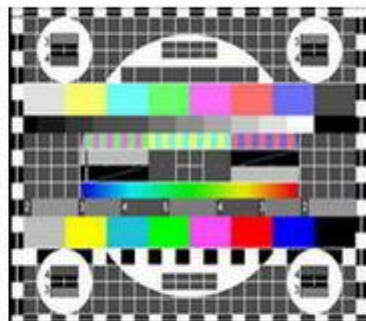


‘C

☞ 4 = Ц

4



”



‘

Е

3

”””



”



“



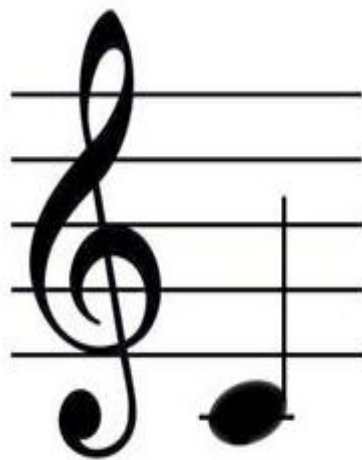
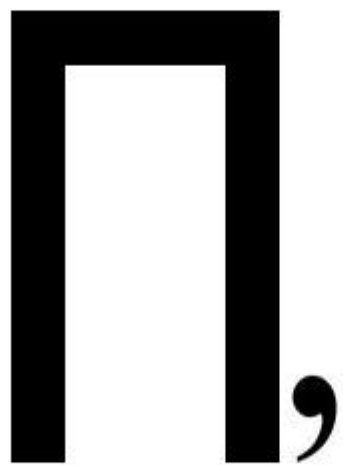
”

ЦЕЯ



”





 4 = П

Как многопользовательская операционная система, ОС Linux содержит механизм **разграничения доступа к данным**, позволяющий как **защитить данные** одного пользователя от нежелательного вмешательства других, так и **разрешить другим доступ** к этим данным для совместной работы.



Манипулирует файлами **не сам пользователь, а запущенный им процесс.**

Поскольку и файл, и процесс создаются и управляются системой, ей нетрудно организовать какую угодно политику доступа одних к другим, основываясь на любых свойствах процессов как субъектов и файлов как объектов системы



При создании объектов файловой системы — файлов, каталогов и т. П., каждому в обязательном порядке приписывается UID — **идентификатор пользователя-владельца файла**, GID — **идентификатор группы**, которой принадлежит файл, тип объекта и набор т. н. **атрибутов**, а также некоторую дополнительную информацию. **Атрибуты** определяют, кто и что с файлом имеет право делать

Утилита id выводит входное имя пользователя и соответствующий ему UID, а также группу по умолчанию и полный список групп, членом которых он является.



Представление прав доступа

Основные атрибуты прав доступа можно представить в виде двенадцати битов двоичного числа, **равных 1, если атрибут установлен, и 0, если нет.**

Порядок битов в числе следующий:

sU|sG|t|rU|wU|xU|rG|wG||xG|rO|wO|xO,

где

- **sU** — это SetUID,
- **sG** — это SetGID,
- **t** — это t-атрибут (sticky-бит),

Атрибуты доступа

- **rU|wU|xU** - права чтения (Read), записи (Write) и выполнения (eXecute) для владельца файла (User);
- **rG|wG|xG** - права чтения (Read), записи (Write) и выполнения (eXecute) для группы файла (Group);
- **rO|wO|xO** - права чтения (Read), записи (Write) и выполнения (eXecute) для всех остальных (Other).

Процессы с установленным битом **sU** выполняются с правами владельца. А с установленным битом **sG** – с правами группы.

В каталоге с установленным **sticky-битом** удалять файлы может только владелец или root. При том устанавливать этот бит может только root, а сбрасывать может владелец и root.

- «-rw-rw-rw-» (Первая черточка - обычный файл, и 9 прав доступа - все могут читать и изменять)
- «drwx-----» (Катал полный доступ (чтение, изменение, выполнение) имеет только владелец файла)
- «-rw-r-----» (Обычный файл, владелец может читать и изменять, группа - читать, остальные - не имеют прав)

- «**drwxr-xr--**» (Каталог, владелец имеет полный доступ, группа - чтение и выполнение, остальные - только чтение)
- «**drwxrwxrwt**» (Каталог, все имеют полный доступ, однако, установлен **sticky**-бит, поэтому права записи в каталог для членов группы и для посторонних ограничены их собственными файлами, и только владелец имеет право изменять список файлов в каталоге, как ему вздумается.)

- **«-rws--x--x»** (Обычный файл, установлен атрибут SetUID. Как и в случае с t-атрибутом, ls выводит букву «s» вместо буквы «x» в тройке «для владельца». Точно так же, если соответствующего x-атрибута нет (что бывает редко), ls выведет «S» вместо «s».)
- **«-rwx--s--x»** (Обычный файл, установлен атрибут SetGID. Утилита ls выводит SetGID в виде «s» вместо «x» во второй тройке атрибутов («для группы»). Замечания касательно «s», «S» и «x» действительно для SetGID так же, как и для SetUID.) права доступа представляются также в двоичном и восьмеричном виде.

Особенности доступа к каталогам

- Если **каталог можно читать (r)**, то это означает, что разрешено только узнать список файлов, содержащихся в этом каталоге. Только список файлов, но не их свойства (размер, права доступа и др.).
- Если **каталог можно исполнять (x)**, то это означает, что в него можно заходить и просматривать содержимое файлов (доступ к которым разрешен для данной категории), узнавать свойства (атрибуты) файлов. Можно изменить содержимое файла (если его разрешено менять), но не имя файла.
- Если **каталог можно изменять (w)**, то это означает, что в нем можно изменять файлы, их имена, удалять их.

Изменение прав доступа

- Изменение прав доступа к указанному файлу (или каталогу) выполняется с помощью команды **chmod** . При создании каталога также можно сразу указать права доступа к нему с помощью команды **mkdir -m** .
- Изменение владельца и группы файлов выполняется с помощью команды **chown** .

- Группу также можно назначить командой **chgrp**.
- Тем же побитовым представлением атрибутов регулируются и права доступа по умолчанию при создании файлов и каталогов.
- Делается это с помощью команды **umask**. Единственный параметр **umask** — восьмеричное число, задающее атрибуты, которые не надо устанавливать новому файлу или каталогу.

- Так, **umask** 0 приведёт к тому, что файлы будут создаваться с атрибутами «**rw-rw-rw-**», а каталоги — «**rwxrwxrwx**».
- Команда **umask 022** убирает из атрибутов по умолчанию права доступа на запись для всех, кроме хозяина (получается «**rw-r--r--**» и «**rwxr-xr-x**» соответственно), а с **umask 077** новые файлы и каталоги становятся для них полностью недоступны («**rw-----**» и «**rwx-----**»).




 1 = Ц



 + Т



 4 = И

Т
Б

