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

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 КС1
1-Base
Руководство администратора
безопасности.
Использование СКЗИ
под управлением ОС Windows

ЖТЯИ.00101-01 91 02
Листов 41

2019 г

Содержание

Аннотация

Настоящее Руководство содержит общее описание средства криптографической защиты информации КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base (ЖТЯИ.00101-01) и рекомендации по использованию СКЗИ в различных автоматизированных системах.

Настоящее Руководство дополняет документ ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть при использовании СКЗИ КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base под управлением операционных систем Windows.

Инструкции администратора безопасности и пользователя различных автоматизированных систем, использующих СКЗИ КриптоПро CSP версии 5.0 КС1, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

1.1 Программно-аппаратные среды функционирования

СКЗИ КриптоПро CSP версии 5.0 КС1 (ЖТЯИ.00101-01) функционирует в следующих группах программно-аппаратных сред:

Windows

Включает программно-аппаратные среды:

Windows 7/8.1/10/Server 2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016/2019 (x64).

Со сроками эксплуатации указанных операционных систем можно ознакомиться по адресу:

https://support.microsoft.com/ru-ru/lifecycle/search

Примечание. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем. Использование СКЗИ под управлением ОС, для которых не выпускаются обновления, не допускается.

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.9.

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

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

2 Установка и удаление дистрибутива ПО СКЗИ

Установка дистрибутива КриптоПро CSP версии 5.0 КС1 должна производиться пользователем, имеющим права администратора.

Для установки СКЗИ КриптоПро CSP версии 5.0 КС1 сначала необходимо установить провайдер, а затем устанавливать остальные модули, входящие в состав комплектации.

Для начала установки программного обеспечения вставьте компакт-диск в дисковод. В стартовом окне выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе (см. рис. 1).

Рисунок 1. Установка СКЗИ КриптоПро CSP

Примечание. Также установка может производиться с дистрибутива, полученного с сайта ООО «КРИПТО-ПРО». В таком случае пользователю нужно запустить файл дистрибутива CSPSetup.exe.

Откроется приветственное окно мастера установки КриптоПро CSP. Для изменения уровня КС (КС1/КС2/КС3) или языка установки нажмите кнопку **Дополнительные опции**. В открывшемся окне укажите язык установки и требуемый уровень безопасности и нажмите кнопку **Установить** (см. рис. 2).

Примечание. По умолчанию в окне установлен флаг **Установить корневые сертификаты**. При установке СКЗИ в хранилище «Доверенные корневые центры сертификации» локального компьютера устанавливаются следующие корневые сертификаты (перечислены значения соответствующих имен субъекта (CN)): CryptoPro GOST Root CA, Минкомсвязь России и Головной удостоверяющий центр.

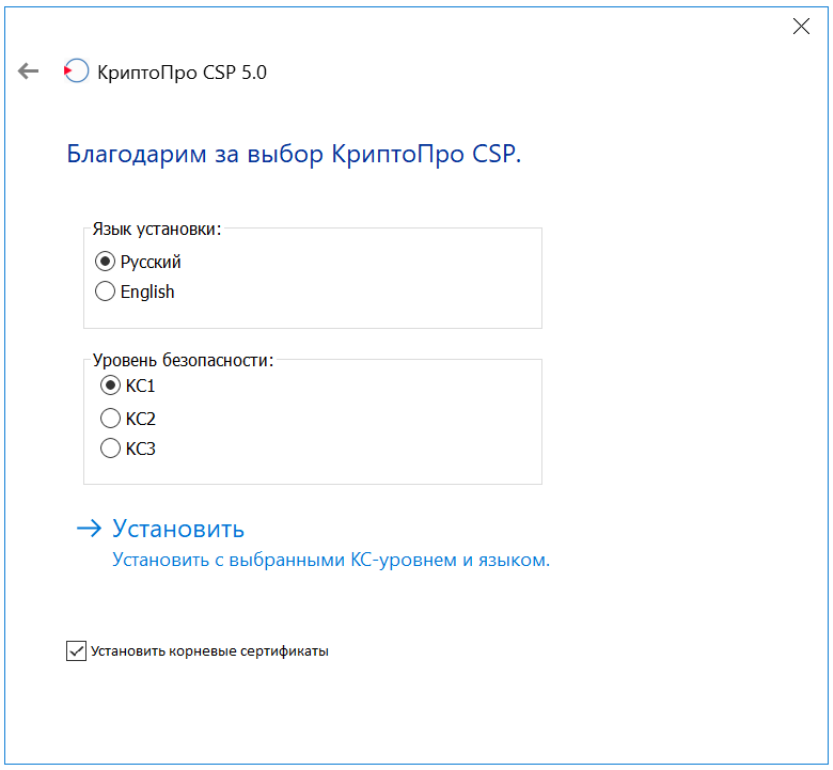

Рисунок 2. Установка СКЗИ КриптоПро CSP

Для дальнейшей установки КриптоПро CSP версии 5.0 КС1 в окне мастера установки нажмите кнопку **Далее** (см. рис. 3).

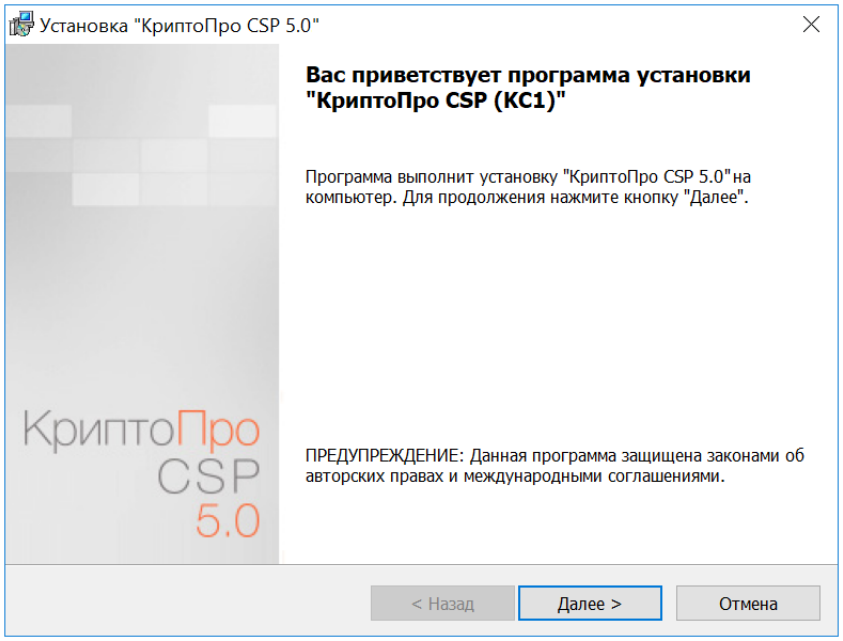

Рисунок 3. Мастер установки КриптоПро CSP версии 5.0 КС1

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование

службы хранения ключей. Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

2.1 Параметры установки КриптоПро CSP версии 5.0 KC1

При установке КриптоПро CSP версии 5.0 KC1 можно использовать различные параметры командной строки, влияющие на устанавливаемые компоненты, начальную настройку продукта и другое.

Для установки КриптоПро CSP введите следующую команду в командной строке и укажите необходимые параметры:

```
msiexec /i <полный или относительный путь к .msi-файлу> <параметры>
```

Следующие опции позволяют не устанавливать соответствующие библиотеки поддержки считывателей и носителей (значение «1» означает не устанавливать):

NOACCORD=1	Аккорд
NOBIO=1	Биологический ДСЧ
NODALLAS=1	Носители Dallas
NODS=1	Считыватели Dallas
NODSRF=1	ДСЧ «Последовательность поставщика»
NOEMV=1	Карта EMV
NOETOKEN=1	Носители eToken
NOFLOPPY=1	Считыватель дискет
NOJCARD=1	Карты JCard
NOPCSC=1	PC/SC
NOREGISTRY=1	Считыватель «Реестр»
NORIC=1	Карты RIC/OSCAR
NORUTOKEN=1	Носитель Rutoken
NOSABLE=1	Соболь
NOSNET=1	SecretNet
NOCHARISMATHICS=1	Charismathics
NOINPAS=1	Global Platform Optelio
NOCPFKC=1	Поддержка унифицированных носителей КриптоПро ФКН 2.0

Следующие опции позволяют управлять регистрацией поддерживаемого оборудования во время

установки КриптоПро CSP версии 5.0 КС1 (значение «0» означает «отключить опцию»; * отмечены опции, включенные по умолчанию):

