127 018, Москва, Сущевский Вал, д.18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 4.0 КС2

2-Base

Руководство администратора безопасности

Использование СКЗИ под управлением ОС Windows

ЖТЯИ.00088-01 91 02
Листов 47

2017 г.

Содержание

Аннотация

Настоящее Руководство дополняет документ «ЖТЯИ.00088-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» при использовании СКЗИ под управлением операционных систем Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» v 4.0, должны разрабатываться с учетом требований настоящего документа.

Список сокращений

АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа абонента в центре сертификации
СФК	Среда функционирования криптосредства
СКЗИ	Средство криптографической защиты информации

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратные среды функционирования

СКЗИ ЖТЯИ.00088-01 функционирует под управлением ОС Windows в программно-аппаратных средах:

Windows XP[1] (x86);
Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016 (x64).

Примечания:
1. Версия POSReady.
2. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем.

1.2. Состав СКЗИ

Исполнение 2-Base класса защиты КС2 выполнено в составе:

- криптосервис;
- криптодрайвер;
- модуль сетевой аутентификации (КриптоПро TLS);
- модуль обработки сертификатов и CMS протокола;
- утилита выработки внешней гаммы;
- утилита командной строки;
- модуль аутентификации пользователя в домене Windows;
- модуль поддержки интерфейса Mozilla NSS;
- сервисные модули (cpverify, wipefile, stunnel);
- библиотека, обеспечивающая подключение и функционирование ключевых носителей (RDK)

и функционирует в группах программно-аппаратных сред п.1.1.

1.3. Ключевые носители

В качестве ключевых носителей используются:

- ГМД 3,5'', USB диски;
- Смарткарты GEMALTO (GemSim1, GemSim2, Optelio, OptelioCL, OptelioCL2, Native);
- eToken, Jacarta;
- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite Novacard;
- Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC;
- Rutoken S;
- Novacard;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- Смарткарта УЭК;
- Смарткарта MS_KEY K;

- ESMART Token;
- Смарткарты Athena IDProtect, MorphoKST, Cha cardOS, Cha JCOP;
- Смарткарты Алиот INPASPOT Series, SCOne Series;
- Rosan;
- Раздел HDD ПЭВМ (в Windows - реестр);
- Идентификаторы Touch-Memory DS1995, DS1996.

Использование ключевых носителей в зависимости от программно-аппаратной платформы отражено в ЖТЯИ.00088-01 30 01. СКЗИ «КриптоПро CSP 4.0». Формуляр, п. 3.8.

	1. 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. 1. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-01 91 01. Руководство администратора безопасности общая часть). 2. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене. 3. Использование носителей других типов - только по согласованию с ФСБ России.

2. Установка дистрибутивов ПО СКЗИ

Установка дистрибутива «КриптоПро CSP» v 4.0 должна производится пользователем, имеющим права администратора.

Для установки СКЗИ «КриптоПро CSP» v 4.0 сначала необходимо установить провайдер, а затем устанавливать остальные модули, входящие в состав комплектации.

Для установки программного обеспечения вставьте компакт-диск в привод считывателя. Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы, имеющий нужный Вам класс защиты и удобный для Вас язык установки. Запустите выполнение установки.

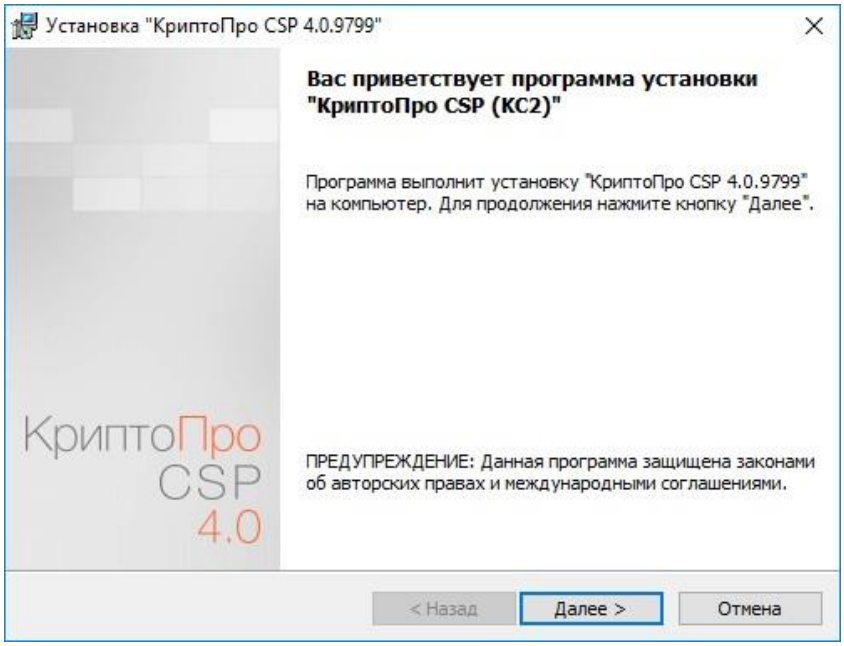

Рисунок 2.1 – Мастер установки «КриптоПро CSP» v 4.0.

Для дальнейшей установки КриптоПро CSP нажмите Далее.

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» v 4.0.

При установке «КриптоПро CSP» v 4.0 можно использовать различные параметры командной строки, влияющие на устанавливаемые компоненты, начальную настройку продукта и т.д.

Для их использования необходимо запускать установку следующим образом:

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

Следующие опции позволяют не устанавливать соответствующие библиотеки поддержки:

NODALLAS=1	Носители Dallas
NODS=1	Считыватели Dallas
NODSRF=1	ДСЧ «Последовательность поставщика»
NOEMV=1	Карта EMV
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

Следующие опции позволяют управлять регистрацией поддерживаемого оборудования во время установки «КриптоПро CSP» v 4.0 (значение «0» означает «отключить опцию»; звездочкой отмечены опции, включенные по умолчанию):

REGETOKEN=1	Зарегистрировать все носители «Alladin eToken» * (отдельные типы: REGETOKENJAVA10, REGETOKENJAVA10B, REGETOKENM420, REGETOKENM420B, REGETOKEN16, REGETOKEN32, REGETOKENR2)
REGFLOPPY=буквы	Зарегистрировать считыватель «дискета» для букв, указанных через запятую
REGPNPFLOPPY=1	Зарегистрировать считыватель «Все съемные носители» *
REGDSRF=путь	Зарегистрировать ДСЧ «Последовательность поставщика» и задать путь (без «\» на конце) к папке с dsrfnet
REGDS1410E=порты	Зарегистрировать считыватель «DS1410E» (список портов через запятую: LPT1,LPT2,...)
REGDS9097E=порты	Зарегистрировать считыватель «DS9097E» (список портов через запятую: COM1,COM2,...)
REGDS9097U=порты	Зарегистрировать считыватель «DS9097U» (список портов через запятую: COM1,COM2,...)
REGDS199X=1	Зарегистрировать носитель «DS199x»
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 смарткарт» *
REGALLPCSC=1	Зарегистрировать подключенные считыватели смарткарт
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»
NOETOKENWL=1	Не регистрировать носители «Alladin eToken» 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 *

Управление режимами работы:

CPCSPR=1	Для версии КС1 позволяет выбрать режим службы хранения ключей (только при установке)
MEDIACSPS=1	Регистрировать в системе отдельный провайдер для каждого типа ключевых носителей (только при установке)
CACHED=N	Настройка кэширования ключей. Если N=0, то выключено, если N>0, то задает размер кэша (только при установке и только для режима службы хранения ключей)
CSPDELETEKEYS=1	При удалении продукта удалит так же все настройки и все ключевые контейнеры из реестра
STRENGTHENEDKEYUSAGECONTROL=1	Включить режим усиленного контроля использования ключей (только при установке; режим обязателен к использованию)

Указание серийных номеров лицензий:

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

Стандартные параметры Windows Installer (подробнее – см. документацию: http://msdn.microsoft.com/en-us/library/aa367988.aspx):

INSTALLDIR=	Путь установки
INSTALLDIR64=	Путь установки для 64-разрядных компонент
REBOOT=R	Не перезагружать компьютер после установки
ADDLOCAL=модули	Задает список дополнительных модулей, которые следует установить (список через запятую). Существующие дополнительные модули: reprov, driver, compat.
REMOVE=модули	Для уже установленного продукта удаляет указанные модули

Дополнительные параметры.

