

Программный комплекс «Litoria for Citrix»
Руководство системного программиста

Аннотация

В документе приводится руководство системного программиста программного комплекса «Litoria for Citrix» версия 3.0.2-5 (далее ПК «Litoria for Citrix», ПК или комплекс).

Раздел «Общие сведения о программном комплексе» содержит сведения о назначении, основных функциях, условиях применения комплекса, а также перечень входных и выходных данных комплекса.

В разделе «Структура ПК «Litoria for Citrix» указаны состав комплекса и взаимодействие его компонентов, описаны интерфейсы основных компонентов.

В соответствующих разделах приведена информация о действиях, которые необходимо выполнить перед использованием комплекса.

В разделе «Сообщения системному программисту» описаны пути к файлу, содержащему сообщения об ошибках, возникших при использовании ПК «Litoria for Citrix», а также приведены коды ошибок и их расшифровка.

Содержание

1	Общие сведения о программном комплексе	4
1.1	Описание функций программного комплекса	4
1.1.1	Создание ЭП	4
1.1.2	Передача информации по виртуальным каналам Citrix	4
1.2	Требования к техническим средствам	4
1.3	Требования к программному обеспечению	5
1.4	Общая характеристика входной и выходной информации	5
1.4.1	Входные данные	5
1.4.2	Выходные данные	5
2	Структура ПК «Litoria for Citrix»	6
2.1	Интерфейсы CVCServer.dll	9
2.1.1	Интерфейс GetCertificates	10
2.1.2	Интерфейс FindKeyContainer	10
2.1.3	Интерфейс CVCFreePtrMemory	10
2.1.4	Интерфейс SignHash	10
2.1.5	Интерфейс CVCStartCachingContainer	10
2.1.6	Интерфейс CVCEndCachingContainer	11
2.1.7	Интерфейс SignXML	11
3	Настройка комплекса	12
3.1	Подготовка среды использования	12
3.2	Установка и настройка криптопровайдера под управлением ОС Windows	13
3.3	Установка и настройка СКЗИ «КриптоПро CSP»	13
3.4	Установка комплекса	18
4	Сообщения системному программисту	19
4.1	Коды ошибок COM-сервиса	19
4.2	Коды ошибок библиотеки «cryptoPlatform»	19

1 Общие сведения о программном комплексе

ПК «Litoria for Citrix» предназначен для передачи криптографически защищенной информации с помощью технологии Citrix Virtual Channel (CVC) в системах юридически значимого документооборота, использующих терминальный доступ. Над передаваемой информацией может быть выполнена операция создания электронной подписи (ЭП) с использованием криптографической платформы «Litoria Crypto Platform» и криптопровайдера, реализованного в соответствии с технологией Microsoft Cryptographic Service Provider (CSP).

Комплекс состоит из серверной и клиентской частей. При использовании COM-интерфейсов серверной части программного комплекса «Litoria for Citrix» программист может осуществить следующие операции:

- создание усиленной ЭП для файлов произвольного типа;
- передача информации по виртуальным каналам Citrix.

1.1 Описание функций программного комплекса

1.1.1 Создание ЭП

Электронная подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки и полученный в результате криптографического преобразования информации с использованием ключа ЭП. С помощью ЭП можно идентифицировать владельца сертификата ключа проверки ЭП, а также установить отсутствие искажения информации в электронном документе.

Для создания ЭП должен быть осуществлен выбор сертификата ключа проверки ЭП.

1.1.2 Передача информации по виртуальным каналам Citrix

Передача информации по виртуальным каналам Citrix осуществляется при помощи COM-сервиса и динамических библиотек.

По виртуальным каналам может передаваться файл любого типа и размера.

1.2 Требования к техническим средствам

Минимальные требования к рабочей станции, на которую устанавливается клиентская часть ПК «Litoria for Citrix», обусловлены применением операционной системы (ОС): процессор P4, оперативная память 1 Гб, жесткий диск не менее 20Гб, видеоадаптер, свободный USB-порт при использовании электронных идентификаторов или других USB-устройств для хранения цифровых сертификатов.

Минимальные требования к производительности сервера, на который устанавливается

серверная часть ПК «Litoria for Citrix», обусловлены применением ОС.

1.3 Требования к программному обеспечению

Клиентская часть программного комплекса «Litoria for Citrix» функционирует под управлением следующих ОС:

- Windows 7 (32 бит/64 бит);
- Windows 8/8.1 (32 бит/64 бит);
- Windows 10 (32 бит/64 бит);
- RedOS версии 7.3 или выше (64 бит).

Серверная часть программного комплекса «Litoria for Citrix» функционирует под управлением следующих ОС:

- Windows Server 2008 R2;
- Windows Server 2012/2012R2/2016/2019 (64 бит).

Для работы комплекса дополнительно должно быть установлено следующее программное обеспечение:

- криптопровайдер, реализованный в соответствии с технологией Microsoft CSP;
- Microsoft .NET Framework 4.0;
- Citrix Receiver 3.4 или выше (для клиентской части комплекса);
- Citrix XenApp 6.0 или выше (для серверной части).

1.4 Общая характеристика входной и выходной информации

1.4.1 Входные данные

ПК «Litoria for Citrix» в совокупности с криптографической платформой «Litoria Crypto Platform» выполняет функцию создания ЭП для файлов произвольного типа.

1.4.2 Выходные данные

В результате выполнения операции создания ЭП на выходе ПК «Litoria for Citrix» может формировать файлы с расширениями, приведенными в таблице 1.1.

Таблица 1.1 – Расширения выходных файлов

Тип файла	Расширение файла	Назначение
Подписанный файл	.p7s, .sig	подписан в BASE-64
Подписанный файл	.xml	подписан в BASE-64

2 Структура ПК «Litoria for Citrix»

ПК «Litoria for Citrix» состоит из клиентской и серверной частей. Модульный состав комплекса представлен в таблице 2.1.

Таблица 2.1 – Модульный состав ПК

Название части комплекса	Имя файла	Назначение файла
Серверная часть	api-ms-win-core-console-l1-1-0.dll	Библиотеки, входящие в распространяемый пакет Microsoft Visual Studio C++, необходимые для запуска комплекса
	api-ms-win-core-console-l1-2-0.dll	
	api-ms-win-core-datetime-l1-1-0.dll	
	api-ms-win-core-debug-l1-1-0.dll	
	api-ms-win-core-errorhandling-l1-1-0.dll	
	api-ms-win-core-file-l1-1-0.dll	
	api-ms-win-core-file-l1-2-0.dll	
	api-ms-win-core-file-l2-1-0.dll	
	api-ms-win-core-handle-l1-1-0.dll	
	api-ms-win-core-heap-l1-1-0.dll	
	api-ms-win-core-interlocked-l1-1-0.dll	
	api-ms-win-core-libraryloader-l1-1-0.dll	
	api-ms-win-core-localization-l1-2-0.dll	
	api-ms-win-core-memory-l1-1-0.dll	
	api-ms-win-core-namedpipe-l1-1-0.dll	
	api-ms-win-core-processenvironment-l1-1-0.dll	
	api-ms-win-core-processthreads-l1-1-0.dll	
	api-ms-win-core-processthreads-l1-1-1.dll	
	api-ms-win-core-profile-l1-1-0.dll	
	api-ms-win-core-rtlsupport-l1-1-0.dll	
	api-ms-win-core-string-l1-1-0.dll	
	api-ms-win-core-synch-l1-1-0.dll	
	api-ms-win-core-synch-l1-2-0.dll	
	api-ms-win-core-sysinfo-l1-1-0.dll	
	api-ms-win-core-timezone-l1-1-0.dll	
	api-ms-win-core-util-l1-1-0.dll	
	api-ms-win-core-xstate-l2-1-0.dll	
	api-ms-win-crt-conio-l1-1-0.dll	
	api-ms-win-crt-convert-l1-1-0.dll	
	api-ms-win-crt-environment-l1-1-0.dll	
	api-ms-win-crt-filestream-l1-1-0.dll	
	api-ms-win-crt-heap-l1-1-0.dll	
	api-ms-win-crt-locale-l1-1-0.dll	
	api-ms-win-crt-math-l1-1-0.dll	
	api-ms-win-crt-multibyte-l1-1-0.dll	
	api-ms-win-crt-private-l1-1-0.dll	
	api-ms-win-crt-process-l1-1-0.dll	
	api-ms-win-crt-runtime-l1-1-0.dll	
	api-ms-win-crt-stdio-l1-1-0.dll	
	api-ms-win-crt-string-l1-1-0.dll	

	api-ms-win-crt-time-l1-1-0.dll api-ms-win-crt-utility-l1-1-0.dll concr140.dll msvc140.dll msvc140_1.dll msvc140_2.dll msvc140_atomic_wait.dll msvc140_codecvt_ids.dll ucrtbase.dll vcruntime140.dll	
	cryptoPlatform.dll	Библиотека программного интерфейса основных криптографических операций.
	CryptoPlatformCSharpWrapper.dll	Вспомогательная библиотека для обеспечения связи между SAPSign.dll и cryptoPlatform.dll
	CVCServer.dll	Библиотека для передачи информации между сервером и клиентом.
	Newtonsoft.Json.dll	Библиотека работы с JSON нотацией
	SAPSign.dll	СОМ-сервис, предоставляющий набор интерфейсов.
Клиентская часть	api-ms-win-core-console-l1-1-0.dll api-ms-win-core-console-l1-2-0.dll api-ms-win-core-datetime-l1-1-0.dll api-ms-win-core-debug-l1-1-0.dll api-ms-win-core-errorhandling-l1-1-0.dll api-ms-win-core-file-l1-1-0.dll api-ms-win-core-file-l1-2-0.dll api-ms-win-core-file-l2-1-0.dll api-ms-win-core-handle-l1-1-0.dll api-ms-win-core-heap-l1-1-0.dll api-ms-win-core-interlocked-l1-1-0.dll api-ms-win-core-libraryloader-l1-1-0.dll api-ms-win-core-localization-l1-2-0.dll api-ms-win-core-memory-l1-1-0.dll api-ms-win-core-namedpipe-l1-1-0.dll api-ms-win-core-processenvironment-l1-1-0.dll api-ms-win-core-processthreads-l1-1-0.dll api-ms-win-core-processthreads-l1-1-1.dll api-ms-win-core-profile-l1-1-0.dll api-ms-win-core-rtlsupport-l1-1-0.dll api-ms-win-core-string-l1-1-0.dll api-ms-win-core-synch-l1-1-0.dll api-ms-win-core-synch-l1-2-0.dll api-ms-win-core-sysinfo-l1-1-0.dll api-ms-win-core-timezone-l1-1-0.dll api-ms-win-core-util-l1-1-0.dll	Библиотеки, входящие в распространяемый пакет Microsoft Visual Studio C++, необходимые для запуска комплекса

	api-ms-win-core-xstate-l2-1-0.dll api-ms-win-crt-conio-l1-1-0.dll api-ms-win-crt-convert-l1-1-0.dll api-ms-win-crt-environment-l1-1-0.dll api-ms-win-crt-filesystem-l1-1-0.dll api-ms-win-crt-heap-l1-1-0.dll api-ms-win-crt-locale-l1-1-0.dll api-ms-win-crt-math-l1-1-0.dll api-ms-win-crt-multibyte-l1-1-0.dll api-ms-win-crt-private-l1-1-0.dll api-ms-win-crt-process-l1-1-0.dll api-ms-win-crt-runtime-l1-1-0.dll api-ms-win-crt-stdio-l1-1-0.dll api-ms-win-crt-string-l1-1-0.dll api-ms-win-crt-time-l1-1-0.dll api-ms-win-crt-utility-l1-1-0.dll concurt140.dll msvcp140.dll msvcp140_1.dll msvcp140_2.dll msvcp140_atomic_wait.dll msvcp140_codecvt_ids.dll ucrtbase.dll vcruntime140.dll	
	cryptoPlatform.dll	Библиотека программного интерфейса основных криптографических операций.
	CVCCClient.dll	Библиотека для передачи информации между сервером и клиентом

Взаимодействие компонентов комплекса представлено на рисунке 2.1.

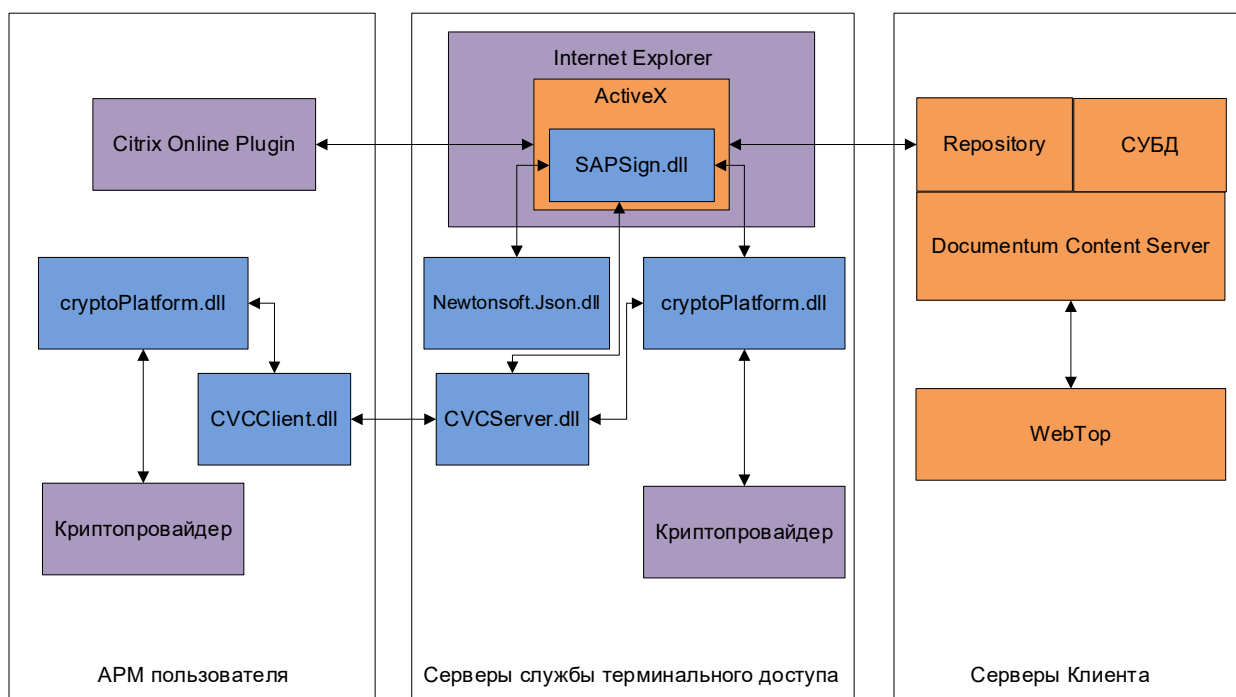


Рисунок 2.1 – Взаимодействие компонентов комплекса

На сервере библиотека CVCTServer.dll предоставляет ActiveX компоненту dll-интерфейсы, с помощью которых вызываются криптографические функции библиотеки cryptoPlatform.dll. Для передачи информации по виртуальным каналам от сервера клиенту и обратно используются интерфейсы библиотек CVCTServer.dll и CVCCClient.dll. На клиентском рабочем месте обмен данными происходит между виртуальными каналами и библиотекой cryptoPlatform.dll.

2.1 Интерфейсы CVCTServer.dll

Описание и назначение интерфейсов библиотеки CVCTServer.dll представлены в таблице 2.2.

Таблица 2.2 – Интерфейсы библиотеки CVCTServer.dll

Интерфейс	Назначение
InitCVCTServer	Инициализация CVC сервера
DelInitCVCTServer	Деинициализация CVC сервера
GetCertificates	Получение списка сертификатов
FindKeyContainer	Поиск контейнера ключа по сертификату
CVCFreePtrMemory	Освобождение выделенной памяти
CVCStartCachingContainer	Начало кеширования контейнера
CVCEndCachingContainer	Окончание кеширования контейнера
SignCMS	Подпись cms
SignXML	Подпись xml

2.1.1 Интерфейс InitCVCServer

Заголовок объявления интерфейса:

```
void InitCVCServer();
```

2.1.2 Интерфейс DelInitCVCServer

Заголовок объявления интерфейса:

```
void DelInitCVCServer();
```

2.1.3 Интерфейс CVCFreePtrMemory

Заголовок объявления интерфейса:

```
void CVCFreePtrMemory(char*& memory);
```

Входные параметры:

memory – указатель на память, которую необходимо освободить.

2.1.4 Интерфейс GetCertificates

Заголовок объявления интерфейса:

```
bool GetCertificates(const char* store, char*& response, unsigned int& length);
```

Входные параметры:

store – название хранилища сертификатов;

response – результат выполнения операции (ответ);

length – длина результата операции (ответа).

2.1.5 Интерфейс FindKeyContainer

Заголовок объявления интерфейса:

```
bool FindKeyContainer(const char* certificateBase64, const char* pinCode, char*& response,  
unsigned int& responseLength);
```

Входные параметры:

certificateBase64e – сертификат в формате base64;

pinCode – ПИН-код к контейнеру;

response – результат выполнения операции (ответ);

responseLength – длина результата операции (ответа).

2.1.6 Интерфейс CVCStartCachingContainer

Заголовок объявления интерфейса:

```
bool CVCStartCachingContainer(const char* certificateBase64, const char* pinCode, char*&  
response, unsigned int& responseLength);
```

Входные параметры:

certificateBase64 – сертификат в формате base64;

pinCode – ПИН-код к контейнеру;

response – результат выполнения операции (ответ);

responseLength – длина результата операции (ответа).

2.1.7 Интерфейс CVCEndCachingContainer**Заголовок объявления интерфейса:**

bool CVCEndCachingContainer(char& response, unsigned int& responseLength);*

Входные параметры:

response – результат выполнения операции (ответ);

responseLength – длина результата операции (ответа).

2.1.8 Интерфейс SignCMS**Заголовок объявления интерфейса:**

bool SignCMS(const char data, unsigned int dataSize, const char* certificateBase64, const char* pinCode, const char* hashAlgorithm, unsigned int flags, const char* tspAddress, char*& response, unsigned int& responseLength);*

Входные параметры:

data – данные для подписи;

dataSize – размер данных для подписи;

certificateBase64 – сертификат в формате base64;

pinCode – ПИН-код к контейнеру;

hashAlgorithm – алгоритм хеширования;

flags – флаги, определяющие тип подписи (отделённая = 0x00000001; усовершенствованная = 0x00000200; со штампом времени = 0x00000400;).

tspAddress – адрес службы штампов времени;

response – результат выполнения операции (ответ);

responseLength – длина результата операции (ответа).

2.1.9 Интерфейс SignXML**Заголовок объявления интерфейса:**

bool SignXML(const char data, unsigned int dataSize, const char* pTransformBlock, const char* certificateBase64, const char* pinCode, const char* pHashAlgorithm, const char* pSignAlgorithm, unsigned int flags, const char* tspAddress, unsigned int xmlType, char*&*

response, unsigned int& responseLength);

Входные параметры:

data – данные для подписи;

dataSize – размер данных для подписи;

pTransformBlock – блок трансформации (только для старого типа документов), необходим, чтобы указать оригинальный путь внутри большого документа, так как подписывается только часть документа;

certificateBase64 – сертификат в формате base64;

pinCode – пин-код к контейнеру;

hashAlgorithm – алгоритм хеширования;

pSignAlgorithm – алгоритм подписи;

flags – флаги, определяющие тип подписи (отделённая = 0x00000001; усовершенствованная = 0x00000200; со штампом времени = 0x00000400;).

tspAddress – адрес службы штампов времени;

xmlType – тип xml файла, который необходимо подписать: 0(старый тип), 1(для ISO20022);

response – результат выполнения операции (ответ);

responseLength – длина результата операции (ответа).

3 Настройка комплекса

3.1 Подготовка среды использования

Для использования ПК «Litoria for Citrix» необходим терминальный сервер и учетная запись пользователя.

Для настройки выбранной учетной записи необходимо выполнить следующие действия:

1. Выпустить сертификат и записать его на смарт-карту.
2. На терминальном сервере опубликовать приложение «%windir%\system32\cmd.exe».
3. На сервере создать интерактивный сеанс (должен появиться профиль пользователя).
4. На сервере и клиенте под управлением ОС Windows установить криптопровайдер, реализованный в соответствии с технологией Microsoft CSP. На клиенте под

управлением ОС Linux установить СКЗИ «КриптоПро CSP»¹ с поддержкой графического представления.

5. При использовании электронного идентификатора eToken в оснастке криптопровайдера для всех носителей типа eToken отключить опцию, определяющую использование eToken для входа в ОС.

3.2 Установка и настройка криптопровайдера под управлением ОС Windows

Прежде чем приступать к получению и установке дистрибутива криптопровайдера, необходимо убедиться, что операционная система установлена, настроена и пользователь, который выполняет установку, обладает необходимыми правами на установку программного обеспечения.

Установка дистрибутива криптопровайдера должна производиться пользователем, имеющим права администратора, в соответствии с эксплуатационной документацией на использование криптопровайдера под управлением ОС Windows.

3.3 Установка и настройка СКЗИ «КриптоПро CSP»

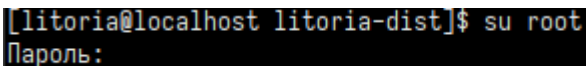
Прежде чем приступать к получению и установке дистрибутива СКЗИ «КриптоПро CSP», необходимо убедиться, что операционная система установлена, настроена и пользователь, который выполняет установку, обладает необходимыми правами на установку программного обеспечения.

Установка дистрибутива СКЗИ «КриптоПро CSP» должна производиться пользователем, имеющим права администратора, в соответствии с эксплуатационной документацией на использование СКЗИ под управлением соответствующей ОС семейства Linux.

Дистрибутив СКЗИ «КриптоПро CSP» можно приобрести на сайте <https://cryptopro.ru> для ОС AltLinux, RedOS в виде пакета *.rpm (linux-amd64_rpm.tgz)*.

Для установки СКЗИ «КриптоПро CSP» в ОС RedOS необходимо выполнить следующие действия:

1. Выполнить вход под учетной записью администратора (рисунок 3.1) `su root`.



```
[litoria@localhost litoria-dist]$ su root
Пароль:
```

Рисунок 3.1 – Вход под учетной записью администратора

2. Извлечь все файлы из архива с помощью команды `tar -xzvf linux-amd64.tgz` (рисунок 3.2).

¹ Установка и настройка СКЗИ «КриптоПро CSP» описана в разделе 3.3.

```
[litoria@localhost litoria-dist]$ tar -zxvf linux-amd64.tgz
linux-amd64/
linux-amd64/cprocsp-stunnel-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-rdr-vityaz-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-rdr-ancud-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-jakarta-64-5.0.1148-4.x86_64.rpm
linux-amd64/cprocsp-cptools-gtk-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-cpopenssl-110-devel-5.0.11635-6.noarch.rpm
linux-amd64/cprocsp-curl-64-5.0.11635-6.x86_64.rpm
linux-amd64/install_gui.sh
linux-amd64/lsb-cprocsp-rdr-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-pkcs11-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-capilite-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-rdr-maxim-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-rutoken-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-ca-certs-5.0.11635-6.noarch.rpm
linux-amd64/cprocsp-rdr-novacard-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-rosan-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-rdr-accord-64-5.0.11635-6.x86_64.rpm
linux-amd64/linux-amd64.ini
linux-amd64/lsb-cprocsp-rdr-crypton-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-xer2print-5.0.11635-6.noarch.rpm
linux-amd64/sobol-1-8.src.rpm
linux-amd64/cprocsp-rdr-emv-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-devel-5.0.11635-6.noarch.rpm
linux-amd64/integrity.sh
linux-amd64/cprocsp-rdr-esmart-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-cpfkc-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-mskey-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-ipsec-esp-64-5.0.11635-6.src.rpm
linux-amd64/install.sh
linux-amd64/lsb-cprocsp-kc1-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-drv-64-5.0.11635-6.src.rpm
linux-amd64/cprocsp-ipsec-devel-5.0.11635-6.noarch.rpm
linux-amd64/cprocsp-ipsec-genpsk-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-gui-gtk-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rsa-64-5.0.11635-6.x86_64.rpm
linux-amd64/ifd-rutokens-1.0.1-1.x86_64.rpm
linux-amd64/lsb-cprocsp-base-5.0.11635-6.noarch.rpm
linux-amd64/uninstall.sh
linux-amd64/cprocsp-ipsec-ike-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-inpasport-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-cloud-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-drv-devel-5.0.11635-6.noarch.rpm
linux-amd64/cprocsp-cpopenssl-110-gost-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-cloud-gtk-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-cpopenssl-110-base-5.0.11635-6.noarch.rpm
linux-amd64/cprocsp-rdr-pcsc-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-compat-altlinux-64-1.0.0-1.noarch.rpm
linux-amd64/install.desktop
linux-amd64/cprocsp-cpopenssl-110-64-5.0.11635-6.x86_64.rpm
linux-amd64/cpverify
linux-amd64/cprocsp-rdr-kst-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-kc2-64-5.0.11635-6.x86_64.rpm
linux-amd64/lsb-cprocsp-rdr-sobol-64-5.0.11635-6.x86_64.rpm
linux-amd64/cprocsp-rdr-infocrypt-64-5.0.11635-6.x86_64.rpm
[litoria@localhost litoria-dist]$
```

Рисунок 3.2 – Распаковка архива СКЗИ «КриптоПро CSP»

3 Перейти в директорию распаковки архива СКЗИ «КриптоПро CSP» с помощью

команды `cd linux-amd64`.

