

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



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Руководство программиста

ЖТЯИ.00101-02 96 01  
Листов 14

---

**© ООО «КРИПТО-ПРО», 2000-2021. Все права защищены.**

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 R2 KC1; 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

|          |                                                                                  |           |
|----------|----------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Описание программных интерфейсов</b>                                          | <b>4</b>  |
| <b>2</b> | <b>Требования к операционной системе для встроенного применения. Linux.</b>      | <b>5</b>  |
| 2.1      | Требования к библиотекам ОС                                                      | 5         |
| 2.2      | Требования к системным утилитам                                                  | 6         |
| 2.3      | Требования к файловой системе                                                    | 6         |
| 2.4      | Требования к службам                                                             | 7         |
| 2.5      | Требования к системе управления пакетами                                         | 7         |
| <b>3</b> | <b>Требования к операционной системе для встроенного применения. Solaris.</b>    | <b>8</b>  |
| 3.1      | Требования к библиотекам ОС                                                      | 8         |
| 3.2      | Требования к системным утилитам                                                  | 10        |
| 3.3      | Требования к файловой системе                                                    | 11        |
| 3.4      | Требования к службам                                                             | 11        |
| 3.5      | Требования к системе управления пакетами                                         | 11        |
| <b>4</b> | <b>Требования к использованию функций</b>                                        | <b>12</b> |
| <b>5</b> | <b>Особенности использования режима усиленного контроля использования ключей</b> | <b>14</b> |

## Аннотация

Настоящий документ описывает состав функций и тестовое ПО СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base и предназначен для разработки прикладного ПО с непосредственным вызовом функций СКЗИ, а также определяет требования к операционным системам при встраивании СКЗИ.

## 1 Описание программных интерфейсов

Использование низкоуровневого интерфейса криптопровайдера, позволяющего выполнять такие функции как генерация и работа с ключами, шифрование/расшифрование данных, хэширование и электронная подпись, описывается в файле CSP\_5\_0.chm – System Program Interface (CryptoAPI).

Файл CSP\_5\_0.chm в полном объеме относится к дистрибутивам **mini**.

Файл CSP\_5\_0.chm относится к дистрибутивам **web** в части документации, которая определяет функциональность с признаком verify context.



**Примечание.** Дистрибутивы с приставкой **mini** представляют собой форму исполнения KC1, реализующую функции СКЗИ, такую, что регистрация в операционной системе не предусматривается. Вопрос целостности данного исполнения должен обеспечиваться разработчиком приложений.

Дистрибутивы с приставкой **web** представляют собой форму исполнения KC1, реализующую функции СКЗИ, такую, что в ней отсутствуют модули поддержки ключевых носителей.

При использовании данного типа дистрибутивов для аутентификации требуется использовать дополнительные механизмы.

Использование интерфейса SSPI, содержащего реализацию протокола TLS, обеспечивающего работу с пакетами безопасности при выборе и инициализации пакета, с удостоверениями субъектов безопасности, установление соединений, передачу данных, распределение памяти, описывается в файле SSPI\_5\_0.chm – Security Support Provider Interface (SSPI).

Использование высокоуровневого интерфейса CryptoAPI, обеспечивающего набор функций для обработки сертификатов, списков отозванных сертификатов, расширенного использования ключа, работы с провайдером, выработки значения функции хэширования и электронной подписи, зашифрования и расшифрования данных, работы с хранилищем сертификатов и поддержки идентификатора объекта, описано в файле CAPILite\_5\_0.chm – CryptoAPI Lite (CAPILite).

Общая информация, используемая для создания модуля поддержки считывателей, носителей и датчиков случайных чисел, содержащая необходимые описания и определения, содержится в файле reader\_5\_0.chm.

Интерфейс PKCS#11, реализующий базовое описание RSA Labs v2.30, с доработками в соответствии с требованиями поддержки российских стандартов на реализацию криптографических функций описан в файле PKCS11\_5\_0.chm.

Подробнее об их установке и настройке можно узнать на [портале техподдержки](#) и [форуме КриптоПро](#).

## 2 Требования к операционной системе для встроенного применения. Linux.

### 2.1 Требования к библиотекам ОС

LSB 4.0, раздел III. Base Libraries.