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

Для удаления КриптоПро CSP:

msiexec /x {54A08450-B343-40B0-924E-68F031450996}

Примеры:

msiexec /i "d:\КриптоПро CSP 4.0\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 4.0\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», 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.

3. Обновление «КриптоПро CSP v 4.0»

Для обновления «КриптоПро CSP» v 4.0 на ОС Windows необходимо:

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

– удалить штатными средствами ОС дистрибутив КриптоПро CSP;

– установить аналогичный новый дистрибутив КриптоПро CSP;

– при необходимости внести изменения в настройки.

Ключи и сертификаты сохраняются автоматически.

4. Варианты встраивания «КриптоПро CSP» v 4.0 и «КриптоПро TLS» в прикладное ПО

4.1. Встраивание на уровне CryptoAPI 2.0.

«КриптоПро CSP» v 4.0 может быть использовано в прикладном программном обеспечении (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0, описание которого приведено в программной документации MSDN (Microsoft Developer Network):

http://msdn.microsoft.com/en-us/library/windows/desktop/aa380239.aspx.

В этом случае способ выбора криптографического алгоритма в прикладном ПО может определяться идентификатором алгоритма открытого ключа отправителя/получателя, содержащегося в сертификате X.509.

Встраивание на уровне CryptoAPI 2.0 позволяет воспользоваться набором функций, решающих большинство проблем, связанных с представлением (форматами) различных криптографических сообщений (подписанных, зашифрованных), способами представления открытых ключей в виде цифровых сертификатов, способами хранения и поиска сертификатов в различных справочниках, включая LDAP.

Функции CryptoAPI 2.0 позволяют полностью реализовать представление и обмен данными в соответствии с международными рекомендациями и Инфраструктурой Открытых Ключей (Public Key Infrastructure).

4.2. Встраивание на уровне CSP

«КриптоПро CSP» v 4.0 может быть непосредственно использовано в прикладном программном обеспечении путем загрузки модуля с использованием функции LoadLibrary(). Для этих целей в комплект поставки включается ЖТЯИ.00088-01 96 01 «КриптоПро CSP. v 4.0 Руководство программиста», описывающее состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

4.3. Использование COM интерфейсов

«КриптоПро CSP» v 4.0 может взаимодействовать со следующими COM интерфейсами разработки Microsoft:

- CAPICOM;
- Certificate Enrollment Control;
- Certificate Enrollment API;
- Certificate Services.

4.3.1. CAPICOM

CAPICOM (реализован в файле capicom.dll) предоставляет COM интерфейс, использующий основные функции CryptoAPI 2.0. Этот компонент является добавлением к уже существующему COM интерфейсу Certificate Enrollment Control (xenroll.dll), который реализуют клиентские функции генерации ключей, запросов на сертификаты и обмена с Центром Сертификации.

CAPICOM позволяет использовать функции формирования и проверки электронной подписи, построения и проверки цепочек сертификатов, взаимодействия с различными справочниками сертификатов (включая Active Directory) с использованием Visual Basic, C++,

JavaScript, VBScript и среды разработки Delphi. Использование CAPICOM позволяет реализовать функциональность «тонкого» клиента в интерфейсе браузера Internet Explorer/Microsoft Edge.

CAPICOM является свободно распространяемым, и поставляется в составе Redistributable инструментария разработчика Microsoft Platform SDK.

4.3.2. Certificate Enrollment Control (Windows Server 2003)

COM интерфейс Certificate Enrollment Control (реализован в файле xenroll.dll) предназначен для использования ограниченного количества функций CryptoAPI 2.0, связанных с генерацией ключей, запросов на сертификаты и обработкой сертификатов, полученных от Центра Сертификации с использованием языков программирования Visual Basic, C++, JavaScript, VBScript и среды разработки Delphi.

Этот интерфейс используют различные Центры Сертификации (VeriSign, Thawte и т. д.) при формировании запросов на сертификат пользователей на платформе Windows Server 2003.

4.3.3. Certificate Enrollment API (Windows 2008/7/2008R2/8/2012/8.1/2012R2/10)

Интерфейсы Certificate Enrollment API (реализованные в файле certenroll.dll) предназначены для генерации ключей, запросов на сертификаты, обработки сертификатов, полученных от Центра Сертификации с использованием различных языков программирования.

Этот интерфейс используют различные Центры Сертификации (VeriSign, Thawte и т. д.) при формировании запросов на сертификат пользователей на платформе Windows 2008/7/2008R2/8/2012.

4.3.4. Certificate Services

Certificate Services включает в себя несколько COM интерфейсов, позволяющих изменить функциональность Центра Сертификации, входящего в состав ОС Windows Server. При помощи данных интерфейсов возможно изменение:

– обработки поступающих от пользователей запросов на сертификаты;

– состава данных (в том числе дополнений X.509), записываемых в издаваемые центром сертификаты;

– способа публикации (хранения) изданных центром сертификатов.

4.4. Использование СКЗИ на платформе Microsoft .NET Framework

Компанией ООО «КРИПТО-ПРО» был разработан программный продукт «КриптоПро .NET», позволяющий использовать средство криптографической защиты информации «КриптоПро CSP» v 4.0 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 www.cryptopro.ru.

4.5. Использование СКЗИ в веб-браузерах

«КриптоПро CSP» v 4.0 может быть использовано в веб-браузерах на различных программно-аппаратных платформах путём вызова функций «КриптоПро ЭЦП Browser plug-in», входящего в состав «КриптоПро PKI SDK» (ПАК «Службы УЦ»).

«КриптоПро ЭЦП Browser plug-in» содержит компоненту ActiveX для работы в Microsoft Internet Explorer/Microsoft Edge и плагин NPAPI для других веб-браузеров, поддерживающих данный интерфейс встраивания плагинов. Функции СКЗИ можно вызывать из сценариев JavaScript, содержащихся в отображаемой веб-браузером странице.

Подробная информация доступна странице плагина по адресу http://www.cryptopro.ru/products/cades/plugin.

4.6. 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.

	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;

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

	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.

4.7. Завершение сессии

Корректное завершение сессии осуществляется вызовом функции ApplyControlToken.

4.8. 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.

