

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты.

Волков Тимофей Евгеньевич

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	19

List of Tables

2.1	Установленные права и разрешённые действия	11
2.2	Минимальные права для совершения операций	17

List of Figures

2.1	Создание учётной записи пользователя guest	6
2.2	Вход в систему пользователем guest	7
2.3	Командная строка guest	7
2.4	Информация о пользователе	8
2.5	Файл /etc/passwd	8
2.6	Поддиректории директории home	9
2.7	Расширенные атрибуты	9
2.8	Права доступа и расширенные атрибуты директории dir1	10
2.9	Изменение прав доступа	10
2.10	Попытка создания в директории dir1 файла file1	11

1 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.

2 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создать учётную запись пользователя `guest` (fig. 2.1) (используя учётную запись администратора)

`useradd guest`

и задать пароль для пользователя `guest` (fig. 2.1)

`passwd guest`

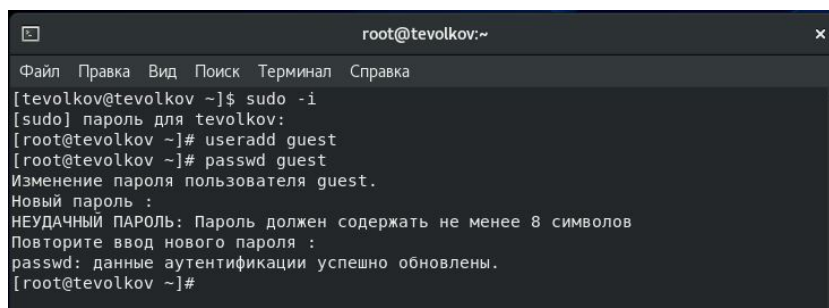
A screenshot of a terminal window titled 'root@tevolkov:~'. The terminal shows the following commands and output: [tevolkov@tevolkov ~]\$ sudo -i, [sudo] пароль для tevolkov:, [root@tevolkov ~]# useradd guest, [root@tevolkov ~]# passwd guest. The passwd command prompts for a new password, which is rejected as being too short (less than 8 characters), and then prompts to repeat the password. After successful entry, it displays 'passwd: данные аутентификации успешно обновлены.' and returns to the root prompt [root@tevolkov ~]#.

Figure 2.1: Создание учётной записи пользователя `guest`

Войти в систему от имени пользователя `guest` (fig. 2.2).

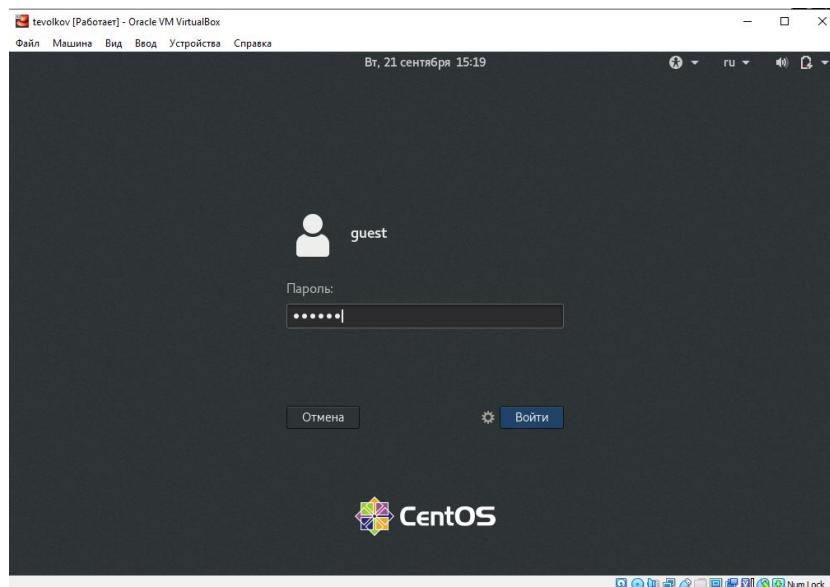


Figure 2.2: Вход в систему пользователем guest

Определить директорию, в которой вы находитесь, командой *pwd* (fig. 2.4).
Директория */home/guest* является домашней для пользователя *guest*.

