

Отчёт по лабораторной работе №2

дисциплина: Информационная безопасность

Быстров Глеб Андреевич

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	10
5	Выводы	23
	Список литературы	24

Список иллюстраций

4.1	Создание новой учетной записи	10
4.2	Создание пароля	10
4.3	Вход в систему	11
4.4	Определение дирректории	11
4.5	Уточнение пользователя	11
4.6	Команды id и group	11
4.7	Приглашение командной строки	12
4.8	Просмотр файла	12
4.9	Существующие в системе директории	13
4.10	Расширенные атрибуты установлены на поддиректориях	13
4.11	Работа с поддиректорией	13
4.12	Снятие атрибутов и проверка ls -l	14
4.13	Работа с файлом в дирректории	14

Список таблиц

4.1	Установленные права и разрешенные действия	15
4.2	Минимальные права для совершения операций	22

1 Цель работы

В данной лабораторной работе мне будет необходимо получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2 Задание

Последовательно выполнить пункты по настройке доступа через команды в терминале для нового пользователя.

3 Теоретическое введение

В Linux у каждого файла и каждого каталога есть два владельца: пользователь и группа.

Эти владельцы устанавливаются при создании файла или каталога. Пользователь, который создаёт файл становится владельцем этого файла, а первичная группа, в которую входит этот же пользователь, так же становится владельцем этого файла. Чтобы определить, есть ли у вас как у пользователя права доступа к файлу или каталогу, оболочка проверяет владение ими. [1].

Выделяют три категории пользователей, которым могут предоставляться права на файл:

- Сам владелец (u – user) объекта – конкретный пользователь, чье имя числится в атрибутах файла как имя владельца этого файла. Обычно если пользователь создает файл, то он автоматически записывается как его владелец.
- Группа (g – group), к которой принадлежит владелец файла. Когда в Linux создается пользователь, то для него создается одноименная группа. Однако средствами администрирования системы можно объединять пользователей в различные группы. При этом конкретный пользователь может входить в состав нескольких групп. Группы позволяют предоставлять права доступа к ресурсам сразу нескольким людям, но при этом ограниченному кругу лиц.
- Все остальные (o – other) – это все те, кто не является владельцем файла и не принадлежит к группе владельца файла. То есть любой посторонний пользователь.

Чтение, запись, выполнение – это то, что можно делать с существующим файлом, возможные действия над ним. У каждой категории пользователей (владельца, группы, остальных) должны быть свои права на каждое вышеупомянутое действие.

- Право на чтение (r – read) означает, что файл можно просматривать. Например, открыть файл и, если он текстовый, прочитать содержащийся в нем текст. Если это файл изображения, то можно посмотреть изображение. Наличие права только на чтение не позволяет изменять файл. То есть нельзя будет исправить текст или подрисовать что-то к картинке.
- Право на запись (w – write) позволяет изменять файл, то есть дописывать в него информацию или заменять ее другой.
- Право на исполнение (x – execution) имеет смысл не для всех файлов, хотя может быть установлено для любого. Это право позволяет исполнять файл как программу, при этом в файле должны быть записаны инструкции для процессора, то есть файл должен быть исполняемой программой.

Первые три записи – это права владельца, вторые три записи – права группы, последняя тройка – права на файл для всех остальных. Если обозначить каждое право соответствующей буквой, и все права всем предоставляются, то получится такая запись: `rw xrwxrwx` [2].

Рассмотрим подробнее, что значат условные значения флагов прав:

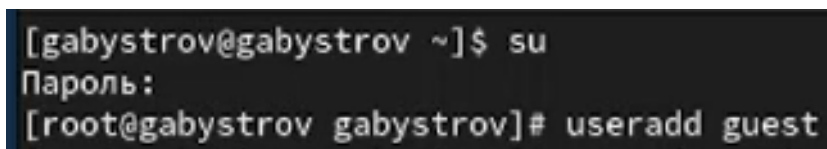
- - нет прав, совсем;
- x - разрешено только выполнение файла, как программы но не изменение и не чтение;
- w- - разрешена только запись и изменение файла;
- wx - разрешено изменение и выполнение, но в случае с каталогом, вы не можете посмотреть его содержимое;
- r- - права только на чтение;

r-x - только чтение и выполнение, без права на запись;
rw- - права на чтение и запись, но без выполнения;
rwx - все права;
-s - установлен SUID или SGID бит, первый отображается в поле для владельца, второй для группы;
-t - установлен sticky-bit, а значит пользователи не могут удалить этот файл [3].

Использование команды ls с опцией -l выведет на экран «длинную» распечатку, в которой будут, среди прочего, отражены права доступа к файлу [4].

4 Выполнение лабораторной работы

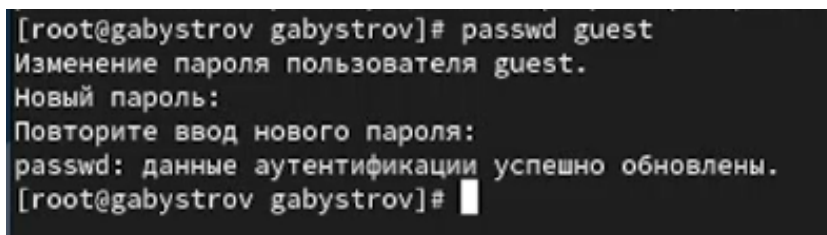
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (использовал учётную запись администратора): `useradd guest` (рис. 4.1).



```
[gabystrov@gabystrov ~]$ su
Пароль:
[root@gabystrov gabystrov]# useradd guest
```

Рис. 4.1: Создание новой учетной записи

2. Задал пароль для пользователя guest (использовал учётную запись администратора): `passwd guest` (рис. 4.2).



```
[root@gabystrov gabystrov]# passwd guest
Изменение пароля пользователя guest.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@gabystrov gabystrov]#
```

Рис. 4.2: Создание пароля

3. Вошёл в систему от имени пользователя guest (рис. 4.3).

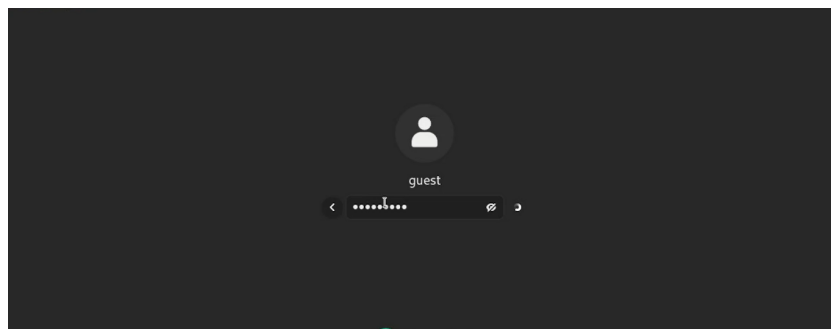


Рис. 4.3: Вход в систему

4. Определил директорию, в которой нахожусь, командой `pwd`. С приглашением командной строки совпадает. Является домашней директорией (рис. 4.4).

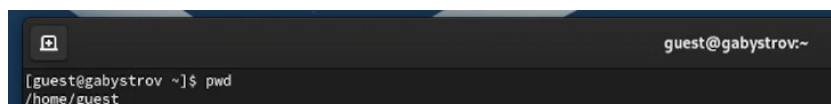


Рис. 4.4: Определение дирректории

5. Уточнил имя пользователя командой `whoami`. (рис. 4.5).

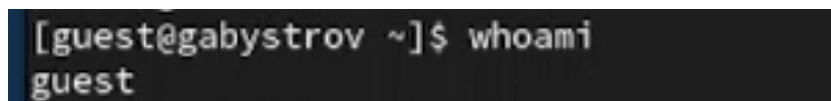


Рис. 4.5: Уточнение пользователя

6. Уточнил имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения с выводом команды `groups` совпадают (рис. 4.6).