REGACCORDRDR=1	Зарегистрировать считыватель "Аккорд" во время установки
REGACCORDRND=1	Зарегистрировать ДСЧ "Аккорд" во время установки
REGBIO=1	Зарегистрировать биологический ДСЧ *
REGCHARISMATHICS=1	Зарегистрировать все носители "Charismathics" во время установки
REGESMARTTOKEN=1	Зарегистрировать носители "ESMARTToken" во время установки
REGEMUL=1	Зарегистрировать эмулятор носителя во время установки
REGETOKEN=1	Зарегистрировать все носители "Aladdin eToken", отдельные типы: REGETOKENJAVA10, REGETOKENJAVA10B, REGETOKENM420, REGETOKENM420B, REGETOKEN16, REGETOKEN32
REGGTOKEN=1	Зарегистрировать все носители "eToken GOST"
REGFLOPPY=буквы	Зарегистрировать считыватель "Дискета" (FAT12/FLOPPY) для букв, указанных через запятую
REGPNPFLOPPY=1	Зарегистрировать считыватель "Все съемные носители" *
REGHDIMAGE=1	Зарегистрировать считыватель "Директория"
REGDSRF=путь	Зарегистрировать ДСЧ "Последовательность поставщика" и задать путь (без "\" на конце) к папке с db1, db2
REGDS1410E=порты	Зарегистрировать считыватель "DS1410E" (порты - список портов через запятую: LPT1,LPT2,...)
REGDS9097E=порты	Зарегистрировать считыватель "DS9097E" (порты - список портов через запятую: COM1,COM2,...)
REGDS9097U=порты	Зарегистрировать считыватель "DS9097U" (порты - список портов через запятую: COM1,COM2,...)
REGDS199X=1	Зарегистрировать носитель "DS199x"
REGEMV=1	Зарегистрировать носитель "MPCOS EMV"
REGGEMALTO=1	Зарегистрировать носитель "GEMALTO"
REGINPAS=1	Зарегистрировать носители "ИНПАС"
REGOSCAR=1	Зарегистрировать носитель "Оскар"
REGOSCAR2=1	Зарегистрировать носитель "Оскар2" *
REGTRUST=1	Зарегистрировать носитель "Магистра" *

REGTRUSTS=1	Зарегистрировать носитель "Магистра Сбербанк/BGS" *
REGTRUSTD=1	Зарегистрировать носитель "Магистра Debug" *
REGPNPPCSC=1	Зарегистрировать считыватель "Все считыватели смарт-карт" *
REGREGISTRY=1	Зарегистрировать считыватель "Реестр"
REGRIC=1	Зарегистрировать носитель "РИК"
REGRUTOKEN=1	Зарегистрировать носитель "Rutoken" *
REGSABLERDR=1	Зарегистрировать считыватель "Соболь"
REGSABLERND=1	Зарегистрировать ДСЧ "Соболь"
NOWL=1	Не регистрировать носители для Winlogon
NOESMARTTOKENWL=1	Не регистрировать носители "ESMARTTOKEN" для Winlogon
NOETOKENWL=1	Не регистрировать носители "Aladdin eToken" для Winlogon
NOGEMALTOWL=1	Не регистрировать носители "GEMALTO" для Winlogon
NOOSCAR2WL=1	Не регистрировать носитель "Оскар2" для Winlogon
NOTRUSTWL=1	Не регистрировать носитель "Магистра" для Winlogon
NOTRUSTSWL=1	Не регистрировать носитель "Магистра Сбербанк/BGS" для Winlogon
NOTRUSTDWL=1	Не регистрировать носитель "Магистра Debug" для Winlogon
NORUTOKENWL=1	Не регистрировать носитель "Rutoken" для Winlogon *
NOUECWL=1	Не регистрировать носители "УЭК" для Winlogon
NOCHARISMATHICSWL=1	Не регистрировать носители "Charismathics" для Winlogon
NOINPASWL=1	Не регистрировать носители "ИНПАС" для Winlogon

Следующие опции предназначены для управления режимами работы КриптоПро CSP:

TIMEWARNING2001=4294967295	Отключить предупреждения использования ГОСТ 34.10-2001
NODIAGTRACKDISABLE=1	Не отключать функции телеметрии Windows
NOINTERACTIVESERVICES=1	Позволяет не разрешать интерактивные сервисы Windows, отключенные по умолчанию на Windows 8
CPCSPR=1	Позволяет выбрать режим службы хранения ключей (только при установке)

CACHED=N	Настройка кэширования ключей. Если N=0, то выключено, если N>0, то задает размер кэша (только при установке)
CSPDELETEKEYS=1	При удалении продукта удалит так же все настройки и все ключи из реестра
INSTALLCPCERT=1	Установить сертификат подписи кода КРИПТО-ПРО в хранилище "Доверенные издатели" (позволяет избежать запрос на установку драйвера на Windows 7+)
CERTSTOREPARAMSSUPPORTED=1	Включить поддержку параметров PP_USER_CERTSTORE/ PP_ROOT_CERTSTORE
FULLCNGREGISTER=1	Зарегистрировать Key Storage Provider (CNG)
CNGOIDCONTROL=1	Зарегистрировать CNG Algid в таблице OID
LICERRORLEVEL=[1][2][4]	Битовая маска отключения отображения ошибок лицензии: 001 IDS_CSP_CORRUPTED 010 IDS_CSP_EXPIRED, IDS_WRONG_LICENSE_TYPE, IDS_CSP_EXPIRED_CERT_BAD 100 IDS_CSP_EXPIRE_IN ...
ENABLEDEFAULTREADER=1	Разрешить изменять считыватель по умолчанию в панели CSP
ENABLEDTBSDISPLAY=1	Использовать устройства визуализации подписи
ENABLEOIDMODIFY=1	Разрешить изменять настройки алгоритмов в панели CSP
DISABLEEXTENDEDMASTERSECRET=0	Не отключать TLS Extended Master Secret
DEFAULTCLOUDAUTHSERVER	Задаёт адрес по умолчанию сервера аутентификации DSS
DEFAULTCLOUDRESTSERVER	Задаёт адрес по умолчанию REST-сервера DSS

Следующие опции позволяют указать устанавливаемые компоненты СКЗИ:

FOREIGN=1	Установить компоненту "Поддержка RSA/ECDSA"
REPROV=1	Установить компоненту "Revocation Provider"
DRIVER=1	Установить компоненту "Драйверная библиотека CSP"
COMPAT=1	Установить компоненту "Совместимость с КриптоПро CSP 3.0"
NODRIVER=1	Не устанавливать компоненту "Драйверная библиотека CSP" (ставится по умолчанию на Windows Server 2008)
NOCPROCTRL=1	Не устанавливать компоненту "Совместимость с продуктами Microsoft" (ставится по умолчанию)
NOCCID=1	Не устанавливать драйвер CCID (Chip/Smart Card Interface Devices)

Следующие опции предназначены для указания серийных номеров лицензий продуктов:

COMPANYNAME=	Указать название организации, использующей лицензию
USERNAME=	Указать имя пользователя, использующего лицензию
PIDKEY=	Использовать указанный серийный номер CSP
WLPIDKEY=	Использовать указанный серийный номер Winlogon
RPPIDKEY=	Использовать указанный серийный номер Revocation Provider
OCSPAPIPIDKEY=	Использовать указанный серийный номер OCSP Client
TSPAPIPIDKEY=	Использовать указанный серийный номер TSP Client

Доступны следующие стандартные параметры Windows Installer (подробнее см. документацию Microsoft):

PATCH=патчи	Установить продукт вместе с патчами (список полный путей к .msp-файлам через точку с запятой)
INSTALLDIR=...	Путь установки
INSTALLDIR64=...	Путь установки для 64-компонент
REBOOT=R	Не перезагружать компьютер после установки
REMOVE=модули	Для уже установленного продукта удаляет указанные модули (cproctrl, reprov, driver, compat)
ADDLOCAL=модули	Для уже установленного продукта устанавливает указанные модули (cproctrl, reprov, driver, compat, foreign)

Дополнительные параметры установки:

/qb	установка без мастера
/qn	установка без окон
/L*v файл	создание журнала установки

Пример:

```
msiexec /i "d:\КриптоПро CSP 5.0\csp-win32-kc1-rus.msi" INSTALLDIR="d:\csp" /L*v "c:\temp\csp.log" /qb
```

В указанном примере запускается .msi-файл, расположенный по адресу d:\КриптоПро CSP 5.0\csp-win32-kc1-rus.msi, установка программного обеспечения будет производиться в директорию d:\csp, журнал установки будет находиться по адресу c:\temp\csp.log, установка будет выполняться без мастера.

2.2 Удаление ПО СКЗИ

Рекомендуется сначала удалить установленные продукты через «Установку и удаление программ» Панели управления, перезагрузить компьютер, и затем запустить cspclean.exe. Утилита предназначена для очистки компьютера от не удалённых элементов продуктов «КРИПТО-ПРО». После завершения работы утилиты обязательно перезагрузите компьютер.

Для удаления КриптоПро CSP через командную строку введите следующую команду:

```
msiexec /x {50F91F80-D397-437C-B0C8-62128DE3B55E}
```

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Windows необходимо:

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

2) удалить штатными средствами ОС дистрибутив КриптоПро CSP;

3) установить аналогичный новый дистрибутив КриптоПро CSP;

4) при необходимости внести изменения в настройки.

Примечание. Ключи и сертификаты сохраняются автоматически.

4 Настройка СКЗИ

4.1 Включение режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. Данный режим должен быть включён при инсталляции СКЗИ, либо через контрольную панель КриптоПро CSP, вкладка «Безопасность» (см. рис. 4).

Примечание. Отключение режима усиленного контроля использования ключей допускается исключительно в тестовых целях.

