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 Linux

ЖТЯИ.00087-03 91 03
Листов 31

2018 г.

© ООО «КРИПТО-ПРО», 2000-2018. Все права защищены.

Авторские права на средства криптографической защиты информации типа КриптоПро CSP и эксплуатационную документацию к ним зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 4.0 R4; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "КРИПТО-ПРО" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

Аннотация

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

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

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратные среды

СКЗИ «КриптоПро CSP» v 4.0 R4 под управлением ОС типа Linux используется в следующих программно-аппаратных средах:

Linux Standard Base ISO/IEC 23360 (ia32, x64), программно-аппаратные среды, удовлетворяющие стандарту LSB 4.x (https://www.linuxbase.org/lsb-cert/productdir.php?by_lsb):

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);
ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);
ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64);
КП «ОС «СинтезМ-К» (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, MIPS);
ОС Лотос (x86, x64);
Astra Linux Special Edition, Common Edition (x64, MIPS, Эльбрус);
МСВСфера 6.3 Сервер (x64, ARM64).
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);
Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14 (x64).

Со сроками эксплуатации операционных систем, в среде которых функционирует СКЗИ, можно ознакомиться по следующим адресам:

http://wiki.centos.org/About/Product
https://fedoraproject.org/wiki/Releases/
http://support.novell.com/lifecycle/
http://support.novell.com/lifecycle/lcSearchResults.jsp?st=-1&sl=-1&sg=1&pid=1000
http://mandriva.ru/resheniya/uslugi/cikl_jizni_produktov/
http://www.mvista.com/support_lifecycle.php

1.2. Ключевые носители

В качестве ключевых носителей закрытых ключей и ключей ЭП могут использоваться:

- ГМД 3,5", USB диски;
- Смарткарты GEMALTO (GemSim1, GemSim2, Optelio, OptelioCL, OptelioCL2, Native);
- eToken, Jacarta;
- USB-токены Рутокен ЭЦП (Flash, Bluetooth), Рутокен Lite Novacard;
- Смарткарты Рутокен Lite SC, Рутокен ЭЦП SC;
- Rutoken S;
- Novacard;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- Смарткарта УЭК;
- Токен++ Lite;
- ESMART Token;
- Смарткарты Алиот INPASPOT Series, SCOne Series;
- Rosan;
- Раздел HDD ПЭВМ (в Windows - реестр);

	1. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.
	1. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-03 91 01. Руководство администратора безопасности общая часть).
	2. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене.
	3. Использование носителей других типов - только по согласованию с ФСБ России.

2. Установка дистрибутива ПО СКЗИ

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

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

В ОС Linux 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-3.6.1-4.noarch.rpm**

Для удаления пакета используется команда:

rpm -e <имя_пакета>

Например: **rpm -e lsb-cprocsp-base-3.6.1-4**

Имя пакета может не включать версию.

Например: **rpm -e lsb-cprocsp-base**

На ОС, основанных на Debian (Debian/Ubuntu), для установки пакетов используется команда:

alien -kci <файл_пакета>

Например: **alien -kci ./lsb-cprocsp-base-3.6.1-4.noarch.rpm**

На ОС, основанных на Debian (Debian/Ubuntu), для установки 32-битных пакетов на 64-битную ОС используется команда:

dpkg-architecture -ai386 -c alien -kci <файл_пакета>

Возможно, потребуется установить программу alien из стандартного репозитория ОС.

На ОС, основанных на Debian (Debian/Ubuntu), для удаления пакетов используется команда:

dpkg -P <имя_пакета_без_версии>

Например: **dpkg -P lsb-cprocsp-base**

Файлы из пакетов устанавливаются в /opt/cprocsp.

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.

Пакеты могут быть независимыми от архитектуры (noarch в имени файла пакета), тогда они устанавливаются на любую архитектуру. Пакеты могут быть предназначены для архитектуры IA32 (i486 в имени файла пакета), а также для архитектуры AMD64 (x86_64 в имени файла пакета), тогда они устанавливаются на ОС, собранную под соответствующую архитектуру. Часто 64-битные ОС одновременно поддерживают и 32-битные приложения, и 64-битные, тогда при необходимости можно устанавливать оба комплекта. Исключением являются драйверы – они устанавливаются в точном соответствии с архитектурой ядра ОС.

В ОС Linux модули ядра не обладают бинарной совместимостью, они привязаны к конкретной версии ядра ОС. Поэтому модуль ядра поставляется в виде пакета .src.rpm. Такой тип пакета позволяет собрать модуль для нужной версии ядра. Для его установки следует при помощи rpmbuild собрать из пакета .src.rpm обычный пакет .rpm, а затем установить пакет .rpm так же как остальные пакеты.

На большинстве дистрибутивов сборку пакета .rpm можно осуществить командой:

rpmbuild --rebuild --define "kernel_release `uname -r`" <путь к файлу пакета>

Для сборки требуется, чтобы на машине были установлены средства сборки (компилятор), а также заголовочные файлы ядра. Заголовочные файлы ядра должны находиться в /lib/modules/ и обычно их можно установить в составе соответствующего пакета из репозитория дистрибутива.

