

127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
<https://CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 KC1

1-Base

Руководство администратора
безопасности.

Использование СКЗИ
под управлением ОС FreeBSD

ЖТЯИ.00101-01 91 04
Листов 28

© ООО «КРИПТО-ПРО», 2000-2019. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию к нему зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 5.0 КС1; 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

Список сокращений	5
1 Основные технические данные и характеристики СКЗИ	6
1.1 Программно-аппаратные среды функционирования	6
1.2 Ключевые носители	6
2 Установка дистрибутива ПО СКЗИ	7
3 Обновление ПО СКЗИ	9
4 Настройка СКЗИ	10
4.1 Доступ к утилите для настройки СКЗИ	10
4.2 Ввод серийного номера лицензии	10
4.3 Настройка оборудования СКЗИ	10
4.4 Установка параметров журналирования	11
4.5 Настройка криптопровайдера по умолчанию	12
4.6 Включение режима усиленного контроля использования ключей	12
4.7 Настройка параметров алгоритмов	13
5 Установка сопутствующих пакетов	14
5.1 Библиотека libcurl	14
6 Состав и назначение компонент ПО СКЗИ	15
6.1 Базовые модули СКЗИ	15
6.1.1 Библиотека libcsp	15
6.1.2 Библиотека libcspr	15
6.1.3 Драйверная библиотека drvcspr	15
6.1.4 Модули сетевой аутентификации КриптоПро TLS	15
6.1.5 Модуль crverify	15
6.1.6 Модуль wipefile	16
6.2 Модули подсистемы программной среды функционирования криптосредства (СФ)	16
6.2.1 Модуль libcap20	16
6.2.2 Библиотека libdrdr	16
6.2.3 Модули устройств хранения ключевой информации	16
6.2.4 Библиотека libdrsup	16
6.2.5 Модули датчиков случайных чисел	16
6.2.6 Библиотека libasn1data поддержки протокола ASN1	16
7 Требования по защите от НСД	17
7.1 Организационно-технические меры защиты от НСД	17
7.2 Дополнительные настройки ОС FreeBSD	19
8 Требования по криптографической защите	24
Приложение А. Управление протоколированием	27

Аннотация

Настоящее Руководство дополняет документ ЖТЯИ.00101-01 91 01. КристоПро CSP. Руководство администратора безопасности. Общая часть при использовании СКЗИ под управлением ОС FreeBSD.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КристоПро CSP версия 5.0 КС1 Исполнение 1-Base, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
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
СФ	Среда функционирования
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 функционирования

СКЗИ КriptoПро CSP версии 5.0 KC1 (ЖТЯИ.00101-01) под управлением ОС FreeBSD используется в программно-аппаратных средах:

ОС FreeBSD 11/12, pfSense 2.x (x86, x64).

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

<http://www.freebsd.org/security/security.html>, раздел **Supported FreeBSD releases**

<https://lists.freebsd.org/pipermail/freebsd-announce/2016-October/001754.html>

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-01 30 01. КriptoПро CSP. Формуляр, п. 3.9.

Использование носителей других типов допускается только по согласованию с ФСБ России.



Примечание. 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 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 FreeBSD для установки, удаления и обновления ПО применяются пакеты (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, используемые инсталлятором для конфигурирования среды. Этот архив имеет расширение .tbz. Для идентификации его как пакета, файл содержит 5 файлов, описывающих архив (+CONTENTS, +COMMENT, +DESC, +INSTALL, +DISPLAY).

Для установки пакета используется команда:

```
pkg_add <файл_пакета> (pkg add <файл_пакета> для FreeBSD 10)
```

Например: `pkg_add ./cpro-base-5.0_0.tbz`

Для удаления пакета используется команда:

```
pkg_delete <имя_пакета> (pkg delete <файл_пакета> для FreeBSD 10)
```

Например: `pkg_delete cpro-base-5.0_0`

Файлы из пакетов устанавливаются в /opt/cpro-csp.

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 (см. [табл. 1](#)).

