

Отчёт по лабораторной работе №2

Информационная безопасность

Дискреционное разграничение прав в Linux. Основные атрибуты

Выполнил: Махорин Иван Сергеевич,
НПИБд-02-21, 1032211221

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
3.1	Атрибуты файлов	6
3.2	Заполнение таблицы 2.1	12
3.3	Заполнение таблицы 2.2	15
4	Вывод	17
5	Список литературы. Библиография	18

Список иллюстраций

3.1	useradd guest	6
3.2	passwd guest	6
3.3	guest	7
3.4	pwd	7
3.5	whoami	8
3.6	id и groups	8
3.7	Совпадение	8
3.8	cat /etc/passwd	9
3.9	ls -l /home/	10
3.10	lsattr /home	10
3.11	mkdir dir1	11
3.12	chmod 000 dir1	11
3.13	“test” > /home/guest/dir1/file1	12

1 Цель работы

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

2 Теоретическое введение

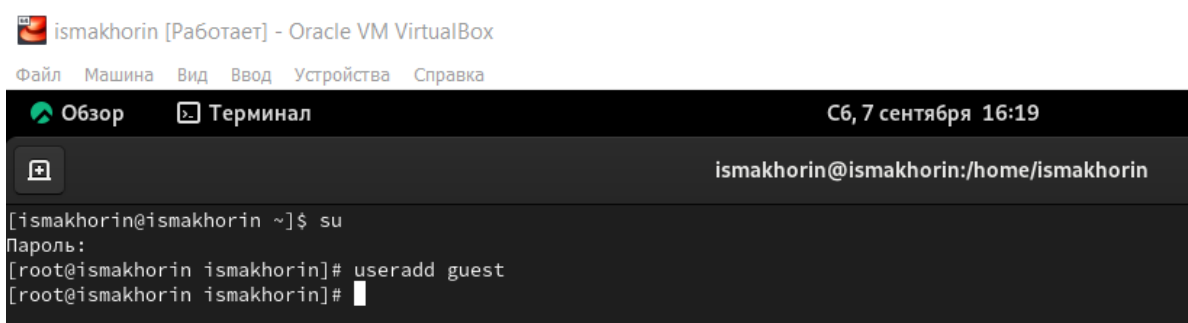
Операционная система — то комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы [2].

3 Выполнение лабораторной работы

3.1 Атрибуты файлов

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора): `useradd guest`

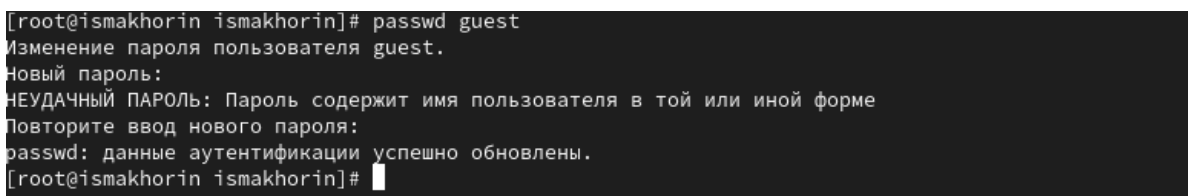


The screenshot shows a terminal window titled "ismakhorin [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a toolbar with "Обзор" and "Терминал" buttons. The terminal content shows the user "ismakhorin@ismakhorin:/home/ismakhorin" at the prompt. The user enters "su" to become root. The root prompt is "[root@ismakhorin ismakhorin]#". The root user enters "useradd guest". The terminal shows the command being executed successfully.

```
ismakhorin@ismakhorin ~]$ su
Пароль:
[root@ismakhorin ismakhorin]# useradd guest
[root@ismakhorin ismakhorin]#
```

Рис. 3.1: `useradd guest`

2. Далее зададим пароль для пользователя guest (используя также учётную запись администратора): `passwd guest`



The screenshot shows a terminal window with the root prompt "[root@ismakhorin ismakhorin]#". The root user enters "passwd guest". The terminal shows the command being executed successfully, with prompts for "Новый пароль:" and "Повторите ввод нового пароля:". The terminal shows the command being executed successfully.

```
[root@ismakhorin ismakhorin]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль содержит имя пользователя в той или иной форме
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@ismakhorin ismakhorin]#
```

Рис. 3.2: `passwd guest`

3. Войдём в систему от имени пользователя guest.

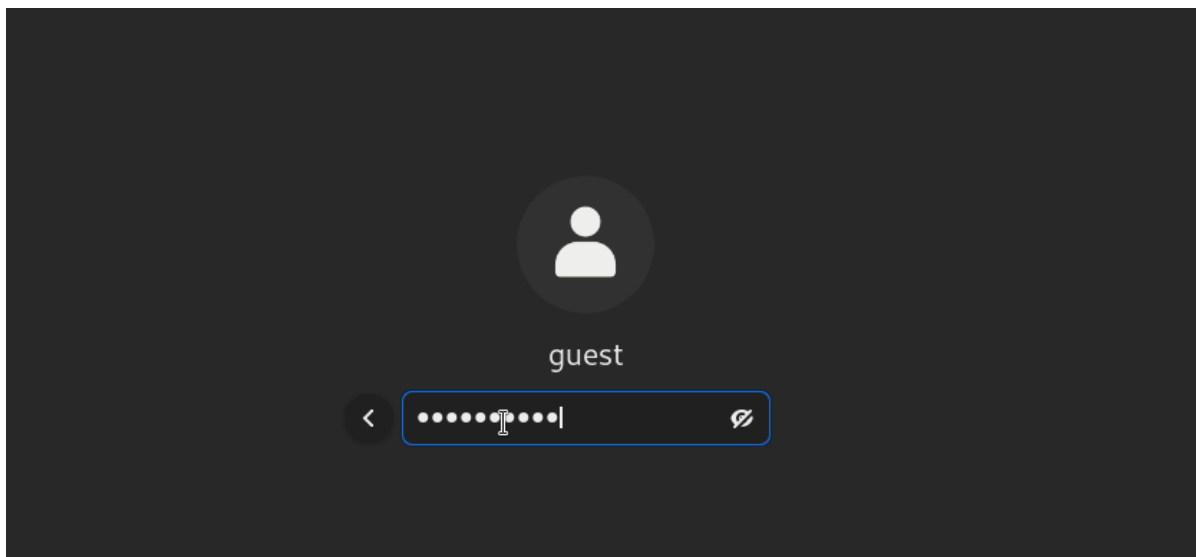


Рис. 3.3: guest

4. Определим директорию, в которой мы находимся, командой `pwd`. После чего сравним её с приглашением командной строки.

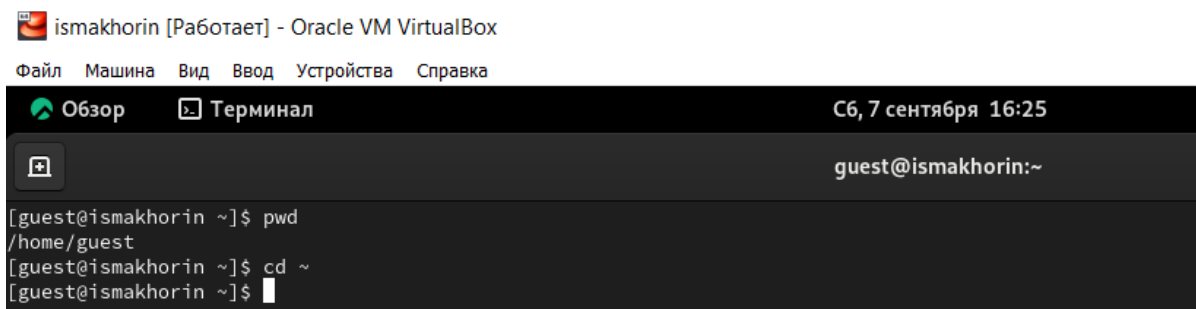


Рис. 3.4: pwd

5. Затем уточним имя нашего пользователя командой `whoami`.

