

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



Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Руководство администратора
безопасности.

Использование СКЗИ
под управлением ОС Mac OS

ЖТЯИ.00101-02 91 07
Листов 25

© ООО «КРИПТО-ПРО», 2000-2021. 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 R2 KC1; на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО «КРИПТО-ПРО» документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

Список сокращений	5
1 Основные технические данные и характеристики СКЗИ	6
1.1 Программно-аппаратные среды функционирования	6
1.2 Ключевые носители	6
2 Установка дистрибутива ПО СКЗИ	7
3 Обновление ПО СКЗИ	9
4 Настройка СКЗИ	10
4.1 Доступ к утилите для настройки СКЗИ	10
4.2 Ввод серийного номера лицензии	10
4.3 Настройка оборудования СКЗИ	10
4.4 Установка параметров журналирования	11
4.5 Настройка криптопровайдера по умолчанию	12
4.6 Включение режима усиленного контроля использования ключей	12
4.7 Настройка параметров алгоритмов	12
5 Состав и назначение компонент ПО СКЗИ	14
5.1 Базовые модули СКЗИ	14
5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)	15
5.2.1 Модуль libscapi20	15
5.2.2 Модули устройств хранения ключевой информации	15
5.2.3 Модули датчиков случайных чисел	16
6 Встраивание СКЗИ в прикладное ПО	17
7 Требования по защите от НСД	18
7.1 Организационно-технические меры защиты от НСД	18
7.2 Дополнительные настройки ОС Mac OS X	18
8 Требования по криптографической защите	22
Приложение А. Управление протоколированием	24

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КристоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционной системы Mac OS.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КристоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Mac OS, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
APM	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

1.1 Программно-аппаратные среды функционирования

СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Mac OS X используется в программно-аппаратных средах:

Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14/10.15/11 (x64, ARM64)

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

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



Примечание. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

2 Установка дистрибутива ПО СКЗИ

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора — под учётной записью root или с использованием команды sudo.

СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Mac OS X для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, используемые 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/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 (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	
CPRORbase	Базовый пакет КриптоПро CSP, устанавливается первым
CPRORdr	Модуль поддержки основных приложений, считывателей и ДСЧ
CPRORkc1	Провайдер класса KC1
CPRORcpl	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...)
Дополнительные пакеты	
CPRORdp	Модули поддержки PCSC-считывателей, смарт-карт
CPRORp11	Модуль поддержки PKCS11
CPRORcspd	Пакет для разработчика приложений, использующих КриптоПро CSP
CPRORdrv	Драйверная библиотека
CPRORdrvд	Пакет для разработчика драйверов
CPRORcurl	Библиотека libcurl с поддержкой российских криптоалгоритмов
CPRORcptools	Графическое приложение для доступа к основным функциям и настройкам КриптоПро CSP
CPRORdcloud	Модуль взаимодействия с КриптоПро DSS — КриптоПро Cloud CSP
CPRORstnl	Универсальный SSL/TLS туннель
CPRORcacerts	Корневые сертификаты доверенных ЦС
Поддержка ключевых носителей	
CPRORdedoc	Модуль поддержки платформы eDoc (УЛГ)
CPRORdemv	Модуль поддержки смарт-карт Gemalto (EMV)
CPRORdesmart	Модуль поддержки смарт-карт и токенов ESMART
CPRORdrinfocrypt	Модуль поддержки токенов InfoCrypt
CPRORdinpaspot	Модуль поддержки смарт-карт Alioth
CPRORdjacarta	Модуль поддержки смарт-карт и токенов JaCarta
CPRORdkst	Модуль поддержки смарт-карт MorphoKST
CPRORdmskey	Модуль поддержки токенов Multisoft MS_Key
CPRORdnovacard	Модуль поддержки смарт-карт Novacard
CPRORdrosan	Модуль поддержки смарт-карт Rosan
CPRORdrutoken	Модуль поддержки смарт-карт и токенов Рутокен

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Mac OS необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
 - набор установленных пакетов;
 - настройки провайдера (для простоты можно сохранить `/etc/opt/cprosp/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 `crconfig`, 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:

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

Для ввода лицензии выполните:

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

Серийный номер следует вводить с соблюдением регистра символов.

