

# Дискреционное разграничение прав в Linux. Основные атрибуты

---

Мансур Абдулфазов<sup>1</sup>

11 сентября, 2024, Москва, Россия

<sup>1</sup>Российский Университет Дружбы Народов

# Цели и задачи работы

---

## Цель лабораторной работы

Получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

# **Процесс выполнения лабораторной работы**

---

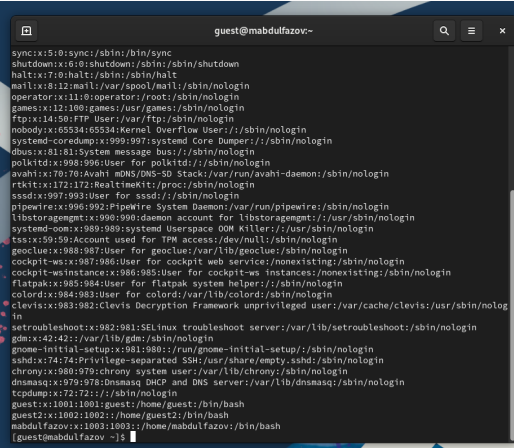
# Определяем UID и группу



```
guest@mabdufzov:~  
[mabdufzov@mabdufzov ~]$ su guest  
Пароль:  
[guest@mabdufzov mabdufzov]$ pwd  
/home/mabdufzov  
[guest@mabdufzov mabdufzov]$ cd  
[guest@mabdufzov ~]$ pwd  
/home/guest  
[guest@mabdufzov ~]$ whoami  
guest  
[guest@mabdufzov ~]$ id guest  
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel)  
[guest@mabdufzov ~]$ groups guest  
guest : guest wheel  
[guest@mabdufzov ~]$
```

**Figure 1:** Информация о пользователе guest

# Файл с данными о пользователях

A terminal window with a dark background and light text. The title bar shows 'guest@mabdufazzov:~'. The terminal displays the output of a command that lists the contents of the /etc/passwd file. Each line represents a system or user account, showing the username, UID, GID, and the path to the user's shell or a description. The list includes various system users like sync, shutdown, halt, mail, operator, games, ftp, nobody, systemd-coredump, dbus, polkitd, avahi, rtkit, sssd, pipewire, libstoragemgmt, systemd-oom, tss, geoclue, cockpit-ws, flatpak, colord, clevis, setroubleshoot, and gdm, followed by regular users guest, guest2, mabdufazzov, and mabdufazzov. The prompt at the bottom is [guest@mabdufazzov ~]\$.

```
guest@mabdufazzov:~  
sync:x:510:sync:/sbin:/bin/sync  
shutdown:x:610:shutdown:/sbin:/sbin/shutdown  
halt:x:710:halt:/sbin:/sbin/halt  
mail:x:812:mail:/var/spool/mail:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin  
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin  
dbus:x:81:81:System message bus:/sbin/nologin  
polkitd:x:998:996:User for polkitd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
sssd:x:997:993:User for sssd:/sbin/nologin  
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin  
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin  
systemd-oom:x:989:989:systemd Userspace OOM Killer:/usr/sbin/nologin  
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin  
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin  
cockpit-ws:x:987:986:User for cockpit web service:/nonexisting:/sbin/nologin  
cockpit-wsinstance:x:986:985:User for cockpit-ws instances:/nonexisting:/sbin/nologin  
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin  
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin  
clevis:x:983:982:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:981:980:/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin  
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
tcpdump:x:72:72:/sbin/tcpdump  
guest:x:1001:1001:guest:/home/guest:/bin/bash  
guest2:x:1002:1002:/home/guest2:/bin/bash  
mabdufazzov:x:1003:1003:/home/mabdufazzov:/bin/bash  
[guest@mabdufazzov ~]$
```

Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
10
[guest@mabdufzov ~]$
[guest@mabdufzov ~]$ ls -l /home
итого 8
drwx-----, 14 guest      guest      4096 сен 11 10:12 guest
drwx-----,  3 guest2     guest2     78 сен 17 2023 guest2
drwx-----, 14 mabdufzov  mabdufzov 4096 сен 11 10:10 mabdufzov
[guest@mabdufzov ~]$
```

Figure 3: Расширенные атрибуты

# Атрибуты директории

```
[guest@mabdufzov ~]$  
[guest@mabdufzov ~]$ cd  
[guest@mabdufzov ~]$ mkdir dir1  
[guest@mabdufzov ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 guest guest 6 сен 11 10:18 dir1  
[guest@mabdufzov ~]$ chmod 000 dir1  
[guest@mabdufzov ~]$ ls -l | grep dir1  
d----- . 2 guest guest 6 сен 11 10:18 dir1  
[guest@mabdufzov ~]$ echo test > dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest@mabdufzov ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[guest@mabdufzov ~]$
```

Figure 4: Снятие атрибутов с директории



# Права и разрешённые действия

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

**Figure 5:** Минимальные права для совершения операций

## **Выводы по проделанной работе**

---

В ходе выполнения лабораторной работы были получены навыки работы с атрибутами файлов и сведения о разграничении доступа.