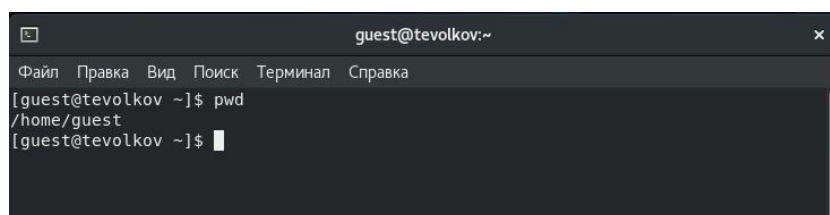
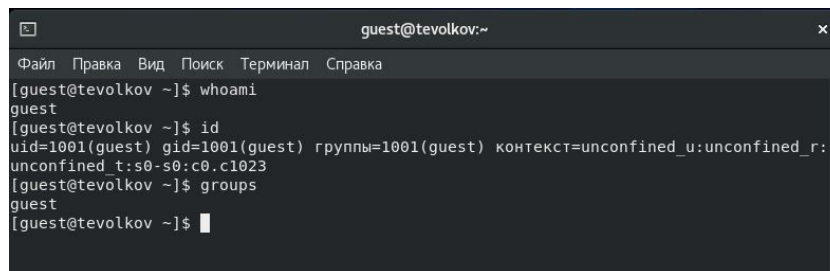


Figure 2.3: Командная строка guest

Уточнить имя вашего пользователя командой *whoami*. Уточнить имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой *id* (fig. 2.4). Выведенные значения *uid*, *gid* и др. запомнить.

Команда *groups* выводит только название группы, которой принадлежит пользователь.

id выводит идентификатор пользователя, группы, контекст безопасности.

A terminal window titled 'guest@tevolkov:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows the following commands and output:

```
[guest@tevolkov ~]$ whoami
guest
[guest@tevolkov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:
unconfined t:s0-s0:c0.c1023
[guest@tevolkov ~]$ groups
guest
[guest@tevolkov ~]$
```

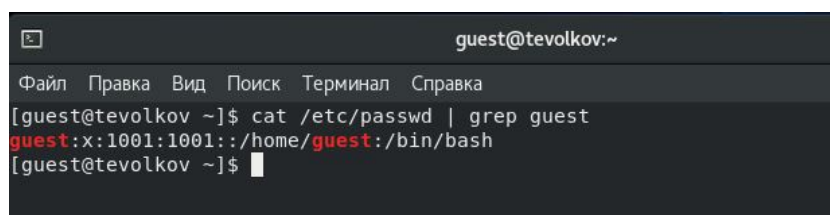
Figure 2.4: Информация о пользователе

Имя пользователя совпадает с именем пользователя в приглашении командной строки.

Просмотреть файл `/etc/passwd` используя программу `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания (fig. 2.5):

```
cat /etc/passwd | grep guest
```

Значения `uid` и `gid` пользователя совпадают с их значениями в предыдущих пунктах.

A terminal window titled 'guest@tevolkov:~' with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal shows the following command and output:

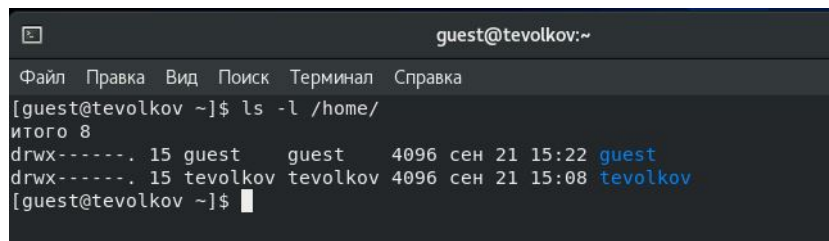
```
[guest@tevolkov ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@tevolkov ~]$
```

Figure 2.5: Файл `/etc/passwd`

Определить существующие в системе директории командой (fig. 2.6):

```
ls -l /home/
```

Вывелся список поддиректорий директории `/home`. Права к директориям имеются только у их владельца, которые могут просматривать директорию, создавать папки или файлы внутри директории и переходить в директорию.



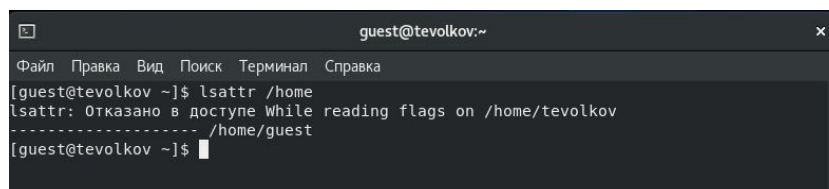
```
guest@tevolkov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@tevolkov ~]$ ls -l /home/  
итого 8  
drwx-----. 15 guest    guest    4096 сен 21 15:22 guest  
drwx-----. 15 tevolkov tevolkov  4096 сен 21 15:08 tevolkov  
[guest@tevolkov ~]$
```

Figure 2.6: Поддиректории директории home

Проверить, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории */home* (fig. 2.7), командой:

lsattr /home

Расширенные атрибуты для *guest* не установлены. Доступа к расширенным атрибутам *tevolkov* нет.



```
guest@tevolkov:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@tevolkov ~]$ lsattr /home  
lsattr: Отказано в доступе while reading flags on /home/tevolkov  
----- /home/guest  
[guest@tevolkov ~]$
```

Figure 2.7: Расширенные атрибуты

Создать в домашней директории поддиректорию *dir1* командой
mkdir dir1

Определить командами *ls -l* и *lsattr*, какие права доступа и расширенные атрибуты были выставлены на директорию *dir1* (fig. 2.8).

