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 KC1 1-Base

Руководство администратора безопасности. Использование СКЗИ под управлением ОС AIX

ЖТЯИ.00101-01 91 06
Листов 27

2019 г

Содержание

Аннотация

Настоящее Руководство дополняет документ ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть при использовании СКЗИ под управлением ОС AIX.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base, 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 версии 5.0 КС1 (ЖТЯИ.00101-01) 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.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.9.

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.

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, устанавливается первым.
cprocsp-rdr	cprocsp-base	Основные приложения, считыватели и ДСЧ.
cprocsp-kc1	cprocsp-rdr	Провайдер КС1.
cprocsp-capilite	cprocsp-rdr, cprocsp-kc1	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS. . .).
Дополнительные пакеты		
cprocsp-devel	cprocsp-base	Пакет для разработчика.
cprocsp-stunnel	cprocsp-capilite	Универсальный SSL/TLS туннель.

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС AIX необходимо:

- запомнить текущую конфигурацию 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 (обычно в `/var/log/messages`). Существует возможность изменения настроек журналирования различных модулей продукта. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений. Для получения справки по настройкам журналирования:

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

Модули, для которых поддерживается журналирование:
- cpcsp — ядро криптопровайдера
- capi10 — CryptoAPI 1.0
- cpext — дополнения для CryptoAPI 2.0
- capi20 — CryptoAPI 2.0
- capilite — CAPILite
- libcspr — библиотека для подключения к провайдеру в сервисе или к HSM-серверу
- cryptsrv — служба хранения ключей
- libssp — TLS
- cppkcs11 — PKCS11
- cpdrv — драйвер
- dmntcs — тестовое приложение для обращения к тестовому драйверу

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>
```

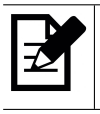
4.6 Включение режима усиленного контроля использования ключей

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 Установка сопутствующих пакетов

Для передачи по сети запросов на сертификаты, CRL и т.п., а также для поддержки дополнительных ключевых считывателей и носителей может потребоваться установка дополнительных пакетов.

Если сопутствующие пакеты скачиваются из Интернета, необходимо подтвердить их целостность, проверив подпись или хэш. Если источник не обеспечивает такие механизмы, допускается использование пакетов только с диска с дистрибутивом СКЗИ, где эти механизмы используются. На диске пакеты лежат в папке \extra.

5.1 Библиотека libcurl

Используется для передачи запросов на сертификаты, CRL и т.п. по сети.

С сайта разработчика проекта можно скачать пакет с исходными текстами для самостоятельной сборки. Как правило, там же есть 32-битные бинарные пакеты.

32-битный бинарный пакет доступен на сайте производителя ОС: http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/rpmgroups.html

После установки библиотек необходимо зарегистрировать пути к ним. Например:

```
/opt/cprocsp/sbin/ppc/cpconfig -ini '\config\apppath' -add string libcurl.so /usr/local/lib/libcurl.so
```

