

Отчёт

по лабораторной работе 2

Радимов Игорь Ринадович

Содержание

1	Цель работы	5
2	Задание	6
3	Теория	7
4	Выполнение лабораторной работы	8
5	Библиография	17
6	Выводы	18

List of Tables

List of Figures

4.1	рис.1. Создание новой ученой записи.	8
4.2	рис.2. Задание пароля для quest.	9
4.3	рис.3. Авторизация.	9
4.4	рис.4. Определяем диреторию.	10
4.5	рис.5. Кто я?	10
4.6	рис.6. groups	10
4.7	рис.7. Результат выполнения cat /etc/passwd.	11
4.8	рис.8. Права на директориях iradimov и quest.	11
4.9	рис.9. Расширенные атрибуты iradimov и quest.	12
4.10	рис.10. Создаем в домашней директории поддиректорию.	12
4.11	рис.11. Права 000 для dir1.	12
4.12	рис.12. Проверка действий для прав 000.	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

Необходимо изучить основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux на практике. Также нужно заполнить таблицу прав доступа.

3 Теория

Права доступа имеют всего 3 опции – чтение, запись и запуск на выполнение, устанавливаемые для владельца, группы и прочих пользователей (для папки запуск на выполнение означает просмотр содержимого – списка файлов и вложенных папок).

Права можно задавать либо буквами r (read), w (Write) и x (eXecute), либо в двоичной системе (точнее в восьмеричной с использованием цифр от 0 до 7, но на основе двоичной системы).

Праву на чтение (r) соответствует значение 4, записи (w) – 2 и выполнению/просмотру файлов (x) – 1. Комбинируя эти значения, можно получать разные права. Например: - $6 = (4 + 2)$ – чтение и запись - $5 = (4 + 1)$ – чтение и исполнение

Первыми задаются права доступа для владельца, затем для группы и в конце для всех прочих.

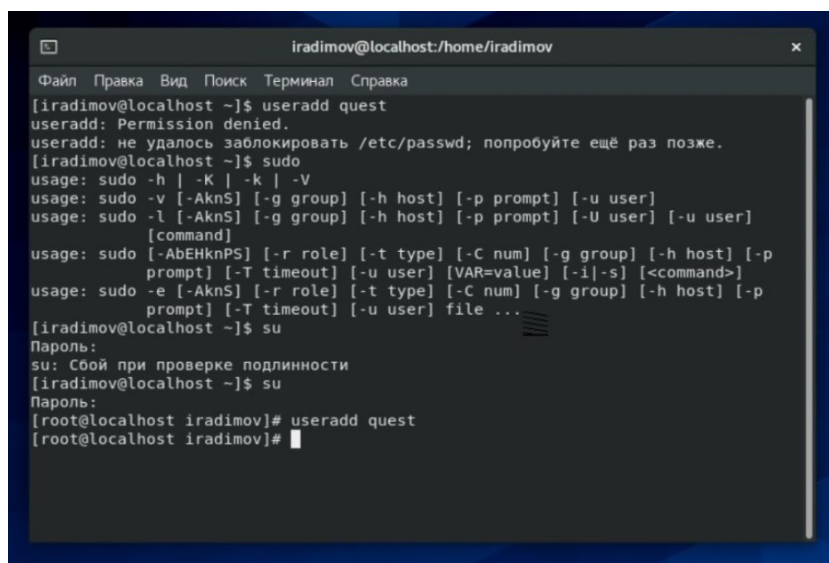
Обычно для документов и файлов данных устанавливаются права 644 или 664. Это означает, что владелец может читать и изменять файл (включая удаление), члены группы в первом случае только читать, а во втором изменять, а все прочие – только читать.

Для исполняемых файлов и папок обычно задаются права 755 или 775. Значения те же, что и в предыдущем абзаце плюс присутствует право на выполнение или просмотр списка вложенных объектов.

Если задавать права доступа буквами, то указываются нужные права в виде rwx, а то, что нужно пропустить, заменяется дефисом. То есть, 644 соответствует rw-r--r-, а 755 – rwxr-xr-x.