СКЗИ КриптоПро CSP для своего функционирования требует следующие библиотеки базовой операционной системы (список библиотек по пакетам):

|                    |                      |                       |
|--------------------|----------------------|-----------------------|
| cprocsp-curl       | libXau.so.6          | libdl.so.2            |
| libc.so.6          | libxcb.so.1          | libgcc_s.so.1         |
| libdl.so.2         | libXdmcp.so.6        | /lib/ld-linux.so.2    |
| libgcc_s.so.1      | libXext.so.6         | libm.so.6             |
| libidn.so.11       | libXm.so.3           | libpthread.so.0       |
| /lib/ld-linux.so.2 | libXmu.so.6          | libstdc++.so.6        |
| libm.so.6          | libXp.so.6           | linux-gate.so.1       |
| libpthread.so.0    | libXt.so.6           |                       |
| librt.so.1         | linux-gate.so.1      |                       |
| libstdc++.so.6     |                      | lsb-cprocsp-kc1       |
| libz.so.1          |                      | libc.so.6             |
| linux-gate.so.1    | cprocsp-rdr-pcsc     | libdl.so.2            |
|                    | libc.so.6            | libgcc_s.so.1         |
|                    | libdl.so.2           | /lib/ld-linux.so.2    |
| cprocsp-ipsec-ike  | libgcc_s.so.1        | libm.so.6             |
| libc.so.6          | /lib/ld-linux.so.2   | libncurses.so.5       |
| libgcc_s.so.1      | libm.so.6            | libpthread.so.0       |
| /lib/ld-linux.so.2 | libpthread.so.0      | libstdc++.so.6        |
| libm.so.6          | libstdc++.so.6       | linux-gate.so.1       |
| libstdc++.so.6     | linux-gate.so.1      |                       |
| linux-gate.so.1    |                      | lsb-cprocsp-kc2       |
|                    | cprocsp-rsa          | libc.so.6             |
|                    | libc.so.6            | libdl.so.2            |
|                    | libdl.so.2           | libgcc_s.so.1         |
|                    | libgcc_s.so.1        | /lib/ld-linux.so.2    |
|                    | /lib/ld-linux.so.2   | libm.so.6             |
|                    | libm.so.6            | libpthread.so.0       |
|                    | libpthread.so.0      | libstdc++.so.6        |
|                    | libstdc++.so.6       | linux-gate.so.1       |
|                    | linux-gate.so.1      |                       |
|                    |                      | lsb-cprocsp-ocsp-util |
| cprocsp-npcades    | lsb-cprocsp-cades    | libc.so.6             |
| libc.so.6          | libc.so.6            | libgcc_s.so.1         |
| libdl.so.2         | libdl.so.2           | /lib/ld-linux.so.2    |
| libgcc_s.so.1      | libgcc_s.so.1        | libm.so.6             |
| /lib/ld-linux.so.2 | /lib/ld-linux.so.2   | libpthread.so.0       |
| libm.so.6          | libm.so.6            | libstdc++.so.6        |
| libpthread.so.0    | libpthread.so.0      | linux-gate.so.1       |
| libstdc++.so.6     | libstdc++.so.6       |                       |
| linux-gate.so.1    | linux-gate.so.1      |                       |
|                    |                      | lsb-cprocsp-pkcs11    |
| cprocsp-rdr-gui    |                      | libc.so.6             |
| libc.so.6          |                      | libgcc_s.so.1         |
| libdl.so.2         |                      | /lib/ld-linux.so.2    |
| libgcc_s.so.1      |                      | libm.so.6             |
| libICE.so.6        |                      | libstdc++.so.6        |
| /lib/ld-linux.so.2 |                      | linux-gate.so.1       |
| libm.so.6          |                      |                       |
| libpthread.so.0    |                      |                       |
| libSM.so.6         |                      |                       |
| libstdc++.so.6     |                      |                       |
| libuuid.so.1       | lsb-cprocsp-capilite |                       |
| libX11.so.6        | libc.so.6            |                       |

