127 028, 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 КС1

1-Base

Руководство администратора безопасности

Использование СКЗИ под управлением ОС Solaris

ЖТЯИ.00087-01 91 05
Листов 34

2016 г.

Содержание

Аннотация

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

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

Список сокращений

АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
Сертификат	Электронный документ, подтверждающий принадлежность ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись

1. Основные технические данные и характеристики СКЗИ

1.1. Программно-аппаратные среды

СКЗИ «КриптоПро CSP» под управлением ОС типа Solaris используется в следующих программно-аппаратных средах:

ОС Solaris 10/11 (sparc, ia32, x64).

При необходимости использования СКЗИ уровня ядра ОС архитектуры IA32 для ОС Solaris 10 следует обновить систему до исправления 142901-03 и установить исправление IDR144030.

Со сроками эксплуатации операционных систем, в среде которых функционирует СКЗИ, можно ознакомиться по следующему адресу:

<http://www.sun.com/service/eosl/solaris/solaris_vintage_eol_5.2005.xml

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);
- Novacard;
- Смарткарты РИК (ОСКАР 1, ОСКАР 2, Магистра, TRUST, TRUSTS, TRUSTD);
- 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. 2. Хранение закрытых ключей на HDD ПЭВМ и USB дисках (в реестре ОС Windows, в разделе HDD при работе под управлением других ОС) допускается только при условии распространения на HDD, USB диск или на ПЭВМ с HDD требований по обращению с ключевыми носителями (п.6.7 ЖТЯИ.00087-01 91 01. Руководство администратора безопасности общая часть). 3. Все вышеперечисленные носители используются только в качестве пассивного хранилища ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене. 4. Использование носителей других типов - только по согласованию с ФСБ России.

2. Установка дистрибутива ПО СКЗИ

Установка, удаление и обновление ПО осуществляется с правами 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 Solaris для установки, удаления и обновления ПО применяются пакеты (packages). Пакет – распакованный архив дистрибутива (фактически это папка), содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. Архив имеет расширение .tar.gz и является обычным архивом gzip.

Перед установкой архивы дистрибутива надо распаковать:

for i in *.tar.gz;do gzip -cd $i|tar -xf -;done

Для установки пакета используется команда:

pkgadd -d <папка_с_пакетами> <имя_пакета>

Например: **pkgadd -d . CPRObase**

Для удаления пакета используется команда:

pkgrm <имя_пакета>

Например: **pkgrm CPRObase**

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 для 32-битной архитектуры, а также для 64-битной архитектуры (имя пакета заканчивается на x), 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 установить оба комплекта. Исключением являются драйверы: они устанавливаются в точном соответствии с архитектурой ядра ОС.

Таблица 1 - зависимостЬ и назначения пакетов (для простоты описаны 32-битные пакеты).

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
CPRObase		Базовый пакет, устанавливается первым. Не зависит от архитектуры, поэтому для 64-битного комплекта этот пакет устанавливается из 32-битного комплекта.
CPROrdr	CPRObase	Основные приложения, считыватели и ДСЧ.
CPROcpl	CPROrdr	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS…).
CPROkc1	CPROrdr	Провайдер КС1.
Дополнительные пакеты		
CPROrdg	CPROrdr, SUNWmfrun, SUNWxwrtl	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги.
CPROrdp	CPROrdr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт (РИК, Оскар, Магистра…).
CPROcspd	CPRObase	Пакет, предназначенный для разработчика.

CPROdrv	CPRObase	Драйверная библиотека.
CPROdrvd	CPROcspd	Пакет, предназначенный для разработчика драйверов.
CPROstnl	CPRObase	Универсальный SSL/TLS туннель.

3. Обновление ПО СКЗИ

Для обновления СКЗИ на ОС Solaris 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 «КриптоПро CSP» 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 СКЗИ 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 CPROkc1, 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 CPROrdg 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 ДСЧ КПИМ:

```
# ./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 CPROrdp. После подключения считывателя узнайте имя устройства:

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

Для добавления считывателия 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/adm/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
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 -policy -set StrengthenedKeyUsageControl -value 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.

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.

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 программного обеспечения СКЗИ

6.1. Базовые модули СКЗИ

ПО СКЗИ содержит базовые модули:

Setup – модуль инсталляции ПО СКЗИ.
libcsp – динамически загружаемая библиотека КриптоПро CSP.
libcspst - статическая 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.

В названиях дистрибутивов СКЗИ используется нотация:
CPRO – префикс;
csp – криптопровайдер;
drv – загружаемый модуль ядра ОС;
[d] - опционально – указывает на документацию (тестовые примеры);
[x] - опционально – указывает на 64-битовую версию ОС; SPARC;
i386 – платформа Intel;
sparc – платформа SPARC.

6.1.1. Модуль SETUP

Модуль **Setup** обеспечивают инсталляцию программного обеспечения СКЗИ КриптоПро CSP. В процессе инсталляции производится контроль целостности ПО СКЗИ с использованием модуля cpverify.

6.1.2. Библиотеки libcsp и libcspst

Библиотеки **libcsp** и **libcspst** реализуют целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, клавиатурный ДСЧ.

6.1.3. Библиотека libcspr

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

6.1.4. 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.

6.1.5. Модули сетевой аутентификации КриптоПро TLS

Модуль **libssp** обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS. Общее описание протокола приведено в соответствующем разделе документа "ЖТЯИ.00087-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть."

6.1.6. Модуль cpverify

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

6.1.7. Модуль wipefile

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

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 доступа к ключевым носителям

Библиотека **librdrrdr** (release) обеспечивает унифицированный интерфейс доступа к ключевым носителям вне зависимости от их типа.

6.2.3. Модули устройств хранения ключевой информации

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

- **librdrfat12** к дисководу, дискете 3.5", разделу HDD

6.2.4. Библиотека librdrsup поддержки доступа к ключевым носителям

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 физическими датчиками случайных чисел.

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 в прикладное программное обеспечение должны выполняться требования раздела 17 документа «ЖТЯИ.00087-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть» и документа «ЖТЯИ.00087-01 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.00087-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть».

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

Под управлением UNIX-подобных операционных систем СКЗИ КриптоПро CSP должно использоваться с программным обеспечением:

- Certmgr (КриптоПро Certmgr).
- CryptCP.
- Apache Trusted TLS (Digt).
- Trusted TLS (Digt).

При использовании СКЗИ под управлением ОС Solaris необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом ставится задача не только обеспечить дополнительную защиту сервера 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 сервера;
- установка программных обновлений;
- организация процедуры резервного копирования и хранения резервных копий.
- Дополнительные настройки ОС Solaris касаются следующего:
- ограничение доступа пользователей и настройки пользовательского окружения;
- ограничение сетевых соединений;
- ограничения при монтировании файловых систем;
- ограничения на запуск процессов;
- 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).

Доступ персонала в серверную комнату должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

Кроме этого, при использовании в качестве сервера компьютера SUN SPARC, следует установить пароль для доступа к консоли, выполнив следующее:

• При загрузке системы в режиме диалога с интерпретатором команд загрузчика ввести следующие команды:

<ok> password

<ok> setenv security-mode command

• После загрузки системы, с консоли после регистрации от имени суперпользователя ввести следующие команды:

eeprom security-mode=command

eeprom security-password=

и ввести пароль на доступ к консоли.

Внимание! В случае если суперпользователь забудет пароль, возникнет необходимость замены ППЗУ первичного загрузчика в сервисном центре SUN.

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 производится комиссией с составлением акта об уничтожении.

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

2. Для пользователя root выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 6 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 пользователю root

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

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

5. В ОС Solaris 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.

6. При использовании СКЗИ «КриптоПро CSP» на ЭВМ, 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.

7. 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».

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

9. При использовании платформы Intel в BIOS, а при использовании платформы Sparc в PROM 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.

