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 R2 KC1
Исполнение 1-Base
Руководство администратора
безопасности.
Использование СКЗИ
под управлением ОС FreeBSD

ЖТЯИ.00101-02 91 04
Листов 26

2021 г

Содержание

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционных систем FreeBSD.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС FreeBSD, 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 «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС FreeBSD используется в программно-аппаратных средах:

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.00101-02 30 01. КриптоПро CSP. Формуляр, п. 3.10.

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, использующиеся 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).

Примечание. Для автоматической установки основных пакетов СКЗИ можно воспользоваться скриптом `install.sh`, входящим в состав дистрибутива.

Для удаления СКЗИ используйте скрипт `uninstall.sh`.

Для установки пакета используется команда:

```
pkg_add <файл_пакета>
```

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

(`pkg install <файл_пакета>` для FreeBSD 11+)

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 (для простоты описаны 32-битные пакеты)

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
cpro-base		Базовый пакет КриптоПро CSP, устанавливается первым
cpro-rdr	cpro-base	Модуль поддержки основных приложений, считывателей и ДСЧ

cpro-kc1	cpro-rdr	Провайдер класса KC1
cpro-kc2	cpro-rdr	Провайдер класса KC2, 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-rdr-gui-gtk	cpro-rdr	Графический интерфейс для диалоговых операций
cpro-rdr-pcsc	cpro-rdr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт
cpro-pkcs11	cpro-rdr	Модуль поддержки PKCS11
cpro-devel	cpro-base	Пакет для разработчика приложений, использующих КриптоПро CSP
cpro-drv	cpro-base	Драйверная библиотека
cpro-drv-devel	cpro-devel	Пакет для разработчика драйверов
cpro-curl	cpro-capilite	Библиотека libcurl с поддержкой российских криптоалгоритмов
cpro-rdr-cloud	cpro-capilite	Модуль взаимодействия с КриптоПро DSS — КриптоПро Cloud CSP
cpro-stunnel	cpro-capilite	Универсальный SSL/TLS туннель
cpro-ca-certs	cpro-capilite	Корневые сертификаты доверенных ЦС
cpro-ipsec-devel	cpro-devel	Пакет для разработчика приложений, использующих КриптоПро IPsec
cpro-ipsec-esp		Модуль ядра (LKM) КриптоПро IPsec ESP
cpro-ipsec-genpsk	cpro-rdr	Утилиты PSK
cpro-ipsec-ike	cpro-rdr	Динамические библиотеки уровня пользователя
Поддержка ключевых носителей		
cpro-rdr-cpfkc	cpro-rdr-pcsc	Модуль поддержки ФКН с поддержкой SESPAKE
cpro-rdr-edoc	cpro-rdr-pcsc	Модуль поддержки платформы eDoc (УЛГ)
cpro-rdr-emv	cpro-rdr-pcsc	Модуль поддержки смарт-карт Gemalto (EMV)
cpro-rdr-infocrypt	cpro-rdr-pcsc	Модуль поддержки токенов InfoCrypt
cpro-rdr-inpaspot	cpro-rdr-pcsc	Модуль поддержки смарт-карт Alioth
cpro-rdr-kst	cpro-rdr-pcsc	Модуль поддержки смарт-карт MorphoKST
cpro-rdr-mskey	cpro-rdr-pcsc	Модуль поддержки токенов Multisoft MS_Key
cpro-rdr-novacard	cpro-rdr-pcsc	Модуль поддержки смарт-карт Novacard
cpro-rdr-rosan	cpro-rdr-pcsc	Модуль поддержки смарт-карт Rosan
cpro-rdr-rutoken	cpro-rdr-pcsc	Модуль поддержки смарт-карт и токенов Рутокен

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС FreeBSD необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
  - набор установленных пакетов;
  - настройки провайдера (для простоты можно сохранить /etc/opt/cprocsp/config[64].ini);
- удалить штатными средствами ОС все пакеты СКЗИ;
- установить аналогичные новые пакеты СКЗИ;
- при необходимости внести изменения в настройки (можно посмотреть diff старого и нового config[64].ini);
- ключи и сертификаты сохраняются автоматически.

4 Настройка СКЗИ

4.1 Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/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 cpconfig из соответствующей папки.

4.2 Ввод серийного номера лицензии

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

Для просмотра информации о лицензии выполните:

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

Для ввода лицензии выполните:

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

Серийный номер следует вводить с соблюдением регистра символов.

4.3 Настройка оборудования СКЗИ

Утилита cpconfig также предназначена для изменения набора устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел. Предустановленными являются считыватели flash-носителей и образ дискеты на жестком диске.

Для просмотра списка настроенных считывателей:

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

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

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

Для просмотра списка настроенных ДСЧ:

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

Для консольного БиоДСЧ требуется пакет cpro-kc1. Для добавления консольного БиоДСЧ:

```
# ./cpconfig -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 "АРМ 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-rdp. 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. Существует возможность изменения настроек журналирования различных модулей СКЗИ. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений.

Для получения справки по настройкам журналирования:

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

Подробнее опции управления протоколированием модулями СКЗИ см. в Приложении А.

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 Состав и назначение компонент ПО СКЗИ

5.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

`libcsp`	динамически загружаемая библиотека КриптоПро CSP; реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
`libcspr`	обеспечивает удаленный доступ к криптопровайдеру, функционирующему как отдельный сервис
`drvcsp`	динамически загружаемый модуль ядра; реализует целевые функции криптографической защиты информации (кроме формирования ЭП) и работу с ключами
`libssp`	обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS (общее описание протокола приведено в документе ЖТЯИ.00101-02 90 01. Описание реализации)
`cpverify`	модуль контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на ПЭВМ пользователя
`wipefile`	модуль удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях
`cryptcp`	приложение командной строки для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов (подробное описание см. в ЖТЯИ.00101-02 93 01. Приложение командной строки для подписи и шифрования файлов)
`certmgr`	приложение командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами (подробное описание см. в ЖТЯИ.00101-02 93 02. Приложение командной строки для работы с сертификатами)
`stunnel`	приложение для создания TLS-туннеля, предназначенного для создания TLS защищенного соединения между клиентом и локальным (Iinetd-запускаемым) или удаленным сервером (подробное описание см. в ЖТЯИ.00101-02 93 03. Приложение для создания TLS-туннеля)

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

5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

5.2.1 Модуль libcapi20

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

5.2.2 Модули устройств хранения ключевой информации

Библиотека librdrsup обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевой информации.

Следующие модули обеспечивают реализацию доступа к конкретным типам ключевых носителей:

`librdrcpfkc.so`	токены и смарт-карты с поддержкой SESPAKE
`librdrcloud.so`	облачный токен
`librdredoc.so`	платформа eDoc (УЛГ)
`librdremv.so`	смарт-карты Gemalto (EMV)
`librdrfat12.so`	съемные диски и раздел HDD/SDD
`librdrinfocrypt.so`	токены InfoCrypt
`librdrinpaspot.so`	смарт-карты Alioth
`librdrkst.so`	смарт-карты MorphoKST
`librdrmskey.so`	токены Multisoft MS_Key
`librdrnova.so`	смарт-карты Novacard
`librdrpcsc.so`	базовый считыватель носителей, поддерживающих интерфейс PC/SC
`librdrric.so`	смарт-карты Оскар и Форос (Магистра)
`librdrrosan.so`	смарт-карта Rosan
`librdrrutoken.so`	смарт-карты и токены Рутокен

5.2.3 Модули датчиков случайных чисел

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

5.2.4 Библиотека libasn1data поддержки протокола ASN1