|                    |                      |                    |
|--------------------|----------------------|--------------------|
| libm.so.6          | lsb-cprosp-rdr-fkc   | libm.so.6          |
| libpthread.so.0    | libc.so.6            | libpthread.so.0    |
| libstdc++.so.6     | libdl.so.2           | libstdc++.so.6     |
| linux-gate.so.1    | libgcc_s.so.1        | linux-gate.so.1    |
|                    | /lib/ld-linux.so.2   |                    |
| lsb-cprosp-rdr     | libm.so.6            | rtsupcp            |
| libc.so.6          | libpthread.so.0      | libc.so.6          |
| libdl.so.2         | libstdc++.so.6       | libgcc_s.so.1      |
| libgcc_s.so.1      | linux-gate.so.1      | /lib/ld-linux.so.2 |
| /lib/ld-linux.so.2 |                      | libm.so.6          |
| libm.so.6          | lsb-cprosp-rdr-sobol | libpthread.so.0    |
| libpthread.so.0    | libc.so.6            | libstdc++.so.6     |
| libstdc++.so.6     | libdl.so.2           | linux-gate.so.1    |
| linux-gate.so.1    | libgcc_s.so.1        |                    |
|                    | /lib/ld-linux.so.2   |                    |

Кроме того, пакету `lsb-cprosp-capilite` для работы с сетью необходим либо пакет `cprosp-curl`, либо пакет `curl` (последний можно взять из дистрибутива ОС, из поставки CSP или [с сайта разработчика](#)). При отсутствии этого пакета базовая функциональность сохранится, но такие функции работы с сетью как автоматическое выкачивание CRL или запрос сертификата на УЦ через утилиту `сруптср` будут недоступны.

Пакету `lsb-cprosp-rdr-rcsc` для работы со смарт-картами необходим пакет `libpcsc-lite` из дистрибутива ОС. В зависимости от того, какой дистрибутив Linux используется, название пакета может варьироваться (`libpcsc-lite`, `libpcsc-lite1`).

## 2.2 Требования к системным утилитам

### LSB 4.0, раздел VI. Commands and Utilities

Для установки необходимого пакета `lsb-cprosp-base` требуются утилиты:

- `cat`
- `chmod`
- `cp`
- `crontab`
- `echo`
- `fgrep`
- `grep`
- `ln`
- `mkdir`
- `rm`
- `sed`
- `sysctl`
- `test`
- `true`
- `dpkg` (только для Debian и Ubuntu)

Для установки всех остальных пакетов (за исключением `cprosp-drv-devel`) достаточно подмножества этих утилит. Для установки `cprosp-drv-devel` также необходима утилита `uname`.

## 2.3 Требования к файловой системе

### LSB 4.x, раздел VI. Execution Environment 16. File System Hierarchy

Необходимы следующие разделы со следующими возможностями:

Таблица 1. Необходимые разделы

|                   |                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /opt/cproscsp     | После установки дистрибутива для функционирования продукта достаточно прав только на чтение.                                                                                  |
| /etc/opt/cproscsp | После установки дистрибутива для функционирования продукта достаточно прав только на чтение. При изменении настроек и операциях с лицензией также необходимы права на запись. |
| /var/opt/cproscsp | Во время работы с CSP необходимы права на чтение и на запись. Содержимое директории должно сохраняться между перезагрузками.                                                  |

## 2.4 Требования к службам

### LSB 4.0, раздел VIII. System Initialization 20. System Initialization 20.1. Cron Jobs

Необходимо базовое функционирование cron.

Для использования в качестве отчуждаемого ключевого носителя USB-флэш-накопителя необходимо функционирование службы udev.

## 2.5 Требования к системе управления пакетами

### LSB 4.0, раздел X. Package Format and Installation

Необходима поддержка механизма установки rpm.

## 3 Требования к операционной системе для встроенного применения. Solaris.

### 3.1 Требования к библиотекам ОС

СКЗИ КриптоПро CSP для своего функционирования требует следующие библиотеки базовой операционной системы (список библиотек по пакетам):