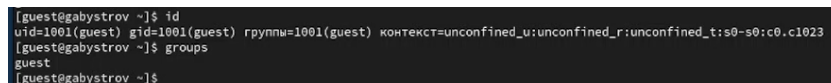
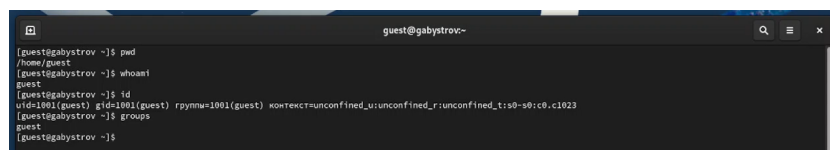


Рис. 4.6: Команды `id` и `group`

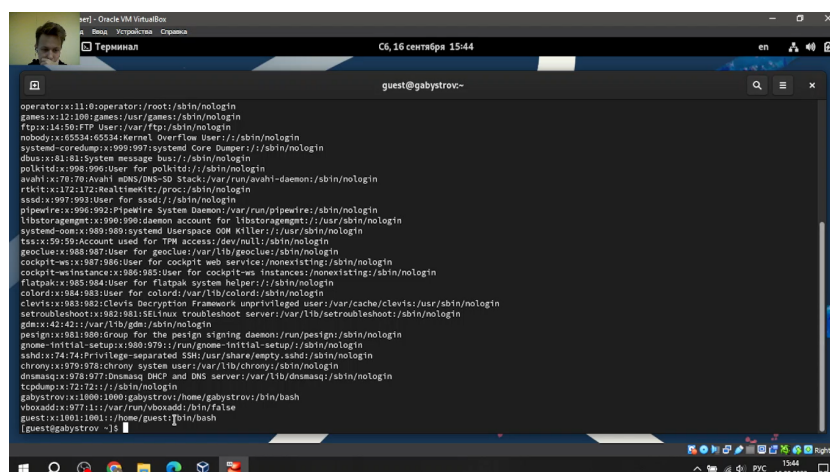
7. Полученная информация об имени пользователя с данными, выводимыми в приглашении командной строки совпадает (рис. 4.7).



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

Рис. 4.7: Приглашение командной строки

8. Просмотрел файл /etc/passwd командой `cat /etc/passwd`. Нашёл в нём свою учётную запись. Определил uid пользователя (1001). Определил gid пользователя (1001). Найденные значения совпадают с полученными в предыдущих пунктах (рис. 4.8).



```
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  
sasldev:x:997:993:User for sasldev:/sbin/nologin  
pipewire:x:996:992:Pipewire System Daemon:/var/run/pipewire:/sbin/nologin  
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/usr/sbin/nologin  
systemd-nomv:x:989:989:systemd Userspace DOM Killer:/usr/sbin/nologin  
ts:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin  
geoclue:x:988:987:User for geoclue:/var/lib/geoclue:/sbin/nologin  
cockpit-ws:x:987:986:User for cockpit web services/none/setting:/sbin/nologin  
cockpit-ws-instance:x:986:985:User for cockpit-ws instances/none/setting:/sbin/nologin  
flatpak:x:985:984:User for flatpak system helper:/sbin/nologin  
colord:x:984:983:User for colord:/var/lib/colord:/sbin/nologin  
clevis:x:983:982:clevis Decryption Framework unprivileged user:/var/cache/levis:/usr/sbin/nologin  
setroubleshoot:x:982:981:SELinux troubleshoot server:/var/lib/setroubleshoot:/sbin/nologin  
gdm:x:42:42:/var/lib/gdm:/sbin/nologin  
pesign:x:981:980:Group for the pesign signing daemon:/run/pesign:/sbin/nologin  
gnome-initial-setup:x:980:979:/run/gnome-initial-setup:/sbin/nologin  
smbd:x:74:74:Privilege-separated SMB:/usr/share/empty.smbd:/sbin/nologin  
chrony:x:979:978:chrony system user:/var/lib/chrony:/sbin/nologin  
dnsmasq:x:978:977:dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin  
tcpdump:x:72:72:/sbin/nologin  
gabystrov:x:1000:1000:gabystrov:/home/gabystrov:/bin/bash  
vboxadd:x:977:11:/var/run/vboxadd:/bin/false  
guest:x:1001:1001:/home/guest:/bin/bash  
[guest@gabystrov ~]$
```

Рис. 4.8: Просмотр файла

9. Определил существующие в системе директории командой `ls -l /home/`. Удалось получить список поддиректорий директории /home. На директориях установлены права для чтения, записи и выполнения только для пользователя (рис. 4.9).

```
[guest@gabystrov ~]$ ls -l /home/
итого 8
drwx-----, 14 gabystrov gabystrov 4096 сен 16 15:36 gabystrov
drwx-----, 14 guest guest 4096 сен 16 15:40 guest
```

Рис. 4.9: Существующие в системе директории

10. Проверил какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: `lsattr /home`. Удалось увидеть расширенные атрибуты директории только для пользователя. Не удалось увидеть расширенные атрибуты директорий других пользователей? (рис. 4.10).

