

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Разин Никита Андреевич, НБИбд-402-18

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	14
	Список литературы	15

List of Tables

List of Figures

4.1	Рис 1. Команда <code>useradd guest1</code>	8
4.2	Рис 2. Вход в систему от имени пользователя <code>guest1</code>	9
4.3	Рис 3. Команда <code>cat /etc/passwd</code>	10
4.4	Рис 4. Список поддиректорий директории <code>/home</code>	10
4.5	Рис 4. Расширенные атрибуты, установленные на поддиректориях, находящихся в директории <code>/home</code>	11
4.6	Рис 5. Команды <code>mkdir dir1</code> и <code>ls -l</code>	11
4.7	Рис 6. Команда <code>lsattr</code>	11
4.8	Рис 7. Команда <code>chmod 000 dir1</code>	12
4.9	Рис 8. Попытка создания в директории <code>dir1</code> файла <code>file1</code>	12
4.10	Рис 9. Заполнение таблицы и проверка разрешённых действий . .	13

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.

2 Задание

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

3 Теоретическое введение

Для каждого каталога и файла вы можете задать права доступа. Точнее права доступа автоматически задаются при создании каталога (файла), а вы, при необходимости, можете их изменить. Какая может быть необходимость?

Например, вам нужно, чтобы к вашему файлу-отчету смогли получить доступ пользователи — члены вашей группы. Или вы создали обычный текстовый файл, содержащий инструкции командного интерпретатора. Чтобы этот файл стал сценарием, вам нужно установить право на выполнение для этого файла. [1]

Для записи кода режима доступа используется восьмеричная запись чисел. Как уже было отмечено, код доступа содержит три «триады» битов — для пользователя, группы и всех остальных, именно в таком порядке. Битам из первой триады соответствуют значения в восьмеричной записи 400, 200 и 100. Для второй триады (т. е. для группы) — 40, 20 и 10. Наконец, для третьей (все остальные) — 4, 2 и 1. В свою очередь, первому биту в каждой триаде соответствует доступ на чтение (r — «read»). Второму — на запись (w — «write») и третьему — на выполнение, т. е. x — «execute».[2]

4 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе с помощью команды `useradd guest` необходимо было создать нового пользователя `guest`, также я задал пароль и после данные аутентификации были успешно обновлены (рис. 1)

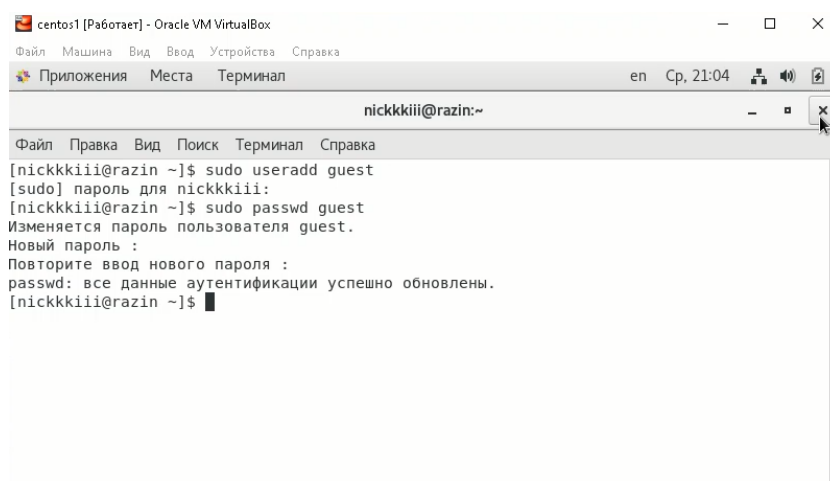
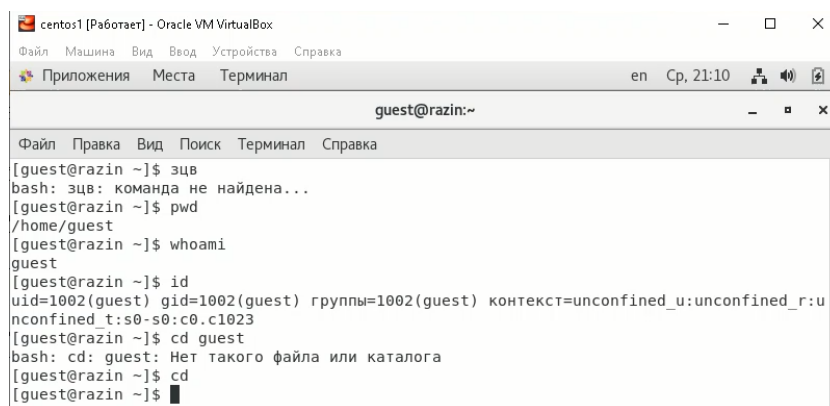


Figure 4.1: Рис 1. Команда `useradd guest`

После я вошел в систему от имени пользователя `guest`, запустил терминал, командой `pwd` определил директорию, в которой я находился, и именно она являлась моей домашней директорией, также уточнил имя пользователя командой `whoami` (рис. 2)

