127 018, Москва, Сущевский вал, д.16/5
Телефон: (495) 780 4820
Факс: 4095) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 3.6

Руководство администратора безопасности

Использование СКЗИ под управлением ОС FreeBSD

ЖТЯИ.00050-02 90 02-03
Листов 17

2010

- 2 -

Содержание

1. Аннотация

Настоящее Руководство дополняет документ "ЖТЯИ.00050-02 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть" при использовании СКЗИ под управлением ОС FreeBSD.

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

2. Список сокращений

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

3. Основные технические данные и характеристики СКЗИ

СКЗИ ЖТЯИ.00050-02 разработано в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

3.1. Программно-аппаратная среда

СКЗИ ЖТЯИ.00050-02 под управлением ОС FreeBSD используется в программно-аппаратных средах ОС FreeBSD 7/8 (IA32).

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

<http://www.freebsd.org/security/security.html> и
<http://lists.freebsd.org/pipermail/freebsd-stable/2008-April/041676.html>.

3.2. Варианты исполнения СКЗИ

СКЗИ ЖТЯИ.00050-02 для работы с ОС FreeBSD 7/8 изготовляется и распространяется в двух вариантах исполнения:

Исполнение 1 – СКЗИ класса защиты КС1.

Исполнение 2 – СКЗИ класса защиты КС2.

3.3. Ключевые носители

В качестве ключевых носителей закрытых ключей могут использоваться:

ГМД 3,5’’;
USB диски
Раздел HDD ПЭВМ

Примечания. 1. Допускается хранение закрытых ключей в разделе HDD при условии распространения на HDD или ПЭВМ с HDD требований по обращению с ключевыми носителями, в том числе и после удаления ключей.

2. Перечень ключевых носителей по исполнениям СКЗИ и программно-аппаратным платформам см. Формуляр ЖТЯИ.00050-02 30 01, п.п. 3.8, 3.9.

4. Состав и назначение компонент программного обеспечения СКЗИ

4.1. Базовые модули СКЗИ

ПО СКЗИ содержит базовые модули:

libcsp – динамически загружаемая библиотека КриптоПро CSP.

libcspf - библиотека работы с удалённым КриптоПро CSP

libcspdrv – 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);

i386 – платформа Intel.

4.1.1. Библиотека libcsp

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

4.1.2. Библиотека libcspf

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

4.1.3. Драйверная библиотека libcspdrv

Библиотека **libcspdrv**, используемая как динамически загружаемый модуль ядра ОС, реализует целевые функции криптографической защиты информации (кроме формирования ЭЦП) и работу с ключами.

4.1.4. Модули сетевой аутентификации КриптоПро TLS

Модуль **libssp** обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS. Общее описание протокола приведено в соответствующем разделе документа ЖТЯИ.00050-02 90 0 2. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

Протокол TLS (RFC 2246) 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.

4.1.5. Модуль cpverify

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

4.1.6. Модуль wipefile

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

4.2. Модули ПКЗИ

4.2.1. Модуль libcapilite

Модуль **libcapilite** 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.

4.2.2. Библиотека librdrrdr

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

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

- **librdrfat12** к дисководу и дискете 3.5" и разделу жесткого диска
- **librdrpcsc** к считывателям смарт-карт и eToken, поддерживающим интерфейс PC/SC

4.2.4. Библиотека librdrsup

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

4.2.5. Модули датчиков случайных чисел

Библиотеки **librdrrndm** и **librdrrndmbio** обеспечивают поддержку работы с физическими датчиками случайных чисел.

4.2.6. Библиотека libasn1data поддержки протокола ASN1

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

5. Установка дистрибутива ПО КриптоПро CSP

Установка, удаление и обновление ПО осуществляется с правами администратора: под учётной записью root или с использованием команды sudo.

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).

Для установки пакета используется команда:

pkg_add <файл_пакета>

Например: **pkg_add ./CPRObase-3.6.1_0.tbz**

Для удаления пакета используется команда:

pkg_delete <имя_пакета>

Например: **pkg_delete CPRObase-3.6.1_0**

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.

Таблица зависимостей и назначения пакетов.

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
CPRObase-…		Базовый пакет, ставится первым.
CPROrdr-…	CPRObase-…	Основные приложения, считыватели и ДСЧ.
CPROcpl-…	CPROrdr-…	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS…).
CPROkc1-…	CPROrdr-…	Провайдер КС1.
CPROkc2-…	CPROrdr-…	Провайдер КС2, ставится только там, где в этом есть необходимость. В этом случае CPROkc1-… не ставится.
Дополнительные пакеты		
CPROrdg-…	CPROrdr-…, open-motif, XFree86-libraries	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги.

- 7 -

CPROrdp-…	CPROrdr-…, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт (РИК, Оскар, Магистра…).
CPROcspd-…	CPRObase-…	Пакет для разработчика.
CPROdrv-…	CPRObase-…	Драйверная библиотека.
CPROdrvd-…	CPROcspd-…	Пакет для разработчика драйверов.
CPROstnl-…	CPRObase-…	Универсальный SSL/TLS туннель.

