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 R4 КС1

1-Base

Руководство администратора безопасности

Использование СКЗИ под управлением ОС SailfishOS

ЖТЯИ.00087-03 91 10
Листов 20

2018 г.

Содержание

Аннотация

Настоящее Руководство дополняет документ «ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» при использовании СКЗИ под управлением ОС SailfishOS.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» v 4.0 R4, должны разрабатываться с учетом требований настоящего документа.

Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
ДСЧ	Датчик случайных чисел
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
Провайдер	Исполняемый модуль или набор исполняемых модулей, позволяющих осуществлять криптографические операции.
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность ключа проверки электронной подписи или открытого ключа и определенных атрибутов конкретному абоненту
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратная среда

СКЗИ «КриптоПро CSP» v 4.0 R4 под управлением ОС SailfishOS используется в программно-аппаратной среде SailfishOS версии 2.1.1.12 (ARMv7).

1.2. Ключевые носители

В качестве ключевых носителей ключей ЭП и закрытых ключей выступают разделы накопителей, входящих в состав мобильных устройств под управлением ОС SailfishOS.

	1. Хранение закрытых ключей на устройстве под управлением ОС SailfishOS допускается только при условии распространения на это устройство требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть). 2. Носители в составе устройств под управлением ОС SailfishOS используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на устройстве. 3. Использование носителей других типов - только по согласованию с ФСБ России.

2. Установка дистрибутива ПО КриптоПро CSP

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора (например, с использованием команды devel-su).

СКЗИ «КриптоПро CSP» требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС SailfishOS для установки, удаления и обновления ПО применяются пакеты (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. В операционных системах Linux используется менеджер пакетов RPM (Red Hat Package Manager), который является гибким инструментом для установки, удаления, обновления и сборки программных пакетов. Пакеты, представленные в виде файла с расширением .rpm, содержат в себе непосредственно файлы ПО и информацию для конфигурирования среды.

Для установки пакета используется команда:

rpm -i <файл_пакета>

Например: **rpm -i ./lsb-cprocsp-base-4.0.9958-4.noarch.rpm**

Для удаления пакета используется команда:

rpm -e <имя_пакета>

Например: **rpm -e lsb-cprocsp-base-4.0.9958-4**

Имя пакета может не включать версию.

Например: **rpm -e lsb-cprocsp-base**

Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей, а удаляться в обратном порядке. Условно можно считать правильным порядком тот, который описан в таблице зависимостей и назначения пакетов.

Таблица 2.1 - Зависимости и назначения пакетов.

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
lsb-cprocsp-base	lsb	Базовый пакет, устанавливается первым., если только не нужны compat-пакеты.
lsb-cprocsp-rdr	lsb-cprocsp-base	Основные приложения, считыватели и ДСЧ.
lsb-cprocsp-kc1	lsb-cprocsp-rdr	Провайдер КС1.
lsb-cprocsp-capilite	lsb-cprocsp-rdr lsb-cprocsp-kc1	программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS…).
Дополнительный пакет		
lsb-cprocsp-devel	lsb-cprocsp-base	Пакет для разработчика.
cprocsp-stunnel	lsb-cprocsp-base	Универсальный SSL/TLS туннель.

3. Обновление СКЗИ КриптоПро CSP

Для обновления ПО СКЗИ на ОС SailfishOS необходимо:

- запомнить текущую конфигурацию CSP:
  - набор установленных пакетов;
  - настройки провайдера (для простоты можно сохранить /etc/opt/cprocsp/config.ini);
- удалить штатными средствами ОС все пакеты СКЗИ;
- установить аналогичные новые пакеты СКЗИ;
- при необходимости внести изменения в настройки (можно посмотреть diff старого и нового config.ini);
- ключи и сертификаты сохраняются автоматически.

4. Настройка СКЗИ

4.1. Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/cprocsp/sbin/arm.

4.2. Ввод серийного номера лицензии

При установке программного обеспечения «КриптоПро CSP» без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

```
# cpconfig -license -view
```

Для ввода лицензии выполните:

```
# cpconfig -license -set <серийный_номер>
```

Серийный номер следует вводить с соблюдением регистра символов.

4.3. Настройка оборудования СКЗИ

Утилита cpconfig также предназначена для изменения набора устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел. Предустановленными являются считыватели flash-носителей и файлов на жестком диске, а также консольный БиоДСЧ и считыватель внешней гаммы.

Для просмотра списка настроенных считывателей:

```
# ./cpconfig -hardware reader -view
```

Для просмотра списка настроенных ДСЧ:

```
# ./cpconfig -hardware rndm -view
```

Для использования внешней гаммы надо скопировать файлы с данными, полученными на "АРМ выработки внешней гаммы". Пример копирования файлов (положим, что они лежат в /tmp/db[1,2]):

```
# cp /tmp/db1/kis_1  /var/opt/cprocsp/dsrf/db1/kis_1
# cp /tmp/db2/kis_1  /var/opt/cprocsp/dsrf/db2/kis_1
```

При необходимости консольный БиоДСЧ и считыватель внешней гаммы возможно добавить вручную.

Для консольного БиоДСЧ требуется пакет пакет lsb-cprocsp-kc1, кроме того он работает только с КС1 провайдером. Для добавления консольного БиоДСЧ:

```
# ./cpconfig -hardware rndm -add bio_tui -level 5 -name "Console BioRNG"
```

Для добавления использования внешней гаммы:

```
# ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
# ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1
# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1
```

4.4. Установка параметров журналирования

СКЗИ позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал (обычно в

/var/log/messages). Существует возможность изменения настроек журналирования различных модулей продукта. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений. Для получения справки по настройкам журналирования:

```
# cpconfig -loglevel -help
```

Модули, для которых поддерживается журналирование:

cpcsp - ядро криптопровайдера

capi10 - CryptoAPI 1.0

cpext – дополнения для CryptoAPI 2.0

capi20 - CryptoAPI 2.0

libcspr – библиотека для подключения к провайдеру в сервисе или к HSM-серверу

libssp - TLS

cppkcs11 - PKCS11

cpdrv - драйвер

dmntcs – тестовое приложение для обращения к тестовому драйверу

4.5. Настройка криптопровайдера по умолчанию

Проводить настройку криптопровайдера по умолчанию нужно только в особых случаях для совместимости. Для просмотра типов доступных криптопровайдеров:

```
$ ./cpconfig -defprov -view_type
```

Для просмотра свойств криптопровайдера нужного типа:

```
# ./cpconfig -defprov -view -provtype <provtype>
```

Для установки провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -setdef -provtype <provtype> -provname <provname>
```

Для получения имени провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -getdef -provtype <provtype>
```

4.6. Включение режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. После успешной инсталляции необходимо включить данный режим, выполнив команду:

```
#./cpconfig -ini '\config\parameters' -add long StrengthenedKeyUsageControl 1
```

Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей или запустить утилиту csptest, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел.

```
# ./csptest -keyset -verifycontext -hard_rng
```

Использование СКЗИ без включения режима усиленного контроля использования ключей разрешается исключительно в тестовых целях.

5. Состав и назначение компонент программного обеспечения СКЗИ

5.1. Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

libcsp –библиотека «КриптоПро CSP», ядро провайдера.

libcspr - библиотека работы с удалённым «КриптоПро CSP».

libssp – библиотека сетевой аутентификации «КриптоПро TLS».

cpverify – модуль контроля целостности.

wipefile – модуль надёжного удаления файлов вместе с содержимым.

cryptcp - модуль для подписи и шифрования файлов, запроса выдачи сертификатов Удостоверяющим Центром.

certmgr - утилита командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами.

stunnel – модуль для создания TLS-туннеля.

В названиях дистрибутивов СКЗИ в качестве префикса используется обозначение cprocsp.

5.1.1. Библиотека libcsp

Библиотека **libcsp** реализует целевые функции криптографической защиты информации, работу с ключами, первичную обработку запроса получения доступа к ключевым носителям и БиоДСЧ.

5.1.2. Библиотека libcspr

Библиотека **libcspr** обеспечивает доступ к криптопровайдеру, функционирующему как отдельный сервис.

5.1.3. Библиотека сетевой аутентификации КриптоПро TLS

Библиотека **libssp** реализует протокол сетевой аутентификации КриптоПро TLS и использует криптографические функции КриптоПро CSP для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером. Общее описание протокола приведено в документе «ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть».

Протокол TLS (RFC 2246) используется для защиты соединений в клиент-серверных технологиях.

5.1.4. Модуль cpverify

Модуль **cpverify** предназначен для контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на устройстве пользователя.

5.1.5. Модуль wipefile

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

5.1.6. Модуль cryptcp

Модуль предназначен для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов, а также запроса выдачи сертификатов Удостоверяющим Центром.

5.1.7. Модуль certmgr

Модуль может устанавливать, удалять, раскодировать, экспортировать и отображать сертификаты или CRL из файлового хранилища или ключевого контейнера.

5.1.8. Модуль stunnel

Модуль для создания защищённого TLS-соединения между клиентом и локальным или удалённым сервером.

5.2. Модули подсистемы программной СФК

5.2.1. Модуль libcapi20

Модуль libcapi20 используется для управления сертификатами открытых ключей, а также для обеспечения выполнения криптографических запросов на уровне интерфейса CryptoAPI v. 2.0. Интерфейс модуля libcapi20 является подмножеством интерфейса CryptoAPI v. 2.0.

5.2.2. Модуль librdrfat12

Модуль librdrfat12 используется для получения доступа к flash-носителям и разделу жесткого диска.

5.2.3. Библиотека librdrsup

Библиотека librdrsup обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей и уровень абстракции от операционной системы.

5.2.4. Модули датчиков случайных чисел

Библиотеки librdrdsrf и librdrrndmbio обеспечивают поддержку работы с внешней гаммой и БиоДСЧ соответственно.

5.2.5. Библиотека libcpasn1 поддержки формата ASN1

Библиотека libcpasn1 содержит функции преобразования структур данных в машинно-независимое представление.

6. Встраивание СКЗИ КриптоПро CSP в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 17 документа «ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть», документа «ЖТЯИ.00087-03 96 01. Руководство программиста» и п. 1.5 документа «ЖТЯИ.00087-03 30 01. Формуляр».

7. 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 СКЗИ ЖТЯИ.00087-03 91 01. Руководство администратора безопасности. Общая часть.

При эксплуатации СКЗИ на платформе SailfishOS при обработке конфиденциальной информации для конкретного мобильного устройства, работающего под управлением ОС SailfishOS, должны выполняться действующие в Российской Федерации требования по защите открытой (конфиденциальной) информации от утечки по техническим каналам. Данное требование не предъявляется в случае эксплуатации СКЗИ на платформе SailfishOS при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС SailfishOS, в помещениях, в которых ведутся переговоры секретного содержания или проводятся работы секретного характера, без проведения его специальных исследований и специальной проверки запрещаются.

При использовании СКЗИ «КриптоПро CSP» под управлением ОС SailfishOS необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом ставится задача не только обеспечить дополнительную защиту устройства и ОС от НСД, но и обеспечить бесперебойный режим работы и исключить возможности "отказа в обслуживании", вызванного внутренними причинами (например - переполнением файловых систем).

К организационно-техническим мерам относятся:

- обеспечение физической безопасности устройства;
- установка программных обновлений;
- организация процедуры резервного копирования и хранения резервных копий.

Дополнительные настройки SailfishOS касаются следующего:

- ограничение доступа пользователей и настройки пользовательского окружения;
- ограничение сетевых соединений;
- ограничения на запуск процессов и установку программ;
- ограничение количества "отправляемой наружу" системной информации;
- настройка подсистемы протоколирования и аудита.

7.1. Организационно-технические меры

1. Обеспечение физической безопасности устройства

Следует исключить возможность доступа неавторизованного персонала к устройству. Для этого необходимо либо осуществлять личный контроль за устройством, либо хранить его в запираемом сейфе.

Доступ персонала к устройству должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

2. Организация процедуры резервного копирования и хранения резервных копий

При определении регламента резервного копирования и хранения резервных копий следует обеспечить ответственное хранение резервных копий и определить процедуру выдачи резервных копий ответственному персоналу и уничтожения вышедших из употребления носителей.

Резервные копии должны храниться в запираемых сейфах либо в зашифрованном виде на ЭВМ.

Стандартными мерами по организации ответственного хранения носителей являются:

- маркировка носителей;

- составление описи хранимых носителей с указанием серийных (инвентарных) номеров, дат записи носителей, фамилией сотрудника, создавшего копию для каждого шкафа(сейфа);
- периодическая сверка описи и содержимого сейфов (шкафов);
- организация ответственного хранения и выдачи ключей от сейфов (шкафов);
- возможное опечатывание (опломбирование) сейфов(шкафов).

Уничтожение вышедших из употребления носителей должно производиться комиссией с составлением акта об уничтожении.

3. При использовании СКЗИ «КриптоПро CSP» на мобильных устройствах SailfishOS, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

4. Право доступа к мобильным устройствам SailfishOS с установленным ПО СКЗИ «КриптоПро CSP» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ «КриптоПро CSP».

5. На технических средствах, оснащенных СКЗИ «КриптоПро CSP», должно использоваться только лицензионное программное обеспечение фирм-производителей.

6. На компьютере, к которому подключается устройство, должны отсутствовать средства разработки и отладки ПО. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ «КриптоПро CSP».

7. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ «КриптоПро CSP», по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях. Также необходимо обеспечить невозможность использования устройства с установленным СКЗИ посторонним лицам, не являющимися пользователями устройства.

8. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро CSP» после ввода ключевой информации.

9. Необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование устройства или на SailfishOS.

10. После инсталляции SailfishOS следует установить все рекомендованные производителем операционной системы программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

7.2. Дополнительные настройки SailfishOS и операционных систем, к которым подключается устройство

Индивидуальная настройка SailfishOS

В настройках SailfishOS в разделе «Безопасность – Блокировка устройства» необходимо включить пароли. Необходимо задать сложность пароля и настройки для количества попыток ввода пароля, соответствующие политике безопасности.

Корпоративная настройка SailfishOS

Корпоративная настройка SailfishOS может быть выполнена средствами набора управления мобильными устройствами (англ. Mobile device management, MDM). Данные средства не поставляются в комплекте с операционной системой, но могут работать с ОС SailfishOS путём использования предусмотренного системного API.

Путём создания профилей средствами MDM или в индивидуальном порядке в рамках корпоративной настройки на каждом устройстве SailfishOS, на котором эксплуатируется СКЗИ «КриптоПро CSP», должно быть применены следующие параметры:

a) На вход в устройство должен быть установлен пароль со следующими настройками:

- максимальный срок действия пароля не должен превышать 3 месяца;
- устанавливаемый пароль должен не совпадать с последними 6 использованными паролями;
- сложность пароля и настройки для удаления данных в случае неправильного ввода пароля должны соответствовать политике безопасности организации.

b) Должны быть отключены все разрешения, которые не являются необходимыми для выполнения работы. Должна быть отключена возможность установки приложений. Если эта возможность необходима для работы, её необходимо оставить, но настроить ограничения через средства MDM (см. ниже).

c) Если в организации имеется сервер для управления мобильными устройствами (MDM server), то необходимо настроить подключение к нему. Сервер может быть использован для получения настроек (в том числе новых профилей настроек) и приложений.

Настройка ОС, к которой подключается устройство

1. Выполните рекомендации по дополнительной настойке ОС из руководства администратора безопасности для соответствующей ОС.

2. Если на устройстве хранятся закрытые ключи, резервные копии устройства, сделанные при помощи встроенных средств SailfishOS, то они должны быть зашифрованы. Для зашифрования под управлением ОС Windows может быть использовано ПО КриптоПро EFS.

8. Требования по криптографической защите

Должны выполняться требования:

1. Использования только лицензионного системного программного обеспечения.

2. Раздела 16 документа ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

3. Перед началом работы должен быть проведен контроль целостности с помощью вызова /etc/init.d/cprocsp check. Контролем целостности должны быть охвачены файлы, указанные в п. 15.

4. Настройки операционной системы для работы с СКЗИ по п.7.2.

5. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.

6. Исключения из программного обеспечения мобильного устройства с установленным СКЗИ средств отладки.

7. Пароль, используемый для аутентификации пользователей, должен содержать не менее 8 символов алфавита мощности не менее 10. Периодичность смены пароля – не реже одного раза в 3 месяца.

8. Периодичности тестового контроля криптографических функций - 10 минут (выполняется автоматически).

9. Ежесуточной перезагрузки мобильного устройства.

10. Периодичности останова мобильного устройства - 1 месяц.

11. Запрещается использовать режим простой замены (ECB) ГОСТ 28147-89 для шифрования информации, кроме ключевой.

12. Должно даваться предупреждение о том, что при использовании режима шифрования CRYPT_SIMPLEMIX_MODE материал, обрабатываемый на одном ключе, автоматически ограничивается величиной 4 MB.

13. Должно быть запрещено использование СКЗИ для защиты телефонных переговоров без принятия в системе мер по защите от информативности побочных каналов, специфических при передаче речи.

14. При эксплуатации СКЗИ необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

15. Контролем целостности должны быть охвачены файлы:

/opt/cprocsp/bin/arm/certmgr
/opt/cprocsp/bin/arm/cpverify
/opt/cprocsp/bin/arm/cryptcp
/opt/cprocsp/bin/arm/csptest
/opt/cprocsp/bin/arm/csptestf
/opt/cprocsp/bin/arm/der2xer
/opt/cprocsp/bin/arm/genkpim
/opt/cprocsp/bin/arm/inittst
/opt/cprocsp/bin/arm/wipefile
/opt/cprocsp/sbin/arm/cpconfig
/opt/cprocsp/sbin/arm/mount_flash.sh
/opt/cprocsp/sbin/arm/unreg_prov_type_name.sh
/opt/cprocsp/lib/arm/libasn1data_XER.so.4.0.4
/opt/cprocsp/lib/arm/libcapi10.so.4.0.4
/opt/cprocsp/lib/arm/libcapi20.so.4.0.4
/opt/cprocsp/lib/arm/libcpalloc.so.0.0.0
/opt/cprocsp/lib/arm/libcpasn1.so.4.0.4

/opt/cprocsp/lib/arm/libcpext.so.4.0.4
/opt/cprocsp/lib/arm/libcplib.so.4.0.4
/opt/cprocsp/lib/arm/libcpui.so.4.0.4
/opt/cprocsp/lib/arm/libcsp.so.4.0.4
/opt/cprocsp/lib/arm/libenroll.so.4.0.4
/opt/cprocsp/lib/arm/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/arm/librdrfat12.so.4.0.4
/opt/cprocsp/lib/arm/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/arm/librdrsup.so.4.0.4
/opt/cprocsp/lib/arm/libssp.so.4.0.4
/opt/cprocsp/lib/arm/libsspdrv.a
/opt/cprocsp/lib/arm/liburlretrieve.so.4.0.4

Приложение 1. Контроль целостности программного обеспечения

В дополнение к дистрибутиву поставляются скриптовые файлы integrity.sh, запуском которых можно убедиться в целостности дистрибутива до его установки.

Программное обеспечение СКЗИ имеет средства обеспечения контроля целостности ПО СКЗИ, которые выполняются периодически.

Если в результате периодического контроля целостности появляются сообщения о нарушении целостности контролируемого файла, пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО СКЗИ «КриптоПро CSP» с дистрибутива, или системное ПО.

Модуль cpverify позволяет осуществлять контроль целостности установленного программного обеспечения. Контроль целостности файлов осуществляется периодически (несколько раз в сутки) или при ручном запуске программы контроля целостности, а также динамически для уже загруженных исполняемых модулей.

cpverify filename [-alg algid] [hashvalue] [-inverted_halfbytes <inv>] - проверка целостности файла с именем filename по алгоритму algid. Если не указан параметр hashvalue, то значение хэш-функции для сравнения берется из файла <filename.hsh>. Параметр algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512. Если algid не указан, то используется GR3411. [-inverted_halfbytes <inv>] указывается, если полубайты в hashvalue переверуты. По-умолчанию inv устанавливается в 1 для GR3411 и в 0 для GR3411_2012_256 и GR3411_2012_512.

cpverify -mk filename [-alg algid] [-inverted_halfbytes <inv>] - вычисление значения хэш функции для файла с именем filename. Параметр algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512. Если algid не указан, то используется GR3411. [-inverted_halfbytes <inv>] указывается, если необходимо перевернуть полубайты в hashvalue. По-умолчанию inv устанавливается в 1 для GR3411 и в 0 для GR3411_2012_256 и GR3411_2012_512.

cpverify -file_sign filename -cont cont_name [-pin password][-provname Provname] [-provtype Provtype] - подписывает файл с именем filename с помощью ключа, взятого из контейнера с именем cont_name. Поле password - пароль защиты контейнера. Поля Provname и Provtype указывают, какой провайдер необходимо использовать. Поле Provtype может принимать значения 75,80 и 81. Если Provtype не указан, то используется 75.

cpverify -file_verify filename [signval] -timestamp date - Проверяет подпись файла с именем filename. Если signval не указан, то значение для сравнения берется из файла <filename>.sgn. В поле date необходимо указать дату, когда подпись была создана, в формате dd.mm.yyyy.

Приложение 2. Управление протоколированием

Для включения/отключения значения log используйте:

Для задания уровня протоколирования
/opt/cprocsp/sbin/arm/cpconfig –loglevel cpcsp -mask <уровень протоколирования>
Для задания формата протокола зарегистрированных событий
/opt/cprocsp/sbin/arm/cpconfig –loglevel cpcsp -format <формат протокола>
Для просмотра маски текущего уровня и формата протокола
/opt/cprocsp/sbin/arm/cpconfig –loglevel cpcsp -view

Значением параметра <уровень протоколирования> является битовая маска:

N_DB_ERROR = 0x1 # сообщения об ошибках
N_DB_LOG = 0x8 # сообщения о вызовах

Значением параметра <формат протокола> является битовая маска:

DBFMT_MODULE = 0x1 # выводить имя модуля
DBFMT_THREAD = 0x2 # выводить номер нитки
DBFMT_FUNC = 0x8 # выводить имя функции
DBFMT_TEXT = 0x10 # выводить само сообщение
DBFMT_HEX = 0x20 # выводить HEX дамп
DBFMT_ERR = 0x40 # выводить GetLastError

Лист регистрации изменений

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					