

# Дискреционное разграничение прав в Linux. Основные атрибуты

---

Завен Карапетян<sup>1</sup>

8 сентября, 2024, Москва, Россия

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

# Цели и задачи работы

---

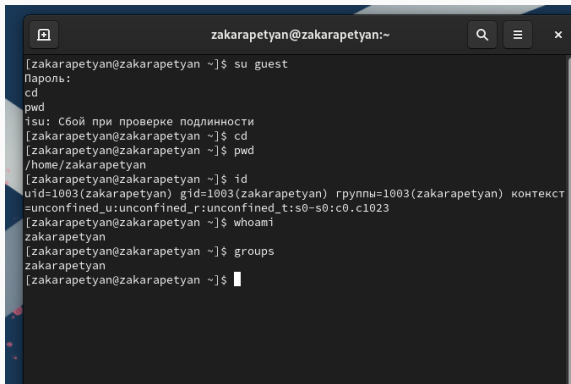
## Цель лабораторной работы

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**

---

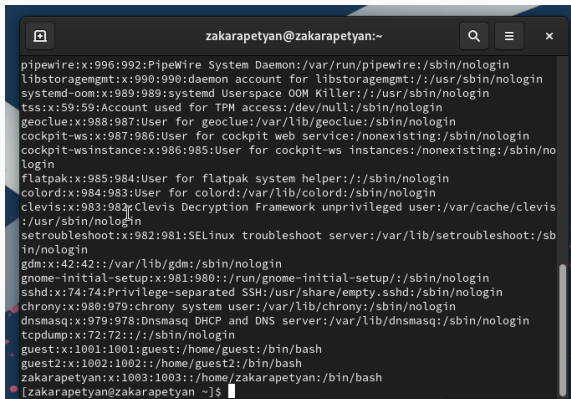
# Определяем UID и группу



```
zakarapetyan@zakarapetyan:~  
[zakarapetyan@zakarapetyan ~]$ su guest  
Пароль:  
cd  
pwd  
isu: Сбой при проверке подлинности  
[zakarapetyan@zakarapetyan ~]$ cd  
[zakarapetyan@zakarapetyan ~]$ pwd  
/home/zakarapetyan  
[zakarapetyan@zakarapetyan ~]$ id  
uid=1003(zakarapetyan) gid=1003(zakarapetyan) группы=1003(zakarapetyan) контекст  
=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[zakarapetyan@zakarapetyan ~]$ whoami  
zakarapetyan  
[zakarapetyan@zakarapetyan ~]$ groups  
zakarapetyan  
[zakarapetyan@zakarapetyan ~]$
```

**Figure 1:** Информация о пользователе guest

# Файл с данными о пользователях

A terminal window titled 'zakarapetyan@zakarapetyan:~' displays the output of the 'cat /etc/passwd' command. The window has a dark background with a light blue border. The output lists system and regular users with their IDs, names, and shell paths.

```
zakarapetyan@zakarapetyan:~  
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:/usr/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:GDM User:/var/lib/gdm:/sbin/nologin  
gnome-initial-setup:x:981:980:GNOME Initial Setup:/usr/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/nologin  
guest:x:1001:1001:guest:/home/guest:/bin/bash  
guest2:x:1002:1002:guest2:/home/guest2:/bin/bash  
zakarapetyan:x:1003:1003:zakarapetyan:/home/zakarapetyan:/bin/bash  
[zakarapetyan@zakarapetyan ~]$
```

Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
[zakarapetyan@zakarapetyan ~]$  
[zakarapetyan@zakarapetyan ~]$  
[zakarapetyan@zakarapetyan ~]$ ls -l /home  
итого 8  
drwx-----. 14 guest      guest      4096 сен 10  2023 guest  
drwx-----.  3 guest2     guest2     78 сен 17  2023 guest2  
drwx-----. 14 zakarapetyan zakarapetyan 4096 сен  8 10:04 zakarapetyan  
[zakarapetyan@zakarapetyan ~]$
```

Figure 3: Расширенные атрибуты

# Атрибуты директории

```
[zakarapetyan@zakarapetyan ~]$  
[zakarapetyan@zakarapetyan ~]$ cd  
[zakarapetyan@zakarapetyan ~]$ mkdir dir1  
[zakarapetyan@zakarapetyan ~]$ ls -l | grep dir1  
drwxr-xr-x. 2 zakarapetyan zakarapetyan 6 сен 8 10:06 dir1  
[zakarapetyan@zakarapetyan ~]$ chmod 000 dir1/  
[zakarapetyan@zakarapetyan ~]$ ls -l | grep dir1  
d-----, 2 zakarapetyan zakarapetyan 6 сен 8 10:06 dir1  
[zakarapetyan@zakarapetyan ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[zakarapetyan@zakarapetyan ~]$ cd dir1/  
bash: cd: dir1/: Отказано в доступе  
[zakarapetyan@zakarapetyan ~]$
```

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.