

Лабораторная работа № 3

Дискреционноеразграничение прав в Linux. Два пользователя

Абдуллаев Сайидазизхон Шухратович

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Ход работы	9
Выводы	18

Список иллюстраций

1	Вход в систему	9
2	Пароль для новой учетной записи	10
3	Добавление в группу	10
4	Определение домашней директории	11
5	Уточнение id пользователя guest	12
6	Уточнение id пользователя guest1	12
7	Уточнение id пользователя guest	13
8	Регистрация в группе	13
9	Изменение прав директории	14
10	Процесс проверки разрешенных операций	15
11	Заполненная таблица	16
12	Проверка минимально необходимых прав для выполнения операций внутри директории	17

Список таблиц

Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

Задание

Закрепить дискреционное разграничение прав для групп в Linux.

Теоретическое введение

Linux в целом и Ubuntu в частности - системы многопользовательские, т.е. на одном компьютере может быть несколько различных пользователей, каждый со своими собственными настройками, данными и правами доступа к различным системным функциям. Кроме пользователей в Linux для разграничения прав существуют группы. Каждая группа так же как и отдельный пользователь обладает неким набором прав доступа к различным компонентам системы и каждый пользователь-член этой группы автоматически получает все права группы. То есть группы нужны для группировки пользователей по принципу одинаковых полномочий на какие-либо действия, вот такая тавтология. Каждый пользователь может состоять в неограниченном количестве групп и в каждой группе может быть сколько угодно пользователей¹). Один из подходов к разграничению доступа — так называемый дискреционный - предполагает назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют. Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей. Чтобы получить доступ к файлам в Linux, используются разрешения. Эти разрешения назначаются трем объектам: файлу, группе и другому объекту. Для управления правами используется команда `chmod`. При использовании `chmod` в относительном режиме вы работаете с тремя индикаторами, чтобы указать, что вы хо-

тите сделать. Сначала вы указываете, для кого вы хотите изменить разрешения. Для этого вы можете выбрать между пользователем (u), группой (g) и другими (o). Затем вы используете оператор для добавления или удаления разрешений из текущего режима или устанавливаете их абсолютно. В конце вы используете r(read), w(write) и x(execute), чтобы указать, какие разрешения вы хотите установить. При использовании `chmod` вы можете устанавливать разрешения для пользователя (user), группы (group) и других (other). Помимо основных разрешений, о которых вы только что прочитали, в Linux также есть набор расширенных разрешений. Это не те разрешения, которые вы устанавливаете по умолчанию, но иногда они предоставляют полезное дополнение.

Ход работы

1. Заходим под учётной записью пользователя guest, созданной при выполнении предыдущей лабораторной работы (Рис. [-@fig:001]).

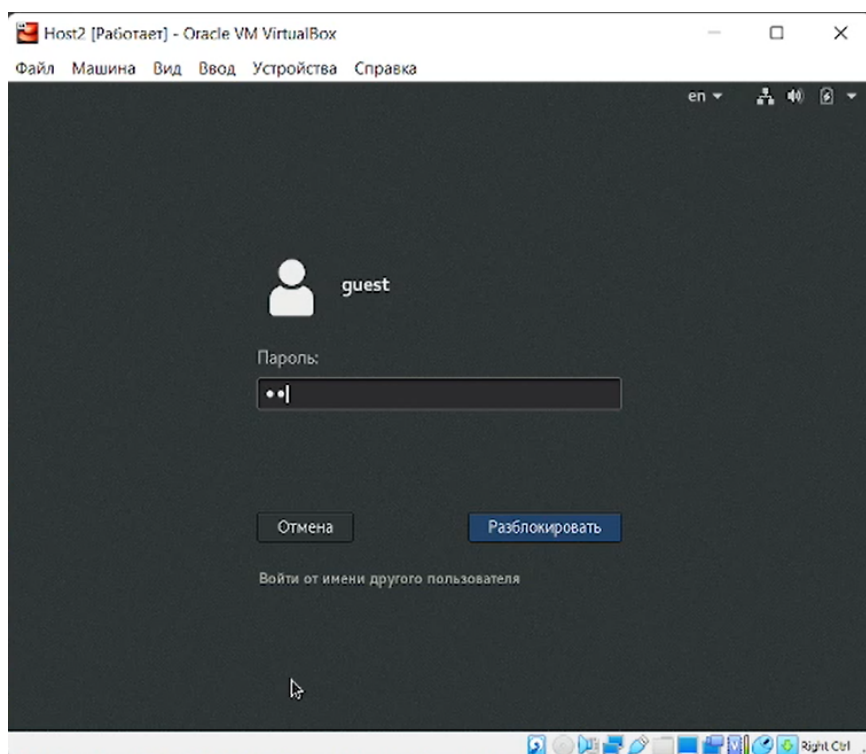


Рис. 1: Вход в систему

2. Аналогично создаем второго пользователя guest2 (используя учётную запись администратора) и задаем пароль. (Рис. [-@fig:002]).

