**104.5 Права доступа и владельцы файлов.**

Студент должен уметь управлять доступом к объектам файловой системы, опираясь на механизмы разрешений и владельцев.

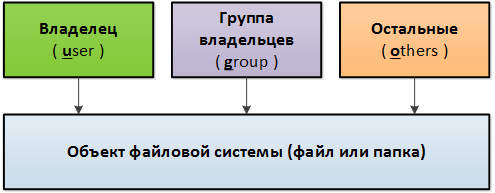
**Изучаем**:

* управление доступом к файлам и папкам;
* использование специальных битов;
* способы работы с масками создания файлов;
* работы с разрешением доступа для групп.

**Термины и утилиты:**

* chmod
* umask
* chown
* chgrp

В классической линуксовой файловой системе можно задавать права доступа на основе трех принадлежностей: владелец объекта, группа владельцев, все остальные.



*Рисунок 1. Владельцы объектов*

Посмотреть текущие права доступа, равно как и владельце можно при помощи команды **stat**, например:

***stat file.txt***

Изменить владельца объекта можно при помощи команды **chown**, например:

***chown root file.txt*** (сделать суперпользователя владельцем файла file.txt);

Изменить группу владельцев объекта можно при помощи команды **chgrp**, например:

***chgrp users file.txt*** (сделать группу users группой владельцев файла file.txt);

Команда chgrp редко используется, так как возможны следующие варианты использования команды chown:

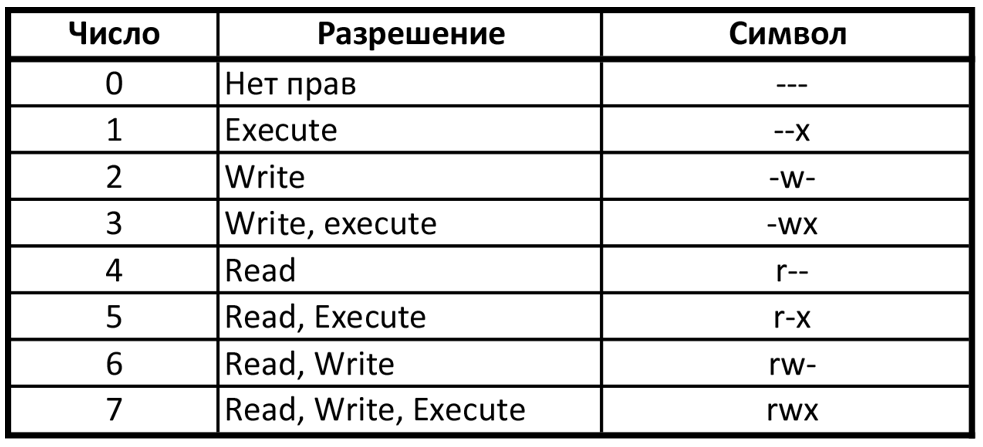
***chown :users file.txt*** (сделать группу users группой владельцев файла file.txt);

***chown root:users file.txt*** (сделать суперпользователя владельцем файла file.txt и группу users группой владельцев файла file.txt);

\_\_\_

Для установки разрешений на доступ к объекту файловой системы Linux использует комбинации трех стандартных прав: чтение, запись и выполнение.

Права можно устанавливать, как указывая буквенные комбинации (r- read, w – write и x - execute), так и числовые (4 – read, 2 – write, 1 - execute), значения которых суммируются.



*Рисунок 2. Права доступа к объектам*

Права доступа назначаются отдельно для владельца, группы владельцев и остальных.



*Рисунок 3. Права доступа к объектам*

Для установки прав доступ используется команда chmod, например:

***chmod 750 script*** (полные права владельцу, чтение и выполнение группе, ничего остальным);

***chmod u+w script*** (дать право записи владельцу);

***chmod ugo-x script*** (отобрать у всех право выполнения файла);

Просмотр прав доступа при помощи команды **stat** или полного вывода информации о содержимом текущего каталога **ls –l** показывает права доступа в буквенном виде, например:

***rwxrw-r-- script*** (полные права владельцу, чтение и запись группе, чтение остальным);

Право выполнения, установленное на каталог говорит о возможности заходить в эту папку указанному пользователю или группе.

\_\_\_

При работе с объектами файловой системы можно указывать маски создания файлов и папок, т.е. разрешения доступа по умолчанию для вновь создаваемых объектов.

Текущую маску можно посмотреть выполнив команду **umask** (в Ubuntu по умолчанию 022):

**umask** (отобразить числовое значение маски);

***umask –s*** (отобразить символное значение маски).

Umask рассчитывается в восьмеричной системе счисления, и показывает какие биты следует сбросить в создаваемом объекте (побитовое И между побитовым НЕ маски и полным доступом). Напомни что полный доступ на директории – 777, а на файлы – 666. Что все это значит (<https://ru.wikipedia.org/wiki/Umask> ):

Максимальные права установленные на директорию могут быть равны: 111 111 111

Маска 022 в восмеричной системе счисления выглядит как: 000 010 010

Ее побитовое НЕ (маски) выглядит как: 111 101 101

Располагаем их в столбик и выполняем операцию И:

111 111 111

111 101 101

-----------------

111 101 101 или в двоичной системе счисления 755 (rwx r-x r-x)

Установить маску можно также командой **umask**, например:

***umask 072*** (полный доступ владельцу, нет доступа группе владельцев, чтение всем остальным).

\_\_\_

Помимо группировки стандартных прав доступа (чтение, запись, выполнение), в Linux присутствуют специальные биты, устанавливающие дополнительные права доступа.

Доступны для использования следующие виды битов:

* **suid** - бит запуска от имени владельца;
* **sgid** - бит запуска от имени группы владельцев;
* **sticky**  - бит защиты содержимого.

SUID (значение s или 4) применяется для запуска файла от имени владельца файла. Его можно установить командами:

***chmod u+s script***

***chmod 4755 script***

SGID (значение s или 2) применяется для доступа к файлам и папкам от имени группы владельцев, его можно установить командами:

***chmod g+s script***

***chmod 2755 script***

sticky-bit (значение t или 1) применяется для возможности изменения структуры каталогов только владельцем папки, его можно установить командами:

***chmod o+t folder***

***chmod 1755 folder***

Эти биты можно устанавливать одновременно, например:

***chmod ug+s script***

***chmod 3755 folder***