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 AIX

ЖТЯИ.00101-02 91 06
Листов 26

2021 г

# 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 . . . . . 11
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) . . . . . 14
5.2.1 Модуль libcapi20 . . . . . 14
5.2.2 Модули устройств хранения ключевой информации . . . . . 15
5.2.3 Библиотека librdrsup . . . . . 15
5.2.4 Модули датчиков случайных чисел . . . . . 15
5.2.5 Библиотека libasn1data поддержки протокола ASN1 . . . . . 15

**6 Встраивание СКЗИ в прикладное ПО** . . . . . **16**

**7 Требования по защите от НСД** . . . . . **17**
7.1 Организационно-технические меры защиты от НСД . . . . . 17
7.2 Дополнительные настройки ОС AIX . . . . . 17

**8 Требования по криптографической защите** . . . . . **21**

**Приложение А. Управление протоколированием** . . . . . **24**

# 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 AIX.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС AIX, 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 AIX используется в программно-аппаратных средах:

ОС AIX 6/7 (POWER)

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

http://www.ibm.com/software/support/systemsp/lifecycle/

## 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 AIX 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 AIX 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.

Для удаления СКЗИ используйте скрипт `uninstall.sh`.

**Для установки пакета** используется команда:

```
rpm -i <файл_пакета>
```

Например: `rpm -i ./lsb-cprocsp-base-5.0-aix.5.3.noarch.rpm`

**Для удаления пакета** используется команда:

```
rpm -e <имя_пакета>
```

Например: `rpm -e lsb-cprocsp-base-5.0-aix.5.3`

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

Также управление пакетами можно выполнять через графическую оболочку smitty.

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 ставятся на любую архитектуру. Пакеты могут быть для архитектуры ppc32 (ppc в имени файла пакета), а также для архитектуры ppc64 (ppc64 в имени файла пакета), тогда они ставятся на ОС, собранную под соответствующую архитектуру. Часто 64-битные ОС одновременно поддерживают и 32-битные приложения, и 64-битные, тогда при необходимости можно ставить оба комплекта.

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

| Имя пакета | Зависимости | Назначение пакета |
|---|---|---|
| **Обязательные пакеты** | | |
| cprocsp-base | | Базовый пакет КриптоПро CSP, устанавливается первым |
| cprocsp-rdr | cprocsp-base | Модуль поддержки основных приложений, считывателей и ДСЧ |
| cprocsp-kc1 | cprocsp-rdr | Провайдер класса КС1 |
| cprocsp-capilite | cprocsp-rdr, cprocsp-kc1 | CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS. . . ) |
| **Дополнительные пакеты** | | |
| cprocsp-pkcs11 | cprocsp-rdr | Модуль поддержки PKCS11 |
| cprocsp-devel | cprocsp-base | Пакет для разработчика приложений, использующих КриптоПро CSP |
| cprocsp-stunnel | cprocsp-capilite | Универсальный SSL/TLS туннель |
| cprocsp-curl | cprocsp-capilite | Библиотека libcurl с поддержкой российских криптоалгоритмов |
| cprocsp-ca-certs | cprocsp-capilite | Корневые сертификаты доверенных ЦС |
| cprocsp-xer2print | cprocsp-base | Скрипты и xsl-шаблоны для конвертации xer-файлов в pdf/ps/html |

# 3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС AIX необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
  - набор установленных пакетов;
  - настройки провайдера (для простоты 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);
- 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 после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

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

Для ввода лицензии выполните:

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

Серийный номер следует вводить с соблюдением регистра символов.

## 4.3 Настройка оборудования СКЗИ

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

Для просмотра списка настроенных считывателей:

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

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

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

Для просмотра списка настроенных ДСЧ:

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

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

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

Для добавления использования внешней гаммы:

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

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

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

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

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

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

Для 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 |
| `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 (linetd-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;
- [d] (опционально) — указывает на документацию (тестовые примеры);
- ppc/ppc64 — платформа PowerPC 32/64 бита.

## 5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

### 5.2.1 Модуль libcapi20

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

capilite является подмножеством интерфейса CryptoAPI 2.0.

### 5.2.2 Модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:
- librdrfat12 — к съемным дискам и разделу HDD/SDD

### 5.2.3 Библиотека librdrsup

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

### 5.2.4 Модули датчиков случайных чисел

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

### 5.2.5 Библиотека libasn1data поддержки протокола ASN1

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

# 6 Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ КриптоПро CSP в прикладное программное обеспечение должны выполняться требования раздела 4 документа ЖТЯИ.00101-02 90 01. КриптоПро CSP. Правила пользования и документа ЖТЯИ.00101-02 96 01. КриптоПро CSP. Руководство программиста.

Для использования библиотек КриптоПро CSP в ОС AIX в прикладных приложениях при линковке библиотек и исполняемых файлов с библиотеками КриптоПро CSP необходимо использовать C++ компоновщик (xlC_r).

При работе с КриптоПро CSP в дочерних потоках рекомендуется устанавливать размер стека для потока не менее 700 KB:

- с помощью pthread_attr_init() и pthread_attr_setstacksize() задать размер;
- передать атрибут в pthread_create();
- уничтожить его вызовом pthread_attr_destroy().

# 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 AIX 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 AIX 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 AIX

Настройки ОС AIX 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) Используя утилиту smitty, следует установить следующие директивы для всех пользователей системы:
- Expiration date — не больше 180 дней с момента создания
- Number of failed logins before locked=10 (количество неверных попыток регистрации пользователя)
- Soft core file size=0K (для запрета создания core-файлов)
- UMASK=022 (параметр задает маску создания файла по-умолчанию)
- Another user can su = False (параметр ограничивает возможность регистрации суперпользователя через утилиту su)

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

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

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

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

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

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

### Ограничения при монтировании файловых систем

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

### Настройка сетевых сервисов

1) Следует ограничить функциональность сервисов, не используемых в данной системе (например, путем редактирования файла `/etc/inittab`). Следует запретить следующие сервисы (при их наличии в системе):
- echo
- discard
- daytime
- chargen
- finger
- systat
- netstat
- tftp
- telnet

2) Используя утилиту smitty, отключить неиспользуемые сетевые сервисы и службы, запускаемые при старте системы.

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

4) 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. 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

5) 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 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
chmod 400 /usr/bin/uuencode
```

6) 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/prtconf
chmod g-s /usr/sbin/swap
```

### 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) Следует удостоверится, что только пользователь root имеет доступ на запись для файлов содержащих информацию о протоколируемых событиях.

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.

5) Следует протоколировать сетевые соединения (включая дату/время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение).

# 8 Требования по криптографической защите

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

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

Контролем целостности должны быть охвачены файлы:

## AIX (PowerPC 32 bits)

```
/opt/cprocsp/bin/ppc/cryptcp
/opt/cprocsp/bin/ppc/certmgr
/opt/cprocsp/bin/ppc/inittst
/opt/cprocsp/bin/ppc/csptestf
/opt/cprocsp/bin/ppc/der2xer
/opt/cprocsp/lib/ppc/libcapi20.so.4.0.5
/opt/cprocsp/lib/ppc/libcpext.so.4.0.5
/opt/cprocsp/lib/ppc/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/ppc/libasn1data.so.4.0.5
/opt/cprocsp/lib/ppc/libssp.so.4.0.5
/opt/cprocsp/lib/ppc/libenroll.so.4.0.5
/opt/cprocsp/lib/ppc/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/ppc/curl
/opt/cprocsp/lib/ppc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ppc/libcpcurl.a
/opt/cprocsp/lib/ppc/libcsp.so.4.0.5
/opt/cprocsp/lib/ppc/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/ppc/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/ppc/cpverify
/opt/cprocsp/bin/ppc/wipefile
/opt/cprocsp/bin/ppc/csptest
/opt/cprocsp/lib/ppc/librdrrndm.so.4.0.5
/opt/cprocsp/lib/ppc/librdrsup.so.4.0.5
/opt/cprocsp/lib/ppc/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/ppc/librdrfat12.so.4.0.5
/opt/cprocsp/lib/ppc/libcapi10.so.4.0.5
/opt/cprocsp/lib/ppc/libcpui.so.4.0.5
/opt/cprocsp/sbin/ppc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ppc/cpconfig
/opt/cprocsp/sbin/ppc/mount_flash.sh
/opt/cprocsp/lib/ppc/librsaenh.so.4.0.5
/opt/cprocsp/sbin/ppc/stunnel_thread
/opt/cprocsp/sbin/ppc/stunnel_fork
/opt/cprocsp/sbin/ppc/stunnel_hsm
```

## AIX (PowerPC 64 bits)

```
/opt/cprocsp/bin/ppc/cryptcp
/opt/cprocsp/bin/ppc/certmgr
```

```
/opt/cprocsp/bin/ppc/inittst
/opt/cprocsp/bin/ppc/csptestf
/opt/cprocsp/bin/ppc/der2xer
/opt/cprocsp/lib/ppc/libcapi20.so.4.0.5
/opt/cprocsp/lib/ppc/libcpext.so.4.0.5
/opt/cprocsp/lib/ppc/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/ppc/libasn1data.so.4.0.5
/opt/cprocsp/lib/ppc/libssp.so.4.0.5
/opt/cprocsp/lib/ppc/libenroll.so.4.0.5
/opt/cprocsp/lib/ppc/liburlretrieve.so.4.0.5
/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/ppc64/libcapi20.so.4.0.5
/opt/cprocsp/lib/ppc64/libcpext.so.4.0.5
/opt/cprocsp/lib/ppc64/libpkixcmp.so.4.0.5
/opt/cprocsp/lib/ppc64/libasn1data.so.4.0.5
/opt/cprocsp/lib/ppc64/libssp.so.4.0.5
/opt/cprocsp/lib/ppc64/libenroll.so.4.0.5
/opt/cprocsp/lib/ppc64/liburlretrieve.so.4.0.5
/opt/cprocsp/bin/ppc/curl
/opt/cprocsp/lib/ppc/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ppc/libcpcurl.a
/opt/cprocsp/bin/ppc64/curl
/opt/cprocsp/lib/ppc64/libcpcurl.so.4.2.0
/opt/cprocsp/lib/ppc64/libcpcurl.a
/opt/cprocsp/lib/ppc/libcsp.so.4.0.5
/opt/cprocsp/lib/ppc64/libcsp.so.4.0.5
/opt/cprocsp/lib/ppc/libcppkcs11.so.4.0.5
/opt/cprocsp/lib/ppc64/libcppkcs11.so.4.0.5
/opt/cprocsp/bin/ppc/cpverify
/opt/cprocsp/bin/ppc/wipefile
/opt/cprocsp/bin/ppc/csptest
/opt/cprocsp/lib/ppc/librdrrndm.so.4.0.5
/opt/cprocsp/lib/ppc/librdrsup.so.4.0.5
/opt/cprocsp/lib/ppc/librdrdsrf.so.4.0.5
/opt/cprocsp/lib/ppc/librdrfat12.so.4.0.5
/opt/cprocsp/lib/ppc/libcapi10.so.4.0.5
/opt/cprocsp/lib/ppc/libcpui.so.4.0.5
/opt/cprocsp/sbin/ppc/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ppc/cpconfig
/opt/cprocsp/sbin/ppc/mount_flash.sh
/opt/cprocsp/bin/ppc64/cpverify
/opt/cprocsp/bin/ppc64/wipefile
/opt/cprocsp/bin/ppc64/csptest
/opt/cprocsp/lib/ppc64/librdrrndm.so.4.0.5
/opt/cprocsp/lib/ppc64/librdrsup.so.4.0.5
/opt/cprocsp/lib/ppc64/librdrdsrf.so.4.0.5
```

```
/opt/cprocsp/lib/ppc64/librdrfat12.so.4.0.5
/opt/cprocsp/lib/ppc64/libcapi10.so.4.0.5
/opt/cprocsp/lib/ppc64/libcpui.so.4.0.5
/opt/cprocsp/sbin/ppc64/unreg_prov_type_name.sh
/opt/cprocsp/sbin/ppc64/cpconfig
/opt/cprocsp/sbin/ppc64/mount_flash.sh
/opt/cprocsp/lib/ppc/librsaenh.so.4.0.5
/opt/cprocsp/lib/ppc64/librsaenh.so.4.0.5
/opt/cprocsp/sbin/ppc/stunnel_thread
/opt/cprocsp/sbin/ppc/stunnel_fork
/opt/cprocsp/sbin/ppc/stunnel_hsm
/opt/cprocsp/sbin/ppc64/stunnel_thread
/opt/cprocsp/sbin/ppc64/stunnel_fork
/opt/cprocsp/sbin/ppc64/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** |
|---|---|
| `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 |

1) RH7.3, RH9.0

Для определения **уровня протокола** (`levelmask`, см. табл. А2):
`/usr/CPROcsp/sbin/cpconfig -loglevel <name> -mask <levelmask>`

Для задания **формата протокола** (`formatmask`, см. табл. А3):
`/usr/CPROcsp/sbin/cpconfig -loglevel <name> -format <formatmask>`

Для просмотра текущих значений уровня и формата протокола:
`/usr/CPROcsp/sbin/cpconfig -loglevel <name> -view`

2) для RH 7.3, RH 9.0 уровня ядра

`insmod drvcsp.o log_level=<levelmask>`

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, ...) |

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 |

# 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 | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |