

Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Калинина Кристина Сергеевна

Содержание

Цель работы	5
Теоретические сведения	6
Выполнение лабораторной работы	8
Выводы	14
Список литературы	15

List of Figures

0.1	Создание учетной записи пользователя guest2	8
0.2	Добавление пользователя guest2 в группу guest	8
0.3	Вход в систему от двух пользователей	9
0.4	Использование команды whoami, id и pwd	9
0.5	Уточнение группы пользователя, и тех, кто также входит в эту группу	9
0.6	Просмотр файла '/etc/group'	10
0.7	Регистрация пользователя guest2 в группе guest	10
0.8	Изменение прав директории '/home/guest'	11
0.9	Процесс заполнения таблицы	11
0.10	Таблица «Установленные права и разрешённые действия для групп»	12
0.11	Таблица “Минимальные права для совершения операций от имени пользователей входящих в группу”	13

List of Tables

Цель работы

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

Теоретические сведения

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. [1]

Для каждого файла в Linux задается набор разрешений. Разрешения могут быть следующими:

- `r` — `read` — возможность открытия и чтения файла. Для директории это возможность просматривать содержимое директории.
- `w` — `write` — возможность изменения файла. Для директории это возможность добавлять, удалять или переименовывать файлы в директории.
- `x` — `execute` — возможность выполнения файла (запуска файла). [2]

Набор разрешений состоит из 3 блоков `rwX`:

- Первый блок `rwX` определяет права доступа для владельца-пользователя.

- Второй блок `gwx` определяет права доступа для владельца-группы.
- Третий блок `gwx` определяет права доступа для всех остальных. [2]

Для каждого файла или директории в Linux задаются права доступа. Они задаются тремя атрибутами: набором разрешений, именем владельца, именем группы.

Набор разрешений — это три блока прав доступа: права доступа для владельца файла, права доступа для группы, права доступа для всех остальных.

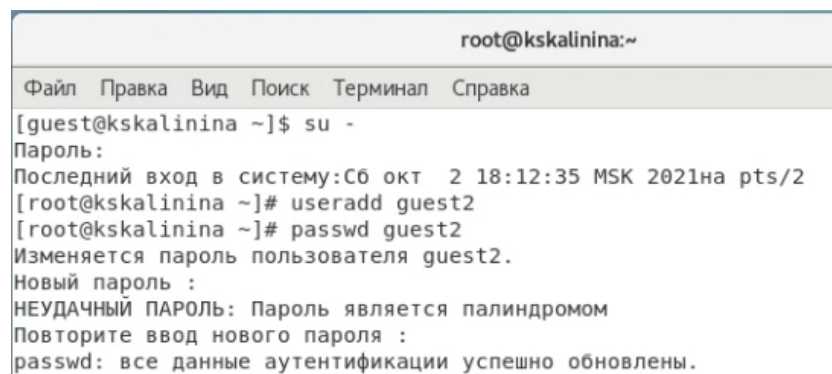
Разрешения записываются символами `r`, `w`, `x`.

Набор разрешений состоит из трех блоков и записывается в виде трех `gwx`, записанных друг за другом в виде одного «слова».

Если какая-либо возможность отключена (запрещена), то вместо соответствующего символа в наборе разрешений ставится прочерк (символ минус). [2]

Выполнение лабораторной работы

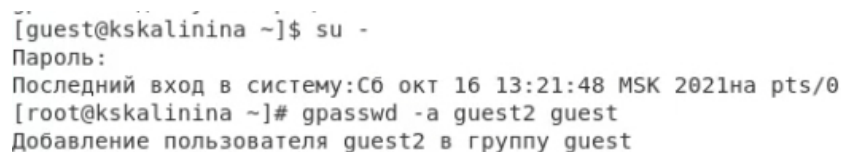
1. В установленной при выполнении предыдущей лабораторной работы операционной системе вошла в учётную запись пользователя guest и создала пользователя guest2, а также задала ему пароль (fig. 0.1).



```
root@kskalinina:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@kskalinina ~]$ su -  
Пароль:  
Последний вход в систему:Сб окт  2 18:12:35 MSK 2021на pts/2  
[root@kskalinina ~]# useradd guest2  
[root@kskalinina ~]# passwd guest2  
Изменяется пароль пользователя guest2.  
Новый пароль :  
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом  
Повторите ввод нового пароля :  
passwd: все данные аутентификации успешно обновлены.
```

