

# Презентация по выполнению индивидуального проекта №1

Основы информационной безопасности

---

Малюга В. В.

8 марта 2024

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Малюга Валерия Васильевна
- студентка группы НКАбд-04-23
- Российский университет дружбы народов
- <https://github.com/vvmalyuga>

## Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

1. Работа с атрибутами файлов
2. Заполнение таблицы “Установленные права и разрешённые действия” (см. табл. 2.1)
3. Заполнение таблицы “Минимальные права для совершения операций” (см. табл. 2.2)

**Операционная система** — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем. [1]

**Права доступа** определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].



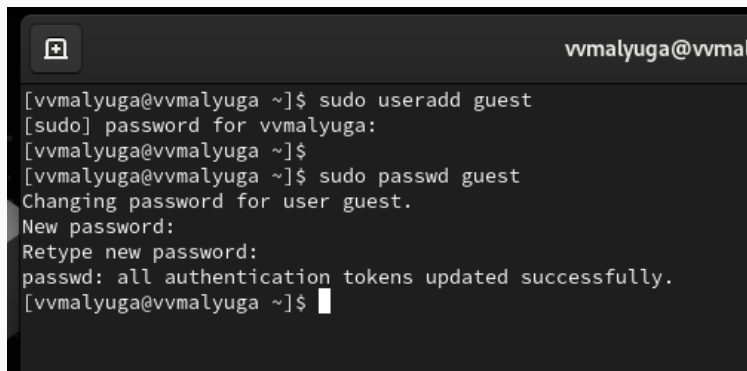
# Атрибуты файлов

---



## Атрибуты файлов

В операционной системе Rocky создаю нового пользователя guest через учетную запись администратора. Далее задаю пароль для созданной учетной записи (рис. 1).

A terminal window with a dark background. The title bar shows a window icon on the left and the text 'vvmalyuga@vvmalyuga' on the right. The terminal content shows a series of commands and their outputs: a user is added with 'sudo useradd guest', the password is set with 'sudo passwd guest', and a confirmation message is displayed. The prompt returns to the user's shell.

```
[vvmalyuga@vvmalyuga ~]$ sudo useradd guest
[sudo] password for vvmalyuga:
[vvmalyuga@vvmalyuga ~]$
[vvmalyuga@vvmalyuga ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[vvmalyuga@vvmalyuga ~]$
```


**Рис. 1:** Добавление пароля для пользователя

# Атрибуты файлов

---

## Атрибуты файлов

Сменяю пользователя в системе на только что созданного пользователя guest. Определяю с помощью команды `pwd`, что я нахожусь в директории `/home/guest/`. Эта директория является домашней, ведь в приглашении командой строкой стоит значок `~`, указывающий, что я в домашней директории (рис. 2).

A terminal window with a dark background. The title bar shows a window icon on the left and the text 'guest@vmmalyuga:~' on the right. The terminal content shows three lines of text: the first line is '[guest@vmmalyuga ~]\$ pwd', the second line is '/home/guest', and the third line is '[guest@vmmalyuga ~]\$ cd'. Below the third line, there is another prompt '[guest@vmmalyuga ~]\$' followed by a white cursor block.

```
guest@vmmalyuga:~  
[guest@vmmalyuga ~]$ pwd  
/home/guest  
[guest@vmmalyuga ~]$ cd  
[guest@vmmalyuga ~]$
```

**Рис. 2:** Текущая директория



Уточняю имя пользователя. В выводе команды `groups` информация только о названии группы, к которой относится пользователь. В выводе команды `id` можно найти больше информации: имя пользователя и имя группы, также коды имени пользователя и группы (рис. 3)

```
[guest@vvmalyuga ~]$ cd
[guest@vvmalyuga ~]$ whoami
guest
[guest@vvmalyuga ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vvmalyuga ~]$ groups
guest
[guest@vvmalyuga ~]$
```

