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 CSP
Версия 5.0 KC2
2-Base
Руководство администратора
безопасности.
Использование JavaCSP и JavaTLS

ЖТЯИ.00102-01 91 12
Листов 33

2019 г

Содержание

Аннотация

Настоящее Руководство дополняет документ ЖТЯИ.00102-01 91 01. Руководство администратора безопасности. Общая часть при использовании модулей КриптоПро JCSP и КриптоПро JTLS (далее — JavaCSP и JavaTLS) средства криптографической защиты информации КриптоПро CSP версия 5.0 КС2 Исполнение 2-Base.

Модули JavaCSP и JavaTLS предоставляют доступ к реализациям российских криптографических алгоритмов и функционируют под управлением виртуальной Java-машины.

Инструкции администратора безопасности и пользователям различных автоматизированных систем, использующих модули JavaCSP и JavaTLS СКЗИ КриптоПро CSP версия 5.0 КС2 Исполнение 2-Base, должны разрабатываться с учетом требований настоящего документа.

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
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

КриптоПро JCSP является криптопровайдером Java. КриптоПро JCSP не реализует российские криптографические алгоритмы самостоятельно. Все криптографические операции осуществляются путём использования соответствующих вызовов криптопровайдера КриптоПро CSP.

1.1 Программно-аппаратные среды функционирования

КриптоПро JavaCSP функционирует под управлением следующих Java-машин:

- Java-машины производства Oracle «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе;
- Java-машины производства Oracle «Java(TM) 10 Runtime Environment, Standard Edition» версии 10 и «Java(TM) 11 Runtime Environment, Standard Edition» версии 11 на 64-битной платформе;
- Java-машины J9VM производства IBM «Java(TM) 7 Runtime Environment, Standard Edition» версии 1.7 и «Java(TM) 8 Runtime Environment, Standard Edition» версии 1.8 на 32-битной и 64-битной платформе.
- Java-машины «OpenJDK» версий 7, 8, 10, 11 на 32-битной и 64-битной платформе.
- Java-машины «Liberica» версий 8, 10, 11 на 32-битной и 64-битной платформе.

КриптоПро JavaCSP должен использоваться с сертифицированными Java-машинами, соответствующим требованиям безопасности разработчика. Защищенность криптографических объектов, создаваемых и обрабатываемых криптопровайдером, зависит от степени защищенности и корректности Java-машины, и может быть снижена при использовании виртуальных машин, не имеющих сертификата.

Со списком сертифицированных Java-машин можно ознакомиться по следующим адресам:

https://developer.ibm.com/javasdk/downloads/

http://www.oracle.com/technetwork/java/javase/downloads/index.html

https://openjdk.java.net/

https://bell-sw.com/pages/java-11.0.2/

1.2 Состав СКЗИ

КриптоПро JavaCSP выполнен в следующем составе:

- криптопровайдер (модуль на прикладном уровне);
- модуль сетевой аутентификации (JavaTLS);
- модуль обработки сертификатов и работы с CMS;
- библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK);
- модуль поддержки интерфейса под управлением виртуальной Java-машины;
- набор модулей и Java-классов для поддержки интерфейса JCA.

1.3 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражено в ЖТЯИ.00102-01 30 01. КриптоПро CSP. Формуляр, п. 3.9.

Использование носителей других типов допускается только по согласованию с ФСБ России.

Примечание. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

2 Установка и удаление дистрибутивов ПО СКЗИ

К установке и эксплуатации программного обеспечения, имеющего в своем составе СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.

При установке программного обеспечения СКЗИ необходимо:

• На технических средствах, оснащенных СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей.

• Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

• Аппаратуру, на которой устанавливается СКЗИ, следует получать у добросовестного производителя, проверяя наличие подтверждающих работоспособность документов.

• Рекомендуется установка средств защиты от НСД и при использовании СКЗИ в соответствии с классом КС2.

• При установке Java получить у производителя последнюю официальную версию, содержащую все программные обновления, связанные с безопасностью.

• Перед установкой СКЗИ проверить программное обеспечение ПЭВМ на отсутствие вредоносного ПО и программных закладок.

• Предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленным СКЗИ (путем опечатывания системного блока и разъемов ПЭВМ и контроля печатей администратором безопасности).

• После установки КриптоПро JavaCSP, но до начала его использования, необходимо воспользовавшись утилитой командной строки CPVerify.Prompt создать хранилища контролируемых файлов, как описано в CPVerify.

2.1 Способы установки

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JavaCSP 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
```

Или программно, с помощью Security.addProvider:

```
Security.addProvider(new JCSP()); // провайдер JCSP
Security.addProvider(new RevCheck());// провайдер проверки сертификатов JCPRevCheck
                                     //(revocation-провайдер)
Security.addProvider(new CryptoProvider());// провайдер шифрования JCryptoP
```

Библиотеки должны быть добавлены в classpath.

Для установки КриптоПро JavaCSP на ПЭВМ с установленной Java-машиной версии 1.7 или 1.8 следуйте описанной ниже инструкции.

Основной способ установки КриптоПро JavaCSP состоит в запуске командного файла, входящего в состав дистрибутива СКЗИ; 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 необходимо иметь права администратора на данной рабочей станции.

2.2 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.

2.3 Установка на Windows

В случае использования Java-машин версии 10 и выше:

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

Установка КриптоПро JavaCSP на ОС Windows с установленной Java-машиной версии 1.7 или 1.8 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, в ней необходимо перейти на вкладку **Java CSP**. При необходимости введите лицензию, как это описано в разделе Проверка и ввод лицензии.

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`.

2.3.1 Установка с помощью графического инсталлятора

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

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

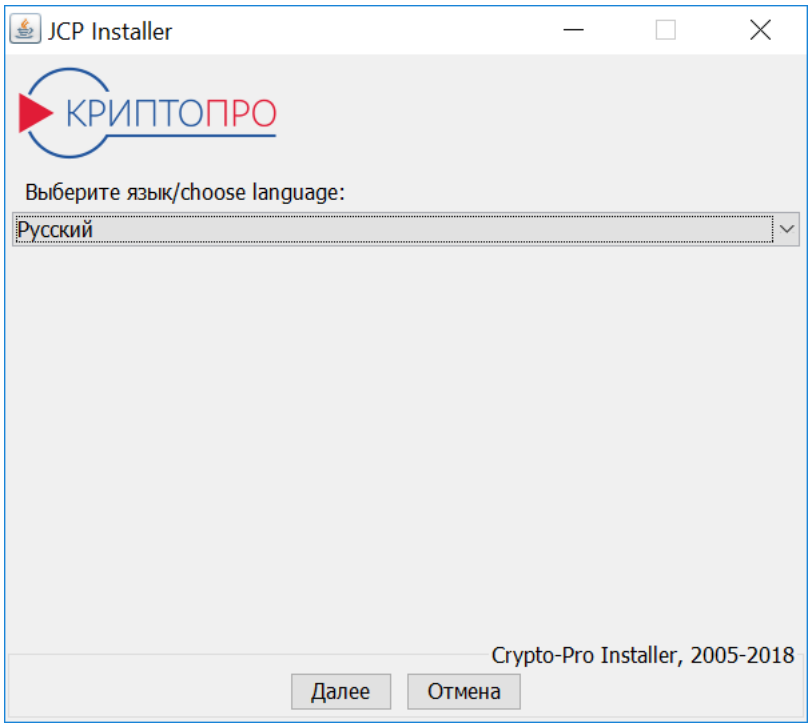

Рисунок 1. Окно выбора языка инсталлятора

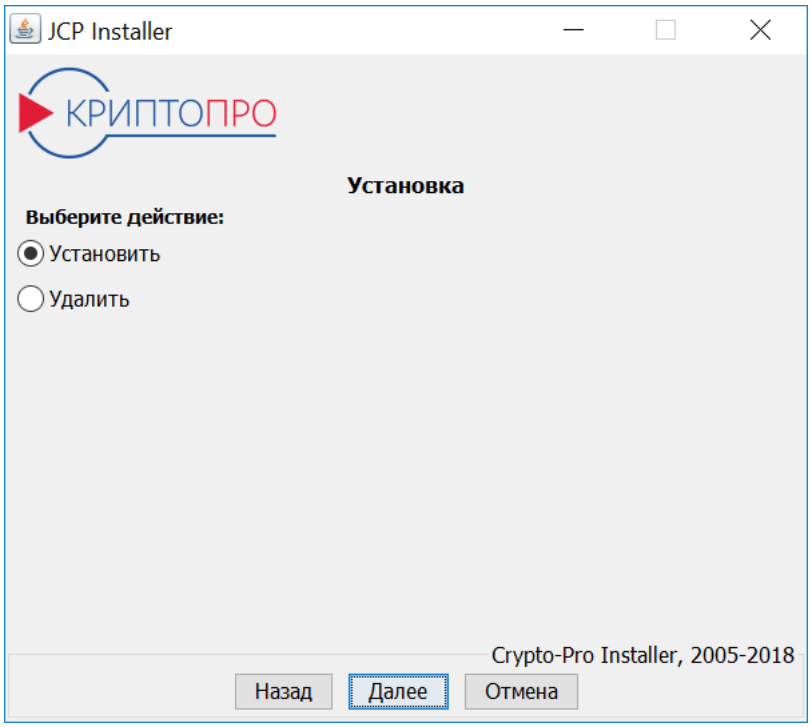

Рисунок 2. Окно выбора действия

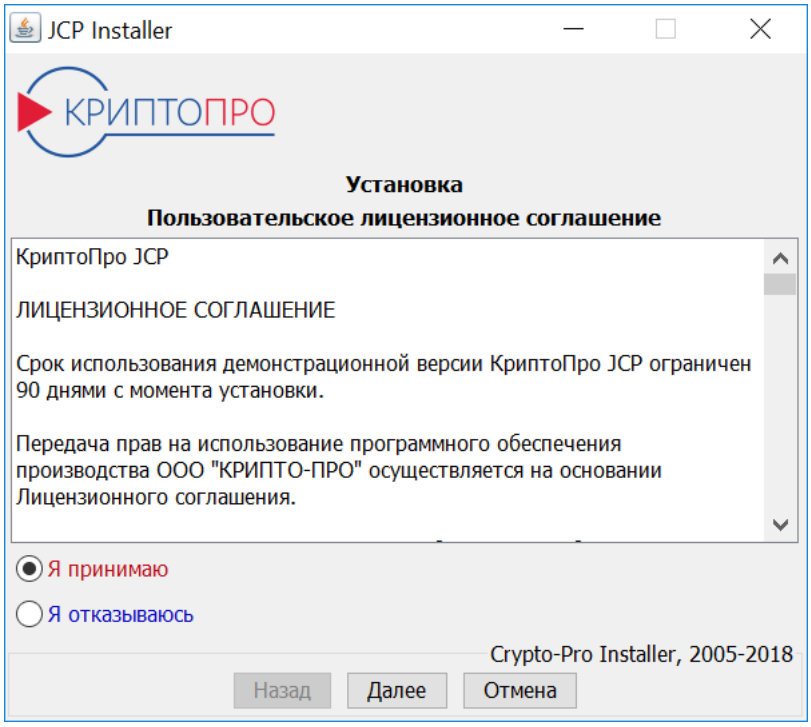

Рисунок 3. Окно с лицензионным соглашением

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).

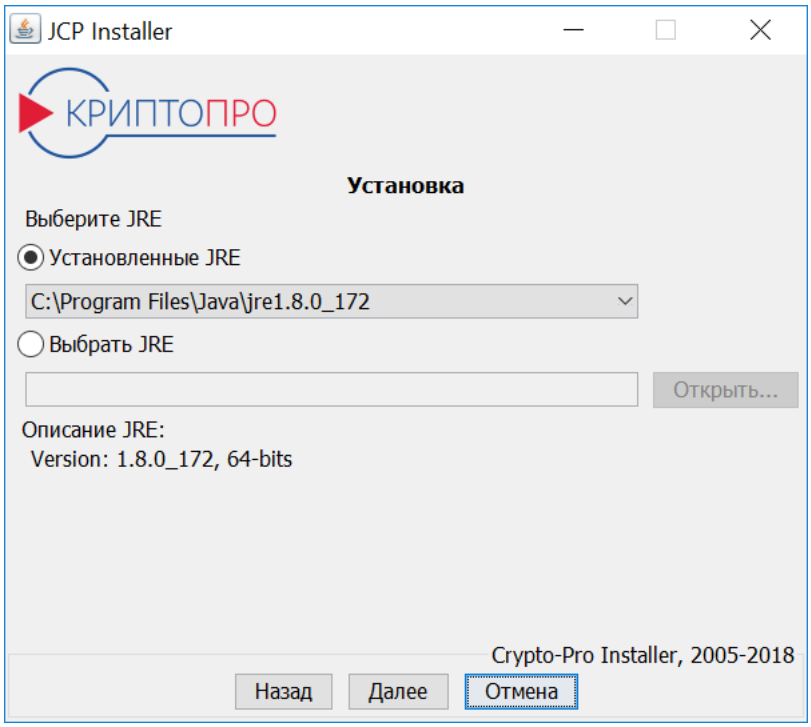

Рисунок 4. Окно выбора JRE

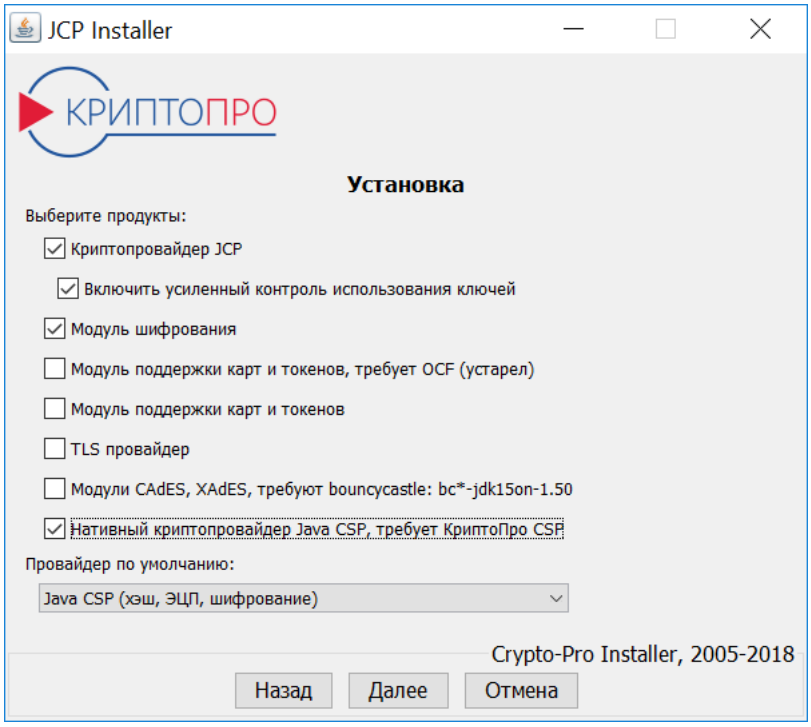

Рисунок 5. Окно выбора продукта

При установке провайдера можно указать, какой из них будет использоваться по умолчанию. В дальнейшем это настройку можно изменить в панели на закладке «Алгоритмы». В зависимости от приоритета тот или иной провайдер 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.