10. При использовании платформы Intel, средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств и PCI-устройств при использовании ПАК защиты от НСД,

11. 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.

12. Вход в BIOS (PROM) ЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю пользователя root. Пароль для входа в BIOS (PROM) должен быть известен только пользователю root и быть отличным от пароля пользователя root для входа в ОС Solaris.

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

14. На компьютере устанавливается только одна ОС. На машине не устанавливается средств разработки ПО и отладчики. 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.

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

16. Должно быть реализовано физическое затирание содержимого удаляемых файлов с использованием программы Wipe из состава СКЗИ.

17. Должны быть отключены все неиспользуемые на данной ЭВМ сетевые протоколы.

18. В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть отключено использование JavaScript, VBScript, ActiveX и других программных объектов загружаемых из сети.

19. 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.

20. 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.

21. Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ «КриптоПро CSP», исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

22. Из состава системы должно быть исключено все оборудование, которое может создавать угрозу безопасности ОС Solaris. Также следует избегать использования любых нестандартных аппаратных средств, имеющих возможность влиять на нормальный ход работы компьютера или ОС Solaris.

23. После инсталляции ОС Solaris следует установить с сайта http://www.sunsolve.sun.com/ все рекомендованные программные обновления и программные обновления, связанные с безопасностью (recommended and security patches) от компании SUN, существующие на момент инсталляции.

24. На все директории, содержащие системные файлы ОС Solaris и каталоги СКЗИ, устанавливают права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись.

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

26. В ОС Solaris используется виртуальная память. Область виртуальной памяти должна быть организована на отдельном HDD и доступ к ней должен иметь только пользователь root. По окончании работы СКЗИ содержимое виртуальной памяти должно затираться с помощью утилиты 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 не подлежащим ремонту. Этот HDD уничтожается по правилам уничтожения ключевых носителей.

8.1.2. Дополнительные настройки ОС Solaris

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

Для сохранения возможности "откатить" внесенные изменения следует сохранить модифицируемые файлы в "безопасном" месте (на внешнем носителе или на не монтируемой автоматически файловой системе). Желательно скопировать изменяемые файлы (каталоги) с сохранением структуры каталогов.

Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

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

PASSREQ=YES (требует использования паролей)

SUPATH=/usr/sbin:/usr/bin (задает значение переменной PATH после выполнения команды su);

RETRIES=3 (задает число повторных попыток регистрации пользователя программой login)

SYSLOG_FAILED_LOGINS=0 (директива предписывает протоколировать все попытки неудачной регистрации пользователя)

UMASK=077 (параметр задает маску создания файла по-умолчанию).

CONSOLE=/dev/console (параметр ограничивает возможность регистрации суперпользователя только системной консолью и запрещает удаленные регистрации суперпользователя);

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

umask 077 (umask 027);

3. Для отключения возможности доступа пользователя root к рабочей станции по сети раскомментировать строку "CONSOLE" в файле /etc/default/login;

4. Создать (отредактировать существующий) файл /etc/shells и поместить в него имена (с полным путем) только для тех исполняемых файлов оболочек, которые установлены в системе. По умолчанию, содержимое файла /etc/shells может быть таким:

/bin/bash	/usr/bin/bash
/bin/csh	/usr/bin/csh
/bin/ksh	/usr/bin/ksh
/bin/sh	/usr/bin/sh
/sbin/sh	/usr/bin/zsh

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

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

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

8. Отключить службу RPC удаленного вызова процедур, для чего следует удалить файл /etc/rc2.d/s71rpc;

9. 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.

10. Установить минимальную длину пароля в 8 символов в файле /etc/default/passwd директивой PASSLENGTH=8. Там же возможно задать минимальное и максимальное "время жизни" пароля в неделях параметрами MINWEEKS и MAXWEEKS.

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

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

daemon	uucp
bin	nuucp
sys	listen
adm	nobody4
lp	nobody
smtp	noaccess

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

Ограничения при монтировании файловых систем

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

1. Установить опцию nosuid при монтировании файловых систем /opt и /var.

2. Ограничить размер файловой системы /tmp опцией size. При этом значение опции size должно быть меньше размера области подкачки (swap). Поскольку, ОС Solaris монтирует файловую систему /tmp в область подкачки, то использование данной опции предотвратит ее переполнение.

При инсталляции системы следует выделить для файловых систем /, /usr, /usr/local, /var, /opt, /export разные разделы диска для предотвращения переполнения критичных файловых систем (/, /var) за счет, например, пользовательских данных и обеспечения возможности монтирования файловых систем /usr и /opt 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.d/cron.allow
echo root > /etc/cron.d/at.allow
```