|                  |                 |                 |
|------------------|-----------------|-----------------|
| libc_psr.so.1    | libaio.so.1     | libCrun.so.1    |
| libmd_psr.so.1   | libc.so.1       | libCstd.so.1    |
| libCstd_isa.so.1 | libCrun.so.1    | libdl.so.1      |
| libnspr_flt4.so  | libCstd.so.1    | libdoor.so.1    |
| libCrun.so.1     | libdl.so.1      | libgen.so.1     |
| libCstd.so.1     | libm.so.2       | libldap.so.5    |
| libICE.so.6      | libmd.so.1      | libm.so.2       |
| libSM.so.6       | libpthread.so.1 | libmd.so.1      |
| libX11.so.4      | librt.so.1      | libmp.so.2      |
| libXext.so.0     | libthread.so.1  | libnsl.so.1     |
| libXm.so.4       | libaio.so.1     | libnspr4.so     |
| libXt.so.4       | libc.so.1       | libnss3.so      |
| libXtsol.so.1    | libCrun.so.1    | libnssutil3.so  |
| libadm.so.1      | libCstd.so.1    | libplc4.so      |
| libaio.so.1      | libdl.so.1      | libplds4.so     |
| libbsm.so.1      | libm.so.2       | libpthread.so.1 |
| libc.so.1        | libmd.so.1      | librt.so.1      |
| libcmd.so.1      | libpthread.so.1 | libsasl.so.1    |
| libdl.so.1       | librt.so.1      | libscf.so.1     |
| libdoor.so.1     | libthread.so.1  | libsocket.so.1  |
| libgen.so.1      |                 | libssl3.so      |
| lib/libldap.so.5 |                 | libthread.so.1  |
| libm.so.1        | CPROcpl         | libuutil.so.1   |
| libm.so.2        | libaio.so.1     | libz.so.1       |
| libmd.so.1       | libc.so.1       | libaio.so.1     |
| libmp.so.2       | libCrun.so.1    | libc.so.1       |
| libnsl.so.1      | libCstd.so.1    | libCrun.so.1    |
| libnspr4.so      | libdl.so.1      | libCstd.so.1    |
| libnss3.so       | libm.so.2       | libdl.so.1      |
| libplc4.so       | libmd.so.1      | libdoor.so.1    |
| libplds4.so      | libpthread.so.1 | libgen.so.1     |
| libpthread.so.1  | librt.so.1      | libldap.so.5    |
| librt.so.1       | libthread.so.1  | libm.so.2       |
| libsasl.so.1     | libaio.so.1     | libmd.so.1      |
| libscf.so.1      | libc.so.1       | libmp.so.2      |
| libsecdb.so.1    | libCrun.so.1    | libnsl.so.1     |
| libsocket.so.1   | libCstd.so.1    | libnspr4.so     |
| libsoftokn3.so   | libdl.so.1      | libnss3.so      |
| libssl3.so       | libm.so.2       | libnssutil3.so  |
| libthread.so.1   | libmd.so.1      | libplc4.so      |
| libtsol.so.2     | libpthread.so.1 | libplds4.so     |
| libuutil.so.1    | librt.so.1      | libpthread.so.1 |
| libvolmgt.so.1   | libthread.so.1  | librt.so.1      |
| libz.so.1        |                 | libsasl.so.1    |
|                  |                 | libscf.so.1     |
|                  | CPROcurl        | libsocket.so.1  |
|                  | libaio.so.1     | libssl3.so      |
|                  | libc.so.1       |                 |

```
libpthread.so.1      libmp.so.2           libgen.so.1
libutil.so.1         libnsl.so.1          libICE.so.6
libz.so.1            libpthread.so.1      libm.so.2
librt.so.1           libscf.so.1          libmd.so.1
libsocket.so.1       libstdc++.so.1        libmp.so.2
libnsl.so.1          libthread.so.1        libnsl.so.1
libpthread.so.1      libutil.so.1          libpthread.so.1
librt.so.1           libscf.so.1          librt.so.1
libstdc++.so.1       libsecdb.so.1         libscf.so.1
libcurses.so.1       libSM.so.6            libsecdb.so.1
libdl.so.1           libsocket.so.1        libSM.so.6
libm.so.2            libthread.so.1        libsocket.so.1
libmd.so.1           libtsol.so.2          libthread.so.1
libpthread.so.1      libutil.so.1          libtsol.so.2
librt.so.1           libX11.so.4           libutil.so.1
libthread.so.1       libXext.so.0          libX11.so.4
libaio.so.1          libXm.so.4            libXext.so.0
libc.so.1            libXt.so.4            libXm.so.4
libCrun.so.1         libXtso.1            libXt.so.4
libCstd.so.1         libXtso.1            libXtso.1
libcurses.so.1       libaio.so.1          libXtso.1
libdl.so.1           libbsm.so.1          libaio.so.1
libm.so.2            libc.so.1            libbsm.so.1
libmd.so.1           libcmd.so.1          libc.so.1
libpthread.so.1      libdl.so.1           libcmd.so.1
librt.so.1           libdoor.so.1         libdl.so.1
libthread.so.1       libgen.so.1          libdoor.so.1
libgen.so.1          libICE.so.6          libgen.so.1
libm.so.2            libm.so.2            libICE.so.6
libmd.so.1          libmd.so.1           libm.so.2
libmp.so.2          libmp.so.2           libmd.so.1
libnsl.so.1         libnsl.so.1          libmp.so.2
libpthread.so.1     libpthread.so.1      libnsl.so.1
librt.so.1          libthread.so.1       libpthread.so.1
libscf.so.1         libvolmgt.so.1       librt.so.1
libsocket.so.1       libadm.so.1          libscf.so.1
libthread.so.1      libaio.so.1          libsecdb.so.1
libutil.so.1        libc.so.1            libSM.so.6
libaio.so.1         libCrun.so.1         libsocket.so.1
libc.so.1           libCstd.so.1         libthread.so.1
libCrun.so.1        libdl.so.1           libtsol.so.2
libCstd.so.1        libgen.so.1          libutil.so.1
libdl.so.1          libm.so.2            libX11.so.4
libdoor.so.1        libmd.so.1           libXext.so.0
libgen.so.1         libpthread.so.1      libXm.so.4
libm.so.2           librt.so.1          libXt.so.4
libmd.so.1          libthread.so.1       libXtso.1
libmp.so.2          libvolmgt.so.1
libnsl.so.1
libpthread.so.1
librt.so.1
libscf.so.1
libsocket.so.1
libthread.so.1
libutil.so.1
libaio.so.1
libc.so.1
libCrun.so.1
libCstd.so.1
libdl.so.1
libdoor.so.1
libgen.so.1
libm.so.2
libmd.so.1
libmp.so.2
```

|                 |                 |                 |
|-----------------|-----------------|-----------------|
| libnsl.so.1     | librt.so.1      | librt.so.1      |
| libpthread.so.1 | libscf.so.1     | libthread.so.1  |
| librt.so.1      | libsocket.so.1  | libvolmgt.so.1  |
| libscf.so.1     | libthread.so.1  | libadm.so.1     |
| libsocket.so.1  | libuutil.so.1   | libaio.so.1     |
| libthread.so.1  |                 | libc.so.1       |
| libuutil.so.1   |                 | libCrun.so.1    |
| libaio.so.1     | CPR0rdr         | libCstd.so.1    |
| libc.so.1       | libadm.so.1     | libdl.so.1      |
| libdl.so.1      | libaio.so.1     | libgen.so.1     |
| libdoor.so.1    | libc.so.1       | libm.so.2       |
| libgen.so.1     | libCrun.so.1    | libmd.so.1      |
| libm.so.2       | libCstd.so.1    | libpthread.so.1 |
| libmd.so.1      | libdl.so.1      | librt.so.1      |
| libmp.so.2      | libgen.so.1     | libthread.so.1  |
| libnsl.so.1     | libm.so.2       | libvolmgt.so.1  |
| libpthread.so.1 | libmd.so.1      |                 |
|                 | libpthread.so.1 |                 |

Кроме того, пакету CPR0scr1 для работы с сетью необходим либо пакет CPR0curl из поставки КриптоПро CSP, либо пакет curl (последний можно взять из дистрибутива ОС, из поставки КриптоПро CSP или [с сайта разработчика](#)). При отсутствии этого пакета базовая функциональность сохранится, но такие функции работы с сетью как автоматическое выкачивание CRL или запрос сертификата на УЦ через утилиту cscrtps будут недоступны.

Пакету CPR0rdr для работы со смарт-картами необходим пакет pcsclite (например, пакет SUNWpcsclite из дистрибутива ОС).

## 3.2 Требования к системным утилитам

Для установки необходимых пакетов CPR0base, CPR0rdr необходимо функционирование утилит:

- o cat
- o chmod
- o cp
- o crontab
- o echo
- o fgrep
- o grep
- o ln
- o mv
- o rm
- o sed
- o sysctl
- o test
- o true

Для установки всех остальных пакетов за исключением CPR0drv и CPR0drvd достаточно подмножества этих утилит.

Для установки CPR0drv также необходимы утилит:

- o add\_drv
- o isainfo
- o rem\_drv
- o sync

Для установки CPR0drvд:

- add\_drv
- isainfo
- rem\_drv
- sync
- uname

### 3.3 Требования к файловой системе

Необходимы следующие разделы со следующими возможностями:

Таблица 2. Необходимые разделы файловой системы

|                   |                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /opt/cproscsp     | После установки дистрибутива для функционирования продукта достаточно прав только на чтение.                                                                                  |
| /etc/opt/cproscsp | После установки дистрибутива для функционирования продукта достаточно прав только на чтение. При изменении настроек и операциях с лицензией также необходимы права на запись. |
| /var/opt/cproscsp | Во время работы с CSP необходимы права на чтение и на запись. Содержимое директории должно сохраняться между перезагрузками.                                                  |

### 3.4 Требования к службам

Необходимо базовое функционирование cron.

Для работы с отчуждаемыми носителями типа USB flash drive необходимо функционирование службы Volume Management.

### 3.5 Требования к системе управления пакетами

Необходимо штатное функционирование системы управления пакетами.

## 4 Требования к использованию функций

Необходимо выполнять контроль кодов ошибок, возникающих при отклонениях от штатного выполнения команд.

Таблица 3. Коды ошибок

| Код ошибки (DEC) | Код ошибки (HEX) | Описание ошибки                                                 |
|------------------|------------------|-----------------------------------------------------------------|
| 536871012        | 20000064         | Мало памяти                                                     |
| 536871013        | 20000065         | Не удалось открыть файл                                         |
| 536871014        | 20000066         | Операция отменена пользователем                                 |
| 536871015        | 20000067         | Некорректное преобразование BASE64                              |
| 536871016        | 20000068         | Если указан параметр '-help', то других быть не должно          |
| 536871112        | 200000C8         | Указан лишний файл                                              |
| 536871113        | 200000C9         | Указан неизвестный ключ                                         |
| 536871114        | 200000CA         | Указана лишняя команда                                          |
| 536871115        | 200000CB         | Для ключа не указан параметр                                    |
| 536871116        | 200000CC         | Не указана команда                                              |
| 536871117        | 200000CD         | Не указан необходимый ключ                                      |
| 536871118        | 200000CE         | Указан неверный ключ                                            |
| 536871119        | 200000CF         | Параметром ключа '-q' должно быть натуральное число             |
| 536871120        | 200000D0         | Не указан входной файл                                          |
| 536871121        | 200000D1         | Не указан выходной файл                                         |
| 536871122        | 200000D2         | Команда не использует параметр с именем файла                   |
| 536871123        | 200000D3         | Не указан файл сообщения                                        |
| 536871212        | 2000012C         | Не удалось открыть хранилище сертификатов                       |
| 536871213        | 2000012D         | Сертификаты не найдены                                          |
| 536871214        | 2000012E         | Найдено более одного сертификата (ключ '-1')                    |
| 536871215        | 2000012F         | Команда подразумевает использование только одного сертификата   |
| 536871216        | 20000130         | Неверно указан номер                                            |
| 536871217        | 20000131         | Нет используемых сертификатов                                   |
| 536871218        | 20000132         | Данный сертификат не может применяться для этой операции        |
| 536871219        | 20000133         | Цепочка сертификатов не проверена                               |
| 536871220        | 20000134         | Криптопровайдер, поддерживающий необходимый алгоритм, не найден |

|           |          |                                                          |
|-----------|----------|----------------------------------------------------------|
| 536871221 | 20000135 | Неудачный ввод пароля ключевого контейнера               |
| 536871312 | 20000190 | Не указана маска файлов                                  |
| 536871313 | 20000191 | Указаны несколько масок файлов                           |
| 536871314 | 20000192 | Файлы не найдены                                         |
| 536871315 | 20000193 | Задана неверная маска                                    |
| 536871316 | 20000194 | Неверный хэш                                             |
| 536871412 | 200001F4 | Ключ '-start' указан, а выходной файл нет                |
| 536871413 | 200001F5 | Содержимое файла - не подписанное сообщение              |
| 536871414 | 200001F6 | Неизвестный алгоритм подписи                             |
| 536871415 | 200001F7 | Сертификат автора подписи не найден                      |
| 536871416 | 200001F8 | Подпись не найдена                                       |
| 536871417 | 200001F9 | Подпись не верна                                         |
| 536871418 | 20000200 | Штамп времени не верен                                   |
| 536871512 | 20000258 | Содержимое файла — не зашифрованное сообщение            |
| 536871513 | 20000259 | Неизвестный алгоритм шифрования                          |
| 536871514 | 2000025A | Не найден сертификат с соответствующим секретным ключом  |
| 536871612 | 200002BC | Не удалось инициализировать COM                          |
| 536871613 | 200002BD | Контейнеры не найдены                                    |
| 536871614 | 200002BE | Не удалось получить ответ от сервера                     |
| 536871615 | 200002BF | Сертификат не найден в ответе сервера                    |
| 536871616 | 200002C0 | Файл не содержит идентификатор запроса                   |
| 536871617 | 200002C1 | Некорректный адрес ЦС                                    |
| 536871618 | 200002C2 | Получен неверный Cookie                                  |
| 536871712 | 20000320 | Серийный номер содержит недопустимое количество символов |
| 536871713 | 20000321 | Неверный код продукта                                    |
| 536871714 | 20000322 | Не удалось проверить серийный номер                      |
| 536871715 | 20000323 | Не удалось сохранить серийный номер                      |
| 536871716 | 20000324 | Не удалось загрузить серийный номер                      |
| 536871717 | 20000325 | Лицензия просрочена                                      |