Так как наличие средств отладки и разработки на системах, в которых эксплуатируется СКЗИ, недопустимо, администратор (разработчик ПКЗИ) должен собрать пакет на специальном выделенном рабочем месте и обеспечивать его доверенную установку в целевую систему.

Таблица 2.1 - Зависимости и назначения пакетов (для простоты описаны 32-битные пакеты).

Имя пакета	Зависимости	Назначение пакета
Пакеты для предварительной установки		
cprocsp-compat-altlinux		Пакет совместимости с ОС AltLinux, утснаваливается первым – до lsb-cprocsp-base.
cprocsp-compat-splat		Пакет совместимости с ОС SPLAT, устанавливается первым – до lsb-cprocsp-base.
sobol		Драйвер для Соболя. Требуется при наличии устройства.
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-capilite	lsb-cprocsp-rdr	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS…).
lsb-cprocsp-kc1	lsb-cprocsp-rdr	Провайдер КС1.
lsb-cprocsp-kc2	lsb-cprocsp-rdr	Провайдер КС2, устанавливается только там, где в этом есть необходимость. В этом случае lsb-cprocsp-kc1 не ставится.
Дополнительные пакеты		
cprocsp-rdr-gui	lsb-cprocsp-rdr, Motif, X11	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги.
cprocsp-rdr-pcsc	lsb-cprocsp-rdr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт (РИК, Оскар, Магистра…).
lsb-cprocsp-rdr-sobol	lsb-cprocsp-rdr, sobol	Модуль поддержки Соболя.
lsb-cprocsp-devel	lsb-cprocsp-base	Пакет для разработчика.
cprocsp-drv	lsb-cprocsp-base	Драйверная библиотека.
cprocsp-drv-devel	lsb-cprocsp-devel	Пакет для разработчика драйверов.
cprocsp-stunnel	lsb-cprocsp-base	Универсальный SSL/TLS туннель.
cprocsp-rdr-emv	lsb-cprocsp-rdr	Модуль поддержки EMV

3. Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Linux необходимо:

- запомнить текущую конфигурацию CSP:
  - набор установленных пакетов;
  - настройки провайдера (для простоты можно сохранить /etc/opt/cprocsp/config[64].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[64].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/<название_архитектуры>. Если установлены пакеты СКЗИ для двух архитектур, например, ia32 и x64, то действия по настройке нужно проводить дважды – для каждой архитектуры cpconfig-ом из соответствующей папки.

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 образ дискеты на жестком диске.

Для просмотра списка настроенных считывателей:

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

Считыватель дискет не устанавливается по умолчанию, так как при отсутствии дискеты в дисководе перечисление контейнеров сильно замедляется. Для добавления считывателя дискет:

```
# ./cpconfig -hardware reader -add FAT12_0 -name "Floppy Drive"
```

Для просмотра списка настроенных ДСЧ:

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

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 графического БиоДСЧ требуется пакет cprocsp-rdr-gui и X-сервер, кроме того он работает только с КС1 провайдером. Для добавления графического БиоДСЧ:

```
# ./cpconfig -hardware rndm -add bio_gui -level 4 -name "GUI 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
```

Также надо скопировать файлы с данными, полученными на "АРМ выработки внешней гаммы", 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
```

Для работы со считывателем PC/SC требуется пакет cprocsp-rdr-pcsc. После подключения считывателя узнайте имя устройства:

```
# /opt/cprocsp/bin/ia32/csptest -card -enum
Gemplus  GemPC  Twin 00 00
Total:
[ErrorCode:  0x00000000]
```

Для добавления считывателя используйте это имя:

```
# ./cpconfig -hardware reader -add "Gemplus  GemPC  Twin 00 00"
```

Для получения подробной справки по cpconfig:

```
# ./cpconfig -help
# ./cpconfig -hardware –help
```

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
capi20 - CryptoAPI 2.0
capilite - CAPILite
libcspr
cryptsrv - служба хранения ключей (КС2)
libssp - TLS
cppkcs11 - PKCS11
cpdrv - драйвер
dmntcs
```

4.5. Настройка криптопровайдера по умолчанию

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. Установка сопутствующих пакетов

Для передачи по сети запросов на сертификаты, CRL и т.п., а также для поддержки дополнительных ключевых считывателей и носителей может потребоваться установка дополнительных пакетов.

Если сопутствующие пакеты скачиваются из Интернета, необходимо подтвердить их целостность, проверив подпись или хэш. Если источник не обеспечивает такие механизмы, допускается использование пакетов только с диска с дистрибутивом СКЗИ, где эти механизмы используются. На диске пакеты лежат в папке \extra.

На сертифицированные ФСТЭК дистрибутивы ALTLinux запрещается ставить пакеты из сети (например, с использованием apt-get).

5.1. Библиотека libcurl

Используется для передачи запросов на сертификаты, CRL и т.п. по сети.

С сайта разработчика проекта http://curl.haxx.se/ можно скачать пакет с исходными текстами для самостоятельной сборки. Как правило, там же есть 32-битные версии бинарных пакетов и иногда 64-битные.

