

Отчёт по лабораторной работе №2

Информационная безопасность

Дискреционное разграничение прав в Linux. Основные атрибуты.

Кармацкий Никита Сергеевич,
НФИбд-01-21, 1032210061

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.0.1	1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись пользователя guest	6
2.0.2	2. Зададим пароль пользователя guest	7
2.0.3	3. Войдем в систему от имени пользователя guest	8
2.0.4	4. Определим директорию, в которой мы находимся с помощью команды pwd. Сравним и определим является ли она нашей домашней директорией	9
2.0.5	5. Уточним имя нашего пользователя командой whoami.	10
2.0.6	6. Уточним группу пользователя, а так же группы в которые входит он. Сравним вывод команды id с выводом команды groups	11
2.0.7	7. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки	12
2.0.8	8. Просмотрим файл /etc/passwd и найдем в нем свою учетную запись и uid пользователя. Так же определим gid пользователя. Сравним значения с выводом предыдущих пунктов	13
2.0.9	9. Определим существующие в системе директории командой. Проверим какие права установлены на директории	14
2.0.10	10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home	15
2.0.11	12. Попытаемся создать файл в директории dir1 .	18

2.0.12	13. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории(файлов),определив опытным путём,какие операции разрешены, а какие нет.Если операция разрешена, занесем е втаблицу знак «+», если не разрешена, знак«-». . .	19
2.0.13	14. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1	23
3	Вывод	24
4	Список литературы. Библиография	25

Список иллюстраций

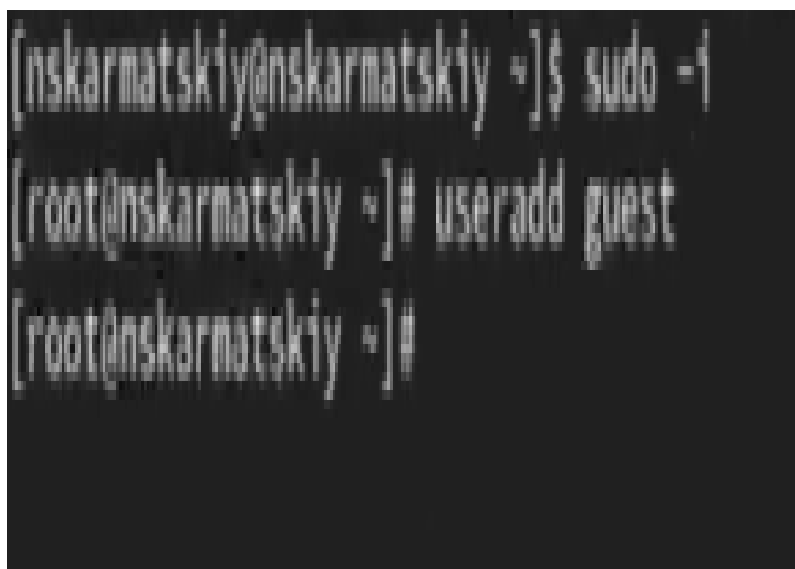
2.1	(рис. 1. Новый пользователь guest)	6
2.2	(рис. 2. Установка пароля для пользовател guest)	7
2.3	(рис. 3. Вход в систему под новым пользователем)	8
2.4	(рис. 4. Определение директории)	9
2.5	(рис. 5. Уточнение имени нашего пользователя)	10
2.6	(рис. 6. Уточнение группы пользователя)	11
2.7	(рис. 7. Сравнение данных)	12
2.8	(рис. 8. Просмотр файла /etc/passwd)	13
2.9	(рис. 9. Права на директориях)	14
2.10	(рис. 10. Проверка прав)	15
2.11	(рис. 10.1 Проверка расширенных атрибутов)	16
2.12	(рис. 11. Проверка атрибутов каталога)	17
2.13	(рис. 12. Попытка создания файла)	18
2.14	(рис. 13. Проверка доступных действий)	19

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 Выполнение лабораторной работы

