

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Хусайнова Фароиз Дилшодовна

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
4 Выводы	18

Список таблиц

3.1	Установленные права и разрешенные действия	14
3.2	Минимальные права для совершения операций	17

Список иллюстраций

3.1	Создание учетной записи guest.	7
3.2	Задания пароля для учетной записи	8
3.3	Вход в систему от имени пользователя guest.	8
3.4	Определение текущей директории и переход в нее.	9
3.5	Уточнение имени пользователя.	9
3.6	Сравнение полученной информации	10
3.7	Команда cat /etc/passwd	10
3.8	Команда cat /etc/passwd.	11
3.9	Фильтрованный вывод строки.	11
3.10	Определение существующих в системе директорий	12
3.11	Проверка установленных расширенных атрибутов	12
3.12	Создание директории dir1.	13

1 Цель работы

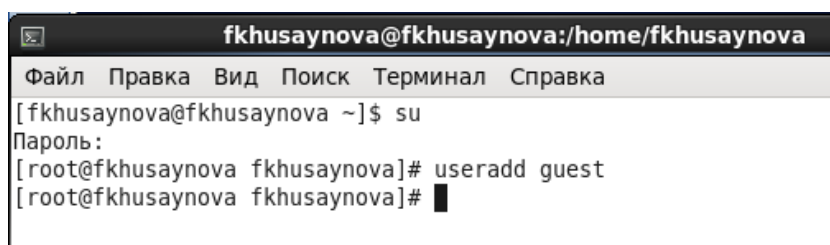
Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

1. Создать учетную запись пользователя guest.
2. Используя созданную учетную запись, войти в терминал и выполнить базовые операции с директориями и файлами.
3. Заполнить таблицу “Установленные права и разрешенные действия”
4. Заполнить таблицу “Минимальные права для совершения операций”

3 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest (используя учётную запись администратора) (рис - @fig:001)

A screenshot of a terminal window. The title bar shows the user 'fkhusaynova' at host 'fkhusaynova' in the directory '/home/fkhusaynova'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal content shows the user typing 'su' at the prompt '[fkhusaynova@fkhusaynova ~]\$'. After a password is entered (indicated by 'Пароль:'), the prompt changes to root '[root@fkhusaynova fkhusaynova]#'. The user then types 'useradd guest', and the prompt remains at root after the command is executed. A cursor is visible at the end of the last line.

```
fkhusaynova@fkhusaynova:/home/fkhusaynova
Файл Правка Вид Поиск Терминал Справка
[fkhusaynova@fkhusaynova ~]$ su
Пароль:
[root@fkhusaynova fkhusaynova]# useradd guest
[root@fkhusaynova fkhusaynova]#
```

Рис. 3.1: Создание учетной записи guest

Задала пароль для пользователя guest (используя учётную запись администратора) (рис - @fig:002).

```
fkhusaynova@fkhusaynova:/home/fkhusaynova
Файл Правка Вид Поиск Терминал Справка
[fkhusaynova@fkhusaynova ~]$ su
Пароль:
[root@fkhusaynova fkhusaynova]# useradd guest
[root@fkhusaynova fkhusaynova]#
```

Рис. 3.2: Задание пароля для учетной записи

Вошла в систему от имени пользователя guest (рис -@fig:003).