5. Состав и назначение компонент программного обеспечения СКЗИ

Программное обеспечение СКЗИ «КриптоПро CSP» v 4.0 при функционировании под управлением ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 состоит из следующих компонент:

1. Сервисные модули;
2. Модули настройки встроенной подсистемы программной среды функционирования комплекса (СФК) ОС Windows;
3. Модули сопряжения «КриптоПро CSP» v 4.0 со встроенной подсистемой программной СФК ОС Windows и интерфейс криптографического сервиса;
4. СКЗИ «КриптоПро CSP» v 4.0, реализующее целевые функции криптопровайдера в форме:
   - библиотек, загружаемых в адресное пространство приложения;
   - криптографического сервиса хранения ключей;
   - криптографического драйвера;
   - библиотек протокола «КриптоПро TLS».

5.1. Сервисные модули

Сервисные модули обеспечивают контроль целостности дистрибутива «КриптоПро CSP» v 4.0, его установку и удаление из операционной системы, а также конфигурацию параметров СКЗИ для каждого пользователя.

5.1.1. Модуль контроля целостности дистрибутива

Модуль cpverify.exe, см. Приложение А, предназначен для контроля целостности дистрибутива при установке и использовании ПО СКЗИ «КриптоПро CSP» v 4.0 на компьютере пользователя (поставляется совместно с дистрибутивом).

5.1.2. Дистрибутив

Дистрибутив СКЗИ «КриптоПро CSP» v 4.0 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 csp-win32-kc1-rus.msi разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ «КриптоПро CSP» v 4.0.

5.1.3. Модуль конфигурации

Модуль cpconfig.cpl обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ «КриптоПро CSP» v 4.0, а также содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации.

5.1.4. Модуль Wipefile

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

5.1.5. Модуль контроля целостности в драйвере

Для работы с любым отладчиком модуль контроля целостности в драйвере должен быть отключен. Порядок отключения данного модуля описан в документе «ЖТЯИ.00088-01 96 01. КриптоПро CSP v 4.0. Руководство программиста».

5.2. Модули настройки подсистемы программной СФК ОС Windows

Модули предназначены для обеспечения использования ПО СКЗИ «КриптоПро CSP» v 4.0 в подсистеме программной СФК ОС Windows. Модули также реализуют форматы криптографических сообщений, используемых в защищенной электронной почте (S/MIME), Office 2007/2010, Authenticode и функциях CryptoAPI 2.0, форматы сертификатов и их обработку.

Полный перечень поддерживаемых приложений Microsoft приведен в документе ЖТЯИ.00088-01 90 01. КриптоПро CSP v 4.0. Описание реализации.

Модули настройки классифицируются как подсистема программной СФК и ответственны за использование криптопровайдера «КриптоПро CSP» v 4.0 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.).

5.2.1. 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 СКЗИ «КриптоПро CSP» v 4.0;

– формирование и разбор криптографических сообщений и сертификатов открытых ключей.

5.2.2. Модули инициализации настройки встроенной подсистемы программной СФК ОС Windows

Модуль инициализации для ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 реализован в виде драйвера CProCtrl.sys. Драйвер обеспечивает загрузку определенных динамических библиотек (DLL) в адресное пространство процессов, использующих СКЗИ «КриптоПро CSP» v 4.0.

Дополнительно этот модуль осуществляет контроль целостности установленного ПО «КриптоПро CSP» v 4.0 и подсистемы программной СФК (периодический и при загрузке ОС).

5.2.3. 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» v 4.0.

Настройка заключается в добавлении программной СФК возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером «КриптоПро CSP» v 4.0.

5.2.4. 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» v 4.0, при использовании в ПО Microsoft Outlook и Microsoft Outlook Express.

5.2.5. 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» v 4.0.

5.2.6. 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.

5.2.7. 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» v 4.0.

5.2.8. 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.

5.2.9. 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.

5.2.10. 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» v 4.0.

Модуль cpExSec.dll загружается в виртуальное адресное пространство процесса MS Outlook, и настраивает его для правильной работы с «КриптоПро CSP» v 4.0.

5.2.11. Модуль настройки XML

Модуль cpXML.dll загружается в виртуальное адресное пространство процессов, использующих XML, и позволяет применять алгоритмы «КриптоПро CSP» v 4.0 для подписи XML.

5.2.12. 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» v 4.0.

5.3. Криптопровайдер «КриптоПро CSP» v 4.0

5.3.1. 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.

5.3.2. Интерфейсная библиотека криптографического сервиса

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

5.4. СКЗИ «КриптоПро CSP» v 4.0

Собственно, СКЗИ «КриптоПро CSP» v 4.0 реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, доступ к физическому ДСЧ.

5.4.1. Реализация СКЗИ 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.

5.4.2. Реализация криптопровайдера в форме подгружаемых библиотек

Интерфейс cpcspi.dll реализует целевые функции криптографической защиты информации для Интерфейсной библиотеки криптопровайдера (см. 5.3.1) в варианте функционирования ПО «КриптоПро CSP» v 4.0 без использования Интерфейса криптографического сервиса (см. 5.3.2).

5.4.3. 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» v 4.0 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.

5.4.4. Интерфейсные модули ДСЧ

Обеспечивают реализацию доступа к следующим типам ДСЧ:

- sable.dll ДСЧ электронного замка «Соболь»
- accord.dll ДСЧ АМДЗ «Аккорд»
- apmdz.dll ДСЧ АМДЗ «КРИПТОН-ЗАМОК»
- maxim.dll ДСЧ АПМДЗ «МАКСИМ-М1»

5.4.5. Панель управления ресурсами СКЗИ «КриптоПро CSP» v 4.0

Управление ресурсами СКЗИ «КриптоПро CSP» v 4.0 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 и сертификатами открытых ключей;
- параметрами СКЗИ.

5.5. Модуль аутентификации в домене Windows

Модуль winlogonmgmt.dll обеспечивает аутентификацию на базе электронной подписи с использованием алгоритмов ГОСТ 34.10-2001, ГОСТ 34.11-94.

Модуль аутентификации обеспечивает разграничение доступа к сети домена Windows либо к локальной машине Windows на основе проверки ЭП, выработанной с использованием ключа доступа, расположенного на ключевом носителе пользователя в ключевом контейнере СКЗИ ЖТЯИ.00088-01. Сертификат открытого ключа проверки подписи заносится в системе при регистрации пользователя домена Windows.

5.6. Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки сетевой аутентификации реализуется в форме подгружаемой библиотеки и реализует подмножество интерфейса Microsoft SSPI(SSP/AP) (см. соответствующий 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.

5.7. Подсистема программной СФК «КриптоПро CSP» v 4.0

5.7.1. Интерфейс доступа к ключевым носителям

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

5.7.2. Интерфейсные модули устройств хранения ключевой информации

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

fat12.dll	к дисководу и дискете 3.5"
reg.dll	к системнному реестру и ключам в них
sable.dll	к электронному замку "Соболь"
dallas.dll	к считывателю Touch-memory Dallas
ric.dll	к смарткарте РИК и Оскар
emv.dll	к смарткарте MPCOS EMV/3DES
hs.dll	к электронному ключу eToken
pcsc.dll	к считывателям смарткарт и eToken, поддерживающим интерфейс PC/SC
ds199x.dll	к таблеткам DS1996, DS1995.

5.7.3. Библиотека поддержки доступа к ключевым носителям

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

5.7.4. Модуль ASN1

Поддерживает функции преобразования структур данных в машинно-независимое представление.

5.7.5. Использование ключей реестра Windows

Установка программного обеспечения должна производится 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» v 4.0 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\Crypto Pro\Settings - полный доступ.

Для изменения конфигурации СКЗИ «КриптоПро CSP» v 4.0 с использованием панели управления (Control Panel), кроме того, требуется полный доступ к ключу реестра HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro.

1. По умолчанию «КриптоПро CSP» v 4.0 может использовать до 65536 описателей криптографических объектов. Для увеличения этого значения необходимо добавить в реестр (HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters) параметр DWORD, равный требуемому числу описателей, но не более 1048576.
2. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00088-01 91 01. Руководство администратора безопасности общая часть).

6. Криптографический интерфейс CryptoAPI 2.0

СКЗИ может быть использовано прикладным программным обеспечением (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0 (описание – в документации MSDN - Microsoft Developer Network). В этом случае способ выбора криптографического алгоритма в прикладном программном обеспечении может определяться информацией, содержащейся в сертификатах открытых ключей X.509.

Криптографический интерфейс CryptoAPI 2.0 позволяет:

1. Обеспечить прикладному уровню доступ к криптографическим функциям для генерации ключей, формирования/проверки электронной цифровой подписи, шифрования/расшифрования данных в условиях изолирования прикладного уровня от уровня реализаций криптографических функций. Приложениям и прикладным программистам не нужно детально вникать в особенности реализации того или иного алгоритма или изменять в зависимости от алгоритма прикладные программы.
2. Обеспечить одновременное использование разных алгоритмов и различных их реализаций как программных, так и аппаратных.

Общая архитектура криптографических функций показана на Рисунке 6.1.

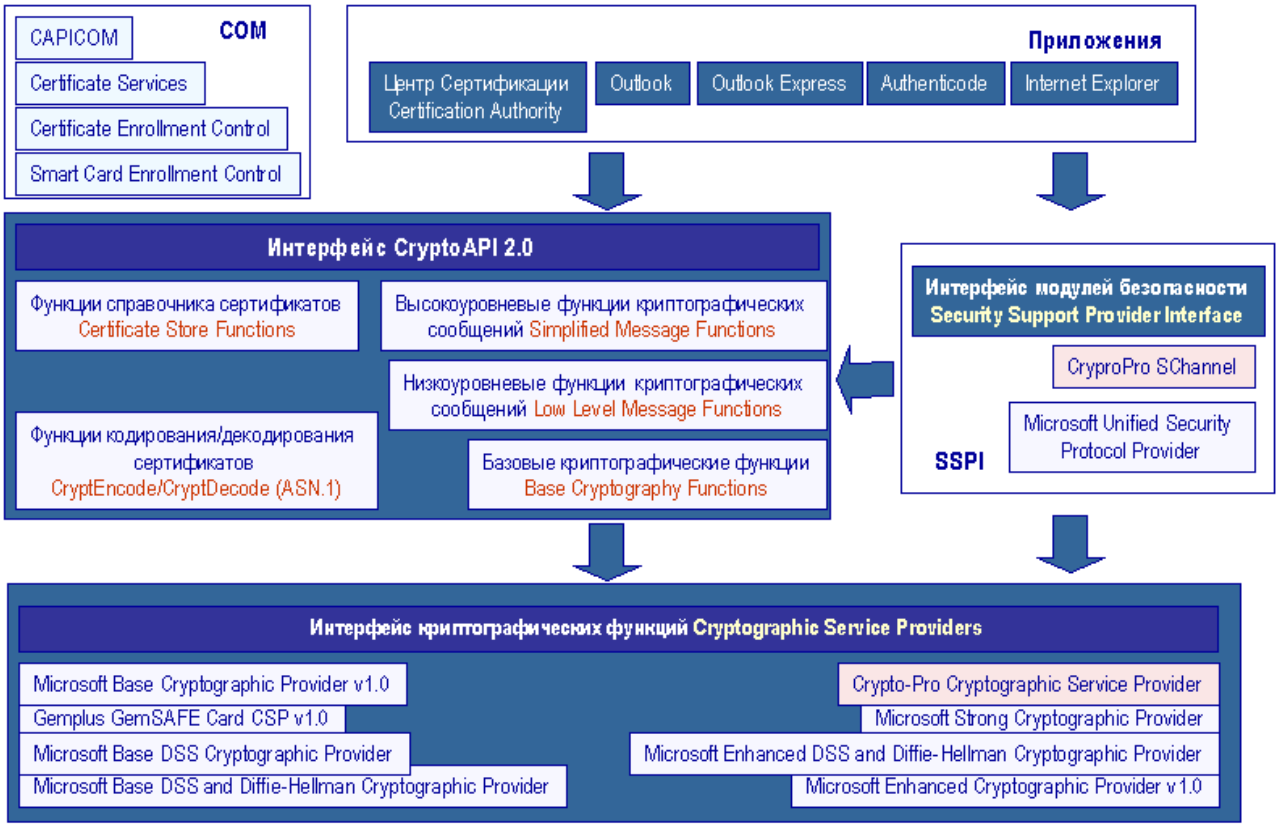

Рисунок 6.1 - Архитектура криптографических функций в ОС Windows

Общая архитектура CryptoAPI 2.0 представлена пятью основными функциональными группами:

1. Базовые криптографические функции:

– функции инициализации (работы с контекстом). Эти функции предоставляют приложению возможность выбрать определенный криптопровайдер по типу имени или по требуемой функциональности;

– функции генерации ключей. Эти функции предназначены для формирования и хранения криптографических ключей различных типов;

– функции обмена ключами. Эти функции предназначены для того, чтобы приложения могли обмениваться различными типами ключевой информации для обеспечения взаимодействия между собой;

2. Функции кодирования/декодирования.

Данные функции предназначены для преобразования (кодирования) из внутреннего представления объектов, используемых в CryptoAPI, во внешнее представление и обратно. В качестве внешнего представления объектов используется формат ASN.1 (Abstract Syntax Notation One), определенный серией рекомендаций X.680. К этой же группе функций относится набор функций, позволяющих расширить функциональность CryptoAPI путем реализации и регистрации собственных типов объектов;

3. Функции работы со справочниками сертификатов.

Эта группа функций предназначена для хранения и обработки сертификатов в различных типах справочников. Причем в качестве справочника могут использоваться самые различные типы хранилищ: от простого файла до LDAP;

4. Высокоуровневые функции обработки криптографических сообщений.

Эта группа функций (Simplified Message Functions) в первую очередь предназначена для использования в прикладном ПО. С помощью этих функций можно

– Зашифровать/расшифровать сообщение от одного пользователя к другому;

– Подписать данные;

– Проверить подпись данных.

Эти функции (также, как и функции низкого уровня) оперируют сертификатами открытых ключей X.509 для адресации отправителя/получателя данных. В качестве формата данных, формируемых функциями, используется формат PKCS#7 (RFC 2315) или CMS (RFC 2630).

5. Низкоуровневые функции обработки криптографических сообщений.

Данная группа функций (Low Level Message Functions) предназначена для аналогичных целей, что и группа высокоуровневых функций, но обладает большей функциональностью и требует от прикладного программиста более детальных знаний в области прикладной криптографии.

7. Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ «КриптоПро CSP» v 4.0 в прикладное программное обеспечение должны выполняться требования раздела 17 документа «ЖТЯИ.00088-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» и документа «ЖТЯИ.00088-01 96 01. КриптоПро CSP. Руководство программиста».

8. Особенности работы 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»). Работа СКЗИ при отключённом режиме допускается исключительно в тестовых целях.