Таблица 1. Зависимости и назначения пакетов

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
cpro-base-...		Базовый пакет, устанавливается первым.
cpro-rdr-...	cpro-base-...	Основные приложения, считыватели и ДСЧ.
cpro-kc1-...	cpro-rdr-...	Провайдер КС1.
cpro-kc2-...	cpro-rdr-...	Провайдер КС2, устанавливается только там, где в этом есть необходимость. В этом случае cpro-kc1-... обычно не ставится.
cpro-capilite-...	cpro-rdr-..., cpro-kc1-... или cpro-kc2-...	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...).
Дополнительные пакеты		
cpro-rdg-...	cpro-rdr-..., open-motif, XFree86-libraries	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги.
cpro-rdp-...	cpro-rdr-..., pcsclite	Модули поддержки PCSC-считывателей, смарт-карт (РИК, Оскар, Магистра...).
cpro-cspd-...	cpro-base-...	Пакет для разработчика.
cpro-drv-...	cpro-base-...	Драйверная библиотека.
cpro-drvd-...	cpro-cspd-...	Пакет для разработчика драйверов.
cpro-stnl-...	cpro-capilite-...	Универсальный SSL/TLS туннель.
cpro-rdemv-...	cpro-rdr-...	Модуль поддержки EMV.

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС FreeBSD необходимо:

- запомнить текущую конфигурацию CSP;
 - набор установленных пакетов;
 - настройки провайдера (для простоты можно сохранить `/etc/opt/cprosp/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 `crconfig`, которая входит в состав дистрибутива и расположена в директории `/opt/cpro-csp/sbin/<название_архитектуры>`. Если установлены пакеты СКЗИ для двух архитектур, например, `ia32` и `x64`, то действия по настройке нужно проводить дважды — для каждой архитектуры с помощью `crconfig` 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:

```
# crconfig -license -view
```

Для ввода лицензии выполните:

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

Серийный номер следует вводить с соблюдением регистра символов.

4.3 Настройка оборудования СКЗИ

Утилита `crconfig` 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:

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

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

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

Для просмотра списка настроенных ДСЧ:

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

Для консольного БиоДСЧ требуется пакет `cpro-ks1`. Для добавления консольного БиоДСЧ:

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

Для графического БиоДСЧ требуется пакет cpro-rdg и X-сервер. 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/cpro-csp/dsrf/db1/kis_1
```

```
# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cpro-csp/dsrf/db2/kis_1
```

Также необходимо скопировать файлы с данными, полученными с помощью "APM выработки внешней гаммы". Для этого выполните команды (при условии, что файлы находятся в /tmp/db[1,2]):

```
# cp /tmp/db1/kis_1 /var/opt/cpro-csp/dsrf/db1/kis_1
```

```
# cp /tmp/db2/kis_1 /var/opt/cpro-csp/dsrf/db2/kis_1
```

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

```
# /opt/cpro-csp/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:

- crpcsp — ядро криптопровайдера
- capi10 — CryptoAPI 1.0
- capi20 — CryptoAPI 2.0
- cpssp — TLS
- cpxt — дополнения для CryptoAPI 2.0
- cloud — Cloud CSP
- pcsc — PC/SC

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
```



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

4.7 Настройка параметров алгоритмов

Для установки параметров алгоритмов (для провайдеров типа 75):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2001 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2001 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 80):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2012 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2012 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 81):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el512 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el512 <OID>
```

Перечень поддерживаемых в КриптоПро CSP идентификаторов криптографических параметров алгоритмов указан в CSP_5_0.chm.

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 можно скачать пакет с исходными текстами для самостоятельной сборки. Как правило, там же есть 32-битные бинарные пакеты.

32-битный бинарный пакет доступен на сайте производителя ОС: <ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-current/All/>

Также можно собрать библиотеку из портов /usr/ports/ftp/curl.