4.3 Настройка оборудования СКЗИ

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

Для просмотра списка настроенных считывателей:

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

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

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

Для просмотра списка настроенных ДСЧ:

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

Для консольного БиоДСЧ требуется пакет `CPR0kc1`. Для добавления консольного БиоДСЧ:

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

Для графического БиоДСЧ требуется пакет `CPR0rdg` 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/cproscsp/dsrf/db1/kis_1
```

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

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

```
# cp /tmp/db1/kis_1 /var/opt/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 позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал. Существует возможность изменения настроек журналирования различных модулей СКЗИ. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений.

Для получения справки по настройкам журналирования:

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

Подробнее опции управления протоколированием модулями СКЗИ см. в [Приложении А](#).

4.5 Настройка криптопровайдера по умолчанию

Для просмотра типов доступных криптопровайдеров:

```
# ./cpconfig -defprov -view_type
```

Для просмотра свойств криптопровайдера нужного типа:

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

Для установки провайдера по умолчанию для нужного типа:

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

Для получения имени провайдера по умолчанию для нужного типа:

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

4.6 Включение режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. После успешной инсталляции необходимо включить данный режим, выполнив команду:

```
#./cpconfig -ini '\config\parameters' -add long StrengthenedKeyUsageControl 1
```

Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей или запустить утилиту csptest, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел:

```
# ./csptest -keyset -verifycontext -hard_rng
```



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

4.7 Настройка параметров алгоритмов

Для установки параметров алгоритмов (для провайдеров типа 75):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

Для установки параметров алгоритмов (для провайдеров типа 80):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

Для установки параметров алгоритмов (для провайдеров типа 81):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

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

5 Состав и назначение компонент ПО СКЗИ

5.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

libcsp	динамически загружаемая библиотека КриптоПро CSP; реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
libcspr	обеспечивает удаленный доступ к криптопровайдеру, функционирующему как отдельный сервис
drvcspr	динамически загружаемый модуль ядра; реализует целевые функции криптографической защиты информации (кроме формирования ЭП) и работу с ключами
libssp	обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS (общее описание протокола приведено в документе ЖТЯИ.00101-02 90 01. Описание реализации)
cpverify	модуль контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на ПЭВМ пользователя
wipefile	модуль удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях
cryptcp	приложение командной строки для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов (подробное описание см. в ЖТЯИ.00101-02 93 01. Приложение командной строки для подписи и шифрования файлов)
certmgr	приложение командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами (подробное описание см. в ЖТЯИ.00101-02 93 02. Приложение командной строки для работы с сертификатами)
stunnel	приложение для создания TLS-туннеля, предназначенного для создания TLS защищенного соединения между клиентом и локальным (inetd-запускаемым) или удаленным сервером (подробное описание см. в ЖТЯИ.00101-02 93 03. Приложение для создания TLS-туннеля)
cptools	графическое приложение, предоставляющее доступ к основным функциям и настройкам КриптоПро CSP (подробное описание см. в ЖТЯИ.00101-02 92 06. Инструкция по использованию. Инструменты КриптоПро)

В названиях дистрибутивов СКЗИ используются следующие обозначения:

- CPRO — префикс;
- csp — криптопровайдер;

- `drv` — загружаемый модуль ядра ОС;
- `[d]` (опционально) — указывает на документацию (тестовые примеры);
- `i386` — платформа Intel.

