

# **Дискреционное разграничение прав в Linux. Основные атрибуты**

---

Данил Исаев<sup>1</sup>

11 сентября, 2024, Москва, Россия

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

## Цели и задачи работы

---

## Цель лабораторной работы

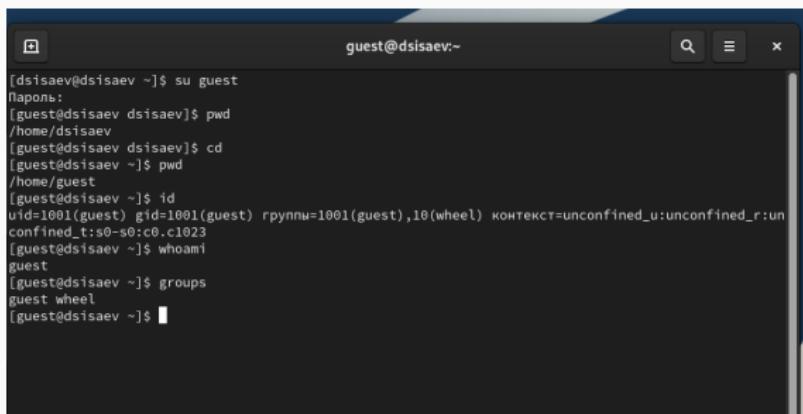
---

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

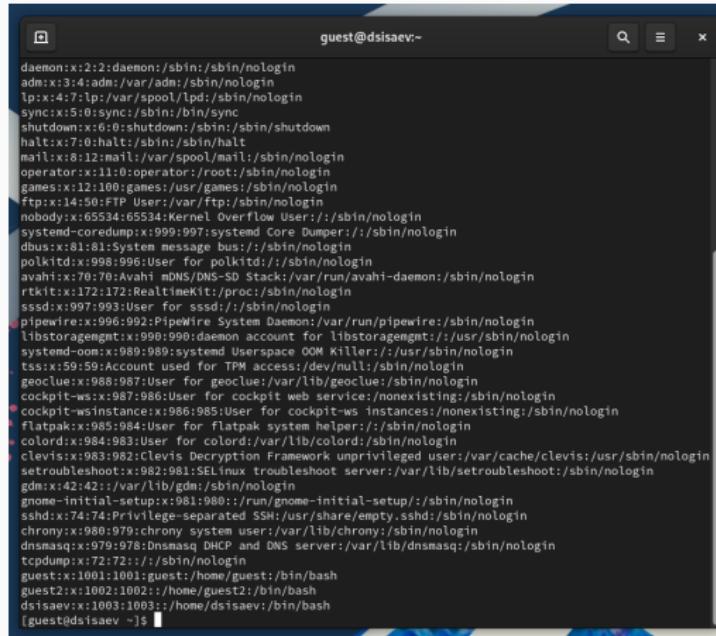


The screenshot shows a terminal window titled "guest@dsisaev:~". The terminal displays the following command-line session:

```
[dsisaev@dsisaev ~]$ su guest
Password:
[guest@dsisaev dsisaev]$ pwd
/home/dsisaev
[guest@dsisaev dsisaev]$ cd
[guest@dsisaev ~]$ pwd
/home/guest
[guest@dsisaev ~]$ id
uid=1001(guest) gid=1001(guest) rprvnnw=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:un
confined_t:s0-s0:c0.c1023
[guest@dsisaev ~]$ whoami
guest
[guest@dsisaev ~]$ groups
guest wheel
[guest@dsisaev ~]$
```

**Figure 1:** Информация о пользователе guest

# Файл с данными о пользователях



The screenshot shows a terminal window with the title "guest@dsisaev:~". The window displays the contents of the /etc/passwd file. The file lists numerous users, each entry consisting of a login name, password hash, user ID, group ID, and a list of shell programs and environment variables. Some entries are marked with a red highlight, indicating specific users of interest.

```
daemon:x:2:2:daemon:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12: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:Avahi mDNS+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:system 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/nologin
guest:x:1001:1001:guest:/home/guest:/bin/bash
guest2:x:1002:1002::/home/guest2:/bin/bash
dsisaev:x:1003:1003::/home/dsisaev:/bin/bash
[guest@dsisaev ~] $
```

Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
[guest@dsisaev ~]$ ls -l /home
итого 8
drwx----- 14 dsisaev dsisaev 4096 сен 11 10:46 dsisaev
drwx----- 14 guest    guest    4096 сен 11 10:48 guest
drwx-----  3 guest2   guest2   78 сен 17  2023 guest2
[guest@dsisaev ~]$ █
```

Figure 3: Расширенные атрибуты

# Атрибуты директории

```
[guest@dsisaev ~]$ cd
[guest@dsisaev ~]$ nkdir dir1
bash: nkdir: command not found...
[guest@dsisaev ~]$ ls -l | grep dir1
[guest@dsisaev ~]$ mkdir dir1
[guest@dsisaev ~]$ ls -l | grep dir1
drwxr-xr-x. 2 guest guest 6 сен 11 10:53 dir1
[guest@dsisaev ~]$ chmod 000 dir1/
[guest@dsisaev ~]$ ls -l | grep dir1
d-----. 2 guest guest 6 сен 11 10:53 dir1
[guest@dsisaev ~]$ echo test > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@dsisaev ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@dsisaev ~]$ █
```

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**

---

## Вывод

---

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