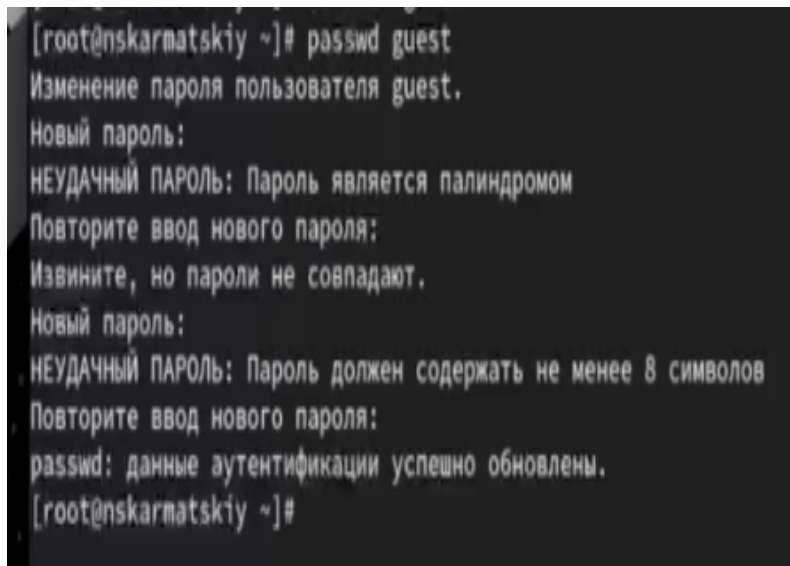
2.0.1 1. В установленной при выполнении предыдущей лабораторной работы операционной системе создаем учётную запись пользователя guest



```
[nskarmatskiy@nskarmatskiy ~]$ sudo -i
[root@nskarmatskiy ~]# useradd guest
[root@nskarmatskiy ~]#
```

Рис. 2.1: (рис. 1. Новый пользователь guest)

2.0.2 2. Зададим пароль пользователя guest



```
[root@nskarmatskiy ~]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля:
Извините, но пароли не совпадают.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@nskarmatskiy ~]#
```

Рис. 2.2: (рис. 2. Установка пароля для пользовател guest)

2.0.3 3. Войдем в систему от имени пользователя guest

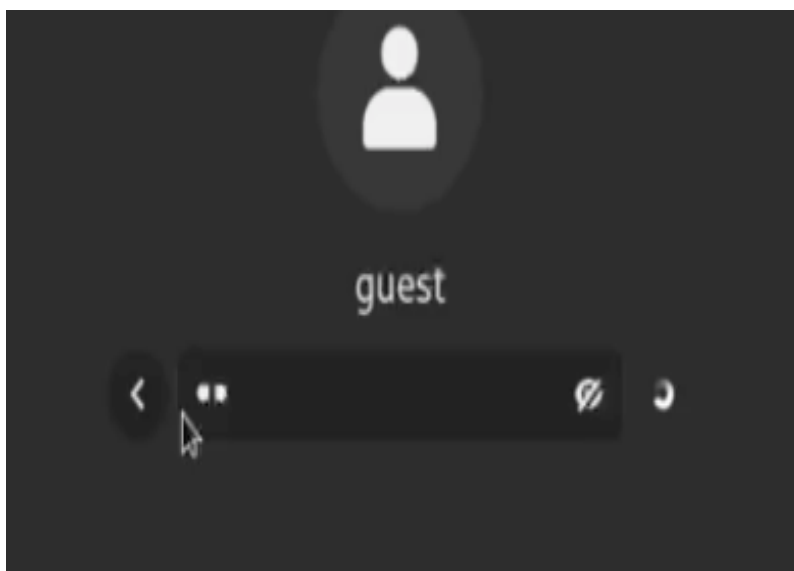


Рис. 2.3: (рис. 3. Вход в систему под новым пользователем)

