Утвержден

ВЕМР.00118-01-/ЛУ

ПС «Купол-СКЗИ для Linux»

Инструкция по загрузке и настройке

ВЕМР.00118-01 99 01

Листов 14

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

2019

Литера $О_1$

АННОТАЦИЯ

Настоящий документ содержит сведения о назначении, функциях и структуре программного средства «Купол-СКЗИ для Linux» ВЕМР.00118-01 (далее по тексту – ПС «Купол-СКЗИ для Linux»). Описаны условия его выполнения, приведены сведения по установке и настройке, описаны процедуры запуска, завершения.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ СРЕДСТВЕ

1.1. Назначение программного средства

1.1.1. ПС «Купол-СКЗИ для Linux» предназначено для построения защищённых распределённых хранилищ данных.

1.2. Условия выполнения программного средства

1.2.1. ПС «Купол-СКЗИ для Linux» функционирует на ПЭВМ с характеристиками не ниже следующих:

- процессор Intel Core 2 Duo 1,8 ГГц;
- оперативная память 2048 Мбайт;
- жесткий диск 100 Гбайт;
- сетевая плата Fast Ethernet 100 Мбит/с.

1.2.2. Программное средство функционирует в среде ОС СН «Astra Linux 1.6 Special Edition» (Смоленск).

2. УСТАНОВКА И НАСТРОЙКА ПРОГРАММНОГО СРЕДСТВА

2.1. Установка программного средства

2.1.1. Для установки комплекса программ необходимо:

– выполнить установку и настройку (в соответствии с п. 2.1.2 настоящего документа) ОС СН «Astra Linux 1.6 Special Edition» (Смоленск).

– скопировать на локальную машину каталог kupolcore/bin, находящийся на компакт–диске ВЕМР.00118-02 12 02 Исполняемые файлы. В данном каталоге расположены бинарные файлы модулей и конфигурационные файлы (operator - файл, содержащий цифровые данные оператора РР, rrwserv.cfg - конфигурационный файл сервера, содержит имена директорий и команды вызовов модулей areestr и creestr, stopserv - файл, необходимый для остановки сервера РР).

2.1.2. Для настройки ОС СН «Astra Linux 1.6 Special Edition» (Смоленск) необходимо выполнить следующие действия:

1) механизм замкнутой программной среды должен быть настроен для работы в штатном режиме. Настройка режима функционирования осуществляется посредством графической утилиты fly-admin-smc («Панель управления — Безопасность — Политика безопасности — Замкнутая программная среда») или путем редактирования конфигурационного файла /etc/digsig/digsig_initramfs.conf. Для использования штатного режима функционирования необходимо установить для параметра DIGSIG_ELF_MODE значение:

```
DIGSIG_ELF_MODE=1
```

Для включения замкнутой программной среды в каталог /etc/digsig/keys необходимо поместить (при наличии) переданный публичный ключ (например компания_pub_key.gpg). В файле /etc/digsig/digsig_initramfs.conf установить параметры:

```
DIGSIG_ENFORCE=1

DIGSIG_LOAD_KEYS=1
```

Выполнить:

```
update-inutramfs -u -k all
```

Перезагрузить компьютер.

2) с использованием средств управления дискреционными ПРД пользователям должен быть запрещен доступ к библиотеке libpcprofile.so;

3) с использованием средств управления мандатными ПРД всем отчуждаемым носителям, используемым на объекте эксплуатации, должны быть присвоены мандатные метки, соответствующие грифу обрабатываемой информации. Все отчуждаемые носители должны быть учтены режимно-секретным отделом организации, эксплуатирующей автоматизированную систему. Использование неучтенных отчуждаемых носителей должно быть запрещено;

4) с использованием средств управления дискреционными ПРД пользователям, не обладающим привилегиями администратора, должен быть запрещен запуск (использование) средств создания символических ссылок;

5) в случае разрешения интерактивного входа суперпользователя root для предотвращения подбора его пароля необходимо заблокировать возможность его удаленного входа в ОС посредством включения PAM-модуля pam_securetty в файл сценария /etc/pam.d/common-auth. Для этого необходимо в «Primary block» в указанном файле первой строкой добавить:

```
auth required pam_securetty.so
```