К директории *dir1* имеют полный доступ владелец, пользователи группы владельца, и у остальных пользователей нет только возможности именовать файлы и поддиректории.

```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@tevolkov ~]$ mkdir dir1  
[guest@tevolkov ~]$ ls -l  
итого 0  
drwxrwxr-x. 2 guest guest 6 сен 21 16:24 dir1  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Видео  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Документы  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Загрузки  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Изображения  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Музыка  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Общедоступные  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Шаблоны  
[guest@tevolkov ~]$ lsattr  
----- ./Рабочий стол  
----- ./Загрузки  
----- ./Шаблоны  
----- ./Общедоступные  
----- ./Документы  
----- ./Музыка  
----- ./Изображения  
----- ./Видео  
----- ./dir1  
[guest@tevolkov ~]$
```

Figure 2.8: Права доступа и расширенные атрибуты директории dir1

Снять с директории dir1 все атрибуты командой
`chmod 000 dir1`
и проверить с её помощью правильность выполнения команды (fig. 2.9)
`ls -l`

```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@tevolkov ~]$ chmod 000 dir1  
[guest@tevolkov ~]$ ls -l  
итого 0  
d----- . 2 guest guest 6 сен 21 16:24 dir1  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Видео  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Документы  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Загрузки  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Изображения  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Музыка  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Общедоступные  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 'Рабочий стол'  
drwxr-xr-x. 2 guest guest 6 сен 21 15:21 Шаблоны  
[guest@tevolkov ~]$
```

Figure 2.9: Изменение прав доступа

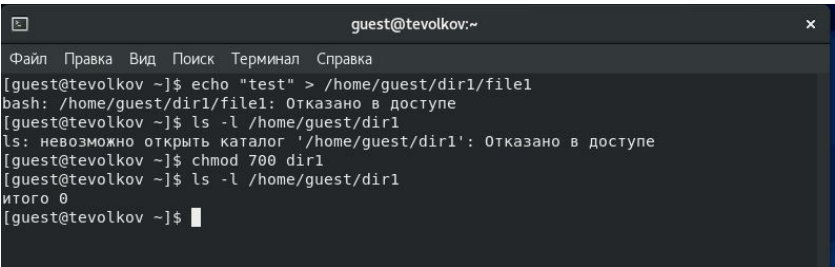
Попытаться создать в директории dir1 файл file1 (fig. 2.10) командой
`echo "test" > /home/guest/dir1/file1`
Так как у guest нет прав доступа к директории dir1 было отказано в доступе.
Оценить, как сообщение об ошибке отразилось на создании файла (перед этим

вернул права доступа пользователю) (fig. 2.10).

Проверить командой

`ls -l /home/guest/dir1`

file1 не находится внутри директории dir1.



```
guest@tevolkov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@tevolkov ~]$ echo "test" > /home/guest/dir1/file1  
bash: /home/guest/dir1/file1: Отказано в доступе  
[guest@tevolkov ~]$ ls -l /home/guest/dir1  
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе  
[guest@tevolkov ~]$ chmod 700 dir1  
[guest@tevolkov ~]$ ls -l /home/guest/dir1  
итого 0  
[guest@tevolkov ~]$
```

Figure 2.10: Попытка создания в директории dir1 файла file1

Заполнить таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занести в таблицу знак «+», если не разрешена, знак «-».

Например, в табл. приведено краткое описание стандартных каталогов Unix.

Table 2.1: Установленные права и разрешённые действия

Права	Пра-	Со-	Уда-	За-	Чте-	Сме-	Про-	Пере-	Смена
ди-	ва	зда-	ле-	пись	ние	на	смотрим	имено-	атрибу-
ректо-	фай-	ние	ние	в	фай-	ди-	файлов в	вание	тов
рии	ла	фай-	фай-	файл	ла	ректо-	директо-	файла	файла
		ла	ла			рии	рии		
—	—	-	-	-	-	-	-	-	-
(000)	(000)								
—	-x	-	-	-	-	-	-	-	-
(000)	(100)								
—	-w-	-	-	-	-	-	-	-	-
(000)	(200)								

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
— (000)	-wx (300)	-	-	-	-	-	-	-	-
— (000)	r— (400)	-	-	-	-	-	-	-	-
— (000)	r-x (500)	-	-	-	-	-	-	-	-
— (000)	rw- (600)	-	-	-	-	-	-	-	-
— (000)	rwX (700)	-	-	-	-	-	-	-	-
-x (100)	— (000)	-	-	-	-	+	-	-	+
-x (100)	-x (100)	-	-	-	-	+	-	-	+
-x (100)	-w- (200)	-	-	+	-	+	-	-	+
-x (100)	-wx (300)	-	-	+	-	+	-	-	+
-x (100)	r— (400)	-	-	-	+	+	-	-	+
-x (100)	r-x (500)	-	-	-	+	+	-	-	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
-x (100)	rw- (600)	-	-	+	+	+	-	-	+
-x (100)	rwX (700)	-	-	+	+	+	-	-	+
-w- (200)	— (000)	-	-	-	-	-	-	-	-
-w- (200)	-x (100)	-	-	-	-	-	-	-	-
-w- (200)	-w- (200)	-	-	-	-	-	-	-	-
-w- (200)	-wX (300)	-	-	-	-	-	-	-	-
-w- (200)	r— (400)	-	-	-	-	-	-	-	-
-w- (200)	r-x (500)	-	-	-	-	-	-	-	-
-w- (200)	rw- (600)	-	-	-	-	-	-	-	-
-w- (200)	rwX (700)	-	-	-	-	-	-	-	-
-wX (300)	— (000)	+	+	-	-	+	-	+	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
-wx (300)	-x (100)	+	+	-	-	+	-	+	+
-wx (300)	-w- (200)	+	+	+	-	+	-	+	+
-wx (300)	-wx (300)	+	+	+	-	+	-	+	+
-wx (300)	r- (400)	+	+	-	+	+	-	+	+
-wx (300)	r-x (500)	+	+	-	+	+	-	+	+
-wx (300)	rw- (600)	+	+	+	+	+	-	+	+
-wx (300)	rwX (700)	+	+	+	+	+	-	+	+
r- (400)	— (000)	-	-	-	-	-	+	-	-
r- (400)	-x (100)	-	-	-	-	-	+	-	-
r- (400)	-w- (200)	-	-	-	-	-	+	-	-
r- (400)	-wx (300)	-	-	-	-	-	+	-	-

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
r-	r-	-	-	-	-	-	+	-	-
(400)	(400)								
r-	r-x	-	-	-	-	-	+	-	-
(400)	(500)								
r-	rw-	-	-	-	-	-	+	-	-
(400)	(600)								
r-	rwX	-	-	-	-	-	+	-	-
(400)	(700)								
r-x	—	-	-	-	-	+	+	-	+
(500)	(000)								
r-x	-x	-	-	-	-	+	+	-	+
(500)	(100)								
r-x	-w-	-	-	+	-	+	+	-	+
(500)	(200)								
r-x	-wX	-	-	+	-	+	+	-	+
(500)	(300)								
r-x	r-	-	-	-	+	+	+	-	+
(500)	(400)								
r-x	r-x	-	-	-	+	+	+	-	+
(500)	(500)								
r-x	rw-	-	-	+	+	+	+	-	+
(500)	(600)								

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
r-x (500)	rwX (700)	-	-	+	+	+	+	-	+
rw- (600)	— (000)	-	-	-	-	-	+	-	-
rw- (600)	-x (100)	-	-	-	-	-	+	-	-
rw- (600)	-w- (200)	-	-	-	-	-	+	-	-
rw- (600)	-wx (300)	-	-	-	-	-	+	-	-
rw- (600)	r— (400)	-	-	-	-	-	+	-	-
rw- (600)	r-x (500)	-	-	-	-	-	+	-	-
rw- (600)	rw- (600)	-	-	-	-	-	+	-	-
rw- (600)	rwX (700)	-	-	-	-	-	+	-	-
rwX (700)	— (000)	+	+	-	-	+	+	+	+
rwX (700)	-x (100)	+	+	-	-	+	+	+	+

Права ди- ректо- рии	Пра- ва фай- ла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- ректо- рии	Про- смотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
rwX (700)	-w- (200)	+	+	+	-	+	+	+	+
rwX (700)	-wx (300)	+	+	+	-	+	+	+	+
rwX (700)	r- (400)	+	+	-	+	+	+	+	+
rwX (700)	r-x (500)	+	+	-	+	+	+	+	+
rwX (700)	rw- (600)	+	+	+	+	+	+	+	+
rwX (700)	rwX (700)	+	+	+	+	+	+	+	+

На основании заполненной таблицы определить те или иные минимально необходимые права для выполнения операций внутри директории *dir1* (табл. 2.2).

Table 2.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	-wx (300)	— (000)
Удаление файла	-wx (300)	— (000)
Чтение файла	-x (100)	r- (400)
Запись в файл	-x (100)	-w- (200)
Переименование файла	-wx (300)	— (000)

Операция	Минимальные права на директорию	Минимальные права на файл
Создание поддиректории	-wx (300)	— (000)
Удаление поддиректории	-wx (300)	— (000)

3 Выводы

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