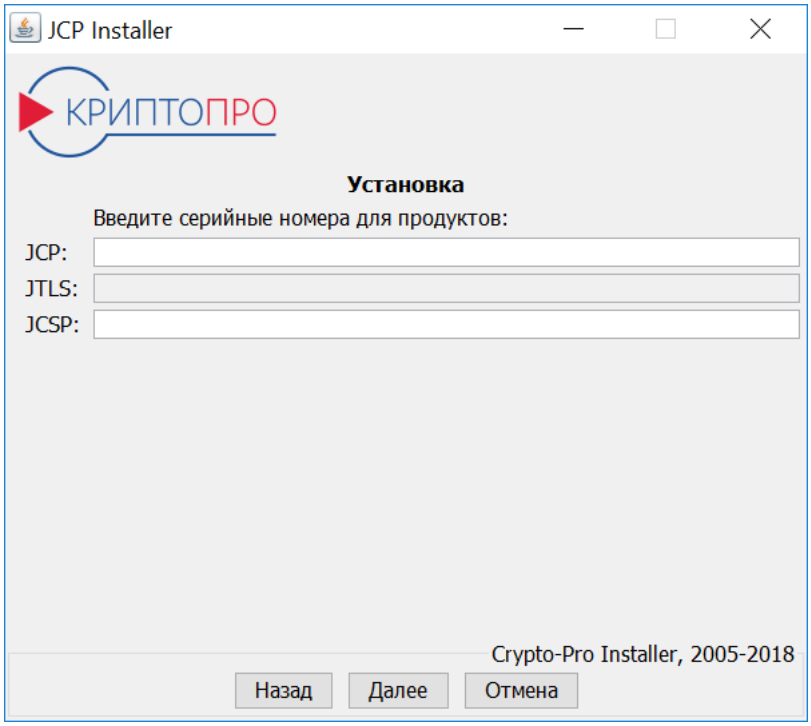

Рисунок 6. Окно ввода серийных номеров продуктов

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

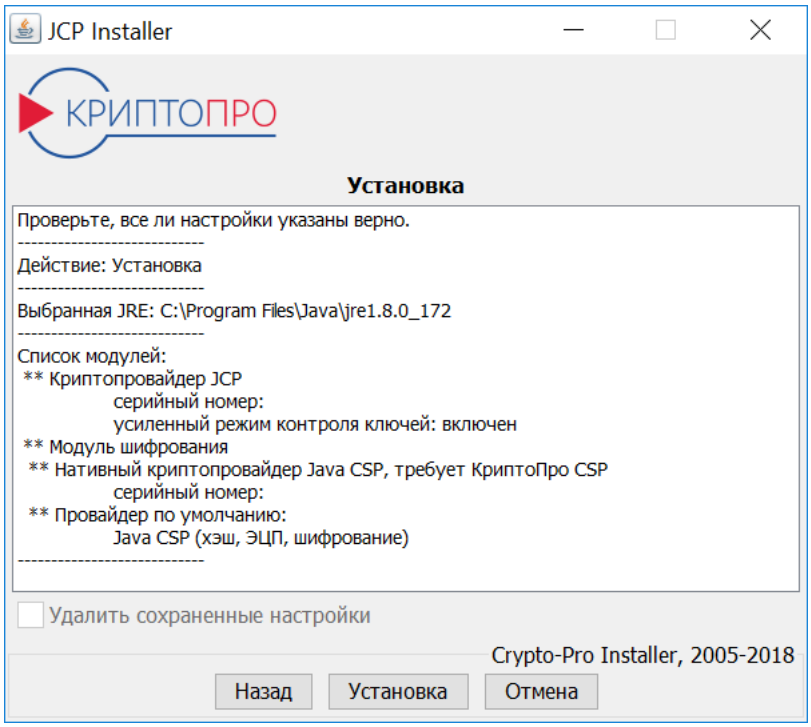

Рисунок 7. Окно проверки настроек установки/удаления

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

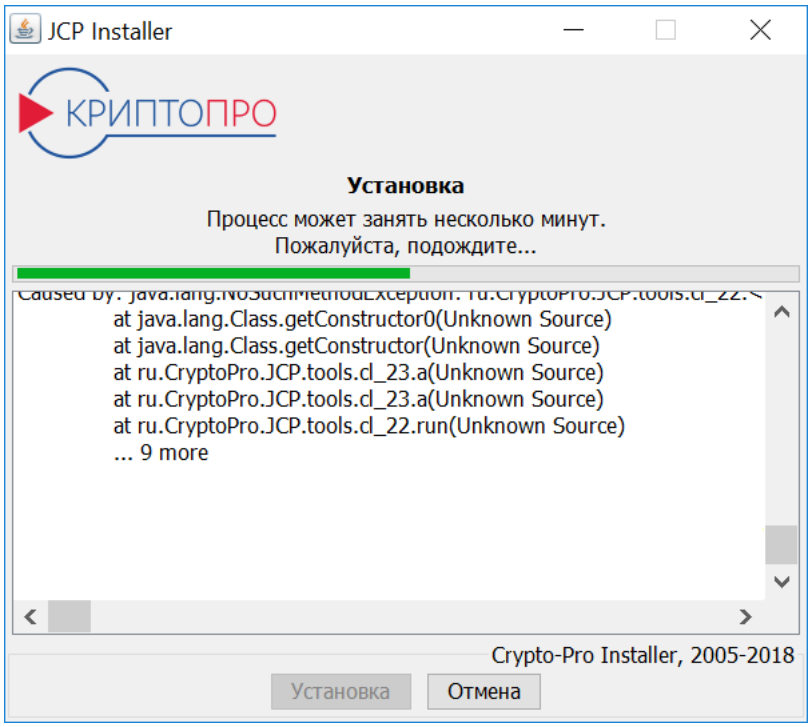

Рисунок 8. Окно процесса установки

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

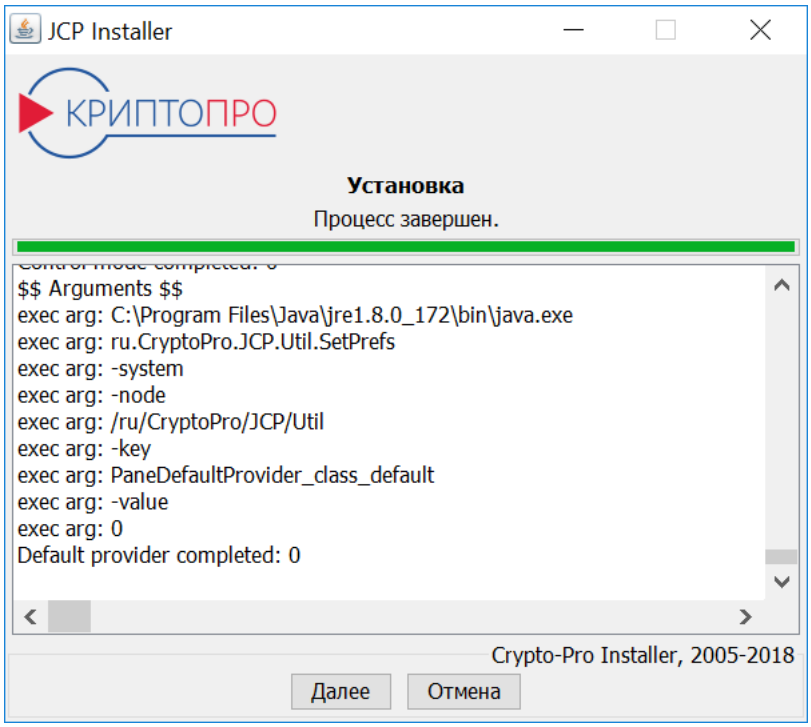

Рисунок 9. Окно с результатами установки

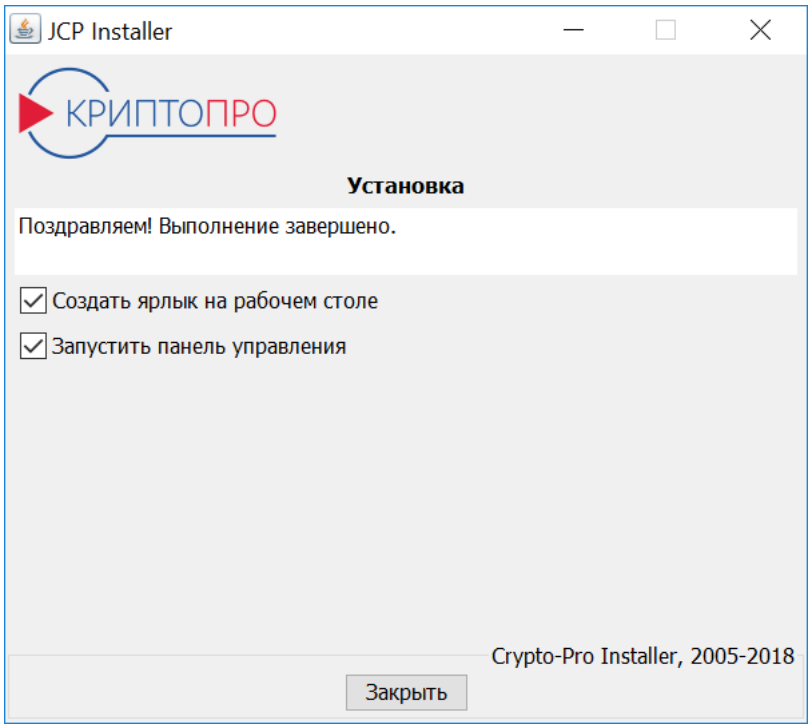

Рисунок 10. Завершение установки

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

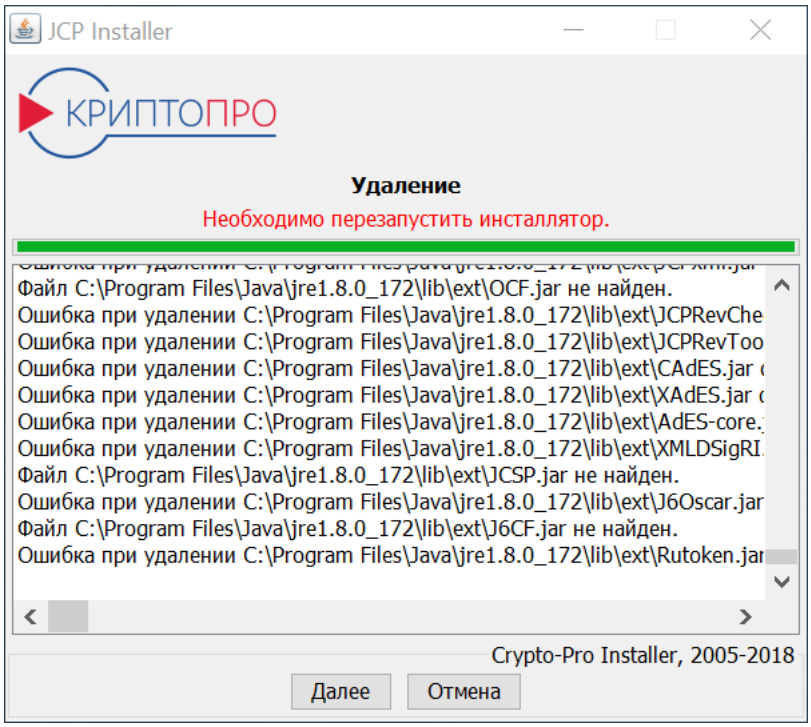

Рисунок 11. Ошибка при удалении компонентов

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.

2.3.2 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 JCSP и cpSSL в C:\ProgramFiles\Java\jre7 с указанием серийного номера для JCSP и назначением JCSP провайдером по умолчанию:

```
setup_console.bat "C:\Program Files\Java\jre7" -force -ru -install -jre "C:\Program Files\
Java\jre7" -jcp -jcsp -cpssl -serial_jcsp  XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -default_provider 1
```

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

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

В этом случае после удаления JCSP все еще остается провайдером по умолчанию. Для изменения провайдера по умолчанию воспользуйтесь закладкой «Алгоритмы».

2.4 Установка на UNIX и Mac OS

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JavaCSP в случае эксплуатации ПО в ОС *nix не требуется.

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

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

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

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

Для **удаления** КриптоПро JavaCSP 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 JavaCSP, 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. 2.3.2.

2.5 Локальная установка вызовом Java

В случае использования Java-машин версии 10 и выше:

Установка КриптоПро JavaCSP не требуется.

При установке КриптоПро JavaCSP 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.

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`.

2.6 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 откройте закладку **Java CSP** и нажмите кнопку **Ввод лицензии**. В открывшемся окне введите имя пользователя, название организации и серийный номер продукта (см. рис. 12).

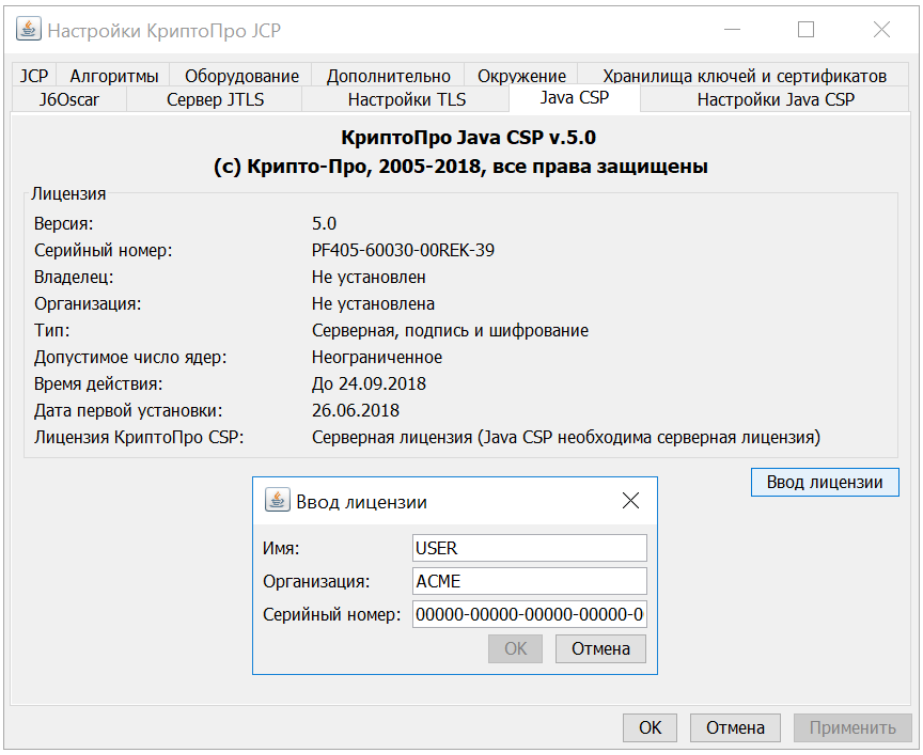

Рисунок 12. Ввод лицензии

2.7 Политики безопасности

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

2.7.1 Права доступа для JCSP.jar

В случае использования Java-машин версии 10 и выше:

КриптоПро JavaCSP запускается из каталога пользователя.

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";

};
```

