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

КРИПТОПРО

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 КС1
1-Base
Руководство администратора
безопасности.
Использование СКЗИ
под управлением ОС Mac OS

ЖТЯИ.00101-01 91 07
Листов 28

2019 г

© 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

Аннотация

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

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро 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

СКЗИ КриптоПро CSP разработана в соответствии с криптографическим интерфейсом фирмы Microsoft — Cryptographic Service Provider (CSP).

1.1 Программно-аппаратные среды функционирования

СКЗИ КриптоПро CSP версии 5.0 КС1 (ЖТЯИ.00101-01) под управлением ОС Mac OS X используется в программно-аппаратных средах:

Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14 (x64).

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

http://www.apple.com/support/

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-01 30 01. КриптоПро 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 Mac OS X для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. Дистрибутив поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет.

Для управления пакетами используются стандартные средства для управления пакетами Mac OS.

Для **установки пакета через графический интерфейс** откройте двойным щелчком образ диска с дистрибутивом (dmg), а затем двойным щелчком по файлу пакета (mpkg) запустите установку. Для установки следуйте указаниям мастера. После завершения установки можно отмонтировать диск стандартными средствами ОС.

Для **установки из командной строки** примонтируйте диск:

```
hdiutil attach ru.cryptopro.csp-5.0.dmg
```

Установите пакет при помощи системной утилиты installer:

```
cd /Volumes/ru.cryptopro.csp-5.0
```

```
installer -pkg ru.cryptopro.csp-5.0.mpkg -target "/"
```

Отмонтируйте диск:

```
hdiutil detach /Volumes/ru.cryptopro.csp-5.0
```

Для **удаления пакета** используется скрипт `uninstall_csp`, который поставляется вместе с дистрибутивом. Необходимо запустить данный скрипт с правами суперпользователя.

Файлы из пакетов устанавливаются в `/opt/cprocsp`.

Пакет дистрибутива КриптоПро CSP содержит в себе более мелкие пакеты, обеспечивающие работу разных подсистем криптопровайдера. При установке КриптоПро CSP можно выборочно устанавливать эти пакеты. При этом некоторые пакеты являются обязательными и будут установлены в любом случае, некоторые — дополнительными и их можно устанавливать или не устанавливать в зависимости от предполагаемого использования КриптоПро CSP. Краткое описание пакетов дано в таблице назначения пакетов (см. табл. 1).

Пакеты имеют архитектуру universal binary и содержат в себе 32-разрядную (i386) и 64-разрядную (x86_64) подсистемы.

Таблица 1. Назначения пакетов

Имя пакета	Назначение пакета
Обязательные пакеты	
CPRObase	Базовый пакет, устанавливается первым.
CPROrdr	Основные приложения, считыватели и ДСЧ.
CPROkc1	Провайдер КС1.
CPROcpl	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS. . .).
Дополнительные пакеты	
CPROcspd	Пакет для разработчика. Пакет будет установлен по умолчанию.
CPROcurl	Утилита curl и библиотека libcurl для работы с сетью с поддержкой SSL/TLS через КриптоПро CSP. Пакет будет установлен по умолчанию.
CPROp11	Интерфейс PKCS11 для доступа к фукнциям криптопровайдера. Пакет не будет установлен по умолчанию.
CPROrdp	Модули поддержки PCSC-считывателей, смарт-карт (РИК, Оскар, Магистра. . .). Пакет не будет установлен по умолчанию.
CPROdrvd	Пакет для разработчика драйверов. Пакет не будет установлен по умолчанию.
CPROstnl	Универсальный SSL/TLS туннель. Пакет не будет установлен по умолчанию.
CPROrdemv	Модуль поддержки EMV.

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Mac OS необходимо:

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

4 Настройка СКЗИ

4.1 Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/cprocsp/sbin/.

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 CPROkc1. Для добавления консольного БиоДСЧ:

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

Для графического БиоДСЧ требуется пакет CPROrdg 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/cprocsp/dsrf/
db1/kis_1

# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/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/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/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/system.log), так же может быть использована утилита «Консоль», являющаяся удобным инструментом просмотра системных событий в Mac OS. 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 — дополнения для CryptoAPI 2.0
- capi20 — CryptoAPI 2.0
- capilite — CAPILite
- libcspr — библиотека для подключения к провайдеру в сервисе или к HSM-серверу
- cryptsrv — служба хранения ключей
- libssp — TLS
- cppkcs11 — PKCS11
- cpdrv — драйвер
- dmntcs — тестовое приложение для обращения к тестовому драйверу

