

**Отчёт по лабораторной работе №3.
Дискреционное разграничение прав в
Linux. Два пользователя**

дисциплина: Информационная безопасность

Рыбалко Элина Павловна

Содержание

Цель работы	5
Техническое обеспечение	6
Объект/Предмет исследования	7
Теоретическое введение	8
Выполнение лабораторной работы	9
Вывод	17
Список литературы	18

Список иллюстраций

1	Создание учётной записи	9
2	Задание пароля	9
3	Создание второй учётной записи	10
4	Добавление в группу	10
5	Определение директорий, уточнение имени, группы и id guest . .	11
6	Определение директорий, уточнение имени, группы и id guest2 .	11
7	Просмотр файла /etc/passwd	12
8	Регистрация в группу	12
9	Изменение прав директории	12
10	Снятие атрибутов	13
11	Проверка разрешённых операций	14
12	Проверка разрешённых операций	15
13	«Установленные права и разрешённые действия»	16
14	Минимальные права для совершения операций	16

Список таблиц

Цель работы

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

Техническое обеспечение

Лабораторная работа подразумевает наличие на виртуальной машине VirtualBox операционной системы Linux (дистрибутив Rocky или CentOS). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs.dk.sci.pfu.edu.ru/common/files/iso/).

Объект/Предмет исследования

Операционная система Linux.

Теоретическое введение

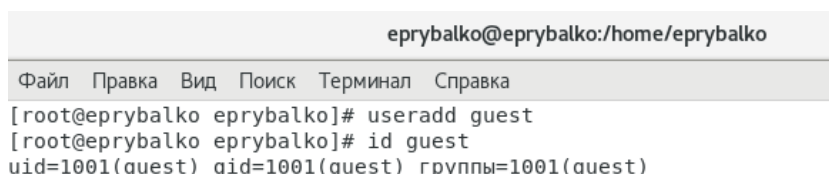
В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ. *discretion* — чье-либо усмотрение) — 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. [2].

Выполнение лабораторной работы

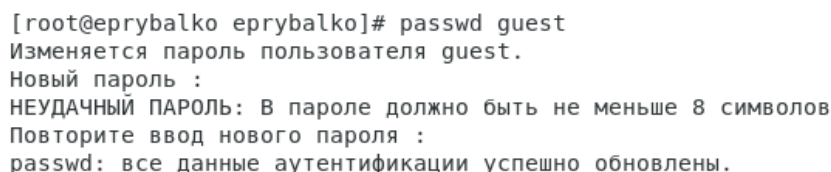
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора) (см. рис. -@fig:001).



```
eprybalko@eprybalko:/home/eprybalko
Файл Правка Вид Поиск Терминал Справка
[root@eprybalko eprybalco]# useradd guest
[root@eprybalko eprybalco]# id guest
uid=1001(guest) gid=1001(guest) группы=1001(guest)
```

Рис. 1: Создание учётной записи

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



```
[root@eprybalko eprybalco]# passwd guest
Изменяется пароль пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 2: Задание пароля

3. Аналогично создайте второго пользователя guest2.

```
[root@eprybalko eprybalko]# useradd guest2
[root@eprybalko eprybalko]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 8 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 3: Создание второй учётной записи

4. Добавьте пользователя guest2 в группу guest (см. рис. -@fig:004).

```
[root@eprybalko eprybalko]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
```

Рис. 4: Добавление в группу

5. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли.
6. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки (см. рис. -@fig:005, -@fig:006).

С приглашениями командной строки директории совпадают.

7. 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 (см. рис. -@fig:005, -@fig:006).

Информация команды groups с выводом команд id -Gn и id -G совпадает.

```
eprybalko@eprybalko:/h... x guest@eprybalko:~ x guest2@eprybalko:~ x
[eprybalko@eprybalko ~]$ su - guest
Пароль:
Последний вход в систему:Вт сен 13 15:09:24 MSK 2022на :1
[guest@eprybalko ~]$ pwd
/home/guest
[guest@eprybalko ~]$ whoami
guest
[guest@eprybalko ~]$ groups guest
guest : guest
[guest@eprybalko ~]$ id -Gn
guest
[guest@eprybalko ~]$ id -G
1001
```

Рис. 5: Определение директорий, уточнение имени, группы и id guest

```
eprybalko@eprybalko:/h... x guest@eprybalko:~ x guest2@eprybalko:~ x
[eprybalko@eprybalko ~]$ su - guest2
Пароль:
[guest2@eprybalko ~]$ pwd
/home/guest2
[guest2@eprybalko ~]$ whoami
guest2
[guest2@eprybalko ~]$ groups guest2
guest2 : guest2 guest
[guest2@eprybalko ~]$ id -Gn
guest2 guest
[guest2@eprybalko ~]$ id -G
1002 1001
```

Рис. 6: Определение директорий, уточнение имени, группы и id guest2

8. Сравните полученную информацию с содержимым файла /etc/group. Просмотрите файл командой (см. рис. -@fig:007).

