

## Лабораторная работа 2

Чичкина Ольга, 1032217621

2024 год

### Цель работы

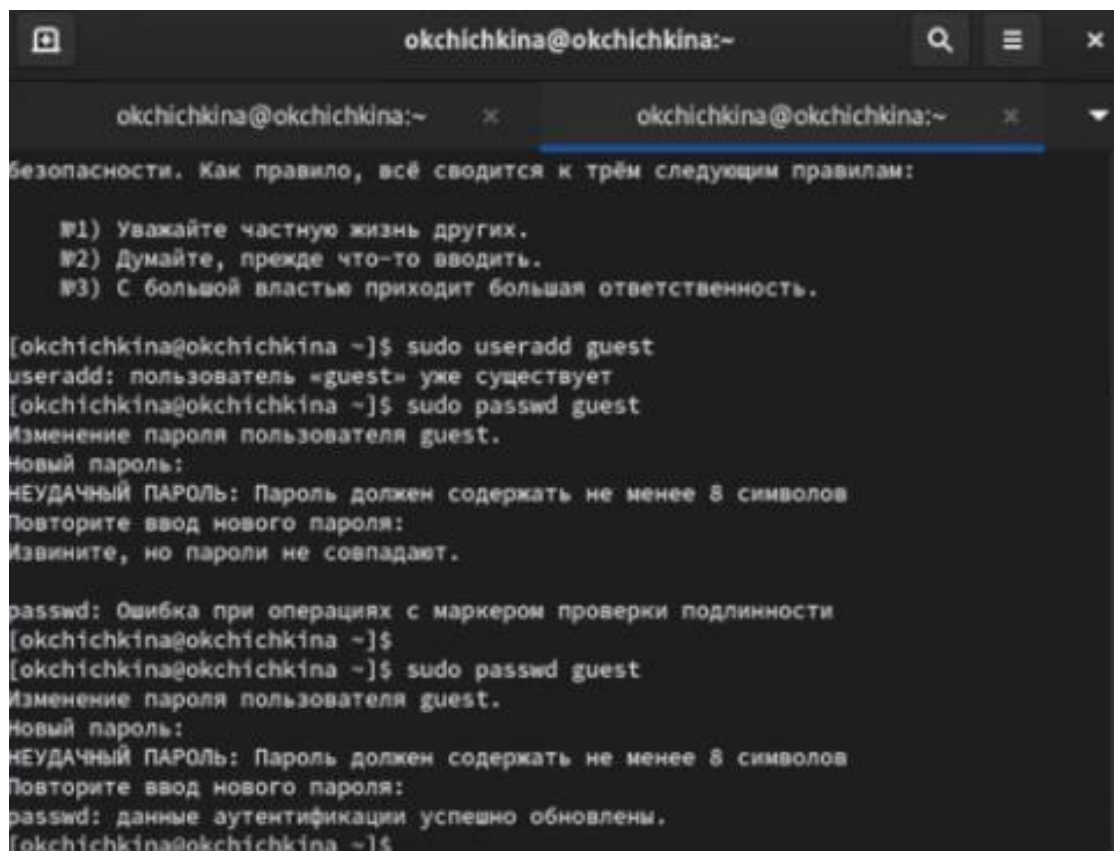
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

### Задание

Постарайтесь последовательно выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт.

### Выполнение лабораторной работы

Сначала нужно создать нового пользователя по имени `guest`, задать его пароль и зайти в систему от его имени (рис. [-@fig:001]).



```
okchichkina@okchichkina:~  
okchichkina@okchichkina:~  
безопасности. Как правило, всё сводится к трём следующим правилам:  
  
#1) Уважайте частную жизнь других.  
#2) Думайте, прежде что-то вводить.  
#3) С большой властью приходит большая ответственность.  
  
[okchichkina@okchichkina ~]$ sudo useradd guest  
useradd: пользователь «guest» уже существует  
[okchichkina@okchichkina ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов  
Повторите ввод нового пароля:  
Извините, но пароли не совпадают.  
  
passwd: Ошибка при операциях с маркером проверки подлинности  
[okchichkina@okchichkina ~]$  
[okchichkina@okchichkina ~]$ sudo passwd guest  
Изменение пароля пользователя guest.  
Новый пароль:  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов  
Повторите ввод нового пароля:  
passwd: данные аутентификации успешно обновлены.  
[okchichkina@okchichkina ~]$
```

*useradd/pwd*

Этот пользователь оказался в папке `/home/guest` – по умолчанию домашняя папка пользователя `/home/<имя_пользователя>`. Эта папка выглядит не так в приглашении командной строки – там, домашняя папка пользователя сокращается до `~`.