2.0.4 4. Определим директорию, в которой мы находимся с помощью команды `pwd`. Сравним и определим является ли она нашей домашней директорией

```
[guest@nskarmatskiy ~]$ pwd
/home/guest
[guest@nskarmatskiy ~]$ ls
Видео      Загрузки  Музыка    'Рабочий стол'
Документы  Изображения  Общедоступные  Шаблоны
[guest@nskarmatskiy ~]$ cd
[guest@nskarmatskiy ~]$ cd ~
[guest@nskarmatskiy ~]$ pwd
/home/guest
[guest@nskarmatskiy ~]$
```

Рис. 2.4: (рис. 4. Определение директории)

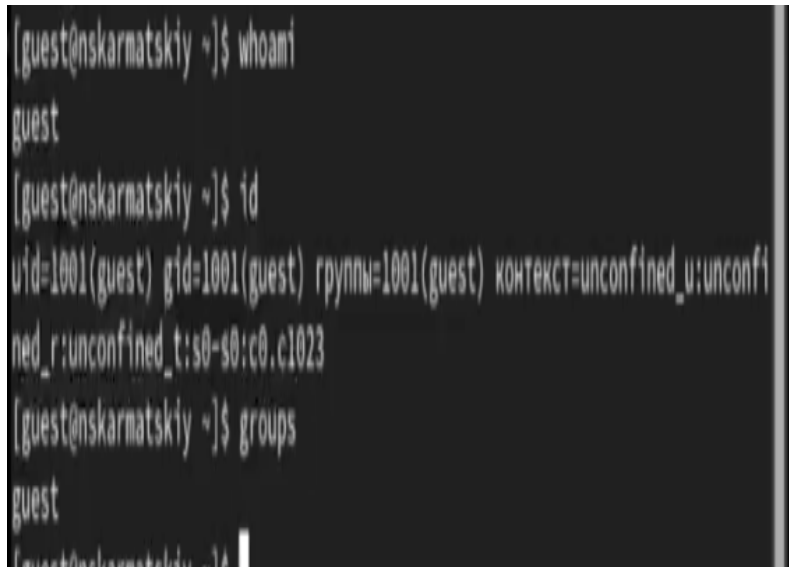
Мы находимся в той же директории, что и наша домашняя

2.0.5 5. Уточним имя нашего пользователя командой whoami.



Рис. 2.5: (рис. 5. Уточнение имени нашего пользователя)

2.0.6 6. Уточним группу пользователя, а так же группы в которые входит он. Сравним вывод команды `id` с выводом команды `groups`

A terminal window with a dark background and light-colored text. The prompt is [guest@nskarmatskiy ~]\$. The first command is whoami, which outputs guest. The second command is id, which outputs uid=1001(guest) gid=1001(guest) rpynm=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023. The third command is groups, which outputs guest.

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

Рис. 2.6: (рис. 6. Уточнение группы пользователя)

Выводы двух команд идентичны, никаких разностей нет

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

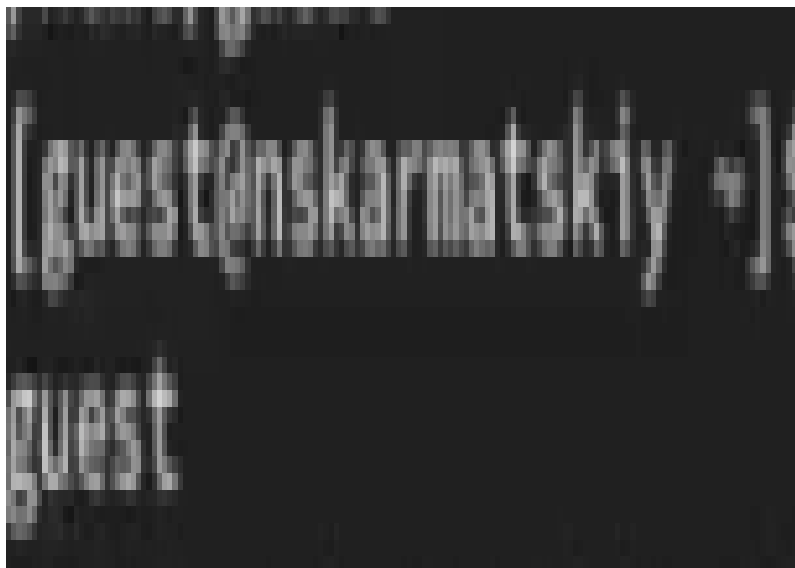


Рис. 2.7: (рис. 7. Сравнение данных)

