

# Отчёт по лабораторной работе №2

## Дисциплина: Основы информационной безопасности

Выполнил: Маметкадыров Ынтымак

### Цель работы

Получить навыки работы в консоли с правами и атрибутами файлов и директорий, а также проверка необходимых прав для выполнения различных действий для работы с файлами и директориями.

### Теоретическое введение

Атрибуты --- это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые --- для группы пользователей, последние --- для всех остальных пользователей в системе.

Установка атрибутов производится командой `chmod`. Установка бита чтения (`r`) позволяет сделать файл доступным для чтения. Наличие бита записи (`w`) позволяет изменять файл. Установка бита запуска (`x`) позволяет запускать файл на исполнение.

Более подробно см. в `[@gnu-doc:bash]`.

### Выполнение лабораторной работы

Создаём нового пользователя `guest` командой `useradd`, затем устанавливаем для него пароль с помощью команды `passwd guest` (рис. `[-@fig:001]`).

```
[itmametskadihrov@itmametskadihrov ~]$ sudo useradd guest
[sudo] пароль для itmametskadihrov:
[itmametskadihrov@itmametskadihrov ~]$ sudo passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[itmametskadihrov@itmametskadihrov ~]$
```

{ #fig:001

width=70% }

Заходим в систему от имени пользователя `guest`, используя только что установленный пароль.

Выполняем команду `pwd`, которая показывает, что мы находимся в домашнем каталоге пользователя `guest`. Уточняем имя пользователя командой `whoami`, ожидаемо получаем вывод

guest. С помощью команды `id` узнаём, что `uid = 1001`, `gid = 1001` (guest). При вводе команды `groups` убеждаемся, что группа состоит из одного пользователя guest (рис. [-@fig:002]).

```
[guest@itmametskadihrov ~]$ whoami
guest
[guest@itmametskadihrov ~]$
```

{ #fig:002 width=70% }

В содержимом файла `/etc/passwd` находим информацию о пользователе, что соответствует данным, полученным с помощью команды `id` и `pwd`. Далее определяем содержимое каталога `/home`. С помощью команды `ls -l /home/` видим две домашние директории: `anpolienko` и `guest` с их атрибутами `gwx` в первом бите для каждой. С помощью команды `lsattr /home` можем увидеть расширенные атрибуты только текущего пользователя. Далее создаём новый каталог `dir1` и можем увидеть, что у него больше атрибутов по сравнению со стандартными директориями (рис. [-@fig:003]).

```
[guest@itmametskadihrov ~]$ ls -l /home/
итого 8
drwx-----. 14 guest          guest          4096 сен 16 22:47 guest
drwx-----. 14 itmametskadihrov itmametskadihrov 4096 сен  8 18:30 itmametskadihrov
[guest@itmametskadihrov ~]$
```

⌏

{ #fig:003 width=70% }

Меняем директории `dir1` атрибуты с помощью команды `chmod 000`. Далее, при попытке создать файл, видим сообщение об ошибке, т.к. забрали права на всё у всех пользователей. Файл, соответственно, тоже не создаётся (рис. [-@fig:004]).

```

[guest@itmametkadihrov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@itmametkadihrov ~]$ groups
guest
[guest@itmametkadihrov ~]$ /etc/passwd
bash: /etc/passwd: Отказано в доступе
[guest@itmametkadihrov ~]$ 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
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-User-space OOM Killer:/:usr/sbin/nologin

```

```
{ #fig:004 width=70% }
```

Далее изучим, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого будем пытаться создать файл командой `touch`, удалить его командой `rm`, записать в файл командой `echo >`, прочитать файл командой `cat`, сменить директорию командой `cd`, просмотреть директорию командой `ls`, переименовать файл командой `rename` и сменить атрибуты командой `chattr`.

В случае успеха будет записывать `+`, в случае ошибки доступа будем записывать `-`. Соберём данные в таблицу `[-@tbl:std-dir]`.