4 Выполнение лабораторной работы

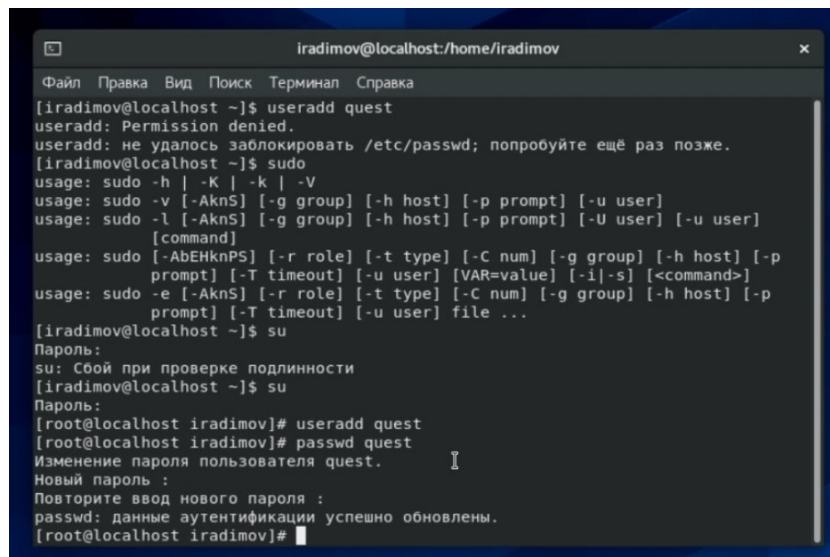
1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя quest (используя учётную запись root):(рис.1). Для перехода в учётную запись root использую команду su, для создания учетной записи командой useradd quest.



```
iradimov@localhost:/home/iradimov
Файл Правка Вид Поиск Терминал Справка
[iradimov@localhost ~]$ useradd quest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[iradimov@localhost ~]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
[command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] file ...
[iradimov@localhost ~]$ su
Пароль:
su: Сбой при проверке подлинности
[iradimov@localhost ~]$ su
Пароль:
[root@localhost iradimov]# useradd quest
[root@localhost iradimov]#
```

Figure 4.1: рис.1. Создание новой ученой записи.

2. Был задан пароль для пользователя quest, используя учётную запись root (рис.2).



```
iradimov@localhost:~/home/iradimov
Файл Правка Вид Поиск Терминал Справка
[iradimov@localhost ~]$ useradd quest
useradd: Permission denied.
useradd: не удалось заблокировать /etc/passwd; попробуйте ещё раз позже.
[iradimov@localhost ~]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
[command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
prompt] [-T timeout] [-u user] file ...
[iradimov@localhost ~]$ su
Пароль:
su: Сбой при проверке подлинности
[iradimov@localhost ~]$ su
Пароль:
[root@localhost iradimov]# useradd quest
[root@localhost iradimov]# passwd quest
Изменение пароля пользователя quest.
Новый пароль :
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@localhost iradimov]#
```

Figure 4.2: рис.2. Задание пароля для quest.

3. Вошёл в систему от имени пользователя quest (рис.3).

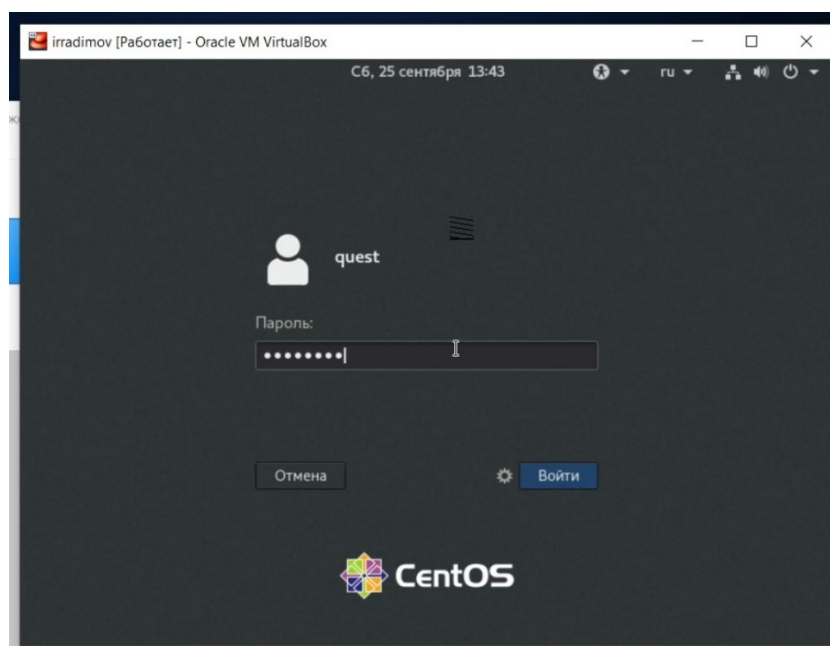
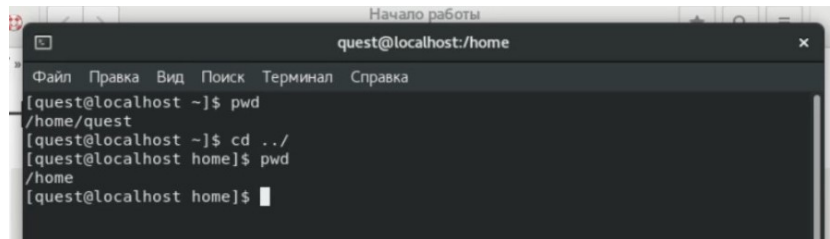


