

**Отчёт по лабораторной работе №2.
Дискреционное разграничение прав в
Linux. Основные атрибуты**

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	Вход в систему под новым пользователем	10
4	Определение директории	10
5	Уточнение имени пользователя	11
6	Уточнение имени и группы пользователя	11
7	Просмотр файла /etc/passwd	12
8	Просмотр файла /etc/passwd	12
9	Определение директорий	12
10	Просмотр расширенных атрибутов	13
11	Создание поддиректории, просмотр прав и атрибутов	13
12	Снятие атрибутов	14
13	Попытка создания файла	14
14	Проверка наличия файла	15
15	«Установленные права и разрешённые действия»	15
16	Минимальные права для совершения операций	16

Список таблиц

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.

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

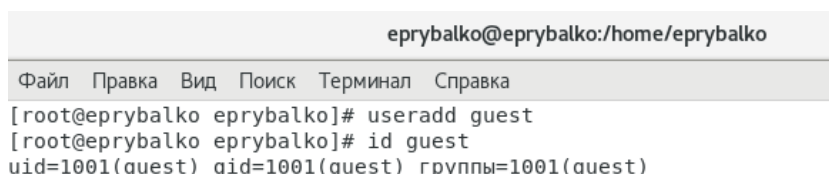
В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

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

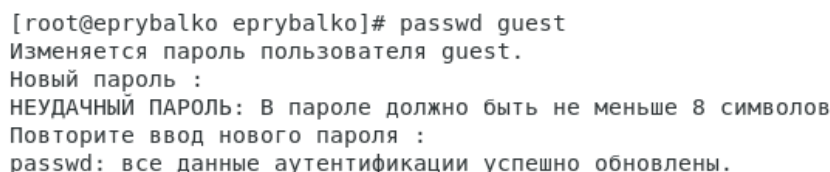
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора) (см. рис. -@fig:001).



```
eprybalko@eprybalko:/home/eprybalko
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@eprybalko eprybalako]# useradd guest
[root@eprybalko eprybalako]# 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 eprybalako]# 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. Войдите в систему от имени пользователя guest. (см. рис. -@fig:003).

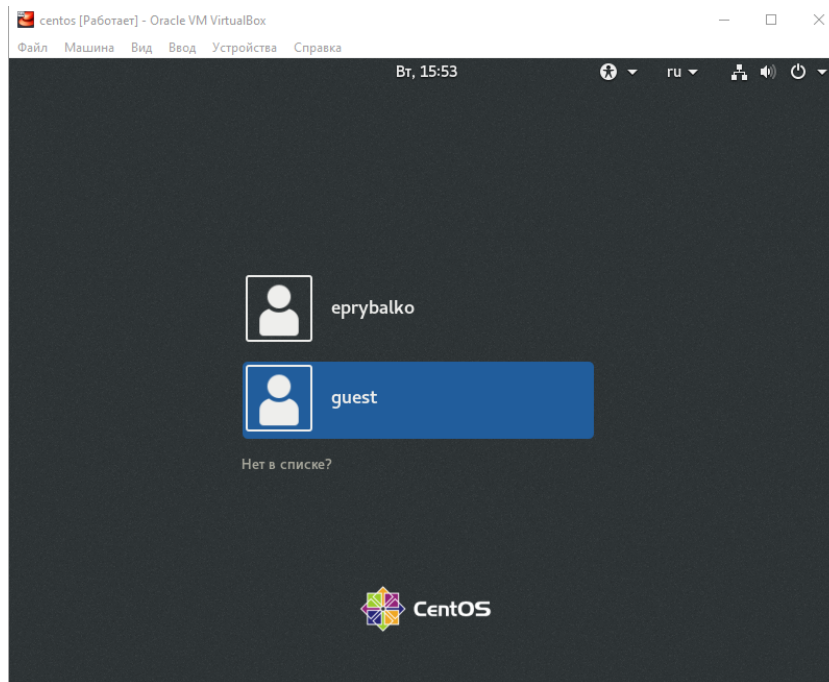


Рис. 3: Вход в систему под новым пользователем

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 (см. рис. -@fig:004).

Директория, в которой мы находимся совпадает с приглашением командной строки и с домашней директорией.

```
guest@eprybalko:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@eprybalko ~]$ pwd  
/home/guest  
[guest@eprybalko ~]$ echo ~  
/home/guest
```

Рис. 4: Определение директории

5. Уточните имя вашего пользователя командой `whoami` (см. рис. -@fig:005).

```
[guest@eprybalko ~]$ whoami  
guest
```

Рис. 5: Уточнение имени пользователя

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` (см. рис. -@fig:006).

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

Рис. 6: Уточнение имени и группы пользователя

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

Информация совпадает.

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 (см. рис. -@fig:007, -@fig:008).

```
guest@eprybalko:~  
Файл Правка Вид Поиск Терминал Справка  
setroubleshoot:x:994:991::/var/lib/setroubleshoot:/sbin/nologin  
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin  
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
radvd:x:75:75:radvd user:/:/sbin/nologin  
chrony:x:993:988::/var/lib/chrony:/sbin/nologin  
unbound:x:992:987:Unbound DNS resolver:/etc/unbound:/sbin/nologin  
qemu:x:107:107:qemu user:/:/sbin/nologin  
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sbin/nologin  
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/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  
gnome-initial-setup:x:989:983::/run/gnome-initial-setup:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
tcpdump:x:72:72::/sbin/nologin  
eprybalko:x:1000:1000:eprybalko:/home/eprybalko:/bin/bash  
vboxadd:x:988:1::/var/run/vboxadd:/bin/false  
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 7: Просмотр файла /etc/passwd

```
[guest@eprybalko ~]$ cat /etc/passwd | grep guest  
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 8: Просмотр файла /etc/passwd

9. Определите существующие в системе директории. (см. рис. -@fig:009). Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?

Список поддиректорий получить не удалось. Обе директории имеют права на чтение, запись и исполнение только для владельца директорий.