4 Запустить установку СКЗИ «КриптоПро CSP» с помощью скрипта `./install_gui.sh` (рисунок 3.3).

```
[root@localhost litoria-dist]# cd linux-amd64/  
[root@localhost linux-amd64]# ./install_gui.sh |
```

Рисунок 3.3 – Запуск установки СКЗИ «КриптоПро CSP»

5 В результате выполнения скрипта появится графическая консоль установки СКЗИ «КриптоПро CSP» (рисунок Рисунок 3.4).

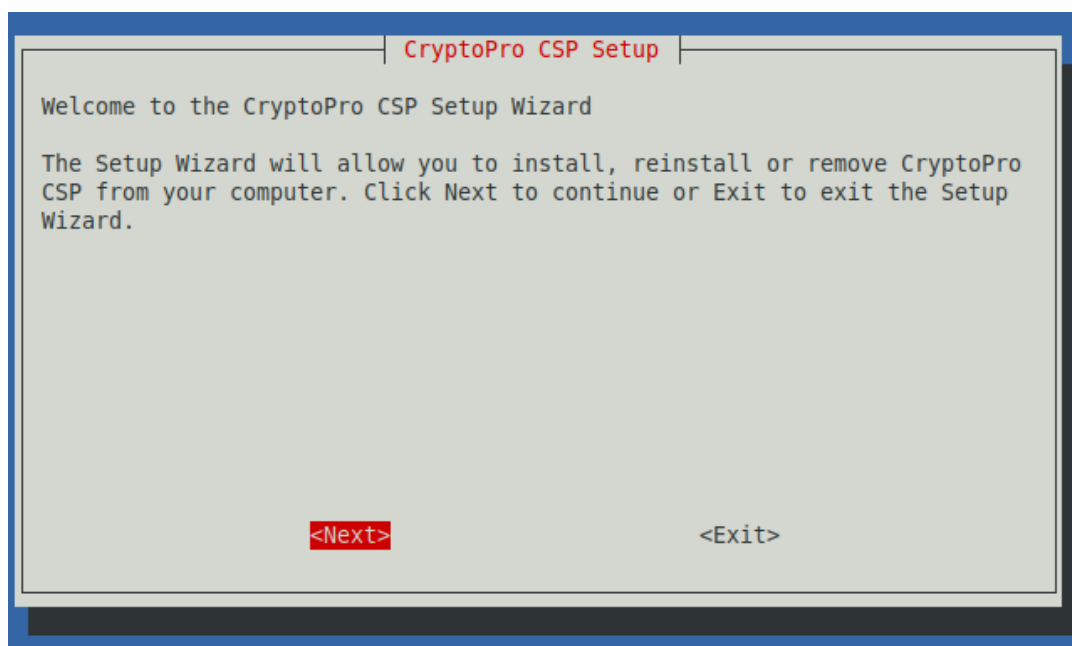


Рисунок 3.4 – Графическая консоль установки СКЗИ «КриптоПро CSP»

6 Нажать **«Next»** для продолжения установки СКЗИ «КриптоПро CSP».

7 В следующем окне выбрать компоненты для установки в соответствии с рисунком 3.5 и нажать **«Next»** для продолжения установки.

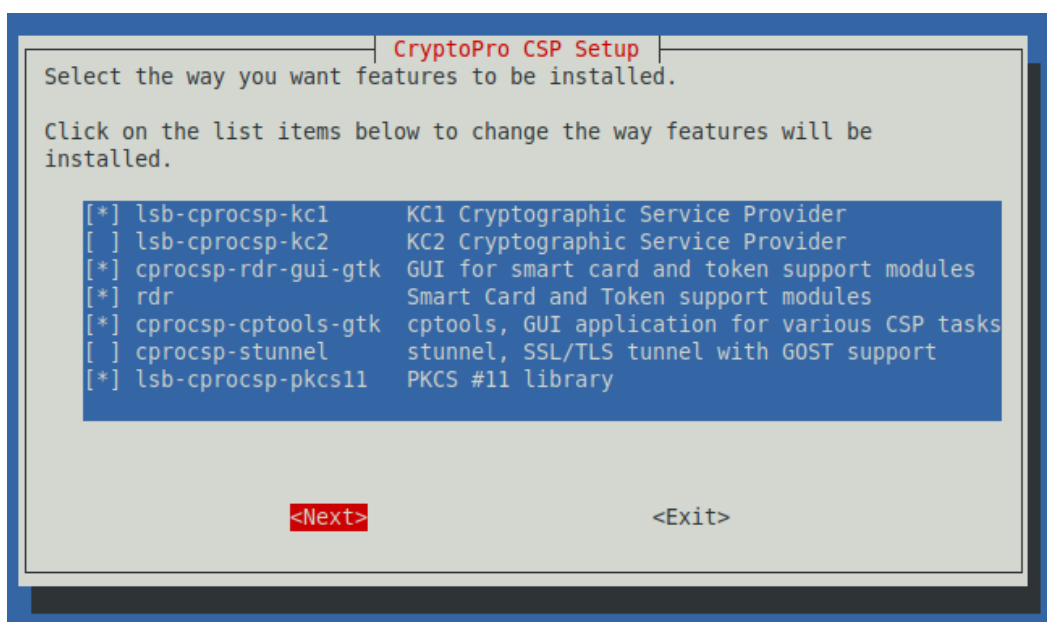


Рисунок 3.5 – Выбор компонентов для установки

8 В появившемся окне подтвердить выбор устанавливаемых компонентов по кнопке **«Install»** (рисунок 3.6).

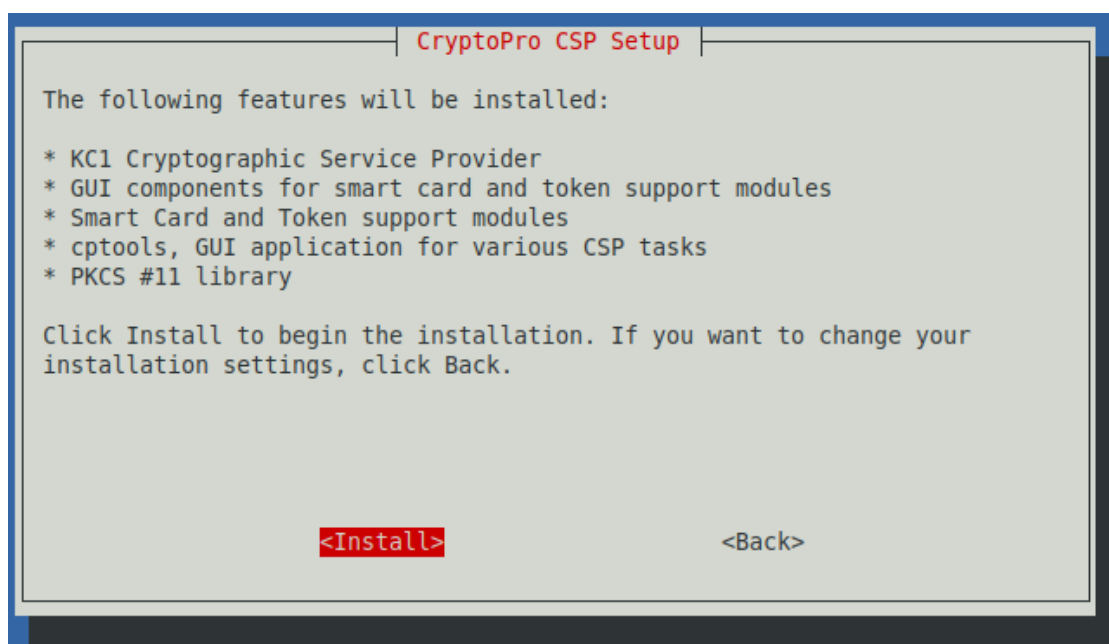
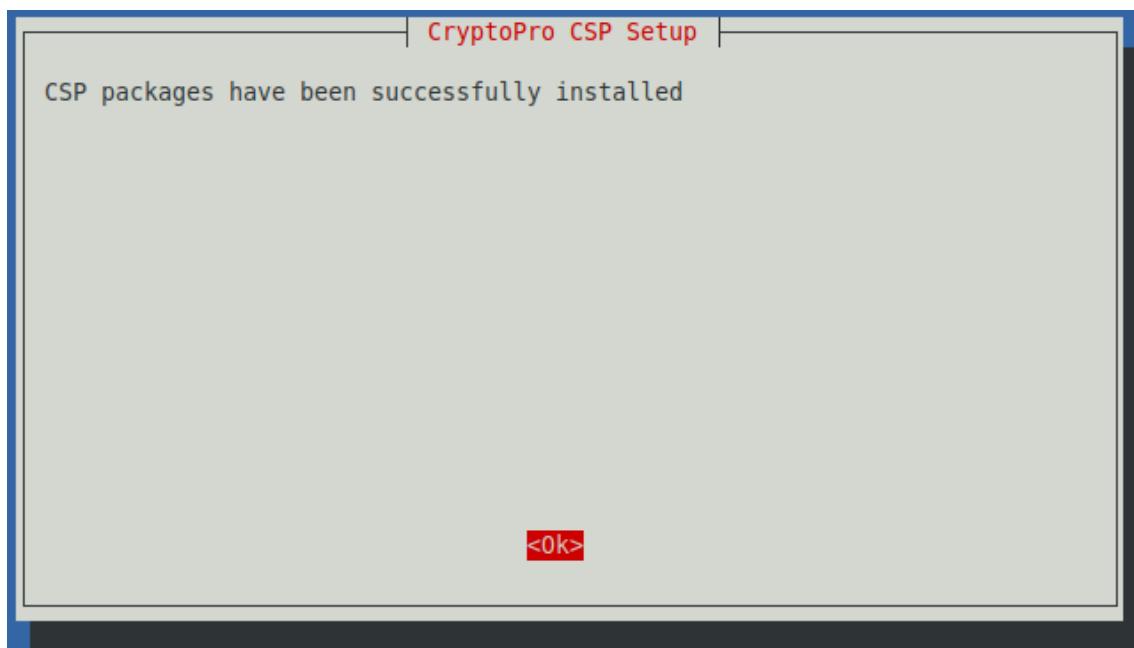


Рисунок 3.6 – Подтверждение установки компонентов СКЗИ

9 По завершению установки в окне с сообщением об успешной установке выбранных компонентов СКЗИ «КриптоПро CSP» нажать **«Ok»** (рисунок 3.7).



10 Рисунок 3.7 – Успешная установка компонентов СКЗИ «КриптоПро CSP»

В случае неудачной установки, необходимо изучить сообщение об ошибке, выводимое в консоли, и обратиться в техподдержку СКЗИ «КриптоПро CSP».