**Примечание.** Кроме кодов, приведенных в таблице, приложение может возвращать код любой системной ошибки.

## 5 Особенности использования режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей, необходимый для использования в СКЗИ вне тестовой эксплуатации, осуществляет контроль доверенности открытых ключей, срока действия ключей подписи и ключевого обмена, а также корректности инициализации программных ДСЧ. Это накладывает дополнительные требования к выполнению ряда операций, функционал которых предоставляется криптопровайдером.

1) Функции, при выполнении которых предполагается выработка случайных данных (CryptGenKey для временных ключей, CryptGenRandom), будут возвращать ошибку, если программный ДСЧ не был инициализирован с физического ДСЧ и провести инициализацию в данный момент невозможно (например, в системе не установлен ни один физический ДСЧ). Для исправления ошибки следует произвести установку хотя бы одного физического ДСЧ (например, БиоДСЧ, внешней гаммы, аппаратного ДСЧ), после чего произвести инициализацию программного ДСЧ одним из следующих способов:

- а) воспользоваться утилитой csptest:  
# ./csptest -keyset -verifycontext -hard\_rng
- б) произвести выработку долговременного ключа с помощью функции CryptGenKey;
- в) произвести вызов функции CryptSetProvParam с флагом PP\_USE\_HARDWARE\_RNG.

2) Функция CryptVerifySignature() принимает на вход дескриптор открытого ключа, с помощью которого производится проверка подписи. При включённом режиме усиленного контроля использования ключей допустимо передавать этой функции дескрипторы следующих ключей:

- а) Дескриптор ключа, извлечённого из контейнера (AT\_SIGNATURE, AT\_KEYEXCHANGE).
- б) Дескриптор ключа, полученного из сертификата открытого ключа. Для получения этого дескриптора необходимо получить структуру CERT\_CONTEXT, содержащую информацию о необходимом сертификате, с помощью функций CertCreateCertificateContext/CertFindCertificateInStore. Затем требуется вызвать функцию CryptImportPublicKeyInfoEx, передав ей указатель на структуру CERT\_CONTEXT.pCertInfo.SubjectPublicKeyInfo типа CERT\_PUBLIC\_KEY\_INFO. Функция CryptImportPublicKeyInfoEx вернёт необходимый дескриптор.

3) Функции, использующие долговременные ключи, будут возвращать ошибку, в случае если их срок действия истёк. Срок действия ключей ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012 составляет 1 год 3 месяца. Получить информацию о сроке действия ключа можно с помощью контрольной панели КриптоПро CSP (закладка **Сервис — Протестировать**), либо осуществить вызов функции CryptGetKeyParam с параметром KP\_NOTAFTER.

4) Для обеспечения контроля доверенности сертификатов открытых ключей при использовании СКЗИ под управлением ОС Windows при наличии корневого сертификата, установленного в доверенное хранилище КриптоПро локального компьютера (Доверенные корневые сертификаты КриптоПро CSP, CryptoPro Trusted Roots, CryptoProTrustedStore), осуществляется построение цепочки сертификатов. В случае, если такую цепочку построить невозможно, функция CertFindCertificateInStore, на вход которой передаётся структура CERT\_CONTEXT, соответствующая недоверенному сертификату, и функция проверки подписи CMS (CryptMsgControl), в случае если CMS-подпись не содержит указание на доверенный сертификат, будут завершаться с ошибкой. Для того, чтобы избавиться от ошибки, необходимо установить необходимый корневой сертификат в доверенное хранилище КриптоПро (см. ЖТЯИ.00101-02 91 02. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows).