127 018, Москва, Сущевский Вал, д.18
Телефон: (495) 9954820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

УТВЕРЖДЕНЫ

ЖТЯИ.00088-03 95 01-ЛУ

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 4.0 R4 КС2

2-Base

Правила пользования

ЖТЯИ.00088-03 95 01
Листов 50

2018 г.

Содержание

1. Аннотация

Данный документ содержит правила пользования средства криптографической защиты информации (СКЗИ) «КриптоПро CSP» версия 4.0 R4, его состав, назначение, ключевую систему, требования по защите от НСД.

Документ предназначен для администраторов информационной безопасности учреждений, осуществляющих установку, обслуживание контроль за соблюдением требований к эксплуатации средств СКЗИ, а также администраторам Серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющим настройку рабочих мест для работы со средствами СКЗИ.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 4.0 R4 должны разрабатываться с учетом требований настоящих Правил.

2. Назначение СКЗИ. Условия эксплуатации

СКЗИ «КриптоПро CSP» версия 4.0 R4 предназначено для защиты открытой информации в информационных системах общего пользования (вычисление и проверка ЭП) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах (шифрование и расшифрование информации, вычисление и проверка имитовставки, вычисление значения хэш-функции, вычисление и проверка ЭП).

При эксплуатации СКЗИ «КриптоПро CSP» версия 4.0 R4 должны выполняться следующие требования:

– Средствами СКЗИ не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

– Допускается использование СКЗИ для криптографической защиты персональных данных.

– Ключевая информация является конфиденциальной.

– Срок действия ключа проверки ЭП – не более 15 лет после окончания срока действия соответствующего ключа ЭП.

– Внешняя гамма, используемая для инициализации состояния программного ДСЧ, является конфиденциальной.

– СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. В случае их отсутствия рекомендуется по возможности использовать существующие антивирусные средства защиты. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

– Размещение СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется установленным порядком.

– ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ.

– Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

– Встраивание СКЗИ в другие средства возможно только с использованием функций, указанных в Приложении 2. В случае использования прочих вызовов функций программных интерфейсов (уровней встраивания) СКЗИ необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

– При эксплуатации СКЗИ должны использоваться только сертификаты открытых ключей, выпущенные доверенным органом сертификации. В качестве такого органа должен выступать сертифицированный ФСБ России Удостоверяющий центр (УЦ), выпускающий сертификаты и поддерживающий списки отозванных сертификатов в соответствии с Регламентом УЦ, а также служба

корпоративной системы, обеспечивающая доверенные справочники сертификатов открытых ключей с поддержкой актуальности включаемых в справочники сертификатов.

Порядок организации и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации сведений, составляющих конфиденциальную информацию, осуществляется в соответствии с документами «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (Приказ ФАПСИ № 152 от 13 июня 2001 года), «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Приказ ФСБ России № 66 от 9 февраля 2005 года) и другими руководящими документами по обеспечению безопасности информации.

СКЗИ «КриптоПро CSP» версии 4.0 R4 можно эксплуатировать со следующими программными продуктами без проведения дополнительных тематических исследований и/или оценки влияния:

- приложения, входящие в состав ОС;
- приложение командной строки для формирования запроса на сертификат certreq;
- MS Outlook (Office 2003, Office 2007, Office 2010, Office 2013, Office 2016);
- сервер IIS;

Следующие программные компоненты СКЗИ «КриптоПро CSP» версии 4.0 R4 можно использовать без проведения дополнительных тематических исследований:

- приложение командной строки для подписи и шифрования файлов cryptcp;
- приложение командной строки для работы с сертификатами certmgr;
- приложение для создания TLS-туннеля stunnel.

Использование СКЗИ «КриптоПро CSP» версии 4.0 R4 с выключенным режимом усиленного контроля использования ключей не допускается. Включение данного режима описано в документах ЖТЯИ.00088-03 91 02. Руководство администратора безопасности. Windows, ЖТЯИ.00088-03 91 03. Руководство администратора безопасности. Linux, ЖТЯИ.00088-03 91 04. Руководство администратора безопасности. FreeBSD, ЖТЯИ.00088-03 91 05. Руководство администратора безопасности. Solaris, ЖТЯИ.00088-03 91 06. Руководство администратора безопасности. AIX.

3. Порядок распространения СКЗИ

Установочные модули СКЗИ «КриптоПро CSP» v 4.0 R4 и комплект эксплуатационной документации к нему могут поставляться пользователю Уполномоченной организацией двумя способами:

1. На носителе (CD, DVD - диски);

2. Посредством загрузки через Интернет.

Для получения возможности загрузки установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации пользователь направляет свои учетные данные Уполномоченной организации. Учетные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

После получения Уполномоченной организацией учетных данных пользователю предоставляется доступ на страницу загрузки установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации. При загрузке пользователем установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и комплекта эксплуатационной документации Уполномоченной организацией присваивается учетный номер, идентифицирующий экземпляр СКЗИ «КриптоПро CSP» v 4.0 R4, предоставленный пользователю.

На странице загрузки вместе с дистрибутивом и документацией размещается отделенная электронная подпись, для проверки которой необходимо использовать утилиту cpverify, полученную доверенным образом и содержащую ключ проверки данной электронной подписи.

Установка СКЗИ «КриптоПро CSP» v 4.0 R4 на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей СКЗИ «КриптоПро CSP» v 4.0 R4 и эксплуатационной документации.

1. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной.

2. Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

4. Основные технические данные и характеристики

4.1. Программно-аппаратные среды функционирования СКЗИ

Windows

Включает программно-аппаратные среды:

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

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

CentOS 4/5/6 (x86, x64);
CentOS 7 (x86, x64, POWER, ARM, ARM64);
ОСь (OS-RT) (x64);
ТД ОС АИС ФССП России (GosLinux) (x86, x64);
Red OS (x86, x64);
Fedora 27/28/29 (x86, x64, ARM);
Oracle Linux 4/5/6 (x86, x64);
Oracle Linux 7 (x64);
OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
AlterOS (x64);
SUSE Linux Enterprise Server 11SP4 (x86, x64);
SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64);
Red Hat Enterprise Linux 4/5/6 (x86, x64);
Red Hat Enterprise Linux 7 (x64, POWER, ARM64);
Синтез-ОС.РС (x86, x64);
КП «ЗОС «СинтезМ» в роли «Графический клиент» (x64);
КП «ОС «СинтезМ-К» в роли «Графический клиент» (x64);
Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);
Ubuntu 18.04/18.10 (x86, x64);
Linux Mint 17/18/19 (x86, x64);
Debian 7/8/9 (x86, x64, POWER, ARM, ARM64);
ОС Лотос (x86, x64);
Astra Linux Special Edition, Common Edition (x64, Эльбрус);
МСВСфера 6.3 Сервер (x64, ARM64).

Unix

Включает программно-аппаратные среды:

ОС Эльбрус версия 3 (Эльбрус);
ALT Linux 6/7 (x86, x64, ARM);
Альт Сервер 8, Альт 8 СП Сервер (x86, x64, ARM, ARM64);

Альт Рабочая станция 8, Альт Рабочая станция К 8, Альт 8 СП Рабочая станция (x86, x64, ARM, ARM64);

ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);

РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);

FreeBSD 11, pfSense 2.x (x86, x64);

AIX 6/7 (POWER).

Solaris

Включает программно-аппаратные среды:

Solaris 10 (sparc, x86, x64);

Solaris 11 (sparc, x64).

Примечания:

1. Версия POSReady.

4.2. Ключевая система и ключевые носители

СКЗИ «КриптоПро CSP» v 4.0 R4 является системой с открытым распределением ключей на основе асимметричной криптографии с использованием закрытого ключа на одной стороне и соответствующего ему открытого ключа информационного взаимодействия на другой стороне.

Пользователь включается в систему и исключается из неё установленным Удостоверяющим центром порядком.

Пользователь, обладающий правом подписи и/или шифрования данных, вырабатывает на своем рабочем месте или получает у администратора безопасности (в зависимости от принятой политики безопасности) личные закрытый ключ (ключ ЭП) и открытый ключ (ключ проверки ЭП). На основе каждого открытого ключа (ключа проверки ЭП) Удостоверяющим Центром формируется сертификат открытого ключа (сертификат ключа проверки ЭП).

4.2.1. Ключевой носитель

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 Rutoken S;
- Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC;
- Рутокен S;
- Novacard;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- Смарткарта УЭК;
- Смарткарта MS_KEY K;
- Токен++ Lite;
- 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.00088-03 30 01. КриптоПро CSP. Формуляр, п. 3.8.

	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 используютсядолжны использоваться 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.

4.2.2. Размеры и сроки действия ключей

Длины ключей электронной подписи:

ключ электронной подписи	256 или 512 бит;
ключ проверки электронной подписи	512 или 1024 бит.

Длины ключей, используемых при шифровании:

закрытый ключ	256 бит или 512 бит;
открытый ключ	512 бит или 1024 бита;
симметричный ключ	256 бит.

При эксплуатации СКЗИ «КриптоПро CSP» v 4.0 R4 должны соблюдаться следующие сроки использования пользовательских закрытых ключей и сертификатов:

- максимальный срок действия закрытого ключа ЭП-256 (ключа ЭП) - 1 год 3 месяца;
- максимальный срок действия закрытого ключа ЭП-512 (ключа ЭП) - 1 год 3 месяца;
- максимальный срок действия открытого ключа ЭП-256 (ключа проверки ЭП) - 15 лет;
- максимальный срок действия открытого ключа ЭП-512 (ключа проверки ЭП) - 15 лет;
- максимальный срок действия закрытых и открытых ключей обмена – 1 год 3 месяца.

При формировании закрытого ключа в контейнер записывается дата истечения срока действия этого ключа, по истечении которого в зависимости от значения параметра ControlKeyTimeValidity возможны различные варианты использования этого ключа.

Значение «0» параметра не накладывает никаких ограничений на использование ключа.

Значение «1» параметра запрещает формирование ЭП и шифрование в контексте этого ключа (возможно расшифрование ранее зашифрованных сообщений) (значение по умолчанию);

Значение «2» параметра запрещает любые действия с закрытым ключом.

Срок действия ключа берется из (в порядке уменьшения приоритета):

- Расширения контейнера ключа;
- Расширения сертификата ключа;
- Даты создания ключа + 1 год 3 месяца.

Изменение параметра ControlKeyTimeValidity

Для операционных систем группы Windows необходимо изменить значение ключа реестра

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 64-битных операционных систем),

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\ControlKeyTimeValidity (для 32-битных операционных систем).

Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig с помощью команды

./cpconfig -ini \config\parameters -add long ControlKeyTimeValidity <значение>

4.2.3. Хранение ключевых носителей

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

Запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации.

В случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

При хранении ключей в реестре Windows и на HDD ПЭВМ требования по хранению личных ключевых носителей распространяются на ПЭВМ (HDD ПЭВМ) (в том числе и после удаления ключей из реестра, из HDD).

В случае невозможности отчуждения ключевого носителя с ключевой информацией от ПЭВМ организационно-техническими мероприятиями должен быть исключен доступ нарушителей к ПЭВМ с ключами.

Пользователь, имеющий действующий сертификат и соответствующий ему ключ ЭП, в любой момент времени (но не позднее недели) до окончания срока действия действующего закрытого ключа, может произвести формирование нового ключа ЭП.

Формирование нового ключа ЭП, запроса на сертификат, передача запроса в ЦР и получение сертификата производится согласно последовательности, описанной в разделе 8.5 «Формирование ключей пользователя».

Ключевые носители с ключом ЭП, срок действия которого истек, уничтожаются путем переформатирования (очистки), о чем делается запись в «Журнале пользователя сети».

К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

– Потеря ключевых носителей.

– Потеря ключевых носителей с их последующим обнаружением.

– Увольнение сотрудников, имевших доступ к ключевой информации.

– Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.

– Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

– Нарушение печати на сейфе с ключевыми носителями.

Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника)

Различаются два вида компрометации закрытого ключа: **явная** и **неявная**. Первые четыре события трактуются как явная компрометация ключей. Следующие три требуют специального рассмотрения в каждом конкретном случае.

При компрометации ключа у пользователя он должен немедленно прекратить связь по сети с другими пользователями.

Пользователь (или администратор безопасности организации) должен немедленно известить ЦР (УЦ) о компрометации ключей пользователя.

Информация о компрометации может передаваться в УЦ по телефону с сообщением заранее условленного пароля, зарегистрированного в «Карточке оповещения о компрометации».

После компрометации ключей пользователь формирует новый закрытый ключ и запрос на сертификат. Так как пользователь не может использовать скомпрометированный ключ для формирования ЭП и передачи запроса в защищенном виде по сети, запрос на сертификат вместе с бланками доставляется лично пользователем (администратором безопасности) в Центр Регистрации.

При хранении ключей на HDD ПЭВМ необходимо использовать парольную защиту.

СКЗИ может функционировать и хранить ключевую информацию в двух режимах:

– в памяти приложения;

– в «Службе хранения ключей», реализованной в виде системного сервиса.

Ключи находятся в кэше до завершения приложения или до выключения компьютера (остановки службы), что позволяет использовать закрытый ключ даже после закрытия криптографического контекста.

Функционирование и хранение ключей СКЗИ «КриптоПро CSP» v 4.0 R4 в «Службе хранения ключей» обеспечивает дополнительную защиту ключевой информации от других приложений, выполняющихся на ПЭВМ, но может незначительно замедлить производительность системы.

В случае необходимости проведения ремонтных и регламентных работ аппаратной части СКЗИ/СФК необходимо обеспечить невозможность доступа нарушителя к ключевой информации, содержащейся в аппаратной части СКЗИ/СФК. Конкретный перечень мер должен быть определен исходя из условий эксплуатации СКЗИ.

4.2.4. Уничтожение ключей на ключевых носителях

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

Об уничтожении ключей делается соответствующая запись в «Журнале пользователя сети» (см. Ведение журналов п.8.11).

4.2.5. Взаимодействие с пользователем при работе с ключевыми носителями

При работе с ключевыми носителями СКЗИ может использовать какой-либо пользовательский интерфейс (UI). Это может происходить, например, при необходимости выбрать носитель или ввести PIN. Чтобы отключить пользовательский интерфейс (например, для автоматизации), в некоторых приложениях существует опция -silent. Также возможно запретить СКЗИ отображать пользовательский интерфейс глобально для всех приложений на данном ПК. Для этого в настройках СКЗИ нужно задать параметр force_silent равным единице (см. ниже), force_silent равный нулю вернёт поведение по умолчанию. Если же вызовы функций требуют отображения пользовательского интерфейса, будет возвращена ошибка NTE_SILENT_CONTEXT.

Изменение параметра force_silent:

Для операционных систем группы Windows необходимо изменить значение ключа реестра

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\force_silent (для 64-битных операционных систем),

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters\force_silent (для 32-битных операционных систем).

Настройка СКЗИ для остальных ОС осуществляется с помощью утилиты cpconfig:

./cpconfig -ini '\config\parameters' -add long force_silent 1

5. Состав СКЗИ

Исполнение 2-Base класса защиты КС2 выполнено в следующем составе:

– криптосервис;
– криптодрайвер;
– модуль сетевой аутентификации (КриптоПро TLS);
– модуль обработки сертификатов и CMS протокола;
– утилита выработки внешней гаммы;
– утилита командной строки для шифрования файлов;
– утилита командной строки для работы с сертификатами;
– модуль аутентификации пользователя в домене Windows;
– пакет разработчика для использования протоколов IPsec (IPsec SDK);
– пакет разработчика для встраивания СКЗИ (CSP SDK);
– 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.4.

СКЗИ «КриптоПро CSP» v 4.0 R4 функционирует на одном из двух уровней:

– уровень приложения;
– уровень ядра ОС.

В состав СКЗИ «КриптоПро CSP» v 4.0 R4 входят:

– Библиотеки dll, сервисы, драйверы «КриптоПро CSP».
– Модуль сетевой аутентификации «КриптоПро TLS».
– Модуль «КриптоПро Winlogon».
– Криптографический интерфейс «КриптоПро CSP».
– Программный датчик случайных чисел (ПДСЧ) с инсталляцией от физического ДСЧ (ФДСЧ) встраиваемого программно-аппаратного комплекса (ПАК) защиты от НСД, внешней гаммы.
– Контроль целостности программного обеспечения.
– Система инженерно-криптографической защиты.
– Система защиты от НСД (используется опционально).

5.1. Состав подсистемы СФК

В состав подсистемы СФК входят следующие компоненты:

– Приложение (Прикладное программное обеспечение, использующее СКЗИ).
– Интерфейс SSPI (подмножество интерфейса криптографических протоколов Secure Support Provider Interface (SSPI, CryptoAPI v. 2.0) для реализации протокола сетевой аутентификации TLS v. 1.0 (под управлением ОС Windows).
– Модули настройки ОС Windows для обеспечения функционирования СКЗИ.
– Интерфейс CryptoAPI 2.0.
– Средства Crypt32(Win32,64) для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс «КриптоПро CSP» под управлением ОС Windows.
– Средства CapiLite - для обеспечения работы с сертификатами с использованием интерфейса CryptoAPI 2.0 через криптографический интерфейс «КриптоПро CSP» под управлением ОС семейства UNIX (Linux , FreeBSD, Solaris, AIX).

– Криптографический интерфейс «КриптоПро CSP».
– Штатные интерфейсы ключевых носителей.

ASN.1 - система кодирования/декодирования данных в форматах ASN.1.

Состав модулей СКЗИ и подсистемы программной СФК для соответствующих программно-аппаратных сред конкретизируется в дополнениях ЖТЯИ.00088-03 91 02, ЖТЯИ.00088-03 91 03, ЖТЯИ.00088-03 91 04, ЖТЯИ.00088-03 91 05, ЖТЯИ.00088-03 91 06 к настоящему документу.

6. Обеспечение контроля целостности

Контроль целостности дистрибутива обеспечивается при помощи утилиты cpverify.exe, полученной доверенным способом в соответствии с Приложением 1.

СКЗИ КриптоПро CSP позволяет осуществлять динамический контроль целостности ПО.

7. Требования по встраиванию и использованию ПО СКЗИ

Встраивание СКЗИ в защищаемые информационные системы должно производиться в соответствии с Положением ПКЗ-2005. Встраивание должны проводить организации, имеющие лицензию на право проведения таких работ.

При создании защищенной информационной системы должны быть определены модель возможных угроз и политика ее безопасности. В зависимости от политики безопасности определяется необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

Защита от закладок, вирусов, модификации системного и прикладного ПО должна быть обеспечена использованием, средств антивирусной защиты и организационных мероприятий.

Правила встраивания и использования СКЗИ

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

1. При использовании открытого ключа или ключа проверки ЭП должны быть обеспечены его авторизация, достоверность, целостность и идентичность с помощью процедур Удостоверяющего центра.

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

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

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

5. При вызове приложением функции СКЗИ в прикладном программном обеспечении должна быть предусмотрена проверка кода завершения вызываемой функции.

8. Требования по защите от НСД

8.1. Общие требования по организации работы по защите от НСД

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

Наряду с применением средств защиты от НСД необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

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

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться администратором безопасности на основе требований документации на средства защиты от НСД.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением требований по безопасности.

Администратор безопасности не должен иметь возможности доступа к конфиденциальной информации пользователей.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе.

8.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

– Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.

– Должны быть приняты меры, исключающие несанкционированное вскрытие корпусов и средств, входящих в состав СКЗИ.

– Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

– Размещение СКЗИ «КриптоПро CSP» версия 4.0 R4 в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

– СКЗИ «КриптоПро CSP» версия 4.0 R4 вводиться в эксплуатацию и выводится из эксплуатации в соответствии с документацией на СКЗИ.

8.3. Требования по установке СКЗИ, общесистемного и специального ПО на ПЭВМ

1. ПЭВМ, на которых используется СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ «КриптоПро CSP» версия 4.0 R4.

2. Инсталляция СКЗИ «КриптоПро CSP» версия 4.0 R4 на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.

3. К установке общесистемного и специального программного обеспечения, а также СКЗИ «КриптоПро CSP» версия 4.0 R4, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

4. При установке программного обеспечения СКЗИ «КриптоПро CSP» версия 4.0 R4 следует:

5. На технических средствах, предназначенных для работы с СКЗИ, использовать только лицензионное программное обеспечение фирм - изготовителей.

6. При установке ПО СКЗИ на ПЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент СФК.

7. На ПЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.

– Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ).

– После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ, а также его окружения в соответствии с документацией.

– Программное обеспечение, устанавливаемое на ПЭВМ с СКЗИ не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;

- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

8.4. Меры по обеспечению защиты от НСД

При использовании СКЗИ должны выполняться следующие меры по защите информации от НСД:

– необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;

– личный пароль пользователь не имеет права сообщать никому;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

– указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

– средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

– администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

ЗАПРЕЩАЕТСЯ:

– оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ (в том числе смарт-карты), после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

– записывать на ключевые носители постороннюю информацию;

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

– не использовать нестандартные, измененные или отладочные версии ОС.

– исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

– исключить возможность удаленного управления, администрирования и модификации ОС и её настроек.

– на ПЭВМ должна быть установлена только одна операционная система.

– правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.

– все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).

– режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.

– всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

– необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системный реестр;
- файлы и каталоги;
- временные файлы;
- журналы системы;
- файлы подкачки;
- кэшируемая информация (пароли и т.п.);
- отладочная информация.

Кроме того, необходимо организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

– должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

– необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

– в случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

– при использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, организация VPN сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

– организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

– организовать и использовать комплекс мероприятий антивирусной защиты.

– должно быть запрещено использование СКЗИ для защиты речевой информации.

– должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.

ЗАПРЕЩАЕТСЯ:

– использовать ключи свыше срока, указанного в настоящих правилах.

– осуществлять несанкционированное копирование ключевых носителей.

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер (за исключением случаев, предусмотренных данными правилами).

– вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя.

– подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.

– работать на компьютере, если во время его начальной загрузки не проходит встроенный тест ОЗУ, предусмотренный в ПЭВМ.

– вносить какие-либо изменения в программное обеспечение СКЗИ.

– изменять настройки, установленные программой установки СКЗИ или администратором.

– использовать синхропосылки, вырабатываемые не средствами СКЗИ.

– обрабатывать на ПЭВМ, оснащенной СКЗИ, информацию, содержащую государственную тайну.

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ КриптоПро CSP.

– осуществлять несанкционированное вскрытие системных блоков ПЭВМ.

– приносить и использовать в помещении, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

Рекомендуется аппаратуру, на которой устанавливается СКЗИ, проверить на отсутствие аппаратных закладок.

8.5. Действия при компрометации ключей

В случае компрометации ключей по факту компрометации должно быть проведено служебное расследование. Скомпрометированные ключи выводятся из действия.

Выведенные из действия скомпрометированные ключевые носители после проведения служебного расследования уничтожаются, о чем делается запись в «Журнале пользователя сети».

Скомпрометированные ключи подлежат замене.

Подробные действия при компрометации ключей описаны в п. 6.8 документа «ЖТЯИ.00088-03 91 01. Руководство администратора безопасности. Общая часть.»

8.6. Требования по подключению СКЗИ для работы по общедоступным каналам передачи данных

1. 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.

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

- Порядок подключения СКЗИ к каналам.
- 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.

3. Перечень стандартных 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.

4. Должен быть обеспечен организационно-технический контроль запросов на установление соединения абонентов по протоколу TLS с использованием эфемерных ключей, исключающих возможность использования абонентом не своих атрибутов соединения (такие, как Client_Id и т.п.).

5. 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.

6. При установке параметров, позволяющих создавать соединения, отличные от криптографически защищенных, в соответствии с настоящими правилами (TLS на основе сертификатов ключей ГОСТ Р 34.10-2001), должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информации. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с СКЗИ по требованиям информационной безопасности.

8.7. Требования по использованию в СКЗИ программно-аппаратных средств защиты от НСД

СКЗИ должно использоваться со средством защиты от НСД, входящим в комплект поставки согласно формуляру на изделие. В качестве программно-аппаратных средств защиты от НСД в СКЗИ могут использоваться сертифицированный электронный замок «Соболь», программно-аппаратный комплекс «КРИПТОН-ЗАМОК», АМДЗ «Аккорд» и АПМДЗ «МАКСИМ-М1». Идентификационные данные указанных средств приведены в документе «ЖТЯИ.00088-03 30 01. КриптоПро CSP. Формуляр», п.3.10.

8.7.1. Электронный замок «Соболь»

Система **Электронный замок** предназначена для организации защиты компьютера от входа посторонних пользователей. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе **Электронный замок** как пользователи данного компьютера.

Электронный замок «Соболь» используется на платформах

- Windows (платформа IA32);
- Linux (платформа IA32);
- FreeBSD 7/8/9/10 (платформа IA32);
- Solaris 10/11 (платформа IA32).

Электронный замок «Соболь» обеспечивает:

– регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;

– запрос персонального идентификатора и пароля пользователя при загрузке компьютера;

– возможность блокирования входа в систему зарегистрированного пользователя;

– ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;

– контроль целостности файлов на жестком диске (только в ОС Windows);

– контроль целостности физических секторов жесткого диска (только в ОС Windows);

– аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска и CD-ROM диска.

Установка и настройка электронного замка на АРМ пользователя должна производиться в соответствии с эксплуатационной документацией. Перед эксплуатацией электронного замка в составе АРМ пользователя необходимо ознакомиться с комплектом документации (в соответствии с паспортом УВАЛ.00300-04 ПС/ КБДЖ.468243.067 ТУ) на данный комплекс и принять рекомендуемые в документации защитные организационные меры.

Настройка электронного замка на требуемую конфигурацию выполняется администратором безопасности. Настройка должна исключать возможность вмешательства пользователя в процессы загрузки операционной системы и прикладного ПО и проверки целостности программной среды.

9. Установка дистрибутивов ПО СКЗИ

Установка ПО «КриптоПро CSP» версия 4.0 R4 в зависимости от используемой платформы производится в соответствии с дополнениями ЖТЯИ.00088-03 91 02, ЖТЯИ.00088-03 91 03, ЖТЯИ.00088-03 91 04, ЖТЯИ.00088-03 91 05, ЖТЯИ.00088-03 91 06, к документу ЖТЯИ.00088-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть».

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

Перед установкой необходимо осуществить контроль целостности установочных модулей дистрибутива при помощи утилиты cpverify.exe, входящей в состав дистрибутива СКЗИ КриптоПро CSP.

10. Нештатные ситуации при эксплуатации СКЗИ

Ниже приведен основной перечень нештатных ситуаций и соответствующие действия персонала при их возникновении.

Таблица 1 - Действия персонала в нештатных ситуациях

№п/п	Нештатная ситуация	Действия персонала
1.	Эвакуация, угроза нападения, взрыва и т.п., стихийные бедствия, аварии общего характера в Центре управления ключевой системой.	Остановить все ЭВМ. Персонал, имеющий доступ к ключам, обязан сдать все имеющиеся у него в наличии ключевые носители администратору безопасности. Администратор безопасности упаковывает все ключевые носители, регистрационные карточки сертификатов открытых ключей пользователей, сертификаты ключей проверки ЭП пользователей в опечатываемый контейнер, который выносит в безопасное помещение или здание. Опечатанный контейнер должен находиться под охраной до окончания действия нештатной ситуации и восстановления нормальной работы аппаратных и программных средств СКЗИ. Администратор безопасности оповещает по телефонным каналам общего пользования всех пользователей о приостановке работы системы. В случае наступления события, повлекшего за собой долговременный выход из строя аппаратных средств СКЗИ, администратор безопасности уничтожает всю ключевую информацию с носителей, находящихся в контейнере.
2.	Компрометация одного из личных ключевых носителей.	Порядок действий при компрометации ключей описан в разделе 9.5 «Действия при компрометации ключей».
3.	Выход из строя первого личного ключевого носителя.	Необходимо сообщить по телефону в УЦ о факте выхода из строя личного ключевого носителя и обеспечить его доставку в УЦ для выяснения причин выхода из строя. Для работы используется второй личный ключевой носитель.
4.	Выход из строя второго личного ключевого носителя (при условии, что первый тоже вышел из строя).	Пользователь, у которого вышли из строя оба личных ключевых носителя, является в УЦ для повторной регистрации (без изменения данных регистрации).
5.	Отказы и сбои в работе аппаратной части АРМ со встроенной СКЗИ.	При отказах и сбоях в работе аппаратной части АРМ со встроенной СКЗИ необходимо остановить работу, по возможности локализовать неисправность и в дальнейшем произвести ремонт в установленном порядке и, при необходимости, переустановку СКЗИ.
6.	Отказы и сбои в работе средств защиты от НСД.	При отказах и сбоях в работе средств защиты от НСД, администратор безопасности, должен восстановить работоспособность средств НСД. При необходимости переустановить программно-аппаратные средства НСД.
7.	Утеря личного ключевого носителя.	Утеря личного ключевого носителя приводит к компрометации хранящегося в нем ключа. Порядок действий при компрометации ключей описан в разделе 9.5 «Действия при компрометации ключей».
8.	Отказы и сбои в работе программных средств вследствие не выявленных ранее ошибок в программном	При отказах и сбоях в работе программных средств, вследствие не выявленных ранее ошибок в программном обеспечении, необходимо остановить работу, локализовать по возможности причину отказов и сбоев и вызвать разработчика данного ПО или его представителя для устранения причин, вызывающих отказы и сбои.

№п/п	Нештатная ситуация	Действия персонала
	обеспечении.	
9.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, вследствие случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
10.	Отказы в работе программных средств вследствие ошибок оператора.	При отказах в работе программных средств, вследствие ошибок оператора, оператор сообщает о данном факте лицу, ответственному за безопасность функционирования программных и аппаратных средств. Ответственный за безопасность функционирования программных и аппаратных средств дает соответствующие указания обслуживающему персоналу по восстановлению правильной работы программных средств в установленном порядке.

Все нештатные ситуации должны отражаться в «Журнале пользователя сети».

11. Встраивание СКЗИ

При встраивании СКЗИ «КриптоПро CSP» в прикладные системы необходимо проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований в следующих случаях:

1) если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;

2) при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации (далее - государственные органы);

3) при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд (далее - организации, выполняющие государственные заказы);

4) если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;

5) при обрабатывании информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путем использования средств криптографической защиты;

6) при обрабатывании информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации.

Указанную проверку необходимо проводить по ТЗ, согласованному с 8 Центром ФСБ России.

Для исключения возможности влияния аппаратных компонентов СФК на функционирование СКЗИ должны быть выполнены следующие требования:

- в ПО BIOS ПЭВМ должны быть определены установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске.
- вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов;
- средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность бесконтрольного изменения аппаратной части рабочей станции и подключения внешних устройств.
- установка СКЗИ производится только лицами, имеющими допуск к работам (в соответствии с нормами по безопасности, принятыми в организации);
- подключаемое к ПЭВМ оборудование не должно создавать угроз безопасности ОС и СКЗИ, установленных на ПЭВМ;
- ПЭВМ, на которой устанавливается СКЗИ, должна выполнять процедуры самоконтроля основных аппаратных компонентов после каждого сброса системы включая момент появления питания;

• к эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на СКЗИ.

В условиях:

- если информация, обрабатываемая ПАК, подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации в федеральных органах исполнительной власти и в органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты обрабатываемой ПАК информации, в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд;

для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ необходимо проведение исследований на соответствие ПО BIOS СВТ, на которых установлено СКЗИ «Временным методическим рекомендациям к проведению исследований программного обеспечения BIOS по документированным возможностям».

12. Использование программных интерфейсов

Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00088-03 30 01 может производиться без создания новых СКЗИ в случае использования вызовов интерфейсов CryptoAPI СКЗИ из перечня Приложения 2. Данные вызовы могут использоваться как напрямую, так и опосредованно через промежуточные интерфейсы.

В случае использования наапрямую или опосредованно) в программном обеспечении прочих вызовов интерфейсов CryptoAPI СКЗИ необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

Приложение 1. Контроль целостности программного обеспечения

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.

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>679837307CDC7AA1E4BDBB75194A24D42C782079AF08E2D362D7624A90D604C7</
Tag>
</entry>
<entry name="verifier.exe">
<Path>C:\WINDOWS\system32\verifier.exe</Path>
<Algid>00008021</Algid>
<Tag>9DF987B89A323BEBC3C29BAC0AED42A4F5BD651892AAE79F1EC1D05288D06B9C</
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.

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 2. Перечень вызовов, использование которых при разработке систем на основе СКЗИ «КриптоПро CSP» с учетом п.1.5 Формуляра ЖТЯИ.00088-03 30 01 возможно без дополнительных тематических исследований:

Функция	Описание	Ограничения на использование функции
Функции инициализации и настройки провайдера		
CryptAcquireContext	Функция CryptAcquireContext используется для создания дескриптора криптопровайдера с именем ключевого контейнера, определённым параметром pszContainer	
CryptReleaseContext	Функция CryptReleaseContext используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext.	
CryptContextAddRef	Управляет счетчиком дескрипторов созданного CryptAcquireContext.	
CryptEnumProviders	Перечисление установленных криптопровайдеров	
CryptEnumProviderTypes	Перечисление установленных типов криптопровайдеров	
CryptGetDefaultProvider	Получение контекста провайдера, установленного в системе по умолчанию	
CryptGetProvParam	Функция CryptGetProvParam получает параметры криптопровайдера.	
CryptSetProvParam	Функция CryptSetProvParam устанавливает параметры криптопровайдера.	
FreeCryptProvFromCertEx	Функция используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext или через CNG.	
CryptInstallDefaultContext, CryptSetProvider, CryptSetProviderEx, CryptUninstallDefaultContext	Функции управления контекстом провайдера по умолчанию	
Функции генерации и обмена ключами, создание конфигурирование и удаление ключей		

CryptGenKey	Функция CryptGenKey генерирует случайные криптографические ключи или ключевую пару (закрытый/открытый ключи).	
CryptDestroyKey	Функция CryptDestroyKey удаляет ключ, передаваемый через параметр hKey. После удаления ключ (дескриптор ключа) не может использоваться.	
CryptExportKey	Функция CryptExportKey используется для экспорта криптографических ключей из ключевого контейнера криптопровайдера, сохраняя их в защищённом виде.	Разрешено экспортировать только открытые ключи (PUBLICKEYBLOB).
CryptGenRandom	Функция CryptGenRandom заполняет буфер случайными байтами.	
CryptGetKeyParam	Функция CryptGetKeyParam возвращает параметры ключа.	
CryptGetUserKey	Функция CryptGetUserKey возвращает дескриптор одной из долговременных ключевых пар в ключевом контейнере.	
CryptImportKey	Функция CryptImportKey используется для импорта криптографического ключа из ключевого блоба в контейнер криптопровайдера.	Разрешено импортировать только открытые ключи (PUBLICKEYBLOB).
CryptSetKeyParam	Функция CryptSetKeyParam устанавливает параметры ключа.	Разрешено использование только со следующими символьными аргументами: KP_CERTIFICATE, KP_CIPHEROID, KP_DHOID, KP_HASHOID.
Функции обработки криптографических сообщений		
CryptSignMessage	Функция CryptSignMessage создает хэш определенного содержания, подписывает хэш и затем производит закодирование и текста исходного сообщения, и подписанного хэша	
CryptVerifyMessageSignature	Функция CryptVerifyMessageSignature проверяет электронно-цифровую подпись подписанного сообщения.	
CryptVerifyDetachedMessageSignature	Функция CryptVerifyDetachedMessageSig	

	nature проверяет подписанное сообщение, содержащее отсоединенную (detached) подпись или подписи	
CryptDecodeMessage	Функция декодирует, расшифровывает и проверяет сообщение	
CryptDecryptAndVerifyMessageSignature	Функция декодирует и проверяет сообщение	
CryptEncryptMessage	Функция CryptEncryptMessage зашифровывает и производит закодирование сообщения. Аутентичность сообщения не обеспечивается.	
CryptDecryptMessage	Функция CryptDecryptMessage производит раскодирование и расшифрование сообщения. Проверка аутентичности сообщения не производится. Примечание: Не допускается автоматический анализ результата работы функции, направленный на проверку корректности сообщения.	
CryptGetMessageCertificates	Функция возвращает хранилище сертификатов и списки аннулированных сертификатов из сообщения	
CryptGetMessageSignerCount	Функция возвращает количество подписавших сообщение	
CryptHashMessage	Функция создает хэшированное сообщение	
CryptSignAndEncryptMessage	Функция создает подписанное и зашифрованное сообщение	
CryptSignMessageWithKey	Функция создает подписанное сообщение	
CryptVerifyDetachedMessageHash	Функция проверяет открепленный хэш	
CryptVerifyMessageHash	Функция проверяет хэшированное сообщение	
CryptVerifyMessageSignatureWithKey	Функция проверяет подписанное сообщение	
CryptMsgCalculateEncodedLength	Функция CryptMsgCalculateEncodedLength вычисляет максимальное количество байтов, необходимое для закодированного криптографического	

	сообщения, заданного типом сообщения, параметрами кодирования и общей длиной информации, которая должна быть закодирована.	
CryptMsgOpenToEncode	Функция CryptMsgOpenToEncode открывает криптографическое сообщение для закодирования и возвращает дескриптор открытого сообщения.	
CryptMsgOpenToDecode	Функция CryptMsgOpenToDecode открывает криптографическое сообщение для раскодирования и возвращает дескриптор открытого сообщения.	
CryptMsgUpdate	Функция CryptMsgUpdate пополняет текст криптографического сообщения.	
CryptMsgGetParam	Функция CryptMsgGetParam получает параметр сообщения после того, как криптографическое сообщение было раскодировано или закодировано.	
CryptMsgControl	Функция CryptMsgControl выполняет контрольное действие.	
CryptMsgClose	Функция CryptMsgClose закрывает дескриптор криптографичекого сообщения.	
CryptMsgDuplicate	Функция CryptMsgDuplicate дублирует дескриптор криптографического сообщения путем увеличения счетчика ссылок	
Функции работы с алгоритмами хэширования		
CryptCreateHash	Функция CryptCreateHash инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование только со следующими символьными аргументами: CALG_GR3411, CALG_GR3411_2012_256, CALG_GR3411_2012_512, CALG_GR3411_HMAC, CALG_GR3411_2012_256_HMAC, CALG_GR3411_2012_512_HMAC, CALG_SHAREDKEY_HASH.
CryptDestroyHash	Функция CryptDestroyHash	

	удаляет объект функции хэширования.	
CryptDuplicateHash	Функция CryptDuplicateHash создаёт точную копию объекта функции хэширования, включая все его переменные, определяющие внутреннее состояние объекта функции хэширования.	
CryptGetHashParam	Функция CryptGetHashParam возвращает параметры объекта функции хэширования и значение функции хэширования.	
CryptHashData	Функция CryptHashData передаёт данные указанному объекту функции хэширования.	
CryptSetHashParam	Функция CryptSetHashParam устанавливает параметры объекта хэширования.	Разрешено использование только с символьными аргументами HP_HASHSIZE, HP_OID/KP_HASHOID, HP_OPEN.
CryptSignHash	Функция CryptSignHash возвращает значение электронной цифровой подписи от значения функции хэширования.	
CryptVerifySignature	Функция CryptVerifySignature осуществляет проверку цифровой подписи.	Разрешено использование только с дескрипторами ключей, полученных ранее с помощью вызова CryptImportPublicKeyInfo (CryptImportPublicKeyInfoEx) из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy
Функции работы с сертификатами, списками аннулированных сертификатов, хранилищем сертификатов		
Списки аннулированных сертификатов		
CertAddCRLContextToStore	Функция CertAddCRLContextToStore добавляет контекст COC в хранилище сертификатов.	
CertAddCRLLinkToStore	Функция создает ссылку на список аннулированных сертификатов в другом хранилище	
CertAddEncodedCRLToStore	Функция CertAddEncodedCRLToStore создает контекст COC из закодированного COC и добавляет его в хранилище	

	сертификатов. Функция создает копию контекста СОС перед добавлением его в хранилище.	
CertEnumCRLsInStore	Функция CertEnumCRLsInStore получает первый или следующий СОС в хранилище. Эта функция используется в цикле для того, чтобы последовательно получить все СОС в хранилище.	
CertFreeCRLContext	Функция CertFreeCRLContext освобождает контекст СОС, уменьшая счетчик ссылок на единицу. Когда счетчик ссылок обнуляется, функция CertFreeCRLContext освобождает память, выделенную под контекст СОС.	
CertCreateCRLContext	Функция CertCreateCRLContext создает контекст СОС из закодированного СОС. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного СОС.	
CertDeleteCRLFromStore	Функция удаляет список аннулированных сертификатов из хранилища	
CertDuplicateCRLContext	Функция CertDuplicateCRLContext дублирует контекст СОС, увеличивая счетчик ссылок на СОС на единицу.	
CertFindCRLInStore	Функция CertFindCRLInStore находит первый или следующий контекст СОС в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara. Эта функция может быть использована в цикле для того, чтобы найти	

	все СОС в хранилище сертификатов, удовлетворяющие заданному критерию поиска.	
CertDeleteCertificateFromStore	Функция CertDeleteCertificateFromStore удаляет определенный контекст СОС из хранилища сертификатов.	
CertFindCertificateInCRL	Функция осуществляет поиск заданного сертификата в списке аннулированных сертификатов	
CertGetCRLFromStore	Функция CertGetCRLFromStore получает первый или следующий контекст СОС для определенного издателя сертификата из хранилища сертификатов. Эта функция также осуществляет возможную проверку СОС.	
CertSerializeCRLStoreElement	Функция сериализации списка аннулированных сертификатов со своими свойствами	
Расширенные свойства сертификата списка отозванных (СОС) сертификатов и CTL		
CertGetCRLContextProperty	Функция CertGetCRLContextProperty получает расширенные свойства определенного контекста СОС.	
CertSetCRLContextProperty	Функция CertSetCRLContextProperty устанавливает расширенные свойства определенного контекста СОС.	
CertGetCertificateContextProperty	Функция CertGetCertificateContextProperty получает информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertEnumCertificateContextProperties	Функция CertEnumCertificateContextProperties позволяет перечислить информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertSetCertificateContextProperty	Функция CertSetCertificateContextPropert	