**Рис. 3:** Информация о пользователе



Имя пользователя в приглашении командной строкой совпадает с именем пользователя, которое выводит команда `whoami` (рис. 4)

```
[guest@vvmalyuga ~]$ 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:4:7: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
tss:x:59:59:Account used for TPM access:/usr/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
sssd:x:997:995:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/sbin/nologin
pipewire:x:995:992:PipeWire System Daemon:/run/pipewire:/usr/bin/pipewire
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/lib/libstoragemgmt:/usr/sbin/libstoragemgmt
cockpit-wsinstance:x:989:988:User for cockpit-ws instances:/usr/share/cockpit-wsinstance:/usr/sbin/cockpit-wsinstance
flatpak:x:988:987:User for flatpak system helper:/usr/share/flatpak:/usr/sbin/flatpak
colord:x:987:986:User for colord:/var/lib/colord:/usr/sbin/colord
clevis:x:986:985:Clevis Decryption Framework unprivileged user:/usr/share/clevis:/usr/sbin/clevis
setroubleshoot:x:985:984:SELinux troubleshoot server:/usr/share/setroubleshoot:/usr/sbin/setroubleshoot
gdm:x:42:42:/var/lib/gdm:/usr/sbin/gdm
staprunpriv:x:159:159:systemtap unprivileged user:/usr/share/staprunpriv:/usr/sbin/staprunpriv
design:x:984:983:Group for the design signing daemon:/usr/share/design:/usr/sbin/design
gnome-initial-setup:x:983:982:/usr/share/gnome-initial-setup:/usr/sbin/gnome-initial-setup
chrony:x:982:981:chrony system user:/usr/share/chrony:/usr/sbin/chrony
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/sshd
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/usr/share/dnsmasq:/usr/sbin/dnsmasq
tcpdump:x:72:72:/usr/share/tcpdump:/usr/sbin/tcpdump
vvmalyuga:x:1000:1000:vvmalyuga:/home/vvmalyuga:/bin/bash
vboxadd:x:980:1:/usr/share/vboxadd:/usr/sbin/vboxadd
```

## Коды пользователей и групп

В выводе получаю коды пользователя и группы, адрес домашней директории (рис. 5).

```
[guest@vvmalyuga ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@vvmalyuga ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Mar  8 18:39 guest
drwx-----. 18 vvmalyuga vvmalyuga 4096 Mar  8 18:32 vvmalyuga
[guest@vvmalyuga ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vvmalyuga
----- /home/guest
[guest@vvmalyuga ~]$ mkdir dir1
```

**Рис. 5:** Просмотр файла passwd



## Создание папки и изменение ее атрибутов

Права у директории `vvmalyuga` и `guest`: `drwx---`.

Создаю поддиректорию `dir1` для домашней директории.

Расширенные атрибуты командой `lsattr` посмотреть у директории не удастся, но атрибуты есть: `drwxr-xr-x`, их удалось посмотреть с помощью команды `ls -l` (рис. 6).

```

[guest@vvmalyuga ~]$ mkdir dir1
[guest@vvmalyuga ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Desktop
drwxr-xr-x. 2 guest guest 6 Mar  8 18:48 dir1
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Documents
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Music
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Public
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Templates
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Videos
[guest@vvmalyuga ~]$
[guest@vvmalyuga ~]$ lsattr
```

## Изменение атрибутов

Снимаю атрибуты командой `chmod 000 dir1`, при проверке с помощью команды `ls -l` видно, что теперь атрибуты действительно сняты (рис. 7). Попытка создать файл в директории `dir1`. Выдает ошибку: "Permission denied" (рис. 7).

```
----- ./dir1
[guest@vvmalyuga ~]$ chmod 000 dir1
[guest@vvmalyuga ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
lsattr: Permission denied While reading flags on ./dir1
[guest@vvmalyuga ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Desktop
d------. 2 guest guest 6 Mar  8 18:48 dir1
```

# Изменение атрибутов

---

Вернув права директории и использовав снова команду `ls -l` можно убедиться, что файл не был создан

```
[guest@vvmalyuga ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@vvmalyuga ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@vvmalyuga ~]$
```

**Рис. 8:** Проверка содержимого директории

## 15. Таблица “Минимальные права для совершения операций”

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание	d(300)	-

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

...