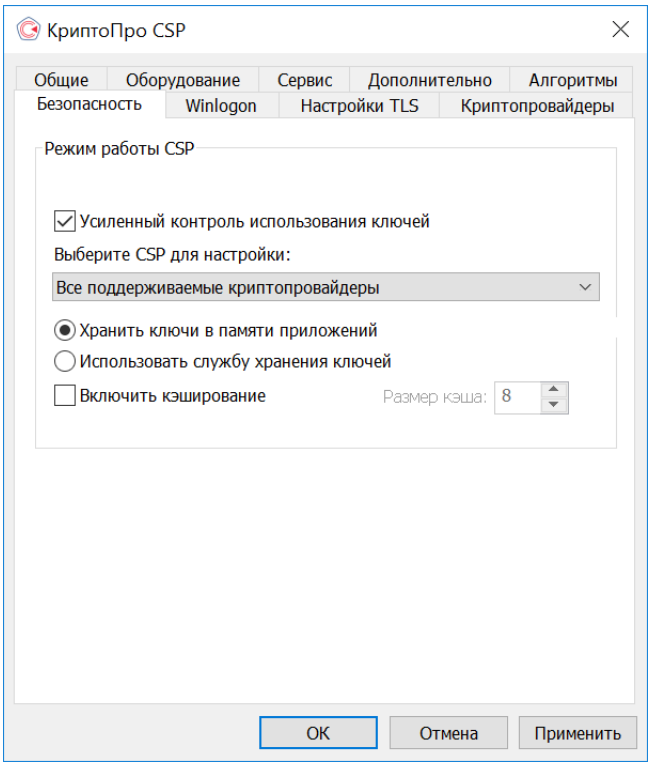

Рисунок 4. Включение режима усиленного контроля использования ключей в контрольной панели КриптоПро CSP версии 5.0 КС1

Проверить, включён ли режим усиленного контроля использования ключей, можно в контрольной панели КриптоПро CSP (вкладка «Безопасность»), либо просмотрев значение ключа `StrengthenedKeyUsageControl` в ветке реестра: для 64-разрядной операционной системы `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CryptoPro\Cryptography\CurrentVersion\Parameters\StrengthenedKeyUsageControl` , для 32-разрядной операционной системы `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\Parameters\StrengthenedKeyUsageControl`.

В случае, если включение режима усиленного контроля использования ключей производилось не на этапе инсталляции СКЗИ (через контрольную панель или редактор реестра ОС Windows) или в ходе инсталляции СКЗИ не удалось получить случайные данные с датчика случайных чисел (в этом случае инсталлятор отображает окно об ошибке, см. рис. 5), необходимо выполнить команду:

```
csptest.exe -keyset -verifycontext -hard_rng
```

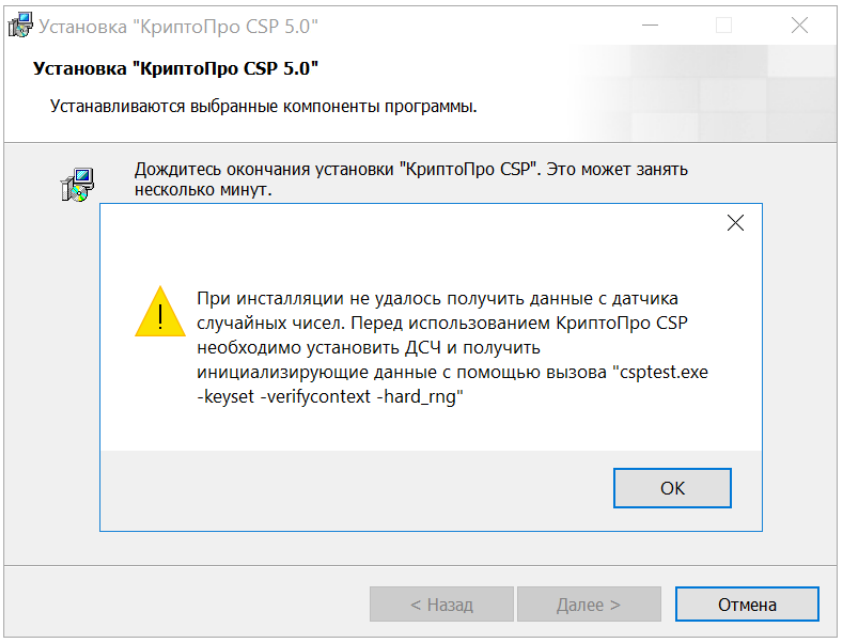

Рисунок 5. Ошибка получения данных с датчика случайных чисел при инсталляции СКЗИ

Если режим усиленного контроля использования ключей включался не при инсталляции СКЗИ, после включения режима необходимо произвести перезагрузку компьютера.

В криптопровайдере КриптоПро CSP версии 5.0 КС1 для ключей ГОСТ Р 34.10-2001/2012 реализован дополнительный контроль доверенности сертификата ключа проверки электронной подписи, для чего совершается построение цепочек сертификатов до доверенных ключевых сертификатов, находящихся в хранилище локального компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots»). Данное хранилище сертификатов автоматически создаётся при инсталляции КриптоПро CSP версии 5.0 КС1. После успешного завершения инсталляции необходимо в обязательном порядке произвести установку доверенных корневых сертификатов в хранилище CryptoProTrustedStore с помощью оснастки Сертификаты либо же с помощью утилиты `certmgr`:

```
certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer
```

Примечание. Работа СКЗИ без установки доверенных корневых сертификатов в хранилище CryptoProTrustedStore допускается исключительно в тестовых целях.

После проведения установки доверенных корневых сертификатов в хранилище CryptoProTrustedStore следует перезагрузить компьютер.

Сертификаты открытых ключей ГОСТ Р 34.10-2001/2012, для которых нельзя построить цепочку к корневым сертификатам в хранилище CryptoProTrustedStore, являются недоверенными. Для их удаления можно воспользоваться утилитами `certmgr` либо `cryptcp`:

```
certmgr.exe -delete -cert -store uMy -dn CN=test-user
```

```
cryptcp.exe -delcert -dn CN=test-user -uMy
```

4.2 Отключение функций телеметрии на ОС Windows 10/Server 2016

Примечание. Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/Server 2016.

Для отключения функций телеметрии на ОС Windows 10/Server 2016 необходимо выполнить следующие действия:

1) Проверить наличие и статус сервиса DiagTrack (Панель управления → Система и безопасность → Администрирование → Службы).

2) Если сервис запущен, то остановить его.

3) Удалить запись регистрации сервиса DiagTrack из реестра (Пуск → Выполнить → `regedit`, раздел `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`. Здесь необходимо найти и удалить папку DiagTrack).

4) Удалить подготовленные к отправке данные, которые сохраняются в четырех файлах с расширением *.rbs, хранящихся в директории `%ProgramData%\Microsoft\Diagnosis`. Имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs. Для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить.

5) Остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессе своей остановки.

6) Удалить файл, в который автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные. Путь к файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в значении FileName. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра `HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger`. Конфигурация целевой сессии хранится в данном ключе под записью AutoLogger-DiagTrack-Listener. В настоящее время данные сохраняются в файл `%ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl`.

7) Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра.

Данные действия необходимо выполнять после каждого кумулятивного обновления, поскольку данные обновления являются по сути полной переустановкой ОС и удаленные сервисы восстанавливаются.

5 Использование СКЗИ на платформе Microsoft .NET Framework

Компанией ООО «КРИПТО-ПРО» разработан программный продукт «КриптоПро .NET», позволяющий использовать средство криптографической защиты информации КриптоПро CSP версии 5.0 КС1 на платформе Microsoft .NET Framework. КриптоПро .NET реализует набор интерфейсов для доступа к криптографическим операциям .NET Cryptographic Provider:

- хэширование;
- подпись;
- шифрование;
- MAC;
- генерация ключей и т.д.

Кроме того, КриптоПро .NET позволяет использовать стандартные классы Microsoft для высокоуровневых операций:

- разбор сертификата;
- построение и проверка цепочки сертификатов;
- обработка CMS сообщений;
- установление защищенного обмена через SSL/TLS, HTTPS и FTPS;
- XML подпись и шифрование.

Подробную информацию, дистрибутивы, документацию и сценарии использования можно найти на сайте продукта. При использовании должны выполняться требования п. 1.5 ЖТЯИ.00101-01 30 01. Формуляр.

6 Состав и назначение компонент ПО СКЗИ

Программное обеспечение СКЗИ КриптоПро CSP версии 5.0 КС1 при функционировании под управлением ОС Windows состоит из следующих компонент:

1) Сервисные модули;
2) Модули настройки встроенной подсистемы программной среды функционирования (СФ) ОС Windows;
3) СКЗИ КриптоПро CSP версии 5.0 КС1, реализующее целевые функции криптопровайдера в форме:
   - библиотек, загружаемых в адресное пространство приложения;
   - криптографического сервиса хранения ключей;
   - криптографического драйвера;
   - библиотек протокола «КриптоПро TLS».
4) Модуль поддержки сетевой аутентификации КриптоПро TLS.

6.1 Сервисные модули

Сервисные модули обеспечивают контроль целостности дистрибутива КриптоПро CSP версии 5.0 КС1, его установку и удаление из операционной системы, а также конфигурацию параметров СКЗИ для каждого пользователя.

6.1.1 Модуль контроля целостности дистрибутива

Модуль `cpverify.exe` (см. Приложение А документа ЖТЯИ.00101-01 95 01. Правила пользования), предназначен для контроля целостности дистрибутива при установке и использовании ПО СКЗИ КриптоПро CSP версии 5.0 КС1 на компьютере пользователя (поставляется совместно с дистрибутивом).

6.1.2 Дистрибутив

Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 поставляется в виде пакета «Windows Installer» (файл csp-win32-kc1-rus.msi или подобное название. В названии файла установщика присутствует обозначение платформы, для которой он предназначен, класс защиты и язык установки). При запуске файл установщика разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ КриптоПро CSP версии 5.0 КС1.