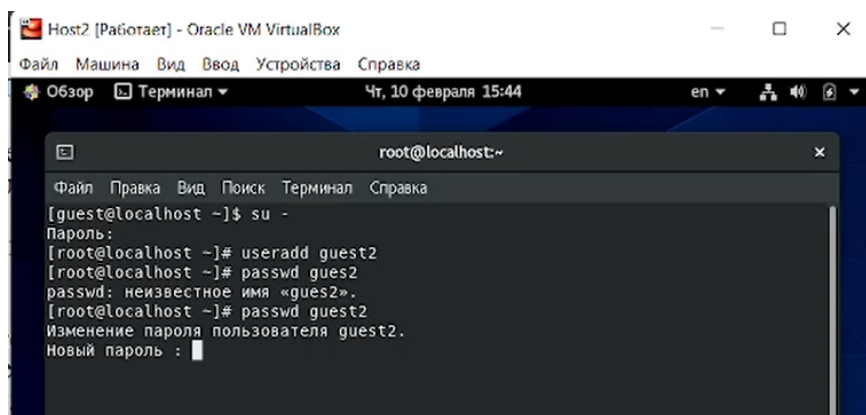


Рис. 2: Пароль для новой учетной записи

3. Добавляем пользователя guest2 в группу guest. (Рис. [-@fig:003]).

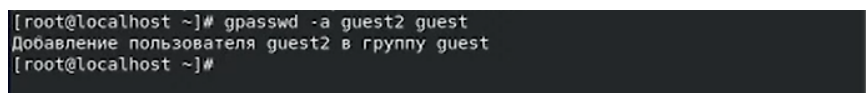


Рис. 3: Добавление в группу

4. Осуществляем вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли и. Для обоих пользователей командой pwd определяем директорию, в которой мы находимся. (Рис. [-@fig:004]).