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

2.7.2 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.

2.7.3 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.

2.7.4 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, в случае использования Java-машин версии 10 и выше — HKEY_CURRENT_USER\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 учетной записи root. Для их автоматического создания с правильными правами доступа достаточно создать контейнер из-под root или, в случае использования Java-машин версии 10 и выше, выполнить запуск configure.sh из папки дистрибутива.

3 Обновление ПО СКЗИ

Для обновления КриптоПро JavaCSP необходимо:

1) запомнить текущую конфигурацию JavaCSP (установленные считыватели, носители, параметры алгоритмов по умолчанию и т.п.);

2) удалить СКЗИ КриптоПро JavaCSP встроенными средствами (см. Установка и удаление дистрибутивов ПО СКЗИ);

3) установить аналогичный новый дистрибутив КриптоПро JavaCSP (см. Установка и удаление дистрибутивов ПО СКЗИ);

4) при необходимости внести изменения в настройки.

Ключи и сертификаты сохраняются автоматически.

4 Состав и назначение компонент ПО СКЗИ

Основной архитектурной особенностью ПО СКЗИ КриптоПро JavaCSP является то, что подсистема программной среды функционирования криптосредства (СФ) не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми ключами, незавершенными значениями хэш-функций и т.п. осуществляются в недоступных пользователю объектах; операции экспорта отсутствуют. СКЗИ КриптоПро JavaCSP не реализует российские криптографические алгоритмы самостоятельно. Все криптографические операции осуществляются путём использования соответствующих вызовов криптопровайдера КриптоПро CSP.

4.1 Структура СКЗИ

Общая структура СКЗИ КриптоПро JavaCSP представлена на рис. 13.

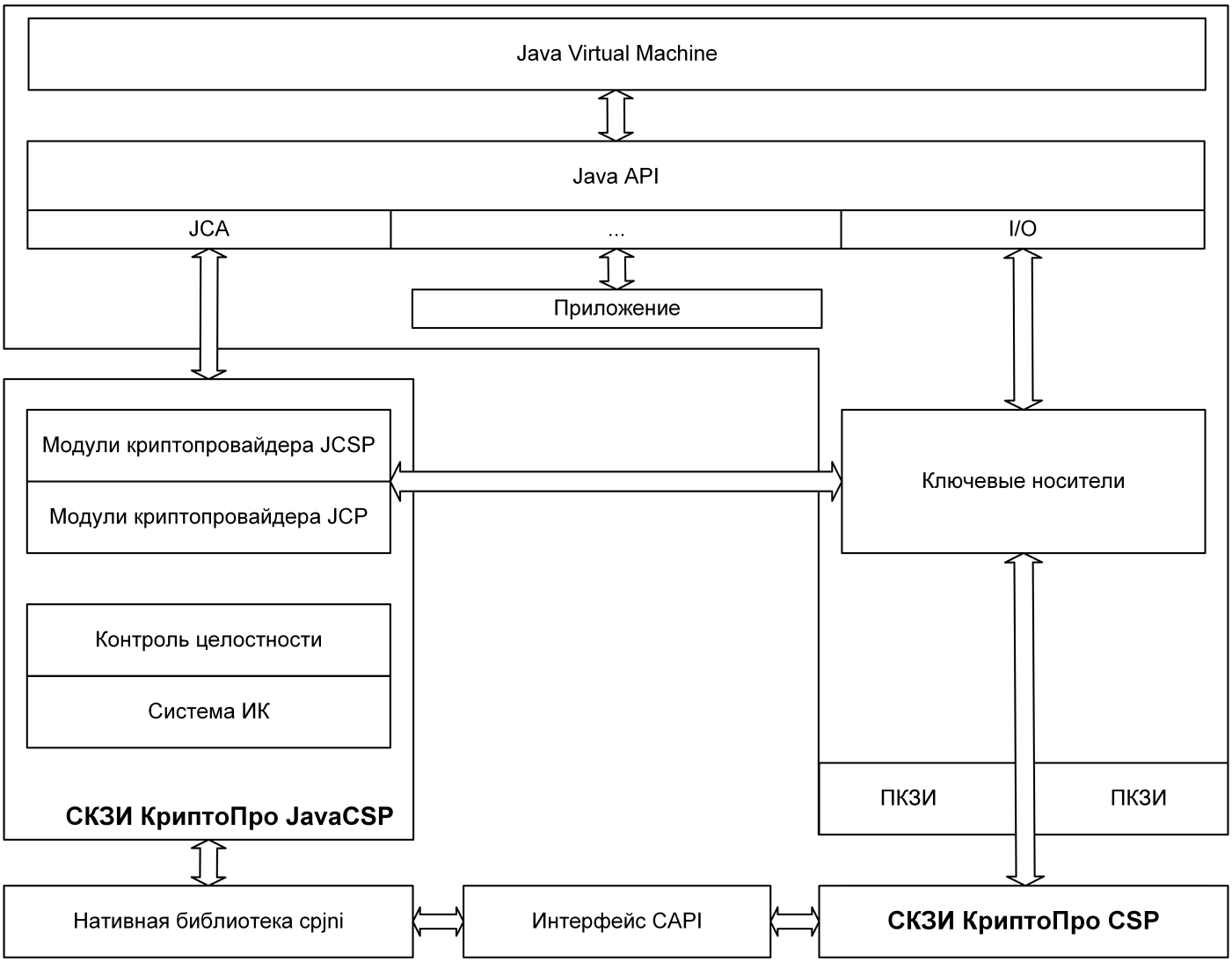

Рисунок 13. Структура СКЗИ КриптоПро JavaCSP

4.2 Состав ПО СКЗИ

В состав КриптоПро JavaCSP входят:

- Криптопровайдер КриптоПро CSP для исполнений по уровню КС2;
- Библиотека cspjni, реализующая JNI интерфейс для взаимодействия с криптопровайдером КриптоПро CSP 5.0 КС2.

В состав подсистемы программной СФ входят следующие компоненты:

- Подсистема настройки провайдера;
- Java-машина.

5 Встраивание СКЗИ в прикладное ПО

Встраивание СКЗИ могут производить организации, имеющие лицензию на право проведения таких работ, а работы по встраиванию должны проводиться в соответствии с Положением ПКЗ-2005.

Для обеспечения защиты электронных документов и создания защищенной автоматизированной системы в первую очередь используют криптографические методы защиты, которые позволяют обеспечить защиту целостности, авторства и конфиденциальности электронной информации и реализовать их в виде программных или аппаратных средств, встраиваемых в автоматизированную систему.

Использование криптографических средств требует, как правило, применения также организационно-технических мер защиты.

