

# **Информационная безопасность. Отчет по лабораторной работе № 2**

**Дискреционное разграничение прав в Linux. Основные атрибуты**

Горбунова Ярослава Михайловна

# Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	16
4	Список литературы	17

# List of Figures

2.1	Создание учётной записи пользователя guest . . . . .	6
2.2	Задание пароля для пользователя guest . . . . .	6
2.3	Вход в систему от имени пользователя guest. Определение текущей директории. Переход в домашний каталог . . . . .	7
2.4	Имя, группа пользователя, группы, куда входит пользователь (команды id, groups) . . . . .	7
2.5	Просмотр файла /etc/passwd . . . . .	9
2.6	Существующие в системе поддиректорий директории /home/ . .	9
2.7	Существующие в системе поддиректорий директории /home/ . .	10
2.8	Права доступа и расширенные атрибуты для dir1. Снятие всех атрибутов с директории dir1 . . . . .	11
2.9	Попытка создания в директории dir1 файла file1. Проверка . . . .	12
2.10	Таблица 2.1. Установленные права и разрешённые действия (часть 1) . . . . .	13
2.11	Таблица 2.1. Установленные права и разрешённые действия (часть 2) . . . . .	14
2.12	Таблица 2.1. Установленные права и разрешённые действия (часть 3) . . . . .	14
2.13	Таблица 2.2. Минимальные права для совершения операций . . .	15

## List of Tables

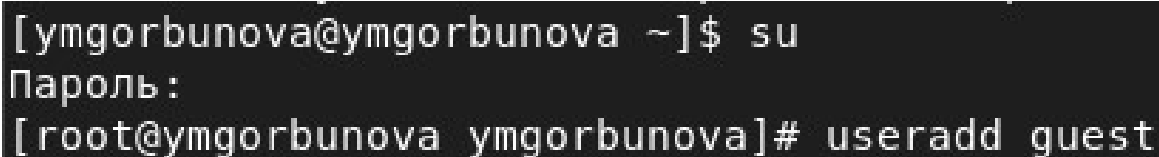
# 1 Цель работы

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 [1].

## 2 Выполнение лабораторной работы

Постарайтесь последовательно выполнить все пункты, занося ваши ответы на поставленные вопросы и замечания в отчёт [2].

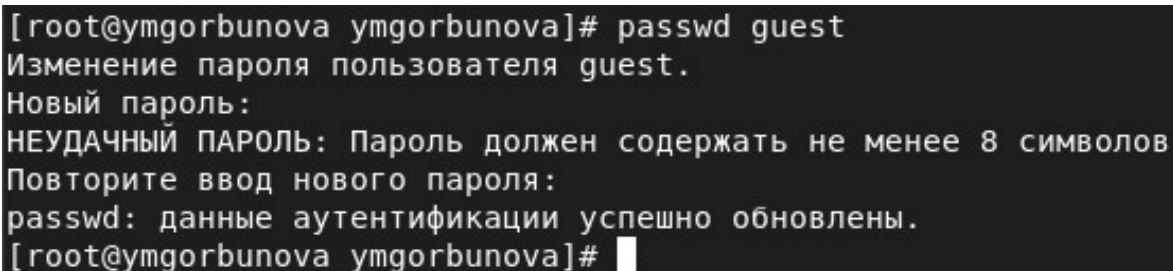
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора) (fig. 2.1): `useradd guest`



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

Figure 2.1: Создание учётной записи пользователя guest

2. Задайте пароль для пользователя guest (используя учётную запись администратора) (fig. 2.2): `passwd guest`



```
[root@ymgorbunova ymgorbunova]# 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.
[root@ymgorbunova ymgorbunova]#
```

Figure 2.2: Задание пароля для пользователя guest

3. Войдите в систему от имени пользователя guest (fig. 2.3).

