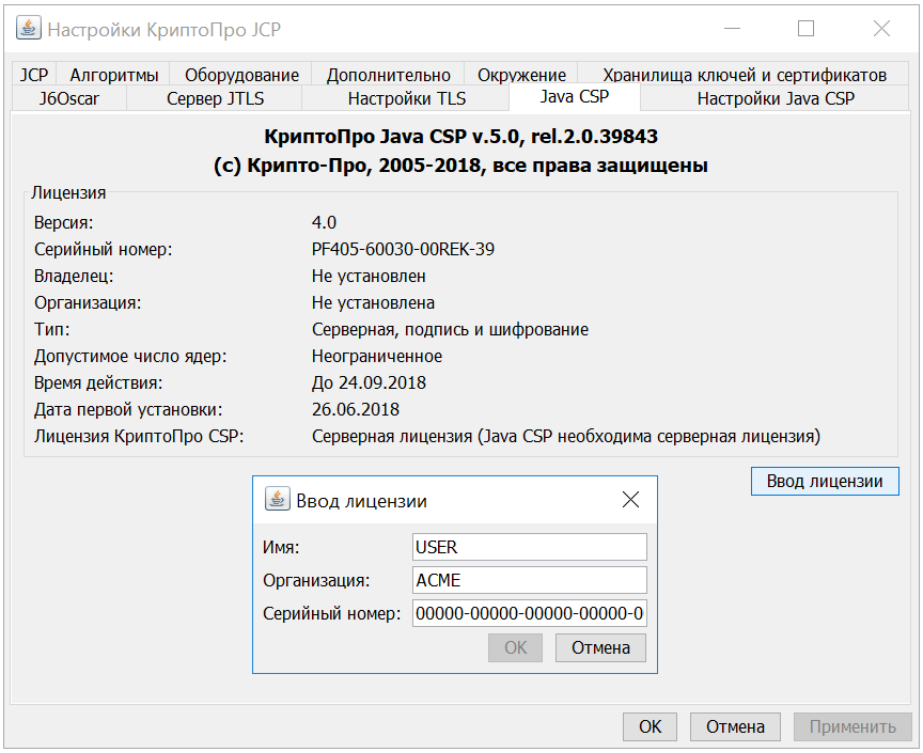


Рисунок 12. Ввод лицензии

## 1.7 Политики безопасности

Политики безопасности описываются в файле `${java.home}/lib/security/java.policy`

### 1.7.1 Права доступа для JCSP.jar

КриптоПро JavaCSP 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 JCSP.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";

};
```

где:

<usedProperty> — Property, используемые при настройке каких-либо путей.

### 1.7.2 Права доступа для администратора JavaCSP

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/S/P.

### 1.7.3 Права доступа для приложений

Установленные на виртуальную машину Java приложения не должны иметь доступ к ключам. Для этого все приложения, установленные на виртуальную машину Java, 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 также к смарт-карте и дискете) или устанавливать в этот каталог только приложения производителей, полученные доверенным способом.

### 1.7.4 Права доступа пользователя

Пользователь JavaCSP 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/S/P;

• 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.

# 2 Контрольная панель

КриптоПро JavaCSP не имеет собственной контрольной панели. Он добавляет собственные закладки **Java CSP** и **Настройки Java CSP** на контрольную панель JCP. В данном разделе приводится описание закладок КриптоПро JavaCSP, которые являются инструментом, позволяющим устанавливать и изменять лицензию криптопровайдера, параметры криптопровайдера и криптоалгоритмов.

Для запуска контрольной панели в Windows используйте:

```
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 используемой Вами системе способом.

## 2.1 Закладка «Java CSP»

Закладка **Java CSP** (см. рис. 13) предназначена для просмотра информации о текущей лицензии на использование криптопровайдера КриптоПро JavaCSP, а также для установки новой лицензии.