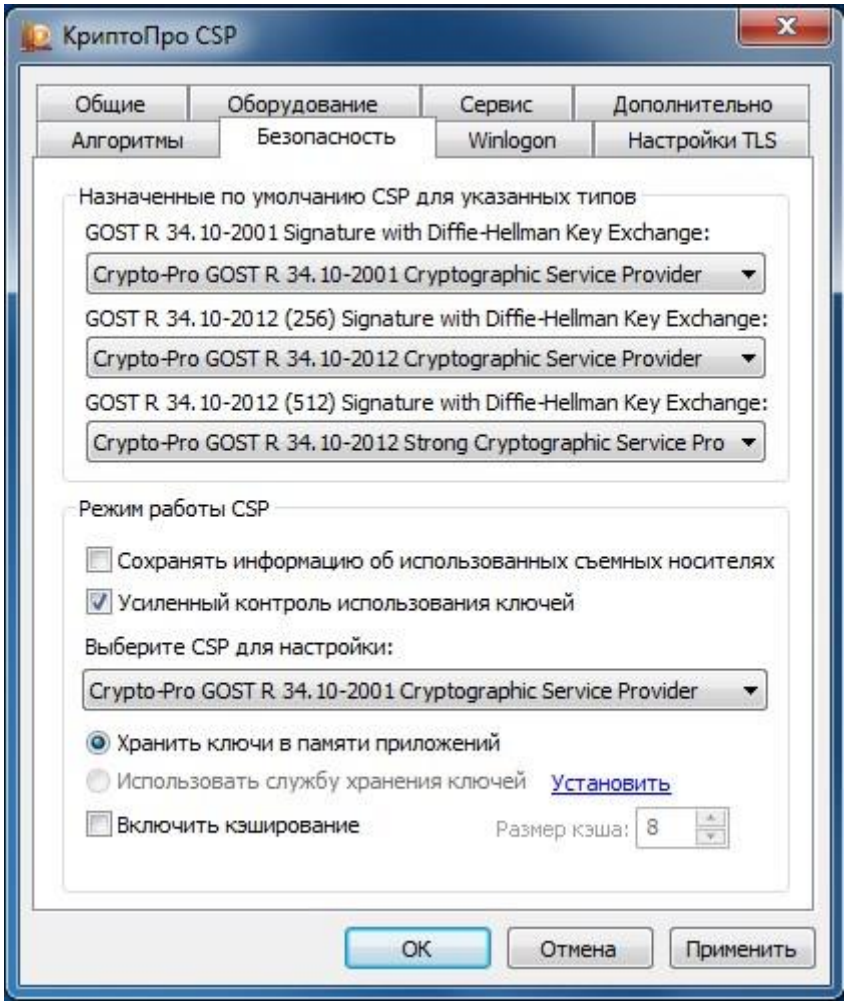

Рисунок 8.1. - Включение режима усиленного контроля использования ключей в контрольной панели КриптоПро CSP.

Проверить, включён ли режим усиленного контроля использования ключей, можно в контрольной панели КриптоПро CSP (вкладка «Безопасность»), либо просмотрев значение ключа StrengthenedKeyUsageControl в ветке реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\StrengthenedKeyUsageControl (для 64-разрядной операционной системы),

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\StrengthenedKeyUsageControl (для 32-разрядной операционной системы).

В случае, если включение режима усиленного контроля использования ключей производилось не на этапе инсталляции СКЗИ (через контрольную панель, редактор групповой политики 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. рисунок 8.2), необходимо выполнить команду:

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

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

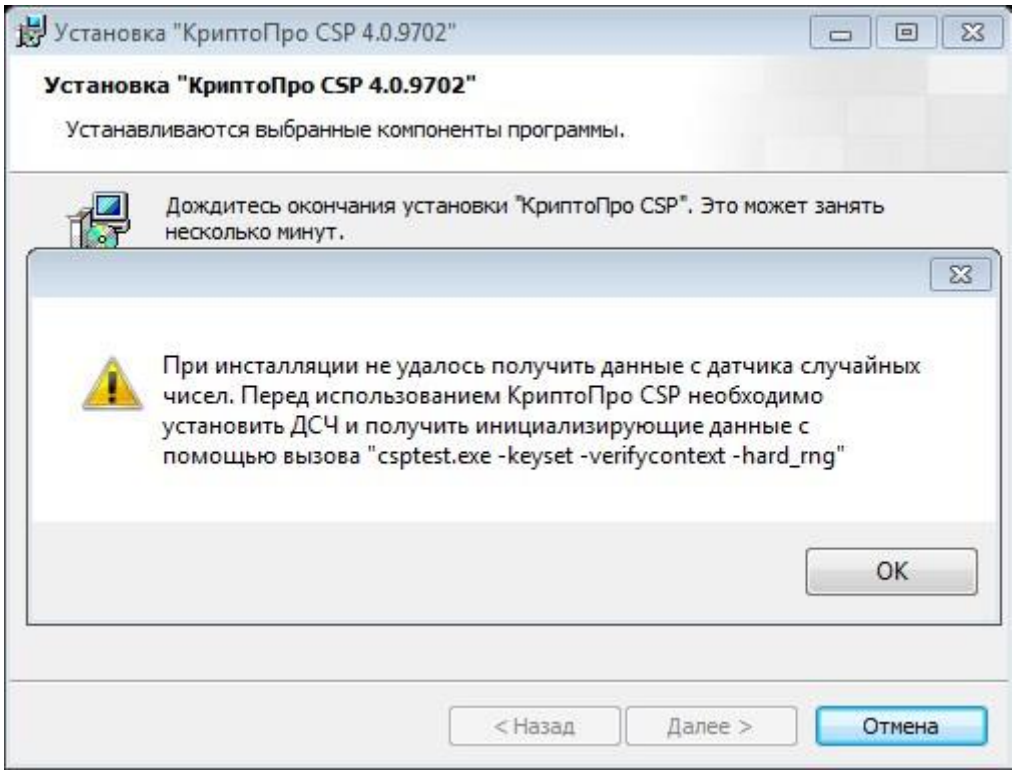

Рисунок 8.2. – Ошибка получения данных с датчика случайных чисел при инсталляции СКЗИ

В криптопровайдере «КриптоПро CSP» v 4.0 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» v 4.0. 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
```

Внимание! 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
```

9. Требования по организационно-техническим и административным мерам обеспечения эксплуатации СКЗИ

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме разделов 15 и 16 документа «ЖТЯИ.00088-01 91 01. КриптоПро CSP v 4.0. Руководство администратора безопасности. Общая часть».

При подключении СКЗИ к общедоступным каналам передачи данных должна быть обеспечена безопасность защищенной связи. При этом должны быть определены:

- Порядок подключения СКЗИ к каналам.
- Выделено лицо, ответственное за безопасность работы по общедоступным каналам.
- Разработан типовой регламент защищенной связи, включающий:
  - политику безопасности защищенной связи;
  - допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных;
  - перечень допустимых сетевых протоколов;
  - защиту сетевых соединений (перечень допустимых сетевых экранов);
  - система и средства антивирусной защиты.

Порядок подключения СКЗИ к каналам связи должен быть определен эксплуатирующей организацией.

Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам, как правило, должен быть администратор безопасности.

Перечень штатных средств ОС, может включаться администратором в типовой регламент без проведения дополнительных исследований по оценке их влияния на СКЗИ. При этом должны выполняться:

1. своевременное обновление программных средств, включенных в состав регламента;
2. контроль среды функционирования СКЗИ;
3. определение и контроль за использованием сетевых протоколов;
4. соблюдение правил пользования СКЗИ и средой функционирования СКЗИ.