6. Обновление СКЗИ КриптоПро CSP

Для обновления КриптоПро CSP на ОС FreeBSD 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 КриптоПро CSP
- установить аналогичные новые пакеты КриптоПро CSP
- при необходимости внести изменения в настройки (можно посмотреть diff старого и нового config[64].ini)
- ключи и сертификаты сохраняются автоматически

7. Настройка СКЗИ КриптоПро CSP

7.1. Доступ к утилите для настройки СКЗИ КриптоПро CSP

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.

7.2. 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.

7.3. Настройка оборудования СКЗИ КриптоПро CSP

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/list_pcsc
```

available reader: Gemplus GemPC Twin 00 00

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
```

7.4. Установка параметров журналирования

СКЗИ КриптоПро CSP позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал (обычно в /var/log/messages). Существует возможность изменения настроек журналирования различных модулей продукта. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений. Для получения справки по настройкам журналирования:

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

Модули, для которых поддерживается журналирование:

cpcsp - ядро криптопровайдера

capi10 - CryptoAPI 1.0

cpext

capi20 - CryptoAPI 2.0

capilite - CAPILite

libcspr

cryptsrv - служба хранения ключей (КС2)

libssp - TLS

cppkcs11 - PKCS11

cpdrv - драйвер

dmntcs

7.5. 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>
```

8. Встраивание СКЗИ КриптоПро CSP в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 7 документа "ЖТЯИ.00050-02 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

9. 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 раздела 12 документа "ЖТЯИ.00050-02 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

9.1. Общие меры защиты от НСД ПО с установленными СКЗИ для ОС FreeBSD

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 ЖТЯИ.00050-02 под управлением ОС FreeBSD 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 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 электронного замка (см. соответствующий раздел в документе ЖТЯИ.00050-02 90 0 2. КриптоПро CSP. Руководство администратора безопасности. Общая часть.), что означает:

1. Выполнение загрузки с фиксированного носителя;
2. Обеспечение контроля целостности ОС и прикладного программного обеспечения до загрузки на загрузочном диске и других подключенных дисках.

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

9.1.1. Организационно-технические меры

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

9.1.1.2. 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.

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.

9.1.1.3. 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.

9.1.1.4. 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.

9.1.1.5. 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 администратору.

9.1.1.6. 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.

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

9.1.1.8. 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.

9.1.1.9. При использовании СКЗИ ЖТЯИ.00050-02 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.

9.1.1.10. Право доступа к рабочим местам с установленным ПО СКЗИ «КриптоПро CSP» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ ЖТЯИ.00050-02

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

9.1.1.12. В BIOS определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске: 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.

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

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

9.1.1.15. При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ ЖТЯИ.00050-02, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ с использованием программы CPVERIFY.

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

9.1.1.17. На компьютере устанавливается только одна ОС. На компьютере 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 ЖТЯИ.00050-02. Следует избегать попадания в систему программ, позволяющих при ошибках ОС получать привилегии root.

9.1.1.18. Ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время.

9.1.1.19. Реализовать физическое затирание содержимого удаляемых файлов с использованием программы Wipefile из состава СКЗИ.

9.1.1.20. Отключить сетевые протоколы, которые не используются на данной ЭВМ.

9.1.1.21. В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных отключить использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, в прикладных программах.

9.1.1.22. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ ЖТЯИ.00050-02, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

9.1.1.23. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ ЖТЯИ.00050-02 после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

9.1.1.24. 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 компьютера или ОС FreeBSD.

9.1.1.25. После инсталляции ОС FreeBSD следует установить с сайта http://www.freebsd.org/ все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

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

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

9.1.1.28. В ОС FreeBSD используется виртуальная память. Область виртуальной памяти должна быть организована на отдельном жестком диске. По окончании работы СКЗИ содержимое виртуальной памяти должно затираться с использованием средств ОС. В случае аварийного останова ЭВМ, при следующей загрузке необходимо в режиме “single user” очистить область виртуальной памяти программой wipefile, входящей в состав СКЗИ ЖТЯИ.00050-02. В случае выхода из строя жесткого диска, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а жесткий диск считается не подлежащим ремонту. Этот жесткий диск уничтожается по правилам уничтожения ключевых носителей.

9.1.2. 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).

9.1.2.1. Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

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

   Login-retries=3 (задает число повторных попыток регистрации пользователя программой login)

   passwordtime=30d для ограничения срока действия пароля 30-ю 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 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 убедится, 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	uucp
bin	nuucp
sys	listen
adm	nobody
lp	noaccess
smtp	

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

9.1.2.2. Ограничения при монтировании файловых систем

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

1. 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".

9.1.2.3. Ограничения на запуск процессов

1. 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

9.1.2.4. Настройка сетевых сервисов

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

   Как минимум, следует запретить следующие сервисы:

echo	systat
discard	netstat
daytime	tftp
chargen	telnet
finger	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. Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора, необходимо запретить маршрутизацию, выполнив команду sysctl –w net.inet.ip.forwarding=0.
4. Следует запретить прием из внешней сети "широковещательных" (broadcast) пакетов, а также передачу ответов на принятые "широковещательные" пакеты.
5. Запретить суперпользователю доступ по ftp, для этого добавить "root" в файл /etc/ftpusers
6. 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
noaccess	

2. 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
```

3. 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
```

9.1.2.5. 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/ftpwelcome следующих директив:

```
BANNER=""
```

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

9.1.2.6. Настройка подсистемы протоколирования и аудита

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

```
auth.notice     /var/log/authlog
```

или

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

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

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

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

5. 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

10. Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 12 документа ЖТЯИ.00050-02 90 02 в части, касающейся ОС FreeBSD.

Конкретно должны выполняться требования:

1. Использование только лицензионного системного программного обеспечения.
2. Настройка операционной системы для работы с СКЗИ по п. 7.
3. При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.
4. Исключение из программного обеспечения ПЭВМ с установленным СКЗИ средств отладки.
5. СКЗИ должно эксплуатироваться на рабочих станциях и серверах с установленными средствами антивирусной защиты, сертифицированными Федеральной Службой Безопасности РФ по классу Б2 для рабочих станций.
6. 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.
7. Периодичность тестового контроля криптографических функций - 10 минут.
8. Ежесуточная перезагрузка ПЭВМ.
9. Периодичность останова ПЭВМ с обязательной проверкой системы охлаждения процессорного блока ПЭВМ - 1 месяц.
10. **Запрещается** использовать режим простой замены (ECB) ГОСТ 28147-89 для шифрования информации, кроме ключевой.
11. Должно даваться предупреждение о том, что при использовании режима шифрования CRYPT_SIMPLEMIX_MODE материал, обрабатываемый на одном ключе, автоматически ограничивается величиной 4 MB.
12. При функционировании СКЗИ должны выполняться требования эксплуатационной документации на ПАК защиты от НСД.
13. Должно быть запрещено использование СКЗИ для защиты телефонных переговоров без принятия в системе мер по защите от информативности побочных каналов, специфических при передаче речи.
14. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.
15. Перед началом работы СКЗИ необходимо провести контроль целостности.
16. Контролем целостности должны быть охвачены файлы:

FreeBSD (32-bit)

libcspr.so.3, libcspr.la, libcsp_kc2.so.3, libcsp_kc2.la, cryptsrv, cryptcp, certmgr, inittst, csptestf, der2xer, sv, libcapi20.so.3, libcapi20.la, libcpext.so.3, libcpext.la, libcapilite.so.3, libcapilite.la, libpkixcmp.so.3, libpkixcmp.la, libasn1data.so.3, libasn1data.la, libssp.so.3, libssp.la, libcsp.so.3, libcsp.la, librdrrndmbio_tui.so.3, librdrrndmbio_tui.la, set_driver_license.sh, libcpcdrv_emul.a, pkcs11_initialize, pkcs11_set_pin, pkcs11_generate_key, pkcs11_generate_key_pair, pkcs11_hash, pkcs11_sign, pkcs11_verify, pkcs11_sign_hash, pkcs11_verify_hash, pkcs11_encrypt, pkcs11_decrypt, pkcs11_save_state, pkcs11_encrypt_sign, libcppkcs11.so.1, libcppkcs11.la, libcsppkcs11.so.1, libcsppkcs11.la, list_pcsc, librdrpcsc.so.3, librdrpcsc.la, librdrric.so.3, librdrric.la, cpverify, wipefile, csptest, librdrrdr.so.3, librdrrdr.la, librdrrndm.so.3, librdrrndm.la, librdrsup.so.3, librdrsup.la, librdrdsrf.so.3, librdrdsrf.la, librdrfat12.so.3, librdrfat12.la, libcapi10.so.3, libcapi10.la, libcpui.so.3, libcpui.la, cpconfig, mount_flash.sh.

- 17 -

Приложение 1. Контроль целостности программного обеспечения

Программное обеспечение СКЗИ КриптоПро CSP имеет средства обеспечения контроля целостности ПО СКЗИ, которые должны выполняются периодически. Вместе с дистрибутивом поставляются файлы с именами **hashes.<dist_name>**, содержащие контрольные значения хеш-функции на файлы дистрибутива <dist_name>. Строки каждого такого файла состоят из двух полей – имени файла и значения хеш-функции на него. Файлы проверяются при помощи утилиты **cpverify.** Например, возможен следующий фрагмент кода для проверки всех файлов всех дистрибутивов:

```
eval `cat hashes.*|awk '{print "cpverify "$0" && " }END{print "true"}'`
```

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.

- 18 -

Приложение 2. Управление протоколированием

Для включения/отключения значение log используйте:

a) FreeBSD

Для задания уровня протокола

/usr/CPROcsp/sbin/cpconfig –loglevel cpcsp -mask 0x9

Для задания формата протокола

/usr/CPROcsp/sbin/cpconfig –loglevel cpcsp - format 0x19

Для просмотра маски текущего уровня и формата протокола

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

b) для FreeBSD уровня ядра

Не поддерживается.

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

- 19 -

Лист регистрации изменений

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

- 20 -