Лабораторная работа No 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Кекишева Анастасия Дмитриевна

Содержание

Список таблиц

Список иллюстраций

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

1. Создатьучётную запись пользователя guest и задайть пароль и проделать последовательность команд, описанных в [1], которые направлены на изучения поведения прав дикерторий и файлов.
2. Заполнить таблицу «Установленные права и разрешённые действия»;
3. Заполнить таблицу «Минимально необходимые права для выполнения операций внутри директории».

3 Теоретическое введение

Дискреционное разграничение прав в Linux

Дискреционный подход к разграничение допсупа (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.

В рамках дискреционного разграничения доступа каждому файлу назначен пользователь-владелец и группа-владелец файла. Назначаются владельцы файлов при их создании — обычно пользователем — владельцем файла становится пользователь, создавший файл, а группой — владельцем файла становится его первичная группа.[2]

Атрибуты файлов в Linux

У каждого файла имеется определённый набор свойств в файловой системе. Например, это права доступа, владелец, имя, метки времени. В Linux каждый файл имеет довольно много свойств, например, права доступа устанавливаются трижды (для владельца, группы и всех прочих), метки времени также бывают трёх разных видов (время создание, доступа и изменения).[3]

Часть свойств файлов в текущей директории можно посмотреть командой: ls -l

Пример свойств одного из файлов:

-rw-rw-r– 1 mial users 262144 авг 18 15:04 custom-x.cramfs.img

- Первая группа из трех символов обозначает права доступа владельца файла или директории (u - user).
- Вторая группа из трех символов обозначает права доступа на файл или директорию для системной группы (g - group).
- Третья группа из трех символов обозначает права доступа на файл или директорию для всех остальных (o - other).

Каждая из трёх групп может содержать разный набор символов:

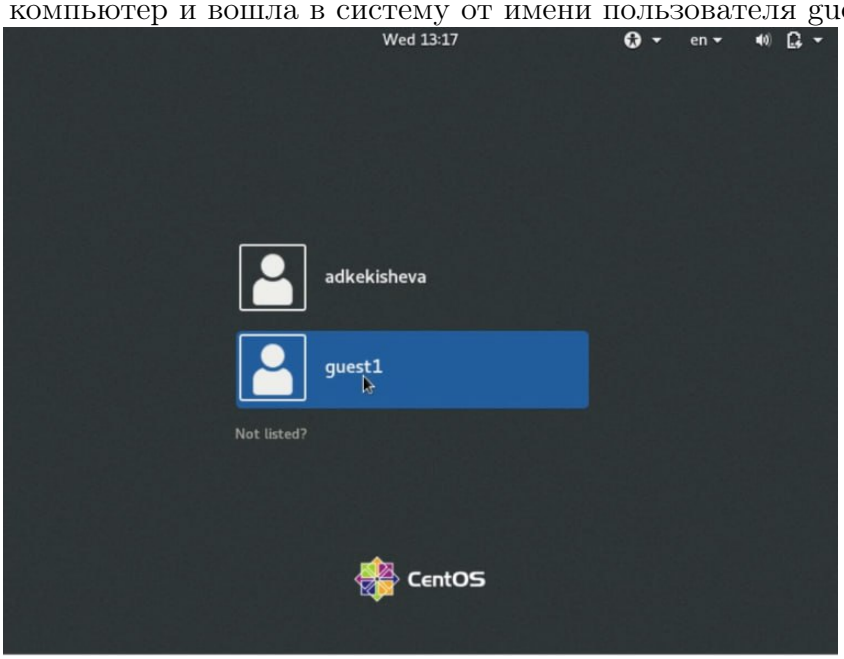
r - read, то есть, право доступа на чтение файла или директории. w - write, то есть, право на изменение и удаление файла или директории. x - execute, то есть, право на запуск файла как программы или вход в директорию.