При создании защищенной автоматизированной системы необходимо определить модель угроз и политику ее безопасности. В зависимости от политики безопасности определяется необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

КриптоПро JavaCSP в первую очередь предназначено для встраивания в прикладное программное обеспечение. Функции КриптоПро JavaCSP могут быть использованы:

- через интерфейс функций JCA, что позволяет применять весь инструментарий Java. Для этих целей разработчики могут воспользоваться программной документацией, содержащейся в Java 2 SDK, а также поставляемым тестовым ПО. Подробная информация содержится в документе ЖТЯИ.00102-01 96 02. КриптоПро CSP. Руководство программиста JavaCSP.
- в стандартном прикладном ПО Java.

При встраивании КриптоПро JavaCSP в прикладное программное обеспечение или использовании его в составе стандартного прикладного ПО должны выполняться следующие требования:

1) При использовании ключей проверки ЭП должна быть обеспечена целостность и идентичность ключа проверки ЭП. Это может быть реализовано:

- путем заверения ключа проверки ЭП доверенной стороной (например, в случае использования сертификатов ключей проверки подписи);
- путем доверенного распространения и хранения ключей проверки ЭП в виде справочников.

2) При использовании сертификатов ключей проверки подписи, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата ключа ЭП доверенной стороны, с использованием которого проверяются остальные сертификаты ключей проверки пользователей.

3) Криптографическое средство, с помощью которого производится заверение ключей проверки ЭП или справочников ключей проверки ЭП, должно быть сертифицировано по классу, соответствующему принятой политике безопасности.

4) Для отзыва (вывода из действия) ключей проверки подписи должны использоваться средства, позволяющие произвести авторизацию отзывающего лица (в этих целях может быть использован список отозванных сертификатов, заверенный ЭП доверенной стороны).

5) При вызове функций КриптоПро JavaCSP в прикладном программном обеспечении необходимо, при возникновении критических исключений блокировать криптографические вызовы, а при возникновении других исключений, корректно их обрабатывать (см. ЖТЯИ.00102-01 96 02. КриптоПро CSP. Руководство программиста JavaCSP).

Возможна ситуация, когда установленная JRE имеет экспортные ограничения. США запрещают экспорт «сильной» криптографии и JavaCSP с длиной ключа 256 бит попадает под это ограничение. Ограничения устанавливаются файлами `local_policy.jar` и `US_export_policy.jar` в каталоге `<JRE>/jre/lib/security`.

Для снятия экспортных ограничений необходимо скачать файл `jce_policy.zip` с политиками со страницы http://www.oracle.com/technetwork/java/javase/downloads/index.html

Следует выбрать "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files" версии 7 или 8. Для отладки можно просто скопировать `US_export_policy.jar` в `local_policy.jar` (оба файла должны присутствовать).

6 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 документа ЖТЯИ.00102-01 91 01. Руководство администратора безопасности. Общая часть.

6.1 Принципы защиты информации от НСД

Защита информации от НСД в автоматизированной системе обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, в том числе:

- применение специальных программно-аппаратных средств защиты;
- организация системы контроля безопасности информации;
- физическая охрана ПЭВМ и ее средств;
- администрирование информационной безопасности;
- учет носителей информации;
- сигнализация о попытках нарушения защиты;
- периодическое тестирование технических и программных средств защиты;
- использование сертифицированных программных и технических и средств.

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

В организации, эксплуатирующей ПО КриптоПро JavaCSP, должна быть выпущена инструкция по защите от НСД к системе, разработанная на базе настоящего документа, руководящих документов ФСТЭК России, действующих нормативных документов самой эксплуатирующей организации.

В организации-пользователе системы должно быть выделено специальное должностное лицо - администратор безопасности, функции которого должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты.

Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на рабочем месте.

Каждый исполнитель работ как пользователь сети конфиденциальной связи должен быть зарегистрирован у администратора службы безопасности.

При осуществлении доступа в глобальные сети передачи данных непосредственно с рабочих мест, оснащенных КриптоПро JavaCSP, должны быть приняты меры, исключающие возможность воздействия нарушителя на СКЗИ по каналам связи, выходящим за пределы контролируемой зоны.

6.2 Организационно-технические меры защиты от НСД

При использовании КриптоПро JavaCSP также следует принять следующие организационные меры:

1) При использовании КриптоПро JavaCSP необходимо наличие механизма локальной аутентификации пользователей ОС.

2) Необходимо разработать и применить политику назначения и смены паролей в соответствии со

следующими правилами:

- Длина пароля должна быть не менее 8 символов;
- Количество подряд следующих попыток аутентификации одного субъекта доступа должно быть не более 3. При превышении числа подряд идущих попыток аутентификации одного субъекта доступа установленного предельного значения доступ этого субъекта к СКЗИ блокируется на 1 час (с обеспечением возможности разблокировки учетной записи при обращении пользователя к администратору безопасности);
- Недопустимо при выборе каждого символа пароля ограничиваться менее, чем 10 вариантами;
- Периодичность смены пароля не должна превышать 6 месяцев.

3) Провайдер JavaCSP должен использоваться в среде, защищенной от действий внешнего нарушителя, и в корпоративных сетях, защищенных от внутреннего нарушителя.

4) Необходимо ограничить возможность вывода информации с используемой ПЭВМ через порты COM, LPT, USB, IEEE 1394, а также средствами Bluetooth, Wi-Fi и аналогичных. Использование в качестве пассивного хранилища ключевой информации Bluetooth-носителя возможно только при наличии заключения ФСБ России на данное устройство.

5) Право доступа к рабочим местам с установленным ПО КриптоПро JavaCSP предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе КриптоПро JavaCSP.

6) Запретить осуществление несанкционированного администратором безопасности копирование ключевых носителей.

7) Запретить разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.

8) Запретить использование ключевых носителей в режимах, не предусмотренных правилами пользования КриптоПро JavaCSP, либо использовать ключевые носители на посторонних ПЭВМ.

9) Запретить запись на ключевые носители посторонней информации.

10) Требования по хранению личных ключевых носителей распространяются на ПЭВМ (в том числе и после удаления ключей с диска).

11) На технических средствах, оснащенных КриптоПро JavaCSP, должно использоваться только лицензионное программное обеспечение фирм-производителей.

