

Astra Linux SE (OC CH) Смоленск 1.6 Red-Book

- [Настройка безопасной конфигурации компьютера для работы с ОС Astra Linux](#)
- [Перед установкой ОС](#)
- [При установке ОС](#)
- [После установки ОС](#)

Настройка безопасной конфигурации компьютера для работы с ОС Astra Linux Перед установкой ОС

1. Если планируется использовать ОС в рекомендованном режиме очистки освобождающихся дисковых ресурсов, то исключить использование дисков SSD.
2. При возможности - установить и настроить на компьютере аппаратно-программный модуль доверенной загрузки (АПМДЗ).
3. Установить "взломостойкий" пароль на BIOS компьютера.



P.S.

"Взломостойкий" пароль это пароль:

- Содержащий не менее 8 символов;
- Не содержащий в себе никаких осмысленных слов (ни в каких раскладках);
- Содержащий в себе буквы в различных регистрах, цифры и спецсимволы.

4. Отключить в BIOS-е Intel SGX (в связи с обнаруженной уязвимостью в механизме).
5. Необходимо обеспечить защиту от "незаметного" вскрытия корпуса и встраивания "имплантов" в соединительные кабели периферийных устройств". Для обеспечения защиты могут использоваться специальные корпуса, защитные крышки, пломбы, пломбирочные ленты, для усложнения скрытной установки "имплантов" рекомендуется использование ПК в форм-факторе ноутбук или моноблок.
6. Исключить использование беспроводных периферийных устройств ввода (мыши, клавиатуры, тачпады и пр.). Отключить по возможности беспроводные системы передачи данных (WiFi, Bluetooth). При необходимости использования WiFi - по возможности использовать для защиты данных сети VPN.
7. При наличии опций для процессоров Intel Execute Disable Bit (XD-Bit) и для процессоров AMD No Execute Bit (NX-Bit) включить их.
8. При наличии на серверах "не доверенных" систем контроля и управления типа ILO, RSA, iDRAC, ThinkServer EasyManage, AMT, iMana - их необходимо отключить, и использовать, при необходимости, альтернативные решения типа IP KVM.
9. Для Intel платформ необходимо устранить уязвимости Intel-SA-00086 в Intel Management Engine (если он интегрирован в процессор) посредством установки обновления микропрограммы Intel Management Engine (производитель оборудования должен обеспечить данную возможность - это либо обновления BIOS, либо ПО для интеграции обновлений). Для частичных проверок используйте: Intel-SA-00086 Detection Tool.
Более подробно: <https://www.intel.ru/content/www/ru/ru/support/articles/000025619/software.html>
10. Установить ОС CH (обязательно **включенным защитным преобразованием диска**), и по возможности обеспечить невозможность физического доступа к жесткому диску, на котором установлена ОС

При установке ОС

1. Создать отдельные дисковые разделы



```
/
/boot
/home
/tmp
/var/tmp
```

Создать отдельные дисковые разделы

Раздел	Рекомендации по установке/настройке
--------	-------------------------------------

/	С защитным преобразованием (при условии, что /boot размещён в отдельном дисковом разделе). Рекомендуется использовать файловую систему ext4.
/boot	Без защитного преобразования!!! Можно использовать файловую систему etx2, ext3, ext4.
/home	С защитным преобразованием. Рекомендуется использовать файловую систему ext4. Рекомендуется монтировать с опциями noexec, nodev, nosuid.
/tmp	С защитным преобразованием. Рекомендуется использовать файловую систему ext4. Рекомендуется монтировать с опциями noexec, nodev, nosuid.
/var/tmp	С защитным преобразованием. Рекомендуется использовать файловую систему ext4. Рекомендуется монтировать с опциями noexec, nodev, nosuid.
swap	Опционально. С защитным преобразованием.



Для всех перечисленных дисковых разделов рекомендуется использовать файловую системы ext4. При выборе размера дисковых размеров следует помнить, что при размере раздела /tmp менее 250МБ весьма вероятно возникновение ошибок при работе с графикой или с большими объёмами данных.

- Разделы `/home` `/tmp` `/var/tmp` рекомендуется монтировать с опциями `noexec`, `nodev`, `nosuid`
- В разделе установщика "Дополнительные настройки ОС" включить:
 - Включить режим замкнутой программной среды;
 - Запретить установку бита исполнения;
 - Использовать по умолчанию ядро Hardened;
 - Запретить вывод меню загрузчика;
 - Включить очистку разделов страничного обмена (помнить, что очистка освобождаемых ресурсов как правило не работает на SSD-дисках);
 - Включить очистку освобождаемых областей для EXT-разделов (помнить, что очистка освобождаемых ресурсов как правило не работает на SSD-дисках);
 - Включить блокировку консоли;
 - Включить блокировку интерпретаторов;
 - Включить межсетевой экран ufw;
 - Включить системные ограничения ulimits;
 - Отключить возможность трассировки ptrace;
- Установить "взломостойкий" пароль на загрузчик Grub (устанавливается по умолчанию при установке ОС). [Инструкция по смене пароля загрузчика.](#)

После установки ОС

- Установить единственным устройством для загрузки ОС жесткий диск, на который была произведена установка ОС.
- Использовать загрузку ядра HARDENED, и [убрать из меню все другие варианты загрузки](#), включая режимы восстановления.
- Удалить модули ядра, ответственные за работу с Intel Management Engine (MEI). [Инструкция по ссылке.](#)
- Установить и выполнить [все доступные обновления безопасности и методические указания для ОС СН Смоленск 1.6.](#)
- При использовании архитектур, отличных от Intel, установить пароль на загрузчик согласно документации.
- Настроить монтирование раздела `/boot` с опциями `ro` (перед обновлением ядра перемонтировать в `rw`).
- Включить режим загрузки secureboot на своих ключах (создать usb-flash носитель с помощью astra-secureboot, и, далее, ключи импортировать в BIOS в соответствии с [инструкцией](#)
- Установить на устройства - жесткие диски максимальный уровень конфиденциальности (на ОС СН Смоленск 1.6 устанавливается автоматически):



```
/dev/sd*
/dev/hd*
/dev/vd*
```

- Отключить доступ к консоли пользователям (данный пункт актуален для ОС СН Смоленск 1.5, так как для ОС СН Смоленск 1.6 правила работают "из коробки"):

Добавить группу astra-console выполнив команду:

```
i addgroup --gid 333 astra-console
```

Создать файл `/etc/rc.local` со следующим содержанием:

```
i #!/bin/sh -e  
chown root:astra-console /dev/{pts,pts/*,ptmx,tty*}  
chmod g+rx /dev/{pts,pts/*,ptmx,tty*}  
chmod o-rx /dev/{pts,pts/*,ptmx,tty*}  
exit 0
```

Добавить правило в файл `/etc/security/access.conf` командой:

```
echo "-:ALL EXCEPT astra-console :LOCAL" >> /etc/security/access.conf
```

Включить в `/etc/pam.d/login` обработку заданных правил командой

```
sed -i 's|.*account.*pam_access.*|account required pam_access.so|' /etc/pam.d/login
```

Для включения доступа к консоли администраторам необходимо добавить их в группу `astra-console`.

10. Включить блокировку интерпретаторов
11. Включить блокировку установки бита исполнения командами

```
echo 1 > /parsecfs/nochmodx  
echo 1 > /etc/parsec/nochmodx
```

или командой

```
astra-nochmodx-lock enable
```

или через графический инструмент `fly-admin-smc`. Подробности см. [ПУК КСЗ п.16.5.1](#)

12. По возможности, включить блокировку макросов с помощью графического инструмента `fly-admin-smc` или инструмента командной строки `astra-macros-lock`:

```
astra-macros-lock enable
```

13. Включить блокировку трассировки `ptrace`
14. Включить контроль цифровой подписи в исполняемых файлах (ELF-файлах) и в `xattr` всех файлов (Режим Замкнутой Программной Среды). Для этого сгенерируйте ключи и подпишите цифровой подписью в `xattr` все основные файлы и каталоги в корневой ФС. Рекомендуется подписывать только каталоги, содержащие неизменяемые (между обновлениями) файлы, а также файлы, содержимое которых изменяет только сам пользователь.
Примерный список каталогов для подписи:

```
i /bin  
/lib  
/lib32  
/lib64  
/sbin  
/usr  
Избранные файлы и каталоги из /etc  
Избранные файлы и каталоги из /boot (например, конфиг grub)  
Избранные файлы и каталоги из /home/<user>  
Избранные файлы и каталоги из /opt  
и т.д.
```

для включения механизмов контроля подписи в исполняемых файлах (ELF-файлах) и в xattr всех файлов можно использовать графический инструмент fly-admin-smc,
или установить в файле /etc/digsig/digsig_initramfs.conf (подробности см. в соответствующем "Руководстве по КСЗ"):

i Для ОС СМ Смоленск 1.6 (см. [ПУК КСЗ п.16.1](#)):
DIGSIG_ELF_MODE=1
DIGSIG_XATTR_MODE=1
Для ОС СМ Смоленск 1.5 (см. [ПУК КСЗ п.13.5](#)):
DIGSIG_ENFORCE=1
DIGSIG_LOAD_KEYS=1
DIGSIG_USE_XATTR=1

после чего выполнить команду:

```
update-initramfs -u -k all
```

и перезагрузить ПК

i **Примечание:**
Включение ЗПС крайне рекомендуется сочетать с блокировкой интерпретаторов
Блокировку интерпретаторов крайне рекомендуется сочетать с включенным МКЦ

15. Включить гарантированное удаление файлов и папок
16. Включить, при наличии возможности, режим киоска для пользователя.
17. Киоск можно настроить с помощью графического инструмента командной строки fly-admin-kiosk ([ПУК КСЗ п.16.3.1](#)).
18. Включить, при наличии возможности, графический киоск Fly
Киоск можно настроить с помощью графического инструмента fly-admin-smc (см. [ПУК КСЗ п.16.3.3](#))
19. Включить, при наличии возможности, второй уровень контроля подписей в расширенных атрибутах (xattr).
(Это можно выполнить в программе fly-admin-smc). (см. [ПУК КСЗ п.16.1](#))
20. Установить мандатный контроль целостности (МКЦ > 0) на всех основных файлах и каталогах в корневой файловой системе.
(в Смоленск 1.6 и в Смоленск 1.5 на апдейтах позже [27-10-2017](#))
Для этого в графическом инструменте fly-admin-smc «Политика безопасности» -> «мандатный контроль целостности» -> «целостность файловой системы» -> установить «высокий 63», или в консоли set-fs-ilev.

i Установку МКЦ рекомендуется проводить после всех настроек безопасности, так как дальнейшее администрирование возможно только под высоким уровнем целостности, и после снятия МКЦ с файловой системы командой unset-fs-ilev

Установка МКЦ на 1.5 апдейт [27-10-2017](#): см. [Мандатный контроль целостности](#)

21. Работу с конфиденциальной информацией под "уровнями конфиденциальности" нужно проводить, используя защитное преобразование файлов (возможность встроена в Файловый менеджер fly-fm).
22. Работу с конфиденциальной информацией в сети необходимо производить, используя защитное преобразование пакетов с помощью создания доверенной VPN сети (средства встроены в ОС).
23. Работу с конфиденциальной информацией при обмене почтой необходимо производить, используя защитные GPG-преобразования писем с помощью плагина для Thunderbird Enigmail (средства встроены в ОС)
24. Установить "взломостойкие" пароли на все учетные записи в ОС

i **P.S.**
"взломостойкий" пароль это пароль

- Содержащий не менее 8 символов;
- Не содержащий в себе никаких осмысленных слов (ни в каких раскладках);
- Содержащий в себе буквы в различных регистрах, цифры и спецсимволы.

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

26. Настроить дисковые квоты в ОС
Для этого установить пакет `quota`, настроить `/etc/fstab`, и использовать `edquota` для установки квот.
27. Настроить ограничения ОС (так называемые ulimits).
Рекомендуемые настройки `/etc/security/limits.conf`:

```
i #размер дампа ядра
* hard core 0

#максимальный размер создаваемого файла
* hard fsize 50000000

#блокировка форк-бомбы(большого количества процессов)
* hard nproc 1000
```

28. Отключить все неиспользуемые сервисы (в т.ч. сетевые) которые запускаются при старте ОС:

```
i В ОС CH Смоленск 1.6 командой systemdgenie или
В ОС CH Смоленск 1.5 командами chkconfig и fly-admin-runlevel
```

29. Включить межсетевой экран ufw и настроить iptables в минимально необходимой конфигурации, необходимой для работы:
по умолчанию все запрещено, кроме необходимых исключений

```
i В ОС CH Смоленск 1.6 командами

• iptables
• ufw
• gufw

В ОС CH Смоленск 1.5 командами

• iptables
• ufw
```

30. Настроить параметры ядра в `/etc/sysctl.conf` (можно использовать графический инструмент `fly-admin-smc` или добавить соответствующие строки в файл `/etc/sysctl.conf`):

```
i fs.suid_dumpable=0
kernel.randomize_va_space=2
kernel.sysrq=0
net.ipv4.ip_forward=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```


после внесения изменений перезагрузить компьютер, и убедиться, что все параметры сохранены правильно.
Сделать проверку можно командой:

```
sudo sysctl -a | more
```

31. При возможности, использовать защитное преобразование домашних каталогов пользователей с помощью допустимых средств, или использовать хранение информации на сетевых дисках или на защищенных от несанкционированного доступа сменных носителях.
32. По возможности, запретить пользователям подключение сменных носителей, к которым может быть осуществлён любой несанкционированный доступ:
В **Смоленск 1.6** такой доступ запрещен по умолчанию.
В **Смоленск 1.5** см. информацию по обновлению безопасности [БЮЛЛЕТЕНЬ № 27082018SE15](#)
33. Настроить систему аудита на сохранение логов на удаленной машине.
Если возможно, использовать систему централизованного протоколирования.
см. [РУК АДМИН п.15](#)
34. 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:

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

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

 Defaults timestamp_timeout=0