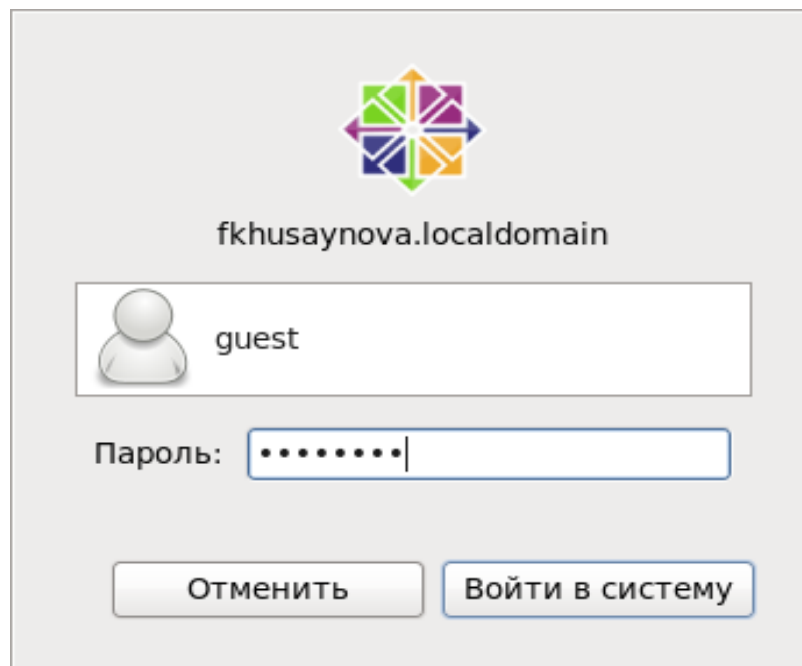
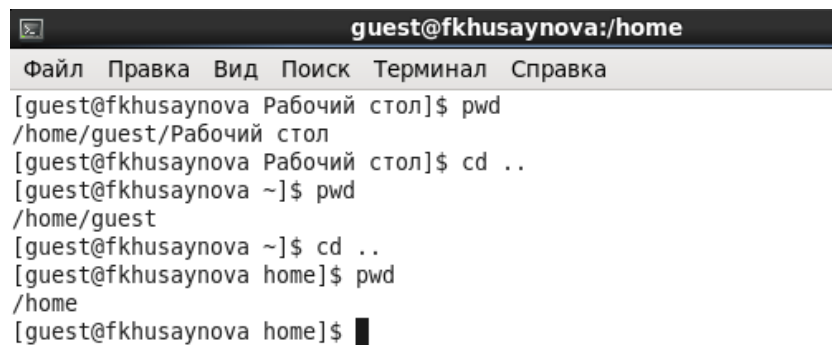


Рис. 3.3: Вход в систему от имени пользователя guest

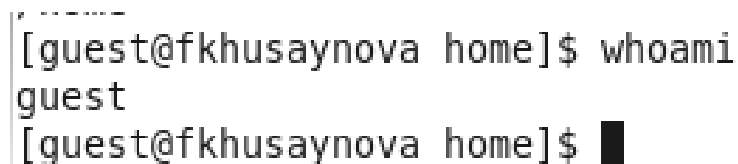
Определила директорию, в которой я нахожусь, командой `pwd`. Определила, что она не является моей домашней директорией. Перешла в свою домашнюю директорию. (рис -@fig:004)



```
guest@fkhusaynova:/home
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@fkhusaynova Рабочий стол]$ pwd
/home/guest/Рабочий стол
[guest@fkhusaynova Рабочий стол]$ cd ..
[guest@fkhusaynova ~]$ pwd
/home/guest
[guest@fkhusaynova ~]$ cd ..
[guest@fkhusaynova home]$ pwd
/home
[guest@fkhusaynova home]$
```

Рис. 3.4: Определение текущей директории. Переход в домашнюю директорию

Уточнила имя своего пользователя командой `whoami` (рис -@fig:005).



```
[guest@fkhusaynova home]$ whoami
guest
[guest@fkhusaynova home]$
```

Рис. 3.5: Уточнение имени пользователя

Уточнила имя своего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Группы совпадают, однако вывод команды `id` объемнее (рис -@fig:006).

```
[guest@fkhusaynova home]$ id
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023
[guest@fkhusaynova home]$ groups
guest
[guest@fkhusaynova home]$ █
```

Рис. 3.6: Уточнение имени, его группы

Просмотрела файл /etc/passwd командой cat /etc/passwd (рис - @fig:007, рис - @fig:009)

```
[guest@fkhusaynova home]$ 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
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:./:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
```

Рис. 3.7: Команда cat /etc/passwd

```

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
pulse:x:498:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
saslauth:x:497:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
gdm:x:42:42:/:var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
fkhusaynova:x:500:500:fkhusaynova:/home/fkhusaynova:/bin/bash
guest:x:501:501:/:home/guest:/bin/bash
[guest@fkhusaynova home]$ █

```

Рис. 3.8: Команда cat /etc/passwd

Нашла свою учетную запись (последняя строчка). Определила uid и gid пользователя (501 и 501 соответственно). Они совпадают со значениями uid и gid, полученными на предыдущих пунктах.