5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

5.2.1 Модуль `libcapi20`

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

5.2.2 Модули устройств хранения ключевой информации

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

Следующие модули обеспечивают реализацию доступа к конкретным типам ключевых носителей:

<code>libdrcloud</code>	облачный токен
<code>libdrcryptoki</code>	доступ к ключам ФКН через интерфейс PKCS#11
<code>libdredoc</code>	платформа eDoc (УЛГ)
<code>libdremv</code>	смарт-карты Gemalto (EMV)
<code>libdresmarttoken</code>	смарт-карты и токены ESMART Token
<code>libdresmarttokengost</code>	смарт-карты и токены ESMART Token ГОСТ
<code>libdrfat12</code>	съёмные диски и раздел HDD/SDD
<code>libdrinfocrypt</code>	токены InfoCrypt
<code>libdrinpaspot</code>	смарт-карты Alioth
<code>libdrjacarta</code>	токены и смарт-карты JaCarta
<code>libdrkst</code>	смарт-карты MorphoKST
<code>libdrmskey</code>	токены Multisoft MS_Key
<code>libdrnova</code>	смарт-карты Novacard
<code>libdrpcsc</code>	базовый считыватель носителей, поддерживающих интерфейс PC/SC
<code>libdroric</code>	смарт-карты Оскар и Форос (Магистра)
<code>libdrrosan</code>	смарт-карта Rosan
<code>libdrtrutoken</code>	смарт-карты и токены Рутокен

5.2.3 Модули датчиков случайных чисел

Библиотеки `libdrand48` и `libdrand48mbio` обеспечивают поддержку работы с физическим ДСЧ программно-аппаратного комплекса защиты от НСД и БиоДСЧ соответственно.

6 Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 4 документа ЖТЯИ.00101-02 95 01. КриптоПро CSP. Правила пользования и документа ЖТЯИ.00101-02 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()`).

7 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 ЖТЯИ.00101-02 95 01. Правила пользования.

При использовании СКЗИ под управлением ОС 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).

7.1 Организационно-технические меры защиты от НСД

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

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

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

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

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

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

6) По окончании работы СКЗИ содержимое виртуальной памяти ОС должно затираться с использованием средств ОС. В случае аварийного останова ПЭВМ, при следующей загрузке необходимо в режиме «single user» очистить область виртуальной памяти программой wipefile, входящей в состав СКЗИ. В случае выхода из строя диска, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а диск считается не подлежащим ремонту и уничтожается по правилам уничтожения ключевых носителей.

7.2 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). Желательно скопировать изменяемые файлы (каталоги) с сохранением структуры каталогов.

Ограничение доступа пользователей и настройки пользовательского окружения

1) Рекомендуется настроить операционную систему в соответствии с руководством https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/331856/End_User_Devices_Security_Guidance_-_Apple_OS_X_10.9.pdf (если Вы используете более новую версию ОС, используйте аналогичное руководство для Вашей версии ОС). Для ограничения доступа в систему выполните следующие пункты руководства:

- отключите функцию автоматического входа в систему (Automatic login);
- создайте предупреждение о доступе к окну входа в систему (access warnings for the login window);
- задайте маску по умолчанию для создания файлов 022.

2) Для пользователя root установить маску режима создания файлов umask=077 или umask=027;

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

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

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

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

7) Проверить идентификаторы пользователя и группы для всех пользователей, перечисленных в файле /etc/passwd. Следует убедиться, что не существует пользователей, имеющих идентификатор пользователя 0 и идентификатор группы 0 кроме, возможно, пользователя root.

Ограничения при монтировании файловых систем

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

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/, изменив значение ключа Disabled на true:

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

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

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

4) Запустить процедуру регистрации запуска процессов (accounting).