4. Определите директорию, в которой вы находитесь, командой `pwd`. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию (fig. 2.3). – Директория, в которой мы находимся совпадает с приглашением командной строки, но не является домашней директорией, поэтому переходим в домашний каталог.

```
[root@ymgorbunova ymgorbunova]# su guest
[guest@ymgorbunova ymgorbunova]$ pwd
/home/ymgorbunova
[guest@ymgorbunova ymgorbunova]$ cd ~
[guest@ymgorbunova ~]$ pwd
/home/guest
[guest@ymgorbunova ~]$
```

Figure 2.3: Вход в систему от имени пользователя guest. Определение текущей директории. Переход в домашний каталог

5. Уточните имя вашего пользователя командой `whoami` (fig. 2.4).
6. Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомните. Сравните вывод `id` с выводом команды `groups` (fig. 2.4). – Вывод команды `id` дает больше информации о пользователе, в то время как команда `groups` дает информацию только о группах.

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

Figure 2.4: Имя, группа пользователя, группы, куда входит пользователь (команды `id`, `groups`)

7. Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. – В приглашении командной строки фигурирует то же имя пользователя, которое получено при просмотре вывода команды `id`.

8. Просмотрите файл `/etc/passwd` командой:

```
cat /etc/passwd
```

Найдите в нём свою учётную запись. Определите `uid` пользователя. Определите `gid` пользователя. Сравните найденные значения с полученными в предыдущих пунктах (fig. 2.5). – Найденные значения полностью совпадают с полученными на предыдущих шагах.

Замечание: в случае, когда вывод команды не умещается на одном экране монитора, используйте прокрутку вверх–вниз (удерживая клавишу `shift`, нажимайте `page up` и `page down`) либо программу `grep` в качестве фильтра для вывода только строк, содержащих определённые буквенные сочетания:

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



```
[guest@ymgorbunova ~]$ 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
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
sssd:x:997:993:User for sssd:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
geoclue:x:994:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:993:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:992:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
setroubleshoot:x:991:986:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:990:985:User for flatpak system helper:/sbin/nologin
colord:x:989:984:User for colord:/var/lib/colord:/sbin/nologin
clevis:x:988:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
systemd-oom:x:981:981:systemd Userspace OOM Killer:/usr/sbin/nologin
pesign:x:980:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin
gnome-initial-setup:x:979:979:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:978:978:/var/lib/chrony:/sbin/nologin
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
ymgorbunova:x:1000:1000:ymgorbunova:/home/ymgorbunova:/bin/bash
vboxadd:x:976:1:/var/run/vboxadd:/bin/false
guest:x:1001:1001:/home/guest:/bin/bash
```

Figure 2.5: Просмотр файла /etc/passwd

## 9. Определите существующие в системе директории командой (fig. 2.6)

`ls -l /home/`

Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях? – Удалось получить список поддиректорий. На обеих установлены полные права для пользователя, не установлены права для остальных пользователей.

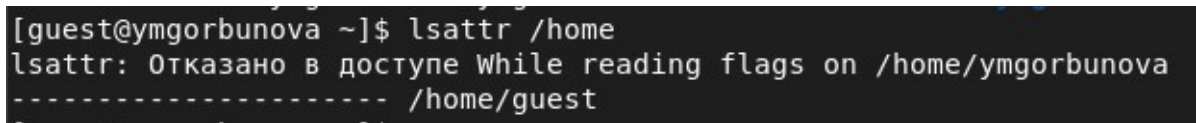
```
[guest@ymgorbunova ~]$ ls -l /home/
итого 4
drwx-----. 3 guest      guest      78 сен 13 14:39 guest
drwx-----. 14 ymgorbunova ymgorbunova 4096 сен 13 14:20 ymgorbunova
```

Figure 2.6: Существующие в системе поддиректорий директории /home/

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

```
lsattr /home
```

Удалось ли вам увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей? – Есть возможность увидеть расширенные атрибуты директории guest, но не удастся увидеть расширенные атрибуты директорий других пользователей.



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

Figure 2.7: Существующие в системе поддиректории директории /home/

11. Создайте в домашней директории поддиректорию dir1 командой

```
mkdir dir1
```

Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` (fig. 2.8). – На директорию были выставлены полные права доступа для пользователя и членов группы и права на чтение, исполнение для остальных пользователей. Никакие расширенные атрибуты не были выставлены.

12. Снимите с директории `dir1` все атрибуты командой

```
chmod 000 dir1
```

и проверьте с её помощью правильность выполнения команды (fig. 2.8)

```
ls -l
```

```

[guest@ymgorbunova ~]$ mkdir dir1
[guest@ymgorbunova ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 сен 13 15:48 dir1
[guest@ymgorbunova ~]$ lsattr
----- ./dir1
[guest@ymgorbunova ~]$ chmod 000 dir1
[guest@ymgorbunova ~]$ ks -l
bash: ks: command not found...
[guest@ymgorbunova ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 13 15:48 dir1

```

Figure 2.8: Права доступа и расширенные атрибуты для dir1. Снятие всех атрибутов с директории dir1

13. Попробуйте создать в директории dir1 файл file1 командой

```
echo "test" > /home/guest/dir1/file1
```

Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? – Отказ получен в силу того, что всем пользователям, даже обладателя, ограничены действия по чтению, записи, исполнению с директорией. Файл действительно не был создан.

Проверьте командой

```
ls -l /home/guest/dir1
```

действительно ли файл file1 не находится внутри директории dir1 (fig. 2.9).

```
[guest@ymgorbunova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@ymgorbunova ~]$ chmod u+rwx dir1
[guest@ymgorbunova ~]$ ls -l /home/guest/dir1
итого 0
[guest@ymgorbunova ~]$
```

Figure 2.9: Попытка создания в директории dir1 файла file1. Проверка

14. Заполните таблицу 2.1 «Установленные права и разрешённые действия», 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 «-» (fig. 2.10 - fig. 2.12).

Замечание 1: при заполнении табл. 2.1 рассматриваются не все атрибуты файлов и директорий, а лишь «первые три»: г, w, x, для «владельца». Остальные атрибуты также важны (особенно при использовании доступа от имени разных пользователей, входящих в те или иные группы). Проверка всех атрибутов при всех условиях значительно увеличила бы таблицу: так 9 атрибутов на директорию и 9 атрибутов на файл дают 218 строк без учёта дополнительных атрибутов, плюс таблица была бы расширена по количеству столбцов, так как все приведённые операции необходимо было бы повторить ещё как минимум для двух пользователей: входящего в группу владельца файла и не входящего в неё. После полного заполнения табл. 2.1 и анализа полученных данных нам удалось бы выяснить, что заполнение её в таком виде излишне. Можно разделить большую таблицу на несколько малых независимых таблиц. В данном примере предлагается рассмотреть 3+3 атрибута, т.е.  $2^6 = 64$  варианта.

Замечание 2: в ряде действий при выполнении команды удаления файла вы можете столкнуться с вопросом: «удалить защищённый от записи пустой обычный файл dir1/file1?» Обратите внимание, что наличие этого вопроса не позволяет сделать правильный вывод о том, что файл можно удалить. В ряде случаев,

при ответе «у» (да) на указанный вопрос, возможно получить другое сообщение:  
«невозможно удалить dirl /file1: Отказано в доступе».