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>
```

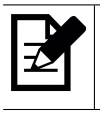
4.6 Включение режима усиленного контроля использования ключей

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.

В состав дистрибутива КриптоПро CSP входит пакет CPROcurl(CPROcurlx), включающий в себя libcurl. Libcurl из состава CSP переработана и поддерживает TLS по российским криптографическим алгоритмам с КриптоПро CSP в качестве криптопровайдера.

Допускается использование оригинальной libcurl, которую можно скачать с сайта разработчика проекта. На сайте доступен пакет с исходными текстами для самостоятельной сборки. Как правило, там же есть бинарные пакеты. Оригинальная библиотека не поддерживает TLS по российским криптографическим алгоритмам с КриптоПро CSP в качестве криптопровайдера.

После установки библиотек надо зарегистрировать пути к ним. Например:

```
# /opt/cprocsp/sbin/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».
- drvcsp — динамически загружаемый модуль ядра.
- libssp — библиотека поддержки модуля сетевой аутентификации «КриптоПро TLS».
- cpverify — модуль контроля целостности.
- wipefile — модуль удаления файлов вместе с содержимым.

В названиях дистрибутивов СКЗИ 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, клавиатурный ДСЧ.

6.1.2 Библиотека libcspr

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

6.1.3 Драйверная библиотека drvcsp

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

6.1.4 Модули сетевой аутентификации КриптоПро TLS

Модуль libssp обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS. Общее описание протокола приведено в документе ЖТЯИ.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 libcapi20

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

6.2.2 Библиотека librdrrdr

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

6.2.3 Модули устройств хранения ключевой информации

Модули обеспечивают реализацию 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
- librdremv к ключевым носителям EMV и Gemalto
- librdrrtsupcp к ключевым носителям Rutoken

6.2.4 Библиотека librdrsup

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

6.2.5 Модули датчиков случайных чисел

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

7 Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ КриптоПро CSP версии 5.0 КС1 в прикладное программное обеспечение должны выполняться требования раздела 8 документа ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и документа ЖТЯИ.00101-01 96 01. КриптоПро CSP. Руководство программиста.

При установке пакета для разработчика (CPROcspd) в директорию /Library/Frameworks будет помещён CPROCSP.framework, содержащий в себе библиотеки CSP. При линковке с фреймворком необходимо указать в параметрах линковщика `-flat_namespace`. При сборке из командной строки флаг указывается в командной строке; при сборке в XCode флаг указывается в «Project – Edit Project Settings – Build – Linking – Other Linker Flags».

При сборке многопоточных приложений настоятельно рекомендуется линковать исполняемый файл с CoreFoundation (добавить в опции линкера «–framework CoreFoundation» либо настроить линковку через свойства проекта в XCode). Это важно для многопоточных приложений, поскольку ввиду особенностей MacOS нельзя производить первое открытие фреймворков, зависящих от CoreFoundation (таких как PCSC), не из главного потока. Поэтому, в случае если на компьютере клиента CSP настроен на работу со смарт-картами, многопоточное приложение, использующее CSP и не слинкованное с CoreFoundation, может не работать и падать в системных функциях инициализации CoreFoundation (CFInitialize()).

8 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 Mac OS X 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).

8.1 Организационно-технические меры защиты от НСД

Для ОС Mac OS X 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 Mac OS X, настраивать безопасность ОС Mac OS X, а также конфигурировать ПЭВМ, на которую установлена ОС Mac OS X.

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 Mac OS X, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в ОС Mac OS X, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Mac OS X, 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 Mac OS X во время установки (таких, как sys, uucp, nuucp и listen), кроме пользователя root, следует удалить.

5) В ОС Mac OS X 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 при использовании ПАК защиты от НСД.

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

12) Вход в BIOS 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 Mac OS X.

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

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

23) После инсталляции ОС Mac OS X следует установить все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

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

25) 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.

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

8.2 Дополнительные настройки ОС Mac OS X

Дополнительные настройки ОС Mac OS X 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 cpverify.

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

Настройки ОС Mac OS X 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) Настройте операционную систему в соответствии с руководством http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf (для Snow Leopard; если Вы используете более новую версию ОС используйте аналогичное руководство для Вашей версии ОС). Для ограничения доступа в систему выполните следующие пункты руководства:

- Chapter 2 «Installing Mac OS X» - «Initial System Setup» - «Turning Off Auto-login»
- Chapter 4 «Securing Global System Settings» - «Configuring Access Warnings» - «Enabling Access Warnings for the Login Window»

- Chapter 6 «Securing Accounts» - «Setting Global Password Policies»
- Задайте маску по умолчанию для создания файлов 022 так, как это описано в Chapter 7 «Securing Data and Using Encryption» - «Changing Global Umask for Stricter Default Permissions»

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:

```
/bim/bash
/bin/csh
/bin/ksh
/bin/tcsh
/bin/sh
/bin/zsh
```

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

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

6) Отредактировать файлы из `/etc/pam.d` 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
- 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 файловых системы /var.