При использовании СКЗИ с другими стандартными программными средствами возможность подключения СКЗИ к общедоступным каналам передачи данных должна быть определена только после проведения дополнительных исследований с оценкой невозможности негативного влияния нарушителя на функционирование СКЗИ, использующего возможности общедоступных каналов.

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.

10. Требования по защите от НСД

СКЗИ «КриптоПро CSP» v 4.0 КС2 (класс защиты КС2) при условии выполнения требований настоящего Руководства, а также выполнения требований п.15 «ЖТЯИ.00088-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» обеспечивает защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

Запрещается использование СКЗИ «КриптоПро CSP» v 4.0 в случае обнаружения отказа оборудования либо программного обеспечения ПАК защиты от НСД.

10.1. Организационно-технические меры защиты от НСД

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 2003/2008/7/2008R2/8/2012/8.1/2012R2/10, 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 месяц, доступ к паролю должен быть обеспечен только пользователю, обладающему правами администратора.
3. Всем пользователям, зарегистрированным в ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10, администратор в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10, 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 2003/2008/7/2008R2/8/2012/8.1/2012R2/10. Не используются нестандартные, измененные или отладочные версии ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 такие, например, как 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.

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 2003/2008/7/2008R2/8/2012/8.1/2012R2/10.

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 вирусов.

22. Должны быть удалены все общие ресурсы на ПЭВМ с установленным СКЗИ «КриптоПро CSP» v 4.0 (в том числе и создаваемые по умолчанию при установке ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10), 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 Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10, 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» v 4.0.

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. Должны использоваться система аудита в соответствие с политикой безопасности, принятой в организации, и организован регулярный анализ результатов аудита.

32. Должен проводиться регулярный просмотр сообщений в журнале событий Event viewer.

33. ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 должна быть настроена на завершение работы при переполнении журнала аудита.

34. Должна быть обеспечена невозможность модификации ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 через общедоступные каналы передачи данных.

35. После инсталляции ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 должен быть установлен последний официальный Service Pack от фирмы Microsoft, существующий на момент установки ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10.

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.

10.2. Настройка системного реестра ОС Windows при установке СКЗИ

На ПЭВМ с ОС Windows 2003/2008/7/2008R2/8/2012/8.1/2012R2/10 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 (ОС Windows XP) в ключе HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters установить параметр EnablePlainTextPassword (REG_DWORD) со значением «0».

10.3. Использование СКЗИ со стандартными программными средствами СФК

Программное обеспечение СКЗИ ЖТЯИ.00088-01 позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 с различным программным обеспечением Microsoft:

– Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server, Windows 2012 Server, Windows 2012R2 Server.

– Электронная почта - MS Outlook (Office 2016, Office 2013, Office 2010, Office 2007, Office 2003, Office XP, Office 2000).

– Электронная почта - Microsoft Outlook Express в составе Internet Explorer/Microsoft Edge.

– Microsoft Word, Excel, Info Path из состава Microsoft Office 2003, 2007, 2010, 2013, 2016.

– Microsoft Exchange Server 2010, 2013.

– Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.

– Службы терминалов для Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server, Windows 2012 Server, Windows 2012R2 Server (включая шлюз служб терминалов).

– Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer/Microsoft Edge – web-сервер IIS, TLS-сервер, TLS-клиент (IE).

– SQL-сервер.

– ISA/TMG сервер.

– Сервер терминалов и клиент (RDP).

– Средства функционирования комплекса разработки ООО «КРИПТО-ПРО» Крипто-Про УЦ, КриптоПро OCSP, КриптоПро TSP, КриптоАРМ, CryptCP, Клиент КриптоПро HSM.

10.4. Требования по организации СКЗИ сетевого подключения к корпоративным сетям и сетям общего доступа.

При подключении СКЗИ к общедоступным каналам передачи данных должна быть обеспечена безопасность защищенной связи. При этом должны быть определены:

– Порядок подключения СКЗИ к каналам.

– Выделено лицо, ответственное за безопасность работы по общедоступным каналам.

– Разработан типовой регламент защищенной связи, включающий:

- политику безопасности защищенной связи;
- допустимый состав прикладных программных средств, для которого должно быть исследовано и обосновано отсутствие негативного влияния на СКЗИ по каналу передачи данных;
- перечень допустимых сетевых протоколов;
- защиту сетевых соединений (перечень допустимых сетевых экранов);
- система и средства антивирусной защиты;

Порядок подключения СКЗИ к каналам связи должен быть определен эксплуатирующей организацией.

Лицом, ответственным за безопасность работы СКЗИ по общедоступным каналам, как правило, должен быть администратор безопасности.

Перечень штатных средств ОС, может включаться администратором в типовой регламент без проведения дополнительных исследований по оценке их влияния на СКЗИ. При этом должны выполняться:

– своевременное обновление программных средств, включенных в состав регламента;

– контроль среды функционирования СКЗИ;

– определение и контроль за использованием сетевых протоколов;

– соблюдение правил пользования СКЗИ и средой функционирования СКЗИ.

При использовании СКЗИ с другими стандартными программными средствами возможность подключения СКЗИ к общедоступным каналам передачи данных должна быть определена только после проведения дополнительных исследований с оценкой невозможности негативного влияния нарушителя на функционирование СКЗИ, использующего возможности общедоступных каналов.

11. Требования по криптографической защите

Должны выполняться требования по криптографической защите разделов 15 и 16 и документа «ЖТЯИ.00088-01 91 01. Руководство администратора безопасности. Общая часть» в части, касающейся ОС Windows.

Перед началом работы должен быть проведен контроль целостности.

Контролем целостности должны быть охвачены 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\cpcspr.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\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)\Crypto Pro\CSP\cpcspr.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\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
\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\cpcspr.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 если целостность данных библиотек нарушена в результате обновления операционной системы, необходимо обратиться к разработчику СКЗИ за разъяснениями о возможности продолжения использования СКЗИ на данной системе.

Приложение А. Контроль целостности программного обеспечения

А.1 Контроль целостности программного обеспечения с помощью алгоритмов хэширования.

Модуль cpverify.exe позволяет осуществлять контроль целостности установленного программного обеспечения. Контроль целостности файлов осуществляется при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности (см. опцию –rv ниже).