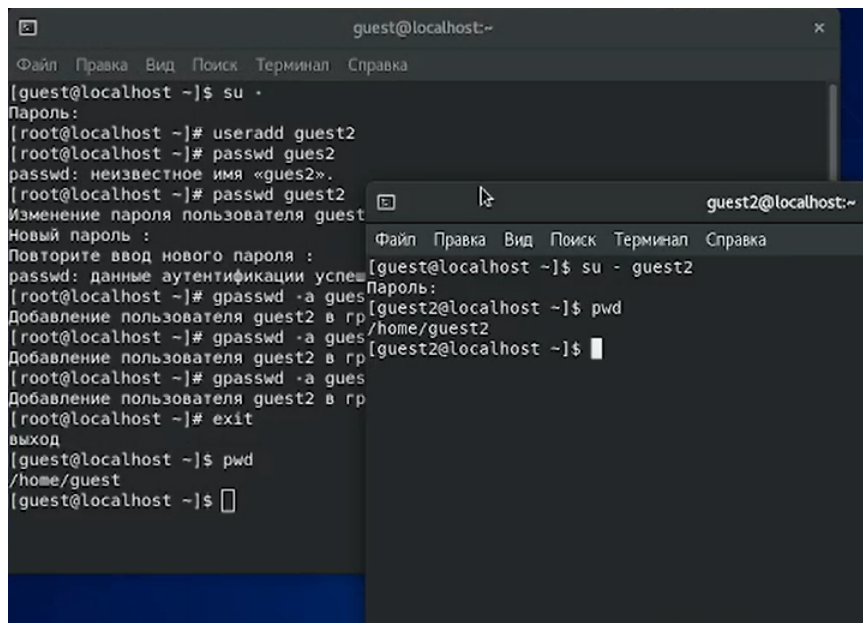


Рис. 4: Определение домашней директории

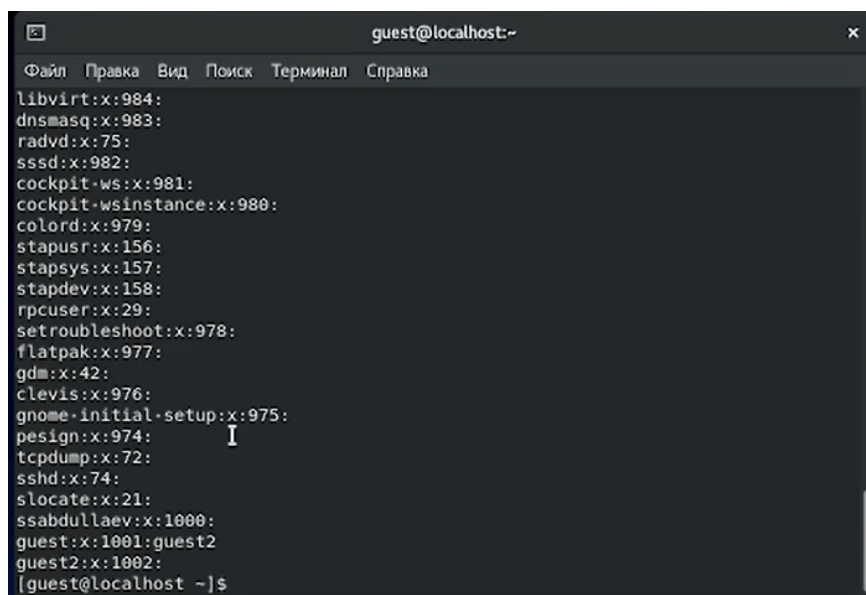
5. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравните вывод команды `groups` с выводом команд `id -Gn` и `id -G`, а также с содержанием файла `/etc/group`. (Рис. [-@fig:005], [-@fig:006], [-@fig:007]).

```
guest@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@localhost ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest@localhost ~]$ groups guest  
guest : guest  
[guest@localhost ~]$ id -Gn  
guest  
[guest@localhost ~]$ id -G  
1001  
[guest@localhost ~]$
```

Рис. 5: Уточнение id пользователя guest

```
guest2@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[guest2@localhost ~]$ id  
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@localhost ~]$ groups guest2  
guest2 : guest2 guest  
[guest2@localhost ~]$
```

Рис. 6: Уточнение id пользователя guest1



```
guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
libvirt:x:984:
dnsmasq:x:983:
radvd:x:75:
sssd:x:982:
cockpit-ws:x:981:
cockpit-wsinstance:x:980:
colord:x:979:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
rpcuser:x:29:
setroubleshoot:x:978:
flatpak:x:977:
gdm:x:42:
clevi:x:976:
gnome-initial-setup:x:975:
pesign:x:974:
tcpdump:x:72:
sshd:x:74:
slocate:x:21:
ssabdullaev:x:1000:
guest:x:1001:guest2
guest2:x:1002:
[guest@localhost ~]$
```

Рис. 7: Уточнение id пользователя guest

- От имени пользователя guest2 выполняем регистрацию пользователя guest2 в группе guest командой `newgrp guest`. (Рис. [-@fig:008]).



```
[guest2@localhost ~]$ newgrp guest
[guest2@localhost ~]$
```

Рис. 8: Регистрация в группе

- От имени пользователя guest изменяем права директории `/home/guest`, разрешив все действия для пользователей группы: `chmod g+rwX /home/guest`, а также снимаем с директории `/home/guest/dir1` все атрибуты командой `chmod 000 dir1[2]`. (Рис. [-@fig:009]).