11 В следующем окне нажать **«Enter the license now»** для активации приобретенной лицензии СКЗИ «КриптоПро CSP» или отложить ввод лицензии по кнопке **«Later»** (рисунок 3.8).

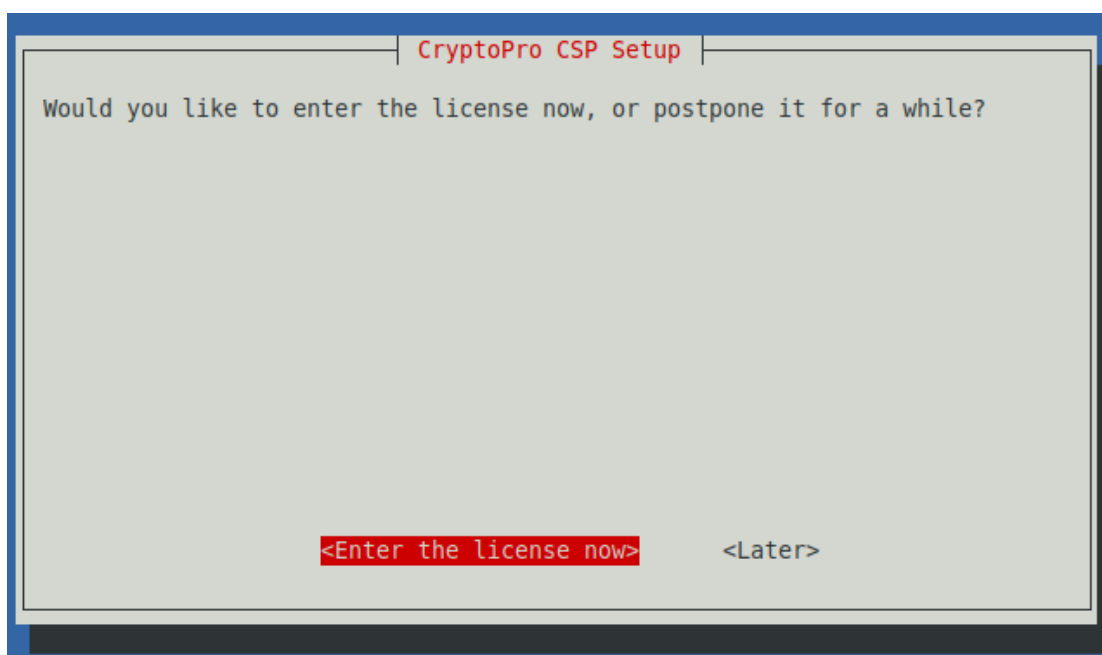


Рисунок 3.8 – Активация лицензии СКЗИ «КриптоПро CSP»

12 В следующем окне для выхода из графической консоли установки СКЗИ

«КриптоПро CSP» нажать **«Exit»** (рисунок 3.9).

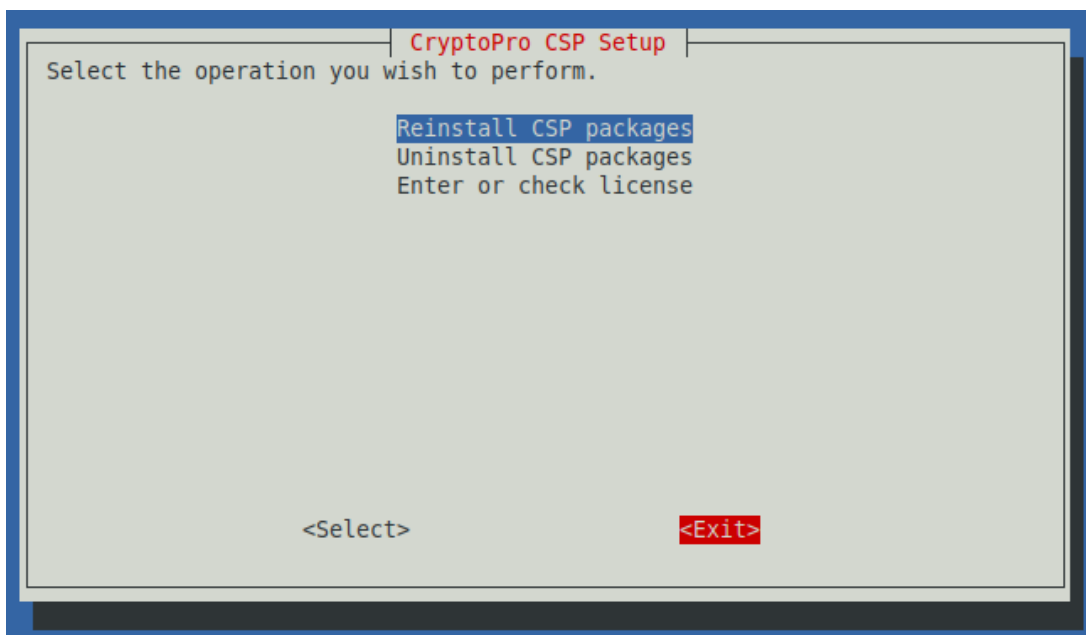


Рисунок 3.9 – Выход из графической консоли СКЗИ «КриптоПро CSP»

3.4 Установка комплекса

Установка серверной части и клиентской части ПК «Litoria for Citrix» описана в документах «ПК «Litoria for Citrix». Руководство по инсталляции (клиент)» и «ПК «Litoria for Citrix». Руководство по инсталляции (сервер)».

4 Сообщения системному программисту

Вся информация об ошибках, произошедших в ПК «Litoria for Citrix», записывается в файл DigSignSerLogs.txt. Расположение файла зависит от используемой ОС (например, «C:\Users\%user_name%\AppData\»).

4.1 Коды ошибок COM-сервиса

В таблице 4.1 указаны коды ошибок, возвращаемые COM-сервисом.

Таблица 4.1 – Коды ошибок, возвращаемые COM-сервисом

Имя ошибки	Номер ошибки	Текст ошибки
CAN_NOT_OPEN_FILE	7801	Ошибка открытия файла.
FILE_HAS_NULL_SIZE	7802	Ошибка работы с файлом. Файл имеет нулевую длину.
CAN_NOT_COPY_FILE	7803	Ошибка копирования файла.
CITRIX_CHANNEL_ERROR	7898	Ошибка работы с виртуальными каналами Citrix.
FUNCTION_CALL_ERROR	7899	Ошибка вызова функции внутри COM-объекта.

4.2 Коды ошибок библиотеки «cryptoPlatform»

В таблице 4.2 указаны коды ошибок, возвращаемые библиотекой «cryptoPlatform».

Таблица 4.2 – Коды ошибок, возвращаемые библиотекой «cryptoPlatform»

№	Имя ошибки	Номер ошибки	Текст ошибки
1.	INIT_CREATE_EDS_ERROR	1000	Ошибка инициализации данных для создания ЭП.
2.	INVALID_CERTIFICATE_BLOB	1001	Неверный блок сертификата подписчика.
3.	NOT_FIND_CERT_IN_MY	1002	Сертификат подписчика отсутствует в хранилище "Личные".
4.	NOT_FIND_HASH_ALG	1003	Алгоритм хэширования не определен.
5.	SIGNING_CERTIFICATE_V2_ERROR	1004	Ошибка формирования атрибута SignerCertificateV2.
6.	SIGNING_CERTIFICATE_ERROR	1005	Ошибка формирования атрибута SignerCertificate.
7.	INIT_FUNC_PARAM_ERROR	1006	Ошибка инициализации параметров функции. Неверный параметр.
8.	NOT_FIND_CRYPT_ALG	1007	Подходящий криптографический алгоритм не определен.
9.	START_CACHING_CONTAINER_ERROR	1008	Ошибка в функции кэширования контейнера.
10.	END_CACHING_CONTAINER_ERROR	1009	Ошибка в функции отмены кэширования контейнера.
11.	CREATE_HASH_ERROR	2000	Ошибка вычисления хэш-значения.

№	Имя ошибки	Номер ошибки	Текст ошибки
12.	GET_APPROPRIATE_CP_ERROR	2001	Не удалось найти подходящий криптопровайдер.
13.	GET_HASH_ALG_ID_ERROR	2002	Не удалось получить подходящий алгоритм хэширования.
14.	ININ_HASH_FILE_ERROR	2003	Ошибка инициализации данных для хэширования файла.
15.	HASHING_FILE_ERROR	2004	Ошибка хэширования файла.
16.	GET_HASH_RESULT_ERROR	2005	Ошибка получения результата хэширования файла.
17.	HASH_ALG_ERROR	2006	Для инициализации механизма хэширования передан алгоритм, не являющийся алгоритмом хэширования.
18.	CREATE_EDS_ERROR	3000	Ошибка создания ЭП.
19.	SIGN_ALG_ERROR	3001	Для инициализации механизма подписи передан алгоритм, не являющийся алгоритмом подписи.
20.	GET_SIGN_PARAM_ERROR	3002	Ошибка определения параметров создания ЭП.
21.	JOIN_SIGN_HASH_ALG_ERROR	3003	Не удалось определить комбинированный алгоритм вычисления хэш-значения и подписи.
22.	FORMAT_EDS_UNKNOWN	3004	Формат создаваемой подписи задан некорректно.
23.	ADD_EDS_ERROR	4000	Ошибка добавления ЭП.
24.	GET_EXISTING_SIGNS_ERROR	4001	Не удалось получить значения подписей из сообщения.
25.	NULL_HMSG	4002	Неверный дескриптор сообщения.
26.	GET_NEW_SIGNER_INDEX_ERROR	4003	Ошибка получения индекса добавленной подписи.
27.	COORDINATE_EDS_ERROR	4004	Ошибка заверки подписи.
28.	INIT_ADD_EDS_BY_HASH_ERROR	4005	Не удалось сформировать данные для удаленной подписи хэш-значения.
29.	SEPARATE_DATA_SIGN_ERROR	4006	Разделение подписанного документа на составляющие не произведено.
30.	ADD_INT0_TO_SIGN_ERROR	4007	Не удалось обновить подпись необходимой дополнительной информацией.
31.	ADD_HASH_EDS_JOIN_ERROR	4008	Произошла ошибка в процессе объединения компонент механизма добавления подписи через удаленную подпись хэш-значения.
32.	JOIN_SIGN_ERROR	4009	Ошибка объединения 2-х отделенных ЭП.
33.	SIGN_HASH_ERROR	4010	Ошибка подписи хэш-значения.
34.	FORMAT_CMS_ERROR	4011	Не удалось сформировать CMS.
35.	ADD_COORD_ARCHIVAL_SIGNATU RE_ERROR	4012	Некорректно осуществлять заверение или добавление подписи, если сообщение содержит одну или несколько подписей с архивными штампами времени.
36.	UPGRADE_SIGNET_TO_ADVANCED _ERROR	5000	Ошибка усовершенствования ЭП.
37.	GET_SIGN_ONLY_ERROR	5001	Не удалось получить значение подписи.