	у устанавливает расширенные свойства для определенного контекста сертификата.	
CertEnumCRLContextProperties	Перечисление расширенных свойств списка аннулированных сертификатов	
CertEnumCTLContextProperties	Перечисление расширенных свойств CTL	
CertGetCTLContextProperty	Получение расширенного свойства CTL	
CertSetCTLContextProperty	Установка расширенных свойств CTL	
CertAddCTLContextToStore	Функция CertAddCTLContextToStore добавляет контекст CTL в хранилище сертификатов	
CertCreateCTLContext	Функция CertCreateCTLContext создает контекст закодированного CTL. Созданный контекст не помещается в хранилище сертификатов. Функция делает копию CTL в созданном контексте.	
CertDuplicateCTLContext	Функция CertDuplicateCTLContext дублирует контекст CTL, увеличивая счетчик ссылок на CTL на единицу.	
CertFreeCTLContext	Функция CertFreeCTLContext освобождает контекст CTL, уменьшая счетчик ссылок на единицу. Когда счетчик ссылок обнуляется, функция CertFreeCTLContext освобождает память, выделенную под контекст CTL.	
Функции работы с сертификатами		
CertAddCertificateContextToStore	Функция CertAddCertificateContextToStore добавляет контекст сертификата в хранилище сертификатов.	
CertAddCertificateLinkToStore	Добавляет ссылку на сертификат в другом хранилище	
CertAddEncodedCertificateToStore	Функция CertAddEncodedCertificateToStore создает контекст сертификата из закодированного сертификата	

	и добавляет его в хранилище сертификатов. Созданный контекст не содержит никаких расширенных свойств.	
CertEnumCertificatesInStore	Функция CertEnumCertificatesInStore получает первый или следующий сертификат в хранилище сертификатов. Эта функция используется в цикле для того, чтобы последовательно получить все сертификаты в хранилище сертификатов.	
CertFreeCertificateContext	Функция CertFreeCertificateContext освобождает контекст сертификата, уменьшая счетчик ссылок на единицу.	
CertCreateCertificateContext	Функция CertCreateCertificateContext создает контекст сертификата из закодированного сертификата. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного сертификата.	
CertDuplicateCertificateContext	Функция CertDuplicateCertificateContext дублирует контекст сертификата, увеличивая счетчик ссылок на единицу.	
CertFindCertificateInStore	Функция CertFindCertificateInStore находит первый или следующий контекст сертификата в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara.	
CertDeleteCertificateFromStore	Функция CertDeleteCertificateFromStore удаляет определенный контекст сертификата из хранилища сертификатов.	
CertGetSubjectCertificateFromStore	Функция CertGetSubjectCertificateFromSt	

	ore получает контекст сертификата из хранилища сертификатов, однозначно определяемый его издателем и серийным номером	
CertGetIssuerCertificateFromStore	Поиск сертификатов издателей заданного сертификата	
CertGetSubjectCertificateFromStore	Поиск сертификата по серийному номеру и издателю	
CertGetValidUsages	Поиск пересечения KeyUsage для массива сертификатов	
CertSerializeCertificateStoreElemene	Сериализация элемента хранилища	
CertComparePublicKeyInfo	Функция CertComparePublicKeyInfo сравнивает два открытых ключа и определяет, являются ли они идентичными	
CertFindExtension	Функция CertFindExtension находит расширение в массиве и возвращает указатель на него.	
CertGetPublicKeyLength	Фукнция CertGetPublicKeyLength возвращает длину ключа в битах.	
CertGetIntendedKeyUsage	Функция CertGetIntendedKeyUsage получает назначение ключа из сертификата.	
CertCompareCertificateName	Функция CertCompareCertificateName сравнивает два сертификата и определяет, являются ли они идентичными.	
CryptSignCertificate	Функция CryptSignCertificate формирует электронную подпись блока закодированных данных TBS.	Разрешено использование только со следующими символьными аргументами: CALG_GR3410, CALG_GR3410_12_256, CALG_GR3410_12_512
OCSP		
CertAddRefServerOcspResponse	Увеличение счетчика ссылок на OCSP ответ	
CertAddRefServerOcspResponseContext	Увеличение счетчика ссылок на контекст OCSP ответа	
CertCloseServerOcspResponse	Закрытие дескриптора OCSP ответа	
CertGetServerOcspResponseContext	Получение контекста OCSP ответа	
CertOpenServerOcspResponse	Открытие дескриптора OCSP ответа для заданной цепочки	

	сертификатов	
Оконные функции		
CertSelectCertificate	Отображение диалога выбора сертификата по заданным критериям	
CryptUIDlgCertMgr	Отображение диалога управления сертификатами	
CryptUIDlgSelectCertificate	Отображение диалога выбора сертификата	
CryptUIDlgSelectCertificateFromStore	Отображение диалога выбора сертификата из хранилища	
CryptUIDlgViewCertificate	Отображение диалога со свойствами сертификата	
CryptUIDlgViewContext	Отображение сертификата, списка аннулированных сертификатов или CTL	
CryptUIDlgViewSignerInfo	Отображение диалога с информацией о подписавшем	
CertSelectionGetSerializedBlob	Сериализация сертификата из структуры, используемой для отображения	
GetFriendlyNameOfCert	Преобразование имени сертификата к «читаемому» виду	
Функции проверки цепочек		
CertVerifyCertificateChainPolicy	Функция CertVerifyCertificateChainPolicy проверяет цепочку сертификатов на достоверность, включая соответствие критерию истинности.	
CertGetCertificateChain	Функция CertGetCertificateChain строит цепочку сертификатов, начиная с последнего сертификата, в обратном направлении до доверенного корневого сертификата, если это возможно.	
CertFreeCertificateChain	Функция CertFreeCertificateChain освобождает цепочку сертификатов путем уменьшения счетчика ссылок. Если счетчик ссылок равен нулю, то память, выделенная под цепочку, освобождается.	
CertCreateCertificateChainEngine	Функция CertCreateCertificateChainEngine создает контекст	

	HCERTCHAINENGINE, который позволяет изменять параметры механизма построения цепочки сертификатов. Позволяет ограничивать множество доверенных сертификатов.	
CertFreeCertificateChainEngine	Функция CertFreeCertificateChainEngine освобождает контекст HCERTCHAINENGINE.	
CertCreateCTLEntryFromCertificate ContextProperties	Создание CTL на основе свойст атрибутов контекста сертификата	
CertDuplicateCertificateChain	Дублирование контекста цепочки.	
CertFindChainInStore	Функция построения цепочки по заданным критериям из хранилища	
CertFreeCertificateChainList	Функция освобождения массива цепочек	
CertIsValidCRLForCertificate	Функция проверки наличия сертификата в списке аннулированных сертификатов	
CertSetCertificateContextProperties FromCTLEntry	Установка свойств в контекст сертификата на основе CTL	
Расширенные свойства сертификата (EKU)		
CertGetEnhancedKeyUsage	Функция CertGetEnhancedKeyUsage получает информацию о расширенном использовании ключа из соответствующего расширения или из расширенных свойств сертификата. Расширенное использование ключа служит признаком правомерного использования сертификата.	
CryptAcquireCertificatePrivateKey	Функция CryptAcquireCertificatePrivateKe y получает дескриптор HCRYPTPROV и параметр dwKeySpec для определенного контекста сертификата.	
Функции работы с идентификаторами		
CryptFindOIDInfo	Функция CryptFindOIDInfo получает первую предопределенную или зарегистрированную структуру CRYPT_OID_INFO, согласованную с определенным типом ключа и с	

