

127 018, Москва, Сушеvский вал, д.18  
Телефон: (495) 995 4820  
Факс: (495) 995 4820  
<http://www.CryptoPro.ru>  
E-mail: [info@CryptoPro.ru](mailto:info@CryptoPro.ru)



Средство Криптографической Защиты Информации	КриптоПро CSP Версия 3.6.1 Руководство администратора безопасности Использование СКЗИ под управлением ОС Mac OS X
---	--

ЖТЯИ.00050-03 90 02-06

Листов 21

**© ООО "КРИПТО-ПРО", 2000-2013. Все права защищены.**

Авторские права на средства криптографической защиты информации типа КриптоПро CSP и эксплуатационную документацию к ним зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент).

Настоящий Документ входит в комплект поставки программного обеспечения СКЗИ КриптоПро CSP версии 3.6.1; 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 .....	4
Список сокращений .....	4
<b>1. Основные технические данные и характеристики СКЗИ .....</b>	<b>5</b>
1.1. Программно-аппаратная среда .....	5
1.2. Варианты исполнения СКЗИ .....	5
1.3. Ключевые носители.....	5
<b>2. Установка дистрибутива ПО КриптоПро CSP .....</b>	<b>5</b>
<b>3. Обновление СКЗИ КриптоПро CSP .....</b>	<b>7</b>
<b>4. Настройка СКЗИ КриптоПро CSP .....</b>	<b>7</b>
4.1. Доступ к утилите для настройки СКЗИ КриптоПро CSP .....	7
4.2. Ввод серийного номера лицензии.....	7
4.3. Настройка оборудования СКЗИ КриптоПро CSP .....	7
4.4. Установка параметров журналирования .....	8
4.5. Настройка криптопровайдера по умолчанию.....	8
<b>5. Установка сопутствующих пакетов .....</b>	<b>8</b>
5.1. Библиотека libcurl.....	9
<b>6. Состав и назначение компонент программного обеспечения СКЗИ.....</b>	<b>9</b>
6.1. Базовые модули СКЗИ .....	9
6.1.1. Библиотека libcsp .....	9
6.1.2. Библиотека libcspr .....	9
6.1.3. Драйверная библиотека drvcspr .....	9
6.1.4. Модули сетевой аутентификации КриптоПро TLS .....	10
6.1.5. Модуль crverify .....	10
6.1.6. Модуль wipefile.....	10
6.2. Модули ПКЗИ.....	10
6.2.1. Модуль libcap20 .....	10
6.2.2. Библиотека libdrdr .....	10
6.2.3. Модули доступа к конкретным типам ключевых носителей и считывателей: ...	10
6.2.4. Библиотека libdrsup .....	10
6.2.5. Модули датчиков случайных чисел .....	10
6.2.6. Библиотека libasn1data поддержки протокола ASN1.....	10
<b>7. Встраивание СКЗИ КриптоПро CSP в прикладное ПО .....</b>	<b>10</b>
<b>8. Требования по организационно-техническим и административным мерам обеспечения эксплуатации СКЗИ 11</b>	
8.1. Общие меры защиты от НСД ПО с установленными СКЗИ на ОС Mac OS X .....	11
8.1.1. Организационно-технические меры .....	12
8.1.2. Дополнительные настройки ОС Mac OS X .....	14
8.2. Требования по размещению технических средств с установленным СКЗИ.....	17
<b>9. Требования по криптографической защите .....</b>	<b>18</b>
Приложение 1. Контроль целостности программного обеспечения.....	19
Приложение 2. Управление протоколированием .....	19
Лист регистрации изменений.....	21

## Аннотация

Настоящее Руководство дополняет документ "ЖТЯИ.00050-03 90 02. КристоПро CSP. Руководство администратора безопасности. Общая часть" при использовании СКЗИ под управлением ОС Mac OS X.

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

## 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 ключа проверки электронной подписи или открытого ключа и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата ключа проверки электронной подписи или открытого ключа абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СРС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник.
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

## 1. Основные технические данные и характеристики СКЗИ

СКЗИ ЖТЯИ.00050-03 разработано в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

### 1.1. Программно-аппаратная среда

СКЗИ ЖТЯИ.00050-03 под управлением ОС Mac OS X используется в программно-аппаратных средах ОС Mac OS X (x64).

