

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 Solaris

ЖТЯИ.00101-02 91 05
Листов 30

© 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	15
5.2.4 Библиотека libasn1data поддержки протокола ASN1	15
6 Требования по защите от НСД	16
6.1 Организационно-технические меры защиты от НСД	16
6.2 Дополнительные настройки ОС Solaris	16
7 Требования по криптографической защите	22
Приложение А. Управление протоколированием	28

Аннотация

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

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

Список определений и сокращений

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

1 Основные технические данные и характеристики СКЗИ

1.1 Программно-аппаратные среды функционирования

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

Solaris 10 (SPARC, x86, x64)
Solaris 11 (SPARC, x64)

При необходимости использования СКЗИ уровня ядра ОС архитектуры IA32 для ОС Solaris 10 следует обновить систему до исправления 142901-03 и установить исправление IDR144030.

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

<http://www.oracle.com/technetwork/server-storage/solaris/overview/releases-jsp-140987.html>

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-02 30 01. КриптоПро CSP. Формуляр, п. 3.10.

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



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

2 Установка дистрибутива ПО СКЗИ

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

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

В ОС Solaris для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — распакованный архив дистрибутива (фактически это папка), содержащий файлы устанавливаемого приложения и файлы, используемые инсталлятором для конфигурирования среды. Архив имеет расширение .tar.gz и является обычным архивом gzip.

Перед установкой архивы дистрибутива необходимо распаковать:

```
for i in *.tar.gz; do gzip -cd $i | tar -xf -; done
```



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

Для удаления СКЗИ используйте скрипт uninstall.sh.

Для установки пакета используется команда:

```
pkgadd -d <папка_с_пакетами> <имя_пакета>
```

Например: pkgadd -d . CPR0base

Для удаления пакета используется команда:

```
pkgrm <имя_пакета>
```

Например: pkgrm CPR0base

Файлы из пакетов устанавливаются в /opt/cproscsp.

Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей, а удаляться в обратном порядке. Условно можно считать правильным порядком тот, который описан в таблице зависимостей и назначения пакетов (см. [табл. 1](#)).

Пакеты могут быть для 32-битной архитектуры, а также для 64-битной архитектуры (имя пакета заканчивается на x), тогда они устанавливаются на ОС, собранную под соответствующую архитектуру. Часто 64-битные ОС одновременно поддерживают и 32-битные приложения, и 64-битные, тогда при необходимости можно установить оба комплекта. Исключением являются драйверы — они устанавливаются в точном соответствии с архитектурой ядра ОС.

Таблица 1. Зависимости и назначения пакетов (для простоты описаны 32-битные пакеты)

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
CPRObase		Базовый пакет КриптоПро CSP, устанавливается первым; не зависит от архитектуры, поэтому для 64-битного комплекта этот пакет устанавливается из 32-битного комплекта
CPROrdrr	CPRObase	Модуль поддержки основных приложений, считывателей и ДСЧ
CPROkc1	CPROrdrr	Провайдер класса KC1
CPROkc2	CPROrdrr	Провайдер класса KC2, устанавливается только там, где в этом есть необходимость; в этом случае CPROkc1 обычно не ставится
CPROcpl	CPROrdrr, CPROkc1 или CPROkc2	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...)
Дополнительные пакеты		
CPROrdg	CPROrdrr, SUNWmfrun, SUNWxwrtl	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги
CPROrdrrp	CPROrdrr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт
CPROp11	CPROrdrr	Модуль поддержки PKCS11
CPROcspd	CPRObase	Пакет для разработчика приложений, использующих КриптоПро CSP
CPROrdrrv	CPRObase	Драйверная библиотека
CPROrdrrvd	CPROcspd	Пакет для разработчика драйверов
CPROcurl	CPROcpl	Библиотека libcurl с поддержкой российских криптоалгоритмов
CPROstnl	CPROcpl	Универсальный SSL/TLS туннель
CPROcacerts	CPROcpl	Корневые сертификаты доверенных ЦС
CPROrdrrnova	CPROrdrrp	Модуль поддержки смарт-карт Novacard

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Solaris необходимо:

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

4 Настройка СКЗИ

4.1 Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты `crconfig`, которая входит в состав дистрибутива и расположена в директории `/opt/cproscsp/sbin/<название_архитектуры>`. Если установлены пакеты СКЗИ для двух архитектур, например, `ia32` и `x64`, то действия по настройке нужно проводить дважды — для каждой архитектуры с помощью `crconfig` из соответствующей папки.