```
[guest@eprybalko ~]$ ls -l /home/  
итого 8  
drwx-----. 15 eprybalco eprybalco 4096 сен 13 11:35 eprybalco  
drwx-----. 3 guest      guest      78 сен 10 12:43 Eprybalco  
drwx-----. 15 guest      guest      4096 сен 13 15:10 guest  
drwx-----. 3          1002      1002      78 сен 13 15:00 quest
```

Рис. 9: Определение директорий

10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home (см. рис. -@fig:010). Удалось ли вам

увидеть расширенные атрибуты директории? Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?

Посмотреть расширенные атрибуты удалось только для пользователя guest. Они отсутствуют.

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

Рис. 10: Просмотр расширенных атрибутов

11. Создайте в домашней директории поддиректорию dir1. Определите командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (см. рис. -@fig:011). Созданная поддиректория имеет права на чтение, запись и исполнение для владельца директории и для группы, у остальных только на чтение и исполнение.

```
[guest@eprybalko ~]$ mkdir dir1
[guest@eprybalko ~]$ ls -l /home/guest
итого 0
drwxrwxr-x. 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
[guest@eprybalko ~]$ lsattr /home/guest
----- /home/guest/Рабочий стол
----- /home/guest/Загрузки
----- /home/guest/Шаблоны
----- /home/guest/Общедоступные
----- /home/guest/Документы
----- /home/guest/Музыка
----- /home/guest/Изображения
----- /home/guest/Видео
----- /home/guest/dir1
```

Рис. 11: Создание поддиректории, просмотр прав и атрибутов

12. Снимите с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверьте с её помощью правильность выполнения команды `ls -l` (см. рис. -@fig:012).

```
[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. 12: Снятие атрибутов

13. Попробуйте создать в директории `dir1` файл `file1`. Объясните, почему вы получили отказ в выполнении операции по созданию файла? Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1` действительно ли файл `file1` не находится внутри директории `dir1` (см. рис. -@fig:013 и рис. -@fig:014).

В связи с тем, что все атрибуты были сняты с поддиректории, то прав на создание файлов у нас нет.

```
[guest@eprybalko ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@eprybalko ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
```

Рис. 13: Попытка создания файла

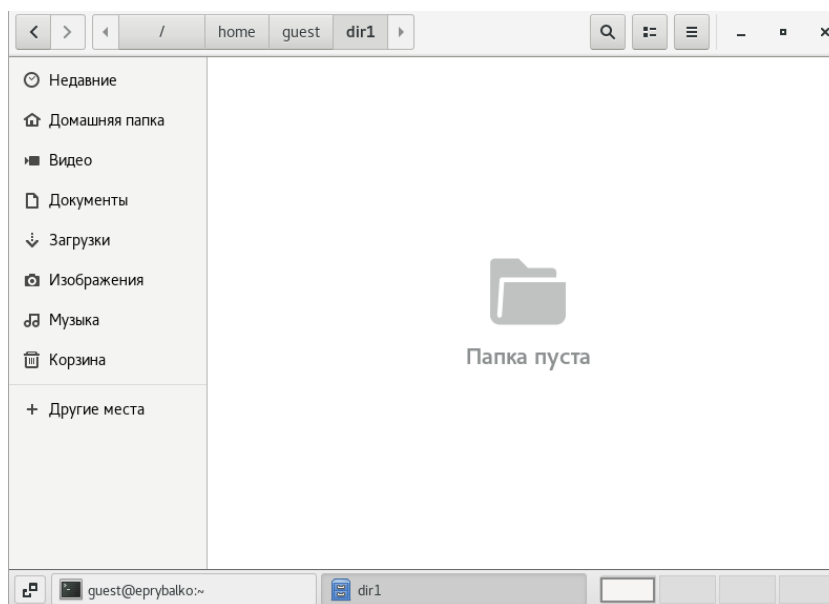


Рис. 14: Проверка наличия файла

14. Заполните таблицу «Установленные права и разрешённые действия» (см. рис. -@fig:015).

Права директории	d(000)	d--x----- (100)	d-w----- -(200)	d-wx----- (300)	dr----- (400)	dr-x----- (500)	drw----- -(600)	drwx----- (700)
Права файла	(000)	---x----- (100)	--w----- (200)	--wx----- (300)	-r----- (400)	-r-x----- (500)	-rw----- (600)	-rwx----- (700)
Создание файла	-	-	+	+	-	-	+	+
Удаление файла	-	-	+	+	-	-	+	+
Запись в файл	-	-	+	+	-	-	+	+
Чтение файла	-	-	-	-	+	+	+	+
Смена директории	-	+	-	+	-	+	-	+
Просмотр файлов в директории	-	-	-	-	+	+	+	+
Переименование файла	-	-	+	+	-	-	+	+
Смена атрибутов файла	-	+	-	+	-	+	-	+

Рис. 15: «Установленные права и разрешённые действия»

3. На основании заполненной таблицы определите те или иные минимально

необходимые права для выполнения операций внутри директории dir1 (см. рис. -@fig:016).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	200	200
Удаление файла	200	300
Запись в файл	200	200
Чтение файла	500	500
Смена директории	100	100
Просмотр файлов в директории	400	400
Переименование файла	200	200
Смена атрибутов файла	100	100

Рис. 16: Минимальные права для совершения операций

Вывод

Приобрели практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

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