6.1.3 Модуль конфигурации

Модуль `cpconfig.cpl` обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ КриптоПро CSP версии 5.0 КС1, а также содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации.

6.1.4 Модуль Wipefile

Модуль `wipefile` используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях.

6.1.5 Модуль контроля целостности в драйвере

Для работы с любым отладчиком модуль контроля целостности в драйвере должен быть отключен. Порядок отключения данного модуля описан в руководстве программиста (CSP_5_0.chm, раздел Архитектура и встраивание СКЗИ).

Примечание. Отключение модуля контроля целостности в драйвере допускается только в тестовом режиме.

6.2 Модули настройки подсистемы программной СФ ОС Windows

Модули предназначены для обеспечения использования ПО СКЗИ КриптоПро CSP версии 5.0 КС1 в подсистеме программной СФ ОС Windows. Модули также реализуют форматы криптографических сообщений, используемых в защищенной электронной почте (S/MIME), Microsoft Office, Authenticode и функциях CryptoAPI 2.0, форматы сертификатов и их обработку.

Примечание. Полный перечень поддерживаемых приложений Microsoft приведен в документе ЖТЯИ.00101-01 90 01. Описание реализации.

Модули настройки классифицируются как подсистема программной СФ и ответственны за использование криптопровайдера КриптоПро CSP версии 5.0 КС1 со стороны приложений. Они обеспечивают вызов сервиса криптографических функций, но не обрабатывают ключевую и криптографически опасную информацию (не имеют доступа к ключам и т. п.).

6.2.1 Модуль расширения и настройки CryptoAPI 2.0

Модуль `cpext.dll` является зарегистрированной в системном реестре Windows динамической библиотекой (DLL) расширения CryptoAPI 2.0 и обеспечивает:

- установку соответствия между идентификаторами объектов (OID) в криптографических сообщениях и сертификатах открытых ключей и функциями КриптоПро CSP версии 5.0 КС1;
- формирование и разбор криптографических сообщений и сертификатов открытых ключей.

6.2.2 Модули инициализации настройки встроенной подсистемы программной СФ ОС Windows

Модуль инициализации для ОС Windows реализован в виде драйвера CProCtrl.sys. Драйвер обеспечивает загрузку определенных динамических библиотек (DLL) в адресное пространство процессов, использующих СКЗИ КриптоПро CSP версии 5.0 КС1.

Дополнительно этот модуль осуществляет контроль целостности установленного ПО КриптоПро CSP версии 5.0 КС1 и подсистемы программной СФ (периодический и при загрузке ОС).

6.2.3 Модуль настройки для системного DLL crypt32.dll

Модуль `cpcrypt.dll` загружается в виртуальное адресное пространство каждого процесса, к которому подгружается `crypt32.dll`, для установления перехватов функций, использующих провайдер КриптоПро CSP версии 5.0 КС1.

Настройка заключается в добавлении программной СФ возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером КриптоПро CSP версии 5.0 КС1.

6.2.4 Модуль настройки для системного DLL inetcomm.dll

Модуль `cpintco.dll` загружается в виртуальное адресное пространство каждого процесса, использующего `inetcomm.dll`, для установления перехватов функций.

Настройка заключается в поддержке дополнительных идентификаторов алгоритмов и возможностей S/MIME, реализуемых криптопровайдером КриптоПро CSP версии 5.0 КС1, при использовании в ПО Microsoft Outlook и Microsoft Outlook Express.

6.2.5 Модуль настройки для системного DLL certocm.dll

Модуль `cpcertocm.dll` загружается в виртуальное адресное пространство процесса установки центра сертификации (CA) ОС Windows.

Модуль позволяет настроить центр сертификации при его установке так, чтобы поддерживались алгоритмы КриптоПро CSP версии 5.0 КС1.

6.2.6 Модуль настройки для системного DLL wininet.dll

Модуль `cpwinet.dll` загружается в виртуальное адресное пространство процесса Internet Explorer/Microsoft Edge, если в него отображается `wininet.dll`.

Модуль позволяет правильно отображать алгоритмы КриптоПро TLS в Internet Explorer/Microsoft Edge.

6.2.7 Модуль настройки для системного DLL advapi32.dll

Модуль `cpadvai.dll` загружается в виртуальное адресное пространство каждого процесса, использующего `advapi32.dll`, для установления перехватов функций.

Настройка заключается в добавлении возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером КриптоПро CSP версии 5.0 КС1.

6.2.8 Модуль настройки для системного DLL kerberos.dll

Модуль `cpkrb.dll` загружается в виртуальное адресное пространство процессов, использующих модуль `kerberos.dll`, и обеспечивает эмуляцию поддержки криптопровайдером стандарта Triple DES.

6.2.9 Модуль настройки TLS

Модуль `cpschan.dll` загружается в виртуальное адресное пространство процесса Internet Explorer/Microsoft Edge, если он использует TLS.

Модуль позволят использовать алгоритмы «КриптоПро TLS» в Internet Explorer/Microsoft Edge.

6.2.10 Модули настройки MS Office

Модуль `cpMSO.dll` загружается в виртуальное адресное пространство процессов MS Word и MS Excell и позволяет подписывать документы с помощью алгоритмов КриптоПро CSP версии 5.0 КС1.

Модуль `cpExSec.dll` загружается в виртуальное адресное пространство процесса MS Outlook, и настраивает его для правильной работы с КриптоПро CSP версии 5.0 КС1.

6.2.11 Модуль настройки XML

Модуль `cpXML.dll` загружается в виртуальное адресное пространство процессов, использующих XML, и позволяет применять алгоритмы КриптоПро CSP версии 5.0 КС1 для подписи XML.

6.2.12 Модуль настройки контроллера домена

Модуль `cpkdc.dll` загружается в виртуальное адресное пространство процессов доменной аутентификации на контроллере домена и обеспечивает возможность использования для проверки подписи

алгоритмов, реализуемых КриптоПро CSP версии 5.0 КС1.

6.3 СКЗИ КриптоПро CSP версии 5.0 КС1

6.3.1 Интерфейсная библиотека криптопровайдера

Интерфейсная библиотека `cpcsp.dll` реализует стандартный интерфейс криптопровайдера, соответствующий спецификации Microsoft Cryptographic Service Provider, и обеспечивает данный интерфейс для обычных приложений через криптографический сервис по RPC, или для привилегированных приложений (имеющих право доступа к устройствам носителей ключевого контейнера) - непосредственно.

6.3.2 Интерфейсная библиотека криптографического сервиса

Интерфейсная библиотека `cpcspr.dll` обеспечивает возможность обращения обычных приложений к сервису криптографических функций по протоколу RPC.

6.3.3 Реализация криптопровайдера в форме сервиса хранения ключей

Модуль `cpcspi.dll` реализует целевые функции криптографической защиты информации при обращении по RPC с локального компьютера для интерфейсной библиотеки криптографического сервиса.

Модуль обеспечивает:
- хранение и работу с контекстом уровня библиотеки;
- хранение криптографических объектов:
  - ключевых пар (постоянных и временных);
  - открытых ключей (временных);
  - ключей сессий (временных симметричных);
  - объектов функции хэширования.
- выполнение криптографических преобразований.

6.3.4 Реализация криптопровайдера в форме подгружаемых библиотек

Интерфейс `cpcspi.dll` реализует целевые функции криптографической защиты информации для Интерфейсной библиотеки криптопровайдера (см. разд. 6.3.1) в варианте функционирования ПО КриптоПро CSP версии 5.0 КС1 без использования Интерфейса криптографического сервиса (см. разд. 6.3.2).

6.3.5 Реализация криптопровайдера в форме драйвера ядра ОС

Интерфейс `cpdrvlib.sys` реализует подмножество целевых функций криптографической защиты информации для Интерфейсной библиотеки криптопровайдера в варианте функционирования ПО КриптоПро CSP версии 5.0 КС1 в ядре ОС Windows. Драйвер поддерживает выполнение функций шифрования, имитозащиты, хэширования, проверки подписи и выработку ключей согласования на эфемерных ключах. Драйвер не поддерживает работу с пользовательскими ключами.

6.3.6 Интерфейс доступа к физическому ДСЧ и БиоДСЧ

Библиотека `cprndm.dll` обеспечивает унифицированный интерфейс доступа к физическому ДСЧ или БиоДСЧ.

6.3.7 Интерфейсные модули ДСЧ

Обеспечивают реализацию доступа к следующим типам ДСЧ:

`bio.dll`	БиоДСЧ
`sable.dll`	ДСЧ электронного замка "Соболь"
`accord.dll`	ДСЧ АМДЗ "Аккорд"
`crypton.dll`	ДСЧ АПМДЗ "КРИПТОН-ЗАМОК"
`maxim.dll`	ДСЧ АПМДЗ "МАКСИМ-М1"

6.3.8 Панель управления ресурсами СКЗИ КриптоПро CSP версии 5.0 КС1

Управление ресурсами СКЗИ КриптоПро CSP версии 5.0 КС1 осуществляется командным файлом `cpconfig.cpl` через панель управления «Свойства — КриптоПро CSP». К основным средствам управления ресурсами СКЗИ относятся средства управления:

- лицензиями;
- ДСЧ;
- библиотеками считывания ключевой информации;
- закрытыми ключами (ключами ЭП) и сертификатами открытых ключей (ключей проверки ЭП);
- параметрами СКЗИ.