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

6 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 ЖТЯИ.00101-02 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).

6.1 Организационно-технические меры защиты от НСД

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

1) Всех пользователей, которые не пользуются установленной ОС (включая стандартных пользователей, которые создаются в ОС во время установки, кроме пользователя root), следует удалить.

2) Необходимо установить минимально необходимый в соответствии с принятой в организации политикой безопасности перечень файлов, для которых требуется запуск с правами пользователя root (установлен флаг SUID). Запуск не входящих в этот перечень файлов с установленным флагом SUID должен контролироваться администратором.

3) Рекомендуется ограничить (с учетом принятой в организации политики безопасности) использование пользователями команд планирования задач и пакетной обработки заданий (например, cron и at). Для нормального функционирования системы минимально необходимым является разрешение использования данных команд только пользователю root (например, путем добавления имени root в файл `/etc/<command>.allow`).

4) Должно быть реализовано физическое затирание конфиденциальной информации с использованием программы wipefile из состава СКЗИ.

5) Права доступа к системным и критичным каталогам, общим ресурсам должны быть установлены в соответствии с политикой безопасности, принятой в организации. На все директории, содержащие системные файлы ОС и файлы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем, кроме Владельца (Owner).

6) По окончании работы СКЗИ содержимое виртуальной памяти ОС 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. В случае выхода из строя диска, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а диск считается не подлежащим ремонту и уничтожается по правилам уничтожения ключевых носителей.

6.2 Дополнительные настройки ОС FreeBSD

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=10 (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 протоколировать 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 umask=077 или umask=027;

3) В файл `/etc/shells` поместить имена только тех исполняемых файлов оболочек, которые установлены в системе.

4) Удалить файл (если он существует) `/.rhosts` из домашних каталогов всех пользователей, включая учетную запись root.

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

6) Запретить rhosts-аутентификацию (например, с помощью комментирования строк, содержащих подстроку "pam_rhosts_auth.so в файле `/etc/pam.conf`).

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.

Ограничения при монтировании файловых систем

- В файле `/etc/fstab` установить опцию монтирования nosuid для файловой системы `/var`.
- Для предотвращения переполнения критичных файловых систем и обеспечения возможности монтирования файловой системы `/usr` в режиме «только для чтения» рекомендуется при инсталляции ОС выделить для файловых систем `/, /usr, /usr/local, /var` разные разделы диска.

Настройка сетевых сервисов

1) Следует ограничить функциональность демона управления сетевыми соединениями inetd (xinetd), если он используется в системе (например, с помощью редактирования файла `/etc/inetd.conf` и файлов в каталоге `/etc/inetd.d`). Следует запретить следующие сервисы (при их наличии в системе):

- 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) Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора, необходимо отключить пересылку IP-пакетов (IP Forwarding).

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

4) Запустить процедуру регистрации запуска процессов (accounting);

5) Если планируется использовать на настраиваемом сервере сервис FTP, необходимо установить перечень пользователей, для которых запрещен (в соответствии с принятой политикой безопасности) доступ к серверу по протоколу FTP (например, путем редактирования файла `/etc/ftpusers`). Следует запретить доступ по FTP для следующих пользователей (при их наличии в системе):

- root
- daemon
- bin
- sys
- sync
- adm
- lp
- mail
- smtp
- uucp
- nuucp
- listen
- nobody
- noaccess

6) Следует ограничить доступ к системным файлам для непривилегированных пользователей (в соответствии с принятой политикой безопасности), например, с помощью выполнения команд:

```
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
```

7) Следует обнулить флаг SGID для некоторых исполняемых файлов (при их наличии в системе):

```
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.).

Для ограничения количества «видимой извне» информации рекомендуется:

• отказаться от стандартного «заголовка», выводимого сервером ftp при ответе пользователю (например, путем указания в файле `/etc/vsftpd/vsftpd.conf` параметра `ftpd_banner`)

• отредактировать файлы `/etc/issue`, `/etc/banners/ftp.msg` и `/etc/motd` с целью разъяснения пользователям правил и политики доступа к серверу ftp.

Настройка подсистемы протоколирования и аудита

1) Установить права на запись в следующие файлы (при их наличии в системе) только для пользователя root:

- /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 протоколировать попытки использования программ su и sudo, например, с помощью добавления в файл `/etc/syslog.conf` строк:

```
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 протокол, например, путем выполнения команд:

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

6) Следует обеспечить протоколирование сетевых соединений, контролируемых демоном inetd (включая дату/время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), например, путем добавления в файл `/etc/syslog.conf` строки:

```
daemon.notice                 /var/log/syslog
```

и заменой в файле `/etc/rc2.d/S72inetsvc` строки

```
/usr/sbin/inetd -s
```

на

```
/usr/sbin/inetd -s -t.
```

7 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-02 95 01. КриптоПро CSP. Правила пользования в части, касающейся ОС FreeBSD.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 6.2.

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/libcpext.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/librdrrndmbio_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/librdrrndm.so.4
/opt/cprocsp/lib/ia32/librdrsup.so.4
/opt/cprocsp/lib/ia32/librdrdsrf.so.4
/opt/cprocsp/lib/ia32/librdrfat12.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/librdremv.so.4
/opt/cprocsp/lib/ia32/librdrpcsc.so.4
/opt/cprocsp/lib/ia32/librdrric.so.4
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/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/inittst
/opt/cprocsp/bin/amd64/csptestf
/opt/cprocsp/bin/amd64/der2xer
/opt/cprocsp/lib/amd64/libcapi20.so.4
/opt/cprocsp/lib/amd64/libcpext.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/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.1000510/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.802000/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.803000/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.804000/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.901000/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.902001/drvcsp.ko
/opt/cprocsp/modules/amd64/kern.osreldate.903000/drvcsp.ko
/opt/cprocsp/lib/amd64/libcpcdrv_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/librdrrndmbio_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/librdrrndm.so.4
/opt/cprocsp/lib/amd64/librdrsup.so.4
/opt/cprocsp/lib/amd64/librdrdsrf.so.4
/opt/cprocsp/lib/amd64/librdrfat12.so.4
/opt/cprocsp/lib/amd64/libcapi10.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/librdremv.so.4
/opt/cprocsp/lib/amd64/librdrpcsc.so.4
/opt/cprocsp/lib/amd64/librdrric.so.4
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/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

Уровень, содержание и методы вывода информации независимо устанавливаются для выделенных модулей аудита (см. табл. А1). Несколько библиотек могут использовать один модуль аудита, возможна и обратная ситуация.

Таблица А1. Модули аудита

Модуль (name)	**Описание**
`capi10`	CryptoAPI 1.0
`capi20`	CryptoAPI 2.0
`ssp`	TLS
`cspr`	клиентский RPC
`cpext`	расширения CryptoAPI
`cloud`	облачный провайдер
`csp`	ядро CSP
`pcsc`	считыватели PC/SC

Для определения **уровня протокола** (`levelmask`, см. табл. А2):

```
/usr/ cpro-csp/sbin/cpconfig -loglevel <name> -mask <levelmask>
```

Для задания **формата протокола** (`formatmask`, см. табл. А3):

```
/usr/ cpro-csp/sbin/cpconfig -loglevel <name> -format <formatmask>
```

Для просмотра текущих значений уровня и формата протокола:

```
/usr/ cpro-csp/sbin/cpconfig -loglevel <name> -view
```

Таблица А2. Уровни протоколирования

N_DB_ERROR = 1 (0x01)	критические ошибки
N_DB_WARN = 2 (0x02)	некритические ошибки
N_DB_CALL = 4 (0x04)	информация о вызове функции
N_DB_LOG = 8 (0x08)	нейтральная информация
N_DB_TRACE = 16 (0x10)	отладочная информация
N_DB_CRUCIAL = 32 (0x20)	информация о важных событий (например, создание ключа, удаление ключевого контейнера, ...)

Таблица А3. Форматы протокола

DBFMT_MODULE = 0x01	выводить имя модуля
DBFMT_THREAD = 0x02	выводить номер нитки
DBFMT_FLINE = 0x04	выводить номер линии
DBFMT_FUNC = 0x08	выводить имя функции
DBFMT_TEXT = 0x10	выводить само сообщение
DBFMT_HEX = 0x20	выводить HEX дамп
DBFMT_ERR = 0x40	выводить GetLastError
DBFMT_PID = 0x80	выводить идентификатор процесса
DBFMT_PROCESS = 0x100	выводить имя процесса

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					