Ограничить число системных сервисов и программ, инициализируемых в процессе загрузки ОС. Для этого:

Из каталога /etc/rcS.d удалить все файлы, кроме:

S30rootusr.sh
S40standardmounts.sh
S50drvconfig
S50drvconfig
S70buildmnttabs

Из каталога /etc/rc2.d удалить все файлы, кроме:

S02MOUNTFSYS
S05RMTMPFILES
S69inet
S72inetsvc
S74syslog
S20sysetup
S25cspcheck
S75cron
S88utmpd

Из каталога /etc/init.d удалить все файлы, кроме:

MOUNTFSYS
RMTMPFILES
inetsvc
standardmounts
dev
inks
cron
drvconfig
buildmnttab
rootusr
sysetup
syslog
inetinit
utmpd
dtlogin

Удалить все файлы из каталога /etc/rc3d.

Удалить все файлы из каталогов /etc/rc0.d и /etc/rc1.d, кроме тех, которые перечислены выше.

Настройка сетевых сервисов

Настройка сетевых сервисов заключается в следующем:

1. Следует ограничить функциональность демона управления сетевыми соединениями inetd. Действие заключается в редактировании файла /etc/inetd.conf. В файле /etc/inetd.conf

следует закомментровать (удалить) строки, содержащие описания тех сервисов, использование которых на конфигурируемом компьютере не является необходимостью.

Как минимум, следует запретить следующие сервисы:

echo	systat
discard	netstat
daytime	tftp
chargen	telnet
finger	

Возможно также сначала закомментировать в файле /etc/inetd.conf описания всех сервисов и затем раскомментировать только используемые.

2. Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора (даже при наличии нескольких сетевых адаптеров), необходимо создать в каталоге /etc файл notrouter нулевой длины.

3. Следует запретить прием из внешней сети "широковещательных" (broadcast) пакетов, а также передачу ответов на принятые "широковещательные" пакеты. Для этого, в конец файла /etc/rc2.d/S69inet следует добавить следующие команды:

ndd -set /dev/ip ip_forward_directed_broadcasts 0

ndd -set /dev/ip ip_respond_to_echo_broadcast 0

4. Следует запретить использование сетевой файловой системы NFS. Для этого следует удалить файлы:

/etc/dfs/dfstab

/etc/rc3.d/S15nfs.server

/etc/rc2.d/S73nfs.client

5. Запретить суперпользователю доступ по ftp, для этого добавить "root" в файл /etc/ftpusers

6. Запустить утилиту контроля системных ресурсов и средств системного аудита ASET с высоким уровнем безопасности: /usr/aset/aset -l high для проверки установок системных файлов и проананлизировать файл отчета, который будет создан в /usr/aset/reports

7. 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:

adm	nobody4
bin	nuucp
daemon	root
listen	smtp
lp	sys
nobody	uucp
noaccese	

8. 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
chmod 400 /usr/bin/uuencode
chmod u-s /usr/lib/fs/ufs/ufsdump
chmod u-s /usr/lib/fs/ufs/ufsrestore

Также следует обнулить флаг SGID для некоторых исполняемых файлов:

chmod g-s /usr/bin/mail
chmod g-s /usr/bin/mailx
chmod g-s /usr/bin/write
chmod g-s /usr/bin/netstat
chmod g-s /usr/bin/nfsstat
chmod g-s /usr/bin/ipcs

chmod g-s /usr/sbin/arp
chmod g-s /usr/sbin/dmesg
chmod g-s /usr/sbin/prtconf
chmod g-s /usr/sbin/swap
chmod g-s /usr/sbin/sysdef
chmod g-s /usr/sbin/wall

chmod g-s /usr/openwin/bin/ff.core
chmod g-s /usr/openwin/bin/mailtool
chmod g-s /usr/openwin/bin/wsinfo
chmod g-s /usr/openwin/bin/xload

chmod g-s /usr/lib/fs/ufs/ufsdump
chmod g-s /usr/lib/fs/ufs/ufsrestore

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 директивы:

BANNER=""

– Отказ от стандартного "заголовка", выводимого сервером telnet при ответе пользователю. Достигается указанием в файле /etc/default/telnetd следующей директивы:

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

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

/var/log/authlog
/var/log/syslog

/var/adm/messages*
/var/adm/sulog
/var/adm/utmp
/var/adm/utmpx

2. Если на настраиваемом сервере используется web-сервер, то следует убедится, что только "владелец" процесса httpd имеет доступ по записи к протоколам httpd.3. Ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команды su – предоставления пользователю административных полномочий.4. Следует протоколировать попытки использования программы su. Для этого, в файл /etc/syslog.conf следует добавить запись:

auth.notice /var/log/authlog

или

auth.notice ifdef (`LOGHOST`, /var/log/authlog, @loghost)

Вторая строка аналогична первой, но указывает, что протокол передается на сервер сбора протоколов. При редактировании файла /etc/syslog.conf в качестве разделителя полей в строке следует использовать символ табуляции

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 sys /var/adm/loginlog

chmod 644 /var/adm/loginlog

Для протоколирования сетевых соединений, контролируемых демоном inetd (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

и в файле /etc/rc2.d/S72inetsvc заменить строку

/usr/sbin/inetd -s

на

/usr/sbin/inetd -s –t

8.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

1. Должны быть приняты меры по защите от 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.

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

3. 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.00087-01 91 01.

3. Перед началом работы должен быть проведен контроль целостности. Контролем целостности должны быть охвачены файлы, указанные в п. 16.

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

13. При функционировании СКЗИ должны выполняться требования эксплуатационной документации на ПАК защиты от НСД.

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

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

16. Контролем целостности должны быть охвачены файлы:

Sparc Solaris (32-bits)

```
/opt/cprocsp/bin/sparc/cryptcp
/opt/cprocsp/bin/sparc/certmgr
/opt/cprocsp/bin/sparc/inittst
/opt/cprocsp/bin/sparc/csptestf
/opt/cprocsp/bin/sparc/der2xer
/opt/cprocsp/lib/sparc/libcapi20.so.4.0.4
/opt/cprocsp/lib/sparc/libcpext.so.4.0.4
/opt/cprocsp/lib/sparc/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/sparc/libasn1data.so.4.0.4
/opt/cprocsp/lib/sparc/libssp.so.4.0.4
/opt/cprocsp/lib/sparc/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/sparc/libcplib.so.4.0.4
/opt/cprocsp/lib/sparc/libcpasn1.so.4.0.4
/opt/cprocsp/lib/sparc/libocsp.so.4.0.4
/opt/cprocsp/lib/sparc/libenroll.so.4.0.4
/opt/cprocsp/lib/sparc/libtsp.so.4.0.4
/opt/cprocsp/lib/sparc/libtspcli.so.4.0.4
/opt/cprocsp/lib/sparc/liburlretrieve.so.4.0.4
/opt/cprocsp/bin/sparc/curl
/opt/cprocsp/lib/sparc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparc/libcpcurl.a
/opt/cprocsp/lib/sparc/libcsp.so.4.0.4
/opt/cprocsp/lib/sparc/librdrrndmbio_tui.so.4.0.4
```

```
/opt/cprocsp/lib/sparc/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/sparc/libxcpui.so.4.0.4
/opt/cprocsp/lib/sparc/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/sparc/librdrric.so.4.0.4
/opt/cprocsp/sbin/sparc/ccid_reg.sh
/opt/cprocsp/bin/sparc/cpverify
/opt/cprocsp/bin/sparc/wipefile
/opt/cprocsp/bin/sparc/csptest
/opt/cprocsp/lib/sparc/librdrrdr.so.4.0.4
/opt/cprocsp/lib/sparc/librdrrndm.so.4.0.4
/opt/cprocsp/lib/sparc/librdrsup.so.4.0.4
/opt/cprocsp/lib/sparc/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/sparc/librdrfat12.so.4.0.4
/opt/cprocsp/lib/sparc/libcapi10.so.4.0.4
/opt/cprocsp/lib/sparc/libcpui.so.4.0.4
/opt/cprocsp/sbin/sparc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparc/cpconfig
/opt/cprocsp/sbin/sparc/mount_flash.sh
/opt/cprocsp/lib/sparc/librdruec.so.4.0.4
/opt/cprocsp/lib/sparc/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/sparc/librsaenh.so.4.0.4
/opt/cprocsp/sbin/sparc/stunnel_thread
/opt/cprocsp/sbin/sparc/stunnel_fork
/opt/cprocsp/sbin/sparc/stunnel_hsm
```

