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 Linux

ЖТЯИ.00101-02 91 03
Листов 33

2021 г

Содержание

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционных систем Linux.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base под управлением ОС Linux, 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 КС1 исполнение 1-Base функционирует в следующих группах программно-аппаратных сред:

LSB Linux
Дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x.

CentOS 6 (x86, x64)
CentOS 7 (x86, x64, POWER, ARM, ARM64)
CentOS 8 (x64, POWER, ARM64)
ОСь (OS-RT) (x64)
ТД ОС АИС ФССП России (GosLinux) (x86, x64)
РЕД ОС 7.1/7.2 (x86, x64, ARM64)
Fedora 28/29/30/31 (x86, x64, ARM, ARM64)
Oracle Linux 6 (x86, x64)
Oracle Linux 7 (x64)
Oracle Linux 8 (x64, ARM64)
OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
AlterOS (x64)
SUSE Linux Enterprise Server 11SP4 (x86, x64)
SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64)
Red Hat Enterprise Linux 6 (x86, x64)
Red Hat Enterprise Linux 7/8 (x64, POWER, ARM64)
Check Point GAiA (x86, x64)
Синтез-ОС.РС (x86, x64)
ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64)
ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64)
КП «ОС «СинтезМ-К» (x64)
Ubuntu 14.04/16.04 (x86, x64, ARM, ARM64)
Ubuntu 18.04/19.10/20.04 (x64, ARM, ARM64)
Halo OS (x64)
Linux Mint 18/19/20 (x86, x64)
Debian 8/9/10 (x86, x64, ARM, ARM64, MIPS)
Лотос (x86, x64)
Astra Linux Special Edition, Common Edition (x86, x64, ARM, ARM64, MIPS, Эльбрус)
МСВСфера 6.3 Сервер (x64, ARM64)
ThinLinux 2 (x64)
ЕМИАС 1.0 (x64)
Мурена 1.4 (ARM9)

Примечание. При эксплуатации СКЗИ необходимо учитывать, что порядок и сроки эксплуатации операционных систем, в среде которых функционирует СКЗИ, определяются производителями операционных систем. Использование СКЗИ под управлением ОС, для которых не выпускаются обновления, не допускается.

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 Linux для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. В операционных системах Linux используется менеджер пакетов RPM (Red Hat Package Manager), который является гибким инструментом для установки, удаления, обновления и сборки программных пакетов. Пакеты, представленные в виде файла с расширением .rpm, содержат в себе непосредственно файлы ПО и информацию для конфигурирования среды.

Примечание. Для автоматической установки основных пакетов СКЗИ можно воспользоваться скриптом `install.sh`, входящим в состав дистрибутива. Также можно выполнить установку в графическом интерфейсе посредством запуска скрипта `install_gui.sh`.

Для удаления СКЗИ используйте скрипт `uninstall.sh`.

Для установки пакета используется команда: `rpm -i <файл_пакета>`

Например: `rpm -i ./lsb-cprocsp-base-5.0-5.noarch.rpm`

Для удаления пакета используется команда: `rpm -e <имя_пакета>`

Например: `rpm -e lsb-cprocsp-base-5.0-5`

Имя пакета может не включать версию, например: `rpm -e lsb-cprocsp-base`

На ОС, основанных на **Debian (Debian/Ubuntu)**, для **установки** пакетов используется команда:

`dpkg -i <файл_пакета>`

Например: `dpkg -i ./lsb-cprocsp-base_5.0-6_all.deb`

На ОС, основанных на **Debian (Debian/Ubuntu)**, для **удаления** пакетов используется команда:

`dpkg -P <имя_пакета_без_версии>`

Например: `dpkg -P lsb-cprocsp-base`

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

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

Пакеты могут быть независимыми от архитектуры (noarch в имени файла пакета), тогда они

устанавливаются на любую архитектуру. Пакеты могут быть предназначены для архитектуры IA32 (i486 в имени файла пакета), а также для архитектуры AMD64 (x86_64 в имени файла пакета), 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 устанавливать оба комплекта. Исключением являются драйверы – они устанавливаются в точном соответствии с архитектурой ядра ОС.

В ОС Linux модули ядра не обладают бинарной совместимостью, они привязаны к конкретной версии ядра ОС. Поэтому модуль ядра поставляется в виде пакета .src.rpm. Такой тип пакета позволяет собрать модуль для нужной версии ядра. Для его установки следует при помощи rpmbuild собрать из пакета .src.rpm обычный пакет .rpm, а затем установить пакет .rpm так же как остальные пакеты.