Проще всего поставить библиотеку встроенным менеджером пакетов.

На ALTLinux, Debian, Ubuntu:

```
# apt-get install curl
```

На CentOS, Fedora, LinuxXP, RedHat:

```
# yum install curl
```

На SuSE:

```
# yast -i curl
```

После установки библиотек надо зарегистрировать пути к ним. Например:

```
# /opt/cprocsp/sbin/ia32/cpconfig -ini '\config\apppath' -add string libcurl.so /usr/local/lib/libcurl.so
# /opt/cprocsp/sbin/amd64/cpconfig -ini '\config\apppath' -add string libcurl.so /usr/local/lib/64/libcurl.so
```

6. Состав и назначение компонент ПО СКЗИ

6.1. Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

libcsp – динамически загружаемая библиотека «КриптоПро CSP».
libcspr - библиотека работы с удалённым «КриптоПро CSP».
drvcsp – динамически загружаемый модуль ядра.
libssp – библиотека поддержки модуля сетевой аутентификации «КриптоПро TLS».
cpverify – модуль контроля целостности.
wipefile – модуль удаления файлов вместе с содержимым.
cryptcp - приложение для подписи и шифрования файлов
certmgr - утилита командной строки для управления
сертификатами, списками отзыва сертификатов (CRL) и хранилищами.
stunnel - приложение для создания TLS-туннеля

В названиях дистрибутивов СКЗИ используются следующие обозначения:
CPRO – префикс;
csp – криптопровайдер;
drv – загружаемый модуль ядра ОС;
[d] - опционально – указывает на документацию (тестовые примеры);
i386 – платформа Intel.

6.1.1. Библиотека libcsp

Библиотека **libcsp** реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ.

6.1.2. Библиотека libcspr

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

6.1.3. Драйверная библиотека drvcsp

Библиотека **drvcsp**, используемая в качестве динамически загружаемого модуля ядра ОС, реализует целевые функции криптографической защиты информации (кроме формирования ЭП) и работу с ключами.

6.1.4. Модули сетевой аутентификации КриптоПро TLS

Модуль **libssp** обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS. 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.

Программное обеспечение «КриптоПро TLS» является реализацией протокола TLS и использует криптографические функции КриптоПро CSP для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером.

6.1.5. Модуль cpverify

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

6.1.6. Модуль wipefile

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

6.1.7. 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.

6.1.8. Модуль certmgr

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

6.1.9. Модуль stunnel

Модуль для создания TLS-туннеля, предназначенного для создания TLS защищенного соединения между клиентом и локальным (Iinetd-запускаемым) или удаленным сервером.

6.2. Модули подсистемы программной СФК

6.2.1. 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 capilite является подмножеством интерфейса CryptoAPI v. 2.0.

6.2.2. Библиотека librdrrdr

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

6.2.3. Модули доступа к конкретным типам ключевых носителей и считывателей:

- **librdrfat12** к дисководу и дискете 3.5" и разделу жесткого диска;
- **librdrpcsc** к считывателям смарткарт и eToken, поддерживающим интерфейс PC/SC;
- **librdremv** к ключевым носителям EMV и Gemalto.

6.2.4. Библиотека librdrsup

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

6.2.5. Модули датчиков случайных чисел

Библиотеки librdrrndm и librdrrndmbio обеспечивают поддержку работы с физическим ДСЧ программно-аппаратного комплекса защиты от НСД и БиоДСЧ соответственно.

6.2.6. Библиотека libasn1data поддержки протокола ASN1

Библиотека libasn1data содержит функции преобразования структур данных в машинно-независимое представление.

7. Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ «КриптоПро CSP» v 4.0 R4 в прикладное программное обеспечение должны выполняться требования раздела 17 документа «ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» и документа «ЖТЯИ.00087-03 96 01. Руководство программиста».

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

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме разделов 15 и 16 документа «ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть».

8.1. Общие меры защиты от НСД ПО с установленными СКЗИ для ОС Linux

Под управлением UNIX-подобных операционных систем СКЗИ «КриптоПро CSP» может использоваться с программным обеспечением:

– Trusted TLS (Digt).

При использовании СКЗИ под управлением ОС Linux необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом должна решаться задача как обеспечения дополнительной защиты сервера и ОС от НСД, так и обеспечения бесперебойного режима работы и исключения «отказа в обслуживании», вызванного внутренними причинами (например - переполнением файловых систем).

К организационно-техническим мерам относятся:

– обеспечение физической безопасности ПЭВМ (сервера);

– установка программных обновлений;

– организация процедуры резервного копирования и хранения резервных копий.

– Дополнительные настройки ОС Linux касаются следующего:

– ограничение доступа пользователей и настройки пользовательского окружения;

– ограничение сетевых соединений;

– ограничения при монтировании файловых систем;

– ограничения на запуск процессов;

– контроль загрузки ОС и контроль целостности системного и прикладного программного обеспечения должен обеспечиваться при помощи программно-аппаратного комплекса защиты от НСД (см. соответствующий раздел в документе «ЖТЯИ.00087-03 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть»), что означает:

1. обеспечение контроля доступа при помощи идентификации пользователя с использованием системы Touch Memory;
2. выполнение загрузки с фиксированного носителя после его контроля;
3. обеспечение контроля целостности ОС и прикладного программного обеспечения до загрузки на загрузочном диске и других подключенных дисках.

– В случае отсутствия помощи программно-аппаратного комплекса защиты от НСД контроль целостности проводится с помощью утилиты cpverify.

– дополнительные настройки ядра ОС;

– настройка сетевых сервисов;

– ограничение количества "видимой извне" информации о системе;

– настройка подсистемы протоколирования и аудита.

8.1.1. Организационно-технические меры

1. С целью исключения возможности загрузки ОС, отличной от установленной на HDD ПЭВМ, ПЭВМ и устройства загрузки должны быть опечатаны. Должен быть обеспечен необходимый контроль целостности печатей.

2. Обеспечение физической безопасности сервера

Следует исключить возможность доступа неавторизованного персонала к консоли, системе питания и дополнительным устройствам, подключенным к защищаемому серверу путем установки оборудования в специально выделенное и запираемое помещение (аппаратную или серверную комнату).

Для исключения сбоев компьютера, вызванных отключением электропитания, необходимо обеспечить электропитание сервера от источника бесперебойного питания достаточной мощности. Как минимум, мощности батарей источника бесперебойного питания должно хватать на время достаточное для корректного автоматического завершения работы сервера.

3. Организация процедуры резервного копирования и хранения резервных копий.

При определении регламента резервного копирования и хранения резервных копий следует обеспечить ответственное хранение резервных копий в запираемых сейфах (шкафах) и определить процедуру выдачи резервных копий ответственному персоналу и уничтожения вышедших из употребления носителей (лент, однократно записываемых дисков и пр.).

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.

4. В системе регистрируется один пользователь, обладающий правами администратора, носящий имя root, на которого возлагается обязанность конфигурировать ОС Linux, настраивать безопасность ОС Linux, а также конфигурировать ПЭВМ, на которую установлена ОС Linux.

5. Для пользователя root выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 8 символов, среди символов пароля должны встречаться заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только администратору.

6. Пользователю root доступны настройки всех пользователей ОС Linux, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в ОС Linux, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Linux, не являющийся пользователем root, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему пользователем root.

7. Всех пользователей ПЭВМ, которые не пользуются данной системой, и всех стандартных пользователей, которые создаются в ОС Linux во время установки (таких, как "sys", "uucp", "nuucp", и "listen"), кроме пользователя root, следует удалить.

8. В ОС Linux существуют исполняемые файлы, которые запускаются с правами пользователя root. Эти файлы имеют установленный флаг SUID. Пользователь root должен определить, каким из этих файлов в рамках определенной в организации политики безопасности не требуется запуск с административными полномочиями, и с помощью сброса флага SUID должен свести количество таких файлов к минимуму. Запуск оставшихся файлов с установленным флагом SUID должен контролироваться пользователем root.

9. При использовании СКЗИ «КриптоПро CSP» на ПЭВМ, 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.

10. Право доступа к рабочим местам 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».

11. На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

12. В BIOS определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на HDD: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

13. Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств и PCI-устройств. Для исключения этой возможности вход в BIOS ЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю пользователя root. Пароль для входа в BIOS должен быть известен только пользователю root и быть отличным от пароля пользователя root для входа в ОС Linux.

14. До загрузки ОС должен быть реализован контроль целостности файлов, критичных для загрузки ОС и программы CPVERIFY.

15. При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ «КриптоПро CSP», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ с использованием программы CPVERIFY.

16. Средствами BIOS должна быть исключена возможность работы на ЭВМ, если во время его начальной загрузки не проходят встроенные тесты ЭВМ (POST).

17. На ПЭВМ устанавливается только одна ОС. На ПЭВМ не устанавливаются средств 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». Следует избегать попадания в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии root.

18. Должно быть ограничено (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время.

19. Должно быть реализовано физическое затирание содержимого удаляемых файлов с использованием программы Wipefile из состава СКЗИ.

20. Должны быть отключены все неиспользуемые сетевые протоколы.

21. В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть отключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, в прикладных программах без проведения дополнительных тематических исследований.

22. 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.

23. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ «КриптоПро CSP» после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

24. Из состава системы должно быть исключено оборудование, которое может создавать угрозу безопасности ОС Linux. Также необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование ПЭВМ или ОС Linux.

25. После инсталляции ОС Linux следует установить все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

26. На все директории, содержащие системные файлы ОС Linux и каталоги СКЗИ, необходимо установить права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись.

27. В связи с тем, что аварийный дамп оперативной памяти может содержать криптографически опасную информацию, в прикладных программах, использующих СКЗИ, следует отключить возможность его создания с помощью функции setrlimit с параметром RLIMIT_CORE=0.