Sparc Solaris (64-bits)

```
/opt/cprocsp/bin/sparc/cryptcp
/opt/cprocsp/bin/sparc/certmgr
/opt/cprocsp/bin/sparc/inittst
/opt/cprocsp/bin/sparc/csptestf
/opt/cprocsp/bin/sparc/der2xer
/opt/cprocsp/lib/sparc/libcapi20.so.4.0.4
/opt/cprocsp/lib/sparc/libcpext.so.4.0.4
/opt/cprocsp/lib/sparc/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/sparc/libasn1data.so.4.0.4
/opt/cprocsp/lib/sparc/libssp.so.4.0.4
/opt/cprocsp/lib/sparc/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/sparc/libcplib.so.4.0.4
/opt/cprocsp/lib/sparc/libcpasn1.so.4.0.4
/opt/cprocsp/lib/sparc/libocsp.so.4.0.4
/opt/cprocsp/lib/sparc/libenroll.so.4.0.4
/opt/cprocsp/lib/sparc/libtsp.so.4.0.4
/opt/cprocsp/lib/sparc/libtspcli.so.4.0.4
/opt/cprocsp/lib/sparc/liburlretrieve.so.4.0.4
/opt/cprocsp/bin/sparcv9/cryptcp
/opt/cprocsp/bin/sparcv9/certmgr
/opt/cprocsp/bin/sparcv9/inittst
/opt/cprocsp/bin/sparcv9/csptestf
/opt/cprocsp/bin/sparcv9/der2xer
/opt/cprocsp/lib/sparcv9/libcapi20.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcpext.so.4.0.4
/opt/cprocsp/lib/sparcv9/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/sparcv9/libasn1data.so.4.0.4
/opt/cprocsp/lib/sparcv9/libssp.so.4.0.4
/opt/cprocsp/lib/sparcv9/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcplib.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcpasn1.so.4.0.4
/opt/cprocsp/lib/sparcv9/libocsp.so.4.0.4
/opt/cprocsp/lib/sparcv9/libenroll.so.4.0.4
/opt/cprocsp/lib/sparcv9/libtsp.so.4.0.4
/opt/cprocsp/lib/sparcv9/libtspcli.so.4.0.4
/opt/cprocsp/lib/sparcv9/liburlretrieve.so.4.0.4
/opt/cprocsp/bin/sparc/curl
```

```
/opt/cprocsp/lib/sparc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparc/libcpcurl.a
/opt/cprocsp/bin/sparcv9/curl
/opt/cprocsp/lib/sparcv9/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparcv9/libcpcurl.a
/opt/cprocsp/lib/sparc/libcpcdrv_emul.a
/opt/cprocsp/lib/sparc/libcsp.so.4.0.4
/opt/cprocsp/lib/sparc/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcsp.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/sparc/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/sparc/libxcpui.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/sparcv9/libxcpui.so.4.0.4
/opt/cprocsp/lib/sparc/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/sparc/librdrric.so.4.0.4
/opt/cprocsp/sbin/sparc/ccid_reg.sh
/opt/cprocsp/lib/sparcv9/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrric.so.4.0.4
/opt/cprocsp/sbin/sparcv9/ccid_reg.sh
/opt/cprocsp/bin/sparc/cpverify
/opt/cprocsp/bin/sparc/wipefile
/opt/cprocsp/bin/sparc/csptest
/opt/cprocsp/lib/sparc/librdrrdr.so.4.0.4
/opt/cprocsp/lib/sparc/librdrrndm.so.4.0.4
/opt/cprocsp/lib/sparc/librdrsup.so.4.0.4
/opt/cprocsp/lib/sparc/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/sparc/librdrfat12.so.4.0.4
/opt/cprocsp/lib/sparc/libcapi10.so.4.0.4
/opt/cprocsp/lib/sparc/libcpui.so.4.0.4
/opt/cprocsp/sbin/sparc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparc/cpconfig
/opt/cprocsp/sbin/sparc/mount_flash.sh
/opt/cprocsp/bin/sparcv9/cpverify
/opt/cprocsp/bin/sparcv9/wipefile
/opt/cprocsp/bin/sparcv9/csptest
/opt/cprocsp/lib/sparcv9/librdrrdr.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrrndm.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrsup.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdrfat12.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcapi10.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcpui.so.4.0.4
/opt/cprocsp/sbin/sparcv9/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparcv9/cpconfig
/opt/cprocsp/sbin/sparcv9/mount_flash.sh
/opt/cprocsp/lib/sparc/librdruec.so.4.0.4
/opt/cprocsp/lib/sparc/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/sparcv9/librdruec.so.4.0.4
/opt/cprocsp/lib/sparcv9/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/sparc/librsaenh.so.4.0.4
/opt/cprocsp/lib/sparcv9/librsaenh.so.4.0.4
/opt/cprocsp/sbin/sparc/stunnel_thread
/opt/cprocsp/sbin/sparc/stunnel_fork
/opt/cprocsp/sbin/sparc/stunnel_hsm
/opt/cprocsp/sbin/sparcv9/stunnel_thread
/opt/cprocsp/sbin/sparcv9/stunnel_fork
/opt/cprocsp/sbin/sparcv9/stunnel_hsm
```