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

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

### 1.2. Варианты исполнения СКЗИ

СКЗИ ЖТЯИ.00050-03 для работы с ОС Mac OS X изготавливается и распространяется в одном варианте исполнения:

Исполнение 1 – СКЗИ класса защиты КС1.

### 1.3. Ключевые носители

В качестве ключевых носителей закрытых ключей и ключей ЭП могут использоваться:

ГМД 3,5";

USB диски

Раздел HDD ПЭВМ



**Примечания.** 1. Допускается хранение закрытых ключей и ключей ЭП 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.00050-03 30 01, п.п. 3.8, 3.9.

## 2. Установка дистрибутива ПО КриптоПро CSP

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-3.6.1.dmg**

Установите пакет при помощи системной утилиты installer:

```
cd /Volumes/ru.cryptopro.csp-3.6.1  
installer -pkg ru.cryptopro.csp-3.6.1.mpkg -target "/"
```

Отмонтируйте диск:

```
hdiutil detach /Volumes/ru.cryptopro.csp-3.6.1
```

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/cproscsp`.

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.

Таблица назначения пакетов.

Имя пакета	Назначение пакета
Обязательные пакеты	
CPRObase	Базовый пакет.
CPROrdr	Основные приложения, считыватели и ДСЧ.
CPROcpl	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...).
CPROkc1	Провайдер KC1.
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 функциям криптопровайдера. Пакет не будет установлен по умолчанию.
CPROrdp	Модули поддержки PCSC-считывателей, смарт-карт (ПИК, Оскар, Магистра...). Пакет не будет установлен по умолчанию.
CPROdrv	Пакет для разработчика драйверов. Пакет не будет установлен по умолчанию.
CPROstnl	Универсальный SSL/TLS туннель. Пакет не будет установлен по умолчанию.
CPROCaDES	КриптоПро ЭЦП SDK (CADES).
CPROOCSPut	Библиотека и клиент OCSP.
CPROTSPutl	Библиотека и клиент TSP.
CPRONpcades	Плагин npcades для работы с ЭП через браузер.
CPROrdemv	Модуль поддержки EMV / Gemalto

Пакеты имеют архитектуру `universal binary` и содержат в себе 32-разрядную (i386) и 64-разрядную (x86\_64) подсистемы.

## 3. Обновление СКЗИ КриптоПро CSP

Для обновления КриптоПро CSP необходимо:

- запомнить текущую конфигурацию CSP:
  - набор установленных пакетов
  - настройки провайдера (для простоты можно сохранить /etc/opt/cproscsp/config[64].ini)
- удалить при помощи скрипта `uninstall_csp`, который поставляется вместе с КриптоПро CSP, 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

## 4. Настройка СКЗИ КриптоПро CSP

### 4.1. Доступ к утилите для настройки СКЗИ КриптоПро CSP

Настройка СКЗИ КриптоПро CSP осуществляется с помощью утилиты `srconfig`, которая входит в состав дистрибутива и расположена в директории `/opt/cproscsp/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 КриптоПро CSP

Утилита `srconfig` также предназначена для изменения набора устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел. Предусмотренными 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 дисковом устройстве 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`, кроме того он работает только с KC1 провайдером. Для добавления консольного БиоДСЧ:

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

Для добавления внешней гаммы:

```
# ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
# ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1
/var/opt/cproscsp/dsrf/db1/kis_1
# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1
/var/opt/cproscsp/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/cproscsp/dsrf/db1/kis_1
# cp /tmp/db2/kis_1 /var/opt/cproscsp/dsrf/db2/kis_1
```

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

```
# /opt/cproscsp/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 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:

```
srcsp - ядро криптопровайдера
capi10 - CryptoAPI 1.0
cpext
capi20 - CryptoAPI 2.0
capilite - CAPI Lite
libcspr
cryptsrv - служба хранения ключей (KC2)
libssp - TLS
cppkcs11 - PKCS11
cpdrv - драйвер
dmntcs
```

## 4.5. Настройка криптопровайдера по умолчанию

Для просмотра типов доступных криптопровайдеров:

```
$ ./cpconfig -defprov -view_type
```

Для просмотра свойств криптопровайдера нужного типа:

```
# ./cpconfig -defprov -view -provtype <provtype>
```

Для установки провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -setdef -provtype <provtype> -provname
<provname>
```

Для получения имени провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -getdef -provtype <provtype>
```

## 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 хеш. 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 <http://curl.haxx.se/>. 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/cproscsp/sbin/cpconfig -ini \config\apppath -add string  
libcurl.so /usr/local/lib/libcurl.so
```

## 6. Состав и назначение компонент программного обеспечения СКЗИ

### 6.1. Базовые модули СКЗИ

ПО СКЗИ содержит базовые модули:

- libcsp – динамически загружаемая библиотека КриптоПро CSP.
- libcspr – библиотека работы с удалённым КриптоПро CSP.
- drvscsp – динамически загружаемый модуль ядра.
- libssp – библиотека поддержки модуля сетевой аутентификации КриптоПро TLS
- crverify – 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.