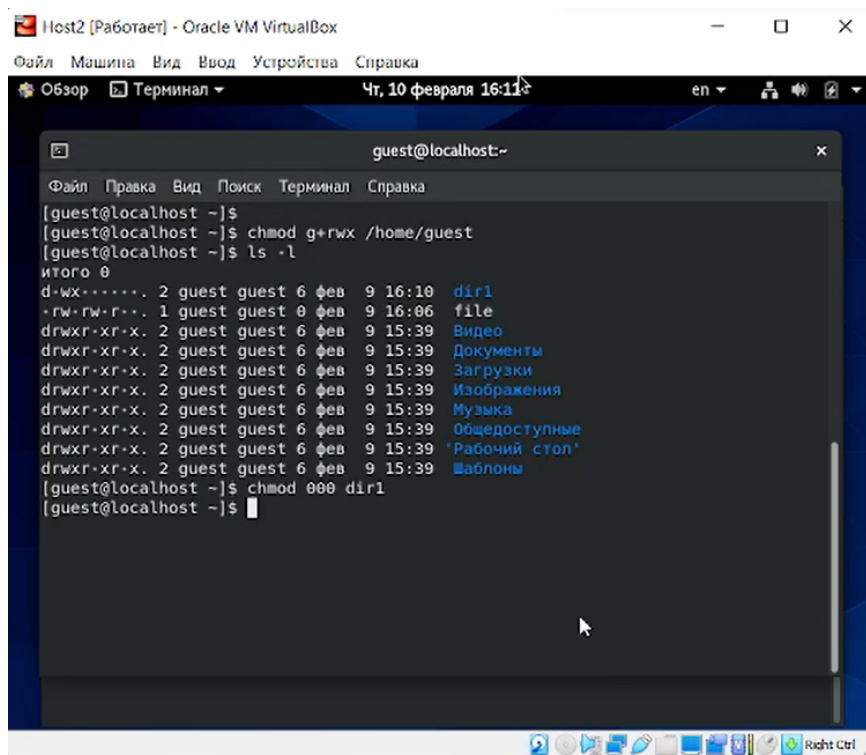
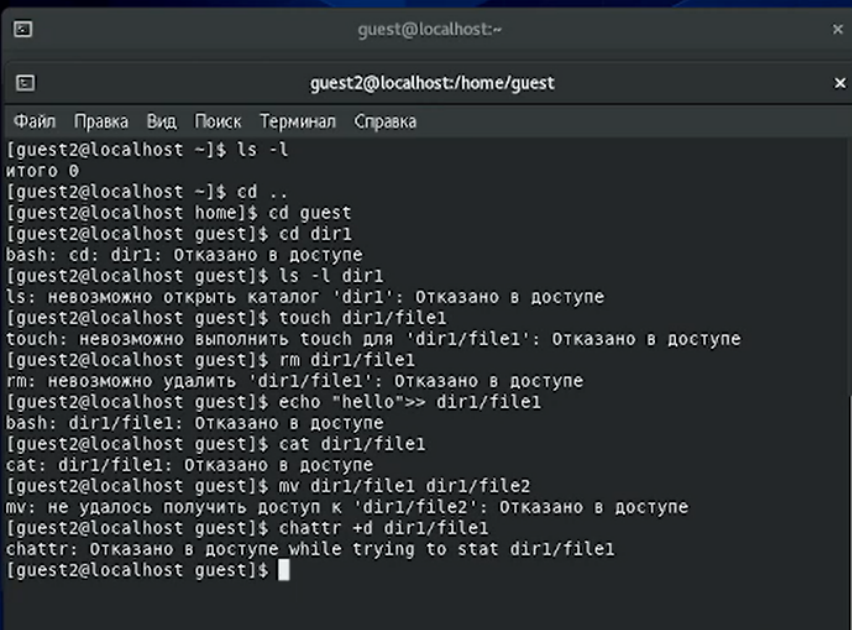


Рис. 9: Изменение прав директории

8. Заполняем таблицу «Установленные права и разрешённые действия», выполняя действия от имени guest и делая проверку от пользователя guest2, определяем опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, заносим в таблицу знак «+», если не разрешена, знак «-». При заполнении таблицы рассматриваем не все атрибуты файлов и директорий, а лишь «первые три»: г, w, x, для «владельца». В итоге рассматриваем 64 варианта[1]. (Рис. [-@fig:010], [-@fig:011]).



```
guest@localhost:~  
guest2@localhost:/home/guest  
Файл Правка Вид Поиск Терминал Справка  
[guest2@localhost ~]$ ls -l  
итого 0  
[guest2@localhost ~]$ cd ..  
[guest2@localhost home]$ cd guest  
[guest2@localhost guest]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest2@localhost guest]$ ls -l dir1  
ls: невозможно открыть каталог 'dir1': Отказано в доступе  
[guest2@localhost guest]$ touch dir1/file1  
touch: невозможно выполнить touch для 'dir1/file1': Отказано в доступе  
[guest2@localhost guest]$ rm dir1/file1  
rm: невозможно удалить 'dir1/file1': Отказано в доступе  
[guest2@localhost guest]$ echo "hello">> dir1/file1  
bash: dir1/file1: Отказано в доступе  
[guest2@localhost guest]$ cat dir1/file1  
cat: dir1/file1: Отказано в доступе  
[guest2@localhost guest]$ mv dir1/file1 dir1/file2  
mv: не удалось получить доступ к 'dir1/file2': Отказано в доступе  
[guest2@localhost guest]$ chmod +d dir1/file1  
chmod: Отказано в доступе while trying to stat dir1/file1  
[guest2@localhost guest]$
```