Все верно, данные одинаковы

2.0.8 8. Просмотрим файл /etc/passwd и найдем в нем свою учетную запись и uid пользователя. Так же определим gid пользователя. Сравним значения с вывод предыдущих пунктов

```

[guest@nskarmatskiy ~]$ 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:996:996: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:996:983: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
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
clevis:x:984:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:983:982:/run/gnome-initial-setup:/sbin/nologin
pesign:x:982:981:Group for the pesign signing daemon:/run/pesign:/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
topdump:x:72:72:/t:/sbin/nologin
nskarmatskiy:x:1000:1000:nskarmatskiy:/home/nskarmatskiy:/bin/bash
guest:x:1001:1001:/home/guest:/bin/bash

```

Рис. 2.8: (рис. 8. Просмотр файла /etc/passwd)

gid: 1001 Значение с выводами предыдущих команд полностью идентичны

2.0.9 9. Определим существующие в системе директории командой. Проверим какие права установлены на директории

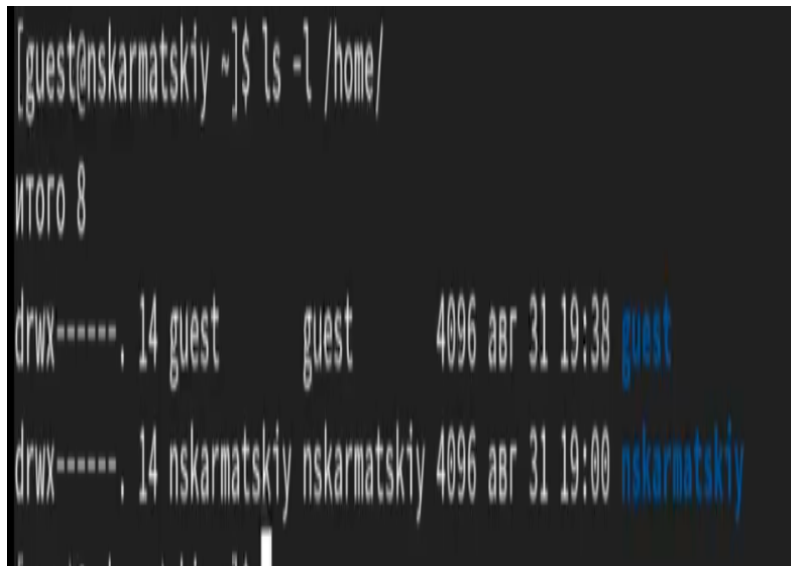


Рис. 2.9: (рис. 9. Права на директориях)

Права на директорию установлены только для пользователя, он может делать все в ней, для других пользователей(кроме root) действия с этим каталогом недоступны

2.0.10 10. Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home

```
[guest@nskarmatskiy ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 авг 31 19:45 dir1
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
```

Рис. 2.10: (рис. 10. Проверка прав)

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

Рис. 2.11: (рис. 10.1 Проверка расширенных атрибутов)

Для всех кроме пользователя недоступна запись в каталоги

Атрибуты никакие не стоят для каталогов ### 11. Создаем директорию dir1 и снимаем с директории все атрибуты


```
[guest@nskarmatskiy ~]$ chmod 000 dir1/  
[guest@nskarmatskiy ~]$ ls -l  
итого 0  
d-----, 2 guest guest 6 авг 31 19:45 dir1  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Видео  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Документы  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Загрузки  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Изображения  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Музыка  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Общедоступные  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 'Рабочий стол'  
drwxr-xr-x, 2 guest guest 6 авг 31 19:38 Шаблоны
```