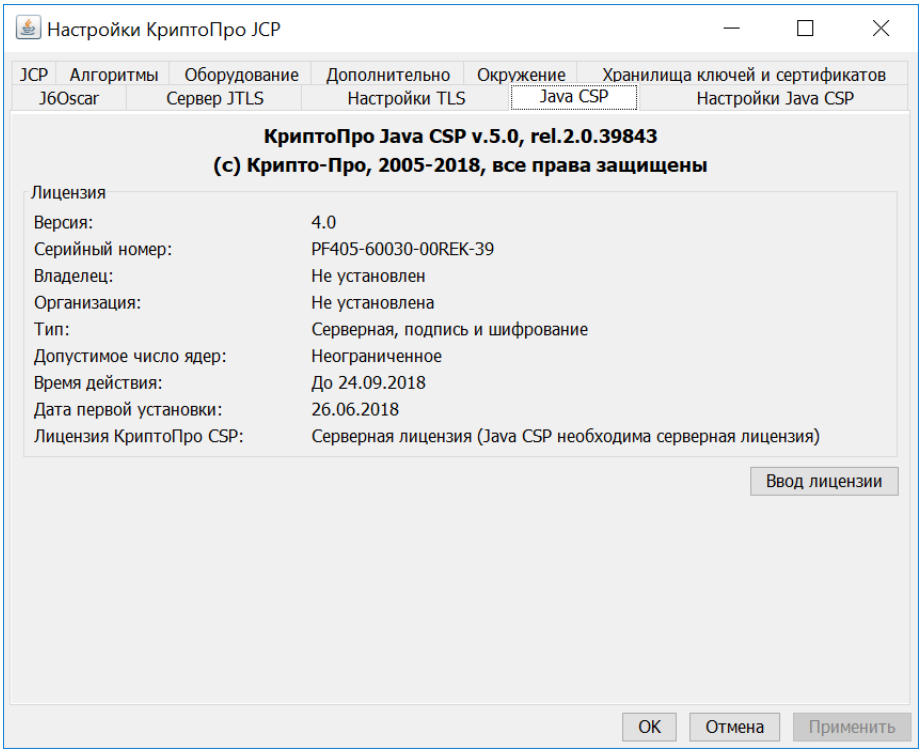


Рисунок 13. Закладка «Java CSP» контрольной панели

При установке криптопровайдера КриптоПро JavaCSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро JavaCSP 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 лицензии нажмите кнопку **Ввод лицензии** и заполните соответствующее поле в открывшемся окне (подробнее см. разд. 1.6).

Если на установленный в системе криптопровайдер КриптоПро CSP установлена клиентская лицензия, то JavaCSP при выполнении криптографических операций проверку собственной лицензии не производит и допускает использование всего функционала. Если же КриптоПро CSP установлен на сервере и имеет серверную лицензию, то и JavaCSP в свою очередь требует серверную лицензию, проверку которой он производит при соответствующих вызовах криптографических функций. По истечении серверной временной лицензии, устанавливаемой по умолчанию, JavaCSP перестанет корректно работать.

В случае использования JTLS (cpSSL) совместно с JavaCSP на сервере помимо серверной лицензии для cpSSL потребуется также серверная лицензия JavaCSP и серверная лицензия CSP.

**Внимание!** Лицензия будет сохранена только после нажатия кнопок «OK» или «Применить».

Закладка **Java CSP** содержит следующую информацию:
- версия криптопровайдера КриптоПро JavaCSP;
- серийный номер лицензии на использование криптопровайдера КриптоПро JavaCSP;
- имя владельца лицензии;
- организация, к которой относится владелец;
- тип лицензии;
- допустимое число процессоров для данной лицензии (не используется);
- время действия лицензии;
- дату первой установки провайдера;
- лицензия на КриптоПро CSP.

## 2.2 Закладка «Настройки Java CSP»

Закладка **Настройки Java CSP** (см. рис. 14) предназначена для просмотра информации о криптопровайдерах, используемых для исполнения криптографических операций, предоставляемых JavaCSP.

