



Linux

Урок 3

# Права и пользователи в GNU/Linux

Пользователи, группы, файлы.

Права доступа.

Суперпользователь

# Вопросы по домашней работе



# План урока

1. Пользователи и группы
2. Права файлов
3. Работа с файлами
4. Суперпользователь

К концу урока мы научимся понимать и уверенно управлять правами доступа в Linux, а также выполнять простейшие операции с файлами и дисками





## Зачем вообще разграничивать доступ?

`rm` — удалить файлы

`-r` — рекурсивно

`-f` — форсировать (и не  
спрашивать подтверждений)

`/` — начиная от корня



# Виды разграничения прав

- DAC (Discretionary Access Control) — дискреционное или избирательное право управление доступом
  - ACL (Access Control List) — список контроля доступа
- MAC (Mandatory Access Control) — мандатное управление доступом (принудительный контроль доступа)



# Виды разграничения прав

- DAC (Discretionary Access Control) — изначально присутствует в UNIX/Linux
- MAC (Mandatory Access Control)
  - SELinux
  - AppArmor
  - ❤️ военные и ФСТЭК

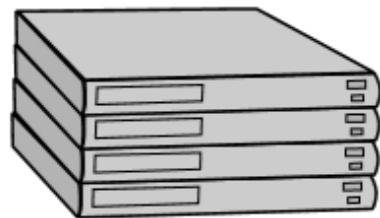




Внешний  
осмотр

Подключение  
оборудования

Изъятие  
оборудования



Субъект  
(действительный)

Субъект  
(номинальный)

Вид доступа

Объект



Инженеру необходимо обеспечить доступ в ЦОД (карта доступа) для осмотра индикаторов серверов, подключения дополнительного оборудования и изъятия из стойки



Процесс  
пользователя



eUID:eGID

Read (r)  
Write (w)  
eXecute (x)



Владелец  
файла:  
UID:GID

Права доступа для:

владельца файла: rwx

группы владельца: r-x

остальных: - - -

Субъект  
(действительный)

Субъект  
(номинальный)

Вид доступа

Объект



Процессу необходимо обеспечить доступ к файлам (идентификатор пользователя и группы), для допустимых правами данного файла действий для данного пользователя или его группы: чтение, запись, выполнение



# Какие пользователи бывают?





## Обычные пользователи

UID (User Identifier) для них  
обычно назначается,  
начиная с 1000



Суперпользователь

его зовут root



и его UID всегда 0







## Демоны

Служебные пользователи или псевдопользователи от лица которых работают, как ни странно демоны — так называются служебные программы и сервера, работающие в фоновом режиме.

UID (User Identifier) для них обычно назначаются в диапазоне от 1 до 999

```
user@vlamp:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:4:sync:/bin:/bin/sync
.....
user:x:1001:1001:user 1:/home/user:/bin/bash
petrov:x:1002:1002:Petrov Petr:/home/user:/bin/bash
```

## /etc/passwd

Хранит данные о пользователях  
и их паролях

(данные о паролях уже не хранит,  
ибо открыт на чтение всем)



# А где же хранятся пароли?

- Если не в `/etc/passwd`?



# А где же хранятся пароли?

- ~~В /etc/passwd~~
- В /etc/shadow в зашифрованном виде. Доступ к /etc/shadow только у root (на запись) и группы shadow (на чтение)



# Что еще содержит /etc/shadow?

- Данные о своем пароле (сроках действия) можно посмотреть с помощью `chage` (буквы `n` в этом слове нет)





# chage

```
user@v1amp:~$ chage -l user
Последний раз пароль был изменён           : апр. 22, 2014
Срок действия пароля истекает                : никогда
Пароль будет деактивирован через             : никогда
Срок действия учётной записи истекает        : никогда
Минимальное количество дней между сменой пароля : 0
Максимальное количество дней между сменой пароля : 99999
Количество дней с предупреждением перед деактивацией пароля : 7
```



# Управление пользователями и группами

- Как создать или удалить пользователя?
- Как создать, удалить группу?
- Как изменить параметры пользователя или группы
- Как заблокировать пользователя?



# Управление пользователями и группами

- Как узнать в каких ты сейчас группах?
- Как изменить GID? Нужно ли выполнить `exit` после этого?



## Пример атрибутов файла

Команда выводит подробную информацию о файле



Проверка прав доступа при доступе к файлу выполняется слева направо до первого совпадения !



# Изменение владельца и группы

- `chown [опции] owner[:group] file ...`
  - `chown -R developer:www-data /var/www`
- `chgrp [опции] group file ...`



# Изменение прав файла: chmod

- символьная форма
  - `chmod [опции] [ugoa][=--+][rwx] file ...`
    - u-user, g-group, o-other, a-all
- числовая форма
  - `chmod [опции] OCTAL-MODE file ...`



# chmod (цифровой формат)

двоичный	восьмеричный	символьный	файл	каталог
000	0	- - -	нет	нет
001	1	- - x	выполнение	сделать текущим
010	2	- w -	запись	нет
011	3	- w x	запись + выполнение	все кроме чтения списка файлов
100	4	r - -	чтение	чтение имен файлов
101	5	r - x	чтение + выполнение	доступ на чтение
110	6	r w -	чтение и запись	чтение имен файлов
111	7	r w x	все права	все права



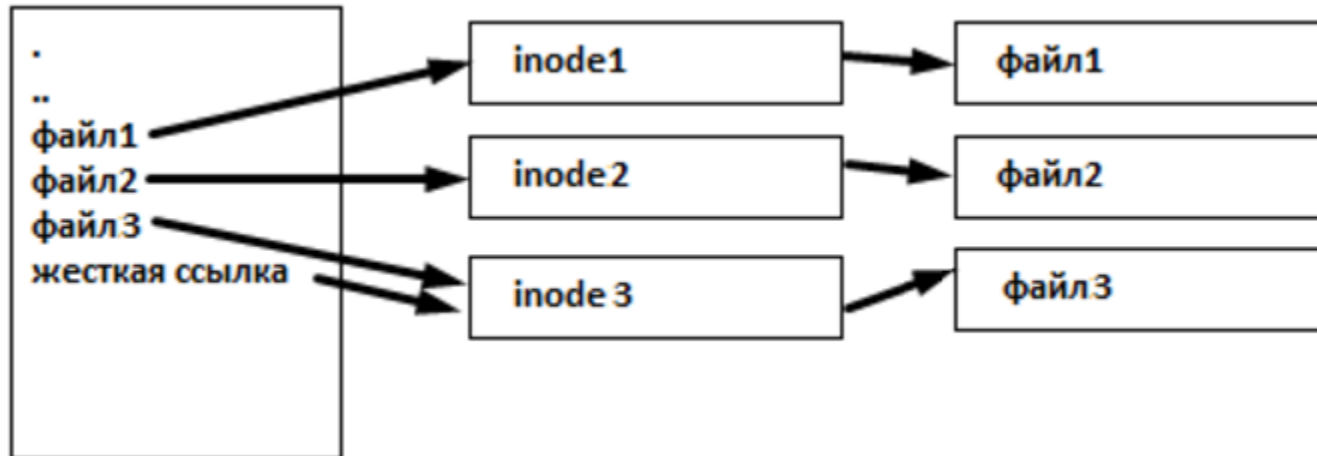
# Атрибут x для директорий

- возможность перейти в директорию
- возможность доступа (чтение, модификация) к айнодам





# Атрибут x для директорий



# Особые права

- SUID (u+s)
- SGID (g+s)
- sticky bit (+t)



# В числовой форме

- `chmod AUGO file`
  - $A = 1 \text{ (sticky)} + 2 \text{ (SGID)} + 4 \text{ (SUID)}$



# Права по умолчанию

- 644 — для файлов
- 755 — для директорий
- Как задать одновременно?



# Права по умолчанию

- `umask UGO`
- для файлов: `666-UGO`
- для директории: `777- UGO`



# Права по умолчанию

- По умолчанию
  - `umask 022`
- Когда удобно
  - `umask 002?`



# Работа с файлами (практика)

- Перемещение и просмотр каталогов
- Просмотр файлов
- Редактирование



# Работа с файлами (практика)

- Копирование
- Перемещение и переименование
- Символические и жесткие ссылки





Вопросы участников ...