Intel Solaris (32-bits)

```
/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.4.0.4
/opt/cprocsp/lib/ia32/libcpext.so.4.0.4
/opt/cprocsp/lib/ia32/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.4
/opt/cprocsp/lib/ia32/libssp.so.4.0.4
/opt/cprocsp/lib/ia32/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/ia32/libcplib.so.4.0.4
/opt/cprocsp/lib/ia32/libcpasn1.so.4.0.4
/opt/cprocsp/lib/ia32/libocsp.so.4.0.4
/opt/cprocsp/lib/ia32/libenroll.so.4.0.4
/opt/cprocsp/lib/ia32/libtsp.so.4.0.4
/opt/cprocsp/lib/ia32/libtspcli.so.4.0.4
/opt/cprocsp/lib/ia32/liburlretrieve.so.4.0.4
/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/lib/ia32/libcsp.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/ia32/libxcpui.so.4.0.4
/opt/cprocsp/lib/ia32/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/ia32/librdrric.so.4.0.4
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/librdrrdr.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndm.so.4.0.4
/opt/cprocsp/lib/ia32/librdrsup.so.4.0.4
/opt/cprocsp/lib/ia32/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/ia32/librdrfat12.so.4.0.4
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.4
/opt/cprocsp/lib/ia32/libcpui.so.4.0.4
/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/librdruec.so.4.0.4
/opt/cprocsp/lib/ia32/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.4
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/sbin/ia32/stunnel_hsm
```