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

Рис. 4.10: Расширенные атрибуты установлены на поддиректориях

11. Создал в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определил командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`: чтение, запись и выполнение для пользователя и групп. Чтение и выполнение для остальных. Расширенных атрибутов нет (рис. 4.11).

```
[guest@gabystrov ~]$ mkdir dir1
[guest@gabystrov ~]$ ls -l
итого 0
drwxr-xr-x, 2 guest guest 6 сен 16 15:47 dir1
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Вакан
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Документы
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Загрузки
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Избранное
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Музыка
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Общедоступные
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Рабочий стол
drwxr-xr-x, 2 guest guest 6 сен 16 15:39 Рабочий стол
[guest@gabystrov ~]$ lsattr
----- /Рабочий стол
----- /Загрузки
----- /Шаблоны
----- /Общедоступные
----- /Документы
----- /Музыка
----- /Избранное
----- /Видео
----- /dir1
```

Рис. 4.11: Работа с поддиректорией

12. Снял с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверил с её помощью правильность выполнения команды `ls -l`. Все было верно (рис. 4.12).

```
[guest@gabystrov ~]$ chmod 000 dir1
[guest@gabystrov ~]$ ls -l
итого 0
d----- . 2 guest guest 6 сен 16 15:55 dir1
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Видео
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Документы
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Изображения
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Музыка
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 16 15:39 Шаблоны
```

Рис. 4.12: Снятие атрибутов и проверка ls -l

13. Попытался создать в директории dir1 файл file1 командой echo "test" > /home/guest/dir1/file1. Получил отказ в выполнении операции по созданию файла так как до этого убрал данное право. Оценил, как сообщение об ошибке отразилось на создании файла. Файл не создался. Проверил командой ls -l /home/guest/dir1 действительно ли файл file1 не находится внутри директории dir1. (рис. 4.13).

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

Рис. 4.13: Работа с файлом в директории

14. Заполнил 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, занес в таблицу знак «+», если не разрешена, знак «-».

Таблица 4.1: Установленные права и разрешенные действия

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
----- (000)	----- (000)	-	-	-	-	-	-	-	-
----- (000)	-- x----- (100)	-	-	-	-	-	-	-	-
----- (000)	- w----- (200)	-	-	-	-	-	-	-	-
----- (000)	- wx----- (300)	-	-	-	-	-	-	-	-
----- (000)	r----- (400)	-	-	-	-	-	-	-	-
----- (000)	r- x----- (500)	-	-	-	-	-	-	-	-
----- (000)	rw----- (600)	-	-	-	-	-	-	-	-
----- (000)	rw- x----- (700)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
--x----- (100)	----- (000)	-	-	-	-	+	-	-	-
--x----- (100)	-- x----- (100)	-	-	-	-	+	-	-	-
--x----- (100)	- w----- (200)	-	-	+	-	+	-	-	-
--x----- (100)	- wx----- (300)	-	-	+	-	+	-	-	-
--x----- (100)	r----- (400)	-	-	-	+	+	-	-	+
--x----- (100)	r- x----- (500)	-	-	-	+	+	-	-	+
--x----- (100)	rw----- (600)	-	-	+	+	+	-	-	+
--x----- (100)	rwX----- (700)	-	-	+	+	+	-	-	+
-w----- (200)	----- (000)	-	-	-	-	-	-	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
-w----- (200)	-- x----- (100)	-	-	-	-	-	-	-	-
-w----- (200)	- w----- (200)	-	-	-	-	-	-	-	-
-w----- (200)	- wx----- (300)	-	-	-	-	-	-	-	-
-w----- (200)	r----- (400)	-	-	-	-	-	-	-	-
-w----- (200)	r- x----- (500)	-	-	-	-	-	-	-	-
-w----- (200)	rw----- (600)	-	-	-	-	-	-	-	-
-w----- (200)	rwX----- (700)	-	-	-	-	-	-	-	-
-wx----- (300)	-----+ (000)	+	+	-	-	+	-	+	-
-wx----- (300)	-- x----- (100)	+	+	-	-	+	-	+	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
-wx----- (300)	- w----- (200)	+	+	+	-	+	-	+	-
-wx----- (300)	- wx----- (300)	+	+	+	-	+	-	+	-
-wx----- (300)	r----- (400)	+	+	-	+	+	-	+	+
-wx----- (300)	r- x----- (500)	+	+	-	+	+	-	+	+
-wx----- (300)	rw----- (600)	+	+	+	+	+	-	+	+
-wx----- (300)	rwX----- (700)	+	+	+	+	+	-	+	+
r----- (400)	----- (000)	-	-	-	-	-	+	-	-
r----- (400)	-- x----- (100)	-	-	-	-	-	+	-	-
r----- (400)	- w----- (200)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
r----- (400)	- wx----- (300)	-	-	-	-	-	+	-	-
r----- (400)	r----- (400)	-	-	-	-	-	+	-	-
r----- (400)	r- x----- (500)	-	-	-	-	-	+	-	-
r----- (400)	rw----- (600)	-	-	-	-	-	+	-	-
r----- (400)	rwX----- (700)	-	-	-	-	-	+	-	-
r-x----- (500)	----- (000)	-	-	-	-	+	+	-	-
r-x----- (500)	-- x----- (100)	-	-	-	-	+	+	-	-
r-x----- (500)	- w----- (200)	-	-	+	-	+	+	-	-
r-x----- (500)	- wx----- (300)	-	-	+	-	+	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
r-x----- (500)	r----- (400)	-	-	+	+	+	+	-	+
r-x----- (500)	r- x----- (500)	-	-	-	+	+	+	-	+
r-x----- (500)	rw----- (600)	-	+	+	+	+	+	-	+
r-x----- (500)	rwX----- (700)	-	+	+	+	+	+	-	+
rw----- (600)	----- (000)	-	-	-	-	-	+	-	-
rw----- (600)	-- x----- (100)	-	-	-	-	-	+	-	-
rw----- (600)	- w----- (200)	-	-	-	-	-	+	-	-
rw----- (600)	- wx----- (300)	-	-	-	-	-	+	-	-
rw----- (600)	r----- (400)	-	-	-	-	-	+	-	-

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rw----- (600)	r- x----- (500)	-	-	-	-	-	+	-	-
rw----- (600)	rw----- (600)	-	-	-	-	-	+	-	-
rw----- (600)	rwX----- (700)	-	-	-	-	-	+	-	-
rwX----- (700)	-----+ (000)	+	+	-	-	+	+	+	-
rwX----- (700)	-- x----- (100)	+	+	-	-	+	+	+	-
rwX----- (700)	- w----- (200)	+	+	+	-	+	+	+	-
rwX----- (700)	- wx----- (300)	+	+	+	-	+	+	+	-
rwX----- (700)	r-----+ (400)	+	+	-	+	+	+	+	+
rwX----- (700)	r- x----- (500)	+	+	-	+	+	+	+	+

Права ди- ректории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Про- смотр фай- лов дирек- тории	Пере- име- нова- ние фай- ла	Смена аттри- бутов файла
rwX----- (700)	rw-----+	+	+	+	+	+	+	+	+
rwX----- (700)	rwX-----+	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы определил те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполнил таблицу.

Таблица 4.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные 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

В данной лабораторной работе мне успешно удалось получить практические навыки работы в консоли с атрибутами файлов, закрепить теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask) [Электронный ресурс]. 2023. URL: <https://habr.com/ru/articles/469667/>.
2. Права доступа к файлам и каталогам [Электронный ресурс]. 2023. URL: <https://younglinux.info/bash/rwx>.
3. Права доступа к файлам в Linux [Электронный ресурс]. 2023. URL: <https://losst.pro/prava-dostupa-k-fajlam-v-linux>.
4. Права доступа к файлам [Электронный ресурс]. 2023. URL: <https://docs.altlinux.org/ru-RU/archive/2.3/html-single/junior/alt-docs-extras-linuxnovice/ch02s08.html>.