После этого мы выясняем информацию про самого этого пользователя (рис. [-@fig:002]).

```
guest@okchichkina:~  
[guest@okchichkina ~]$ pwd  
/home/guest  
[guest@okchichkina ~]$ whoami  
guest  
[guest@okchichkina ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@okchichkina ~]$ groups  
guest  
[guest@okchichkina ~]$ cat
```

### *whoami/id*

В выводе этой команды видно, что имя пользователя равно `guest` – это соответствует первой части приглашения командной строки, до символа `@`. С помощью команды `id` мы узнали, что этот пользователь имеет UID 1001 и GID 1001, а также принадлежит к единственной группе с UID 1001 – `guest` (об этом также сообщает команда `groups`).

Эту же информацию можно определить, посмотрев в системную базу данных пользователей – `/etc/passwd` (рис. [-@fig:003]).

```
guest:x:1001:1001::/home/guest:/bin/bash  
[guest@okchichkina ~]$
```

### *etc/passwd*

Здесь видно, что пользователь `guest` имеет пароль `x` (то есть, он хранится в `/etc/shadow`), UID `1001` и GID `1001`, не имеет полного имени пользователя, имеет домашнюю директорию `/home/guest` и интерпретатор `/bin/bash`.

Попытавшись посмотреть на информацию о папке `/home`, мы видим результат на рис. [-@fig:004].

```
[guest@okchichkina ~]$ ls -l /home/
итого 8
drwx-----. 14 guest      guest      4096 ноя 17 14:57 guest
drwx-----. 14 okchichkina okchichkina 4096 ноя 17 14:51 okchichkina
[guest@okchichkina ~]$
```

*ls /home*

Базовая информация о папках в `/home` доступна: мы видим домашнюю папку для `dmgeneralov` и для `guest`, и они обе имеют права, которые разрешают владельцу все действия, а остальным – никакие. В частности, остальные пользователи не могут выполнять `lsattr` на них, потому что происходит ошибка разрешений при чтении этой информации про `/home/dmgeneralov`, но эта информация (пустая) возвращается для `guest`.

Затем мы создаем папку, настраиваем разрешения для нее, и пытаемся использовать ее (рис. [-@fig:005]).

```
[guest@okchichkina home]$ mkdir dirl
mkdir: невозможно создать каталог «dirl»: Отказано в доступе
[guest@okchichkina home]$ cd
[guest@okchichkina ~]$ mkdir dirl
mkdir: невозможно создать каталог «dirl»: Файл существует
[guest@okchichkina ~]$ ls -l /dirl/
ls: невозможно получить доступ к '/dirl/': Нет такого файла или каталога
[guest@okchichkina ~]$ ls -l dirl
итого 0
[guest@okchichkina ~]$ lsattr dirl
[guest@okchichkina ~]$ lsattr /dirl
lsattr: Нет такого файла или каталога while trying to stat /dirl
[guest@okchichkina ~]$ chmod 000 dirl
[guest@okchichkina ~]$ ls -l dirl
ls: невозможно открыть каталог 'dirl': Отказано в доступе
[guest@okchichkina ~]$
```

*mkdir*

Сначала папка имеет права для чтения-записи для владельца, и только чтения для остальных, и мы можем использовать ее (в том числе читать `lsattr`). После этого мы меняем разрешения с помощью `chmod`, так что никто не имеет никаких прав на доступ к ней. Как результат, мы не можем создать файл в этой папке, и он действительно не создается (что можно подтвердить, посмотрев на эту папку от пользователя `root`).

В выводе команды `ls -l` в начале пишется шифр, который обозначает права на этот файл или папку. В случае папок, этот шифр имеет следующий смысл:

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибута в файла
d——— (000)	———- (000)	-	-	-	-	-	-	-	-
d-x—— (100)	—x—— (100)	-	-	-	-	+	-	-	+
d-w—— (200)	-w——- (200)	-	-	+	-	-	-	-	-
d-wx—— (300)	-wx—— (300)	+	+	+	-	+	-	+	+
dr——— (400)	-r——- (400)	-	-	-	+	-	-	-	-
dr-x—— (500)	-r-x—— (500)	-	-	-	+	+	+	-	-
drw—— (600)	-rw——- (600)	-	-	+	+	-	-	-	-
drwx—— (700)	-rwx—— (700)	+	+	+	+	+	+	+	+

На основании этих данных можно определить минимальные права, которые нужно поставить на файл или папку, если мы хотим разрешить кому-то делать определенные операции с ними:

Операция	Права на директорию	Права на файл
Создание файла	-wx	???
Удаление файла	-wx	—
Чтение файла	-x	r-
Запись в файл	-x	-w-
Переименование файла	-wx	—
Создание поддиректории	-wx	???
Удаление поддиректории	-wx	???

## Выводы

Мы изучили, как использовать базовый дискреционный контроль доступа в Linux, и определили, какие атрибуты позволяют выполнять какие действия над папками или файлами.