№	Имя ошибки	Номер ошибки	Текст ошибки
38.	GET_SIGNER_CERT_ERROR	5002	Не удалось получить информацию о сертификате подписавшего лица.
39.	SEND_REQUEST_ERROR	5003	Не удалось получить информацию из сети.
40.	SIGNER_CERT_CHAIN_ERROR	5004	Цепочка сертификата подписавшего лица составлена не корректно.
41.	TSP_CERT_CHAIN_ERROR	5005	Цепочка сертификата TSA-оператора составлена не корректно.
42.	OCSP_CERT_CHAIN_ERROR	5006	Цепочка сертификата OCSP-оператора составлена не корректно.
43.	CREATE_REVOCATION_VALUES_ERROR	5007	Ошибка формирования атрибутов RevocationValues и CompleteRevocationRefs.
44.	CREATE_CERTIFICATE_VALUES_ERROR	5008	Ошибка формирования атрибутов CompleteCertificateRefs и CertificateValues.
45.	CHECK_PROOF_VALIDITY_ERROR	5009	Ошибка проверки используемых сертификатов на действительность относительно времени внешнего штампа.
46.	SIGNER_CERT_VERIFY_TIME_ERROR	5010	Один или несколько сертификатов цепочки сертификата подписавшего лица недействителен.
47.	TSP_CERT_VERIFY_TIME_ERROR	5011	Один или несколько сертификатов цепочки сертификата TSA-оператора недействителен.
48.	OCSP_CERT_VERIFY_TIME_ERROR	5012	Один или несколько сертификатов цепочки сертификата OCSP-оператора недействителен.
49.	ADD_UNSIGNED_ATTR_ERROR	5013	Ошибка добавления неподписанного атрибута в подпись.
50.	GET_RESULT_ERROR	5014	Ошибка получения результата операции.
51.	GET_CERT_REV_ERROR	5015	Ошибка получения информации об отзыве сертификата.
52.	GET_REV_REF_ERROR	5016	Ошибка формирования ссылки на значение отзыва.
53.	GET_CERT_REF_ERROR	5017	Ошибка формирования ссылки на значение сертификата.
54.	CREATE_XADES_MANIFEST_ERROR	5018	Ошибка создания манифеста XAdES.
55.	CREATE_XADES_RECEIPT_ERROR	5019	Ошибка создания квитанции XAdES.
56.	EXTRACT_RECEIPT_ERROR	5020	Ошибка извлечения квитанции.
57.	XADES_SIGN_ERROR	5021	Ошибка подписи XAdES.
58.	XADES_SIGNED_RECEIPT_ERROR	5022	Ошибка создания подписанной квитанции XAdES.
59.	ADD_RECEIPT_TO_SIGNATURE_ERROR	5023	Ошибка добавления подписанной квитанции в ЭП, на которую эта квитанция создавалась.
60.	VERIFY_XADES_ERROR	5024	Ошибка проверки подписи XAdES.
61.	VERIFY_MANIFEST_ERROR	5025	Ошибка проверки манифеста.
62.	GET_RECEIPT_ERROR	5026	Ошибка получения информации по квитанции.
63.	GET_SIGNATURE_CERT_ERROR	5027	Ошибка получения сертификата подписчика XAdES.

№	Имя ошибки	Номер ошибки	Текст ошибки
64.	ADD_SIGNATURE_NODE_TO_DOCUMENT_ERROR	5028	Ошибка добавления узла с готовой подписью в документ.
65.	CREATE_SOAP_ERROR_RESPONSE	5029	Не удалось создать SOAP конверт с технологическим сообщением об ошибке.
66.	ERROR_PARSE_XML_BUFFER_TO_DOM_OBJECT	5030	Ошибка перевода буфера xml данных в DOM объект.
67.	ERROR_SERIALIZE_SIGNATURE_TO_BUFFER	5031	Ошибка сериализации объекта подписи в буфер.
68.	ERROR_PARSE_RECEIPT_FROM_BUFFER	5032	Ошибка разбора блока данных квитанции из буфера.
69.	ERROR_PARSE_MANIFEST_FROM_BUFFER	5033	Ошибка разбора манифеста из буфера.
70.	ERROR_PARSE_QUALIFYING_PROPERTIES_FROM_STREAM	5034	Ошибка разбора секции QualifyingProperties xml подписи из потока.
71.	ERROR_PARSE_SIGNATURE_FROM_STREAM	5035	Ошибка разбора подписи из потока.
72.	NO_SIGNER_CERTIFICATE	5036	В подписи отсутствует сертификат подписчика.
73.	TOO_MANY_CERTIFICATES_IN_SIGNATURE	5037	В подписи присутствует больше одного сертификата.
74.	ERROR_PARSING_INPUT_DOCUMENT	5038	Ошибка разбора входного документа.
75.	GET_IN_TIME_STAMP_ERROR	6000	Не удалось получить штамп времени на значение подписи или он не корректен.
76.	GET_OUT_TIME_STAMP_ERROR	6001	Не удалось получить штамп времени на доказательства подписи или он не корректен.
77.	TSP_RESPONSE_STATUS_ERROR	6002	Статус ответа службы штампов времени не корректен.
78.	CHECK_TSP_SIGNATURE_ERROR	6003	Полученный штамп времени содержит ошибки.
79.	TSP_CERT_ERROR	6004	Не удалось получить информацию о сертификате TSA-оператора.
80.	TSP_NEEDED_OID_ERROR	6005	Сертификат службы штампов времени не предназначен для установки отметки времени.
81.	VERIFY_TSP_SIGNATURE_ERROR	6006	Подпись штампа времени математически не корректна.
82.	GET_TIME_IN_TIME_STAMP_ERROR	6007	Ошибка получения времени создания внутреннего штампа времени.
83.	GET_TIME_OUT_TIME_STAMP_ERROR	6008	Ошибка получения времени создания внешнего штампа времени.
84.	UPGRADE_IN_TIME_STAMP_ERROR	6009	Не удалось собрать доказательства действительности внутреннего штампа времени.
85.	UNKNOWN_HASH_ALG_ERROR	6010	В запросе указан неизвестный системе алгоритм.
86.	NON_HASH_ALG_ERROR	6011	Указанный в запросе алгоритм не является алгоритмом хеширования.
87.	SIZE_HASH_VALUE_ERROR	6012	Указанный алгоритм поддерживается системой, однако длина хэш-значения не соответствует требуемой.

№	Имя ошибки	Номер ошибки	Текст ошибки
88.	CREATE_TSP_REQUEST_ERROR	6013	Ошибка создания TSP-запроса.
89.	NOT_SUPP_HASH_OID_ERROR	6014	Алгоритм хэширования указанный в запросе не поддерживается для обработки.
90.	GET_CRL_ERROR	7000	Необходимый список отзыва сертификатов не найден.
91.	GET_LOCAL_CRL_ERROR	7001	Ошибка получения списка отзыва из хранилища.
92.	DOWNLOAD_CRL_ERROR	7002	Ошибка получения основного списка отзыва из сети.
93.	CERT_CRL_LOCAL_ERROR	7003	Для проверки передан пустой сертификат.
94.	STORE_CA_ERROR	7004	Ошибка доступа к хранилищу промежуточных центров сертификации.
95.	STORE_ROOT_ERROR	7005	Ошибка доступа к хранилищу корневых центров сертификации.
96.	CERT_CRL_REVOKED	7006	Проверяемый сертификат отозван по списку отзыва.
97.	GET_CRL_URLS_ERROR	7007	Ошибка получения точек распространения списка отзыва.
98.	CRL_NOT_URLS	7008	Сертификат не содержит ни одной точки распространения основного списка отзыва.
99.	CRL_CDP_ERROR	7009	Не удалось определить формат точки распространения списка отзыва.
100.	CRL_TIME_VALIDITY_ERROR	7010	Полученный список отзыва недействительный по времени.
101.	ADD_CRL_TO_STORE_ERROR	7011	Не удалось установить список отзыва в хранилище сертификатов.
102.	CREATE_OCSP_REQUEST_ERROR	7012	Ошибка создания OCSP-запроса.
103.	GET_OCSP_URLS_ERROR	7013	Ошибка получения точек распространения OCSP.
104.	OCSP_NOT_URLS	7014	Сертификат не содержит ни одной точки распространения OCSP.
105.	OCSP_CDP_ERROR	7015	Не удалось определить формат точки распространения OCSP.
106.	GET_ISSUER_ERROR	7016	Поставщик сертификата не определен.
107.	GET_OCSP_RESPONSE_ERROR	7017	Не удалось получить OCSP-ответ.
108.	OCSP_CERT_ERROR	7018	Сертификат OCSP-оператора не определен.
109.	VERIFY_CERT_CHAIN_ERROR	7019	Цепочка проверяемого сертификата составлена некорректно.
110.	VERIFY_CERT_ISSUER_ERROR	7020	Издатель сертификата не определен, либо сертификат самоподписанный.
111.	VERIFY_CERT_BY_CRL_ERROR	7021	Не удалось проверить сертификат по списку отзыва.
112.	VERIFY_CERT_BY_OCSP_ERROR	7022	Не удалось проверить сертификат по OCSP.
113.	FORMATE_CRL_ERROR	7023	Не удалось сформировать список отзыва сертификатов.
114.	FILL_CRL_INFO_ERROR	7024	Ошибка формирования структуры информации списка отзыва сертификатов.

№	Имя ошибки	Номер ошибки	Текст ошибки
115.	SIGN_CRL_INFO_ERROR	7025	Ошибка подписи информации списка отзыва сертификатов.
116.	CERT_OCSP_REVOKED	7026	Проверяемый сертификат отозван по OCSP.
117.	CHECK_CRL_SIGN_ERROR	7028	Ошибка проверки целостности списка отзыва. Список отзыва поврежден или некорректен.
118.	GET_CRL_ISSUER_ERROR	7029	Издатель списка отзыва не определен.
119.	CRL_ISSUER_INFO_UNKNOW	7030	В проверяемом списке отзыва сертификатов отсутствует информация об издателе.
120.	OCSP_RESPONSE_ERROR_STATU S	7031	Статус ответа некорректен.
121.	CHAIN_CERT_OCSP_OPERATOR_E RROR	7032	Ошибка построения цепочки сертификата OCSP-службы.
122.	CHECK_OCSP_RESP_SIGN_ERROR	7033	Ошибка проверки целостности OCSP-ответа.
123.	GET_MAIN_CRL_ERROR	7034	Основной список отзыва не определен.
124.	DOWNLOAD_DELTA_CRL_ERROR	7035	Ошибка получения разностного списка отзыва из сети.
125.	FIND_CRL_ERROR	7036	Ошибка поиска списков отзыва для проверяемого сертификата.
126.	GET_DELTA_CRL_ERROR	7037	Необходимый для проверки разностный список отзыва не определен.
127.	PARSE_OCSP_REQ_ERROR	7100	Ошибка разбора OCSP-запроса.
128.	VERIFY_OCSP_REQ_SIGN_ERROR	7101	Ошибка проверки целостности OCSP-запроса.
129.	INIT_CONVERT_ERROR	8000	Ошибка инициализации преобразования отдельной ЭП в присоединенную.
130.	CONVERT_ERROR	8001	Ошибка преобразования отдельной ЭП в присоединенную.
131.	WRITE_HEADER_ERROR	8002	Ошибка записи заголовка подписи в результирующий файл.
132.	WRITE_DATA_ERROR	8003	Ошибка записи данных в результирующий файл.
133.	WRITE_EDS_ERROR	8004	Ошибка записи данных подписи в результирующий файл.
134.	PROXY_NAME_PASS_ERROR	9000	Необходимые имя пользователя и пароль для прокси заданы не верно.
135.	SEND_HTTP_REQUEST_ERROR	9001	Ошибка сетевого обращения.
136.	VERIFY_TYPE_EDS_ERROR	10000	Ошибка определения типа подписи.
137.	INIT_VERIFY_EDS_ERROR	10001	Ошибка инициализации данных для проверки ЭП.
138.	VERIFY_EDS_VALUE_ERROR	10002	Ошибка проверки математической целостности подписи.
139.	GET_FILE_TYPE_ERROR	10003	Ошибка определения типа данных в файле.
140.	GET_MESSAGE_TYPE_ERROR	10004	Ошибка определения типа сообщения.
141.	VERIFY_SIGN_DATA_ERROR	10005	Ошибка проверки ЭП подписанного сообщения.
142.	GET_DATA_FROM_EDS_ERROR	10006	Невозможно получить исходные данные подписанного сообщения.
143.	SIGNED_IS_DETACHED	10007	Подпись отделенная.