	ключом.	
CryptEnumOIDInfo	Перечисление зарегистрированных идентификаторов и получение информации для них	
Функции работы с хранилищем		
CertOpenStore	Функция CertOpenStore открывает хранилище сертификатов, используя заданный тип провайдера.	
CertDuplicateStore	Функция CertDuplicateStore дублирует дескриптор хранилища, увеличивая счетчик ссылок на хранилища на единицу.	
CertOpenSystemStore	Функция CertOpenSystemStore используется для открытия наиболее часто используемых хранилищ сертификатов.	
CertCloseStore	Функция CertCloseStore закрывает дескриптор хранилища сертификатов и уменьшает счетчик ссылок на хранилища на единицу.	
CertAddStoreToCollection	Добавление хранилища в коллекцию	
CertControlStore	Установка нотификации при различиях в закешированном хранилище и физическом хранилище	
Функции, используемые для работы с открытыми данными и объектами		
CryptImportPublicKeyInfoEx2	Функция CryptImportPublicKeyInfoEx2 импортирует информацию об открытом ключе в CNG и возвращает дескриптор открытого ключа.	
CryptImportPublicKeyInfoEx	Функция CryptImportPublicKeyInfoEx импортирует информацию об открытом ключе в CSP и возвращает дескриптор открытого ключа.	
CryptImportPublicKeyInfo	Функция CryptImportPublicKeyInfo преобразовывает и импортирует информацию об открытом ключе в провайдер и возвращает дескриптор открытого ключа.	
CryptExportPublicKeyInfoEx	Функция	

	CryptExportPublicKeyInfoEx экспортирует информацию об открытом ключе, связанную с соответствующим секретным ключом провайдера.	
CryptExportPublicKeyInfo	Функция CryptExportPublicKeyInfo экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
CertCompareCertificate	Функция CertCompareCertificate сравнивает два сертификата для того, чтобы определить, являются ли они идентичными.	
CertCompareIntegerBlob	Функция CertCompareIntegerBlob сравнивает два целочисленных блоба для определения того, представляют ли они собой два равных числа.	
CryptExportPublicKeyInfoFromBCryptKeyHandle	Экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
Функции кодирования/декодирования		
CryptDecodeObject	Функция CryptDecodeObject используются для декодирования сертификатов, списков аннулированных сертификатов (СОС) и запросов на сертификаты.	
CryptDecodeObjectEx	Функция CryptDecodeObjectEx используются для декодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты	
CryptEncodeObject	Функция CryptEncodeObject используются для кодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты.	
CryptEncodeObjectEx	Функция CryptEncodeObjectEx используются для кодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты.	

Получение объектов из удаленных источников		
CryptRetrieveObjectByUrlA	Функция CryptRetrieveObjectByUrlA получает объект инфраструктуры открытых ключей по заданному URL.	
CryptRetrieveObjectByUrlW	Функция CryptRetrieveObjectByUrlW является unicode версией функции CryptRetrieveObjectByUrlA.	
Дополнительные функции		
CryptBinaryToString	Функция переводит двоичную строку в строку Base64/HEX.	
CryptStringToBinary	Функция переводит строку HEX/Base64 в двоичную строку.	
CertFindAttribute	Функция производит поиск атрибута сертификата по идентификатору.	
CertGetNameString	Функция получает имя владельца или издателя сертификата.	
CertNameToStr	Функция производит раскодирование имени из ASN структуры в DN (RFC1779).	
CertSaveStore	Функция производит запись хранилища сертификатов (включая списки отозванных и доверенных сертификатов) в виде структуры PKCS#7 или бинарного дампа в память или файл.	
CryptFindCertificateKeyProvInfo	Функция осуществляет поиск закрытого ключа, соответствующего открытому ключу сертификата.	
CryptHashPublicKeyInfo	Функция осуществляет ASN1 кодирование и хэширование структуры CERT_PUBLIC_KEY_INFO	
CryptMsgCountersign	Функция вырабатывает добавочную подпись.	
CryptMsgCountersignEncoded	Функция вырабатывает добавочную подпись. (кодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMsgVerifyCountersignatureEncoded	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в	

	PKCS #7).	
CryptMsgVerifyCountersignatureEncodedEx	Функция проверяет добавочную подпись. (декодирует структуру SignerInfo, как определено в PKCS #7).	
CryptMemFree	Функция CryptMemFree освобождает память, которая была выделена с помощью CryptMemAlloc или CryptMemRealloc.	

Литература

1. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
2. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
3. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
4. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
5. ГОСТ Р 34.10-12 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
6. ГОСТ Р 34.11-12 Информационная технология. Криптографическая защита информации. Функция хэширования.
7. ЖТЯИ.00088-03 30 01. КриптоПро CSP. Формуляр.
8. ЖТЯИ.00088-03 90 01. КриптоПро CSP. Описание реализации.
9. ЖТЯИ.00088-03 91 01. КриптоПро CSP. Руководство Администратора безопасности. Общая часть.
10. ЖТЯИ.00088-03 91 02. КриптоПро CSP. Руководство Администратора безопасности. Использование СКЗИ под управлением ОС Windows.
11. ЖТЯИ.00088-03 91 03. КриптоПро CSP. Руководство Администратора безопасности. Использование СКЗИ под управлением ОС Linux.
12. ЖТЯИ.00088-03 91 04. КриптоПро CSP. Руководство Администратора безопасности. Использование СКЗИ под управлением ОС FreeBSD.
13. ЖТЯИ.00088-03 91 05. КриптоПро CSP. Руководство Администратора безопасности. Использование СКЗИ под управлением ОС Solaris.
14. ЖТЯИ.00088-03 91 06. КриптоПро CSP. Руководство Администратора безопасности. Использование СКЗИ под управлением ОС AIX.
15. ЖТЯИ.00088-03 92 01. КриптоПро CSP. Инструкция по использованию. Windows.
16. ЖТЯИ.00088-03 94 01. КриптоПро CSP. АРМ выработки внешней гаммы.
17. ЖТЯИ.00088-03 96 01. КриптоПро CSP. Руководство программиста.
18. [X.680-X.699]. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)
19. [X.509]. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
20. [PKIX]. RFC 2459. Housley, W. Ford, W. Polk, D. Solo, «Internet X.509 Public Key Infrastructure Certificate and CRL Profile», January 1999.
21. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).
22. Приказ ФАПСИ от 13.06.2001г. №152 «Об инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
изм.	измененных	замененных	новых	аннулиро-ванных					