Определение правил пользования данными средствами приводится в документе ЖТЯИ.00101-01 92 01. Инструкция по использованию. Windows.

6.3.9 Интерфейс доступа к ключевым носителям

Библиотека `cprdr.dll` обеспечивает унифицированный интерфейс доступа к ключевым носителям вне зависимости от их типа.

6.3.10 Интерфейсные модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:

accord.dll	считыватель АМДЗ "Аккорд"
cloud.dll	облачный токен
crypton.dll	считыватель АПМДЗ "КРИПТОН-ЗАМОК"
dallas.dll	считыватель Touch-memory Dallas
ds199x.dll	таблетки DS1996, DS1995
emv.dll	смарт-карта MPCOS EMV/3DES
esmarttoken.dll	ESMART Token
esmarttokengost.dll	ESMART Token ГОСТ
fat12.dll	дисковод и дискета 3.5"
infocrypt.dll	токены InfoCrypt

inpaspot.dll	смарт-карта Alioth INPASPOT
jacarta.dll	токены JaCarta
kst.dll	смарт-карты MorphoKST
mskey.dll	смарт-карты Multisoft MS_Key
novacard.dll	смарт-карты Novacard
pcsc.dll	считыватели смарт-карт и eToken, поддерживающие интерфейс PC/SC
reg.dl	системный реестр
ric.dll	смарт-карты РИК и Оскар
rosan.dll	смарт-карта Rosan
rutoken.dll	смарт-карты и токены Рутокен
sable.dll	считыватель электронного замка "Соболь"
safenet.dll	смарт-карты и токены Gemalto и SafeNet

6.3.11 Библиотека поддержки доступа к ключевым носителям

Библиотека `cpsuprt.dll` обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

6.3.12 Модуль ASN1

Поддерживает функции преобразования структур данных в машинно-независимое представление.

6.3.13 Использование ключей реестра Windows

Установка программного обеспечения должна производиться пользователем с правами администратора. При этом программа установки требует доступ к следующим ключам реестра:

- `HKEY_LOCAL_MACHINE` — полный доступ;
- `HKEY_CLASSES_ROOT` — полный доступ.

При использовании СКЗИ КриптоПро CSP версии 5.0 КС1 и создании ключей пользователей без использования флага `CRYPT_LOCALMACHINE` требуется доступ к следующим ключам реестра:

- `HKEY_LOCAL_MACHINE` — чтение, перечисление;
- `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Settings\USERS` — создание подключей, чтение, перечисление;
- `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Settings\USERS\SID` — полный доступ; SID — SID пользователя.

При использовании СКЗИ и создании ключей с использованием флага CRYPT_LOCALMACHINE дополнительно требуется доступ к следующим ключам реестра:

- `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Settings` — полный доступ.

Для изменения конфигурации СКЗИ КриптоПро CSP версии 5.0 КС1 с использованием панели управления (Control Panel), также требуется полный доступ к ключу реестра `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro`.

Примечание.
1) По умолчанию КриптоПро CSP версии 5.0 КС1 может использовать до 65536 дескрипторов криптографических объектов. Для увеличения этого значения необходимо добавить в реестр (`HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\Parameters`) параметр DWORD, равный требуемому числу описателей, но не более 1048576.

2) Хранение закрытых ключей и ключей подписи на HDD ПЭВМ, USB-флэш-накопителях и в реестре ОС Windows допускается только при условии распространения на HDD, USB-флэш-накопители или на ПЭВМ с HDD требований по обращению с ключевыми носителями, в том числе и после удаления ключей (раздел 3 ЖТЯИ.00101-01 95 01. Правила пользования).

6.4 Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки сетевой аутентификации реализуется в форме подгружаемой библиотеки и реализует подмножество интерфейса Microsoft SSPI (SSP/AP) (см. раздел MSDN). Модуль обеспечивает аутентичное защищенное соединение между пользователем и сервером. `cpssl.dll`, `cpsspap.dll` — при установке модуля аутентификации, поддерживающего аутентификацию в домене, `cpsspcore.dll`, `ssp.dll` — без возможности доменной аутентификации.

6.4.1 Инициализация библиотеки SSPI

Производится загрузка библиотеки Secur32.dll.

С помощью функции GetProcAddress получается указатель на функцию InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode).

Вызовом функции InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode) получается таблица функций SSPI.

Вместо использования GetProcAddress, можно подключить библиотеку импорта secur32.lib (входит в MS Platform SDK)

Заполняется структура SCHANNEL_CRED. Поля этой структуры должны быть нулевыми, кроме:
- SchannelCred.dwVersion = SCHANNEL_CRED_VERSION;
- SchannelCred.dwFlags = SCH_CRED_NO_DEFAULT_CREDS | SCH_CRED_MANUAL_CRED_VALIDATION;

Для сервера и не анонимного клиента заполняются также поля:
- SchannelCred.cCreds = 1;
- SchannelCred.paCred = &pCertContext.

Примечание. Контекст сертификата pCertContext должен содержать ссылку на закрытый ключ.

Производится вызов функции создания Credentials: AcquireCredentialsHandle с передачей ей структуры SCHANNEL_CRED и имени пакета - UNISP_NAME («Microsoft Unified Security Protocol Provider»).

Инициализация соединения клиентом производится вызовом InitializeSecurityContext без входного буфера и сервером – вызовом AcceptSecurityContext, после чего идет обычный цикл Handshake.

После установления соединения, но до начала передачи данных, приложение должно выполнить проверку

параметров соединения и сертификата удаленной стороны.

Для получения сертификата удаленной стороны вызывается функция QueryContextAttributes с аргументом SECPKG_ATTR_REMOTE_CERT_CONTEXT.

Для построения цепочки сертификатов рекомендуется использование функции CertGetCertificateChain, описанную в MSDN/Platform SDK/Security, (с флагами проверки, соответствующими выбранному уровню безопасности. Рекомендуется использовать флаг CERT_CHAIN_CACHE_END_CERT | CERT_CHAIN_REVOCATION_CHECK_CHAIN.

Цепочка сертификатов проверяется функцией CertVerifyCertificateChainPolicy, описанной там же, с аргументом pszPolicy, равным OIDCERT_CHAIN_POLICY_SSL, и аргументом pPolicyPara, заполненным следующим образом:

- ZeroMemory(&polHttps, sizeof(HTTPSPolicyCallbackData));
- polHttps.cbStruct = sizeof(HTTPSPolicyCallbackData);
- polHttps.dwAuthType = AUTHTYPE_SERVER;
- polHttps.fdwChecks = 0;
- polHttps.pwszServerName = pwszServerName;
- memset(&PolicyPara, 0, sizeof(PolicyPara));
- PolicyPara.cbSize = sizeof(PolicyPara);
- PolicyPara.pvExtraPolicyPara = &polHttps

Необходимо, чтобы для каждого сертификата в цепочке pCertContext → pCertInfo → SubjectPublickeyInfo → Algoritm → pszObjId pszObjId заканчивалась на szOID_GR3410.

Вызывается функция QueryContextAttributes с аргументом ulAttribute, равным SECPKG_ATTR_CONNECTION_INFO, для получения параметров соединения и их проверки на выполнение условий:

- ConnectionInfo.dwProtocol == SP_PROT_TLS1_CLIENT;
- ConnectionInfo.aiCipher == CALG_G28147, ConnectionInfo.aiHash == CALG_GR3411;
- aiExch=CALG_DH_EX_EPHEM или CALG_DH_EX_SF;

Шифрование/расшифрование реализуется с помощью функций EncryptMessage()/DecryptMessage().

Примечание. Должна быть обеспечена корректная обработка кодов возврата функций SSPI. При этом следует учитывать, что требуется разная обработка в зависимости от того, является код возврата кодом успешного выполнения функции, кодом не фатальной ошибки, не требующей разрыва соединения, или кодом фатальной ошибки, требующей разрыва соединения. Все необрабатываемые коды возврата ошибок должны приводить к разрыву соединения.

Корректное завершение сессии осуществляется вызовом функции ApplyControlToken.

Требования безопасности:

1) Применение модуля поддержки сетевой аутентификации допускается только при использовании открытых ключей сервера и клиента, сертифицированных доверенным центром сертификации.

2) Приложением должны обеспечиваться:

- проверка сертификатов в сообщениях Certificate и CertVerify;
- проверка 12 байт в сообщениях Finished клиента и сервера, являющихся имитовставками к информации всего диалога клиент-сервер в процессе установления сессии;
- контроль соответствия имени клиента (сервера) IP-адресу, по которому установлена сессия.

7 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 документа ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть и раздела 5 ЖТЯИ.00101-01 95 01. Правила пользования.

Для ОС Windows дополнительно должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1) В системе регистрируется один пользователь, обладающий правами администратора, на которого возлагается обязанность конфигурировать ОС Windows, настраивать безопасность ОС, а также конфигурировать ПЭВМ, на которую установлена ОС Windows.

2) Для администратора выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 8 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в 6 месяцев, доступ к паролю должен быть обеспечен только пользователю, обладающему правами администратора.

3) Всем пользователям, зарегистрированным в ОС Windows, администратор в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Windows, не являющийся администратором, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему администратором.

4) На компьютере устанавливается только одна ОС Windows (в случае использования виртуальной инфраструктуры допускается установка одной хостовой и неограниченного числа гостевых ОС). Не используются нестандартные, измененные или отладочные версии ОС Windows (например, Debug/Checked Build). На всех HDD должна быть установлена файловая система NTFS.