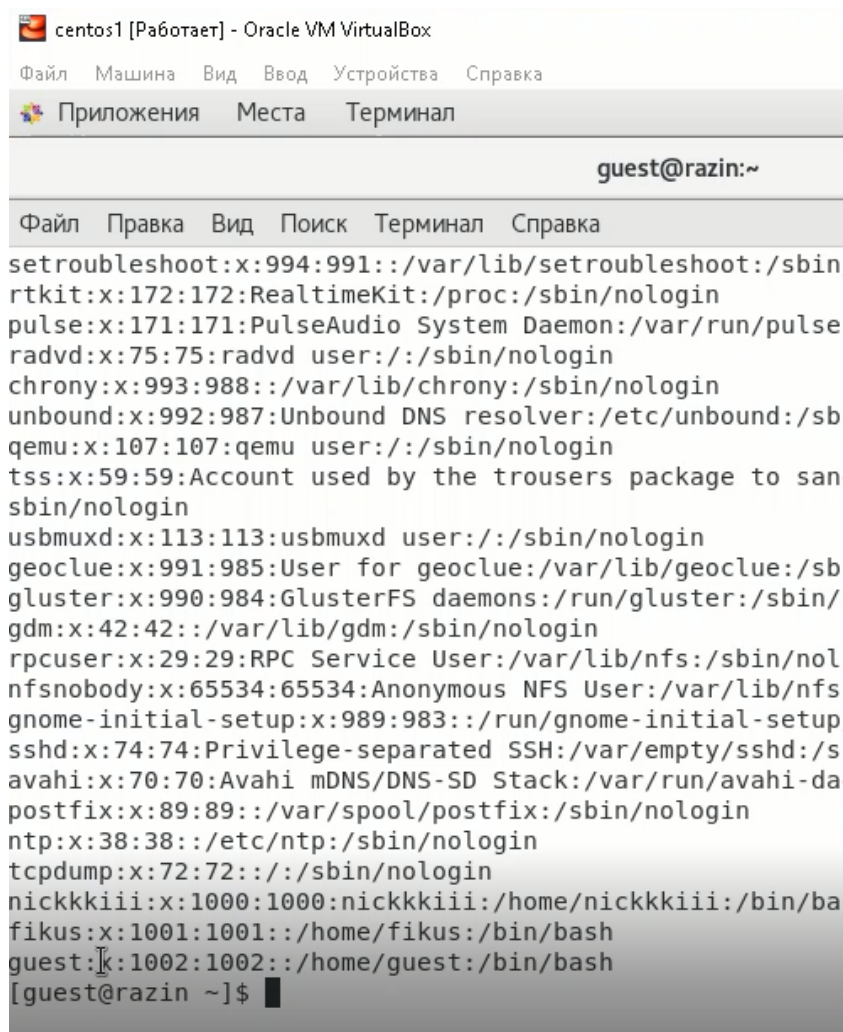


```
centos1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
en  Cp, 21:10
guest@razin:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[guest@razin ~]$ зцв
bash: зцв: команда не найдена...
[guest@razin ~]$ pwd
/home/guest
[guest@razin ~]$ whoami
guest
[guest@razin ~]$ id
uid=1002(guest) gid=1002(guest) группы=1002(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@razin ~]$ cd guest
bash: cd: guest: Нет такого файла или каталога
[guest@razin ~]$ cd
[guest@razin ~]$
```

Figure 4.2: Рис 2. Вход в систему от имени пользователя guest1

Я уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. запомнил.

Затем я просмотрел файл `/etc/passwd` командой `cat /etc/passwd` (рис. 3, нашел в нём свою учётную запись (рис. 3). `Uid` пользователя = 1002, `gid` пользователя = 1002. Эти значения совпадают с полученными ранее.



```
centos1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Приложения  Места  Терминал
guest@razin:~
Файл  Правка  Вид  Поиск  Терминал  Справка
setroubleshoot:x:994:991::/var/lib/setroubleshoot:/sbin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse
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:/sb
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to san
sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:991:985:User for geoclue:/var/lib/geoclue:/sb
gluster:x:990:984:GlusterFS daemons:/run/gluster:/sbin/
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nol
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs
gnome-initial-setup:x:989:983::/run/gnome-initial-setup
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/s
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-da
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
nickkkiii:x:1000:1000:nickkkiii:/home/nickkkiii:/bin/ba
fikus:x:1001:1001::/home/fikus:/bin/bash
guest:k:1002:1002::/home/guest:/bin/bash
[guest@razin ~]$
```

Figure 4.3: Рис 3. Команда cat /etc/passwd

Я определил существующие в системе директории командой `ls -l /home/` (рис. 4) и получил список поддиректорий директории /home.

```
[guest@razin ~]$ ls -l /home/
итого 12
drwx-----. 15 fikus      fikus      4096 сен 29 20:53 fikus
drwx-----. 15 guest      guest      4096 сен 29 21:05 guest
drwx-----. 15 nickkkiii nickkkiii 4096 сен 29 20:51 nickkkiii
[guest@razin ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/nickkkiii
lsattr: Отказано в доступе While reading flags on /home/fikus
----- /home/guest
```

