**Разграничение доступа к подключаемым устройствам**

В Astra Linux доступ к подключаемым устройствам может быть разграничен путем настройки правил udev, использования polkit и ACL (Access Control Lists).

1. **Udev**Правила udev могут быть использованы для разграничения доступа к устройствам путем применения правил в соответствии с различными характеристиками устройства, такими как идентификатор производителя, модель устройства и т.д.

Например:

- Создать группу пользователей, которым разрешено использовать определенное устройство:

# Создать новую группу

sudo groupadd mygroup

# Добавить пользователя в группу

sudo usermod -a -G mygroup myusername

# Создать правило udev для разрешения доступа к определенному устройству

sudo nano /etc/udev/rules.d/20-mydevice.rules

# Добавить следующее правило в файл

SUBSYSTEM=="usb", ATTR{idVendor}=="1234", ATTR{idProduct}=="5678", GROUP="mygroup", MODE="0660"

# Перезапустить udev

sudo udevadm control –reload

1. **Polkit**  
   Polkit может быть использован для установки правил авторизации для конкретных задач в системе.

Например:

- Создайте правило polkit, чтобы разрешить использование определенного устройства

# Создать файл /etc/polkit-1/localauthority/50-local.d/10-mydevice.pkla

sudo nano /etc/polkit-1/localauthority/50-local.d/10-mydevice.pkla

# Вставить следующее содержимое в файл

[Allow group mygroup to access mydevice]

Identity=unix-group:mygroup

Action=org.freedesktop.devicekit.disks.filesystem-mount;org.freedesktop.devicekit.disks.filesystem-unmount-others;

ResultAny=yes

**ACL**  
ACL является дополнительным уровнем разграничения доступа для файловых систем, который позволяет управлять доступом к файлам и каталогам для определенных пользователей и групп. Например:

- Монтирование файловой системы с ACL:

# Установить пакет acl (если он не установлен)

sudo apt-get install acl

# Изменить fstab для файловой системы с опцией acl

/dev/sda1 /mnt/data ext4 defaults,acl 0 2

# Перезагрузить систему или выполнить команду

sudo mount -a

- Установка ACL на файл или каталог:

# Установить права ACL для конкретного файла (-m для добавления прав)

setfacl -m u:username:rw /path/to/file

# Установить права ACL для всех файлов в каталоге (-d для установки на директорию)

setfacl -R -m u:username:rw /path/to/directory

# Просмотр прав ACL для файла или каталога

getfacl /path/to/file\_or\_directory