#### 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 drvscsp

Библиотека **drvscsp**, 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 соответствующем разделе документа "ЖТЯИ.00050-03 90 02. 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 ПКЗИ

#### 6.2.1. Модуль libcap120

Модуль **libcap120** 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 libdrdrv

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

#### 6.2.3. Модули доступа к конкретным типам ключевых носителей и считывателей:

- **libdrfat12** к дисководу и дискете 3.5" и разделу жесткого диска
- **libdrpcsc** к считывателям смарт-карт и eToken, поддерживающим интерфейс PC/SC

#### 6.2.4. Библиотека libdrsup

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

#### 6.2.5. Модули датчиков случайных чисел

Библиотеки **libdr rndm** и **libdr rndmbio** обеспечивают поддержку работы с физическими датчиками случайных чисел.

#### 6.2.6. Библиотека libasn1data поддержки протокола ASN1

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

## 7. Встраивание СКЗИ КриптоПро CSP в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 8 документа "ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть."

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 организационно-техническим и административным мерам обеспечения эксплуатации СКЗИ

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме разделов 12 и 13 документа "ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть."

### 8.1. Общие меры защиты от НСД ПО с установленными СКЗИ на ОС Mac OS X

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.00050-03 под управлением ОС Mac OS X 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 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 электронного замка (см. соответствующий раздел в документе "ЖТЯИ.00050-03 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть."), что означает:
  - Выполнение загрузки с фиксированного носителя;
  - 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.

### 8.1.1. Организационно-технические меры

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.

#### 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.

#### 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 производиться комиссией с составлением акта об уничтожении.

4. В системе регистрируется один пользователь, обладающий правами администратора, носящий имя root, на которого возлагается обязанность конфигурировать ОС Mac OS X, настраивать безопасность, а также конфигурировать ПЭВМ, на которую установлена ОС Mac OS X.
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.
6. Пользователю root доступны настройки всех пользователей ОС Mac OS X, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в Mac OS, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь Mac OS, не являющийся пользователем root, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему пользователем root.
7. Всех пользователей ПЭВМ, которые не пользуются данной системой, и всех стандартных пользователей, которые создаются в Mac OS во время установки (таких, как "sys", "uicp", "nuicp", и "listen"), кроме пользователя root, следует удалить.

8. 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.
9. При использовании СКЗИ ЖТЯИ.00050-03 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.
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.00050-03
11. На технических средствах, оснащенных СКЗИ «КриптоПро CSP» должно использоваться только лицензионное программное обеспечение фирм-производителей.
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.
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 Mac OS X.
14. До загрузки ОС должен быть реализован контроль целостности файлов, критичных для загрузки ОС и программы CPVERIFY.
15. При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ ЖТЯИ.00050-03, самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ с использованием программы CPVERIFY.
16. Средствами BIOS должна быть исключена возможность работы на ЭВМ, если во время его начальной загрузки не проходят встроенные тесты ЭВМ (POST).
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.00050-03. Следует избегать попадания в систему программ, позволяющих при ошибках ОС получать привилегии root.
18. Должно быть ограничено (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время.
19. Должно быть реализовано физическое затирание содержимого удаляемых файлов с использованием программы Wipefile из состава СКЗИ.
20. Должны быть отключены сетевые протоколы, которые не используются на данной ЭВМ.
21. В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть отключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, в прикладных программах.
22. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические

- средства СКЗИ ЖТЯИ.00050-03, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.
23. Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ ЖТЯИ.00050-03 после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.
  24. 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 компьютера или ОС Mac OS X.
  25. После инсталляции ОС Mac OS X следует установить средствами операционной системы все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.
  26. На все директории, содержащие системные файлы ОС Mac OS X и каталоги СКЗИ, необходимо установить права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись.
  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`.
  28. В ОС Mac OS X 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 `wirefile`, входящей в состав СКЗИ ЖТЯИ.00050-03. 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.