Figure 0.1: Создание учетной записи пользователя guest2

2. Добавила пользователя guest2 в группу guest (fig. 0.2).



```
[guest@kskalinina ~]$ su -  
Пароль:  
Последний вход в систему:Сб окт 16 13:21:48 MSK 2021на pts/0  
[root@kskalinina ~]# gpasswd -a guest2 guest  
Добавление пользователя guest2 в группу guest
```

Figure 0.2: Добавление пользователя guest2 в группу guest

3. Осуществила вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (fig. 0.3).


```

guest@kskalinina:~
[guest@kskalinina ~]$ su -
Пароль:
Последний вход в систему:Сб окт  2 18:12:35 MSK 2021на pts/2
[root@kskalinina ~]# useradd guest2
[root@kskalinina ~]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@kskalinina ~]# exit
logout
[guest@kskalinina ~]$

guest2@kskalinina:/home/guest
[guest@kskalinina ~]$ su guest2
Пароль:
[guest2@kskalinina guest]$

```

Figure 0.3: Вход в систему от двух пользователей

- Для обоих пользователей командой `pwd` определила директорию, в которой я нахожусь. Убедилась в том, что в командной строке отображается тоже самое. Также проверила имя пользователя и основную информацию (fig. 0.4).

```

root@kskalinina:~
Пароль:
Последний вход в систему:Сб окт  2 18:12:35 MSK 2021на pts/2
[root@kskalinina ~]# su guest2
[guest2@kskalinina ~]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль является палиндромом
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@kskalinina ~]# exit
logout
[guest@kskalinina ~]$ pwd
/home/guest

guest2@kskalinina:/home/guest
[guest@kskalinina ~]$ su guest2
Пароль:
[guest2@kskalinina guest]$ pwd
/home/guest
[guest2@kskalinina guest]$ whoami
guest2
[guest2@kskalinina guest]$ id
uid=1002(guest2) gid=1002(guest2) rpyнны=1002(guest2)
nfinеd u:unconfined r:unconfined t:s0-s0:c0.c1023
[guest2@kskalinina guest]$ gpasswd -a guest2 guest2

```

Figure 0.4: Использование команды `whoami`, `id` и `pwd`

- Определила командами `'groups guest'` и `'groups guest2'`, в какие группы входят пользователи `guest` и `guest2`. Команды `'id -Gn'` и `'id -G'` показали `id` групп и их именования для пользователя, на котором я нахожусь. Информация оказалась аналогичной той, что вывелась после команды `'groups'` (fig. 0.5).

```

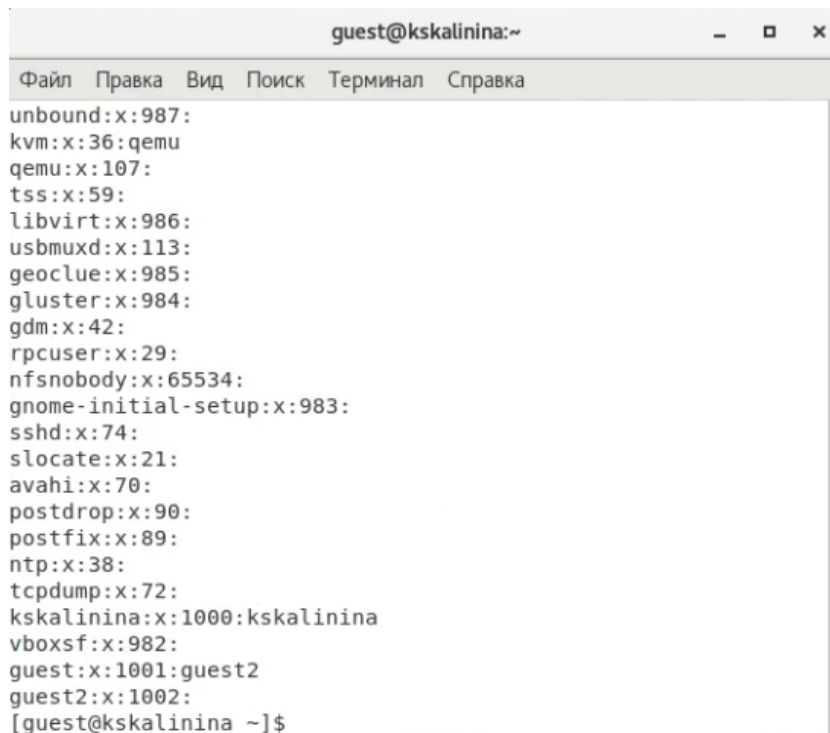
guest@kskalinina:~
/home/guest
[guest@kskalinina ~]$ whoami
guest
[guest@kskalinina ~]$ id
uid=1001(guest) gid=1001(guest) rpyнны=1001(guest) контекст=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023
[guest@kskalinina ~]$ gpasswd -a guest2 guest
passwd: доступ запрещен.
[guest@kskalinina ~]$ su -
Пароль:
Последний вход в систему:Сб окт 16 13:21:48 MSK 2021на pts/0
[root@kskalinina ~]# gpasswd -a guest2 guest
Добавление пользователя guest2 в rpyнны guest
[root@kskalinina ~]# exit
logout
[guest@kskalinina ~]$ groups guest
guest : guest
[guest@kskalinina ~]$ groups guest2
guest2 : guest2 guest
[guest@kskalinina ~]$ id -G
1001
[guest@kskalinina ~]$ id -Gn
guest

guest2@kskalinina:/home/guest
[guest@kskalinina ~]$ su guest2
Пароль:
[guest2@kskalinina guest]$ id
uid=1002(guest2) gid=1002(guest2) rpyнны=1002(guest2),1001(guest)
онрект=unconfined u:unconfined r:unconfined t:s0-s0:c0.c1023
[guest2@kskalinina guest]$ id -G
1002 1001
[guest2@kskalinina guest]$ id -Gn
guest2 guest
[guest2@kskalinina guest]$