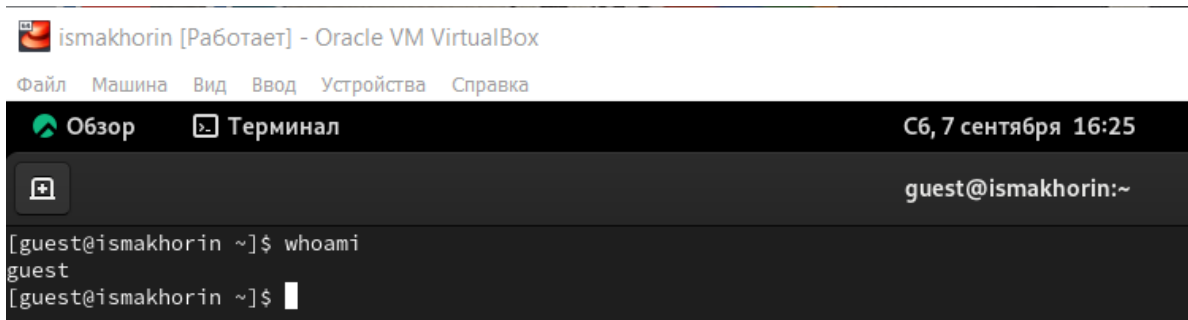


Рис. 3.5: whoami

6. Уточним имя нашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомним и сравним вывод `id` с выводом команды `groups`.