: Установленные права и разрешённые действия {#tbl:std-dir}

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просм. файло. директ.
d (000)	(000)	-	-	-	-	-	-
d --x (100)	(000)	-	-	-	-	+	-
d -w- (200)	(000)	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-
d r-- (400)	(000)	-	-	-	-	-	+
d r-x	(000)	-	-	-	-	+	+

(500)							
d rw- (600)	(000)	-	-	-	-	-	+
d rwx (700)	(000)	+	+	-	-	+	+
d (000)	--x (100)	-	-	-	-	-	-
d --x (100)	--x (100)	-	-	-	-	+	-
d -w- (200)	--x (100)	-	-	-	-	-	-
d -wx (300)	--x (100)	+	+	-	-	+	-
d r-- (400)	--x (100)	-	-	-	-	-	+
d r-x (500)	--x (100)	-	-	-	-	+	+
d rw- (600)	--x (100)	-	-	-	-	-	+
d rwx (700)	--x (100)	+	+	-	-	+	+
d (000)	-w- (200)	-	-	-	-	-	-
d --x (100)	-w- (200)	-	-	+	-	+	-
d -w- (200)	-w- (200)	-	-	-	-	-	-
d -wx (300)	-w- (200)	+	+	+	-	+	-
d r-- (400)	-w- (200)	-	-	-	-	-	+
d r-x (500)	-w- (200)	-	-	+	-	+	+
d rw- (600)	-w- (200)	-	-	-	-	-	+
d rwx (700)	-w- (200)	+	+	+	-	+	+
d (000)	-wx (300)	-	-	-	-	-	-

d --x (100)	-wx (300)	-	-	+	-	+	-
d -w- (200)	-wx (300)	-	-	-	-	-	-
d -wx (300)	-wx (300)	+	+	+	-	+	-
d r-- (400)	-wx (300)	-	-	-	-	-	+
d r-x (500)	-wx (300)	-	-	+	-	+	+
d rw- (600)	-wx (300)	-	-	-	-	-	+
d rwx (700)	-wx (300)	+	+	+	-	+	+
d (000)	r-- (400)	-	-	-	-	-	-
d --x (100)	r-- (400)	-	-	-	+	+	-
d -w- (200)	r-- (400)	-	-	-	-	-	-
d -wx (300)	r-- (400)	+	+	-	+	+	-
d r-- (400)	r-- (400)	-	-	-	-	-	+
d r-x (500)	r-- (400)	-	-	-	+	+	+
d rw- (600)	r-- (400)	-	-	-	-	-	+
d rwx (700)	r-- (400)	+	+	-	+	+	+
d (000)	r-x (500)	-	-	-	-	-	-
d --x (100)	r-x (500)	-	-	-	+	+	-
d -w- (200)	r-x (500)	-	-	-	-	-	-
d -wx (300)	r-x (500)	+	+	-	+	+	-
d r-- (400)	r-x (500)	-	-	-	-	-	+

d r-x (500)	r-x (500)	-	-	-	+	+	+
d rw- (600)	r-x (500)	-	-	-	-	-	+
d rwx (700)	r-x (500)	+	+	-	+	+	+
d (000)	rw- (600)	-	-	-	-	-	-
d --x (100)	rw- (600)	-	-	+	+	+	-
d -w- (200)	rw- (600)	-	-	-	-	-	-
d -wx (300)	rw- (600)	+	+	+	+	+	-
d r-- (400)	rw- (600)	-	-	-	-	-	+
d r-x (500)	rw- (600)	-	-	+	+	+	+
d rw- (600)	rw- (600)	-	-	-	-	-	+
d rwx (700)	rw- (600)	+	+	+	+	+	+
d (000)	rwX (700)	-	-	-	-	-	-
d --x (100)	rwX (700)	-	-	+	+	+	-
d -w- (200)	rwX (700)	-	-	-	-	-	-
d -wx (300)	rwX (700)	+	+	+	+	+	-
d r-- (400)	rwX (700)	-	-	-	-	-	+
d r-x (500)	rwX (700)	-	-	+	+	+	+
d rw- (600)	rwX (700)	-	-	-	-	-	+
d rwx (700)	rwX (700)	+	+	+	+	+	+

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу [-@tbl:std-dir1].

: Минимальные права для совершения операций {#tbl:std-dir1}

Операция	Минимальные права на директорию	Минимальные 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)

## Выводы

Приобрели практические навыки работы с атрибутами директорий и файлов через консоль, выяснили минимальные требования и права для совершения различных действий над файлами и директориями.

## Список литературы{.unnumbered}

1. File attributes in Linux [Электронный ресурс]. ITProffi, 2016