```

Figure 0.5: Уточнение группы пользователя, и тех, кто также входит в эту группу

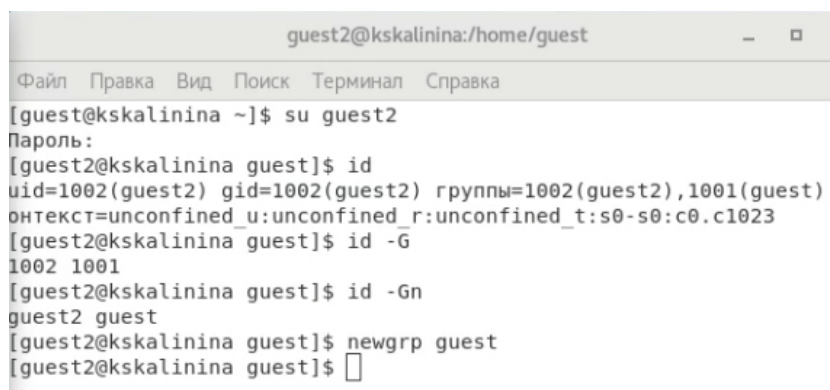
6. Просмотрела файл ‘/etc/group’, он показал аналогичную информацию (fig. 0.6).



```
guest@kskalinina:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
unbound:x:987:  
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:  
kskalinina:x:1000:kskalinina  
vboxsf:x:982:  
guest:x:1001:guest2  
guest2:x:1002:  
[guest@kskalinina ~]$
```

Figure 0.6: Просмотр файла ‘/etc/group’

7. От имени пользователя guest2 выполнила регистрацию пользователя guest2 в группе guest (fig. 0.7).



```
guest2@kskalinina:/home/guest  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@kskalinina ~]$ su guest2  
Пароль:  
[guest2@kskalinina guest]$ id  
uid=1002(guest2) gid=1002(guest2) грппны=1002(guest2),1001(guest) :  
онтекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[guest2@kskalinina guest]$ id -G  
1002 1001  
[guest2@kskalinina guest]$ id -Gn  
guest2 guest  
[guest2@kskalinina guest]$ newgrp guest  
[guest2@kskalinina guest]$
```

Figure 0.7: Регистрация пользователя guest2 в группе guest

8. От имени пользователя guest изменила права директории ‘/home/guest’, решив все действия для пользователей группы (fig. 0.8).

```

guest@kskalinina:~/dir1
Файл Правка Вид Поиск Терминал Справка
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:
kskalinina:x:1000:kskalinina
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
[guest@kskalinina ~]$ chmod g+rxw /home/guest