На большинстве дистрибутивов сборку пакета .rpm можно осуществить командой:

```
rpmbuild --rebuild --define "kernel_release `uname -r`" <путь к файлу пакета>
```

Для сборки требуется, чтобы на машине были установлены средства сборки (компилятор), а также заголовочные файлы ядра. Заголовочные файлы ядра должны находиться в `/lib/modules/` и обычно их можно установить в составе соответствующего пакета из репозитория дистрибутива.

Так как наличие средств отладки и разработки на системах, в которых эксплуатируется СКЗИ, недопустимо, администратор (разработчик СФ) должен собрать пакет на специальном выделенном рабочем месте и обеспечивать его доверенную установку в целевую систему.

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

Имя пакета	Зависимости	Назначение пакета
Пакеты для предварительной установки		
cprocsp-compat-altlinux		Пакет совместимости с ОС AltLinux, устанавливается первым — до lsb-cprocsp-base
cprocsp-compat-splat		Пакет совместимости с ОС SPLAT, устанавливается первым — до lsb-cprocsp-base
sobol		Драйвер для ПАК Соболь, требуется при наличии устройства
Обязательные пакеты		
lsb-cprocsp-base	lsb	Базовый пакет КриптоПро CSP (устанавливается первым, если не нужны compat-пакеты)
lsb-cprocsp-rdr	lsb-cprocsp-base	Модуль поддержки основных приложений, считывателей и ДСЧ
lsb-cprocsp-kc1	lsb-cprocsp-rdr	Провайдер класса КС1
lsb-cprocsp-kc2	lsb-cprocsp-rdr	Провайдер класса КС2, устанавливается только там, где в этом есть необходимость; в этом случае lsb-cprocsp-kc1 обычно не ставится
lsb-cprocsp-capilite	lsb-cprocsp-rdr, lsb-cprocsp-kc1 или lsb-cprocsp-kc2	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS. . .)

Дополнительные пакеты		
cprocsp-rdr-gui	lsb-cprocsp-rdr, Motif, X11	Графический БиоДСЧ, запрос пароля и другие GUI-диалоги
cprocsp-rdr-gui-gtk	lsb-cprocsp-rdr	Графический интерфейс для диалоговых операций
cprocsp-rdr-pcsc	lsb-cprocsp-rdr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт
lsb-cprocsp-pkcs11	lsb-cprocsp-rdr	Модуль поддержки PKCS11
lsb-cprocsp-devel	lsb-cprocsp-base	Пакет для разработчика приложений, использующих КриптоПро CSP
cprocsp-drv	lsb-cprocsp-base	Драйверная библиотека
cprocsp-drv-devel	lsb-cprocsp-devel	Пакет для разработчика драйверов
cprocsp-curl	lsb-cprocsp-capilite	Библиотека libcurl с поддержкой российских криптоалгоритмов
cprocsp-cptools-gtk	lsb-cprocsp-capilite	Графическое приложение для доступа к основным функциям и настройкам КриптоПро CSP
cprocsp-rdr-cloud	lsb-cprocsp-capilite	Модуль взаимодействия с КриптоПро DSS — КриптоПро Cloud CSP
cprocsp-rdr-cloud-gtk	cprocsp-rdr-cloud	Графический интерфейс для диалоговых операций КриптоПро Cloud CSP
cprocsp-stunnel	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель
cprocsp-stunnel-msspi	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель с поддержкой интерфейса msspi
cprocsp-xer2print	lsb-cprocsp-base	Скрипты и xsl-шаблоны для конвертации xer-файлов в pdf/ps/html
lsb-cprocsp-ca-certs	lsb-cprocsp-capilite	Корневые сертификаты доверенных ЦС
cprocsp-ipsec-devel	lsb-cprocsp-devel	Пакет для разработчика приложений, использующих КриптоПро IPsec
cprocsp-ipsec-esp		Модуль ядра (LKM) КриптоПро IPsec ESP
cprocsp-ipsec-genpsk	lsb-cprocsp-rdr	Утилиты PSK
cprocsp-ipsec-ike	lsb-cprocsp-rdr	Динамические библиотеки уровня пользователя
Поддержка считывателей/ДСЧ		
lsb-cprocsp-rdr-accord	lsb-cprocsp-rdr	Модуль поддержки Аккорд-АМДЗ
lsb-cprocsp-rdr-ancud	lsb-cprocsp-rdr	Модуль поддержки устройств производства АНКАД
lsb-cprocsp-rdr-crypton	lsb-cprocsp-rdr	Модуль поддержки АПМДЗ КРИПТОН-ЗАМОК (АНКАД)
lsb-cprocsp-rdr-maxim	lsb-cprocsp-rdr	Модуль поддержки ДСЧ в составе АПМДЗ МАКСИМ М1
lsb-cprocsp-rdr-sobol	lsb-cprocsp-rdr, sobol	Модуль поддержки ПАК Соболь
lsb-cprocsp-rdr-vityaz	lsb-cprocsp-rdr	Модуль поддержки ДСЧ в составе АПМДЗ Витязь-А