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

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

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

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 444 /etc/default/login
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
chmod 400 /usr/bin/uencode
```

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

```
chmod g-s /usr/bin/mail
chmod g-s /usr/bin/mailx
chmod g-s /usr/bin/write
chmod g-s /usr/bin/netstat
chmod g-s /usr/bin/nfsstat
chmod g-s /usr/bin/ipcs
chmod g-s /usr/sbin/arp
chmod g-s /usr/sbin/dmesg
chmod g-s /usr/sbin/prtconf
chmod g-s /usr/sbin/swap
chmod g-s /usr/sbin/sysdef
chmod g-s /usr/sbin/wall
```

Ограничение количества «видимой извне» информации о системе

Обычно, начальную информацию о системе потенциальный нарушитель получает из системных приглашений, выдаваемых сетевыми службами сервера (telnet-сервер, ftp-сервер и пр.).

Для ограничения количества «видимой извне» информации рекомендуется:

- отказаться от стандартного "заголовка выводимого сервером ftp при ответе пользователю.

Достигается указанием в файле /etc/default/ftpd следующей директивы:

```
BANNER=""
```

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

Настройка подсистемы протоколирования и аудита

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

- `/var/log/authlog`
- `/var/log/syslog`
- `/var/log/messages`
- `/var/log/sulog`
- `/var/log/utmp`
- `/var/log/utmpx`

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

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

4) Следует протолировать попытки использования программ `su` и `sudo`, например, с помощью добавления в файл `/etc/syslog.conf` строк:

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

или

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

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

5) Следует обеспечить протоколирование неуспешных попыток регистрации в системе в локальном протокол, например, путем выполнения команд:

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

6) Следует обеспечить протоколирование сетевых соединений, контролируемых демоном `launchd` (включая дату и время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), например, путем редактирования описания сетевых сервисов (`telnet.plist`, `ftp.plist` и другие, если имеются) из `/System/Library/LaunchDaemons/`, добавив строки:

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

8 Требования по криптографической защите

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

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

Контролем целостности должны быть охвачены файлы:

Mac OS

```
/opt/cprocsp/bin//cryptcp
/opt/cprocsp/bin//certmgr
/opt/cprocsp/bin//initst
/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//libpcdrv_emul.a
/opt/cprocsp/lib//libcsp.4.dylib
/opt/cprocsp/lib//libdrndmbio_tui.4.dylib
/opt/cprocsp/lib//libcpkcs11.4.dylib
/opt/cprocsp/lib//libdrmv.4.dylib
/opt/cprocsp/lib//libdresmarttoken.dylib
/opt/cprocsp/lib//libdresmarttokengost.dylib
/opt/cprocsp/lib//libdrndmbio_gui.4.dylib
/opt/cprocsp/lib//libosxcui.4.dylib
/opt/cprocsp/lib//libdrpcsc.4.dylib
/opt/cprocsp/lib//libdrdic.4.dylib
/opt/cprocsp/sbin//ccid_reg.sh
/opt/cprocsp/bin//cpverify
/opt/cprocsp/bin//wipefile
/opt/cprocsp/bin//csptest
/opt/cprocsp/lib//libdrdr.4.dylib
/opt/cprocsp/lib//libdrndm.4.dylib
/opt/cprocsp/lib//libdrsup.4.dylib
/opt/cprocsp/lib//libdrdsrf.4.dylib
/opt/cprocsp/lib//libdrfat12.4.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//libdrtsupcp.4.dylib
```

```
/opt/cprobsp/bin//ssflicense  
/opt/cprobsp/lib//libcpsapssf.1.dylib  
/opt/cprobsp/sbin//stunnel_fork  
/opt/cprobsp/sbin//stunnel_hsm  
/opt/cprobsp/sbin//stunnel_thread
```

Приложение А

Управление протоколированием

Для определения **уровня протокола** (levelmask, см. [табл. 4](#)):

```
/usr/CPR0csp/sbin/cpconfig -loglevel <name> -mask <levelmask>
```

Для задания **формата протокола** (formatmask, см. [табл. 5](#)):

```
/usr/CPR0csp/sbin/cpconfig -loglevel <name> -format <formatmask>
```

Для просмотра текущих значений уровня и формата протокола:

```
/usr/CPR0csp/sbin/cpconfig -loglevel <name> -view
```

Таблица 4. Уровни протоколирования

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

Таблица 5. Форматы протокола

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

Лист регистрации изменений

[illegible]