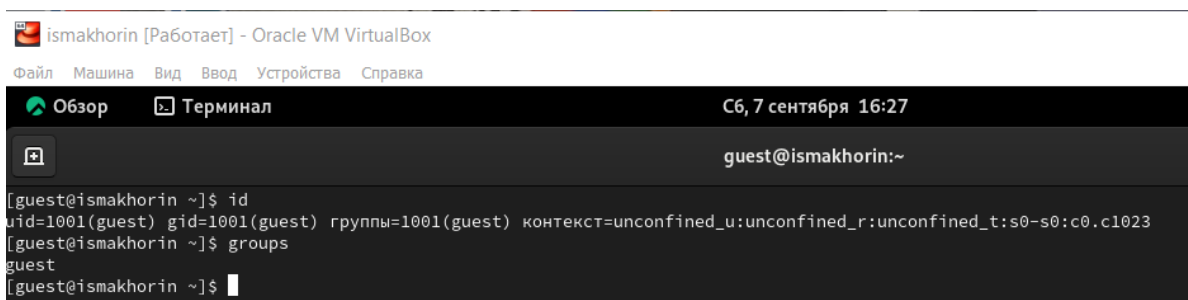


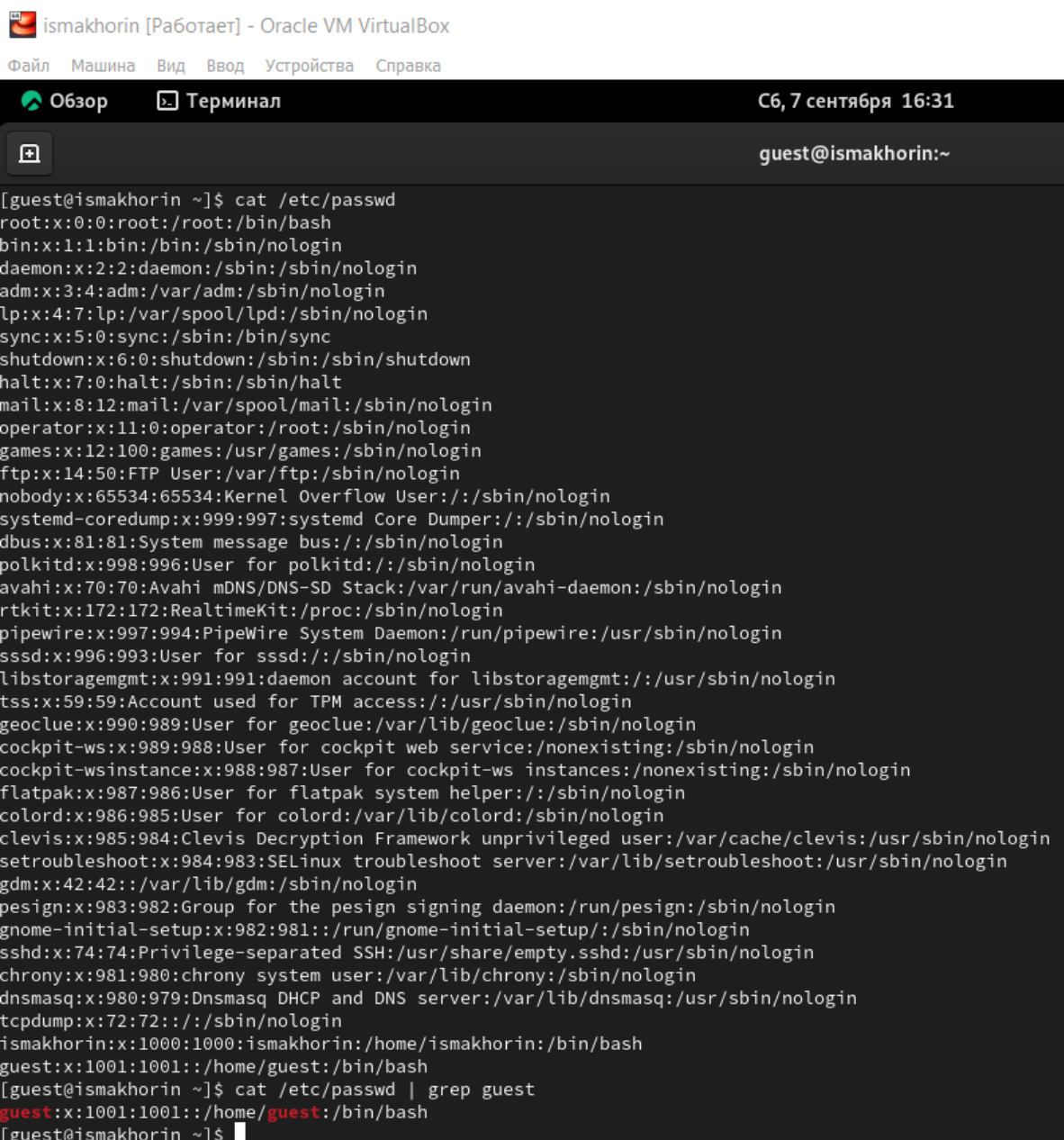
Рис. 3.6: id и groups

7. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки.



Рис. 3.7: Совпадение

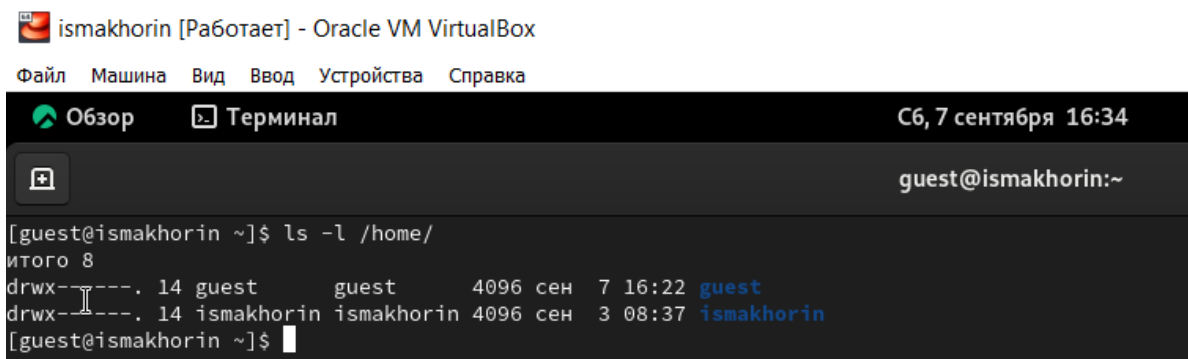
8. Следующим шагом посмотрим файл `/etc/passwd` командой `cat /etc/passwd`. Найдём в нём свою учётную запись, определим `uid` пользователя и `gid` пользователя. После чего сравним найденные значения с полученными в предыдущих пунктах.



```
ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Сб, 7 сентября 16:31
guest@ismakhorin:~
[guest@ismakhorin ~]$ 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
pipewire:x:997:994:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
sssd:x:996:993:User for sssd:/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/usr/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:985:984:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
setroubleshoot:x:984:983:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin
pesign:x:983:982:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:982:981:/:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
chrony:x:981:980:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:980:979:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
ismakhorin:x:1000:1000:ismakhorin:/home/ismakhorin:/bin/bash
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@ismakhorin ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@ismakhorin ~]$
```