5) Права доступа к каталогам `%Systemroot%\System32\Config`, `%Systemroot%\System32\SPOOL`, `%Systemroot%\Repair`,`%Systemroot%\COOKIES`, `%Systemroot%\FORMS`, `%Systemroot%\HISTORY`, `%Systemroot%\SENDTO`, `%Systemroot%\PROFILES`, `%Systemroot%\OCCASHE`, `\TEMP`, а также файлам `boot.ini`, `autoexec.bat`, `config.sys`, `ntdetect.com` и `ntldr` должны быть установлены в соответствии с политикой безопасности, принятой в организации.

6) Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности, что реализуется при помощи ACL или установкой прав доступа при наличии NTFS.

7) Должна быть исключена возможность удаленного редактирования системного реестра.

8) Должна быть проведена установка SECURITY_ATTRIBUTES процессов и потоков в соответствии с требованиями безопасности всей системы в целом.

9) Если нет необходимости, не следует использовать протокол SMB. В случае необходимости использования протокола SMB параметры EnableSecuritySignature (REG_DWORD) и RequareSecuritySignature (REG_DWORD) в ключе `HKLM\System\CurrentControlSet\Services\LanManServer\Parametrs` должны быть установлены со значениями «1».

10) У группы Everyone должны быть удалены все привилегии.

11) Должен быть переименован пользователь Administrator.

12) Должна быть отключена учетная запись для гостевого входа (Guest).

13) Должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке.

14) Должно быть ограничено с учетом выбранной в организации политики безопасности использование

пользователями сервиса Scheduler.

15) Должен быть отключен сервис DCOM.

16) Должны быть отключены сетевые протоколы, не используемые на данной ПЭВМ.

17) В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть исключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносного ПО.

18) Должна быть исключена возможность сетевого администрирования для всех, включая группу Administrators.

19) Должен быть закрыт доступ ко всем не используемым портам.

20) Должны включаться фильтры паролей, устанавливаемые вместе с пакетами обновлений ОС Windows.

21) Должны быть исключены исполнение и открытие файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносного ПО.

22) Должны быть удалены все общие ресурсы на ПЭВМ с установленным СКЗИ КриптоПро CSP версии 5.0 КС1 (в том числе и создаваемые по умолчанию при установке ОС Windows), которые не используются. Права доступа к используемым общим ресурсам должны быть заданы в соответствии с политикой безопасности принятой в организации.

23) После установки операционной системы из каталога `%Systemroot%\System32\Config` должен быть удален файл `sam.sav`.

24) Должны использоваться наиболее защищенные протоколы аутентификации, реализованные в ОС Windows, если функционирование СКЗИ не предусматривает применение других протоколов.

25) По возможности следует применять самые сильные шаблоны безопасности (Templates).

26) Должна быть разработана система назначения и смены паролей.

27) Должно быть запрещено использование функции резервного копирования паролей.

28) Должны быть отключены режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей.

29) Должна быть отключена возможность удаленного администрирования ПЭВМ с установленным СКЗИ КриптоПро CSP версии 5.0 КС1.

30) Должно быть ограничено количество неудачных попыток входа в систему, в соответствие с политикой безопасности (но не более 10), принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток.

31) Должна использоваться система аудита в соответствии с политикой безопасности, принятой в организации, и организован регулярный анализ результатов аудита.

32) Должен проводиться регулярный просмотр сообщений в журнале событий Event viewer с периодичностью не реже 1 раза в неделю.

33) ОС Windows должна быть настроена на завершение работы при переполнении журнала аудита.

34) Должна быть обеспечена невозможность модификации ОС Windows через общедоступные каналы передачи данных (Windows Update, Remote Assistance...).

35) После инсталляции ОС Windows должен быть установлен последний официальный Service Pack от фирмы Microsoft, существующий на момент установки ОС Windows.

36) Должны использоваться подписанные драйверы.

37) На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System).

38) Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.

7.1 Настройка системного реестра ОС Windows при установке СКЗИ

На ПЭВМ с ОС Windows при установке СКЗИ необходимо провести настройку системного реестра:

• в ключе HKLM\System\CurrentControlSet\Control\LSA установить параметр RestrictAnonymous (REG_DWORD) со значением «1» для исключения доступа анонимного пользователя (null-session) к списку разделяемых ресурсов, а также для исключения доступа к содержимому системного реестра;

• для исключения утечки информации при передаче данных по именованному каналу \\server\PIPE\SPOOLSS удалить имя SPOOLSS из ключа HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes;

• в ключе HKLM\System\CurrentControlSet\Services\LanManServer\Parameters установить параметры AutoShareWks и AutoShareServer, имеющие тип REG_DWORD, со значением «0» для запрета автоматического создания скрытых совместных ресурсов;

• в ключе HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon установить параметр CashedLogonCount (REG_DWORD) со значением 0 для отключения кэширования паролей последних десяти пользователей, вошедших в систему;

• в ключе HKLM\System\CurrentControlSet\Services\Eventlog\<LogName> (LogName – имя журнала для которого следует ограничить доступ пользователям группы Everyone) установить параметр RestrictGuestAccess (REG_DWORD) со значением «1» для исключения доступа группы Everyone к системному журналу и журналу приложений;

• в ключе HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagment установить параметр ClearPageFileAtShutDown (REG_DWORD) со значением «1» для включения механизма затирания файла подкачки при перезагрузке;

• в ключе HKLM\System\CurrentControlSet\Control\SecurePipeServers установить в соответствии с политикой безопасности принятой в организации разрешения на доступ к параметру winreg для ограничения удаленного доступа к реестру;

• в ключе HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon установить параметр AllocateFloppies (REG_SZ) со значением «1» для исключения параллельного использования дисковода для гибких дисков;

• в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр AuditBaseObjects (REG_DWORD) со значением «1» для включения аудита на базовые объекты системы;

• в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр FullPrivilegeAuditing (REG_BINARY) со значением «1» для включения аудита привилегий;

• для исключения передачи пароля пользователей по сети в открытом виде в ключе HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters установить параметр EnablePlainTextPassword (REG_DWORD) со значением «0».

8 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть в части, касающейся ОС Windows.

Контролем целостности должны быть охвачены следующие файлы:

Windows 32-bit

```
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files\Common Files\Crypto Pro\AppCompat\CProCtrl.sys
\Program Files\Crypto Pro\CSP\accord.dll
\Program Files\Crypto Pro\CSP\apmdz.dll
\Program Files\Crypto Pro\CSP\bio.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpExSec.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpMSO.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Windows\system32\cpcng.dll
\Program Files\Crypto Pro\CSP\cpconfig.cpl
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files\Crypto Pro\CSP\cpcsp.dll
\Program Files\Crypto Pro\CSP\cpcspi.dll
\Program Files\Crypto Pro\CSP\cpdrvlib.sys
\Program Files\Common Files\Crypto Pro\AppCompat\cpenroll.dll
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files\Crypto Pro\CSP\cpksp.sys
\Program Files\Common Files\Crypto Pro\AppCompat\cpmail.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files\Crypto Pro\CSP\cprdr.dll
\Program Files\Crypto Pro\CSP\cprndm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpsecur.dll
\Windows\system32\cpssl.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpsslsdk.dll
\Windows\system32\cpsspap.dll
\Program Files\Crypto Pro\CSP\cpsuprt.dll
\Program Files\Crypto Pro\CSP\cpui.dll
\Program Files\Crypto Pro\CSP\cpverify.exe
\Program Files\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpxml5.dll
\Program Files\Crypto Pro\CSP\csptest.exe
\Program Files\Crypto Pro\CSP\crypton.dll
\Program Files\Crypto Pro\CSP\dallas.dll
\Program Files\Crypto Pro\CSP\ds199x.dll
\Program Files\Crypto Pro\CSP\dsrf.dll
\Program Files\Crypto Pro\CSP\emv.dll
```

```
\Program Files\Crypto Pro\CSP\esmarttoken.dll
\Program Files\Crypto Pro\CSP\etok.dll
\Program Files\Crypto Pro\CSP\fat12.dll
\Program Files\Crypto Pro\CSP\genkpim.exe
\Program Files\Crypto Pro\CSP\inpaspot.dll
\Program Files\Crypto Pro\CSP\isbc.dll
\Program Files\Crypto Pro\CSP\jcard.dll
\Program Files\Crypto Pro\CSP\kst.dll
\Program Files\Crypto Pro\CSP\novacard.dll
\Program Files\Crypto Pro\CSP\pcsc.dll
\Program Files\Crypto Pro\CSP\reg.dll
\Program Files\Crypto Pro\CSP\ric.dll
\Program Files\Crypto Pro\CSP\rtSupCP.dll
\Program Files\Crypto Pro\CSP\sable.dll
\Program Files\Crypto Pro\CSP\snet.dll
\Program Files\Crypto Pro\CSP\wipefile.exe
\Program Files\Crypto Pro\CSP\esmarttokengost.dll
\Program Files\Crypto Pro\CSP\certmgr.exe
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Windows\system32\inetcomm.dll
\Windows\system32\rastls.dll
\Windows\system32\wininet.dll
\Windows\system32\msi.dll
\Windows\system32\crypt32.dll
\Windows\system32\schannel.dll
\Windows\system32\kerberos.dll
\Windows\system32\certenroll.dll
\Windows\system32\cryptsp.dll*
\Windows\system32\sspicli.dll*
```

* Для ОС Windows Server 2008 под контролем целостности вместо библиотек `cryptsp.dll` и `sspicli.dll` находятся библиотеки `\Windows\system32\advapi32.dll` и `\Windows\system32\secur32.dll`.