Figure 4.3: рис.3. Авторизация.

4. Командой `pwd` была определена текущая директория. Действительно, мы находимся в домашней директории (рис.4). `[quest@localhost ~]$` означает

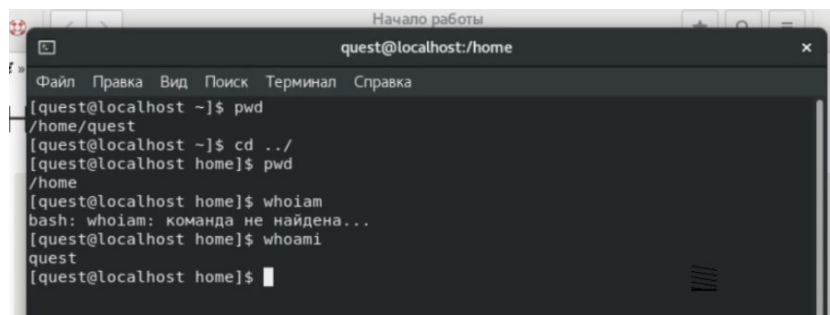
следующее: quest - имя учетной записи пользователя, localhost - имя компьютера, ~ - папка выполнения команды (домашняя).



```
quest@localhost/home
[quest@localhost ~]$ pwd
/home/quest
[quest@localhost ~]$ cd ../
[quest@localhost home]$ pwd
/home
[quest@localhost home]$
```

Figure 4.4: рис.4. Определяем диреторию.

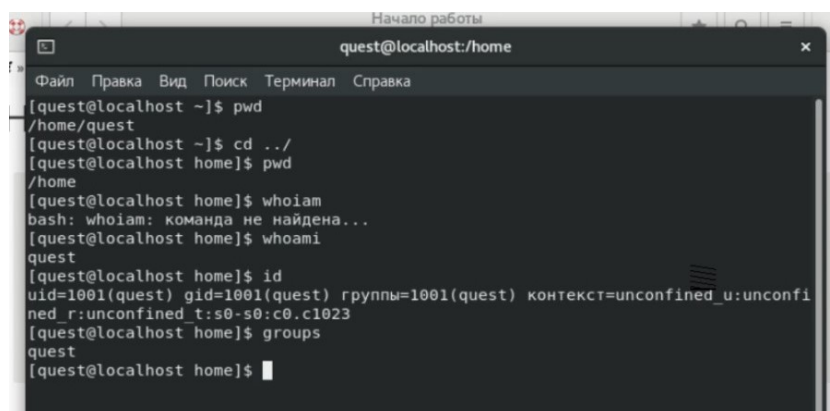
5. Уточняю имя пользователя командой whoami (рис.5).



```
quest@localhost/home
[quest@localhost ~]$ pwd
/home/quest
[quest@localhost ~]$ cd ../
[quest@localhost home]$ pwd
/home
[quest@localhost home]$ whoiam
bash: whoiam: команда не найдена...
[quest@localhost home]$ whoami
quest
[quest@localhost home]$
```

Figure 4.5: рис.5. Кто я?