28. В ОС Linux используется виртуальная память. Область виртуальной памяти должна быть организована на отдельном HDD. По окончании работы СКЗИ содержимое виртуальной памяти должно затираться с использованием средств ОС. В случае аварийного останова ПЭВМ, при следующей загрузке необходимо в режиме "single user" очистить область виртуальной памяти программой wipefile, входящей в состав СКЗИ КриптоПро CSP. В случае выхода из строя HDD, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а HDD считается не подлежащим ремонту. Этот HDD уничтожается по правилам уничтожения ключевых носителей.

8.1.2. Дополнительные настройки ОС Linux

Настройки ОС Linux выполняются путем редактирования (удаления, добавления) различных конфигурационных и командных файлов.

Для сохранения возможности «откатить» внесенные изменения следует сохранять модифицируемые файлы в «безопасном» месте (на внешнем носителе или на не монтируемой автоматически файловой системе).

Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

1. В файле /etc/login.defs следует установить следующие директивы:

PASS_MAX_DAYS=30 (параметр задаёт максимальное время использования пароля)

PASS_MIN_DAYS=30 (параметр задаёт минимальное количество дней между сменами пароля)

PASS_MIN_LEN=6 (устанавливает минимальную длину пароля)

2. В файле /etc/profile установить значения umask=022 (параметр задает маску создания файла по-умолчанию)

3. Для пользователя root установить маску режима создания файлов 077 или 027:

umask 077 (umask 027);

4. Отредактировать файл /etc/shells и поместить в него имена только для тех исполняемых файлов оболочек, которые установлены в системе. По-умолчанию, содержимое файла /etc/shells может быть таким:

/bin/csh

/bin/tcsh

/bin/sh

/bin/bash

5. Удалить файл (если он существует) /.rhosts.

6. Удалить содержимое файла /etc/host.equiv.

7. Отредактировать файл /etc/pam.conf с целью запрета rhosts-аутентификации. Выполняется комментированием всех строк, содержащих подстроку "pam_rhosts_auth.so".

8. Проверить идентификаторы пользователя и группы для всех пользователей, перечисленных в файле /etc/passwd. Следует убедиться, что не существует пользователей, имеющих идентификатор пользователя 0 и идентификатор группы 0 кроме, возможно, пользователя root.

9. Создать перечень программ, которые запускаются с правами администратора, и контролировать его неизменность;

10. Запретить регистрацию в системе пользователей, имеющих следующие «служебные имена»:

daemon	uucp
bin	nuucp

sys	listen
adm	listen
lp	nobody
smtp	noaccess

Действие выполняется путем указания в файле /etc/passwd строки '/bin/false' в поле shell-программы и указания символа 'x' в поле пароля.

Ограничения при монтировании файловых систем

Ограничения при монтировании файловых систем реализуются редактированием файла /etc/fstab:

Установить опцию nosuid при монтировании файловой системы /var.

При инсталляции системы следует выделить для файловых систем /, /usr, /usr/local, /var разные разделы диска для предотвращения переполнения критичных файловых систем (/, /var) за счет, например, пользовательских данных и обеспечения возможности монтирования файловой системы /usr в режиме «только для чтения».

Ограничения на запуск процессов

Следует ограничить использование в системе планировщика задач cron и средств пакетной обработки заданий. Для нормального функционирования системы минимально необходимым является разрешение использования планировщика задач cron и средств пакетной обработки заданий только пользователю root. Для этого следует выполнить следующие команды (от имени суперпользователя):

```
echo root > /etc/cron.allow
echo root > /etc/at.allow
```

Настройка сетевых сервисов

Настройка сетевых сервисов заключается в следующем:

Следует ограничить функциональность демона управления сетевыми соединениями xinetd. Действие заключается в редактировании файла /etc/xinetd.conf и файлов в каталоге /etc/xinetd.d. Как минимум, следует запретить следующие сервисы:

echo	systat
discard	netstat
daytime	tftp
chargen	telnet
finger	nfsd

1. Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора, необходимо в стартовые файлы поместитть команду /sbin/sysctl –w net.ipv4.ip_forward = 0;

2. Следует запретить прием из внешней сети «широковещательных» (broadcast) пакетов, а также передачу ответов на принятые «широковещательные» пакеты;

3. Запретить суперпользователю доступ по ftp, для этого добавить «root» в файл /etc/ftpusers;

4. Запустить процедуру регистрации запуска процессов (accounting) выполнением команды /sbin/accton;

5. Если планируется использовать на настраиваемом сервере сервис FTP, то следует создать (отредактировать) файл /etc/ftpusers со списком пользователей, для которых запрещен доступ к серверу по протоколу FTP. Файл имеет текстовый формат и должен содержать по одному имени пользователя в строке. В списке «запрещенных" пользователей, как минимум, должны быть перечислены следующие имена пользователей:

daemon	uucp
bin	nuucp
sys	listen
adm	listen
lp	nobody
smtp	noaccess

6. Для ограничения доступа к системным файлам для непривилегированных пользователей, из командной строки следует выполнить следующие команды:

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 444 /etc/default/login
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
```

7. Также следует обнулить флаг SGID для некоторых исполняемых файлов:

```
chmod g-s /bin/mail
chmod g-s /usr/bin/write
chmod g-s /bin/netstat
chmod g-s /usr/sbin/nfsstat
chmod g-s /usr/bin/ipcs
chmod g-s /sbin/arp
chmod g-s /bin/dmesg
chmod g-s /sbin/swapon
chmod g-s /usr/bin/wall
```

Ограничение количества «видимой извне» информации о системе

Обычно, начальную информацию о системе потенциальный нарушитель получает из системных приглашений, выдаваемых сетевыми службами сервера (telnet-сервер, ftp-сервер и пр.).

Поэтому, к мерам по ограничению количества «видимой извне» информации о системе относятся:

– Отказ от стандартного «заголовка», выводимого сервером ftp при ответе пользователю. Достигается указанием в файле /etc/default/ftpd следующих директив: BANNER="";

– Редактирование файлов /etc/issue, /etc/ftp-banner и /etc/motd с целью разъяснения пользователям правил и политики доступа к серверу ftp.

Настройка подсистемы протоколирования и аудита

Следует удостовериться, что только пользователь root имеет доступ на запись для следующих файлов:

/var/log/authlog
/var/log/syslog
/var/log/messages
/var/log/sulog
/var/log/utmp
/var/log/utmpx

Если на настраиваемом сервере используется web-сервер, то следует убедиться, что только "владелец" процесса httpd имеет доступ на запись к протоколам httpd

Ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команд su и sudo – предоставления пользователю административных полномочий.

Следует протоколировать попытки использования программ su и sudo. Для этого, в файл /etc/syslog.conf следует добавить запись:

auth.notice /var/log/authlog

или

auth.notice /var/log/authlog, @loghost.

Вторая строка аналогична первой, но указывает, что протокол дополнительно передается на сервер сбора протоколов.

Следует обеспечить протоколирование неуспешных попыток регистрации в системе в локальном протоколе. Для этого, следует выполнить следующие команды:

touch /var/adm/loginlog
chown root /var/adm/loginlog
chgrp root /var/adm/loginlog
chmod 644 /var/adm/loginlog

Для протоколирования сетевых соединений, контролируемых демоном xinetd (включая дату/время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), в файл /etc/syslog.conf следует добавить запись:

daemon.notice /var/log/syslog

8.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

Должны быть приняты меры по защите 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.

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

В случае планирования размещения СКЗИ в помещениях, где присутствует речевая, акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, технические средства иностранного производства, на которых функционируют программные модули СКЗИ, должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации».

9. Требования по криптографической защите

Должны выполняться требования:

1. Использование только лицензионного системного программного обеспечения.

2. Раздел 16 документа ЖТЯИ.00087-03 91 01. «Руководство администратора безопасности. Общая часть».

3. Перед началом работы должен быть проведен контроль целостности. Контролем целостности должны быть охвачены файлы, указанные в п. 14.

4. Настройка операционной системы для работы с СКЗИ по п. 8.1.2.

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

6. Исключение из программного обеспечения ПЭВМ 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. Периодичность тестового контроля криптографических функций - 10 минут.

9. Ежесуточная перезагрузка ПЭВМ.

10. Периодичность останова ПЭВМ с обязательной проверкой системы охлаждения процессорного блока ПЭВМ - 1 месяц.

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

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

13. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.

14. Контролем целостности должны быть охвачены файлы:

Linux (x86)

```
/opt/cprocsp/bin/ia32/curl
/opt/cprocsp/lib/ia32/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ia32/libcpcurl.a
/opt/cprocsp/lib/ia32/libcpcdrv_emul.a
/opt/cprocsp/bin/ia32/cp-genpsk.sh
/opt/cprocsp/bin/ia32/genpsk
/opt/cprocsp/lib/ia32/libike_gost.so.4.0.5
/opt/cprocsp/lib/ia32/libesp_gost.so.4.0.5
/opt/cprocsp/lib/ia32/librdremv.so.4.0.5
/opt/cprocsp/bin/ia32/list_pcsc
/opt/cprocsp/lib/ia32/librdrpcsc.so.4.0.5
/opt/cprocsp/lib/ia32/librdrric.so.4.0.5
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.5
/opt/cprocsp/sbin/ia32/stunnel_hsm
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/bin/ia32/cryptcp
/opt/cprocsp/bin/ia32/certmgr
/opt/cprocsp/bin/ia32/inittst
/opt/cprocsp/bin/ia32/csptestf
/opt/cprocsp/bin/ia32/der2xer
/opt/cprocsp/lib/ia32/libcapi20.so.4.0.5
/opt/cprocsp/lib/ia32/libcpext.so.4.0.5
/opt/cprocsp/lib/ia32/libasn1data_XER.so.4.0.5
```