Рис. 2.12: (рис. 11. Проверка атрибутов каталога)

2.0.11 12. Попробуем создать файл в директории dir1

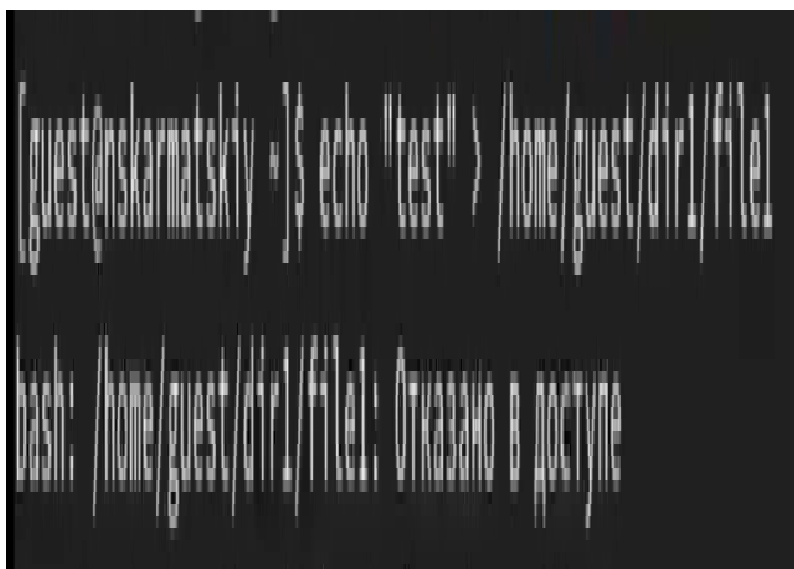


Рис. 2.13: (рис. 12. Попытка создания файла)

2.0.12 13. Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории(файлов),определив опытным путём,какие операции разрешены, а какие нет.Если операция разрешена, занесем е втаблицу знак «+», если не разрешена, знак«-».

```

bash: /home/guest/dir1/rfile: Отказано в доступе
[guest@nskarmatskiy ~]$ ls -l /home/guest/dir1/
ls: невозможно открыть каталог '/home/guest/dir1/': Отказано в доступе
[guest@nskarmatskiy ~]$ ls -l
итого 0
drwxr-xr-x. 2 guest guest 6 авг 31 19:45 dir1
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
[guest@nskarmatskiy ~]$ cd dir1/
bash: cd: dir1/: Отказано в доступе
[guest@nskarmatskiy ~]$ chmod 700 dir1/
[guest@nskarmatskiy ~]$ ls -l
итого 0
drwx-----. 2 guest guest 6 авг 31 19:45 dir1
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Видео
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Документы
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Загрузки
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Изображения
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Музыка
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Общедоступные
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 авг 31 19:38 Шаблоны
[guest@nskarmatskiy ~]$ cd dir1/
[guest@nskarmatskiy dir1]$ chmod 700 dir1/
chmod: невозможно получить доступ к 'dir1/': Нет такого файла или каталога
[guest@nskarmatskiy dir1]$

```

Рис. 2.14: (рис. 13. Проверка доступных действий)

Права ди- рек- то- рии	Права фай- ла	Создан- ла	Удален- ла	Запись в файл	Чтение фай- ла	Смена ди- рек- тории	Просмо- лов фай- ди- рек- то- рии	Преим- ва- ние фай- ла	Смена ат- ри- бу- тов фай- ла
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»

2.0.13 14. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории dir1

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

Таблица 2.2 “Минимальные права для совершения операций”

3 Вывод

Получены практических 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. Библиография

[1] Права доступа в ОС Linux - <https://codechick.io/tutorials/unix-linux/unix-linux-permissions> [2] Руководство по команде lsattr - https://rus-linux.net/MyLDP/consol/Linux_lsattr_command.html