Рис. 10: Процесс проверки разрешенных операций

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директори и	Просмотр файлов в директори и	Переимено вание файла	Смена атрибутов файла
000	000	---	---	---	---	---	---	---	---
010	000	---	---	---	---	+	---	---	---
020	000	---	---	---	---	---	---	---	---
030	000	+	+	---	---	+	---	+	---
040	000	---	---	---	---	---	+	---	---
050	000	---	---	---	---	+	+	---	---
060	000	---	---	---	---	---	+	---	---
070	000	+	+	---	---	+	+	+	---
000	010	---	---	---	---	---	---	---	---
010	010	---	---	---	---	+	---	---	---
020	010	---	---	---	---	---	---	---	---
030	010	+	+	---	---	+	---	+	---
040	010	---	---	---	---	---	+	---	---
050	010	---	---	---	---	+	+	---	---
060	010	---	---	---	---	---	+	---	---
070	010	+	+	---	---	+	+	+	---
000	020	---	---	---	---	---	---	---	---
010	020	---	---	+	---	+	---	---	---
020	020	---	---	---	---	---	---	---	---
030	020	+	+	+	---	+	---	+	---
040	020	---	---	---	---	---	+	---	---
050	020	---	---	+	---	+	+	---	---
060	020	---	---	---	---	---	+	---	---
070	020	+	+	+	---	+	+	+	---
000	030	---	---	---	---	---	---	---	---
010	030	---	---	+	---	+	---	---	---
020	030	---	---	---	---	---	---	---	---
030	030	+	+	+	---	+	---	+	---
040	030	---	---	---	---	---	+	---	---
050	030	---	---	+	---	+	+	---	---
060	030	---	---	---	---	---	+	---	---
070	030	+	+	+	---	+	+	+	---
000	040	---	---	---	---	---	---	---	---
010	040	---	---	---	+	+	---	---	---
020	040	---	---	---	---	---	---	---	---
030	040	+	+	---	+	+	---	+	---
040	040	---	---	---	---	---	+	---	---
050	040	---	---	---	+	+	+	---	---
060	040	---	---	---	---	---	+	---	---
070	040	+	+	---	+	+	+	+	---
000	050	---	---	---	---	---	---	---	---
010	050	---	---	---	+	+	---	---	---
020	050	---	---	---	---	---	---	---	---
030	050	+	+	---	+	+	---	+	---
040	050	---	---	---	---	---	+	---	---
050	050	---	---	---	+	+	+	---	---
060	050	---	---	---	---	---	+	---	---
070	050	+	+	---	+	+	+	+	---
000	060	---	---	---	---	---	---	---	---
010	060	---	---	+	+	+	---	---	---
020	060	---	---	---	---	---	---	---	---
030	060	+	+	+	+	+	---	+	---
040	060	---	---	---	---	---	+	---	---
050	060	---	---	+	+	+	+	---	---
060	060	---	---	---	---	---	+	---	---
070	060	+	+	+	+	+	+	+	---
000	070	---	---	---	---	---	---	---	---
010	070	---	---	+	+	+	---	---	---
020	070	---	---	---	---	---	---	---	---
030	070	+	+	+	+	+	---	+	---
040	070	---	---	---	---	---	+	---	---
050	070	---	---	+	+	+	+	---	---
060	070	---	---	---	---	---	+	---	---
070	070	+	+	+	+	+	+	+	---

Рис. 11: Заполненная таблица

9. На основании заполненной таблицы определяем те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1, внося данные во вторую таблицу[3]. (Рис. [-@fig:012]).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	000
Удаление поддиректории	030	000

Рис. 12: Проверка минимально необходимых прав для выполнения операций внутри директории

Выводы

В результате выполнения данной работы были приобретены практические навыки работы в консоли с атрибутами файлов для группы.