```
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.5
/opt/cprocsp/lib/ia32/libsspdrv.a
/opt/cprocsp/lib/ia32/libssp.so.4.0.5
/opt/cprocsp/lib/ia32/libenroll.so.4.0.5
/opt/cprocsp/lib/ia32/liburlretrieve.so.4.0.5
/opt/cprocsp/lib/ia32/libcsp.so.4.0.5
/opt/cprocsp/lib/ia32/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/ia32/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/librdrrndm.so.4.0.5
/opt/cprocsp/lib/ia32/librdrsup.so.4.0.5
/opt/cprocsp/lib/ia32/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/ia32/librdrfat12.so.4.0.5
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.5
/opt/cprocsp/lib/ia32/libcpui.so.4.0.5
/opt/cprocsp/lib/ia32/libcpalloc.so.0.0.0
/opt/cprocsp/lib/ia32/libjemalloc.so.0.0.0
/opt/cprocsp/sbin/ia32/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ia32/cpconfig
/opt/cprocsp/sbin/ia32/mount_flash.sh
/opt/cprocsp/lib/ia32/librdrsbl.so.4.0.5
```

Linux (x64)

```
/opt/cprocsp/bin/amd64/curl
/opt/cprocsp/lib/amd64/libcpcurl.a
/opt/cprocsp/lib/amd64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/amd64/libcpcdrv_emul.a
/opt/cprocsp/bin/amd64/cp-genpsk.sh
/opt/cprocsp/bin/amd64/genpsk
/opt/cprocsp/lib/amd64/libike_gost.so.4.0.5
/opt/cprocsp/lib/amd64/libesp_gost.so.4.0.5
/opt/cprocsp/lib/amd64/librdremv.so.4.0.5
/opt/cprocsp/bin/amd64/list_pcsc
/opt/cprocsp/lib/amd64/librdrpcsc.so.4.0.5
/opt/cprocsp/lib/amd64/librdrric.so.4.0.5
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/opt/cprocsp/lib/amd64/librsaenh.so.4.0.5
/opt/cprocsp/sbin/amd64/stunnel_fork
/opt/cprocsp/sbin/amd64/stunnel_thread
/opt/cprocsp/sbin/amd64/stunnel_hsm
/opt/cprocsp/bin/amd64/cryptcp
/opt/cprocsp/bin/amd64/certmgr
/opt/cprocsp/bin/amd64/inittst
/opt/cprocsp/bin/amd64/csptestf
/opt/cprocsp/bin/amd64/der2xer
/opt/cprocsp/lib/amd64/libcapi20.so.4.0.5
/opt/cprocsp/lib/amd64/libcpext.so.4.0.5
/opt/cprocsp/lib/amd64/libasn1data.so.4.0.5
/opt/cprocsp/lib/amd64/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/amd64/libsspdrv.a
/opt/cprocsp/lib/amd64/libssp.so.4.0.5
/opt/cprocsp/lib/amd64/libenroll.so.4.0.5
/opt/cprocsp/lib/amd64/liburlretrieve.so.4.0.5
/opt/cprocsp/lib/amd64/libcsp.so.4.0.5
/opt/cprocsp/lib/amd64/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/amd64/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/amd64/cpverify
/opt/cprocsp/bin/amd64/wipefile
/opt/cprocsp/bin/amd64/csptest
```

```
/opt/cprocsp/lib/amd64/librdrrndm.so.4.0.5
/opt/cprocsp/lib/amd64/librdrsup.so.4.0.5
/opt/cprocsp/lib/amd64/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/amd64/librdrfat12.so.4.0.5
/opt/cprocsp/lib/amd64/libcapi10.so.4.0.5
/opt/cprocsp/lib/amd64/libcpui.so.4.0.5
/opt/cprocsp/lib/amd64/libcpalloc.so.0.0.0
/opt/cprocsp/lib/amd64/libjemalloc.so.0.0.0
/opt/cprocsp/sbin/amd64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/amd64/cpconfig
/opt/cprocsp/sbin/amd64/mount_flash.sh
/opt/cprocsp/lib/amd64/librdrsbl.so.4.0.5
```

Linux (ARM)

```
/opt/cprocsp/bin/arm/curl
/opt/cprocsp/lib/arm/libcpcurl.a
/opt/cprocsp/lib/arm/libcpcurl.so.4.2.0
/opt/cprocsp/sbin/arm/stunnel_hsm
/opt/cprocsp/sbin/arm/stunnel_thread
/opt/cprocsp/sbin/arm/stunnel_fork
/opt/cprocsp/bin/arm/cryptcp
/opt/cprocsp/bin/arm/certmgr
/opt/cprocsp/bin/arm/csptestf
/opt/cprocsp/lib/arm/libcapi20.so.4.0.5
/opt/cprocsp/lib/arm/libcpext.so.4.0.5
/opt/cprocsp/lib/arm/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/arm/libasn1data.so.4.0.5
/opt/cprocsp/lib/arm/libssp.so.4.0.5
/opt/cprocsp/lib/arm/libsspdrv.a
/opt/cprocsp/lib/arm/libenroll.so.4.0.5
/opt/cprocsp/lib/arm/liburlretrieve.so.4.0.5
/opt/cprocsp/lib/arm/libcsp.so.4.0.5
/opt/cprocsp/lib/arm/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/bin/arm/cpverify
/opt/cprocsp/bin/arm/wipefile
/opt/cprocsp/bin/arm/csptest
/opt/cprocsp/lib/arm/librdrrndm.so.4.0.5
/opt/cprocsp/lib/arm/librdrsup.so.4.0.5
/opt/cprocsp/lib/arm/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/arm/librdrfat12.so.4.0.5
/opt/cprocsp/lib/arm/libcapi10.so.4.0.5
/opt/cprocsp/lib/arm/libcpui.so.4.0.5
/opt/cprocsp/sbin/arm/unreg_prov_type_name.sh
/opt/cprocsp/sbin/arm/cpconfig
/opt/cprocsp/sbin/arm/mount_flash.sh
```

Linux (POWER)

