ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

РУСБ.10015-01

Руководство по КСЗ. Часть 1

Оперативное обновление 1.7.1

Бюллетень № 2021-1126SE17

Листов 8

2021

АННОТАЦИЯ

В настоящем руководстве приводятся изменения в документ РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» из комплектности изделия РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС), которые необходимо учитывать при настройке и эксплуатации ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17.

Руководство предназначено для администраторов безопасности.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем руководстве приведены изменения в документ РУСБ.10015-01 97 01-1: измененные разделы, подразделы и пункты документа, а также добавленные разделы, подразделы и пункты.

При администрировании комплекса средств защиты ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17 рекомендуется руководствоваться документом РУСБ.10015-01 97 01-1 совместно с настоящим руководством.

2. ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

2.1. Подраздел «4.6. PARSEC-привилегии»

В таблице 8 подраздела 4.6 описание для привилегии `PARSEC_CAP_CAP` изложить в редакции:

Таблица 8

Привилегия Атрибут Битовая маска	Описание

`PARSEC_CAP_CAP`
`pcapcap`
`0x00400`
	Позволяет устанавливать любой непротиворечивый набор привилегий для вызвавшего процесса и читать привилегии, присвоенные процессам

2.2. Пункт «4.13.2. execaps»

В пункте 4.13.2 пример и абзац после него изложить в редакции:

Пример

```
echo 1 | sudo tee /parsecfs/unsecure_setxattr
sudo execaps -c 0x1000 -- tar --xattrs
     --xattrs-include=security.{PDPL,AUDIT,DEF_AUDIT} --acls -xzf
     backup.tar.gz -C /
echo 0 | sudo tee /parsecfs/unsecure_setxattr

echo 1 | sudo tee /parsecfs/unsecure_setxattr
sudo execaps -c 0x1000 -- sudo rsync -a --xattrs --acls /backup/ /
echo 0 | sudo tee /parsecfs/unsecure_setxattr
```

Будет запущен процесс восстановления из резервной копии с установленной привилегией `PARSEC_CAP_UNSAFE_SETXATTR`.

2.3. Пункт «4.13.3. pscaps»

Пункт 4.13.3 изложить в редакции:

Синтаксис:

```
pscaps <pid> [-v, --version] [-h, --help] [действующие полномочия
     [разрешенные полномочия [наследуемые полномочия]]]
```

Если в качестве аргумента указан только идентификатор процесса `pid`, то команда `pscaps` показывает набор PARSEC-привилегий (указанных в виде битовых масок привилегий) процесса.

При указании с командой битовых масок привилегий (в десятичном или шестнадцатеричном виде) будут изменены привилегии процесса `pscaps`. В этом случае в качестве значения `pid` должно быть указано «0» или идентификатор процесса `pscaps`.

Описание опций приведено в таблице 27.

Таблица 27

Опция	Описание
`-h, --help`	Вывести справку и выйти
`-v, --version`	Вывести информацию о версии и выйти

2.4. Подраздел «10.1. Восстановление ОС после сбоев и отказов»

Подраздел 10.1 начиная с абзаца «После серьезного повреждения ФС, когда компьютер невозможно перезагрузить...» и до конца изложить в редакции:

10.1. Восстановление ОС после сбоев и отказов

По тексту...

После серьезного повреждения ФС, когда компьютер невозможно перезагрузить, существует возможность восстановления без переустановки ОС. Для этого необходимо:

1) установить DVD-диск с дистрибутивом ОС в устройство чтения DVD-дисков;

2) загрузить программу установки ОС с DVD-диска;

3) в окне приветствия программы установки выбрать язык установки (русский или английский);

4) в окне приветствия программы установки выбрать «Режим восстановления»;

5) в окне «[!] Лицензия» подтвердить согласие с лицензионным соглашением;

6) в окне «[!] Настройка клавиатуры» выбрать настройки переключения раскладки клавиатуры, после чего программой установки будет выполнена проверка оборудования и первичная загрузка программ;

7) в окне «[!] Настройка сети» задать имя компьютера (можно указать произвольное имя компьютера, настройки восстанавливаемой ОС не изменятся);

8) в окне «[!] Настройка времени» выбрать часовой пояс;

9) в окне «[!] Войти в режим восстановления» последовательно выполнить следующие шаги:

   а) выбрать пункт «Не использовать корневую файловую систему»;

   б) выбрать следующую операцию режима восстановления: «Запуск оболочки в рабочей среде программы установки»;

   в) нажать на кнопку **[<Продолжить>]**.

Будет выполнен переход в режим командной строки под управлением ядра, загруженного с DVD-диска;

10) определить имя раздела, в который была установлена ОС, для этого выполнить команду:

```
blkid
```

На экране монитора должна появиться информация о разделах жесткого диска (если в результате ввода команды на экране монитора нет информации о разделах диска, то повреждения слишком серьезны и необходима полная переустановка системы).

Пример

Вывод выполнения команды `blkid`

```
/dev/sda1: UUID="bc485787-ef37-431c-8c8b-401055066c99" TYPE="ext4"
     PARTUUID="9492e90e-01"
/dev/sda5: UUID="e8987cad-ee16-427a-a768-a9aa896b048c" TYPE="swap"
     PARTUUID="9492e90e-05"
/dev/sr0: UUID="2021-06-11-12-41-04-00" LABEL="Astra 1.7_x86-64 amd64"
     TYPE="iso9660" PTUUID="66c613b0" PTTYPE="dos"
```

В приведенном примере ОС была установлена в раздел `/dev/sda1`;

11) запустить автоматическую проверку и восстановление ФС, выполнив команду:

```
fsck.ext4 -p -f -c /dev/<имя раздела>
```

Пример

Вывод выполнения команды `fsck`

```
/dev/sda1:Updating bad block inode.
/dev/sda1:318177/2297456 files (0.2% non-contiguous), 4157309/9186816
     blocks
```

12) после проверки нажать комбинацию клавиш **<Ctrl+D>** и извлечь DVD-диск с дистрибутивом ОС из устройства чтения DVD-дисков;

13) в окне «[! !] Войти в режим восстановления» выбрать пункт «Перезагрузка системы».

2.5. Пункт «16.1.1. Режимы функционирования»

Первый абзац пункта 16.1.1 изложить в редакции:

Инструменты замкнутой программной среды (ЗПС) предоставляют возможность внедрения ЭЦП[1)] в исполняемые файлы формата ELF, входящие в состав устанавлива-

[1)] Электронная цифровая подпись — строка бит, полученная в результате процесса формирования подписи (применяется для подписи средствами ОС исполняемых файлов с использованием функции хэширования на базе асимметричного криптографического алгоритма (в соответствии с ГОСТ Р 34.11-2012).

емого СПО, и в расширенные атрибуты файловой системы, обеспечивая таким образом динамический контроль целостности.

2.6. Пункт «16.4.6. Блокировка интерпретаторов»

В пункте 16.4.6 перечень блокируемых интерпретаторов дополнить следующими наименованиями:

- nodejs;
- php.

2.7. Подраздел «17.2. Указания по эксплуатации ОС»

В подразделе 17.2 пункт 17.2.1 дополнить перечислением:

17.2.1. Перед началом эксплуатации ОС администратор безопасности должен обеспечить следующие условия:

7) задать значение времени неактивности для блокировки экрана, отредактировав (или создав, если отсутствует) файл `usr/share/fly-wm/theme.master/themerc`, указав в нем строки:

```
[Variables]
ScreenSaverDelay=<время_неактивности_в_секундах>
LockerOnSleep=true
LockerOnDPMS=true
LockerOnLid=true
LockerOnSwitch=true
```