№	Имя ошибки	Номер ошибки	Текст ошибки
144.	UNKNOWN_HASH_ALGS	10008	Ни один из алгоритмов хеширования, представленных в структуре подписанного файла, не поддерживается в системе.
145.	HASH_ALG_NOT_EXIST_SIGN_CONTENT	10009	Алгоритм хеширования не содержится в списке используемых алгоритмов подписанного сообщения.
146.	OPEN_KEY_FIND_ERROR	10010	Не определен сертификат ключа проверки ЭП.
147.	VERIFY_ADVANCED_DECODE_ATTRIBUTES_ERROR	11000	Ошибка декодирования атрибутов усовершенствованной ЭП.
148.	VERIFY_ADVANCED_ENCODE_ATTRIBUTES_ERROR	11001	Ошибка кодирования атрибутов усовершенствованной ЭП.
149.	VERIFY_ADVANCED_CERT_VALUES_ERROR	11002	Отсутствуют значения сертификатов в атрибуте CertificateValues.
150.	CREATE_STORE_ERROR	11003	Ошибка создания дополнительного хранилища сертификатов.
151.	VERIFY_ADVANCED_SIGNER_CERT_CHAIN_ERROR	11004	Ошибка проверки доказательств усовершенствованной ЭП для сертификата подписчика.
152.	SIGNER_CERT_CHAIN_TSP_TIME_ERROR	11005	Один или несколько сертификатов из цепочки сертификата подписчика являлись недействительными на момент получения внешнего штампа времени.
153.	INCLUDE_CERT_CHAIN_IN_ATTRIBUTES_ERROR	11006	В атрибут подписи включены не все сертификаты из цепочки.
154.	CHECK_SIGNER_CERT_BY_CERT_REFS_V2_ERROR	11007	Целостность подписи нарушена. Возможно произошла подмена сертификата подписчика.
155.	CHECK_CERT_REFS_ERROR	11008	Ссылки на значения сертификатов были собраны не для всех сертификатов из цепочки, либо они недействительны.
156.	FIND_REV_VALUE_ERROR	11009	Значения отзывов были собраны не для всех сертификатов из цепочки, либо они недействительны.
157.	VERIFY_ADVANCED_CERT_IS_REVOKED	11010	Проверяемый сертификат на момент создания усовершенствованной ЭП был отозван.
158.	VERIFY_ADVANCED_CREATE_CRL_ERROR	11011	Не удалось сформировать список отзыва.
159.	VERIFY_ADVANCED_TSP_CERT_CHAIN_ERROR	11012	Ошибка проверки доказательств усовершенствованной ЭП для сертификата TSA-оператора.
160.	TSP_CERT_CHAIN_NOW_TIME_ERROR	11013	Один или несколько сертификатов из цепочки сертификата TSA-оператора являются недействительными на текущий момент времени.
161.	VERIFY_ADVANCED_CHECK_REV_VALUES_ERROR	11014	Ошибка проверки корректности значений отзывов.
162.	GET_OCSP_TIME_THIS_UPDATE_ERROR	11015	Ошибка получения времени формирования OCSP-ответа.

№	Имя ошибки	Номер ошибки	Текст ошибки
163.	CHECK_OCSP_ERROR	11016	Ошибка проверки корректности OCSP-ответа.
164.	OCSP_CERT_NOCHECK_ERROR	11017	В сертификате OCSP отсутствует необходимое расширение szOID_PKIX_OCSP_NOCHECK.
165.	VERIFY_OCSP_SIGNATURE_ERROR	11018	Подпись OCSP-ответа математически некорректна.
166.	VERIFY_ADVANCED_CHECK_REV_REFS_ERROR	11019	Ссылки на значения отзывов были собраны не для всех значений отзывов, либо они недействительны.
167.	VERIFY_ADVANCED_OCSP_CERT_CHAIN_ERROR	11020	Ошибка проверки доказательств усовершенствованной ЭП для сертификата OCSP-оператора.
168.	OCSP_CERT_CHAIN_TSP_TIME_ERROR	11021	Один или несколько сертификатов из цепочки сертификата OCSP-оператора являлись недействительными на момент получения внешнего штампа времени.
169.	VERIFY_ADVANCED_IN_TSP_ERROR	11022	Ошибка проверки внутреннего штампа времени и соответствия хэш-значений.
170.	COMPARE_HASH_IN_TSP_ERROR	11023	Хэш-значение подписи не соответствует хэш-значению во внутреннем штампе времени.
171.	VERIFY_ADVANCED_OUT_TSP_ERROR	11024	Ошибка проверки внешнего штампа времени и соответствия хэш-значений.
172.	COMPARE_HASH_OUT_TSP_ERROR	11025	Хэш-значение доказательств подписи не соответствует хэш-значению во внешнем штампе времени.
173.	FIND_OCSP_CERT_ERROR	11026	Не удалось определить сертификат OCSP-оператора.
174.	SINHRON_OSCP_TSP_TIME_ERROR	11027	Время в OCSP-ответе опережает время во внешнем штампе. Сервера OCSP и TSP были не синхронизированы по времени.
175.	OCSP_CERT_KP_OCSP_SIGNING_ERROR	11028	Сертификат службы OCSP не предназначен для подписи OCSP-ответов.
176.	GET_SING_ATTR_ERROR	11029	Ошибка получения атрибута подписи.
177.	FIND_SIGN_ATTR_ERROR	11030	Атрибут с заданным типом отсутствует в подписи.
178.	ADD_SING_ATTR_ERROR	11031	Ошибка добавления атрибута в подпись.
179.	CERT_STATUS_UNKNOWN	11032	Статус проверяемого сертификата не определен.
180.	GET_SIGN_TSP_INFO_ERROR	11033	Ошибка получения информации о штампах времени внутри подписи.
181.	GET_CERT_PROOF_ERROR	11034	Ошибка получения информации об отзыве сертификата.
182.	GET_CRL_INFO_ERROR	11035	Ошибка получения информации о списке отзыва.
183.	FIND_REV_REF_ERROR	11036	Хэш-значение отзыва не найдено либо оно недействительно.
184.	INIT_ENCRYPT_ERROR	12000	Ошибка инициализации данных для шифрования сообщения.

№	Имя ошибки	Номер ошибки	Текст ошибки
185.	INVALID_ENCRYPT_CERTIFICATE_BLOB	12001	Неверный блок сертификата получателя.
186.	INVALID_ENCRYPT_CERTIFICATE	12002	Сертификат получателя не определен.
187.	FIND_ENCRYPT_OID_ERROR	12003	Не найден подходящий алгоритм шифрования.
188.	FIND_SKEY_ERROR	12004	Не найден ключ ЭП, соответствующий сертификату ключа проверки ЭП.
189.	PIN_CODE_ERROR	12005	Набор ключей не существует. Возможно, вы ввели неверный пин код.
190.	INIT_DECRYPT_ERROR	12006	Ошибка инициализации данных для расшифровывания сообщения.
191.	DECRYPT_ERROR	12007	Ошибка расшифровывания сообщения.
192.	ENCRYPT_ERROR	12008	Ошибка шифрования сообщения.
193.	SECURE_DELETE_ERROR	12009	Ошибка гарантированного удаления данных.
194.	PROV_NAME_ERROR	13000	Криптопровайдер не указан.
195.	GET_PROV_TYPE_ERROR	13001	Не удалось определить тип криптопровайдера.
196.	CREATE_KEY_CONTAINER_ERROR	13002	Ошибка создания контейнера ключей.
197.	CREATE_KEY_PAIR_ERROR	13003	Ошибка генерации пары ключей.
198.	GET_PUBLIC_KEY_STRUCT_LEN_ERROR	13004	Ошибка получения длины структуры под экспортируемый ключ проверки ЭП.
199.	GET_PUBLIC_KEY_ERROR	13005	Ошибка экспортирования ключа проверки ЭП.
200.	ENCODE_SUBJECT_INFO_ERROR	13006	Ошибка кодирования информации о владельце сертификата.
201.	SIGN_ADN_ENCODE_CERT_REQ_ERROR	13007	Возникла ошибка в процессе подписания и кодирования запроса на сертификат.
202.	BASE64_ENCODE_ERROR	13008	Ошибка кодирования информации в base64.
203.	INVALID_USING_CERTIFICATE_BLOB	13009	Неверный блок используемого сертификата.
204.	GET_HPROV_ERROR	13010	Не удалось получить контекст криптопровайдера.
205.	GET_PP_ENUMCONTAINERS_ERROR	13011	Ошибка при получении размера имени контейнера секретного ключа.
206.	GET_PROV_NAME_ERROR	13012	Ошибка при получении имени контейнера секретного ключа.
207.	GET_CONTAINER_NAME_ERROR	13013	Имя контейнера ключа не задано и не определено.
208.	SET_PRIVATE_KEY_FOR_CERT_ERROR	13014	Ошибка создания в сертификате ссылки на ключ ЭП.
209.	ADD_CERT_CONTEXT_TO_STORE_ERROR	13015	Не удалось установить сертификат в хранилище сертификатов.
210.	BASE64_DECODE_ERROR	13016	Ошибка декодирования информации из BASE64.
211.	CREATE_CERT_REQUEST_ERROR	13017	Ошибка создания запроса на сертификат.
212.	SET_PRIVATE_KEY_ERROR	13018	Ошибка установки сертификата и создания связки ключ проверки ЭП – ключ ЭП.
213.	GET_CERT_FROM_STORE_ERROR	13019	Ошибка получения сертификата из хранилища.

№	Имя ошибки	Номер ошибки	Текст ошибки
214.	INIT_GET_CERT_LIST_FROM_STORE_ERROR	13020	Ошибка инициализации данных для получения списка сертификатов из заданного хранилища.
215.	GET_CERT_LIST_FROM_STORE_ERROR	13021	Ошибка получения списка сертификатов из заданного хранилища.
216.	GET_CERT_EXT_INFO_ERROR	13022	Ошибка получения расширенной информации о сертификате.
217.	GET_CERT_CHAIN_ERROR	13023	Не удалось получить цепочку сертификации для выбранного сертификата.
218.	CREATE_CERT_CHAIN_ERROR	13024	Цепочка сертификации составлена некорректно.
219.	INVALID_USING_CRL_BLOB	13025	Неверный блок используемого списка отзыва сертификатов.
220.	ADD_CRL_CONTEXT_TO_STORE_ERROR	13026	Не удалось установить список отзыва сертификатов в хранилище.
221.	CREATE_SELF_SIGNED_CERT_ERROR	13027	Ошибка создания самоподписанного сертификата.
222.	FILL_SELF_CERT_INFO_ERROR	13028	Ошибка формирования структуры информации о самоподписанном сертификате.
223.	SIGN_SELF_CERT_ERROR	13029	Ошибка подписи информации о самоподписанном сертификате.
224.	CREATE_USER_CERT_ERROR	13030	Ошибка выпуска сертификата пользователя.
225.	DET_CP_KEY_CONTAINER_ERROR	13031	Ошибка определения информации для доступа к ключу ЭП.
226.	FILL_USER_CERT_INFO_ERROR	13032	Ошибка формирования структуры информации о пользовательском сертификате.
227.	SIGN_USER_CERT_ERROR	13033	Ошибка подписи информации о пользовательском сертификате.
228.	COMPARE_OPEN_KEYS_ERROR	13034	Соответствие ключа проверки ЭП устанавливаемого сертификата и ключа проверки ЭП в контейнере не установлено.
229.	CERT_REQUEST_DATA_ERROR	13035	Данные запроса на сертификат имеют некорректный формат.
230.	FILL_CERT_REQ_INFO_ERROR	13036	Ошибка формирования структуры информации о запросе на сертификат.
231.	GET_CERT_REQ_SIGN_VALUE_ERROR	13037	Не удалось рассчитать значение ЭП на данные запроса на сертификат.
232.	CERT_REQ_SIGN_VALUE_CORRECT_ERROR	13038	Значение подписи запроса на сертификат математически некорректно.
233.	GET_CERT_EXT_ERROR	13039	Не удалось получить информацию о расширениях сертификата.
234.	ADD_CERT_CONTEXT_TO_DEVICE_ERROR	13100	Не удалось установить сертификат на устройство.
235.	STRUCT_GET_ENCODE_ERROR	14000	Ошибка декодирования структуры данных.
236.	STRUCT_BER_DECODE_ERROR	14001	Ошибка кодирования информации в структуру данных.
237.	SET_OID_ERROR	14002	Ошибка декодирования объектного идентификатора.

№	Имя ошибки	Номер ошибки	Текст ошибки
238.	FILE_NAME_ERROR	14003	Имя файла не задано.
239.	CREATE_DVC_REQUEST_ERROR	15000	Ошибка создания DVCS-запроса.
240.	VERIFY_CERT_BLOB_ERROR	15001	Неверный блок проверяемого сертификата.
241.	DVC_REQUEST_TYPE_ERROR	15002	Тип DVCS-запроса некорректен.
242.	CREATE_DVCS_SIGNATURE_ERROR	15003	Ошибка подписи данных протокола DVCS.
243.	VERIFY_DVC_SIGNATURE_ERROR	15004	Ошибка проверки подписи данных протокола DVCS.
244.	PARSE_DVC_ERROR	15005	Ошибка разбора DVC-квитанции.
245.	CREATE_DVC_RESPONSE_ERROR	15006	Ошибка создания DVC-квитанции.
246.	CHANGE_DVC_SERIAL_ERROR	15007	Ошибка замены значения серийного номера в DVC-квитанции.
247.	GET_CRYPT_ALG_FROM_DVCREQ_ERROR	15008	Ошибка получения криптографических алгоритмов из DVCS-запроса.
248.	PROLONGATION_DVC_ERROR	15009	Не удалось выполнить операцию пролонгации квитанции.
249.	GET_DVCS_TYPE_ERROR	15010	Ошибка определения типа DVCS-запроса.
250.	GET_DVC_REQ_INFO_ERROR	15011	Ошибка получения информации из структуры DVCS-запроса.
251.	GET_SUB_DVC_REQ_ERROR	15012	Ошибка получения "подзапроса" из структуры DVCS-запроса.
252.	DVC_REQ_INDEX_ERROR	15013	Индекс запрашиваемого компонента находится вне границ массива.
253.	GET_SIGNED_ALGS_ERROR	15014	Ошибка получения алгоритмов подписи из подписанного сообщения.
254.	MERGE_DVCS_RESP_ERROR	15015	Ошибка объединения нескольких DVCS-ответов в результирующий DVCS-ответ.
255.	INTEGRITY_DVCS_ERROR	15016	Ошибка проверки соответствия DVCS-ответа DVCS-запросу.
256.	NOT_INTEGRITY_DVCS_ERROR	15017	Ответ не соответствует запросу, произошла подмена ответа.
257.	DELETE_AUTH_INFO_ERROR	15018	Ошибка удаления аутентификационной информации из DVC-запроса.
258.	CHECK_CORRESP_TYPE_RESP_ERROR	15019	Тип квитанции dvErrorNote не может быть сопоставлен с исходными данными.
259.	BH_CERT_TRUST_IS_NOT_TIME_VALID	16000	Сертификат или один из сертификатов в цепочке не действителен на текущий момент времени.
260.	BH_CERT_TRUST_IS_REVOKED	16001	Сертификат или один из сертификатов в цепочке отозван.
261.	BH_CERT_TRUST_IS_NOT_SIGNATURE_VALID	16002	Сертификат или один из сертификатов в цепочке искажен (содержит недействительную цифровую подпись).
262.	BH_CERT_TRUST_IS_NOT_VALID_FOR_USAGE	16003	Сертификат или один из сертификатов в цепочке не предназначен для данного использования.

№	Имя ошибки	Номер ошибки	Текст ошибки
263.	BH_CERT_TRUST_IS_UNTRUSTED_ROOT	16004	Сертификат или один из сертификатов в цепочке издан не доверенным центром сертификации.
264.	BH_CERT_TRUST_IS_CYCLIC	16005	Один из сертификатов в цепочке издан центром, сертифицированным проверяемым сертификатом (циклическая цепочка).
265.	BH_CERT_TRUST_IS_PARTIAL_CHAIN	16006	Построение цепочки сертификации не завершено (неполная цепочка).
266.	BH_CERT_MEDI_CERT_CHECK_REVOKED_ERROR	16007	Ошибка проверки отзыва промежуточного сертификата цепочки.
267.	GET_CSP_NAMES_ERROR	17000	Ошибка получения имен криптопровайдеров в системе.
268.	GET_CSP_PARAMS_ERROR	17001	Ошибка получения параметров криптопровайдера.
269.	GET_CERT_FROM_CONTAINER_ERROR	17002	Ошибка получения сертификата ключа подписи из контейнера.
270.	DELETE_CONTAINER_ERROR	17003	Ошибка удаления контейнера ключей.
271.	ARCHIVAL_TIME_STAMPING_ERROR	18000	Ошибка простановки архивного штампа времени.
272.	VERIFY_SIGNATURE_ERROR	18001	Подпись недействительна.
273.	EDS_NOT_ADVANCED_ERROR	18002	Подпись не является усовершенствованной.
274.	FIND_LAST_TIME_STAMP_ERROR	18003	Заверяющий подпись штамп времени не определен.
275.	UPGRADE_LAST_TIME_STAMP_ERROR	18004	Не удалось собрать доказательства действительности заверяющего штампа времени.
276.	REPLACE_LAST_TIME_STAMP_ERROR	18005	Ошибка замены заверяющего штампа в подписи.
277.	CALC_HASH_FOR_ARCHIVAL_TIME_STAMP_ERROR	18006	Не удалось рассчитать хэш-значение для формирования запроса в TSP-службу.
278.	CREATE_ARCHIVE_TIME_ADD_TO_SIGNATURE	18007	Не удалось сформировать архивный штамп времени и добавить его в обрабатываемую подпись.
279.	EDS_ALREADY_ADVANCED_ERROR	18008	Подпись уже является усовершенствованной.
280.	ATS_VERIFY_SEPARATE_ERROR	18009	Не удалось проверить исходную подпись, либо разделить на подпись и данные.
281.	VERIFY_ARCHIVAL_TIME_STAMPS_ERROR	19000	Ошибка проверки корректности архивных штампов времени.
282.	GET_DATA_FROM_SIGN_FILE_ERROR	19001	Не удалось получить данные из файла-подписи.
283.	VERIFY_ADVANCED_OUT_TSP_CERT_CHAIN_ERROR	19002	Ошибка проверки наличия и корректности доказательств действительности цепочки сертификата TSA-оператора внешнего штампа времени на момент формирования первого архивного штампа.

№	Имя ошибки	Номер ошибки	Текст ошибки
284.	CALC_HASH_FOR_VERIFY_ARCHIVAL_TS_ERROR	19003	Не удалось рассчитать хэш-значение для проверки корректности архивного штампа.
285.	COMPARE_HASH_ARCHIVAL_TIME_SATMP_ERROR	19004	Хэш-значение в архивном штампе времени не соответствует вновь вычисленному.
286.	VERIFY_ADVANCED_ARCHIVAL_TSP_CERT_CHAIN_ERROR	19005	Ошибка проверки наличия и корректности доказательств действительности цепочки сертификата TSA-оператора архивного штампа времени на момент формирования последующего архивного штампа.
287.	LAST_ARCHIVAL_TSP_CERT_CHAIN_ERROR	19006	Цепочка сертификата TSA-оператора последнего архивного штампа времени составлена не корректно.
288.	CHECK_LAST_ARCHIVAL_TSP_SIGNATURE_ERROR	19007	Ошибка проверки корректности последнего архивного штампа.
289.	GET_CERT_REQ_EXT_ERROR	20000	Не удалось получить расширения сертификата из запроса на сертификат.
290.	INCORRECT_EKU_EXT_ERROR	20001	Расширение EnhancedKeyUsage имеет некорректный формат.
291.	INCORRECT_KU_EXT_ERROR	20002	Расширение KeyUsage имеет некорректный формат.
292.	FORMATE_CERT_EXTENSIONS_ERROR	20003	Произошла ошибка в процессе формирования asn.1 структур расширений сертификата.
293.	INCORRECT_EXTENSION_PARAMETER_ERROR	20004	Параметры расширения заданы неверно.
294.	FORMATE_EKU_EXT_ERROR	20005	Ошибка формирования расширения EnhancedKeyUsage.
295.	DECODE_ENHANCE_ERROR	20006	Ошибка кодирования одной из целей использования сертификата.
296.	FORMATE_KU_EXT_ERROR	20007	Ошибка формирования расширения KeyUsage.
297.	FORMATE_AKI_EXT_ERROR	20008	Ошибка формирования расширения AuthorityKeyIdentifier.
298.	FORMATE_SKI_EXT_ERROR	20009	Ошибка формирования расширения SubjectKeyIdentifier.
299.	FORMATE_BASIC_CONSTRAINTS_EXT_ERROR	20010	Ошибка формирования расширения BasicConstraints.
300.	FORMATE_CRL_REVOKED_REASON_EXT_ERROR	20011	Ошибка формирования расширения CRLRevokeReason.
301.	FORMATE_CRL_NUMBER_EXT_ERROR	20012	Ошибка формирования расширения CRLNumber.
302.	FORMATE_CRL_DISTRIBUTION_POINTS_EXT_ERROR	20013	Ошибка формирования расширения CRLDistributionPoints.
303.	INCORRECT_CRL_DP_EXT_ERROR	20014	Расширение CRLDistributionPoints имеет некорректный формат.
304.	FORMATE_AUTHORITY_INFO_ACCESS_EXT_ERROR	20015	Ошибка формирования расширения AuthorityInfoAccessSyntax.
305.	INCORRECT_AUTHORITY_INFO_ACCESS_EXT_ERROR	20016	Расширение AuthorityInfoAccessSyntax имеет некорректный формат.

№	Имя ошибки	Номер ошибки	Текст ошибки
306.	FORMATE_CERT_POLICIES_EXT_ERROR	20017	Ошибка формирования расширения CertificatePolicies.
307.	INCORRECT_CERT_POLICIES_EXT_ERROR	20018	Расширение CertificatePolicies имеет некорректный формат.
308.	FORMATE_SUB_SIGN_TOOL_EXT_ERROR	20019	Ошибка формирования расширения SubjectSignTool.
309.	INCORRECT_SUB_SIGN_TOOL_EXT_ERROR	20020	Расширение SubjectSignTool имеет некорректный формат.
310.	FORMATE_ISSUER_SIGN_TOOL_EXT_ERROR	20021	Ошибка формирования расширения IssuerSignTool.
311.	INCORRECT_ISSUER_SIGN_TOOL_EXT_ERROR	20022	Расширение IssuerSignTool имеет некорректный формат.
312.	FORMATE_SUB_ALT_EXT_ERROR	20023	Ошибка формирования расширения SubjectAltName.
313.	INCORRECT_SUB_ALT_NAME_EXT_ERROR	20024	Расширение SubjectAltName имеет некорректный формат.
314.	CREATE_ATTR_CERT_ERROR	21000	Ошибка выпуска атрибутного сертификата.
315.	FORMATE_ATTRCERT_ATTRS_ERROR	21001	Произошла ошибка в процессе формирования asn.1 структур привилегий атрибутного сертификата.
316.	FORMATE_ROLE_ATTR_ERROR	21002	Ошибка формирования атрибута RoleSyntax.
317.	CREATE_CERT_REVOKE_REQ_ERROR	22000	Ошибка создания запроса на отзыв сертификата.
318.	PARSE_CERT_REVOKE_REQ_ERROR	22001	Ошибка разбора запроса на отзыв сертификата.
319.	CREATE_CERT_REVOKE_RESP_ERROR	22002	Ошибка создания ответа на запрос на отзыв сертификата.
320.	BH_TOKEN_NOT_FOUND	70000	Устройство не найдено. ???
321.	BH_INITIALIZE_ERROR	70001	Ошибка инициализации.
322.	BH_GET_SLOT_LIST_ERROR	70002	Ошибка получения списка слотов.
323.	BH_OPEN_SESSION_ERROR	70003	Ошибка открытия сессии.
324.	BH_LOGIN_ERROR	70004	Ошибка авторизации.
325.	BH_LOGOUT_ERROR	70005	Ошибка вылогирования.
326.	BH_DIGIST_INIT_ERROR	70006	Ошибка инициализации хэширования.
327.	BH_DIGIST_ERROR	70007	Ошибка хэширования.
328.	BH_DIGIST_UPDATE_ERROR	70008	Ошибка хэширования; поток, обновление.
329.	BH_DIGIST_FINAL_ERROR	70009	Ошибка при получении значения хэш-значения.
330.	BH_SIGN_INIT_ERROR	70010	Ошибка инициализации создания подписи.
331.	BH_SIGN_ERROR	70011	Ошибка в процессе создания подписи.
332.	BH_VERIFY_INIT_ERROR	70012	Ошибка инициализации проверки подписи.
333.	BH_VERIFY_ERROR	70013	Ошибка в процессе проверки подписи.
334.	BH_FIND_OBJECTS_INIT_ERROR	70014	Ошибка инициализации поиска объектов.
335.	BH_FIND_OBJECTS_ERROR	70015	Ошибка поиска объектов.
336.	BH_FIND_OBJECTS_FINAL_ERROR	70016	Ошибка при получении результата поиска объектов.