```
/opt/cprocsp/bin/ppc64/curl
/opt/cprocsp/lib/lib64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/lib64/libcpcurl.a
/opt/cprocsp/lib/lib64/libcpcdrv_emul.a
/opt/cprocsp/bin/ppc64/cp-genpsk.sh
/opt/cprocsp/bin/ppc64/genpsk
/opt/cprocsp/lib/lib64/libike_gost.so.4.0.4
/opt/cprocsp/lib/lib64/libesp_gost.so.4.0.4
/opt/cprocsp/lib/lib64/librdremv.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/lib64/libxcpui.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_gui_fgtk.so.4.0.4
/opt/cprocsp/lib/lib64/libfgcpui.so.4.0.4
```

```
/opt/cprocsp/sbin/ppc64/xcpui_app
/opt/cprocsp/sbin/ppc64/fgtk_rndm_app
/opt/cprocsp/bin/ppc64/list_pcsc
/opt/cprocsp/lib/lib64/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/lib64/librdrric.so.4.0.4
/opt/cprocsp/sbin/ppc64/ccid_reg.sh
/opt/cprocsp/lib/lib64/librdruec.so.4.0.4
/opt/cprocsp/lib/lib64/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/lib64/librsaenh.so.4.0.4
/opt/cprocsp/sbin/ppc64/stunnel_thread
/opt/cprocsp/sbin/ppc64/stunnel_fork
/opt/cprocsp/sbin/ppc64/stunnel_hsm
/opt/cprocsp/bin/ppc64/cryptcp
/opt/cprocsp/bin/ppc64/certmgr
/opt/cprocsp/bin/ppc64/inittst
/opt/cprocsp/bin/ppc64/csptestf
/opt/cprocsp/bin/ppc64/der2xer
/opt/cprocsp/lib/lib64/libcapi20.so.4.0.4
/opt/cprocsp/lib/lib64/libcpext.so.4.0.4
/opt/cprocsp/lib/lib64/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/lib64/libasn1data.so.4.0.4
/opt/cprocsp/lib/lib64/libsspdrv.a
/opt/cprocsp/lib/lib64/libssp.so.4.0.4
/opt/cprocsp/lib/lib64/libenroll.so.4.0.4
/opt/cprocsp/lib/lib64/liburlretrieve.so.4.0.4
/opt/cprocsp/lib/lib64/libcsp.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/lib64/libcppkcs11.so.4.0.4
/opt/cprocsp/bin/ppc64/cpverify
/opt/cprocsp/bin/ppc64/wipefile
/opt/cprocsp/bin/ppc64/csptest
/opt/cprocsp/lib/lib64/librdrrdr.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndm.so.4.0.4
/opt/cprocsp/lib/lib64/librdrsup.so.4.0.4
/opt/cprocsp/lib/lib64/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/lib64/librdrfat12.so.4.0.4
/opt/cprocsp/lib/lib64/libcapi10.so.4.0.4
/opt/cprocsp/lib/lib64/libcpui.so.4.0.4
/opt/cprocsp/lib/lib64/libcpalloc.so.0.0.0
/opt/cprocsp/lib/lib64/libjemalloc.so.0.0.0
/opt/cprocsp/sbin/ppc64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ppc64/cpconfig
/opt/cprocsp/sbin/ppc64/mount_flash.sh
/opt/cprocsp/lib/lib64/librdrsbl.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 появляется 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 при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности.

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 значение log используйте:

a) RHEL

Для задания уровня протокола

/opt/cprocsp/sbin/<название_архитектуры>/cpconfig –loglevel cpcsp -mask 0x9

Для задания формата протокола

/opt/cprocsp/sbin/<название_архитектуры>/cpconfig –loglevel cpcsp -format 0x19

Для просмотра маски текущего уровня и формата протокола

/opt/cprocsp/sbin/<название_архитектуры>/cpconfig –loglevel cpcsp -view

b) для RHEL уровня ядра

insmod drvcsp.o log_level=0x9

Значением параметра уровнь протокола является битовая маска:

N_DB_ERROR = 1 # сообщения об ошибках

N_DB_LOG = 8 # сообщения о вызовах

Значением параметра формат протокола является битовая маска:

DBFMT_MODULE = 1 # выводить имя модуля

DBFMT_THREAD = 2 # выводить номер нитки

DBFMT_FUNC = 8 # выводить имя функции

DBFMT_TEXT = 0x10 # выводить само сообщение

DBFMT_HEX = 0x20 # выводить HEX дамп

DBFMT_ERR = 0x40 # выводить GetLastError

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					