При помощи перечисленных ниже опций модуль cpverify.exe может быть использован для следующих контрольных целей:

cpverify -mk filename [-alg algid] [-inverted_halfbytes <inv>]– вычисление значения хэш-функции для файла с именем filename с помощью алгоритма algid. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411). [-inverted_halfbytes <inv>] указывается, если полубайты в hashvalue перевернуты (по умолчанию для GR3411 inv принимается равным «1», для алгоритмов GR3411_2012_256 и GR3411_2012_512 «0»).

cpverify filename [-alg algid] [hashvalue] [-inverted_halfbytes <inv>] – проверка целостности файла с именем filename, используя алгоритм algid и хэш-значение hashvalue. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411). Если hashvalue не указан, то хэш-значение берется из файла filename.hsh. [-inverted_halfbytes <inv>] указывается, если полубайты в hashvalue перевернуты (по умолчанию для GR3411 inv принимается равным «1», для алгоритмов GR3411_2012_256 и GR3411_2012_512 «0»).

cpverify -rm [-alg algid] [catname] - вычисление значения хэш-функции для каждого из файлов, содержащихся в каталоге catname в разделе реестра (если catname не указан, то будут пересчитаны все хэш-значения в разделе реестра). Текущее значение хэш-функций при этом заменяется на вновь посчитанное. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411).

cpverify –rv [catname] - проверка целостности файлов из каталога catname в разделе реестра (если catname не указан, то будут проверены все файлы в разделе реестра).

cpverify -xm in_file out_file [-alg algid] [xmlcatname]- вычисление значения хэш-функции для файлов, перечисленных в xml-файле с именем in_file в каталоге xmlcatname (если xmlcatname не указан, то хэш-значения будут посчитаны для всех фалов, перечисленных в xml-файле с именем in_file), и запись полученных значений в xml-файл с именем out_file. Текущее значение хэш-функций при этом заменяется на вновь посчитанное. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411).

cpverify –xv in_file [xmlcatname] - проверка целостности файлов, перечисленных в xml-файле с именем in_file в каталоге xmlcatname (если xmlcatname не указан, то проверка будет выполнена для всех фалов, перечисленных в xml-файле с именем in_file).

cpverify –r2x out_file - формирование xml-файла с именем out_file, содержащего список файлов, находящихся в разделе реестра под контролем целостности, и хэш-значения этих файлов.

cpverify –x2r in_file - установка под контроль целостности файлов, перечисленных в xml-файле с именем in_file.

Список контролируемых модулей зависит от исполнения и может быть получен при помощи команды cpverify –r2x in_file.

Во всех перечисленных выше случаях, если не указано имя каталога xmlcatname, то принимается имя каталога cpcsp, используемое csp для контроля целостности входящих в его состав модулей. Список контролируемых модулей зависит от исполнения и может быть получен при помощи команды cpverify –r2x in_file cpcsp.

Для того, чтобы поставить под контроль целостности установленное программное обеспечение, нужно выполнить следующую последовательность действий:

1. Создать xml-файл, содержащий список устанавливаемых под контроль целостности файлов. Данный xml-файл должен иметь следующую структуру:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CProIntegrity>
<catalog>
<entry name="calc.exe">
<Path>C:\WINDOWS\system32\calc.exe</Path>
<Algid>00008021</Algid>
</entry>
<entry name="verifier.exe">
<Path>C:\WINDOWS\system32\verifier.exe</Path>
<Algid>00008021</Algid>
</entry>
</catalog>
</CProIntegrity>
```

Значение поля Algid должно равняться 00008021.

2. Запустить модуль cpverify –xm in_file out_file TestControl, указав в качестве параметра in_file имя созданного xml-файла. Результатом работы модуля будет являться xml-файл с именем out_file, содержащий вычисленные значения хэш-функции для перечисленных в in_file файлов и имеющий следующую структуру:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CProIntegrity>
<catalog>
<entry name="calc.exe">
<Path>C:\WINDOWS\system32\calc.exe</Path>
<Algid>00008021</Algid>
<Tag>679837307CDC7AA1E4BDBB75194A24D42C782079AF08E2D362D7624A90D
604C7</Tag>
</entry>
<entry name="verifier.exe">
<Path>C:\WINDOWS\system32\verifier.exe</Path>
<Algid>00008021</Algid>
<Tag>9DF987B89A323BEBC3C29BAC0AED42A4F5BD651892AAE79F1EC1D05288D
06B9C</Tag>
</entry>
</catalog>
</CProIntegrity>
```

Значение поля Algid должно равняться 00008021.

3. Установить под контроль целостности файлы, для которых было вычислено значение хэш-функции, используя модуль cpverify –x2r in_file TestControl, где параметром in_file является xml-файл, полученный в результате вычисления значения хэш-функции в пункте 2.

После обновления Windows возможно возникновение ошибки при проверке хэш-значений системных библиотек, используемых СКЗИ. Это будет отражено в системном журнале,

куда по умолчанию записывается информация о результате проведения контроля целостности. В этом случае необходимо:

- уведомить разработчика о несоответствии хэш-значений системных библиотек с целью постановки работ по проведению анализа обновленных системных библиотек, используемых СКЗИ установленным порядком;
- на период до получения результатов исследований следовать инструкциям разработчика, полученным им из специализированной организации.

Для уровня защиты КС2 необходимо включить усиленный режим работы контроля целостности, который блокирует работу СКЗИ в случае возникновения указанной ошибки. Для этого необходимо добавить в реестр (\\REGISTRY\\MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\CProIntegrity) параметр HaltFileCorrupt отличный от нуля.

Для уровня защиты КС1 при получении разрешения от разработчика допускается обновить значения хэш-функций для данных библиотек с помощью команды

cpverify –mksystem.

A.2 Контроль целостности программного обеспечения с помощью алгоритмов подписи

– cpverify -file_verify имя_файла [значение_подписи] -timestamp дата

Проверка подписи файла с именем «имя_файла». Параметр «значение_подписи» необходимо передавать в виде байтовой строки. Если параметр «значение_подписи» не указан, то значение подписи берется из файла имя_файла.sgn. Параметр «дата» указывает, когда подпись была сформирована, необходимо указывать в формате дд.мм.гггг. Данная команда проверяет подпись с прямой последовательностью полубайт, для проверки подписи с обратной последовательностью байт необходимо использовать команду versign с аналогичным набором параметров. Подпись проверяется на открытом ключе из специального сертификата для подписи кода компании «КРИПТО-ПРО».

– cpverify –pe_sign FileName [критерии поиска сертификата] [доп. параметры]

Добавление в файл с именем FileName цифровой подписи в формате authenticode полностью на российских алгоритмах с помощью Microsoft CryptoAPI. С помощью данной команды можно подписать только файлы форматов .exe и .dll.

Для того чтобы подписать файл, необходимо в хранилище «Личное» текущего пользователя иметь установленный сертификат со ссылкой на закрытый ключ, в назначениях которого присутствует «Подписывание кода».

Поиск нужного сертификата осуществляется с помощью следующих критериев:

-name *SubjectName*	Имя субъекта сертификата подписи. Это значение может быть подстрокой полного имени субъекта.
-alg *AlgId*	Алгоритм хэширования для подписи в сертификате. Допустимые значения *GR3411*, *GR3411_2012_256*, *GR3411_2012_512*.
-fp *FingerPrint*	Значение sha1 отпечатка сертификата.
-append	Подпись будет добавлена как второстепенная. Если в файле нет основной подписи или параметр **–append** не передан, то подпись будет добавлена как основная.

Если несколько сертификатов удовлетворяют заданным критериям, то пользователю будет предоставлена возможность вручную выбрать нужный сертификат.

– cpverify –pe_verify FileName [доп. параметры]

Проверка authenticode подписи файла с именем FileName без использования Microsoft CryptoAPI.

-multiple	Проверка всех authenticode подписей, найденных в файле. Если параметр не передан, то будет проверена только основная подпись.

Приложение Б. 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 2000/2003 полностью поддерживает и позволяет создать иерархическую модель центров сертификации.