12) На ПЭВМ, оснащенных КриптоПро JavaCSP, не допускается установка средств разработки и отладки ПО. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности.

В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих КриптоПро JavaCSP. Необходимо исключить попадание в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

13) Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства КриптоПро JavaCSP, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

14) Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется КриптоПро JavaCSP, после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

15) Администратором безопасности должно быть проведено опечатывание системного блока с установленным КриптоПро JavaCSP, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

16) Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС. Также избегают использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС.

17) При использовании КриптоПро JavaCSP на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении

которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

18) В BIOS ПЭВМ определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

19) Средствами BIOS должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в ISA и PCI разъем.

20) Вход в BIOS ПЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС.

21) Средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

22) При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав КриптоПро JavaCSP, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ.

23) Должно быть реализовано физическое затирание содержимого удаляемых файлов, в том числе SWAP файла.

24) Должно быть обеспечено тестирование аппаратуры в объеме самотестирования при перезагрузке не реже чем 1 раз в 15 суток.

25) Переставлять реализацию класса Preferences с помощью property java.util.prefs.PreferencesFactory запрещается.

26) Необходимо обеспечить административными мерами контроль доступа к системным и пользовательским настройкам Java-машины.

6.3 Дополнительные настройки ОС

Для обеспечения требований к установлению пароля должны выполняться следующие настройки операционных систем:

Linux:

В файле `/etc/login.defs` необходимо установить следующие значения:

LOGIN_RETRIES = 3

PASS_MAX_DAYS = 180

PASS_MIN_LEN = 8

В файле /etc/pam.d/common-password необходимо добавить:

```
password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=8
```

AIX:

В файле `/etc/security/user` в секции default необходимо установить следующие значения:

minlen = 8

maxrepeats = 3

maxage=24

Solaris:

В файле `/etc/default/passwd` необходимо установить следующие значения:

PASSLENGTH=8

MAXREPEATS=3

MAXWEEKS=24

Windows:

В групповых политиках перейти в Local Computer Policy→Computer Configuration→Windows Settings→SecuritySettings→Account Policies. В Account Policies установить следующие параметры:

Minimum password length = 8

Maximum password age = 24

Перейти в Local Computer Policy→Computer Configuration→Windows Settings→SecuritySettings→Account Lockout Policies и установить параметр:

Account Lockout threshold = 3

При использовании JavaCSP на платформе Windows Java-машина системные и пользовательские настройки хранит в реестре в разделах `HKEY_CURRENT_USER\Software\JavaSoft\Prefs` и `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs` соответственно.

На платформах Solaris и Linux Java-машина системные и пользовательские настройки хранит в файловой системе. Системные настройки находятся в каталоге `.systemPrefs`, положение которого определяется переменной `java.util.prefs.systemRoot` (по умолчанию `/etc/.java`). Если он недоступен, то `.systemPrefs` находится в каталоге определенном переменной `java.home`.

Пользовательские настройки находятся в каталоге `.java/.userPrefs`, положение которого определяется переменной `java.util.prefs.userRoot`. Если переменная не задана, то каталог `.java/.userPrefs` находится в каталоге определенном переменной `user.home`.

Приложение А
Управление протоколированием

Журналирование работы КриптоПро JavaCSP осуществляется стандартными средствами Java-машины. Формат протокола, поля вывода, уровни протоколирования настраиваются в файле <jre>/lib/logging.properties. Имя класса протокола для JavaCSP: **ru.CryptoPro.JCP.tools.JCPLogger**.

Уровни протоколирования JavaCSP совпадают с уровнями протоколирования Java, ниже они приведены в порядке по возрастанию информативности сообщений, уровень выше включает все сообщения приведенные по тексту ниже. Уровень **ALL** включает все сообщения, уровень **OFF** выключает все сообщения.

При настройках Java-машины по умолчанию включен уровень **INFO**.

Уровни протоколирования JavaCSP:

- **OFF** — В протокол не выводятся никакие сообщения.
- **SEVERE** — Критические ошибки в JavaCSP, функционирование JavaCSP после появления этих ошибок невозможно. К ним относятся ошибки загрузки, ошибки контроля целостности и др.
- **WARNING** — Ошибки JavaCSP. Ошибки не приводящие к отказу функционирования JavaCSP. К ним относятся, например ошибки настройки JavaCSP, неправильный вызов функций JavaCSP.
- **INFO** — Информационные сообщения о загрузке JavaCSP.
- **CONFIG** — Информационные сообщения при получении текущих настроек используемых JavaCSP.
- **FINE** — Информационные сообщения о завершении функции провайдера с ошибкой.
- **FINER** — Информационные сообщения связанные с входом/выходом в/из функции провайдера.
- **FINEST** — Уровень, не используется
- **ALL** — Сам уровень не используется, приводит к выдаче всех сообщений выдаваемых JavaCSP.

При включении уровня, отличного от заданного по умолчанию (**INFO**), следует помнить, что уровни выше **CONFIG** могут значительно замедлить скорость провайдера, а уровни ниже **INFO** привести к несвоевременному обнаружению причин отказа JavaCSP. При обычной работе JavaCSP рекомендуется оставлять настройку уровня выводимых сообщений по умолчанию (**INFO**).

Пример настройки файла `logging.properties` с уровнем **FINE**:

```
...
# Default global logging level.
# This specifies which kinds of events are logged across
# all loggers.  For any given facility this global level
# can be overriden by a facility specific level
# Note that the ConsoleHandler also has a separate level
# setting to limit messages printed to the console.
.level= INFO

############################################################
# Handler specific properties.
# Describes specific configuration info for Handlers.
############################################################

# default file output is in user's home directory.
java.util.logging.FileHandler.pattern = %h/java%u.log
java.util.logging.FileHandler.limit = 50000
```

```
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.XMLFormatter

# Limit the message that are printed on the console to INFO and above.

#java.util.logging.ConsoleHandler.level = INFO
java.util.logging.ConsoleHandler.level = FINE
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter

############################################################
# Facility specific properties.
# Provides extra control for each logger.
############################################################

# For example, set the com.xyz.foo logger to only log SEVERE
# messages:

com.xyz.foo.level = SEVERE

ru.CryptoPro.JCP.tools.JCPLogger.level = FINE
...
```

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					