

# Дискреционное разграничение прав в Linux. Основные атрибуты

---

Владислав Пузырёв<sup>1</sup>

13 сентября, 2023, Москва, Россия

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

# Цели и задачи работы

---

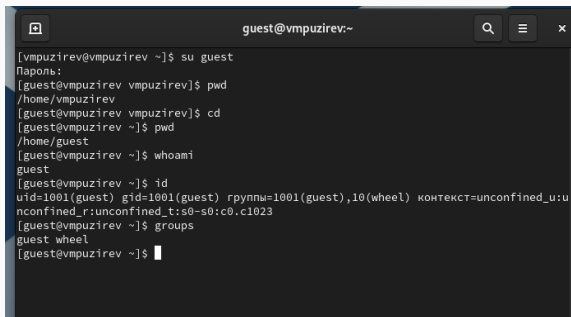
## Цель лабораторной работы

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

A terminal window titled 'guest@vmpuzirev:~' with search, menu, and close icons. It shows a sequence of commands to switch to the 'guest' user and view their details. The output of 'id' shows the user is 'guest' with UID 1001, GID 1001, and is part of the 'wheel' group. The output of 'groups' shows the user belongs to the 'wheel' group.

```
[vmpuzirev@vmpuzirev ~]$ su guest
Пароль:
[guest@vmpuzirev vmpuzirev]$ pwd
/home/vmpuzirev
[guest@vmpuzirev vmpuzirev]$ cd
[guest@vmpuzirev ~]$ pwd
/home/guest
[guest@vmpuzirev ~]$ whoami
guest
[guest@vmpuzirev ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vmpuzirev ~]$ groups
guest wheel
[guest@vmpuzirev ~]$
```

**Figure 1:** Информация о пользователе guest

## Файл с данными о пользователях

```

[guest@vmpuzirev ~]$
[guest@vmpuzirev ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:71: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:x:995:997:systemd Core Daemon:/sbin/nologin
dbus:x:81:81:system message bus:/sbin/nologin
polkitd:x:996:996>User for polkitd:/sbin/nologin
avahi:x:70:78: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/lib/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
ts: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:/nonexistent:/sbin/nologin
cockpit-winsatance:x:986:985>User for cockpit-ws instances:/nonexistent:/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
selinux-troubleshoot: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
ssh: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
vmpuzirev:x:1002:1002:/home/vmpuzirev:/bin/bash
[guest@vmpuzirev ~]$

```

### Figure 2: Содержимое файла /etc/passwd

# Доступ к домашним директориям

```
[guest@vmpuzirev ~]$  
[guest@vmpuzirev ~]$  
[guest@vmpuzirev ~]$ ls -l /home/  
итого 8  
drwx-----. 14 guest      guest      4096 сен 13 16:11 guest  
drwx-----. 14 vmpuzirev vmpuzirev 4096 сен 13 16:09 vmpuzirev  
[guest@vmpuzirev ~]$
```

**Figure 3:** Расширенные атрибуты

# Атрибуты директории

```
[guest@vmpuzirev ~]$ cd
[guest@vmpuzirev ~]$ mkdir dir1
[guest@vmpuzirev ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен 13 16:18 dir1
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Видео
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Документы
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Изображения
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Музыка
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 10 14:33 Шаблоны
[guest@vmpuzirev ~]$ chmod 000 dir1/
[guest@vmpuzirev ~]$ ls -l dir1/
ls: невозможно открыть каталог 'dir1/': Отказано в доступе
[guest@vmpuzirev ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@vmpuzirev ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@vmpuzirev ~]$
```

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.