После установки библиотек необходимо зарегистрировать пути к ним. Например:

```
/opt/cpro-csp/sbin/ia32/cpconfig -ini '\config\apppath' -add string libcurl.so /usr/local/lib/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».
- `drvcspr` — 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 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 `drvcspr`

Библиотека `drvcspr`, 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.00101-01 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.

6.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

6.2.1 Модуль libcap20

Модуль libcap20 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 libdrdrdr

Библиотека libdrdrdr 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:

- libdrfat12 — к дисководу и дискете 3.5"и разделу жесткого диска;
- libdrpcsc — к считывателям смарткарт и eToken, поддерживающим интерфейс PC/SC;
- libdremv — к ключевым носителям EMV и Gemalto.

6.2.4 Библиотека libdrsup

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

6.2.5 Модули датчиков случайных чисел

Библиотеки libdrndm и libdrndmbio 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 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 документа ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и раздела 5 ЖТЯИ.00101-01 95 01. Правила пользования.

При использовании СКЗИ под управлением ОС FreeBSD 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).

7.1 Организационно-технические меры защиты от НСД

Для ОС FreeBSD дополнительно должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

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

2) 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 6 месяцев, доступ к паролю должен быть обеспечен только администратору.

3) Пользователю root доступны настройки всех пользователей ОС FreeBSD, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в ОС FreeBSD, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС FreeBSD, 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 FreeBSD во время установки (таких, как sys, uicr, nuicr и listen), кроме пользователя root, следует удалить.

5) В ОС FreeBSD 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 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.

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, должно использоваться только лицензионное программное обеспечение фирм-производителей.

9) 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.

10) 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 FreeBSD.

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

12) 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.

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

14) 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.

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 Wipefile из состава СКЗИ.

17) Должны быть отключены все неиспользуемые сетевые протоколы.

18) 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.

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

22) После инсталляции ОС FreeBSD следует установить все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

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

24) 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`.

25) В ОС FreeBSD 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.

7.2 Дополнительные настройки ОС FreeBSD

Дополнительные настройки ОС FreeBSD 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.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть), что означает:

- выполнение загрузки с фиксированного носителя после его контроля;
- 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 `crverify`.

- дополнительные настройки ядра ОС;
- настройка сетевых сервисов;
- ограничение количества «видимой извне» информации о системе;
- настройка подсистемы протоколирования и аудита.

Настройки ОС FreeBSD 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). 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/login.defs` следует установить следующие директивы:

- `Login-retries=3` (задает число повторных попыток регистрации пользователя программой `login`)
- `passwordtime=180d` (для ограничения срока действия пароля 180 сутками)
- `coredumpsize=0K` (для запрета создания core-файлов)
- `SYSLOG_FAILED_LOGINS=0` (директива предписывает протолировать все попытки неудачной регистрации пользователя)
- `UMASK=022` (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) 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
/usr/local/bin/bash
```

4) Удалить файл (если он существует) `/.rhosts`.

5) Удалить содержимое файла `/etc/host.equiv`.

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

7) 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`.

8) Создать перечень программ, которые запускаются с правами администратора, и контролировать его неизменность;

9) Запретить регистрацию в системе пользователей, имеющих следующие «служебные имена»:

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

Действие выполняется путем указания в файле `/etc/passwd` строки `'/sbin/nologin'` 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 > /var/cron/allow
```

```
echo root > /var/at/at.allow
```

Настройка сетевых сервисов заключается в следующем:

1) Следует ограничить функциональность демона управления сетевыми соединениями inetd (xinetd). Действие заключается в редактировании файла /etc/inetd.conf. В файле /etc/inetd.conf следует закомментировать (удалить) строки, содержащие описания тех сервисов, использование которых на конфигурируемом компьютере не является необходимым.

Как минимум, следует запретить следующие сервисы:

- echo
- discard
- daytime
- chargen
- finger
- systat
- netstat
- tftp
- telnet
- nfsd

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

2) Используя утилиту sysinstall, отключить неиспользуемые сетевые сервисы, и службы, запускаемых при старте системы, запустить работу подсистемы accounting для контроля запускаемых процессов.

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

4) Запретить суперпользователю доступ по ftp, для этого добавить 'root' в файл /etc/ftpusers;

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
- bin
- sys
- adm
- lp
- smtp
- uucp
- nuucp
- listen
- nobody
- 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
chmod 400 /usr/bin/uencode
```