4.2 Ввод серийного номера лицензии

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

Для просмотра информации о лицензии выполните:

```
# 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 `CPROk1`. Для добавления консольного БиоДСЧ:

```
# ./crconfig -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/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 "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/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/ia32/csptest -card -enum  
Gemplus GemPC Twin 00 00  
Total:  
[ErrorCode: 0x00000000]
```

Для добавления считывателя используйте это имя:

```
# ./cpconfig -hardware reader -add "Gemplus GemPC Twin 00 00"
```

Для получения подробной справки по cpconfig:

```
# ./cpconfig -help
```

```
# ./cpconfig -hardware -help
```

4.4 Установка параметров журналирования

СКЗИ позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал. Существует возможность изменения настроек журналирования различных модулей СКЗИ. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений.

Для получения справки по настройкам журналирования:

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

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

4.5 Настройка криптопровайдера по умолчанию

Для просмотра типов доступных криптопровайдеров:

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

Для просмотра свойств криптопровайдера нужного типа:

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

Для установки провайдера по умолчанию для нужного типа:

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

Для получения имени провайдера по умолчанию для нужного типа:

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

4.6 Включение режима усиленного контроля использования ключей

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

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

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

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



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

4.7 Настройка параметров алгоритмов

Для установки параметров алгоритмов (для провайдеров типа 75):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

Для установки параметров алгоритмов (для провайдеров типа 80):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

Для установки параметров алгоритмов (для провайдеров типа 81):

параметры алгоритма шифрования:

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

параметры алгоритма подписи:

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

параметры алгоритма Диффи-Хеллмана:

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

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

5 Состав и назначение компонент ПО СКЗИ

5.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

libcsp	динамически загружаемая библиотека КриптоПро CSP; реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
libcspr	обеспечивает удаленный доступ к криптопровайдеру, функционирующему как отдельный сервис
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)

В названиях дистрибутивов СКЗИ используются следующие обозначения:

- CPRO — префикс;
- csp — криптопровайдер;
- drv — загружаемый модуль ядра ОС;
- [d] (опционально) — указывает на документацию (тестовые примеры);
- [x] (опционально) — указывает на 64-битовую версию ОС, SPARC;
- i386 — платформа Intel;

- sparc – платформа SPARC.

5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

5.2.1 Модуль libcap120

Модуль libcap120 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 ключевой информации.

Следующие модули обеспечивают реализацию доступа к конкретным типам ключевых носителей:

libdrfat12.so	съемные диски и раздел HDD/SDD
libdrpcsc.so	базовый считыватель носителей, поддерживающих интерфейс PC/SC

5.2.3 Модули датчиков случайных чисел

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

5.2.4 Библиотека libasn1data поддержки протокола ASN1

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

6 Требования по защите от НСД

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

При использовании СКЗИ под управлением ОС Solaris необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом должна решаться задача как обеспечения дополнительной защиты сервера и ОС от НСД, так и обеспечения бесперебойного режима работы и исключения «отказа в обслуживании», вызванного внутренними причинами (например, переполнением файловых систем).

6.1 Организационно-технические меры защиты от НСД

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

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

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

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

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

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

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

6.2 Дополнительные настройки ОС Solaris

Настройки ОС Solaris 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) При использовании в качестве сервера компьютера SUN SPARC, следует установить пароль для доступа к консоли, выполнив следующее:

- При загрузке системы в режиме диалога с интерпретатором команд загрузчика ввести следующие команды:

```
<ok> password  
<ok> setenv security-mode command
```

- После загрузки системы, с консоли после регистрации от имени суперпользователя ввести следующие команды:

```
# eeprom security-mode=command  
# eeprom security-password=
```

и ввести пароль на доступ к консоли.

Внимание! В случае если суперпользователь забудет пароль, возникнет необходимость замены ППЗУ первичного загрузчика в сервисном центре SUN.

2) В файле /etc/default/login следует установить следующие директивы:

- PASSREQ=YES (требует использования паролей)
- SUPATH=/usr/sbin:/usr/bin (задает значение переменной PATH после выполнения команды su);
- RETRIES=10 (задает число повторных попыток регистрации пользователя программой login);
- SYSLOG_FAILED_LOGINS=0 (директива предписывает протолировать все попытки неудачной регистрации пользователя);
- UMASK=022 (параметр задает маску создания файла по-умолчанию);
- CONSOLE=/dev/console (параметр ограничивает возможность регистрации суперпользователя только системной консолью и запрещает удаленные регистрации суперпользователя).

3) Установить минимальную длину пароля в 8 символов в файле /etc/default/passwd директивой PASSLENGTH=8 и максимальное «время жизни» пароля в неделях параметром MAXWEEKS=24.

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

5) Для отключения возможности доступа пользователя root к рабочей станции по сети необходимо раскомментировать строку "CONSOLE" в файле /etc/default/login;

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

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

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

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

10) Отключить службу RPC удаленного вызова процедур, для чего следует удалить файл /etc/rc2.d/s71rpc.

11) 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 и /opt.
- Для предотвращения переполнения файловой системы /tmp ограничить её размер опцией size. При этом значение опции size должно быть меньше размера области подкачки (swap).

• Для предотвращения переполнения критичных файловых систем и обеспечения возможности монтирования /usr и /opt в режиме «только для чтения» рекомендуется при инсталляции ОС выделить для файловых систем /, /usr, /usr/local, /var, /opt, /export разные разделы диска.

Ограничения на запуск процессов

Следует ограничить число системных сервисов и программ, инициализируемых в процессе загрузки ОС. Для этого:

- Из каталога `/etc/rcS.d` удалить все файлы, кроме:

<code>S30rootusr.sh</code>	<code>S50drvconfig</code>
<code>S40standardmounts.sh</code>	<code>S70buildmmttbs</code>
<code>S50drvconfig</code>	

- Из каталога `/etc/rc2.d` удалить все файлы, кроме:

<code>S02MOUNTFSYS</code>	<code>S20syssetup</code>
<code>S05RMTMPFILES</code>	<code>S25cspcheck</code>
<code>S69inet</code>	<code>S75cron</code>
<code>S72inetsvc</code>	<code>S88utmpd</code>
<code>S74syslog</code>	

- Из каталога `/etc/init.d` удалить все файлы, кроме:

<code>MOUNTFSYS</code>	<code>buildmmttab</code>
<code>RMTMPFILES</code>	<code>rootusr</code>
<code>inetsvc</code>	<code>syssetup</code>
<code>standardmounts</code>	<code>syslog</code>
<code>dev</code>	<code>inetinit</code>
<code>inks</code>	<code>utmpd</code>
<code>cron</code>	<code>dtlogin</code>
<code>drvconfig</code>	

- Удалить все файлы из каталога `/etc/rc3d`.
- Удалить все файлы из каталогов `/etc/rc0.d` и `/etc/rc1.d`, кроме тех, которые перечислены выше.

Настройка сетевых сервисов

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

- `echo`
- `discard`
- `daytime`
- `chargen`
- `finger`
- `systat`
- `netstat`
- `tftp`
- `telnet`

Возможно также сначала закомментировать в файле `/etc/inetd.conf` описания всех сервисов и затем раскомментировать только используемые.

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

3) Следует запретить прием из внешней сети "широковещательных" (broadcast) пакетов, а также передачу ответов на принятые "широковещательные" пакеты, например, добавив в конец файла `/etc/rc2.d/S69inet` следующие команды:

```
ndd -set /dev/ip ip_forward_directed_broadcasts 0
```

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

4) Следует запретить использование сетевой файловой системы NFS, удалив файлы:

```
/etc/dfs/dfstab
```

```
/etc/rc3.d/S15nfs.server
```

```
/etc/rc2.d/S73nfs.client
```

5) Запустить утилиту контроля системных ресурсов и средств системного аудита ASET с высоким уровнем безопасности: `/usr/aset/aset -l high` для проверки установок системных файлов и проанализировать файл отчета, который будет создан в `/usr/aset/reports`.

6) 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

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

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 444 /etc/default/login
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
chmod 400 /usr/bin/uuencode
chmod u-s /usr/lib/fs/ufs/ufsdump
chmod u-s /usr/lib/fs/ufs/ufsrestore
```