Windows 64-bit

```
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files (x86)\Crypto Pro\CSP\accord.dll
\Program Files (x86)\Crypto Pro\CSP\apmdz.dll
\Program Files (x86)\Crypto Pro\CSP\bio.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpExSec.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpMSO.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files (x86)\Crypto Pro\CSP\cpcsp.dll
\Program Files (x86)\Crypto Pro\CSP\cpcspi.dll
\Program Files (x86)\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpmail.dll
```

```
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files (x86)\Crypto Pro\CSP\cprdr.dll
\Program Files (x86)\Crypto Pro\CSP\cprndm.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpsecur.dll
\WINDOWS\SysWOW64\cpssl.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpsslsdk.dll
\WINDOWS\SysWOW64\cpsspap.dll
\Program Files (x86)\Crypto Pro\CSP\cpsuprt.dll
\Program Files (x86)\Crypto Pro\CSP\cpui.dll
\Program Files (x86)\Crypto Pro\CSP\cpverify.exe
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\cpxml5.dll
\Program Files (x86)\Crypto Pro\CSP\csptest.exe
\Program Files (x86)\Crypto Pro\CSP\crypton.dll
\Program Files (x86)\Crypto Pro\CSP\dallas.dll
\Program Files (x86)\Crypto Pro\CSP\ds199x.dll
\Program Files (x86)\Crypto Pro\CSP\dsrf.dll
\Program Files (x86)\Crypto Pro\CSP\emv.dll
\Program Files (x86)\Crypto Pro\CSP\esmarttoken.dll
\Program Files (x86)\Crypto Pro\CSP\etok.dll
\Program Files (x86)\Crypto Pro\CSP\fat12.dll
\Program Files (x86)\Crypto Pro\CSP\genkpim.exe
\Program Files (x86)\Crypto Pro\CSP\inpaspot.dll
\Program Files (x86)\Crypto Pro\CSP\isbc.dll
\Program Files (x86)\Crypto Pro\CSP\jcard.dll
\Program Files (x86)\Crypto Pro\CSP\kst.dll
\Program Files (x86)\Crypto Pro\CSP\novacard.dll
\Program Files (x86)\Crypto Pro\CSP\pcsc.dll
\Program Files (x86)\Crypto Pro\CSP\reg.dll
\Program Files (x86)\Crypto Pro\CSP\ric.dll
\Program Files (x86)\Crypto Pro\CSP\rtSupCP.dll
\Program Files (x86)\Crypto Pro\CSP\sable.dll
\Program Files (x86)\Crypto Pro\CSP\snet.dll
\Program Files (x86)\Crypto Pro\CSP\wipefile.exe
\Program Files (x86)\Crypto Pro\CSP\esmarttokengost.dll
\Program Files (x86)\Crypto Pro\CSP\certmgr.exe
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files\Common Files\Crypto Pro\AppCompat\CProCtrl.sys
\Program Files\Crypto Pro\CSP\accord.dll
\Program Files\Crypto Pro\CSP\apmdz.dll
\Program Files\Crypto Pro\CSP\bio.dll
\Program Files\Crypto Pro\CSP\crypton.dll
\WINDOWS\system32\cpsspap.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpadvai.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpcertocm.dll
\Program Files\Crypto Pro\CSP\cpconfig.cpl
\Program Files\Common Files\Crypto Pro\AppCompat\cpcrypt.dll
\Program Files\Crypto Pro\CSP\cpcsp.dll
```

```
\Program Files\Crypto Pro\CSP\cpcspi.dll
\Program Files\Crypto Pro\CSP\cpdrvlib.sys
\Program Files\Common Files\Crypto Pro\Shared\cpext.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpintco.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpkrb.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpmail.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpoutlm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cprastls.dll
\Program Files\Crypto Pro\CSP\cprdr.dll
\Program Files\Crypto Pro\CSP\cprndm.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpschan.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpsecur.dll
\WINDOWS\system32\cpssl.dll
\Program Files\Crypto Pro\CSP\cpsuprt.dll
\Program Files\Crypto Pro\CSP\cpui.dll
\Program Files\Common Files\Crypto Pro\AppCompat\cpwinet.dll
\Program Files\Crypto Pro\CSP\csptest.exe
\Program Files\Crypto Pro\CSP\dallas.dll
\Program Files\Crypto Pro\CSP\ds199x.dll
\Program Files\Crypto Pro\CSP\dsrf.dll
\Program Files\Crypto Pro\CSP\emv.dll
\Program Files\Crypto Pro\CSP\esmarttoken.dll
\Program Files\Crypto Pro\CSP\etok.dll
\Program Files\Crypto Pro\CSP\fat12.dll
\Program Files\Crypto Pro\CSP\inpaspot.dll
\Program Files\Crypto Pro\CSP\isbc.dll
\Program Files\Crypto Pro\CSP\jcard.dll
\Program Files\Crypto Pro\CSP\kst.dll
\Program Files\Crypto Pro\CSP\novacard.dll
\Program Files\Crypto Pro\CSP\pcsc.dll
\Program Files\Crypto Pro\CSP\reg.dll
\Program Files\Crypto Pro\CSP\ric.dll
\Program Files\Crypto Pro\CSP\rtSupCP.dll
\Program Files\Crypto Pro\CSP\sable.dll
\Program Files\Crypto Pro\CSP\snet.dll
\Program Files\Crypto Pro\CSP\certmgr.exe
\Program Files\Crypto Pro\CSP\esmarttokengost.dll
\Program Files (x86)\Common Files\Crypto Pro\AppCompat\detoured.dll
\Program Files\Common Files\Crypto Pro\AppCompat\detoured.dll
\Windows\system32\inetcomm.dll
\Windows\SysWOW64\inetcomm.dll
\Windows\system32\rastls.dll
\Windows\SysWOW64\rastls.dll
\Windows\system32\wininet.dll
\Windows\SysWOW64\wininet.dll
\Windows\system32\msi.dll
\Windows\SysWOW64\msi.dll
\Windows\system32\crypt32.dll
\Windows\SysWOW64\crypt32.dll
\Windows\system32\schannel.dll
```

```
\Windows\SysWOW64\schannel.dll
\Windows\system32\kerberos.dll
\Windows\SysWOW64\kerberos.dll
\Windows\system32\certenroll.dll
\Windows\SysWOW64\certenroll.dll
\Windows\system32\cryptsp.dll*
\Windows\SysWOW64\cryptsp.dll*
\Windows\system32\sspicli.dll*
\Windows\SysWOW64\sspicli.dll*
```

* Для ОС Windows Server 2008 под контролем целостности вместо библиотек `cryptsp.dll` и `sspicli.dll` находятся библиотеки `\Windows\system32\advapi32.dll`, `\Windows\SysWOW64\advapi32.dll`, `\Windows\system32\secur32.dll`, `\Windows\SysWOW64\secur32.dll`.

В случае нарушения целостности данных библиотек в результате обновления операционной системы необходимо обратиться к разработчику СКЗИ за разъяснениями о возможности продолжения использования СКЗИ на данной системе.

Приложение А
Службы сертификации операционной системы Windows

Ведущие мировые производители системного и прикладного программного обеспечения активно интегрируют решения, основанные на Инфраструктуре открытых ключей в операционные системы и приложения. Ярким примером является операционная система Windows, полностью поддерживающая ИОК.

В операционной системе Microsoft Windows в полном объеме реализована Инфраструктура открытых ключей. Эта инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом продуктов и центров сертификации. Простейшая форма иерархии состоит из одного центра сертификации, а в общем случае – из множества с явно определенными отношениями родительский-дочерний.

Инфраструктура открытых ключей, реализованная в операционной системе Microsoft Windows, полностью поддерживает и позволяет создать иерархическую модель центров сертификации (см. рис. 6).

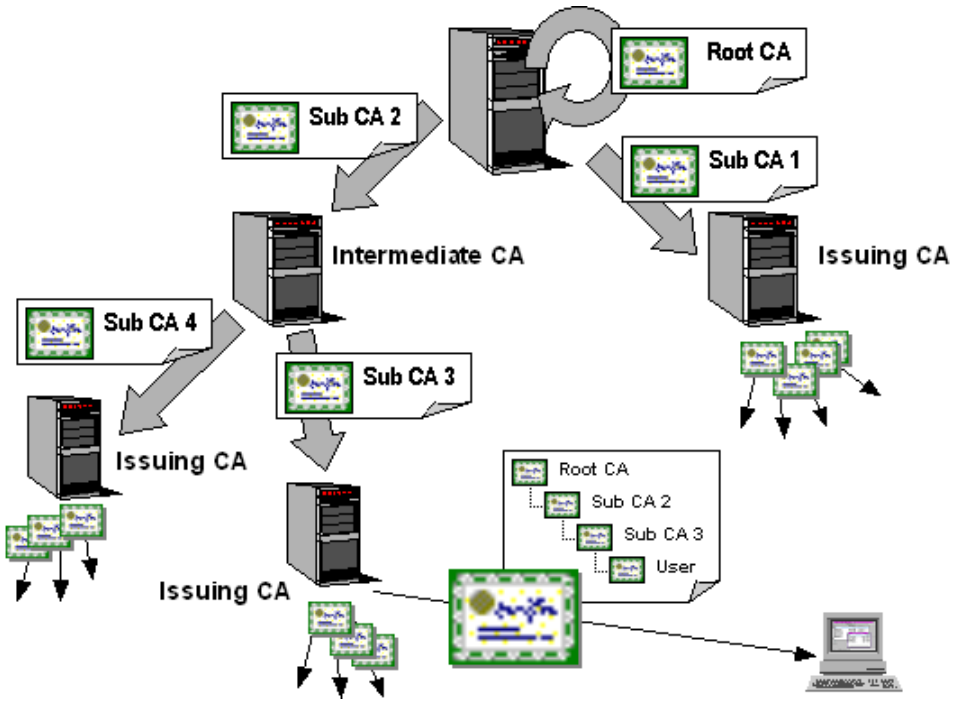

Рисунок 6. Модель построения центров сертификации

В состав служб сертификации операционной системы Windows входят следующие службы и компоненты.