Figure 4.4: Рис 4. Список поддиректорий директории /home

С помощью команды `lsattr /home` проверил, какие расширенные атрибуты

установлены на поддиректориях, находящихся в директории /home. Я смог рассмотреть расширенные атрибуты директории, но при этом я не смог увидеть атрибуты директорий у других пользователей. (рис. 4)

```
[guest@razin ~]$ ls -l /home/
итого 12
drwx-----. 15 fikus      fikus      4096 сен 29 20:53 fikus
drwx-----. 15 guest      guest      4096 сен 29 21:05 guest
drwx-----. 15 nickkkiii nickkkiii  4096 сен 29 20:51 nickkkiii
[guest@razin ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/nickkkiii
lsattr: Отказано в доступе While reading flags on /home/fikus
----- /home/guest
```

Figure 4.5: Рис 4. Расширенные атрибуты, установленные на поддиректориях, находящихся в директории /home

Далее я создал в домашней директории поддиректорию dir1, используя команду mkdir dir1. Определил командами ls -l (рис. 5).

```
[guest@razin ~]$ mkdir dir1
```

Figure 4.6: Рис 5. Команды mkdir dir1 и ls -l

```
[guest@razin ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Figure 4.7: Рис 6. Команда lsattr

После я снял с директории dir1 все атрибуты командой chmod 000 dir1 и проверила правильность выполнения команды с помощью команды lsattr. (рис. 14)

```

[guest@razin ~]$ chmod 000 dir1
[guest@razin ~]$ lsattr
----- ./.Рабочий стол
----- ./.Загрузки
----- ./.Шаблоны
----- ./.Общедоступные
----- ./.Документы
----- ./.Музыка
----- ./.Изображения
----- ./.Видео
lsattr: Отказано в доступе While reading flags on ./dir1

```

Figure 4.8: Рис 7. Команда chmod 000 dir1

Я попытался создать в директории dir1 файл file1 командой echo "test" > /home/guest1/dir1/file1. Я получил отказ в выполнении операции по созданию файла, потому что на предыдущем шаге я лишил владельца директории всех прав, включая право на запись. Я не смог создать файл. Проверила командой ls -l /home/guest/dir1, файл file1 действительно не находится внутри директории dir1. Потом же дал директории право 700 и попытался создать снова файл file1, на этот раз он создался и я проверил это с помощью команды ls внутри поддиректории. Этот файл служил непосредственно файлом для проведения с ним операций, результаты которых заносились в таблицу(рис. 8)

```

[guest@razin ~]$ chmod 700 dir1
[guest@razin ~]$ ls -l
итого 0
drwx-----. 2 guest guest 6 сен 29 21:19 dir1
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Видео
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Документы
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Изображения
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Музыка
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 29 21:05 Рабочий стол
[guest@razin ~]$ cd dir1
[guest@razin dir1]$ echo "test" > /h
[guest@razin dir1]$ ls
file1

```

Figure 4.9: Рис 8. Попытка создания в директории dir1 файла file1

После с помощью операций над расширением или урезанием прав на директорию и файл в нем, я проверял какие операции доступны для проведения над

файлом/директорией, а какие нет. (рис. 9)

	A	B	C	D	E	F	G	H	I	J	K
1	Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Присоединение файла к директории	Переименование файла	Смена атрибутов файла	Имя
2	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
3	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
4	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
5	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	Создание/Удаление/Переименование
6	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
7	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
8	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	-	
9	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
10	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
11	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
12	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
13	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
14	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
15	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
16	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
17	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
18	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
19	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
20	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
21	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
22	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
23	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
24	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
25	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
26	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	

Figure 4.10: Рис 9. Заполнение таблицы и проверка разрешённых действий

Ниже приведены скриншоты данной таблицы :

	A	B	C	D	E	F	G	H	I	J	K
1	Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Присоединение файла к директории	Переименование файла	Смена атрибутов файла	Имя
2	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
3	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
4	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
5	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	Создание/Удаление/Переименование/Изменение атрибутов
6	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
7	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
8	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	-	
9	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
10	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
11	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
12	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
13	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
14	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
15	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
16	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
17	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
18	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
19	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
20	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
21	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
22	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
23	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
24	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
25	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
26	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
27	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
28	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
29	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
30	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
31	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
32	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
33	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
34	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
35	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
36	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
37	Ф-м- (100)	----- (000)	+	+	-	-	+	-	-	+	
38	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
39	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
40	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
41	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
42	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
43	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
44	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
45	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
46	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
47	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
48	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
49	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
50	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
51	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
52	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
53	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
54	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
55	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
56	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
57	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
58	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
59	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
60	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
61	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
62	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
63	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
64	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	
65	Ф-м- (100)	----- (000)	-	-	-	-	+	-	-	-	

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения операций внутри директории dir1 и заполнила таблицу. Для заполнения последних двух строк опытным путем проверила минимальные права. (рис. 18)

Минимальные права для тех или иных операций сосредоточены в правом столбце **min**

5 Выводы

Я получил практические навыки работы в консоли с атрибутами файлов, а также закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Атрибуты файлов в Linux
2. Права доступа и атрибуты файла.