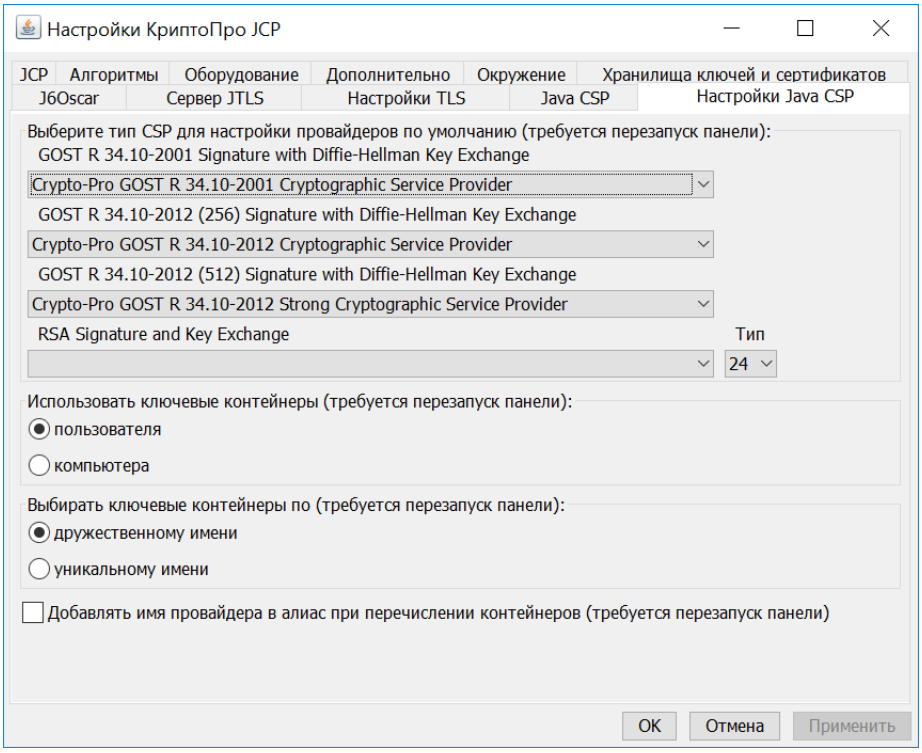


Рисунок 14. Закладка «Настройки Java CSP» контрольной панели

Также закладка предоставляет возможность изменения используемого криптопровайдера каждого типа. По умолчанию установлены криптопровайдеры (указано для случая использования КриптоПро CSP 5.0), указанные в табл. 1

Таблица 1. Используемые JavaCSP по-умолчанию криптопровайдеры

| **Тип провайдера** | **Название используемого по умолчанию провайдера** |
|---|---|
| GOST R 34.10-2001 Signature with Diffie-Hellman Exchange | Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider |
| GOST R 34.10-2012 (256) Signature with Diffie-Hellman Exchange | Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider |
| GOST R 34.10-2012 (512) Signature with Diffie-Hellman Exchange | Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider |

**Примечание.** В случае использования криптопровайдера КРИПТО-ПРО CSP версии 3.9 и ниже, выпадающие списки для типов провайдера GOST R 34.10-2012 (256) Signature with Diffie-Hellman Exchange, GOST R 34.10-2012 (512) Signature with Diffie-Hellman Exchange будут пустыми.

Для смены используемого криптопровайдера необходимо в выпадающем меню выбрать доступный криптопровайдер, после чего нажать кнопку «Применить». После этого изменения вступят в силу. Дополнительно можно выбрать, чьи контейнеры отображать (пользователя или компьютера) и в каком формате (по дружественному имени или уникальному).

Чтобы изменения отображались на закладке «Хранилища ключей и сертификатов», необходим перезапуск панели.

## 2.3 Закладка «Алгоритмы»

Закладка «Алгоритмы» (см. рис. 15) предназначена для просмотра используемых параметров реализованных криптографических алгоритмов. Помимо этого, допускается изменение текущих параметров на любые другие, допустимые соответствующими алгоритмами.