4 Выполнение лабораторной работы

1. Создала учётную запись пользователя guest1 командой useradd guest.Также задала пароль для пользователя guest1 командой passwd guest1.(рис. @fig:001)

```
[root@adkekisheva ~]# useradd guest
useradd: user 'guest' already exists
[root@adkekisheva ~]# useradd guest1
[root@adkekisheva ~]# passwd guest1
Changing password for user guest1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

2. Перезагрузила компьютер и вошла в систему от имени пользователя guest1 (рис. @fig:002).



3. Определила директорию, в которой я нахожусь, командой pwd. Сравните её с приглашением командной строки: в приглашении командной строки у меня написано имя пользователя и нахожусь я в этой же директории, которая

находится в домашней. Также уточнила имя пользователя командой whoami (рис. @fig:003).

```
[guest1@adkekisheva ~]$ pwd
/home/guest1
[guest1@adkekisheva ~]$ whoami
guest1
```

4. Уточнила имя моего пользователя, его группу, а также группы, куда входит пользователь, командой id. Вышло, что uid = gid = 1002 (рис. @fig:004). Сравнила вывод id с выводом команды groups: команда groups выводит письменное название группы, а команда id выдела и числовой вариант и письменный.

```
[guest1@adkekisheva ~]$ id
uid=1002(guest1) gid=1002(guest1) groups=1002(guest1) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@adkekisheva ~]$ groups
guest1
```

Сравнила полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки: они идентичны.

6. Просмотрела файл /etc/passwd командой cat (рис. @fig:005).

```
[guest1@adkekisheva ~]$ 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:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:996:daemon account for libstoragemg
colord:x:997:995:User for colord:/var/lib/colord:/sbin/n
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologi
saned:x:996:994:SANE scanner daemon user:/usr/share/sane
saslauth:x:995:76:Saslauthd user:/run/saslauthd:/sbin/no
abrt:x:173:173::/etc/abrt:/sbin/nologin
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:/sbi
qemu:x:107:107:qemu user:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandb
```

7. С помощью команды grep нашла в файле свою учётную запись. Определить uid, gid пользователя не получилось, информации в файлов нет (рис. @fig:006).

```
[guest1@adkekisheva ~]$ cat /etc/passwd | grep guest1
guest1:x:1002:1002::/home/guest1:/bin/bash
[guest1@adkekisheva ~]$ cat /etc/passwd | grep uid
[guest1@adkekisheva ~]$ cat /etc/passwd | grep id
[guest1@adkekisheva ~]$ cat /etc/passwd | grep user
saned:x:996:994:SANE scanner daemon user:/usr/share/sane:/sbin/nologin
saslauth:x:995:76:Saslauthd user:/run/saslauthd:/sbin/nologin
radvd:x:75:75:radvd user:/:/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
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
[guest1@adkekisheva ~]$ cat /etc/passwd | grep group
[guest1@adkekisheva ~]$ cat /etc/passwd | grep gid
```

8. Определила существующие в системе директории командой ls -l /home/. Мне удалось получить список поддиректорий директории /home. На всех дикреториях уснановлены права чтения, записи и запуска только для владельца, ни группы, никто другой не имеет доступа к ним (рис. @fig:006).

```
[guest1@adkekisheva ~]$ ls -l /home/
total 8
drwx------. 21 adkekisheva adkekisheva 4096 Sep 13 13:16 adkekisheva
drwx------.  3 guest       guest         78 Sep 13 13:06 guest
drwx------. 15 guest1      guest1      4096 Sep 13 13:17 guest1
[guest1@adkekisheva ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/adkekisheva
lsattr: Permission denied While reading flags on /home/guest
---------------- /home/guest1
```

9. Проверила, какие расширенные атрибуты установлены на поддиректо- риях, находящихся в директории /home, командой lsattr /home (рис. @fig:007). Мне удалось увидеть расширенные атрибуты директории – их нет, все минусы. Расширенные атрибуты директорий других пользователей мне не доступны – доступ запрещён.

10. Создала в домашней директории поддиректорию dir1 командой mkdir dir1 и определила командами ls -l и lsattr, какие права доступа и расширенные атрибуты были выставлены на директорию dir1 (рис. @fig:008). Как видим, папку dir1 нельзя только изменять остальным пользователям, для груп и владельца разрешены все действия, а расширенных атрибутов нет.