```

Figure 0.8: Изменение прав директории '/home/guest'

9. Заполнила таблицу «Установленные права и разрешённые действия для групп» (fig. 0.10). Для этого я создала в директории 16 файлов с разными правами на каждом (по два на каждые права для удобства). После этого я меняла права dir1 на guest и пробовала взаимодействовать с каждым из этих файлов на guest2, также пыталась зайти внутрь папки и просмотреть её содержимое (fig. 0.9). Таким образом я проделала необходимые действия с каждым вариантов прав директории и прав файла на пользователе guest2.

```

guest@kskalinina:~
Файл Правка Вид Поиск Терминал Справка
[guest@kskalinina ~]$ ls
[guest@kskalinina ~]$ cd dir1
[guest@kskalinina dir1]$ ls -l
итого 0
----- 1 guest guest 0 окт 16 13:14 file000
----rwx----- 1 guest guest 0 окт 16 13:14 file070
----- 1 guest guest 0 окт 16 13:14 test000
----rwx----- 1 guest guest 0 окт 16 13:14 test070
[guest@kskalinina dir1]$ cd ..
[guest@kskalinina ~]$ chmod 000 dir1
[guest@kskalinina ~]$ ls -l
итого 0
d----- 2 guest guest 66 окт 16 13:14 dir1
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Видео
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Документы
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Загрузки
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Изображения
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Музыка
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Общедоступные
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Рабочий стол
drwxr-xr-x. 2 guest guest 6 окт 2 17:18 Шаблоны
[guest@kskalinina ~]$

```

```

guest2@kskalinina:/home/guest
Файл Правка Вид Поиск Терминал Справка
guest2 guest
[guest2@kskalinina guest]$ newgrp guest
[guest2@kskalinina guest]$ touch /home/guest/dir1/file1
touch: невозможно выполнить touch для «/home/guest/dir1/file1»: Отк
азано в доступе
[guest2@kskalinina guest]$ rm /home/guest/dir1/test000
rm: невозможно удалить «/home/guest/dir1/test000»: Отказано в досту
пе
[guest2@kskalinina guest]$ echo "test" > /home/guest/dir1/file000
bash: /home/guest/dir1/file000: Отказано в доступе
[guest2@kskalinina guest]$ cat /home/guest/dir1/file000
cat: /home/guest/dir1/file000: Отказано в доступе
[guest2@kskalinina guest]$ cd /home/guest/dir1
bash: cd: /home/guest/dir1: Отказано в доступе
[guest2@kskalinina guest]$ ls /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest2@kskalinina guest]$ mv /home/guest/dir1/file000 /home/guest/
dir1/file
mv: не удалось получить доступ к «/home/guest/dir1/file»: Отказано
в доступе
[guest2@kskalinina guest]$ chattr +d /home/guest/dir1/file000
chattr: Отказано в доступе while trying to stat /home/guest/dir1/fi
le000
[guest2@kskalinina guest]$

```

Figure 0.9: Процесс заполнения таблицы

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

Figure 0.10: Таблица «Установленные права и разрешённые действия для групп»

10. На основе полученной информации из таблицы прошлого пункта (fig. 0.10), я смогла определить те или иные минимально необходимые права для выполнения операций внутри директории dir1 от имени пользователей входящих в группу (guest2). Так как в предыдущем пункте не требовалось создавать подкаталог, я дополнительно попробовала создать dir2 внутри dir1 (меняя права dir1) и удалить её, используя пользователя guest2 (fig. 0.11).

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	030	000
Удаление файла	030	000
Чтение файла	010	040
Запись в файл	010	020
Переименование файла	030	000
Создание поддиректории	030	-
Удаление поддиректории	030	-

Figure 0.11: Таблица “Минимальные права для совершения операций от имени пользователей входящих в группу”

Выводы

Таким образом я успешно приобрела практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы

1. Дискреционное разграничение доступа Linux. // Debianinstall. 2018. URL: <https://debianinstall.ru/diskretсионное-razgranichenie-dostupa-linux/> (дата обращения 16.10.2021).
2. Права доступа к файлам в Linux. // Pingvinus. 2018. URL: <https://pingvinus.ru/note/file-permissions> (дата обращения 16.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..