Intel Solaris (64-bits)

```
/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.4.0.4
/opt/cprocsp/lib/ia32/libcpext.so.4.0.4
/opt/cprocsp/lib/ia32/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.4
/opt/cprocsp/lib/ia32/libssp.so.4.0.4
/opt/cprocsp/lib/ia32/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/ia32/libcplib.so.4.0.4
/opt/cprocsp/lib/ia32/libcpasn1.so.4.0.4
/opt/cprocsp/lib/ia32/libocsp.so.4.0.4
/opt/cprocsp/lib/ia32/libenroll.so.4.0.4
/opt/cprocsp/lib/ia32/libtsp.so.4.0.4
```

```
/opt/cprocsp/lib/ia32/libtspcli.so.4.0.4
/opt/cprocsp/lib/ia32/liburlretrieve.so.4.0.4
/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.4.0.4
/opt/cprocsp/lib/amd64/libcpext.so.4.0.4
/opt/cprocsp/lib/amd64/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/amd64/libasn1data.so.4.0.4
/opt/cprocsp/lib/amd64/libssp.so.4.0.4
/opt/cprocsp/lib/amd64/libpkivalidator.so.4.0.4
/opt/cprocsp/lib/amd64/libcplib.so.4.0.4
/opt/cprocsp/lib/amd64/libcpasn1.so.4.0.4
/opt/cprocsp/lib/amd64/libocsp.so.4.0.4
/opt/cprocsp/lib/amd64/libenroll.so.4.0.4
/opt/cprocsp/lib/amd64/libtsp.so.4.0.4
/opt/cprocsp/lib/amd64/libtspcli.so.4.0.4
/opt/cprocsp/lib/amd64/liburlretrieve.so.4.0.4
/opt/cprocsp/bin/ia32/curl
/opt/cprocsp/lib/ia32/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ia32/libcpcurl.a
/opt/cprocsp/bin/amd64/curl
/opt/cprocsp/lib/amd64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/amd64/libcpcurl.a
/opt/cprocsp/lib/ia32/libcpcdrv_emul.a
/opt/cprocsp/lib/ia32/libcsp.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/amd64/libcsp.so.4.0.4
/opt/cprocsp/lib/amd64/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/ia32/libxcpui.so.4.0.4
/opt/cprocsp/lib/amd64/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/amd64/libxcpui.so.4.0.4
/opt/cprocsp/lib/ia32/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/ia32/librdrric.so.4.0.4
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/lib/amd64/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/amd64/librdrric.so.4.0.4
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/librdrrdr.so.4.0.4
/opt/cprocsp/lib/ia32/librdrrndm.so.4.0.4
/opt/cprocsp/lib/ia32/librdrsup.so.4.0.4
/opt/cprocsp/lib/ia32/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/ia32/librdrfat12.so.4.0.4
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.4
/opt/cprocsp/lib/ia32/libcpui.so.4.0.4
/opt/cprocsp/sbin/ia32/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ia32/cpconfig
/opt/cprocsp/sbin/ia32/mount_flash.sh
/opt/cprocsp/bin/amd64/cpverify
/opt/cprocsp/bin/amd64/wipefile
/opt/cprocsp/bin/amd64/csptest
/opt/cprocsp/lib/amd64/librdrrdr.so.4.0.4
/opt/cprocsp/lib/amd64/librdrrndm.so.4.0.4
/opt/cprocsp/lib/amd64/librdrsup.so.4.0.4
/opt/cprocsp/lib/amd64/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/amd64/librdrfat12.so.4.0.4
/opt/cprocsp/lib/amd64/libcapi10.so.4.0.4
```

```
/opt/cprocsp/lib/amd64/libcpui.so.4.0.4
/opt/cprocsp/sbin/amd64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/amd64/cpconfig
/opt/cprocsp/sbin/amd64/mount_flash.sh
/opt/cprocsp/lib/ia32/librdruec.so.4.0.4
/opt/cprocsp/lib/ia32/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/amd64/librdruec.so.4.0.4
/opt/cprocsp/lib/amd64/libcpcvcert.so.4.0.4
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.4
/opt/cprocsp/lib/amd64/librsaenh.so.4.0.4
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/sbin/ia32/stunnel_hsm
/opt/cprocsp/sbin/amd64/stunnel_thread
/opt/cprocsp/sbin/amd64/stunnel_fork
/opt/cprocsp/sbin/amd64/stunnel_hsm
```

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 КриптоПро CSP имеет средства обеспечения контроля целостности ПО СКЗИ, которые должны 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 плгоритму 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 была подпись была создана, в формате dd.mm.yyyy.

Приложение 2. Управление протоколированием

Для включения/отключения значение log используйте:

a) для Solaris i386, SPARC 32

Для задания уровня протокола

/opt/CPROcsp/sbin/cpconfig -loglevel cpcsp -mask 0x9

Для задания формата протокола

/opt/CPROcsp/sbin/cpconfig -loglevel cpcsp -format 0x19

Для просмотра маски текущего уровня и формата протокола

/opt/CPROcsp/sbin/cpconfig –loglevel cpcsp -view

b) для SPARC 64

Для задания уровня протокола

/opt/CPROcsp/sbin/sparcv9/cpconfig -loglevel cpcsp -mask 0x9

Для задания формата протокола

/opt/CPROcsp/sbin/sparcv9/cpconfig -loglevel cpcsp -format 0x19

Для просмотра маски текущего уровня и формата протокола

/opt/CPROcsp/sbin/sparcv9/cpconfig –loglevel cpcsp -view

c) для Solaris i386, SPARC 32, SPARC 64 уровня ядра
/usr/kernel/drv/drvcsp.conf
отредактировать loglevel

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 № сопроводи-тельного докум. и дата	Подп.	Дата
	изменен-ных	замененных	новых	аннулиро-ванных					