6. При помощи команды id выясняем, имя пользователя quest, группа quest, uid=1001, gid=1001, входит только в группу 1001 (quest). Команда groups так же вывела одну группу quest (рис.6).



```
quest@localhost/home
[quest@localhost ~]$ pwd
/home/quest
[quest@localhost ~]$ cd ../
[quest@localhost home]$ pwd
/home
[quest@localhost home]$ whoiam
bash: whoiam: команда не найдена...
[quest@localhost home]$ whoami
quest
[quest@localhost home]$ id
uid=1001(quest) gid=1001(quest) группы=1001(quest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[quest@localhost home]$ groups
quest
[quest@localhost home]$
```

Figure 4.6: рис.6. groups

7. Сравниваем полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки. Имя пользователя во всех командах выводится как quest, что совпадает с именем в приглашении командной строки.
8. В файле /etc/passwd нахожу свою учетную запись, всё совпадает с результатами выполнения команд, из предыдущих пунктов (рис.7).

```

irradimov [Работает] - Oracle VM VirtualBox
Обзор Терминал C6, 25 сентября 13:51 en
quest@localhost/home

Файл Правка Вид Поиск Терминал Справка
libstoragemgmt:x:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
clevis:x:994:990:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
unbound:x:993:989:Unbound DNS resolver:/etc/unbound:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin
rpcbind:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:992:988:GlusterFS daemons:/run/gluster:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
dnsmasq:x:987:987:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
saslauthd:x:986:76:Saslauthd user:/run/saslauthd:/sbin/nologin
sssd:x:985:986:User for sssd:/sbin/nologin
cockpit-ws:x:984:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:983:983:User for cockpit ws instances:/nonexisting:/sbin/nologin
chrony:x:982:982:/var/lib/chrony:/sbin/nologin
colord:x:981:981:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
setroubleshoot:x:980:977:/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:979:976:User for flatpak system helper:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:978:975:/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
tcpdump:x:72:72:/sbin/nologin
iradimov:x:1000:1000:iradimov:/home/iradimov:/bin/bash
quest:x:1001:1001::/home/quest:/bin/bash
[quest@localhost home]$

```

Figure 4.7: рис.7. Результат выполнения cat /etc/passwd.

9. Определил существующие в системе директории командой ls -l /home/. Получаем список поддиректорий директории /home. На директориях iradimov и quest установлены права 700 (рис.8).

```

[quest@localhost home]$ ls -l /home/
итого 8
drwx----- 15 iradimov iradimov 4096 сен 25 13:42 iradimov
drwx----- 15 quest quest 4096 сен 25 13:44 quest

```

Figure 4.8: рис.8. Права на директориях iradimov и quest.

10. С помощью команды lsattr /home пытаемся получить информацию о расширенных атрибутах. Для пользователя iradimov имеем отказ в

доступе, для quest получаем.(рис.9).

```
[quest@localhost ~]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/iradimov
----- /home/quest
[quest@localhost ~]$
```

Figure 4.9: рис.9. Расширенные атрибуты iradimov и quest.

11. С помощью команды `mkdir dir1` создаем в домашней директории поддиректорию `dir1`.(рис.10).

```
[quest@localhost ~]$ pwd
/home/quest
[quest@localhost ~]$ mkdir dir1
[quest@localhost ~]$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка  'Рабочий стол'
```

Figure 4.10: рис.10. Создаем в домашней директории поддиректорию.

12. С помощью команды `chmod 000 dir1` снимаем все атрибуты `dir1`, проверяем. Имеем права 000.(рис.11).

```
[quest@localhost ~]$ chmod 000 dir1
[quest@localhost ~]$ ls -l /dir1
ls: невозможно получить доступ к '/dir1': Нет такого файла или каталога
[quest@localhost ~]$ ls -l
итого 0
d----- 2 quest quest 6 сен 25 13:55 dir1
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Видео
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Документы
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Загрузки
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Изображения
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Музыка
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Общедоступные
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 'Рабочий стол'
drwxr-xr-x. 2 quest quest 6 сен 25 13:44 Шаблоны
[quest@localhost ~]$
```

Figure 4.11: рис.11. Права 000 для dir1.