```
[guest1@adkekisheva ~]$ mkdir dir1
[guest1@adkekisheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Desktop
drwxrwxr-x. 2 guest1 guest1 6 Sep 13 13:36 dir1
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Documents
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Downloads
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Music
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Pictures
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Public
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Templates
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Videos
[guest1@adkekisheva ~]$ lsattr
---------------- ./Desktop
---------------- ./Downloads
---------------- ./Templates
---------------- ./Public
---------------- ./Documents
---------------- ./Music
---------------- ./Pictures
---------------- ./Videos
---------------- ./dir1
```

11. Сняла с директории dir1 все атрибуты командой chmod 000 dir1 и проверила правильность выполнения команды ls -l (рис. @fig:009). Как видим, команда выполнилась верно – прав на папку нет ни у кого.

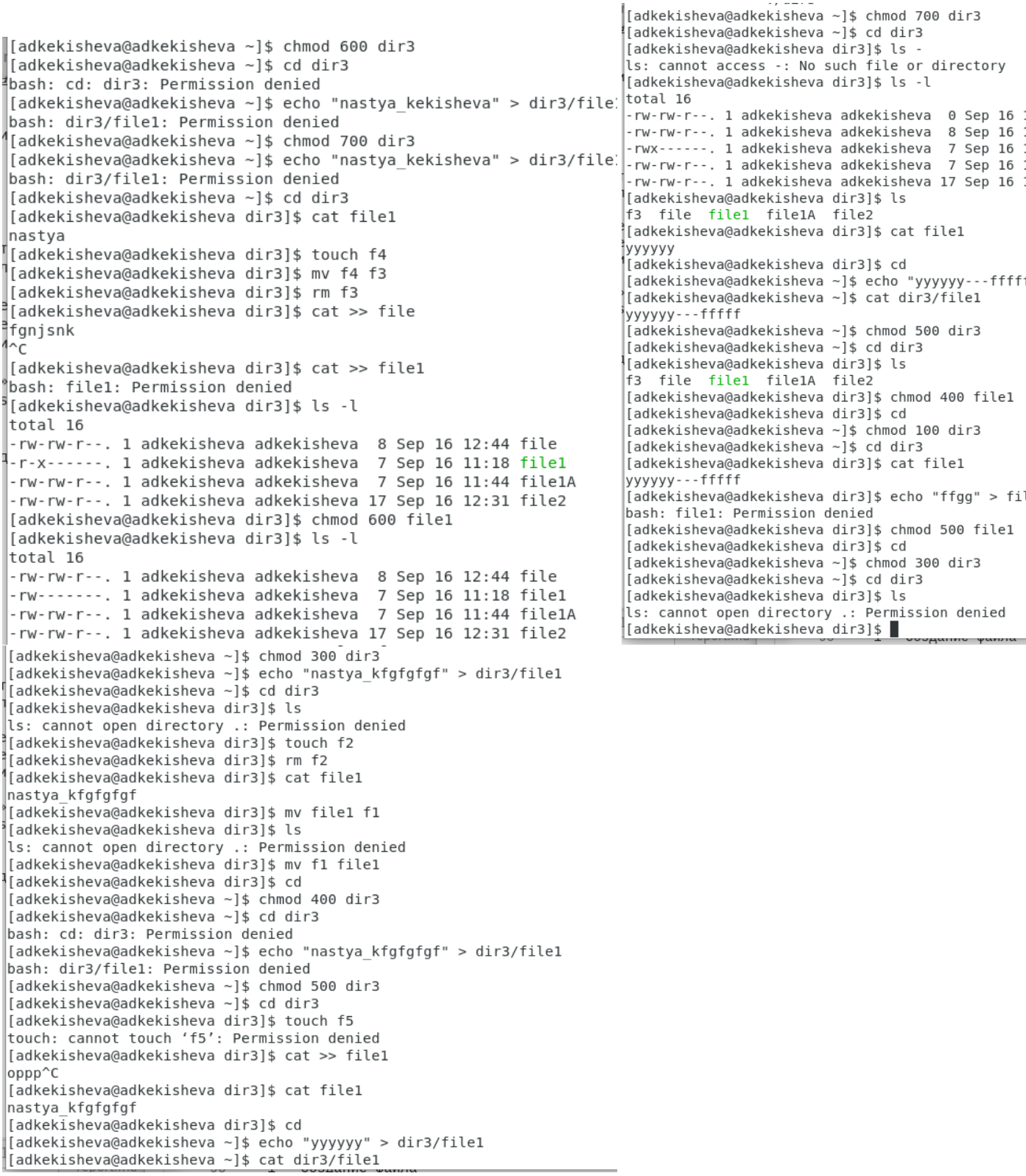
```
[guest1@adkekisheva ~]$ chmod 000 dir1
[guest1@adkekisheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Desktop
d---------. 2 guest1 guest1 6 Sep 13 13:36 dir1
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Documents
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Downloads
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Music
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Pictures
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Public
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Templates
drwxr-xr-x. 2 guest1 guest1 6 Sep 13 13:17 Videos
[guest1@adkekisheva ~]$ echo "hello" > /home/guest1/dir1/file1
bash: /home/guest1/dir1/file1: Permission denied
[guest1@adkekisheva ~]$ ls -l /home/guest1/dir1
ls: cannot open directory /home/guest1/dir1: Permission denied
```

12. Попыталась создать в директории dir1 файл file1 командой echo “test” > /home/guest/dir1/file1, но получила отказ в выполнении, это произошло, так как мы выполни команду chmod 000, которая убрала все наши права на папку и сделала невозможным создание в ней файла. Провела командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1. Точно сказать так нельзя, так как в ошибке он не вывел, что нет такой папки, он просто сказал, что нам отклонено в доступе (рис. @fig:009).

13. Заполнила таблицу «Установленные права и разрешённые действия» @tbl:001 Прверяла права экспериментным пуём, командами touch, mv, rm, ls, ls -l, lsattr, действия представлены на рис. @fig:010, @fig:011, @fig:012, @fig:013, @fig:014. Понятно, что ту не все действия, которые я произвела, но принцип и подход был везде одинаков.