Поддержка ключевых носителей		
cprocsp-rdr-cpfkc	cprocsp-rdr-pcsc	Модуль поддержки ФКН с поддержкой SESPAKE
cprocsp-rdr-edoc	cprocsp-rdr-pcsc	Модуль поддержки платформы eDoc (УЛГ)
cprocsp-rdr-emv	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Gemalto (EMV)
cprocsp-rdr-esmart	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов ESMART
cprocsp-rdr-infocrypt	cprocsp-rdr-pcsc	Модуль поддержки токенов InfoCrypt
cprocsp-rdr-inpaspot	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Alioth
cprocsp-rdr-jacarta	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов JaCarta
cprocsp-rdr-kst	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт MorphoKST
cprocsp-rdr-mskey	cprocsp-rdr-pcsc	Модуль поддержки токенов Multisoft MS_Key
cprocsp-rdr-novacard	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Novacard
cprocsp-rdr-rosan	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Rosan
cprocsp-rdr-rutoken	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов Рутокен

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Linux необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
  - набор установленных пакетов;
  - настройки провайдера (можно сохранить `/etc/opt/cprocsp/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`).

Примечание. Ключи и сертификаты сохраняются автоматически.

4 Настройка СКЗИ

4.1 Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/cprocsp/sbin/<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 cpconfig 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 пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

```
# cpconfig -license -view
```

Для ввода лицензии выполните:

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

Серийный номер следует вводить с соблюдением регистра символов.

4.3 Настройка оборудования СКЗИ

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

Для просмотра списка настроенных считывателей:

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

Для просмотра списка настроенных ДСЧ:

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

Для консольного БиоДСЧ требуется пакет lsb-cprocsp-kc1. Для добавления консольного БиоДСЧ:

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

Для графического БиоДСЧ требуется пакет cprocsp-rdr-gui (или cprocsp-rdr-gui-gtk) и X-сервер. БиоДСЧ регистрируется автоматически при установке указанных пакетов.

Для использования внешней гаммы:

```
# ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3

# ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/
db1/kis_1

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

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