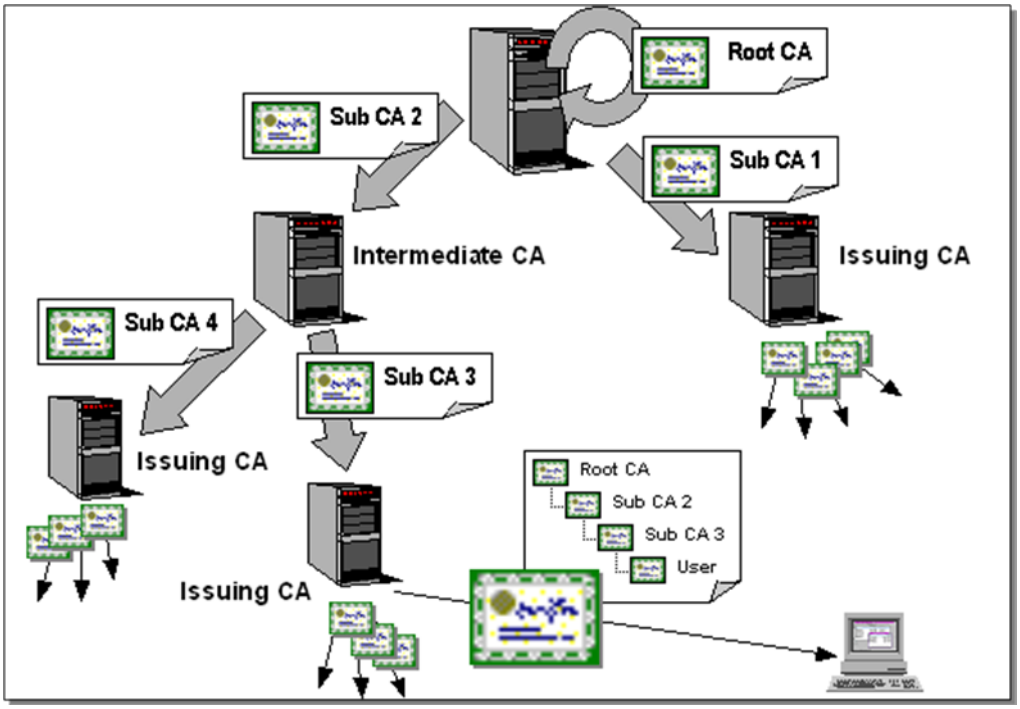

Рисунок Б1- Модель построения центров сертификации

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.

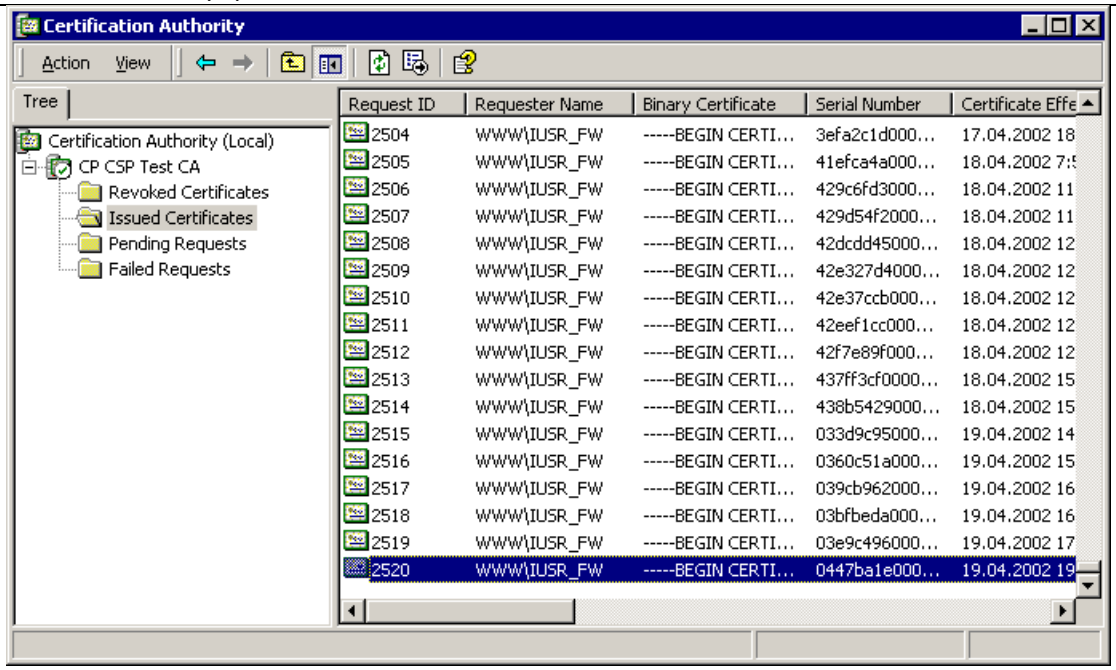

Рисунок Б2 – Консоль центра сертификации

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 сервиса 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 Рисунке Б3.

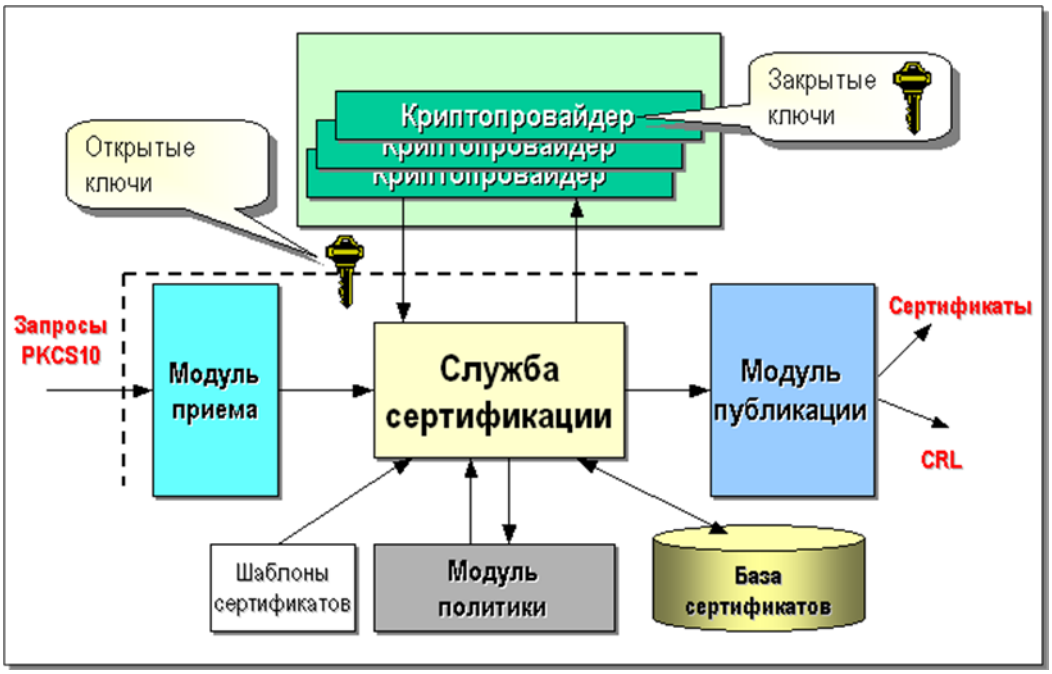

Рисунок Б3 – Архитектура сервиса сертификации.

Приложение В. Управление протоколированием

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

HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node]Crypto Pro\Cryptography\CurrentVersion\debug\

DWORD параметр cpcsp для определения уровня протокола

DWORD параметр cpcsp_fmt для определения формата протокола

Значением параметра уровень протокола является битовая маска:

N_DB_ERROR = 1 # сообщения об ошибках
N_DB_LOG = 8 # сообщения о вызовах

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 № сопроводи-тельного документа, дата	Подпись	Дата
	измененных	замененных	новых	аннулиро-ванных					