```
[adkekisheva@adkekisheva ~]$ chmod 100 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekisheva@adkekisheva dir3]$ cat file1
nastya
[adkekisheva@adkekisheva dir3]$ ls
ls: cannot open directory .: Permission denied
[adkekisheva@adkekisheva dir3]$ touch f2
touch: cannot touch ‘f2’: Permission denied
[adkekisheva@adkekisheva dir3]$ mv file1 f4
mv: cannot move ‘file1’ to ‘f4’: Permission denied
[adkekisheva@adkekisheva dir3]$ cd
[adkekisheva@adkekisheva ~]$ lsattr
---------------- ./Desktop
---------------- ./Downloads
---------------- ./Templates
---------------- ./Public
---------------- ./Documents
---------------- ./Music
---------------- ./Pictures
---------------- ./Videos
---------------- ./gitflow-installer.sh
---------------- ./gitflow
---------------- ./work
---------------- ./biblatex-ms-4.0.tds.tgz
---------------- ./dir2
lsattr: Permission denied While reading flags on ./dir3
[adkekisheva@adkekisheva ~]$ chmod 300 dir3
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ touch f2
[adkekisheva@adkekisheva dir3]$ mv f2 f3
[adkekisheva@adkekisheva dir3]$ rm f3
[adkekisheva@adkekisheva dir3]$ cat file1
nastya
[adkekisheva@adkekisheva dir3]$ touch f2
```