```
/opt/cprocsp/sbin/ppc64/cpconfig -ini '\config\apppath' -add string libcurl.so /usr/local/lib/64/libcurl.so
```

6 Состав и назначение компонент ПО СКЗИ

6.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:
- libcsp — динамически загружаемая библиотека «КриптоПро CSP».
- libssp — библиотека поддержки модуля сетевой аутентификации «КриптоПро TLS».
- cpverify — модуль контроля целостности.
- wipefile — модуль удаления файлов вместе с содержимым.

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.

6.1.1 Библиотека libcsp

Библиотека libcsp реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ.

6.1.2 Модули сетевой аутентификации КриптоПро TLS

Модуль libssp обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS. Общее описание протокола приведено в документе ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

Протокол TLS (RFC 2246) используется для защиты соединений в клиент-серверных технологиях.

Программное обеспечение «КриптоПро TLS» является реализацией протокола TLS и использует криптографические функции КриптоПро CSP для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером.

6.1.3 Модуль cpverify

Модуль cpverify предназначен для контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на ПЭВМ пользователя.

6.1.4 Модуль wipefile

Модуль wipefile используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях.

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 v. 2.0. Интерфейс модуля capilite является подмножеством интерфейса CryptoAPI v. 2.0.

6.2.2 Библиотека librdrrdr

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

6.2.3 Модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:
- librdrfat12 — к дисководу и дискете 3.5"и разделу жесткого диска

6.2.4 Библиотека librdrsup

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

6.2.5 Модули датчиков случайных чисел

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

6.2.6 Библиотека libasn1data поддержки протокола ASN1

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

7 Встраивание СКЗИ в прикладное ПО

При встраивании СКЗИ КриптоПро CSP версии 5.0 KC1 в прикладное программное обеспечение должны выполняться требования раздела 7 документа ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и документа ЖТЯИ.00101-01 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 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().

8 Требования по защите от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 документа ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть и раздела 5 ЖТЯИ.00101-01 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).

8.1 Организационно-технические меры защиты от НСД

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

1) В системе регистрируется один пользователь, обладающий правами администратора, носящий имя root, на которого возлагается обязанность конфигурировать ОС AIX, настраивать безопасность ОС AIX, а также конфигурировать ПЭВМ, на которую установлена ОС AIX.

2) Для пользователя root выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 8 символов, среди символов пароля должны встречаться заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в 6 месяцев, доступ к паролю должен быть обеспечен только администратору.

3) Пользователю root доступны настройки всех пользователей ОС AIX, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в ОС AIX, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС AIX, не являющийся пользователем root, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему пользователем root.

4) Всех пользователей ПЭВМ, которые не пользуются данной системой, и всех стандартных пользователей, которые создаются в ОС AIX во время установки (таких, как sys, uucp, nuucp и listen), кроме пользователя root, следует удалить.

5) В ОС AIX существуют исполняемые файлы, которые запускаются с правами пользователя root. Эти файлы имеют установленный флаг SUID. Пользователь root должен определить, каким из этих файлов в рамках определенной в организации политики безопасности не требуется запуск с административными полномочиями, и с помощью сброса флага SUID должен свести количество таких файлов к минимуму. Запуск оставшихся файлов с установленным флагом SUID должен контролироваться пользователем root.

6) При использовании СКЗИ КриптоПро CSP на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

7) Право доступа к рабочим местам с установленным ПО СКЗИ КриптоПро CSP предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе СКЗИ КриптоПро CSP.

8) На технических средствах, оснащенных СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-производителей.

9) В BIOS определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на HDD: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

10) Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств и PCI-устройств при использовании ПАК защиты от НСД.

11) При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав СКЗИ «КриптоПро CSP», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ с использованием программы CPVERIFY.

12) Вход в BIOS ЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю пользователя root. Пароль для входа в BIOS должен быть известен только пользователю root и быть отличным от пароля пользователя root для входа в ОС AIX.

13) Средствами BIOS должна быть исключена возможность работы на ЭВМ, если во время его начальной загрузки не проходят встроенные тесты.

14) На ПЭВМ устанавливается только одна ОС. На ПЭВМ не устанавливаются средств разработки и отладки ПО. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ КриптоПро CSP. Следует избегать попадания в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии root.

15) Должно быть ограничено (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время.

16) Должно быть реализовано физическое затирание содержимого удаляемых файлов с использованием программы Wipefile из состава СКЗИ.

17) Должны быть отключены все неиспользуемые сетевые протоколы.

18) В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть отключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, в прикладных программах без проведения дополнительных тематических исследований.

19) Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства СКЗИ КриптоПро CSP, по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

20) Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ КриптоПро CSP после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

21) Администратором безопасности должно быть проведено опечатывание системного блока с установленным СКЗИ КриптоПро CSP, исключающее возможность несанкционированного изменения аппаратной части рабочей станции.

22) Из состава системы должно быть исключено оборудование, которое может создавать угрозу безопасности ОС AIX. Также необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование ПЭВМ или ОС AIX.

23) После инсталляции ОС AIX следует установить все рекомендованные программные обновления и программные обновления, связанные с безопасностью, существующие на момент инсталляции.

24) На все директории, содержащие системные файлы ОС AIX и каталоги СКЗИ, необходимо установить права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись.

25) В связи с тем, что аварийный дамп оперативной памяти может содержать криптографически опасную информацию, в прикладных программах, использующих СКЗИ, следует отключить возможность его создания с помощью функции ulimit (установить размер дампа памяти в 0).

26) В ОС AIX используется виртуальная память. Область виртуальной памяти должна быть организована на отдельном жестком диске. По окончании работы СКЗИ содержимое виртуальной памяти должно затираться с использованием средств ОС. В случае аварийного останова ЭВМ, при следующей загрузке необходимо в режиме «single user» очистить область виртуальной памяти программой wipefile, входящей в состав СКЗИ КриптоПро CSP. В случае выхода из строя жесткого диска, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а жесткий диск не подлежащим ремонту. Этот жесткий диск уничтожается по правилам уничтожения ключевых носителей.

8.2 Дополнительные настройки ОС AIX

Дополнительные настройки ОС AIX касаются следующего:

- ограничение доступа пользователей и настройки пользовательского окружения;
- ограничение сетевых соединений;
- ограничения при монтировании файловых систем;
- ограничения на запуск процессов;
- контроль загрузки ОС и контроль целостности системного и прикладного программного обеспечения должен обеспечиваться при помощи программно-аппаратного комплекса защиты от НСД (см. соответствующий раздел в документе ЖТЯИ.00101-01 91 01. КриптоПро CSP. Руководство администратора безопасности. Общая часть);
- дополнительные настройки ядра ОС;
- настройка сетевых сервисов;
- ограничение количества «видимой извне» информации о системе;
- настройка подсистемы протоколирования и аудита.

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

Настройка пользовательского окружения заключается в следующих действиях:

1) Используя утилиту smitty, следует установить следующие директивы для всех пользователей системы:
   - Expiration date — не больше 30 дней с момента создания.
   - Number of failed logins before locked=3 (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 077 или 027: `umask 077 (umask 027)`;

3) Отредактировать файл `/etc/shells` и поместить в него имена только для тех исполняемых файлов оболочек, которые установлены в системе. По-умолчанию, содержимое файла `/etc/shells` может быть таким:

```
/bin/csh
/bin/tcsh
```

```
/bin/sh
/usr/local/bin/bash
```

4) Удалить файл (если он существует) `/.rhosts`.

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

6) Отредактировать файл `/etc/pam.conf` с целью запрета rhosts-аутентификации. Выполняется комментированием всех строк, содержащих подстроку 'pam_rhosts_auth.so'.

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

8) Создать перечень программ, которые запускаются с правами администратора, и контролировать его неизменность;

9) Запретить регистрацию в системе пользователей, имеющих следующие «служебные имена»:

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

Действие выполняется путем указания в файле `/etc/passwd` строки ' ' в поле shell-программы и указания символа 'x' в поле пароля.

Ограничения при монтировании файловых систем

Ограничения при монтировании файловых систем реализуются редактированием файла `/etc/filesystems`:

- Установить опцию nosuid при монтировании файловых системы и /var.

При инсталляции системы следует выделить для файловых систем /, /usr, /usr/local, /var, /opt, /export разные разделы диска для предотвращения переполнения критичных файловых систем (/, /var) за счет, например, пользовательских данных и обеспечения возможности монтирования файловых систем /usr и /opt в режиме "только для чтения".

Ограничения на запуск процессов

Следует ограничить использование в системе планировщика задач cron и средств пакетной обработки заданий. Для нормального функционирования системы минимально необходимым является разрешение использования планировщика задач cron и средств пакетной обработки заданий только пользователю root. Для этого следует выполнить следующие команды (от имени суперпользователя):

```
echo root > /var/adm/cron/allow

echo root > /var/adm/cron/at.allow
```

Настройка сетевых сервисов

Настройка сетевых сервисов заключается в следующем:

1) Следует ограничить функциональность сервисов не используемых в данной системе. Действие заключается в редактировании файла /etc/inittab. В файле /etc/inittab следует закомментровать (удалить) строки, содержащие описания тех сервисов, использование которых на конфигурируемом компьютере не является необходимым.

Как минимум, следует запретить следующие сервисы:

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

2) Используя утилиту smitty, отключить неиспользуемые сетевые сервисы, и службы, запускаемых при старте системы. Следует запретить прием из внешней сети "широковещательных"(broadcast) пакетов, а также передачу ответов на принятые "широковещательные"пакеты.

3) Если планируется использовать на настраиваемом сервере сервис FTP, то следует запретить доступ по протоколу FTP пользователям, для которых запрещен доступ к серверу по протоколу FTP. В списке «запрещенных» пользователей, как минимум, должны быть перечислены следующие имена пользователей:

- adm
- bin
- daemon
- listen
- lp
- nobody
- noaccese
- nobody4
- nuucp
- root
- smtp
- sys
- uucp

4) Для ограничения доступа к системным файлам для непривилегированных пользователей, из командной строки следует выполнить следующие команды:

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 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
```

5) Также следует обнулить флаг SGID для некоторых исполняемых файлов:

```
chmod g-s /usr/bin/mail
chmod g-s /usr/bin/mailx
chmod g-s /usr/bin/write
chmod g-s /usr/bin/netstat
chmod g-s /usr/bin/nfsstat
```

```
chmod g-s /usr/bin/ipcs
chmod g-s /usr/sbin/arp
chmod g-s /usr/sbin/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.).

К мерам по ограничению количества «видимой извне» информации о системе относятся:

- Отказ от стандартного «заголовка», выводимого сервером ftp при ответе пользователю.
- Редактирование файлов /etc/issue, /etc/ftpbanner 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) С учетом выбранной в организации политики безопасности должно быть ограничено 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).

9 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-01 91 01.КриптоПро CSP. Руководство администратора безопасности. Общая часть в части, касающейся ОС AIX.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 8.2.

Контролем целостности должны быть охвачены файлы:

AIX (Power PC 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/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/ppc/librdrrndmbio_tui.so.4.0.5
/opt/cprocsp/lib/ppc64/libcsp.so.4.0.5
/opt/cprocsp/lib/ppc64/librdrrndmbio_tui.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/librdrrdr.so.4.0.5
/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/librdrrdr.so.4.0.5
/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

Для включения/отключения значение log используйте:
1) RH7.3, RH9.0

Для задания уровня протокола:
```
/usr/CPROcsp/sbin/cpconfig -loglevel cpcsp -mask 0x9
```

Для задания формата протокола:
```
/usr/CPROcsp/sbin/cpconfig -loglevel cpcsp -format 0x19
```

Для просмотра маски текущего уровня и формата протокола:
```
/usr/CPROcsp/sbin/cpconfig -loglevel cpcsp -view
```

2) для RH 7.3, RH 9.0 уровня ядра

```
insmod drvcsp.o log_level=0x9
```

Значением параметра уровень протокола является битовая маска:
N_DB_ERROR = 1 # сообщения об ошибках
N_DB_LOG = 8 # сообщения о вызовах

Значением параметра формат протокола является битовая маска:
DBFMT_MODULE = 1 # выводить имя модуля
DBFMT_THREAD = 2 # выводить номер нитки
DBFMT_FUNC = 8 # выводить имя функции
DBFMT_TEXT = 0x10 # выводить само сообщение
DBFMT_HEX = 0x20 # выводить HEX дамп
DBFMT_ERR = 0x40 # выводить GetLastError

Лист регистрации изменений

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					