7) 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
```

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.).

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/ftpwelcome 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

1) 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

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

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

4) Следует протолировать 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.

5) 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 wheel /var/adm/loginlog
chmod 644 /var/adm/loginlog
```

6) 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 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-01 91 01.КриптоПро CSP. Руководство администратора безопасности. Общая часть в части, касающейся ОС FreeBSD.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по [разд. 7.2](#).

Контролем целостности должны быть охвачены файлы:

FreeBSD (x86)

```
/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
/opt/cprocsp/lib/ia32/libcpxext.so.4
/opt/cprocsp/lib/ia32/libasn1data.so.4
/opt/cprocsp/lib/ia32/libasn1data_XER.so.4
/opt/cprocsp/lib/ia32/libssp.so.4
/opt/cprocsp/lib/ia32/libenroll.so.4
/opt/cprocsp/lib/ia32/liburlretrieve.so.4
/opt/cprocsp/bin/ia32/curl
/opt/cprocsp/lib/ia32/libcpcurl.so.6
/opt/cprocsp/lib/ia32/libcpcurl.a
/opt/cprocsp/modules/ia32/kern.osreldate.702000/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.1000510/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.802000/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.803000/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.804000/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.901000/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.902001/drvcsp.ko
/opt/cprocsp/modules/ia32/kern.osreldate.903000/drvcsp.ko
/opt/cprocsp/lib/ia32/libcpcdrv_emul.a
/opt/cprocsp/modules/ia32/kern.osreldate.702000/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.1000510/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.802000/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.803000/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.804000/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.901000/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.902001/cpesp_gost.ko
/opt/cprocsp/modules/ia32/kern.osreldate.903000/cpesp_gost.ko
/opt/cprocsp/bin/ia32/cp-genpsk.sh
/opt/cprocsp/bin/ia32/genpsk
/opt/cprocsp/lib/ia32/libike_gost.so.4
/opt/cprocsp/lib/ia32/libesp_gost.so.4
/opt/cprocsp/lib/ia32/libcsp.so.4
/opt/cprocsp/lib/ia32/libdrndmbio_tui.so.4
```



```
/opt/cprocsp/lib/ia32/libcppkcs11.so.4
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/libdrndm.so.4
/opt/cprocsp/lib/ia32/libdrsup.so.4
/opt/cprocsp/lib/ia32/libdrdsrf.so.4
/opt/cprocsp/lib/ia32/libdrfat12.so.4
/opt/cprocsp/lib/ia32/libcapi10.so.4
/opt/cprocsp/lib/ia32/libcpui.so.4
/opt/cprocsp/lib/ia32/libcpalloc.so.0
/opt/cprocsp/lib/ia32/libjemalloc.so.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/libdremv.so.4
/opt/cprocsp/lib/ia32/libdrpcsc.so.4
/opt/cprocsp/lib/ia32/libdrdic.so.4
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/lib/ia32/libcpcvcert.so.4
/opt/cprocsp/lib/ia32/librsaenh.so.4
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/sbin/ia32/stunnel_hsm
```

