Настройка механизмов защиты и блокировок

Уровни конфиденциальности

По умолчанию в системе мандатного контроля доступа ОССН Смоленск настроено 4 уровня конфиденциальности:

Номер уровня	Название по умолчанию
0	Уровень_0
1	Уровень_1
2	Уровень_2
3	Уровень_3

При необходимости, количество уровней конфиденциальности может быть увеличено до 255.

Для того, чтобы определить уровни конфиденциальности выше созданных по умолчанию,
и назначать их пользователям, необходимо:

- в файле конфигурации мандатных атрибутов файловой системы /usr/sbin/pdp-init-fs
  задать параметру sysmaclev значение, равное максимальному созданному уровню конфиденциальности
- после внесения изменений перезагрузить машину

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления ->
Безопасность ->
Политика безопасности ->
Мандатные атрибуты ->
Уровни целостности

Управление в консольном режиме:

```
userlev --help
```

Проверка состояния:

userlev
0 Уровень_0
1 Уровень_1
2 Уровень_2
3 Уровень_3

Режим Мандатного Контроля Целостности

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления ->
Безопасность ->
Политика безопасности ->
Мандатный контроль целостности

Управление в консольном режиме:

astra-mic-control [enable/disable]

Проверка состояния

cat /proc/cmdline | grep "parsec.max_ilev"

parsec.max_ilev=63 - включен

Режим Мандатного Контроля Целостности ФС

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Мандатный контроль целостности

Управление в консольном режиме

set-fs-ilev
unset-fs-ilev

Режим ЗПС (замкнутой программной среды) в исполняемых файлах

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Замкнутая программная среда

Блокировка консоли для пользователей

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности

Управление в консольном режиме

astra-console-lock [enable/disable]

Проверка состояния

systemctl is-enabled astra-console-lock
enabled включен
disabled выключен
Failed to get unit file state ... сервис не активирован

Блокировка интерпретаторов

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности

Управление в консольном режиме

astra-interpreters-lock [enable/disable]

Проверка состояния

systemctl is-enabled astra-interpreters-lock
enabled включен
disabled выключен
Failed to get unit file state ... сервис не активирован

Блокировка установки бита исполнения

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности

Управление в консольном режиме

astra-nochmodx-lock [enable/disable]

Проверка состояния:

cat /parsecfs/nochmodx
1 включен
0 выключен

Блокировка макросов

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности

Управление в консольном режиме

astra-macros-lock [enable/disable]

Проверка состояния

systemctl is-enabled astra-macros-lock
enabled включен
disabled выключен
Failed to get unit file state ... сервис не активирован

Блокировка трассировки ptrace

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности -> Параметры ядра

Управление в консольном режиме

astra-ptrace-lock [enable/disable]

Проверка состояния

systemctl is-enabled astra-ptrace-lock
enabled включен
disabled выключен
Failed to get unit file state ... сервис не активирован

Гарантированное удаление файлов и папок

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности -> Политика очистки памяти

Управление в консольном режиме

Добавить опцию монтирования secdel в файле /etc/fstab

Межсетевой экран ufw

Управление в графическом режиме

gufw

Управление в консольном режиме

astra-ufw-control [enable/disable]

Проверка состояния

ufw status
Status: active включен
Status: inactive выключен

Системные ограничения ulimits

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности

Управление в консольном режиме

astra-ulimits-control [enable/disable]

Проверка состояния

systemctl is-enabled astra-ulimits-control
enabled включен
disabled выключен
Failed to get unit file state ... сервис не активирован

Блокировка клавиш SysRq

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Настройки безопасности -> Параметры ядра

Управление в консольном режиме

sysctl -w kernel.sysrq=0
sysctl -w kernel.sysrq=1

Проверка состояния

cat /proc/sys/kernel/sysrq
0 включен
1 выключен

Режим ЗПС (замкнутой программной среды) в расширенных атрибутах

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности -> Замкнутая программная среда

Графический киоск

Управление в графическом режиме с помощью графического инструмента fly-admin-smc:

Панель Управления -> Безопасность -> Политика безопасности

Системный киоск

Управление в графическом режиме с помощью графического инструмента fly-admin-kiosk:

Панель Управления -> Безопасность -> Системный киоск