Для того, чтобы вывести только строки, содержащие определенные буквенные сочетания, необходимо воспользоваться программой grep в терминале (рис - @fig:09)

```

[guest@fkhusaynova home]$ cat /etc/passwd | grep guest
guest:x:501:501:/:home/guest:/bin/bash
[guest@fkhusaynova home]$ █

```

Рис. 3.9: Фильтрованный вывод строк

Определила существующие в системе директории командой `ls -l /home/` (рис -@fig:010)

```
[guest@fkhusaynova home]$ ls -l /home/
итого 8
drwx-----. 27 fkhusaynova fkhusaynova 4096 Окт  2 17:40 fkhusaynova
drwx-----. 26 guest      guest      4096 Окт  2 17:54 guest
[guest@fkhusaynova home]$
```

Рис. 3.10: Определение существующих в системе директорий

Мне удалось получить список поддиректорий директории `/home`. На поддиректориях установлены права на чтение (r), запись (w) и исполнение (x).

Проверила, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home` с помощью команды `lsattr /home` (рис -@fig:011)

```
[guest@fkhusaynova home]$ lsattr /home
-----e- /home/guest
lsattr: Отказано в доступе While reading flags on /home/fkhusaynova
[guest@fkhusaynova home]$
```

Рис. 3.11: Проверка установленных расширенных атрибутов

Создала в домашней директории поддиректорию `dir1` командой `mkdir dir1`. (рис -@fig:012)

```
-----  
[guest@fkhusaynova home]$ su  
Пароль:  
[root@fkhusaynova home]# mkdir dir1  
[root@fkhusaynova home]# ls -l  
-----
```

Рис. 3.12: Создание директории dir1

Также с помощью команд `ls -l` и `lsattr` просмотрел, какие атрибуты выставлены на директорию `dir` (`drwxrwxr-x` и `-----e-` соответственно).

Сняла с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверила правильность выполнения команды с помощью `ls -l`

Заполнила таблицу "Установленные права и разрешенные действия", выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет. "+" - операция разрешена, "-" - операция не разрешена (таб. 3.1)

Таблица 3.1: Установленные права и разрешённые действия

Пра-						Сме-			
ва		Со-	Уда-			на			
ди-	Пра-	зда-	ле-	За-	Чте-	ди-	Просмотр	Пере-	Смена
рек-	ва	ние	ние	пись	ние	рек-	файлов в	имено-	атрибу-
то-	фай-	фай-	фай-	в	фай-	то-	директо-	вание	тов
рии	ла	ла	ла	файл	ла	рии	рии	файла	файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	-	-	-	+
d(100)	(100)	-	-	-	-	-	-	-	+
d(100)	(200)	-	-	+	-	-	-	-	+
d(100)	(300)	-	-	+	-	-	-	-	+
d(100)	(400)	-	-	-	+	-	-	-	+
d(100)	(500)	-	-	-	+	-	-	-	+
d(100)	(600)	-	-	+	+	-	-	-	+
d(100)	(700)	-	-	+	+	-	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
ди- рек- то- рии	Пра- ва фай- ла	зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	-
d(300)	(700)	+	+	+	+	+	-	+	-
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	+	-	-	-	-	+	-	+
d(500)	(100)	+	-	-	-	-	+	-	+
d(500)	(200)	+	-	+	-	-	+	-	+
d(500)	(300)	+	-	+	-	-	+	-	+

Пра- ва	Со- зда- ние	Уда- ле- ние	За- пись	Чте- ние	Сме- на	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
ди- рек- то- рии	Пра- ва фай- ла	зда- ние фай- ла	ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	Просмотр файлов в директо- рии	Пере- имено- вание файла	Смена атрибу- тов файла
d(500)	(400)	+	-	-	+	-	+	-	+
d(500)	(500)	+	-	-	+	-	+	-	+
d(500)	(600)	+	-	+	+	-	+	-	+
d(500)	(700)	+	-	+	+	-	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

На основании заполненной выше таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполняя таблицу "Установленные права и разрешенные действия" (таб. 3.2).

Таблица 3.2: Минимальные права для совершения операций

Операция	min права на директорию	min права на файл
Создание файла	(-wx)(3)	(--)(0)
Удаление файла	(-wx)(3)	(--)(0)
Чтение файла	(--x)(1)	(r--)(4)
Запись в файл	(--x)(1)	(-w-)(2)
Переименование файла	(-wx)(3)	(--)(0)
Создание поддиректории	(-wx)(3)	(--)(0)
Удаление поддиректории	(-wx)(3)	(--)(0)

4 Выводы

Таким образом, я получила практически навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.