```
[adkekisheva@adkekisheva ~]$ chmod 200 dir
[adkekisheva@adkekisheva ~]$ cd dir3
bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ cat dir3/file
cat: dir3/file1: Permission denied
[adkekisheva@adkekisheva ~]$ chmod 400 dir
[adkekisheva@adkekisheva ~]$ cd dir3
bash: cd: dir3: Permission denied
[adkekisheva@adkekisheva ~]$ echo "nastya_
bash: dir3/file2: Permission denied
[adkekisheva@adkekisheva ~]$ lsattr
---------------- ./Desktop
---------------- ./Downloads
---------------- ./Templates
---------------- ./Public
---------------- ./Documents
---------------- ./Music
---------------- ./Pictures
---------------- ./Videos
---------------- ./gitflow-installer.sh
---------------- ./gitflow
---------------- ./work
---------------- ./biblatex-ms-4.0.tds.tgz
---------------- ./dir2
---------------- ./dir3
[adkekisheva@adkekisheva ~]$ chmod 500 dir
[adkekisheva@adkekisheva ~]$ cd dir3
[adkekisheva@adkekisheva dir3]$ ls
file1  file1A  file2
[adkekisheva@adkekisheva dir3]$ cat file1
nastya
[adkekisheva@adkekisheva dir3]$ touch f3
touch: cannot touch ‘f3’: Permission denie
[adkekisheva@adkekisheva dir3]$ ls
file1  file1A  file2
[adkekisheva@adkekisheva dir3]$ ls -l
total 12
-r-x------. 1 adkekisheva adkekisheva  7 S
```

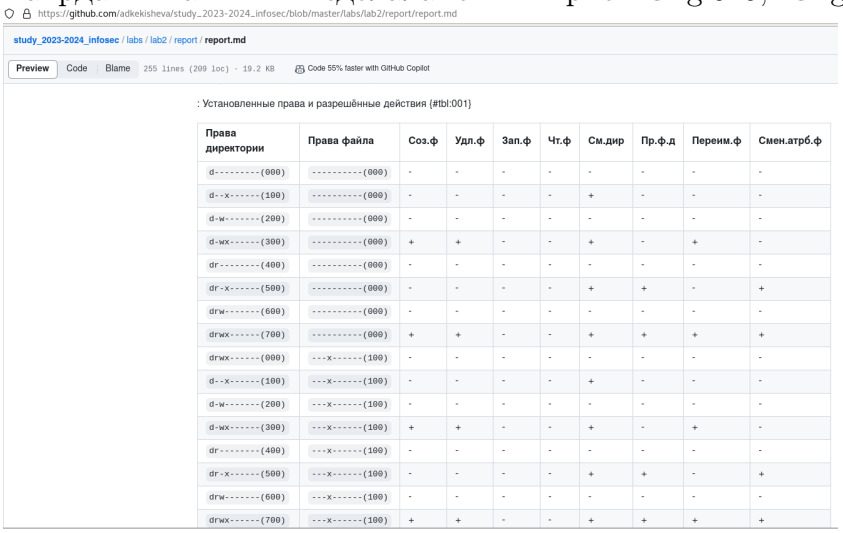


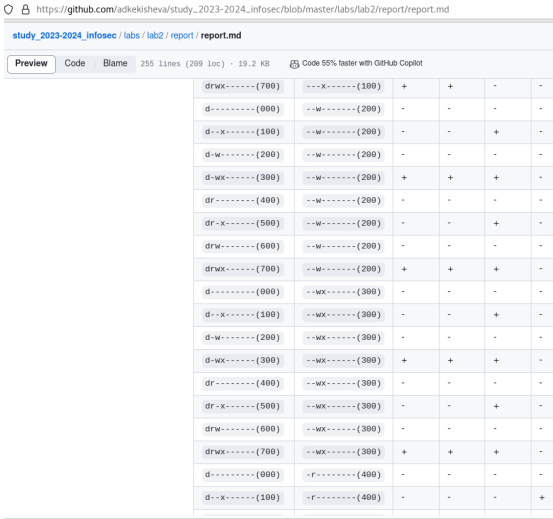
: Установленные права и разрешённые действия {#tbl:001} |Права директо-

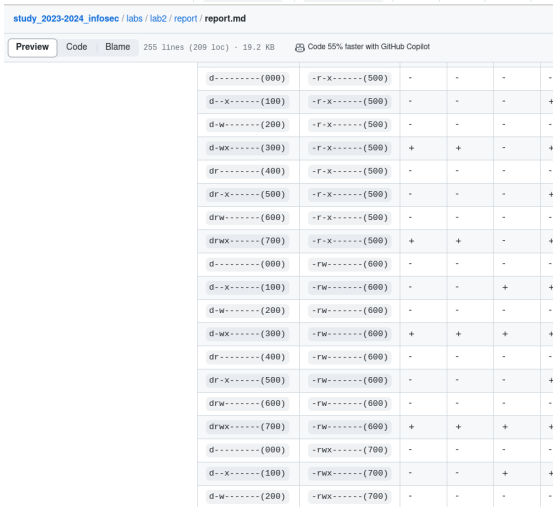
рии|Права файла|Соз.ф|Удл.ф|Зап.ф|Чт.ф|См.дир|Пр.ф.д|Переим.ф|Смен.атрб.ф|
|:—|:—|—|—|—|—|—|—|—|—| |d---------(000)|----------(000)|-|-|-|-|-|-|-|-| |d--x------(100)|---------(000)|-|-|-|-|+|-|-|-| |d-w-------(200)|----------(000)|-|-|-|-|-|-|-|-| |d-wx------(300)|---------(000)|+|+|-|-|+|-|+|-| |dr--------(400)|----------(000)|-|-|-|-|-|-|-|-| |dr-x------(500)|----------(000)|-|-|-|-|+|+|-|+| |drw-------(600)|----------(000)|-|-|-|-|-|-|-|-| |drwx------(700)|----------(000)|+|+|-|-|+|+|+|+| |drwx------(000)|---x------(100)|-|-|-|-|-|-|-|-| |d--x------(100)|---x------(100)|-|-|-|-|+|-|-|-| |d-w-------(200)|---x------(100)|-|-|-|-|-|-|-|-| |d-wx------(300)|---x------(100)|+|+|-|-|+|-|+|-| |dr--------(400)|---x------(100)|-|-|-|-|-|-|-|-| |dr-x------(500)|---x------(100)|-|-|-|-|+|+|-|+| |drw-------(600)|---x------(100)|-|-|-|-|-|-|-|-| |drwx------(700)|---x------(100)|+|+|-|-|+|+|+|+| |d---------(000)|--w-------(200)|-|-|-|-|-|-|-|-| |d--x------(100)|--w-------(200)|-|-|+|-|+|-|-|-| |d-w-------(200)|--w-------(200)|-|-|-|-|-|-|-|-| |d-wx------(300)|--w-------(200)|+|+|+|-|+|-|+|-| |dr--------(400)|--w-------(200)|-|-|-|-|-|-|-|-| |dr-x------(500)|--w-------(200)|-|-|+|-|+|+|-|+| |drw-------(600)|--w-------(200)|-|-|-|-|-|-|-|-| |drwx------(700)|--w-------(200)|+|+|+|-|+|+|+|+| |d---------(000)|--wx------(300)|-|-|-|-|-|-|-|-| |d--x------(100)|--wx------(300)|-|-|+|-|+|-|-|-| |d-w-------(200)|--wx------(300)|-|-|-|-|-|-|-|-| |d-wx------(300)|--wx------(300)|+|+|+|-|+|-|+|-| |dr--------(400)|--wx------(300)|-|-|-|-|-|-|-|-| |dr-x------(500)|--wx------(300)|-|-|+|-|+|+|-|+| |drw-------(600)|--wx------(300)|-|-|-|-|-|-|-|-| |drwx------(700)|--wx------(300)|+|+|+|-|+|+|+|+| |d---------(000)|-r--------(400)|-|-|-|-|-|-|-|-| |d--x------(100)|-r--------(400)|-|-|-|+|+|-|-|-| |d-w-------(200)|-r--------(400)|-|-|-|-|-|-|-|-| |d-wx------(300)|-r--------(400)|+|+|-|+|+|-|+|-| |dr--------(400)|-r--------(400)|-|-|-|-|-|-|-|-| |dr-x------(500)|-r--------(400)|-|-|-|+|+|+|-|+| |drw-------(600)|-r--------(400)|-|-|-|-|-|-|-|-| |drwx------(700)|-r--------(400)|+|+|-|+|+|+|+|+| |d---------(000)|-r-x------(500)|-|-|-|-|-|-|-|-| |d--x------(100)|-r-x------(500)|-|-|-|+|+|-|-|-| |d-w-------(200)|-r-x------(500)|-|-|-|-|-|-|-|-| |d-wx------(300)|-r-x------(500)|+|+|-|+|+|+|-|+| |dr--------(400)|-r-x------(500)|-|-|-|-|-|-|-|-| |dr-x------(500)|-r-x------(500)|-|-|-|+|+|+|-|+| |drw-------(600)|-r-x------(500)|-|-|-|-|-|-|-|-| |drwx------(700)|-r-x------(500)|+|+|-|+|+|+|+|+| |d---------(000)|-rw-------(600)|-|-|-|-|-|-|-|-| |d--x------(100)|-rw-------(600)|-|-|+|+|+|-|-|-| |d-w-------(200)|-rw-------(600)|-|-|-|-|-|-|-|-| |d-wx------(300)|-rw-------(600)|+|+|+|+|+|-|+|-| |dr--------(400)|-rw-------(600)|-|-|-|-|-|-|-|-| |dr-x------(500)|-rw-------(600)|-|-|-|+|+|+|-|+| |drw-------(600)|-rw-------(600)|-|-|-|-|-|-|-|-|

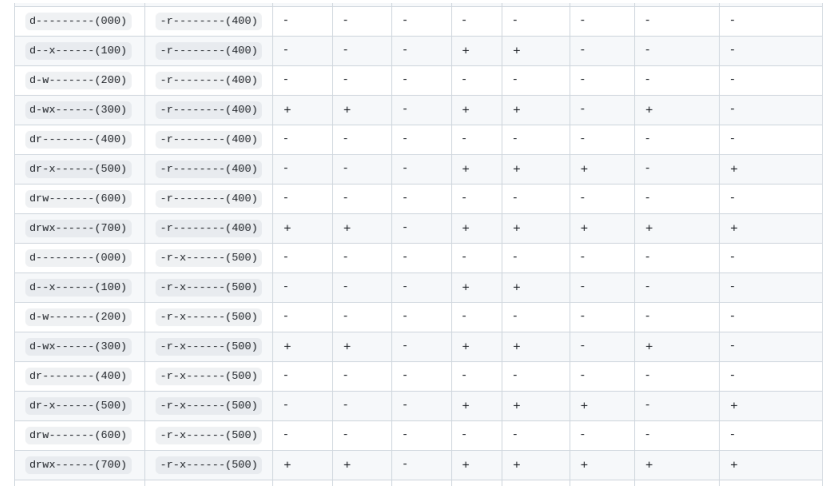
|-| |drwx------(700)|-rw-------(600)|+|+|+|+|+|+|+|+| |d---------(000)|-rwx------(700)|-|-|-|-|-|-|-|-| |d--x------(100)|-rwx------(700)|-|-|+|+|+|-|-|-| |d-w-------(200)|-rwx------(700)|-|-|-|-|-|-|-|-| |d-wx------(300)|-rwx------(700)|+|+|+|+|+|-|+|-| |dr--------(400)|-rwx------(700)|-|-|-|-|-|-|-|-| |dr-x------(500)|-rwx------(700)|-|-|+|+|+|+|-|+| |drw-------(600)|-rwx------(700)|-|-|-|-|-|-|-|-| |drwx------(700)|-rwx------(700)|+|+|+|+|+|+|+|+|

Таблица неконвертируется из-за пандока поэтому я сначала загрузила макрдайн на гит и сделала скины рис. @fig:015, @fig:016, @fig:017, @fig:018.









Далее на основе предыдущей таблицы составила таб.@tbl:002 Минимальные права для совершения операций {#tbl:002}

Операция	Права на директорию	Права на файл
Создание файла	d-wx------ (300)	---------- (000)
Удаление файла	d-wx------ (300)	---------- (000)
Чтение файла	d--x------ (100)	-r-------- (400)
Запись в файл	d--x------ (100)	--w------- (200)
Переименование файла	d-wx------ (300)	----------(000)
Создание поддиректории	d-wx------ (300)	---------- (000)
Удаление поддиректории	d-wx------ (300)	---------- (000)

5 Выводы

1. Создала учётную запись пользователя guest и задайть пароль и проделать последовательность команд, описанных в [1], которые направлены на изучения поведения прав дикерторий и файлов.
2. Заполнила таблицу «Установленные права и разрешённые действия»;
3. Заполнила таблицу «Минимально необходимые права для выполнения операций внутри директории».

Список литературы

1. Лабораторная работа No 4. Дискреционное разграничение прав в Linux. Расширенные атрибуты [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/2090411/r lab_discret_attr.pdf.
2. Терминал Linux. Права доступа к каталогам и файлам в Linux, команды chmod и chown [Электронный ресурс].URL: https://linuxrussia.com/terminal-chmod-chown.html.
3. Обработка Атрибутов Файлов [Электронный ресурс]. URL: http://linux.yaroslavl.ru/docs/setup attr.html.