Рис. 3.8: cat /etc/passwd

9. Определим существующие в системе директории командой: `ls -l /home/`



ismakhorin [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

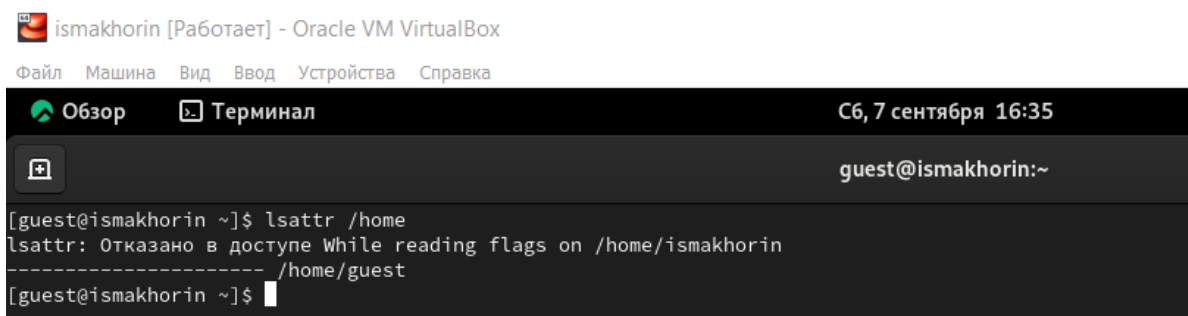
Обзор Терминал С6, 7 сентября 16:34

guest@ismakhorin:~

```
[guest@ismakhorin ~]$ ls -l /home/
итого 8
drwx-----. 14 guest      guest      4096 сен  7 16:22 guest
drwx-----. 14 ismakhorin ismakhorin 4096 сен  3 08:37 ismakhorin
[guest@ismakhorin ~]$
```

Рис. 3.9: ls -l /home/

10. Далее проверм, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: lsattr /home



ismakhorin [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал С6, 7 сентября 16:35

guest@ismakhorin:~

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

Рис. 3.10: lsattr /home

11. Создадим в домашней директории поддиректорию dir1 командой mkdir dir1 и определим командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

ismakhorin [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал С6, 7 сентября 16:40

guest@ismakhorin:~

```
[guest@ismakhorin ~]$ ls
dir1  Видео  Документы  Загрузки  Изображения  Музыка  Общедоступные  'Рабочий стол'  Шаблоны
[guest@ismakhorin ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 сен  7 16:36 dir1
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Видео
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Документы
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Загрузки
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Изображения
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Музыка
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Шаблоны
[guest@ismakhorin ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
[guest@ismakhorin ~]$ S
```

Рис. 3.11: mkdir dir1

12. Снимем с директории dir1 все атрибуты командой `chmod 000 dir1` и проверим с её помощью правильность выполнения команды `ls -l`.

ismakhorin [Работает] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

Обзор Терминал С6, 7 сентября 16:42

guest@ismakhorin:~

```
[guest@ismakhorin ~]$ chmod 000 dir1
[guest@ismakhorin ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен  7 16:36 dir1
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Видео
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Документы
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Загрузки
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Изображения
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Музыка
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен  7 16:22 Шаблоны
[guest@ismakhorin ~]$
```

Рис. 3.12: chmod 000 dir1

13. Попробуем создать в директории dir1 файл file1 командой: echo "test" > /home/guest/dir1/file1 Оценим, как сообщение об ошибке отразилось на создании файла: ls -l /home/guest/dir1

```

ismakhorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  С6, 7 сентября 16:44
guest@ismakhorin:~
[guest@ismakhorin ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@ismakhorin ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог '/home/guest/dir1': Отказано в доступе
[guest@ismakhorin ~]$
  
```

Рис. 3.13: “test” > /home/guest/dir1/file1

3.2 Заполнение таблицы 2.1

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

Права ди- ректо- рии	Права файла	Со- зда- ние файла	Уда- ление файла	За- пись в файл	Чте- ние файла	Сме- на ди- ректо- рии	Про- смотр фай- лов в ди- ректо- рии	Переиме- нование файла	Сме- на атри- бутов 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)	-	-	-	-	-	-	-	-
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)	-	-	+	-	+	+	-	+
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)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

3.3 Заполнение таблицы 2.2

15. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории `dir1`, заполним табл. 2.2.

Операция	Минималь- ные права на директорию	Минималь- ные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименова- ние файла	d(300)	(000)
Создание под- директории	d(300)	(000)

Удаление под-	d(300)	(000)
директории		

Таблица 2.2 “Минимальные права для совершения операций”

4 Вывод

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

5 Список литературы. Библиография

[1] Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

[2] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>