8) 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
chmod g-s /usr/openwin/bin/ff.core
chmod g-s /usr/openwin/bin/mailtool
chmod g-s /usr/openwin/bin/wsinfo
chmod g-s /usr/openwin/bin/xload
chmod g-s /usr/lib/fs/ufs/ufsdump
chmod g-s /usr/lib/fs/ufs/ufsrestore
```

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=""
```

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

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

```
BANNER=""
```

- отредактировать файлы /etc/issue, /etc/ftp-banner 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/adm/messages
- /var/adm/sulog
- /var/adm/utmp
- /var/adm/utmpx

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

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

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

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

или

```
auth.notice          ifdef (`LOGHOST', /var/log/authlog, @loghost)
```

Вторая строка аналогична первой, но указывает, что протокол дополнительно передается на сервер сбора протоколов. При редактировании файла `/etc/syslog.conf` в качестве разделителя полей в строке следует использовать символ табуляции.

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 sys /var/adm/loginlog
chmod 644 /var/adm/loginlog
```

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

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

и заменив в файле `/etc/rc2.d/S72inetsvc` строку

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

на

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

7 Требования по криптографической защите

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

Необходимо выполнить настройку операционной системы для работы с СКЗИ по [разд. 6.2](#).

Контролем целостности должны быть охвачены файлы:

Sparc Solaris (32-bits)

```
/opt/cprocsp/bin/sparc/cryptcp
/opt/cprocsp/bin/sparc/certmgr
/opt/cprocsp/bin/sparc/innittst
/opt/cprocsp/bin/sparc/cspstestf
/opt/cprocsp/bin/sparc/der2xer
/opt/cprocsp/lib/sparc/libcapi20.so.4.0.5
/opt/cprocsp/lib/sparc/libcpeext.so.4.0.5
/opt/cprocsp/lib/sparc/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/sparc/libasn1data.so.4.0.5
/opt/cprocsp/lib/sparc/libssp.so.4.0.5
/opt/cprocsp/lib/sparc/libenroll.so.4.0.5
/opt/cprocsp/lib/sparc/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/sparc/curl
/opt/cprocsp/lib/sparc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparc/libcpcurl.a
/opt/cprocsp/lib/sparc/libcsp.so.4.0.5
/opt/cprocsp/lib/sparc/libdrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/sparc/libdrndmbio_gui.so.4.0.5
/opt/cprocsp/lib/sparc/libxcui.so.4.0.5
/opt/cprocsp/lib/sparc/libdrpcsc.so.4.0.5
/opt/cprocsp/lib/sparc/libdrpic.so.4.0.5
/opt/cprocsp/sbin/sparc/ccid_reg.sh
/opt/cprocsp/bin/sparc/cpverify
/opt/cprocsp/bin/sparc/wipefile
/opt/cprocsp/bin/sparc/cspstest
/opt/cprocsp/lib/sparc/libdrdrdr.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrndm.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrsup.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrsf.so.4.0.5
/opt/cprocsp/lib/sparc/libdrfat12.so.4.0.5
/opt/cprocsp/lib/sparc/libcapi10.so.4.0.5
/opt/cprocsp/lib/sparc/libcpui.so.4.0.5
/opt/cprocsp/sbin/sparc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparc/cpconfig
/opt/cprocsp/sbin/sparc/mount_flash.sh
/opt/cprocsp/lib/sparc/libdruec.so.4.0.5
/opt/cprocsp/lib/sparc/librsaenh.so.4.0.5
/opt/cprocsp/sbin/sparc/stunnel_thread
/opt/cprocsp/sbin/sparc/stunnel_fork
```

/opt/cprocsp/sbin/sparc/stunnel_hsm

Sparc Solaris (64-bits)

/opt/cprocsp/bin/sparc/cryptcp
/opt/cprocsp/bin/sparc/certmgr
/opt/cprocsp/bin/sparc/inittst
/opt/cprocsp/bin/sparc/csptestf
/opt/cprocsp/bin/sparc/der2xer
/opt/cprocsp/lib/sparc/libcapi20.so.4.0.5
/opt/cprocsp/lib/sparc/libcpept.so.4.0.5
/opt/cprocsp/lib/sparc/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/sparc/libasn1data.so.4.0.5
/opt/cprocsp/lib/sparc/libssp.so.4.0.5
/opt/cprocsp/lib/sparc/libenroll.so.4.0.5
/opt/cprocsp/lib/sparc/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/sparcv9/cryptcp
/opt/cprocsp/bin/sparcv9/certmgr
/opt/cprocsp/bin/sparcv9/inittst
/opt/cprocsp/bin/sparcv9/csptestf
/opt/cprocsp/bin/sparcv9/der2xer
/opt/cprocsp/lib/sparcv9/libcapi20.so.4.0.5
/opt/cprocsp/lib/sparcv9/libcpept.so.4.0.5
/opt/cprocsp/lib/sparcv9/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/sparcv9/libasn1data.so.4.0.5
/opt/cprocsp/lib/sparcv9/libssp.so.4.0.5
/opt/cprocsp/lib/sparcv9/libenroll.so.4.0.5
/opt/cprocsp/lib/sparcv9/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/sparc/curl
/opt/cprocsp/lib/sparc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparc/libcpcurl.a
/opt/cprocsp/bin/sparcv9/curl
/opt/cprocsp/lib/sparcv9/libcpcurl.so.4.2.0
/opt/cprocsp/lib/sparcv9/libcpcurl.a
/opt/cprocsp/lib/sparc/libcpcdrv_emul.a
/opt/cprocsp/lib/sparc/libcsp.so.4.0.5
/opt/cprocsp/lib/sparc/libdrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/sparcv9/libcsp.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/sparc/libdrndmbio_gui.so.4.0.5
/opt/cprocsp/lib/sparc/libxcui.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrndmbio_gui.so.4.0.5
/opt/cprocsp/lib/sparcv9/libxcui.so.4.0.5
/opt/cprocsp/lib/sparc/libdrpcsc.so.4.0.5
/opt/cprocsp/lib/sparc/libdrrric.so.4.0.5
/opt/cprocsp/sbin/sparc/ccid_reg.sh
/opt/cprocsp/lib/sparcv9/libdrpcsc.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrrric.so.4.0.5
/opt/cprocsp/sbin/sparcv9/ccid_reg.sh
/opt/cprocsp/bin/sparc/cpverify