13. Пытаемся создать в директории `dir1` файл `file1` командой `echo "test" > /home/quest/dir1/file1`, получаем отказ в доступе (рис.12).

```
[quest@localhost ~]$ echo 'test' > /home/quest/dir1/file1
bash: /home/quest/dir1/file1: Отказано в доступе
[quest@localhost ~]$ ls -l /home/quest/dir1
ls: невозможно открыть каталог '/home/quest/dir1': Отказано в доступе
[quest@localhost ~]$ ls -l /home/quest/
итого 0
d----- 2 quest quest 6 сен 25 13:55 dir1
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Видео
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Документы
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Загрузки
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Изображения
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Музыка
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Общедоступные
drwxr-xr-x 2 quest quest 6 сен 25 13:44 'Рабочий стол'
drwxr-xr-x 2 quest quest 6 сен 25 13:44 Шаблоны
[quest@localhost ~]$
```

Figure 4.12: рис.12. Проверка действий для прав 000.

14. Далее путем последовательного выполнения команд (chmod,touch,rm,echo,mv,cat,ls,cd) для проверки прав доступа для директории и файла заполняем таблицу.

Правка дирек- тории	ПраваСозда- ние файла	Удале- ние файла	Запись в файл	Чте- ние файла	Смена дирек- тории	Просмотр файлов в директории	Переиме- нование файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	+	-	-	-
d(200)	(000)	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	+	-
d(400)	(000)	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	+	+	-	-
d(600)	(000)	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	-
d(000)	(100)	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	+	-	-	-
d(200)	(100)	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	+	-
d(400)	(100)	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	+	+	-	-

Правка дирек- тории	ПраваСозда- ние файла	Удале- ние файла	Запись в файл	Чте- ние файла	Смена дирек- тории	Просмотр файлов в директории	Переиме- нование файла	Смена атрибутов файла
d(600)	(100)	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	+	+	+	-
d(000)	(200)	-	-	-	-	-	-	-
d(100)	(200)	-	-	+	+	-	-	-
d(200)	(200)	-	-	-	-	-	-	-
d(300)	(200)	+	+	+	+	-	+	-
d(400)	(200)	-	-	-	-	+	-	-
d(500)	(200)	-	-	+	+	+	-	-
d(600)	(200)	-	-	-	-	+	-	-
d(700)	(200)	+	+	+	+	+	+	-
d(000)	(300)	-	-	-	-	-	-	-
d(100)	(300)	-	-	+	+	-	-	-
d(200)	(300)	-	-	-	-	-	-	-
d(300)	(300)	+	+	+	+	-	+	-
d(400)	(300)	-	-	-	-	+	-	-
d(500)	(300)	-	-	+	+	+	-	-
d(600)	(300)	-	-	-	-	+	-	-
d(700)	(300)	+	+	+	+	+	+	-
d(000)	(400)	-	-	-	-	-	-	-
d(100)	(400)	-	-	-	+	-	-	+
d(200)	(400)	-	-	-	-	-	-	-
d(300)	(400)	+	+	-	+	-	+	+

Правка дирек- тории	ПраваСозда- ние файла	Удале- ние файла	Запись в файл	Чте- ние файла	Смена дирек- тории	Просмотр файлов в директории	Переиме- нование файла	Смена атрибутов файла
d(400)	(400)	-	-	-	-	+	-	-
d(500)	(400)	-	-	-	+	+	-	+
d(600)	(400)	-	-	-	-	+	-	-
d(700)	(400)	+	+	-	+	+	+	+
d(000)	(500)	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	+
d(200)	(500)	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	+	+
d(400)	(500)	-	-	-	-	-	+	-
d(500)	(500)	-	-	-	+	+	+	+
d(600)	(500)	-	-	-	-	-	+	-
d(700)	(500)	+	+	-	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-
d(100)	(600)	-	-	+	+	+	-	+
d(200)	(600)	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+
d(400)	(600)	-	-	-	-	-	+	-
d(500)	(600)	-	-	+	+	+	+	+
d(600)	(600)	-	-	-	-	-	+	-
d(700)	(600)	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-
d(100)	(700)	-	-	+	+	+	-	+

Правка дирек- тории	ПраваСозда- ние файла	Удале- ние файла	Запись в файл	Чте- ние файла	Смена дирек- тории	Просмотр файлов в директории	Переиме- нование файла	Смена атрибутов файла
d(200)	(700)	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	+	-	-
d(500)	(700)	-	-	+	+	+	-	+
d(600)	(700)	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+

15. После анализа таблицы выше, составляем итоговую таблицу.

Операция	Мин. права на директорию	Мин. права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	400
Запись в файл	300	200
Переименование файла	300	000
Создание поддиректории	300	-
Удаление поддиректории	300	-

5 Библиография

1. ТУИС РУДН

6 Выводы

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