Сервис сертификации

Сервис сертификации предоставляет набор служб для выпуска, управления и использования сертификатов открытых ключей в защищенных технологиях и приложениях, использующих ИОК. Сервис сертификации выполняет основную роль в управлении безопасностью технологий и приложений и обеспечивает процесс достоверного и конфиденциального обмена информацией.

Консоль центра сертификации

Консоль центра сертификации является рабочим местом администратора безопасности, позволяющим управлять сертификатами открытых ключей (см. рис. 7).

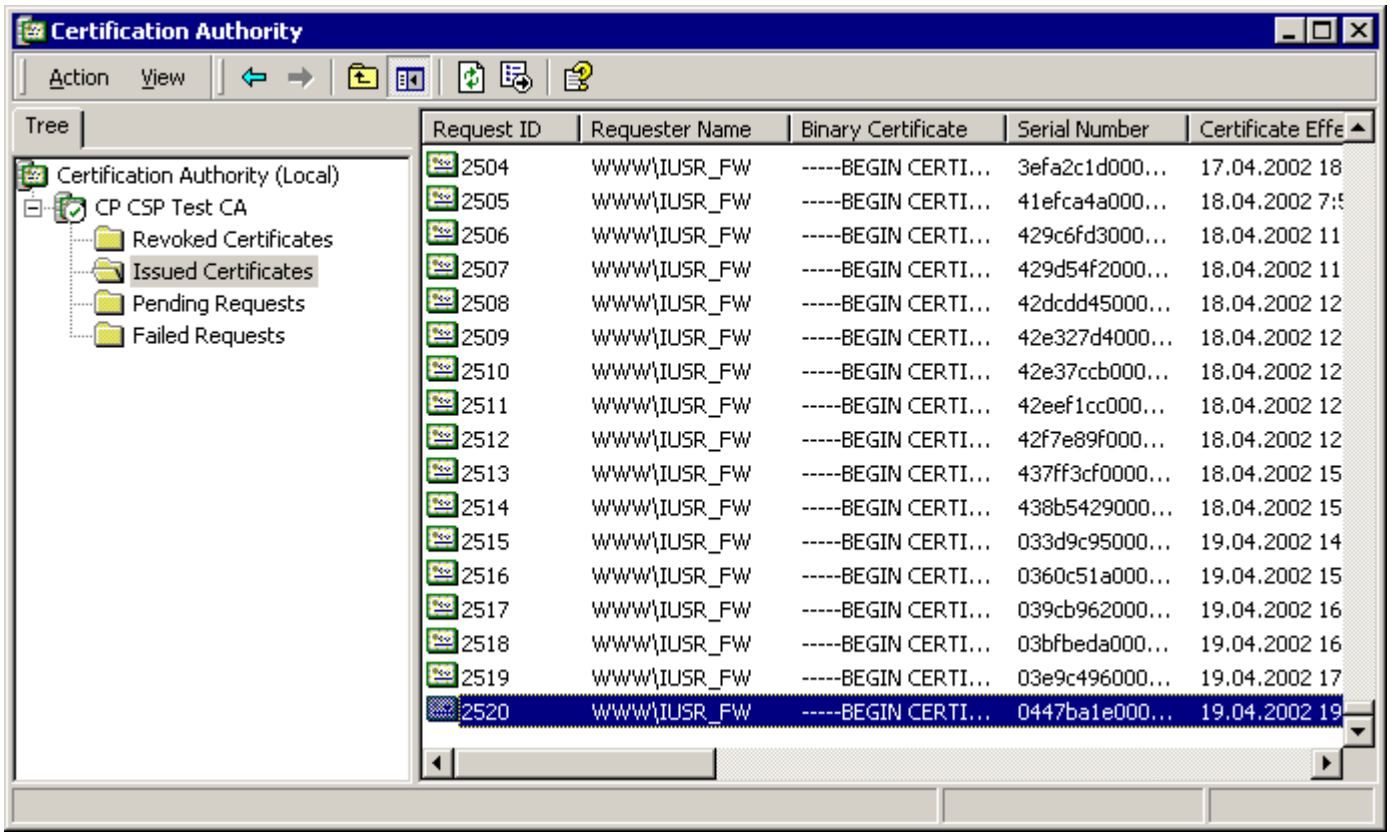

Рисунок 7. Консоль центра сертификации

Средства расширения функциональности сервиса сертификации

Средства расширения функциональности сервиса сертификации предоставляют набор методов, позволяющих изменять и развивать функциональность стандартного сервиса сертификации для удовлетворения потребности конкретной прикладной системы или технологии. Эти средства позволяют интегрировать сервис сертификации с различными сетевыми справочниками и приложениями, формировать состав сертификатов открытых ключей, модифицировать процесс управления сертификатами.

Клиентские средства взаимодействия со службой сертификации

Клиентские средства предоставляют пользователям различные методы для формирования закрытых ключей, запросов на сертификаты и обработки сертификатов, выпущенных службой сертификации.

Архитектура сервиса сертификации представлена на рис. 8.

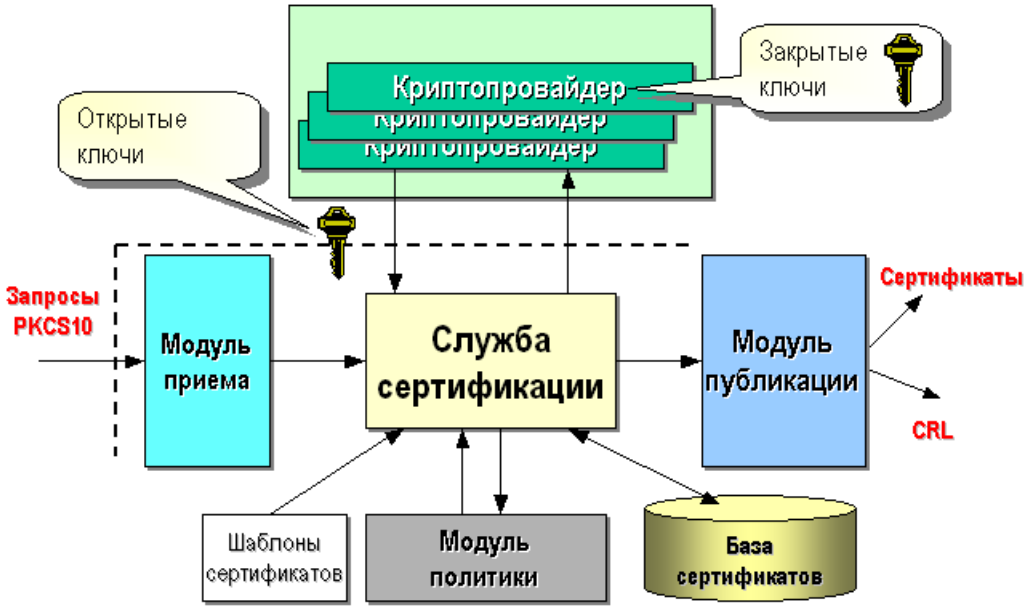

Рисунок 8. Архитектура сервиса сертификации

Приложение Б
Управление протоколированием

Для включения/отключения протоколирования для Windows 32[Windows 64] добавляется в реестр:

`HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]CryptoPro\Cryptography\CurrentVersion\debug\`

- DWORD параметр cpcsp для определения уровня протокола

Значением параметра уровень протокола является битовая маска:
N_DB_ERROR = 1 # сообщения об ошибках
N_DB_LOG = 8 # сообщения о вызовах

- DWORD параметр cpcsp_fmt для определения формата протокола

Значением параметра формат протокола является битовая маска:
DBFMT_MODULE = 1 # выводить имя модуля
DBFMT_THREAD = 2 # выводить номер нитки
DBFMT_FUNC = 8 # выводить имя функции
DBFMT_TEXT = 0x10 # выводить само сообщение
DBFMT_HEX = 0x20 # выводить HEX дамп
DBFMT_ERR = 0x40 # выводить GetLastError

Для включения аудита использования КриптоПро TLS на Windows в реестр `System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\` добавляется параметр:

Значение имени: EventLogging
Тип данных: REG_DWORD

Параметру присваиваются следующие значения:
0x0000 не записывать в журнал
0x0001 журнал сообщений об ошибках
0x0002 журнал предупреждений
0x0004 журнал информационных событий
0x0008 журнал успешных событий

Аудит выполнения процесса cpsspap будет выводиться в журнал приложений Windows.

Настройки ведения журнала вступают в силу после пересоздания мандата.

Лист регистрации изменений

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