```
/opt/cprocsp/bin/sparc/wipefile
/opt/cprocsp/bin/sparc/csptest
/opt/cprocsp/lib/sparc/libdrdrdr.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrndm.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrsup.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrsrfr.so.4.0.5
/opt/cprocsp/lib/sparc/libdrdrfat12.so.4.0.5
/opt/cprocsp/lib/sparc/libcapi10.so.4.0.5
/opt/cprocsp/lib/sparc/libcpui.so.4.0.5
/opt/cprocsp/sbin/sparc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparc/cpconfig
/opt/cprocsp/sbin/sparc/mount_flash.sh
/opt/cprocsp/bin/sparcv9/cpverify
/opt/cprocsp/bin/sparcv9/wipefile
/opt/cprocsp/bin/sparcv9/csptest
/opt/cprocsp/lib/sparcv9/libdrdrdr.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrdrndm.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrdrsup.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrdrsrfr.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdrdrfat12.so.4.0.5
/opt/cprocsp/lib/sparcv9/libcapi10.so.4.0.5
/opt/cprocsp/lib/sparcv9/libcpui.so.4.0.5
/opt/cprocsp/sbin/sparcv9/unreg_prov_type_name.sh
/opt/cprocsp/sbin/sparcv9/cpconfig
/opt/cprocsp/sbin/sparcv9/mount_flash.sh
/opt/cprocsp/lib/sparc/libdruec.so.4.0.5
/opt/cprocsp/lib/sparcv9/libdruec.so.4.0.5
/opt/cprocsp/lib/sparc/librsaenh.so.4.0.5
/opt/cprocsp/lib/sparcv9/librsaenh.so.4.0.5
/opt/cprocsp/sbin/sparc/stunnel_thread
/opt/cprocsp/sbin/sparc/stunnel_fork
/opt/cprocsp/sbin/sparc/stunnel_hsm
/opt/cprocsp/sbin/sparcv9/stunnel_thread
/opt/cprocsp/sbin/sparcv9/stunnel_fork
/opt/cprocsp/sbin/sparcv9/stunnel_hsm
```

Intel Solaris (32-bits)