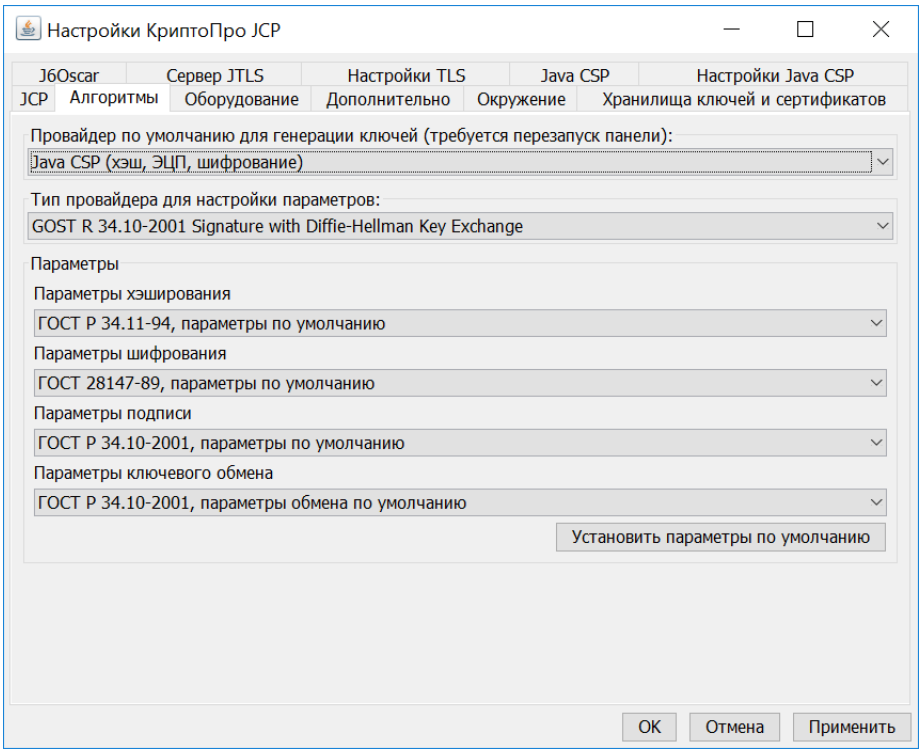


Рисунок 15. Закладка «Алгоритмы» контрольной панели

По умолчанию на закладке «Алгоритмы» определены настройки:

- Провайдер по умолчанию для генерации ключей (требуется перезапуск);
- Тип провайдера для настройки параметров.

По умолчанию на закладке «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 ключевого обмена 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 ключевого обмена 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 параметры ТК26 2 для провайдера ГОСТ Р 34.10-2012 (512).

При установленном провайдере JavaCSP список «Провайдер по умолчанию для генерации ключей»> содержит 2 элемента — провайдер JCP (по умолчанию) и JavaCSP. Данная настройка определяет, какой провайдер будет использоваться при генерации ключей на закладке "Хранилища ключей и сертификатов а также тип провайдера по умолчанию при использовании JTLS и CAdES.

При выборе второго пункта в списке — провайдера JavaCSP — потребуется перезапуск панели для того, чтобы изменения вступили в силу и список доступных контейнеров на закладке «Хранилища ключей и сертификатов» перезагрузился.

## 2.4 Закладка «Хранилища ключей и сертификатов»

Закладка «Хранилища ключей и сертификатов» (см. рис. 16) предназначена для просмотра хранилищ ключей, установленных в системе, просмотра и управления контейнерами в хранилищах.