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d---	---	-	-	-	-	-	-	-	-
d---	--x	-	-	-	-	-	-	-	-
d---	-w-	-	-	-	-	-	-	-	-
d---	-wx	-	-	-	-	-	-	-	-
d---	r--	-	-	-	-	-	-	-	-
d---	r-x	-	-	-	-	-	-	-	-
d---	rw-	-	-	-	-	-	-	-	-
d---	rwX	-	-	-	-	-	-	-	-
d-x	---	-	-	-	-	+	-	-	+
d-x	--x	-	-	-	-	+	-	-	+
d-x	-w-	-	-	+	-	+	-	-	+
d-x	-wx	-	-	+	-	+	-	-	+
d-x	r--	-	-	-	+	+	-	-	+
d-x	r-x	-	-	-	+	+	-	-	+
d-x	rw-	-	-	+	+	+	-	-	+
d-x	rwX	-	-	+	+	+	-	-	+
d-w-	---	-	-	-	-	-	-	-	-
d-w-	--x	-	-	-	-	-	-	-	-
d-w-	-w-	-	-	-	-	-	-	-	-
d-w-	-wx	-	-	-	-	-	-	-	-
d-w-	r--	-	-	-	-	-	-	-	-
d-w-	r-x	-	-	-	-	-	-	-	-
d-w-	rw-	-	-	-	-	-	-	-	-
d-w-	rwX	-	-	-	-	-	-	-	-

Figure 2.10: Таблица 2.1. Установленные права и разрешённые действия (часть 1)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d-wx	---	+	+	-	-	+	-	+	+
d-wx	--x	+	+	-	-	+	-	+	+
d-wx	-w-	+	+	+	-	+	-	+	+
d-wx	-wx	+	+	+	-	+	-	+	+
d-wx	r--	+	+	-	+	+	-	+	+
d-wx	r-x	+	+	-	+	+	-	+	+
d-wx	rw-	+	+	+	+	+	-	+	+
d-wx	rwX	+	+	+	+	+	-	+	+
dr--	---	-	-	-	-	-	+	-	-
dr--	--x	-	-	-	-	-	+	-	-
dr--	-w-	-	-	-	-	-	+	-	-
dr--	-wx	-	-	-	-	-	+	-	-
dr--	r--	-	-	-	-	-	+	-	-
dr--	r-x	-	-	-	-	-	+	-	-
dr--	rw-	-	-	-	-	-	+	-	-
dr--	rwX	-	-	-	-	-	+	-	-
dr-x	---	-	-	-	-	+	+	-	+
dr-x	--x	-	-	-	-	+	+	-	+
dr-x	-w-	-	-	+	-	+	+	-	+
dr-x	-wx	-	-	+	-	+	+	-	+
dr-x	r--	-	-	-	+	+	+	-	+
dr-x	r-x	-	-	-	+	+	+	-	+
dr-x	rw-	-	-	+	+	+	+	-	+
dr-x	rwX	-	-	+	+	+	+	-	+

Figure 2.11: Таблица 2.1. Установленные права и разрешённые действия (часть 2)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
drw-	---	-	-	-	-	-	+	-	-
drw-	--x	-	-	-	-	-	+	-	-
drw-	-w-	-	-	-	-	-	+	-	-
drw-	-wx	-	-	-	-	-	+	-	-
drw-	r--	-	-	-	-	-	+	-	-
drw-	r-x	-	-	-	-	-	+	-	-
drw-	rw-	-	-	-	-	-	+	-	-
drw-	rwX	-	-	-	-	-	+	-	-
drwx	---	+	+	-	-	+	+	+	+
drwx	--x	+	+	-	-	+	+	+	+
drwx	-w-	+	+	+	-	+	+	+	+
drwx	-wx	+	+	+	-	+	+	+	+
drwx	r--	+	+	-	+	+	+	+	+
drwx	r-x	+	+	-	+	+	+	+	+
drwx	rw-	+	+	+	+	+	+	+	+
drwx	rwX	+	+	+	+	+	+	+	+

Figure 2.12: Таблица 2.1. Установленные права и разрешённые действия (часть 3)

15. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2 (fig. 2.13).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d-wx	---
Удаление файла	d-wx	---
Чтение файла	d--x	r--
Запись в файл	d--x	-w-
Переименование файла	d-wx	---
Создание поддиректории	d-wx	---
Удаление поддиректории	d-wx	---

Figure 2.13: Таблица 2.2. Минимальные права для совершения операций

## **3 Выводы**

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.



## **4 Список литературы**

1. Задание к лабораторной работе № 2
2. Методические материалы курса