```
/opt/cprocsp/bin/ia32/cryptcp
/opt/cprocsp/bin/ia32/certmgr
/opt/cprocsp/bin/ia32/innittst
/opt/cprocsp/bin/ia32/csptestf
/opt/cprocsp/bin/ia32/der2xer
/opt/cprocsp/lib/ia32/libcapi20.so.4.0.5
/opt/cprocsp/lib/ia32/libcpext.so.4.0.5
/opt/cprocsp/lib/ia32/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.5
/opt/cprocsp/lib/ia32/libssp.so.4.0.5
/opt/cprocsp/lib/ia32/libenroll.so.4.0.5
/opt/cprocsp/lib/ia32/liburlretrieve.so.4.0.5
```

```
/opt/cprocsp/bin/ia32/curl  
/opt/cprocsp/lib/ia32/libcpcurl.so.4.2.0  
/opt/cprocsp/lib/ia32/libcpcurl.a  
/opt/cprocsp/lib/ia32/libcpcdrv_emul.a  
/opt/cprocsp/lib/ia32/libcsp.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrndmbio_tui.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrndmbio_gui.so.4.0.5  
/opt/cprocsp/lib/ia32/libxcpui.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrpcsc.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrpic.so.4.0.5  
/opt/cprocsp/sbin/ia32/ccid_reg.sh  
/opt/cprocsp/bin/ia32/cpverify  
/opt/cprocsp/bin/ia32/wipefile  
/opt/cprocsp/bin/ia32/csptest  
/opt/cprocsp/lib/ia32/libdrdrdr.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrndm.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrsup.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrdsrf.so.4.0.5  
/opt/cprocsp/lib/ia32/libdrfat12.so.4.0.5  
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.5  
/opt/cprocsp/lib/ia32/libcpui.so.4.0.5  
/opt/cprocsp/sbin/ia32/unreg_prov_type_name.sh  
/opt/cprocsp/sbin/ia32/cpconfig  
/opt/cprocsp/sbin/ia32/mount_flash.sh  
/opt/cprocsp/lib/ia32/libdruec.so.4.0.5  
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.5  
/opt/cprocsp/sbin/ia32/stunnel_thread  
/opt/cprocsp/sbin/ia32/stunnel_fork  
/opt/cprocsp/sbin/ia32/stunnel_hsm
```

Intel Solaris (64-bits)

```
/opt/cprocsp/bin/ia32/cryptcp  
/opt/cprocsp/bin/ia32/certmgr  
/opt/cprocsp/bin/ia32/initst  
/opt/cprocsp/bin/ia32/csptestf  
/opt/cprocsp/bin/ia32/der2xer  
/opt/cprocsp/lib/ia32/libcapi20.so.4.0.5  
/opt/cprocsp/lib/ia32/libcpext.so.4.0.5  
/opt/cprocsp/lib/ia32/libpkixcmp.so.4.0.5  
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.5  
/opt/cprocsp/lib/ia32/libssp.so.4.0.5  
/opt/cprocsp/lib/ia32/libenroll.so.4.0.5  
/opt/cprocsp/lib/ia32/liburlretrieve.so.4.0.5  
/opt/cprocsp/bin/amd64/cryptcp  
/opt/cprocsp/bin/amd64/certmgr  
/opt/cprocsp/bin/amd64/initst  
/opt/cprocsp/bin/amd64/csptestf  
/opt/cprocsp/bin/amd64/der2xer  
/opt/cprocsp/lib/amd64/libcapi20.so.4.0.5
```