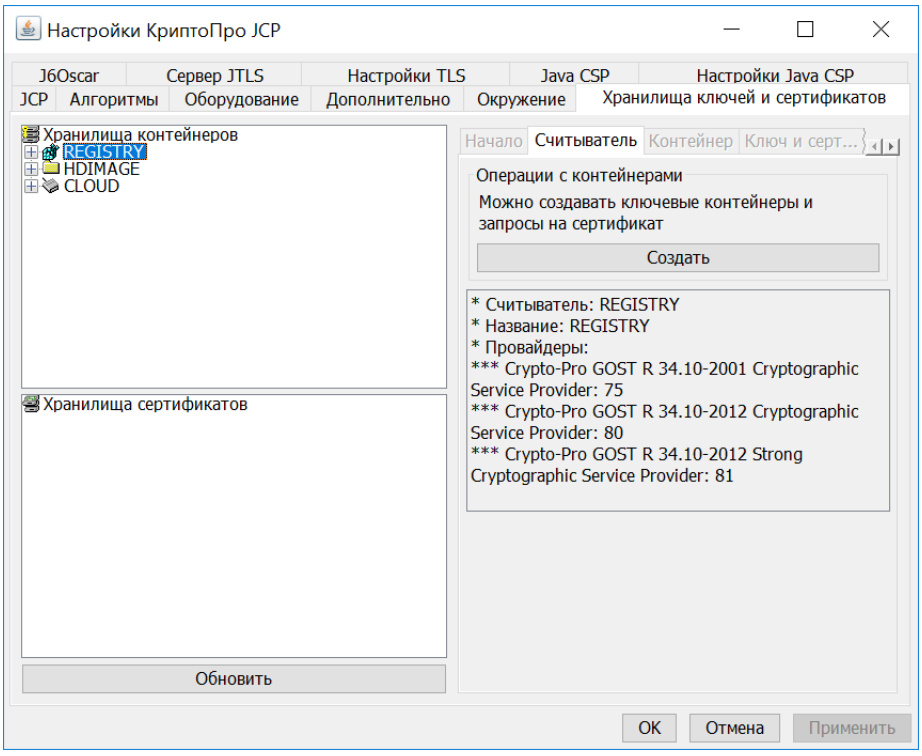


Рисунок 16. Закладка «Хранилища ключей и сертификатов» контрольной панели

С помощью закладки 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.

После установки провайдера КриптоПро JavaCSP в качестве провайдера по умолчанию и перезапуска панели на закладке «Хранилища ключей и сертификатов» будут доступны типы контейнеров, перечисленные в панели КриптоПро CSP.

В случае, если загрузку списка провайдеров произвести не удалось, например, при отсутствии библиотек или неправильной установке, список контейнеров будет пуст. Если провайдером по умолчанию для генерации ключей был JavaCSP, то перед загрузкой контейнеров на закладке «Хранилища ключей и сертификатов» появится сообщение об ошибке (см. рис. 17).

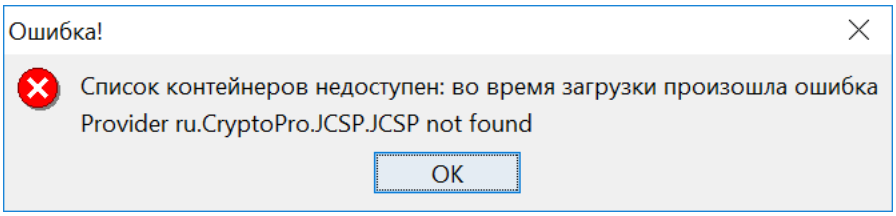


Рисунок 17. Ошибка при загрузке списка контейнеров

В случае, если существует проблема, связанная с провайдером JavaCSP (`JCSP.jar`), то, несмотря на тот факт, что появится указанное выше сообщение, на закладке «Алгоритмы» можно будет выбрать провайдер JCP в качестве провайдера по умолчанию для того, чтобы обеспечить дальнейшую возможность работы.

# 3 Настройка параметров провайдера с помощью Preferences

В некоторых случаях может потребоваться настройка JavaCSP 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
```

Таблица 2. Основные параметры JavaCSP

| **Описание** | **Путь** | **Ключ** | **Соответствует** |
|---|---|---|---|
| Источник ключевых контейнеров — пользователь или компьютер, число (0-1) | ru/CryptoPro/JCSP/params | KeySet_class_default | Закладка «Настройки Java CSP», использование ключевых контейнеров |
| Выбор ключевых контейнеров по имени — дружественному или уникальному | ru/CryptoPro/JCSP/params | NameType_class_default | Закладка «Настройки Java CSP», выбор ключевых контейнеров |
| Имя RSA провайдера | ru/CryptoPro/JCSP/params | DefaultCSPProvider_ RSA_class_default | Закладка «Настройки Java CSP», RSA Signature and Key Exchange |
| Имя провайдера ГОСТ Р 34.10-2001 | ru/CryptoPro/JCSP/params | DefaultCSPProvider_ 2001_class_default | Закладка «Настройки Java CSP», GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange |
| Имя провайдера ГОСТ Р 34.10-2012 (256 бит) | ru/CryptoPro/JCSP/params | DefaultCSPProvider_ 2012_256_class_default | Закладка «Настройки Java CSP», GOST R 34.10-2012(256) Signature with Diffie-Hellman Key Exchange |
| Имя провайдера ГОСТ Р 34.10-2012 (512 бит) | ru/CryptoPro/JCSP/params | DefaultCSPProvider_ 2012_512_class_default | Закладка «Настройки Java CSP», GOST R 34.10-2012(512) Signature with Diffie-Hellman Key Exchange |