Astra Linux CE (ОС ОН) Орёл 2.12 Red-Book

Настройка безопасной конфигурации компьютера для работы с ОС Astra Linux CE 2.12

Перед установкой ОС

1. При возможности - установить и настроить на компьютере аппаратно-программный модуль доверенной загрузки (АПМДЗ)

2. 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.

3. Отключить в BIOS-е Intel SGX (в связи с обнаруженной уязвимостью в механизме).

4. 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, пломбировочные ленты, для усложнения скрытной установки "имплантов" рекомендуется использование ПК в форм-факторе ноутбук или моноблок.

5. Исключить использование беспроводных периферийных устройств вода (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.

6. При наличии опций для процессоров Intel Execute Disable Bit (XD-Bit) и для процессоров AMD No Execute Bit (NX-Bit) включить их.

7. 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.

8. Для Intel платформ необходимо устранить уязвимости Intel-SA-00086 в Intel Management Engine (если он инегрирован 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

9. Установить ОС (обязательно с 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

Раздел	Рекомендации по установке/настройке
/	С защитным преобразованием (при условии, что /boot размещен в отдельном дисковом разделе). Рекомендуется использовать файловую систему ext4.
/boot	Без защитного преобразования. Допускается использовать файловую систему ext2, 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.

При выборе размера дисковых разделов следует помнить, что при размере раздела /tmp менее 250МБ весьма вероятно возникновение ошибок при работе с графикой или с большими объёмами данных.

2. Разделы */home /tmp /var/tmp* рекомендуется монтировать с опциями `noexec,nodev,nosuid`
3. В разделе "Дополнительные настройки ОС" включить:
    a. Использовать по умолчанию ядро Hardened;
    b. Включить блокировку консоли;
    c. Включить блокировку интерпретаторов;
    d. Включить межсетевой экран ufw;
    e. Включить системные ограничения ulimits;
    f. Отключить возможность трассировки ptrace;
    g. Запретить установку бита исполнения;
    h. Включить использование sudo с паролем;

После установки ОС

1. Установить единственным устройством для загрузки ОС жесткий диск, на который была произведена установка ОС
2. Установить "взломостойкий" пароль на загрузчик Grub. При использовании архитектур, отличных от Intel, установить пароль на загрузчик согласно документации.
3. Использовать загрузку ядра HARDENED, и убрать из меню все другие варианты загрузки, включая режимы восстановления.
4. Удалить модули ядра, ответственные за работу с Intel Management Engine (MEI). Инструкция по ссылке.
5. Установить все доступные обновления безопасности ОС Astra Linux:

    для ОС ОН Орёл обновления доступны по мере их выхода: https://download.astralinux.ru/astra/current/orel/repository/

    После установки ОС сразу настроена на работу с репозиторием, и при наличии доступа в интернет, обновление можно выполнить командами:

    sudo apt update && sudo apt upgrade

6. Настроить монтирование раздела */boot* с опциями `ro` (перед обновлением ядра перемонтировать в `rw`).
7. 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
8. Отключить доступ к консоли пользователям, если он не был отключен при установке ОС:

    Создать файл /etc/rc.local со следующим содержимым:

    ```
    #!/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.

9. Включить блокировку интерпретаторов, если она не была включена при установке ОС
10. По возможности, включить блокировку макросов с помощью инструмента командной строки astra-macros-lock:

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

11. Включить блокировку трассировки ptrace, если она не была включена при установке ОС
12. Включить гарантированное удаление файлов и папок
13. Включить, при наличии возможности, режим киоска для пользователя.
14. Работу с конфиденциальной информацией нужно проводить, используя защитное преобразование файлов.
15. Работу с конфиденциальной информацией в сети необходимо производить, используя защитное преобразование пакетов с помощью создания доверенной VPN сети
(средства встроены в ОС).
16. Работу с конфиденциальной информацией при обмене почтой необходимо производить, используя защитные GPG-преобразования писем с помощью плагина для Thunderbird Enigmail
(средства встроены в ОС)
17. Установить "взломостойкие" пароли на все учетные записи в ОС

> **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.

18. Убедиться, что `pam_tally` настроен на блокировку учетных записей при попытках подбора паролей (настроено по умолчанию при установке ОС).
19. Настроить дисковые квоты в ОС
Для этого установить пакет `quota`, настроить */etc/fstab*, и использовать `edquota` для установки квот.
20. Включить ограничения ОС (так называемые ulimits), если они не были включены при установке ОС.
Настроить ограничения ОС.
Рекомендуемые настройки */etc/security/limits.conf*:

> #размер дампа ядра
> * hard core 0
>
> #максимальный размер создаваемого файла
> * hard fsize 50000000
>
> #блокировка форк-бомбы(большого количества процессов)
> * hard nproc 1000

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

```
systemdgenie
```

22. Включить межсетевой экран ufw, если он не был включен при установке ОС.
Настроить iptables в минимально необходимой конфигурации, необходимой для работы: по умолчанию все запрещено, кроме необходимых исключений

- `iptables`

- ufw
- gufw

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

> 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
```

24. Заблокировать исполнение модулей python с расширенным функционалом:

```
find /usr/lib/python* -type f -name "_ctype*" -exec sudo dpkg-
statoverride --update --add root root 640 {} \;
```

25. 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.

26. По возможности, запретить пользователям подключение сменных носителей, к которым может быть осуществлён любой несанкционированный доступ.

27. Настроить систему аудита на сохранение логов на удаленной машине.
Если возможно, использовать систему централизованного протоколирования.

28. Установить и настроить службу fail2ban.

29. Включить запрос пароля при каждом выполнении команды sudo, для чего внести следующие изменения в файл /etc/sudoers:
    a. Для того, чтобы для выполнения первой команды sudo требовалось ввести пароль:
    удалить "NOPASSWD:" из строки:

    > %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