### 8.1.2. Дополнительные настройки ОС Mac OS X

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).

#### 8.1.2.1 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](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:
  - a. Chapter 2 «Installing Mac OS X» - «Initial System Setup» - «Turning Off Auto-login»
  - b. Chapter 4 «Securing Global System Settings» - «Configuring Access Warnings» - «Enabling Access Warnings for the Login Window»
  - c. Chapter 6 «Securing Accounts» - «Setting Global Password Policies»
  - d. 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:

```
/bin/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	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.

#### 8.1.2.2 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".

#### 8.1.2.3 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
```

#### 8.1.2.4 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	nobody4
bin	nuucp
daemon	root
listen	smtp
lp	sys
nobody	uucp
noaccess	

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/uencode
```

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
```



#### 8.1.2.5 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.

#### 8.1.2.6 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.

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 launchd (включая дату/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/>

## 8.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

- Должны быть приняты меры по защите от несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.
- В случае планирования размещения СКЗИ в помещениях, где присутствует речевая, акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, технические средства иностранного производства, на которых функционируют программные модули СКЗИ, должны быть подвергнуты специальной проверке по выявлению устройств, предназначенных для негласного получения информации».

## 9. Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 16 документа ЖТЯИ.00050-03 90 02.

Конкретно должны выполняться требования:

1. Использование только лицензионного системного программного обеспечения.
2. Настройка операционной системы для работы с СКЗИ по п. 5
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. 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.
6. Периодичность тестового контроля криптографических функций - 10 минут.
7. Ежесуточная перезагрузка ПЭВМ.
8. Периодичность останова ПЭВМ с обязательной проверкой системы охлаждения процессорного блока ПЭВМ - 1 месяц.
9. **Запрещается** использовать режим простой замены (ЕСВ) ГОСТ 28147-89 для шифрования информации, кроме ключевой.
10. Должно даваться предупреждение о том, что при использовании режима шифрования CRYPT\_SIMPLEMIX\_MODE материал, обрабатываемый на одном ключе, автоматически ограничивается величиной 4 MB.
11. При функционировании СКЗИ должны выполняться требования эксплуатационной документации на ПАК защиты от НСД.
12. Должно быть запрещено использование СКЗИ для защиты телефонных переговоров без принятия в системе мер по защите от информативности побочных каналов, специфических при передаче речи.
13. Должна быть запрещена работа СКЗИ при включенных в ПЭВМ штатных средствах выхода в радиоканал.
14. Перед началом работы СКЗИ необходимо провести контроль целостности.
15. Контролем целостности должны быть охвачены файлы:

**Mac OS (universal binary i386, x6\_64)**

libcspkfc.3.dylib cryptcp certmgr inittst csptestf der2xer libcapi20.3.dylib libcpext.3.dylib libpkixcmp.3.dylib libasn1data.3.dylib libssp.3.dylib libpkivalidator.3.dylib libcplib.3.dylib libcpasn1.3.dylib libocsp.3.dylib libenroll.3.dylib curl libcpcurl.4.dylib libcpcurl.a libcsp.3.dylib

libdrndmbio\_tui.3.dylib libsaenh.3.dylib libcppkcs11.3.dylib fkchdimgtest libdrdrdfkc.3.dylib  
libdrfkchding.3.dylib libdrpcsc.3.dylib libdrdic.3.dylib cpverify wipefile csptest  
libdrdr.3.dylib libdrndm.3.dylib libdrsup.3.dylib libdrdsrf.3.dylib libdrfat12.3.dylib  
libcapi10.3.dylib libcpui.3.dylib cpconfig mount\_flash.sh libstunnel.dylib

## Приложение 1. Контроль целостности программного обеспечения

В дополнение к дистрибутиву поставляются скриптовые файлы integrity.sh, запуском которых можно убедиться в целостности дистрибутива до его установки.

Программное обеспечение СКЗИ КриптоПро CSP имеет средства обеспечения контроля целостности ПО СКЗИ, которые должны выполняются периодически.

Если в результате периодического контроля целостности появляется сообщения о нарушении целостности контролируемого файла, пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО СКЗИ КриптоПро CSP с дистрибутива, или системное ПО.

## Приложение 2. Управление протоколированием

Для включения/отключения значение log используйте:

### а) 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
```

### б) для 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

[illegible]