При инсталляции системы следует выделить для файловых систем /, /usr, /usr/local, /var, /opt, /export разные разделы диска для предотвращения переполнения критичных файловых систем (/, /var) за счет, например, пользовательских данных и обеспечения возможности монтирования файловых систем /usr 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

Настройка сетевых сервисов заключается в следующем:

1) Следует ограничить функциональность сетевых соединений. Для этого отредактируйте описания всех неиспользуемых сетевых сервисов (по крайней мере telnet.plist, tftp.plist, finger.plist и другие, если имеются) из `/System/Library/LaunchDaemons/`, добавив строки изменив значение ключа Disabled на true:

```
<key>Disabled</key>
<true/>
```

2) 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
- bin
- daemon
- listen
- lp
- nobody
- noaccess
- nobody4
- nuucp
- smtp
- sys
- uucp

7) 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
```

8) 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/default/ftpd` следующей директивы:
`BANNER=""`

• Редактирование файлов `/etc/issue`, `/etc/ftpbanner` 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 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.

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 launchd (включая дату и время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), отредактируйте описания сетевых сервисов (telnet.plist, ftp.plist и другие, если имеются) из /System/Library/LaunchDaemons/, добавив строки:

```
<key>Debug</key>
<true/>
```

9 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 Mac OS.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 8.2.

Контролем целостности должны быть охвачены файлы:

Mac OS

```
/opt/cprocsp/bin//cryptcp
/opt/cprocsp/bin//certmgr
/opt/cprocsp/bin//inittst
/opt/cprocsp/bin//csptestf
/opt/cprocsp/bin//der2xer
/opt/cprocsp/lib//libcapi20.4.dylib
/opt/cprocsp/lib//libcpext.4.dylib
/opt/cprocsp/lib//libpkixcmp.4.dylib
/opt/cprocsp/lib//libasn1data.4.dylib
/opt/cprocsp/lib//libssp.4.dylib
/opt/cprocsp/lib//libenroll.4.dylib
/opt/cprocsp/lib//liburlretrieve.4.dylib
/opt/cprocsp/lib//libcpcdrv_emul.a
/opt/cprocsp/lib//libcsp.4.dylib
/opt/cprocsp/lib//librdrrndmbio_tui.4.dylib
/opt/cprocsp/lib//libcppkcs11.4.dylib
/opt/cprocsp/lib//librdremv.4.dylib
/opt/cprocsp/lib//librdresmarttoken.dylib
/opt/cprocsp/lib//librdresmarttokengost.dylib
/opt/cprocsp/lib//librdrrndmbio_gui.4.dylib
/opt/cprocsp/lib//libosxcpui.4.dylib
/opt/cprocsp/lib//librdrpcsc.4.dylib
/opt/cprocsp/lib//librdrric.4.dylib
/opt/cprocsp/sbin//ccid_reg.sh
/opt/cprocsp/bin//cpverify
/opt/cprocsp/bin//wipefile
/opt/cprocsp/bin//csptest
/opt/cprocsp/lib//librdrrdr.4.dylib
/opt/cprocsp/lib//librdrrndm.4.dylib
/opt/cprocsp/lib//librdrsup.4.dylib
/opt/cprocsp/lib//librdrdsrf.4.dylib
/opt/cprocsp/lib//librdrfat12.4.dylib
/opt/cprocsp/lib//libcapi10.4.dylib
/opt/cprocsp/lib//libcpui.4.dylib
/opt/cprocsp/sbin//unreg_prov_type_name.sh
/opt/cprocsp/sbin//cpconfig
/opt/cprocsp/sbin//mount_flash.sh
/opt/cprocsp/lib//librsaenh.4.dylib
```

```
/opt/cprocsp/lib//librdrrtsupcp.4.dylib
/opt/cprocsp/bin//ssflicense
/opt/cprocsp/lib//libcpsapssf.1.dylib
/opt/cprocsp/sbin//stunnel_fork
/opt/cprocsp/sbin//stunnel_hsm
/opt/cprocsp/sbin//stunnel_thread
```

Приложение А
Управление протоколированием

Для включения/отключения значение log используйте:
1) Mac OS

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
```

2) Mac OS уровня ядра

Не поддерживается.

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

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					