Информация совпадает.



```
eprybalko@eprybalko:/h... x guest@eprybalko:~ x
kvm:x:36:qemu
qemu:x:107:
tss:x:59:
libvirt:x:986:
usbmuxd:x:113:
geoclue:x:985:
gluster:x:984:
gdm:x:42:
rpcuser:x:29:
nfsnobody:x:65534:
gnome-initial-setup:x:983:
sshd:x:74:
slocate:x:21:
avahi:x:70:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
tcpdump:x:72:
eprybalko:x:1000:eprybalko
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
```

Рис. 7: Просмотр файла /etc/passwd

9. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой `newgrp guest` (см. рис. -@fig:008).

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

Рис. 8: Регистрация в группу

10. От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rx /home/guest` (см. рис. -@fig:009).

```
[guest@eprybalko ~]$ chmod g+rx /home/guest
```

Рис. 9: Изменение прав директории

11. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` и проверьте правильность снятия атрибутов с помощью правильность выполнения команды `ls -l` (см. рис. -@fig:010).

```
[guest@eprybalko ~]$ chmod 000 dir1
[guest@eprybalko ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 13 15:32 dir1
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Загрузки
drwxr-xr-x. 2 guest guest 68 сен 13 15:19 Изображения
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Музыка
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Шаблоны
```

Рис. 10: Снятие атрибутов

12. Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, заполните табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-».

Сравните табл. 2.1 (из лабораторной работы № 2) и табл. 3.1. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем `guest2` операций внутри директории `dir1` и заполните табл. 3.2 (см. рис. -@fig:011, рис. -@fig:012, рис. -@fig:013 и рис. -@fig:014).

```
eprybalko@eprybalko:/h... x  guest@eprybalko:~ x  guest2@eprybalko:/hom... x
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Шаблоны
[guest@eprybalko ~]$ chmod 050 dir1
[guest@eprybalko ~]$ ls -l
итого 0
d---r-x---. 2 guest guest 19 сен 20 12:45 dir1
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Документы
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Загрузки
drwxr-xr-x. 2 guest guest 68 сен 13 15:19 Изображения
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Музыка
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Шаблоны
[guest@eprybalko ~]$ chmod 060 dir1
[guest@eprybalko ~]$ chmod 030 dir1
[guest@eprybalko ~]$ chmod 000 dir1
[guest@eprybalko ~]$ ls -l
итого 0
d------. 2 guest guest 19 сен 20 12:45 dir1
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Видео
drwxr-xr-x. 2 guest guest 6 сен 13 15:09 Документы
```

Рис. 11: Проверка разрешённых операций

```
eprybalko@eprybalko:/h... ×    guest@eprybalko:~ ×    guest2@eprybalko:/hom... ×
ls: невозможно открыть каталог .: Отказано в доступе
[guest2@eprybalko dir1]$ ls
ls: невозможно открыть каталог .: Отказано в доступе
[guest2@eprybalko dir1]$ mv file2 file1
[guest2@eprybalko dir1]$ ls -l
ls: невозможно открыть каталог .: Отказано в доступе
[guest2@eprybalko dir1]$ cat file1
cat: file1: Отказано в доступе
[guest2@eprybalko dir1]$ head file1
head: невозможно открыть «file1» для чтения: Отказано в доступе
[guest2@eprybalko dir1]$ ls -l
итого 4
-rw-r--r--. 1 guest2 guest 5 сен 20 12:43 file1
[guest2@eprybalko dir1]$ head file1
test
[guest2@eprybalko dir1]$ echo "test" > file1
[guest2@eprybalko dir1]$ head file1
test
[guest2@eprybalko dir1]$ echo "test2" > file1
[guest2@eprybalko dir1]$ head file1
test2
[guest2@eprybalko dir1]$ head file1
head: невозможно открыть «file1» для чтения: Отказано в доступе
[guest2@eprybalko dir1]$ echo "test2" > file1
bash: file1: Отказано в доступе
[guest2@eprybalko dir1]$ ls -l
ls: невозможно открыть каталог .: Отказано в доступе
[guest2@eprybalko dir1]$ mv file1 file
mv: не удалось получить доступ к «file»: Отказано в доступе
[guest2@eprybalko dir1]$ head file1
test2
```

Рис. 12: Проверка разрешённых операций

Права директории	d(000)	d----x--- (010)	d----w---- (020)	d----wx--- (030)	d---r----- (040)	d---r-x--- (050)	d---rw---- (060)	d---rwx--- (070)
Права файла	(000)	----x--- (010)	----w---- (020)	----wx--- (030)	---r----- (040)	---r-x--- (050)	---rw---- (060)	---rwx--- (070)
Создание файла	-	-	-	+	-	-	-	+
Удаление файла	-	-	-	+	-	-	-	+
Запись в файл	-	-	-	+	-	+	-	+
Чтение файла	-	-	-	+	-	+	-	+
Смена директории	-	+	-	+	-	+	-	+
Просмотр файлов в директории	-	-	-	-	-	+	-	+
Переименование файла	-	-	-	+	-	-	-	+
Смена атрибутов файла	-	+	-	+	-	+	-	+

Рис. 13: «Установленные права и разрешённые действия»

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	030
Удаление файла	030	030
Запись в файл	030	030
Чтение файла	030	030
Переименование файла	030	030
Создание поддиректории	030	030
Удаление поддиректории	030	030

Рис. 14: Минимальные права для совершения операций

Вывод

Приобрели практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Лабораторная работа №3
2. Дискреционное разграничение доступа Linux
3. Руководство по формуле Cmd Markdown
4. Руководство по оформлению Markdown файлов