№	Имя ошибки	Номер ошибки	Текст ошибки
337.	BH_GET_OBJECT_ATTRIBUTE_VALUE_ERROR	70017	Ошибка при получении значения атрибута объекта на устройстве.
338.	BH_SET_OBJECT_ATTRIBUTE_VALUE_ERROR	70018	Ошибка при установке значения атрибута объекта на устройстве.
339.	BH_PKCS7_SIGN_ERROR	70019	Ошибка создания CMS сообщения.
340.	BH_PKCS7_VERIFY_ERROR	70020	Ошибка проверки CMS сообщения.
341.	BH_RANDOM_GENERATION_ERROR	70021	Ошибка генерации случайного числа аппаратными средствами устройства.
342.	BH_GENERATE_KEY_PAIR_ERROR	70022	Ошибка при генерации ключевой пары на устройстве.
343.	BH_GENERATE_SESSION_KEY_ERROR	70023	Ошибка при генерации сессионного ключа на устройстве.
344.	BH_DERIVE_KEY_ERROR	70024	Ошибка создания ключа согласования на токене.
345.	BH_WRAP_KEY_ERROR	70025	Ошибка экспорта сессионного ключа на ключе согласования.
346.	BH_UNWRAP_KEY_ERROR	70026	Ошибка импорта сессионного ключа на ключе согласования.
347.	BH_ENCRYPT_INIT_ERROR	70027	Ошибка инициализации зашифровывания данных.
348.	BH_ENCRYPT_ERROR	70028	Ошибка потокового зашифровывания.
349.	BH_ENCRYPT_FINAL_ERROR	70029	Ошибка завершения операции зашифровывания данных.
350.	BH_DECRYPT_INIT_ERROR	70030	Ошибка инициализации расшифровывания данных.
351.	BH_DECRYPT_ERROR	70031	Ошибка потокового расшифровывания.
352.	BH_DECRYPT_FINAL_ERROR	70032	Ошибка завершения операции расшифровывания.
353.	BH_CREATE_OBJECT_ERROR	70033	Ошибка при создании объекта на устройстве.
354.	BH_DESTROY_OBJECT_ERROR	70034	Ошибка удаления объекта с устройства.
355.	BH_CREATE_CSR_ERROR	70035	Ошибка создания запроса на сертификат.
356.	BH_GET_MECHANISM_LIST_ERROR	70036	Ошибка получения списка механизмов.
357.	BH_GET_MECHANISM_INFO_ERROR	70037	Ошибка получения информации о механизме.
358.	COMPARE_DOCUMENT_HASH_ERROR	70038	Ошибка сравнения хэш-значений документов.
359.	VERIFY_EDS_SIGNATURE_ERROR	70039	Ошибка при проверке сигнатуры подписи.
360.	BH_DLL_ALREADY_INITIALIZED	70040	Модуль pkcs11 уже проинициализирован.
361.	BH_DECODE_STRUCT_ERROR	70041	Ошибка декодирования в структуру данных.
362.	BH_ENCODE_STRUCT_ERROR	70042	Ошибка при кодировании структуры данных.
363.	BH_GET_STRING_ERROR	70043	Ошибка при получении строки.
364.	BH_GET_OID_ERROR	70044	Ошибка при получении ОИД-а.
365.	BH_NO_TOKEN_KEYS_ERROR	70045	Отсутствуют ключи на устройстве.
366.	BH_UNKNOWN_STORE_ERROR	70046	Неизвестное имя хранилища.

№	Имя ошибки	Номер ошибки	Текст ошибки
367.	BH_PARAM_ERROR	70047	Функция вызвана с некорректными параметрами.
368.	BH_CANT_FIND_PRIVATE_KEY_ERROR	70048	На устройстве отсутствует необходимый ключ ЭП.
369.	BH_CANT_FIND_PUBLIC_KEY_ERROR	70049	На устройстве отсутствует необходимый ключ проверки ЭП.
370.	BH_GET_SLOT_INFO_ERROR	70050	Ошибка получения информации о слоте.
371.	BH_GET_TOKEN_INFO_ERROR	70051	Ошибка при получении информации об устройстве.
372.	BH_CANT_LOAD_LIBRARY_ERROR	70052	Невозможно загрузить библиотеку pkcs11.
373.	BH_NO_PIN_CODE_PROVIDED	70053	Функции не передан пин-код к устройству.
374.	BH_CKR_HOST_MEMORY	71001	Недостаточно памяти для выполнения функции.
375.	BH_CKR_SLOT_ID_INVALID	71002	Неправильный идентификатор слота.
376.	BH_CKR_GENERAL_ERROR	71003	Критическая ошибка, связанная с аппаратным обеспечением.
377.	BH_CKR_FUNCTION_FAILED	71004	При выполнении функции возник сбой.
378.	BH_CKR_ARGUMENTS_BAD	71005	Недопустимый аргумент.
379.	BH_CKR_ATTRIBUTE_READ_ONLY	71006	Предпринята попытка присвоения значения атрибуту, который нельзя изменять.
380.	BH_CKR_CANT_LOCK	71007	Приложение не поддерживает защиту потоков от одновременного использования различными функциями.
381.	BH_CKR_ATTRIBUTE_SENSITIVE	71008	Запрашиваемый атрибут недоступен для чтения.
382.	BH_CKR_ATTRIBUTE_TYPE_INVALID	71009	Некорректный тип атрибута.
383.	BH_CKR_ATTRIBUTE_VALUE_INVALID	71010	Атрибут нулевой длины.
384.	BH_CKR_DEVICE_ERROR	71011	Ошибка при обращении к устройству или слоту.
385.	BH_CKR_DEVICE_MEMORY	71012	Для выполнения функции недостаточно памяти в устройстве.
386.	BH_CKR_DEVICE_REMOVED	71013	При выполнении функции устройство было отключено.
387.	BH_CKR_ENCRYPTED_DATA_LENGTH_RANGE	71014	Выбранный механизм не поддерживает расшифровывание данных выбранной длины.
388.	BH_CKR_FUNCTION_NOT_SUPPORTED	71015	Выбранная функция не поддерживается модулем сопряжения или не найден дополнительный подключаемый модуль.
389.	BH_CKR_KEY_HANDLE_INVALID	71016	Функции передан некорректный дескриптор ключа.
390.	BH_CKR_KEY_SIZE_RANGE	71017	Недопустимый размер ключа.
391.	BH_CKR_KEY_TYPE_INCONSISTENT	71018	Данный тип ключа не может использоваться с заданным механизмом.

№	Имя ошибки	Номер ошибки	Текст ошибки
392.	BH_CKR_KEY_FUNCTION_NOT_PERMITTED	71019	Ключ, используемый для выполнения криптографических операций, имеет атрибуты, не позволяющие использовать его для данных операций.
393.	BH_CKR_KEY_NOT_WRAPPABLE	71020	Ключ не может быть экспортирован.
394.	BH_CKR_MECHANISM_INVALID	71021	При выполнении криптографической функции был указан неправильный механизм.
395.	BH_CKR_MECHANISM_PARAM_INVALID	71022	При выполнении криптографической функции были заданы некорректные параметры механизма.
396.	BH_CKR_OBJECT_HANDLE_INVALID	71023	Функции передан некорректный дескриптор объекта.
397.	BH_CKR_OPERATION_ACTIVE	71024	Одна или несколько выполняющихся операций препятствуют выполнению новой операции.
398.	BH_CKR_OPERATION_NOT_INITIALIZED	71025	Выполнение операции без предварительного указания параметров невозможно.
399.	BH_CKR_PIN_INCORRECT	71026	Функции передан неверный пин-код.
400.	BH_CKR_PIN_INVALID	71027	Значение пин-кода содержит недопустимые символы.
401.	BH_CKR_PIN_LEN_RANGE	71028	Недопустимая длина пин-кода.
402.	BH_CKR_PIN_LOCKED	71029	Пин-код заблокирован.
403.	BH_CKR_SESSION_CLOSED	71030	При выполнении функции сеанс был закрыт.
404.	BH_CKR_SESSION_COUNT	71031	Достигнуто предельное количество открытых сеансов для данного устройства.
405.	BH_CKR_SESSION_HANDLE_INVALID	71032	Функции передан некорректный дескриптор сеанса.
406.	BH_CKR_SESSION_PARALLEL_NOT_SUPPORTED	71033	Невозможно открыть параллельный сеанс.
407.	BH_CKR_SESSION_EXISTS	71034	Открыт сеанс работы с тем же устройством. Поэтому устройство не может быть инициализировано с помощью функции C_InitToken.
408.	BH_CKR_SESSION_READ_ONLY_EXISTS	71035	Открыт сеанс только для чтения. Смена режима невозможна.
409.	BH_CKR_SESSION_READ_WRITE_SO_EXISTS	71036	Открыт сеанс чтения/записи. Открыть сеанс только для чтения невозможно.
410.	BH_CKR_SIGNATURE_INVALID	71037	Неправильное значение ЭП или имитовставки.
411.	BH_CKR_SIGNATURE_LEN_RANGE	71038	Значение ЭП неверно по крайней мере по длине.
412.	BH_CKR_TEMPLATE_INCOMPLETE	71039	Для создания объекта недостаточно атрибутов.
413.	BH_CKR_TEMPLATE_INCONSISTENT	71040	Заданные в шаблоне значения атрибутов противоречат друг другу.
414.	BH_CKR_TOKEN_NOT_PRESENT	71041	В момент выполнения функции устройство было отключено.
415.	BH_CKR_TOKEN_NOT_RECOGNIZED	71042	Невозможно определить тип устройства, подключенного к слоту.

№	Имя ошибки	Номер ошибки	Текст ошибки
416.	BH_CKR_TOKEN_WRITE_PROTECTED	71043	Устройство недоступно для записи.
417.	BH_CKR_USER_ALREADY_LOGGED_IN	71044	Устройство уже работает в режиме, включение которого требует ввода данного пин-кода.
418.	BH_CKR_USER_NOT_LOGGED_IN	71045	Неверный режим работы устройства.
419.	BH_CKR_USER_PIN_NOT_INITIALIZED	71046	Начальное значение пин-кода не установлено.
420.	BH_CKR_USER_TYPE_INVALID	71047	Задан некорректный режим работы с модулем сопряжения.
421.	BH_CKR_USER_ANOTHER_ALREADY_LOGGED_IN	71048	Переключение из режима администратора в режим пользователя или из режима пользователя в режим администратора невозможно.
422.	BH_CKR_USER_TOO_MANY_TYPES	71049	Включение одновременно режимов пользователя и администратора невозможно.
423.	BH_CKR_BUFFER_TOO_SMALL	71050	Размер заданного буфера является недостаточным для сохранения результатов функции.
424.	BH_CKR_INFORMATION_SENSITIVE	71051	Запрашиваемый объект недоступен для чтения.
425.	BH_CKR_CRYPTOKI_NOT_INITIALIZED	71052	Выполнение функции без инициализации модуля сопряжения невозможно.
426.	BH_CKR_CRYPTOKI_ALREADY_INITIALIZED	71053	Повторная попытка инициализировать модуль сопряжения без предварительного выполнения функции C_Finalize.
427.	BH_CKR_FUNCTION_REJECTED	71054	Запрос ЭП отклонён пользователем.
428.	BH_SOAP_INFO_ERROR	71055	Ошибка в заполнении структуры soap параметров
429.	BH_SOAP_CREATE_ERROR	71056	Ошибка при создании soap конверта

Список сокращений

CDP	–	CRL Distribution Points
CMS	–	Cryptographic Message Syntax
COM	–	Component Object Model
CRL	–	Certificate Revocation List
CSP	–	Cryptographic Service Provider
CVC	–	Citrix Virtual Channel
DVC	–	Data Validation and Certification
DVCS	–	Data Validation and Certification Server
OCSP	–	Online Certificate Status Protocol
OID	–	Object IDentifier
TSA	–	Time Stamping Authority
TSP	–	Time-Stamp Protocol
USB	–	Universal Serial Bus
ОС	–	Операционная Система
ПК	–	Программный Комплекс
ЭП	–	Электронная Подпись