FreeBSD (x64)

```
/opt/cprocsp/bin/amd64/cryptcp
/opt/cprocsp/bin/amd64/certmgr
/opt/cprocsp/bin/amd64/initst
/opt/cprocsp/bin/amd64/csptestf
/opt/cprocsp/bin/amd64/der2xer
/opt/cprocsp/lib/amd64/libcapi20.so.4
/opt/cprocsp/lib/amd64/libcpevt.so.4
/opt/cprocsp/lib/amd64/libasn1data.so.4
/opt/cprocsp/lib/amd64/libasn1data_XER.so.4
/opt/cprocsp/lib/amd64/libssp.so.4
/opt/cprocsp/lib/amd64/libenroll.so.4
/opt/cprocsp/lib/amd64/liburlretrieve.so.4
/opt/cprocsp/bin/amd64/curl
/opt/cprocsp/lib/amd64/libcpcurl.so.6
/opt/cprocsp/lib/amd64/libcpcurl.a
/opt/cprocsp/modules/amd64/kern.osreldate.801000/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.1000510/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.802000/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.803000/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.804000/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.901000/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.902001/drvvsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.903000/drvvsp.ko
```

```
/opt/cprocsp/lib/amd64/libcpdrv_emul.a
/opt/cprocsp/modules/amd64/kern.osreldate.801000/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.1000510/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.802000/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.803000/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.804000/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.901000/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.902001/cpesp_gost.ko
/opt/cprocsp/modules/amd64/kern.osreldate.903000/cpesp_gost.ko
/opt/cprocsp/bin/amd64/cp-genpsk.sh
/opt/cprocsp/bin/amd64/genpsk
/opt/cprocsp/lib/amd64/libike_gost.so.4
/opt/cprocsp/lib/amd64/libesp_gost.so.4
/opt/cprocsp/lib/amd64/libcsp.so.4
/opt/cprocsp/lib/amd64/libdrndmbio_tui.so.4
/opt/cprocsp/lib/amd64/libcppkcs11.so.4
/opt/cprocsp/bin/amd64/cpverify
/opt/cprocsp/bin/amd64/wipefile
/opt/cprocsp/bin/amd64/csptest
/opt/cprocsp/lib/amd64/libdrndm.so.4
/opt/cprocsp/lib/amd64/libdrsup.so.4
/opt/cprocsp/lib/amd64/libdrdsrf.so.4
/opt/cprocsp/lib/amd64/libdrfat12.so.4
/opt/cprocsp/lib/amd64/libcap10.so.4
/opt/cprocsp/lib/amd64/libcpui.so.4
/opt/cprocsp/lib/amd64/libcpalloc.so.0
/opt/cprocsp/lib/amd64/libjemalloc.so.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/libdremv.so.4
/opt/cprocsp/lib/amd64/libdrpcsc.so.4
/opt/cprocsp/lib/amd64/libdrrric.so.4
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/opt/cprocsp/lib/amd64/libcpcvcert.so.4
/opt/cprocsp/lib/amd64/librsaenh.so.4
/opt/cprocsp/sbin/amd64/stunnel_thread
/opt/cprocsp/sbin/amd64/stunnel_fork
/opt/cprocsp/sbin/amd64/stunnel_hsm
```

Приложение А

Управление протоколированием

Для включения/отключения значение log используйте:

1) FreeBSD

Для задания уровня протокола:

```
/usr/ cpro-csp/sbin/cpconfig -loglevel cpcsp -mask 0x9
```

Для задания формата протокола:

```
/usr/ cpro-csp/sbin/cpconfig -loglevel cpcsp - format 0x19
```

Для просмотра маски текущего уровня и формата протокола:

```
/usr/ cpro-csp/sbin/cpconfig -loglevel cpcsp -view
```

2) для FreeBSD уровня ядра

Управление протоколированием поддерживается на уровне API, смотри «ЖТЯИ.00101-01 96 01. КриптоПро CSP. Руководство программиста».

Значением параметра уровень протокола является битовая маска:

N_DB_ERROR = 1 # сообщения об ошибках

N_DB_LOG = 8 # сообщения о вызовах

Значением параметра формат протокола является битовая маска:

DBFMT_MODULE = 1 # выводить имя модуля

DBFMT_THREAD = 2 # выводить номер нитки

DBFMT_FUNC = 8 # выводить имя функции

DBFMT_TEXT = 0x10 # выводить само сообщение

DBFMT_HEX = 0x20 # выводить HEX дамп

DBFMT_ERR = 0x40 # выводить GetLastError

Лист регистрации изменений

[illegible]