```
/opt/cprocsp/lib/amd64/libcpxext.so.4.0.5
/opt/cprocsp/lib/amd64/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/amd64/libasn1data.so.4.0.5
/opt/cprocsp/lib/amd64/libssp.so.4.0.5
/opt/cprocsp/lib/amd64/libenroll.so.4.0.5
/opt/cprocsp/lib/amd64/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/ia32/curl
/opt/cprocsp/lib/ia32/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ia32/libcpcurl.a
/opt/cprocsp/bin/amd64/curl
/opt/cprocsp/lib/amd64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/amd64/libcpcurl.a
/opt/cprocsp/lib/ia32/libcpcdrv_emul.a
/opt/cprocsp/lib/ia32/libcsp.so.4.0.5
/opt/cprocsp/lib/ia32/libdrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/amd64/libcsp.so.4.0.5
/opt/cprocsp/lib/amd64/libdrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/ia32/libdrndmbio_gui.so.4.0.5
/opt/cprocsp/lib/ia32/libxcpui.so.4.0.5
/opt/cprocsp/lib/amd64/libdrndmbio_gui.so.4.0.5
/opt/cprocsp/lib/amd64/libxcpui.so.4.0.5
/opt/cprocsp/lib/ia32/libdrpcsc.so.4.0.5
/opt/cprocsp/lib/ia32/libdrrric.so.4.0.5
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/lib/amd64/libdrpcsc.so.4.0.5
/opt/cprocsp/lib/amd64/libdrrric.so.4.0.5
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/libdrdr.so.4.0.5
/opt/cprocsp/lib/ia32/libdrndm.so.4.0.5
/opt/cprocsp/lib/ia32/libdrsup.so.4.0.5
/opt/cprocsp/lib/ia32/libdrdsrf.so.4.0.5
/opt/cprocsp/lib/ia32/libdrfat12.so.4.0.5
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.5
/opt/cprocsp/lib/ia32/libcpui.so.4.0.5
/opt/cprocsp/sbin/ia32/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ia32/cpconfig
/opt/cprocsp/sbin/ia32/mount_flash.sh
/opt/cprocsp/bin/amd64/cpverify
/opt/cprocsp/bin/amd64/wipefile
/opt/cprocsp/bin/amd64/csptest
/opt/cprocsp/lib/amd64/libdrdr.so.4.0.5
/opt/cprocsp/lib/amd64/libdrndm.so.4.0.5
/opt/cprocsp/lib/amd64/libdrsup.so.4.0.5
/opt/cprocsp/lib/amd64/libdrdsrf.so.4.0.5
/opt/cprocsp/lib/amd64/libdrfat12.so.4.0.5
/opt/cprocsp/lib/amd64/libcapi10.so.4.0.5
/opt/cprocsp/lib/amd64/libcpui.so.4.0.5
```

```
/opt/cprocsp/sbin/amd64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/amd64/cpconfig
/opt/cprocsp/sbin/amd64/mount_flash.sh
/opt/cprocsp/lib/ia32/libdruec.so.4.0.5
/opt/cprocsp/lib/amd64/libdruec.so.4.0.5
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.5
/opt/cprocsp/lib/amd64/librsaenh.so.4.0.5
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/sbin/ia32/stunnel_hsm
/opt/cprocsp/sbin/amd64/stunnel_thread
/opt/cprocsp/sbin/amd64/stunnel_fork
/opt/cprocsp/sbin/amd64/stunnel_hsm
```

Приложение А

Управление протоколированием

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

Таблица А1. Модули аудита

Модуль (name)	Описание
cap10	CryptoAPI 1.0
cap120	CryptoAPI 2.0
ssp	TLS
cspr	клиентский RPC
cpext	расширения CryptoAPI
cloud	облачный провайдер
csp	ядро CSP
pcsc	считыватели PC/SC

1) Solaris i386, SPARC 32

Для определения **уровня протокола** (levelmask, см. [табл. А2](#)):

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

Для задания **формата протокола** (formatmask, см. [табл. А3](#)):

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

Для просмотра текущих значений уровня и формата протокола:

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

2) SPARC 64

Для определения **уровня протокола** (levelmask, см. [табл. А2](#)):

```
/opt/CPR0csp/sbin/sparcv9/cpconfig -loglevel <name> -mask <levelmask>
```

Для задания **формата протокола** (formatmask, см. [табл. А3](#)):

```
/opt/CPR0csp/sbin/sparcv9/cpconfig -loglevel <name> -format <formatmask>
```

Для просмотра текущих значений уровня и формата протокола:

```
/opt/CPR0csp/sbin/sparcv9/cpconfig -loglevel <name> -view
```

3) Solaris i386, SPARC 32, SPARC 64 уровня ядра

`/usr/kernel/drv/drvcsp.conf`
отредактировать `loglevel`

Таблица A2. Уровни протоколирования

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

Таблица A3. Форматы протокола

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

Лист регистрации изменений

[illegible]