```
# cp /tmp/db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1

# cp /tmp/db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1
```

Для 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`.

4.8 Использование СКЗИ с nginx/Apache

nginx и Apache — ПО с открытым исходным кодом для веб-серверов. Одной из основных функциональностей указанных серверов является построение защищенного соединения с пользователями.

В состав СКЗИ входят модули для nginx 1.18.0 и Apache 2.4.25/2.4.41, обеспечивающие возможность построения защищенного TLS-соединения и работы в рамках этого соединения на ОС семейства Linux с использованием ГОСТ-алгоритмов с помощью вызова функций СКЗИ. При использовании данных модулей для выполнения криптографических операций вместо стандартной OpenSSL-реализации будут вызываться функции SSPI- и CryptoAPI-интерфейсов СКЗИ.

Примечание. ППО nginx 1.18.0 не входит в комплект поставки СКЗИ КриптоПро CSP. Исходные тексты nginx 1.18.0 скачиваются с официального сайта с последующей проверкой контрольной суммы (FBD0B63EB5D43CB5A61526E9D94F1FC536B2DF69ADE3C54CE84BE5D2B8992DB8) с использованием утилиты cpverify (см. Приложение 1 документа ЖТЯИ.00101-02 95 01. Правила пользования, параметры по умолчанию).
После применения патча и сборки nginx для исполняемых модулей должна быть зафиксирована контрольная сумма.

Примечание. Отключение в конфигурационном файле флагов sspi_client_verify_local_crl_only, proxy_ssl_verify_local_crl_only и proxy_ssl_verify_ignore_cn допускается только в тестовых целях.

5 Работа в ОС Astra Linux

5.1 Настройка работы с веб-сервером Apache

Для обеспечения совместной работы СКЗИ и веб-сервера Apache 2.4.25 под управлением ОС Astra Linux необходимо:

1) Установить СКЗИ КриптоПро CSP (см. Установка дистрибутива ПО СКЗИ).

2) Заменить путь в конфигурационном файле mods-enabled/ssl.load до astra_se_mod_ssl.so из состава СКЗИ.

Примечание. astra_se_mod_ssl.so требует наличия openssl-1.0.

3) Сгенерировать сертификаты пользователю, от имени которого будет запущен сервер Apache.

Примечание. Примеры генерации сертификатов описаны в create_certs.sh, install_root_certs.sh. Рекомендуется не запускать данные примеры, а выполнять генерацию сертификатов аналогично.

4) По умолчанию используется конфигурационный файл sites-enabled/default-ssl.conf. Необходимо заменить указанные в нем сертификаты и выставить параметры, аналогичные cpro.conf.

Для тестирования корректности работы веб-сервера можно воспользоваться скриптом (требуется наличие openssl-1.1.0).

Тестовый скрипт не учитывает ошибки, связанные с верификацией сертификата сервера (т.к. тестируется не клиент, а сервер). Для того, чтобы не было ошибок верификации сертификата на клиенте, необходимо добавить в хранилище root сертификат УЦ, который выдал сертификат сервера.

5.2 Настройка работы с веб-сервером nginx

В составе дистрибутива СКЗИ поставляется патч `ng-nginx.1.18.0.patch`, который необходимо применить к исходным текстам дистрибутива веб-сервера nginx 1.18.0.

ППО nginx 1.18.0 не входит в комплект поставки СКЗИ КриптоПро CSP. Исходные тексты nginx 1.18.0 скачиваются с официального сайта с последующей проверкой контрольной суммы (FBD0B63EB5D43CB5A61526E9D94F1FC536B2DF69ADE3C54CE84BE5D2B8992DB8) с использованием утилиты cpverify (см. Приложение 1 документа ЖТЯИ.00101-02 95 01. Правила пользования, параметры по умолчанию).

После применения патча осуществляется сборка «пропатченных» исходных текстов сервера nginx с последующим вычислением ЭП (в соответствии с эксплуатационной документацией на ОС Astra Linux SE) для возможности их использования в замкнутой программной среде (ЗПС) ОС Astra Linux SE.

Примечание. Отключение в конфигурационном файле флагов sspi_client_verify_local_crl_only, proxy_ssl_verify_local_crl_only и proxy_ssl_verify_ignore_cn допускается только в тестовых целях.

5.3 Использование СКЗИ в замкнутой программной среде ОС Astra Linux Special Edition

Для установки СКЗИ КриптоПро CSP в замкнутой программной среде (ЗПС) ОС Astra Linux Special Edition необходимо:

1) Указать следующие параметры в файле /etc/digsig/digsig_initramfs.conf:
   - для ОС Astra Linux SE версии 1.6:

```
DIGSIG_ELF_MODE=1
```

- для ОС Astra Linux SE версии 1.5:

```
DIGSIG_LOAD_KEYS=1
DIGSIG_ENFORCE=1
```

2) Установить пакет совместимости с помощью следующей команды (только для ОС Astra Linux SE версии 1.6):

```
apt install astra-digsig-oldkeys
```

3) Создать директорию для файла ключа с помощью следующей команды:

```
mkdir -p /etc/digsig/keys/legacy/keys/
```

4) Разместить файл ключа cryptopro_pub_key.gpg в директории, созданной на предыдущем шаге, с помощью следующей команды:

```
cp cryptopro_pub_key.gpg /etc/digsig/keys/legacy/keys/
```

5) Обновить диски оперативной памяти с помощью следующей команды:

```
update-initramfs -u -k all
```

6) Выполнить перезагрузку системы.

7) Установить СКЗИ КриптоПро CSP (см. Установка дистрибутива ПО СКЗИ).

Примечание. Настройка и использование ЗПС должны осуществляться в соответствии с эксплуатационной документацией на ОС Astra Linux Special Edition.

5.4 Модуль Check

В состав СКЗИ входит модуль Check, который представляет собой набор самостоятельных (не требующих установки базовых модулей КриптоПро CSP) программных компонентов, выполняющих функции расчета хэш-значения и проверки ЭП и предназначенных для эксплуатации под управлением ОС СН Astra Linux SE.

Модуль реализован как динамически и статически подключаемые библиотеки. Статически подключаемые библиотеки предназначены для использования только в составе ядра ОС Astra Linux SE с проведением установленным для указанной ОС порядком работ по исследованиям ОС СН Astra Linux SE.

Подробнее интерфейс библиотек описан в документе ЖТЯИ.00101-02 96 04. Руководство программиста. Check.

6 Состав и назначение компонент ПО СКЗИ

6.1 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
`drvcsp`	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 (Iinetd-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.

6.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

6.2.1 Модуль libcapi20

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

6.2.2 Модули устройств хранения ключевой информации

Библиотека librdrsup обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевой информации.

Следующие модули обеспечивают реализацию доступа к конкретным типам ключевых носителей:

`librdrcpfkc.so`	токены и смарт-карты с поддержкой SESPAKE
`librdrcloud.so`	облачный токен
`librdrcryptoki.so`	доступ к ключам ФКН через интерфейс PKCS#11
`librdredoc.so`	платформа eDoc (УЛГ)
`librdremv.so`	смарт-карты Gemalto (EMV)
`librdresmarttoken.so`	смарт-карты и токены ESMART Token
`librdresmarttokengost.so`	смарт-карты и токены ESMART Token ГОСТ
`librdrfat12.so`	съемные диски и раздел HDD/SDD
`librdrinfocrypt.so`	токены InfoCrypt
`librdrinpaspot.so`	смарт-карты Alioth
`librdrjacarta.so`	токены и смарт-карты JaCarta
`librdrkst.so`	смарт-карты MorphoKST
`librdrmskey.so`	токены Multisoft MS_Key
`librdrnova.so`	смарт-карты Novacard
`librdrpcsc.so`	базовый считыватель носителей, поддерживающих интерфейс PC/SC
`librdrric.so`	смарт-карты Оскар и Форос (Магистра)
`librdrrosan.so`	смарт-карта Rosan
`librdrrutoken.so`	смарт-карты и токены Рутокен

6.2.3 Модули считывателей

Следующие модули обеспечивают реализацию доступа к конкретным типам считывателей:

`librdraccord.so`	АМДЗ Аккорд
`librdrcrypton.so`	АПМДЗ КРИПТОН-ЗАМОК
`librdrmaxim.so`	АПМДЗ МАКСИМ М1
`librdrsbl.so`	ПАК Соболь
`librdrvityaz.so`	АПМДЗ Витязь-А

6.2.4 Модули датчиков случайных чисел

Следующие модули обеспечивают поддержку работы с ДСЧ:

`librdrdsrf.so`	КриптоПро Исходный материал (ДСДР)
`librdrrndmbio_tui.so`	БиоДСЧ
`librdrrndmbio_gui_fgtk.so`	Графический БиоДСЧ

6.2.5 Библиотека поддержки протокола ASN1

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

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 Linux 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 Linux 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 Linux

Настройки ОС Linux выполняются путем редактирования (удаления, добавления) различных конфигурационных и командных файлов.

Для сохранения возможности «откатить» внесенные изменения следует сохранять модифицируемые файлы в «безопасном» месте (на внешнем носителе или на не монтируемой автоматически файловой системе). Желательно скопировать изменяемые файлы (каталоги) с сохранением структуры каталогов.

Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

1) В файле `/etc/login.defs` следует установить следующие директивы:
   - PASS_MAX_DAYS=180 (параметр задаёт максимальное время использования пароля)
   - PASS_MIN_DAYS=30 (параметр задаёт минимальное количество дней между сменами пароля)
   - PASS_MIN_LEN=8 (параметр задаёт минимальную длину пароля)

2) Для защиты пароля может быть использована библиотека libxcrypt, осуществляющая хранение пароля в виде хэш-значения.

3) В файле `/etc/profile` установить значение umask=022 (параметр задает маску создания файла по-умолчанию)

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

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

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

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

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

9) 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 инсталляции ОС выделить для файловых систем `/, /usr, /usr/local, /var` разные разделы диска.

Настройка сетевых сервисов

1) Следует ограничить функциональность демона управления сетевыми соединениями xinetd, если он используется в системе (например, с помощью редактирования файла `/etc/xinetd.conf` и файлов в каталоге `/etc/xinetd.d`). Следует запретить следующие сервисы (при их наличии в системе):
   - echo
   - discard
   - daytime
   - chargen
   - finger
   - systat
   - netstat
   - tftp
   - telnet
   - nfsd

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) (например, с помощью команды `/sbin/accton`);

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 %/etc/securetty
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop %tcpdump
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
```

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

```
chmod g-s /bin/mail
chmod g-s /usr/bin/write
chmod g-s /bin/netstat
chmod g-s /usr/sbin/nfsstat
chmod g-s /usr/bin/ipcs
chmod g-s /sbin/arp
chmod g-s /bin/dmesg
chmod g-s /sbin/swapon
chmod g-s /usr/bin/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 (например, путем указания в файле /etc/vsftpd/vsftpd.conf параметра ftpd_banner)

• отредактировать файлы /etc/issue, /etc/banners/ftp.msg 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 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         /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 root /var/adm/loginlog
chmod 644 /var/adm/loginlog
```

6) Следует обеспечить протоколирование сетевых соединений, контролируемых демоном xinetd (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
```

8 Требования по криптографической защите

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

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 7.2.

Контролем целостности должны быть охвачены файлы:

Linux (x86)

```
/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/bin/ia32/cp-genpsk.sh
/opt/cprocsp/bin/ia32/genpsk
/opt/cprocsp/lib/ia32/libike_gost.so.4.0.5
/opt/cprocsp/lib/ia32/libesp_gost.so.4.0.5
/opt/cprocsp/lib/ia32/librdremv.so.4.0.5
/opt/cprocsp/bin/ia32/list_pcsc
/opt/cprocsp/lib/ia32/librdrpcsc.so.4.0.5
/opt/cprocsp/lib/ia32/librdrric.so.4.0.5
/opt/cprocsp/sbin/ia32/ccid_reg.sh
/opt/cprocsp/lib/ia32/librsaenh.so.4.0.5
/opt/cprocsp/sbin/ia32/stunnel_hsm
/opt/cprocsp/sbin/ia32/stunnel_thread
/opt/cprocsp/sbin/ia32/stunnel_fork
/opt/cprocsp/bin/ia32/cryptcp
/opt/cprocsp/bin/ia32/certmgr
/opt/cprocsp/bin/ia32/inittst
/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/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/ia32/libasn1data.so.4.0.5
/opt/cprocsp/lib/ia32/libsspdrv.a
/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/lib/ia32/libcsp.so.4.0.5
/opt/cprocsp/lib/ia32/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/ia32/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/ia32/cpverify
/opt/cprocsp/bin/ia32/wipefile
/opt/cprocsp/bin/ia32/csptest
/opt/cprocsp/lib/ia32/librdrrndm.so.4.0.5
/opt/cprocsp/lib/ia32/librdrsup.so.4.0.5
/opt/cprocsp/lib/ia32/librdrdsrf.so.4.0.5
```

```
/opt/cprocsp/lib/ia32/librdrfat12.so.4.0.5
/opt/cprocsp/lib/ia32/libcapi10.so.4.0.5
/opt/cprocsp/lib/ia32/libcpui.so.4.0.5
/opt/cprocsp/lib/ia32/libcpalloc.so.0.0.0
/opt/cprocsp/lib/ia32/libjemalloc.so.0.0.0
/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/librdrsbl.so.4.0.5
```

Linux (x64)

```
/opt/cprocsp/bin/amd64/curl
/opt/cprocsp/lib/amd64/libcpcurl.a
/opt/cprocsp/lib/amd64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/amd64/libcpcdrv_emul.a
/opt/cprocsp/bin/amd64/cp-genpsk.sh
/opt/cprocsp/bin/amd64/genpsk
/opt/cprocsp/lib/amd64/libike_gost.so.4.0.5
/opt/cprocsp/lib/amd64/libesp_gost.so.4.0.5
/opt/cprocsp/lib/amd64/librdremv.so.4.0.5
/opt/cprocsp/bin/amd64/list_pcsc
/opt/cprocsp/lib/amd64/librdrpcsc.so.4.0.5
/opt/cprocsp/lib/amd64/librdrric.so.4.0.5
/opt/cprocsp/sbin/amd64/ccid_reg.sh
/opt/cprocsp/lib/amd64/librsaenh.so.4.0.5
/opt/cprocsp/sbin/amd64/stunnel_fork
/opt/cprocsp/sbin/amd64/stunnel_thread
/opt/cprocsp/sbin/amd64/stunnel_hsm
/opt/cprocsp/bin/amd64/cryptcp
/opt/cprocsp/bin/amd64/certmgr
/opt/cprocsp/bin/amd64/inittst
/opt/cprocsp/bin/amd64/csptestf
/opt/cprocsp/bin/amd64/der2xer
/opt/cprocsp/lib/amd64/libcapi20.so.4.0.5
/opt/cprocsp/lib/amd64/libcpext.so.4.0.5
/opt/cprocsp/lib/amd64/libasn1data.so.4.0.5
/opt/cprocsp/lib/amd64/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/amd64/libsspdrv.a
/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/lib/amd64/libcsp.so.4.0.5
/opt/cprocsp/lib/amd64/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/amd64/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/amd64/cpverify
/opt/cprocsp/bin/amd64/wipefile
/opt/cprocsp/bin/amd64/csptest
/opt/cprocsp/lib/amd64/librdrrndm.so.4.0.5
/opt/cprocsp/lib/amd64/librdrsup.so.4.0.5
```

```
/opt/cprocsp/lib/amd64/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/amd64/librdrfat12.so.4.0.5
/opt/cprocsp/lib/amd64/libcapi10.so.4.0.5
/opt/cprocsp/lib/amd64/libcpui.so.4.0.5
/opt/cprocsp/lib/amd64/libcpalloc.so.0.0.0
/opt/cprocsp/lib/amd64/libjemalloc.so.0.0.0
/opt/cprocsp/sbin/amd64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/amd64/cpconfig
/opt/cprocsp/sbin/amd64/mount_flash.sh
/opt/cprocsp/lib/amd64/librdrsbl.so.4.0.5
```

Linux (ARM)

```
/opt/cprocsp/bin/arm/curl
/opt/cprocsp/lib/arm/libcpcurl.a
/opt/cprocsp/lib/arm/libcpcurl.so.4.2.0
/opt/cprocsp/sbin/arm/stunnel_hsm
/opt/cprocsp/sbin/arm/stunnel_thread
/opt/cprocsp/sbin/arm/stunnel_fork
/opt/cprocsp/bin/arm/cryptcp
/opt/cprocsp/bin/arm/certmgr
/opt/cprocsp/bin/arm/csptestf
/opt/cprocsp/lib/arm/libcapi20.so.4.0.5
/opt/cprocsp/lib/arm/libcpext.so.4.0.5
/opt/cprocsp/lib/arm/libasn1data_XER.so.4.0.5
/opt/cprocsp/lib/arm/libasn1data.so.4.0.5
/opt/cprocsp/lib/arm/libssp.so.4.0.5
/opt/cprocsp/lib/arm/libsspdrv.a
/opt/cprocsp/lib/arm/libenroll.so.4.0.5
/opt/cprocsp/lib/arm/liburlretrieve.so.4.0.5
/opt/cprocsp/lib/arm/libcsp.so.4.0.5
/opt/cprocsp/lib/arm/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/bin/arm/cpverify
/opt/cprocsp/bin/arm/wipefile
/opt/cprocsp/bin/arm/csptest
/opt/cprocsp/lib/arm/librdrrndm.so.4.0.5
/opt/cprocsp/lib/arm/librdrsup.so.4.0.5
/opt/cprocsp/lib/arm/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/arm/librdrfat12.so.4.0.5
/opt/cprocsp/lib/arm/libcapi10.so.4.0.5
/opt/cprocsp/lib/arm/libcpui.so.4.0.5
/opt/cprocsp/sbin/arm/unreg_prov_type_name.sh
/opt/cprocsp/sbin/arm/cpconfig
/opt/cprocsp/sbin/arm/mount_flash.sh
```

Linux (POWER)

```
/opt/cprocsp/bin/ppc64/curl
/opt/cprocsp/lib/lib64/libcpcurl.so.4.2.0
```

```
/opt/cprocsp/lib/lib64/libcpcurl.a
/opt/cprocsp/lib/lib64/libcpcdrv_emul.a
/opt/cprocsp/bin/ppc64/cp-genpsk.sh
/opt/cprocsp/bin/ppc64/genpsk
/opt/cprocsp/lib/lib64/libike_gost.so.4.0.4
/opt/cprocsp/lib/lib64/libesp_gost.so.4.0.4
/opt/cprocsp/lib/lib64/librdremv.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_gui.so.4.0.4
/opt/cprocsp/lib/lib64/libxcpui.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_gui_fgtk.so.4.0.4
/opt/cprocsp/lib/lib64/libfgcpui.so.4.0.4
/opt/cprocsp/sbin/ppc64/xcpui_app
/opt/cprocsp/sbin/ppc64/fgtk_rndm_app
/opt/cprocsp/bin/ppc64/list_pcsc
/opt/cprocsp/lib/lib64/librdrpcsc.so.4.0.4
/opt/cprocsp/lib/lib64/librdrric.so.4.0.4
/opt/cprocsp/sbin/ppc64/ccid_reg.sh
/opt/cprocsp/lib/lib64/librdruec.so.4.0.4
/opt/cprocsp/lib/lib64/librsaenh.so.4.0.4
/opt/cprocsp/sbin/ppc64/stunnel_thread
/opt/cprocsp/sbin/ppc64/stunnel_fork
/opt/cprocsp/sbin/ppc64/stunnel_hsm
/opt/cprocsp/bin/ppc64/cryptcp
/opt/cprocsp/bin/ppc64/certmgr
/opt/cprocsp/bin/ppc64/inittst
/opt/cprocsp/bin/ppc64/csptestf
/opt/cprocsp/bin/ppc64/der2xer
/opt/cprocsp/lib/lib64/libcapi20.so.4.0.4
/opt/cprocsp/lib/lib64/libcpext.so.4.0.4
/opt/cprocsp/lib/lib64/libpkixcmp.so.4.0.4
/opt/cprocsp/lib/lib64/libasn1data.so.4.0.4
/opt/cprocsp/lib/lib64/libsspdrv.a
/opt/cprocsp/lib/lib64/libssp.so.4.0.4
/opt/cprocsp/lib/lib64/libenroll.so.4.0.4
/opt/cprocsp/lib/lib64/liburlretrieve.so.4.0.4
/opt/cprocsp/lib/lib64/libcsp.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/lib64/libcppkcs11.so.4.0.4
/opt/cprocsp/bin/ppc64/cpverify
/opt/cprocsp/bin/ppc64/wipefile
/opt/cprocsp/bin/ppc64/csptest
/opt/cprocsp/lib/lib64/librdrrdr.so.4.0.4
/opt/cprocsp/lib/lib64/librdrrndm.so.4.0.4
/opt/cprocsp/lib/lib64/librdrsup.so.4.0.4
/opt/cprocsp/lib/lib64/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/lib64/librdrfat12.so.4.0.4
/opt/cprocsp/lib/lib64/libcapi10.so.4.0.4
/opt/cprocsp/lib/lib64/libcpui.so.4.0.4
/opt/cprocsp/lib/lib64/libcpalloc.so.0.0.0
/opt/cprocsp/lib/lib64/libjemalloc.so.0.0.0
```

```
/opt/cprocsp/sbin/ppc64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ppc64/cpconfig
/opt/cprocsp/sbin/ppc64/mount_flash.sh
/opt/cprocsp/lib/lib64/librdrsbl.so.4.0.4
```

Приложение А
Управление протоколированием

В состав СКЗИ КриптоПро CSP включена новая система аудита, отличная от предыдущих версий СКЗИ.

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**
`capi10`	CryptoAPI 1.0
`capi20`	CryptoAPI 2.0
`ssp`	TLS
`cspr`	клиентский RPC
`cpext`	расширения CryptoAPI
`cloud`	облачный провайдер
`csp`	ядро CSP
`pcsc`	считыватели PC/SC

Для управления протоколированием конкретного модуля аудита (`name`) необходимо задать уровень протоколирования и формат протокола:

1) Для определения **уровня протокола** (`levelmask`):

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

Значением параметра является шестнадцатеричное число, состоящее из 3 частей, вида 0x0XX0YY0ZZ. Старшая часть (XX) определяет вид информации, которая будет записываться в **syslog**, средняя (YY) — информацию, вывод которой осуществляется в **консоль**, младшая (ZZ) — в текущей реализации не используется.

В каждую часть необходимо установить значение, которое является побитовой суммой необходимых N_DB*-флагов (см. табл. А2).

Таблица А2. 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 событий (например, создание ключа, удаление ключевого контейнера, ...)

2) Для задания **формата протокола** (`formatmask`):

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

или

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name_fmt> -mask <formatmask>
```

Значением параметра является побитовая сумма необходимых DBFMT_*-флагов (см. табл. А3).

Таблица А3. 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

Для просмотра текущих значений уровня и формата протокола:

```
/opt/cprocsp/sbin/<название_архитектуры>/cpconfig -loglevel <name> -view
```

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					