6) используя графическую утилиту fly-admin-smc («Управление политикой безопасности»), запущенную от имени администратора через механизм sudo, в категории «Политики учетной записи» задать следующие значения для настройки политики паролей:

а) «Сложность»:

«Минимальная длина пароля» — 8;

установить флаг «Минимальное количество строчных букв в новом пароле»;

установить флаг «Минимальное количество заглавных букв в новом пароле»;

установить флаг «Минимальное количество цифр в новом пароле»;

установить флаг «Минимальное количество других символов в новом пароле»;

б) «Срок действия»:

установить флаг «Минимальное количество дней между сменами пароля» и в поле задать значение «0 дней»;

установить флаг «Максимальное количество дней между сменами пароля» и в поле задать значение «90 дней»;

Пароль не должен содержать в себе никаких осмысленных слов (ни в каких раскладках).

Дополнительно необходимо запретить повторное использование последних четырех паролей, откорректировав файл /etc/pam.d/common-password. Для этого в указанном файле в строке «...pam_unix.so» добавить параметр `remember=4`;

7) используя графическую утилиту fly-admin-smc («Управление политикой безопасности»), запущенную от имени администратора через механизм sudo (см. электронную справку), в категории «Политики учетной записи» задать следующие значения для настройки блокировки:

установить флаг «Неуспешных попыток» и в поле задать значение 6;

установить флаг «Период блокировки» и в поле задать значение «1800 секунд»;

Убедиться, что `pam_tally` настроен на блокировку учетных записей при попытках подбора паролей (настроено по умолчанию при установке ОС).

Команда faillog показывает содержимое журнала неудачных попыток (файл /var/log/faillog) входа в систему. Также она может быть использована для управления счетчиком неудачных попыток и их ограничением. При запуске faillog без параметров выводятся записи faillog только тех пользователей, у которых имеется хотя бы одна неудачная попытка входа.

8) используя графическую утилиту fly-admin-theme («Программа «Темы рабочего стола»), запущенную от имени администратора через механизм sudo, в разделе «Блокировка» установить флаг «Блокировать экран через» и в поле задать значение «15 мин».

9) Включить запрос пароля при каждом выполнении команды sudo, для чего внести следующие изменения в файл /etc/sudoers:

Для того, чтобы для выполнения первой команды sudo требовалось ввести пароль: удалить "NOPASSWD:" из строки:

```
%astra-admin ALL=(ALL:ALL) NOPASSWD:ALL
```

Для того, чтобы пароль не запоминался для выполнения последующих команд и запрашивался для каждой команды добавить строку:

```
Defaults timestamp_timeout=0
```

10) Для создания пользователя необходимо войти в систему от имени администратора; добавить в систему пользователя командой: `sudo adduser <username>`, задать пароль пользователю командой: `sudo passwd <password>`. Если теперь зайти в систему от имени пользователя и набрать в терминале команду `id`, то будет показана информация о пользователе (его идентификатор, группы). Если набрать команду `macid`, то будет показана информация о мандатном уровне и категориях пользователя. Если теперь снова зайти от имени администратора и набрать команду в терминале: `sudo tail /var/log/auth.log`, то будет выведен фрагмент журнала безопасности. Факт аутентификации пользователя отражен в строке:

```
pam_unix(login:session): session opened for user <username>
```

Информация о зарегистрированных пользователях системы содержится в файлах конфигурации. Изменять эти файлы может только администратор через механизм sudo. Для проверки запрета на доступ несанкционированного пользователя можно попытаться войти в систему от имени несуществующего пользователя, набрав произвольный идентификатор и/или пароль (например, asdf). Затем зайти в систему от имени администратора и набрать команду: `sudo tail /var/log/auth`

Будет показан фрагмент системного журнала событий. Информация о неуспешном входе несанкционированного пользователя показана напротив строки login:

11) Установить мандатный контроль целостности (МКЦ > 0) на всех основных файлах и каталогах в корневой файловой системе. Для этого в графическом ин-

струменте fly-admin-smc «Политика безопасности» -> «мандатный контроль целостности» -> «целостность файловой системы» -> установить «высокий 63».

12) Организация регламентного контроля целостности ОС, прикладного ПО и СЗИ обеспечивается набором программных средств на основе «Another File Integrity Checker» (afick). В указанном наборе реализована возможность для проведения периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования) с последующим сравнением вычисленных значений с эталонными. Эталонные значения контрольных сумм и атрибутов фалов хранятся в БД. База контрольных сумм и атрибутов может быть создана при помощи команды:

```
afick -i
```

Для настройки достаточно параметров, которые указаны в конфигурационном файле по умолчанию (/etc/afick.conf). При запуске afick автоматически установит ежедневное задание для cron. Файл с заданием находится в /etc/cron.daily/afick_cron.

13) Для запуска автоматической процедуры тестирования подсистемы безопасности PARSEC необходимо:

войти в систему от имени администратора;

зайти в каталог /usr/lib/parsec/tests и осуществить запуск скрипта: `sudo run.sh` (или с опцией -v для режима подробного вывода сообщений). При этом на экране монитора будут появляться сообщения о прохождении и результатах выполнения тестов. Подробная информация о результатах тестирования будет записана в файл tests.log, находящийся в каталоге /usr/lib/parsec/tests. Если в тестах хотя бы одна проверка завершится с ошибкой, то вместо строки: Тест ПРОШЕЛ в файле будет содержаться строка: [!] ОШИБКА тестирования.

14) Регистрация событий

Регистрация событий осуществляется подсистемой протоколирования. Для работы, с которой можно использовать как графические утилиты:

- fly-admin-smc («Управление политикой безопасности») — управление протоколированием, привилегиями и мандатными атрибутами пользователей, работа с пользователями и группами;
- fly-admin-viewaudit («Журнал безопасности») — выборочный просмотр протоколов аудита.

Так и утилиты командной строки: getfaud; setfaud; useraud; parselog; kernlog; userlog; psaud.

Сведения, необходимые для работы с вышеназванными утилитами см. в документе: «ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Руководство по КСЗ. Часть 1» раздел «Средства управления протоколированием»

В подсистеме подлежат регистрации следующие события:

- Создание новой, модификация (удаление) существующей учетной записи пользователя.
- Изменение прав пользователя
- Вход / выход пользователей в систему
- расчет контрольных сумм защищаемых файлов.
- проверки контрольных сумм защищаемых файлов.
- попытка получения доступа к защищаемому объекту.
- попытка получения доступа к объекту файловой системы на контролируемом съемном носителе.

Контролю подлежат следующие исполняемые модули:

initus.exe; gencrtk.exe; chpin.exe; rsen.exe; rrec.exe; areestr.exe; creestr.exe; rrwserv.exe, а также конфигурационные файлы rrwserv.cfg, operator, stopserv.

Записи аудита доступа к объекту должны включать не только сам факт разрешенного или запрещенного доступа, но также и причину успеха или отказа.

2.1.3. Установка комплекса программ заключается в установке модулей программного средства:

– Модуль формирования сетевого имени (initus);

– Модуль генерации контейнеров для связи с оператором РР (gencrtk);

– Модуль изменения пароля (chpin);

– Модуль формирования файла для передачи оператору РР (rsen);

– Модуль проверки и экстракции файла (rrec);

– Модуль записи в РР (areestr);

– Модуль извлечения информации из РР по номеру звена (creestr);

– Модуль сервера РР (rrwserv).

2.2. Удаление комплекса программ

2.2.1. Для удаления комплекса программ необходимо выполнить следующие действия:

– удалить каталог bin (который была скопирован с диска при установке).

2.3. Настройка комплекса программ

2.3.1. Дополнительных действий по настройке комплекса программ выполнять не требуется.

3. ЗАПУСК И ЗАВЕРШЕНИЕ КОМПЛЕКСА ПРОГРАММ

3.1. Запуск и завершение

3.1.1. Каждую программу комплекса необходимо запускать в командной строке согласно документу ВЕМР.00118-01 34 01 Руководство оператора.

3.1.2. Для завершения работы программы «Модуль сервера РР» необходимо переместить файл stopserv из директории запуска программы в дочернюю директорию in. Другие программы ПС «Купол-СКЗИ для Linux» завершают свою работу автоматически при выполнении всех необходимых задач.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

РР	–	распределенный реестр
ПС	–	программное средство
ОС	–	операционная система
ПЭВМ	–	персональная электронная вычислительная машина
СН	–	специального назначения

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					