

Отчёт по лабораторной работе 3

Дискреционное разграничение прав в Linux. Два пользователя

Максимова Ксения НБИбд-02-18

Содержание

1	Цель работы	4
2	Задание	5
3	Теоретическое введение	6
4	Выполнение лабораторной работы	8
5	Выводы	20
	Список литературы	21

List of Figures

4.1	Рис 1.Создание нового пользователя	8
4.2	Рис 2.Установка пароля	9
4.3	Рис 3.Создание пользователя guest2	9
4.4	Рис 4.Задание пароля для пользователя guest2	10
4.5	Рис 5.Добавляем пользователя guest2 в группу guest	10
4.6	Рис 6.Осуществляем вход в систему от guest	11
4.7	Рис 7.Осуществляем вход в систему от guest2	11
4.8	Рис 8./home/guest2	12
4.9	Рис 9./home/guest	12
4.10	Рис 10.Команды id, groups guest, id -Gn и id -G для guest	13
4.11	Рис 11.Команды id, groups guest, id -Gn и id -G для guest2	14
4.12	Рис 12. guest2	14
4.13	Рис 13. guest	15
4.14	Рис 14. Регистрация пользователя guest2	15
4.15	Рис 15. Изменение прав директории	16
4.16	Рис 16. Снимаем все права	17
4.17	Рис 17. Таблица “Разрешенные права и действия для пользователей групп”	18
4.18	Рис 18. Таблица “Минимальные права для совершения операций”	19

1 Цель работы

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

2 Задание

Создать двух пользователей в ранее установленной операционной системе на виртуальной машине, определить установленные права, разрешенные действия и минимальные права для совершения операций

3 Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но одна из самых важных - это система прав доступа к файлам. Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в Linux продуманы очень хорошо [1].

Права доступа к файлу или директории можно изменить с помощью команды `chmod`. Атрибуты файла или каталога можно указать как буквами так и цифрами. Установить необходимые атрибуты можно для владельца файла (u), группы (g) или остальных пользователей (o) [1].

Права доступа к какому-либо объекту в системе обозначаются с помощью 10 символов, записанных в строку [2].

1. Первый символ в строке обозначает тип данных
2. Следующие три символа обозначают права для владельца файла или директории
3. После - права для определенной группы пользователей
4. Последние четыре символа - права для остальных пользователей

Рассмотрим, какими правами может быть наделен файл или директория:

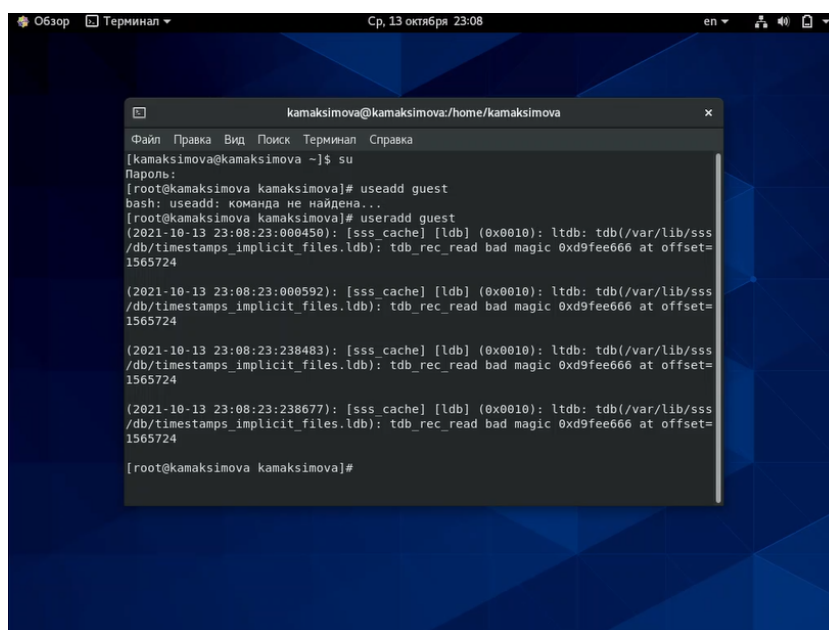
- r - read, то есть, право доступа на чтение файла или директории.
- w - write, то есть, право на изменение и удаление файла или директории.
- x - execute, то есть, право на запуск файла как программы или вход в директорию.

Таким образом, можно ограничить или расширить права на файл тех или иных пользователей

Права доступа для пользователей группы определяются второй триадой символов в строке прав, как и любой другой пользователь или владелец, пользователь группы может получить права на чтение, изменение или удаление, а так же запуск файла [3]

4 Выполнение лабораторной работы

В установленной операционной системе создаем учётную запись пользователя guest с помощью команды useradd

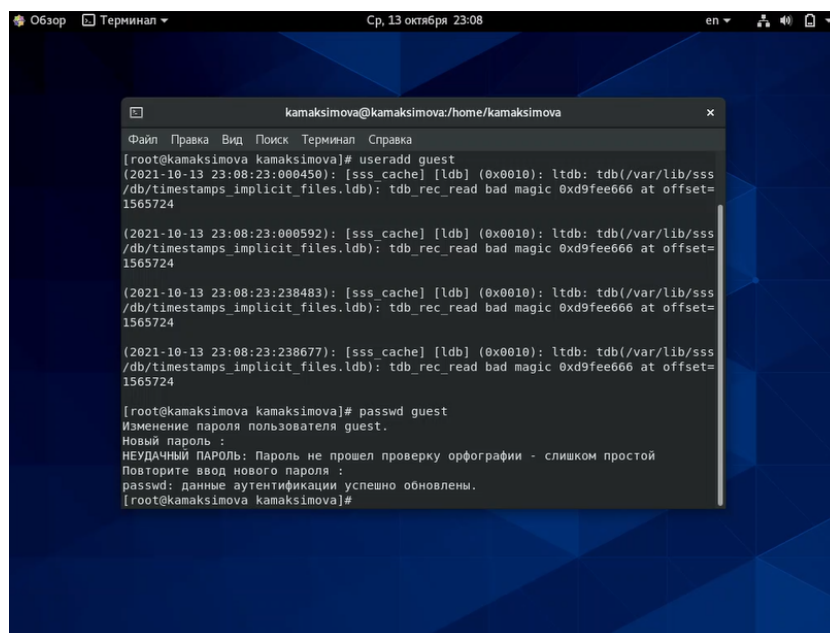


```
kamaksimova@kamaksimova:~/home/kamaksimova
Файл Правка Вид Поиск Терминал Справка
[kamaksimova@kamaksimova ~]$ su
Пароль:
[root@kamaksimova kamaksimova]# useradd guest
bash: useradd: команда не найдена...
[root@kamaksimova kamaksimova]# useradd guest
(2021-10-13 23:08:23:000450): [sss_cache] [ldb] (0x0010): ldb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:000592): [sss_cache] [ldb] (0x0010): ldb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:238483): [sss_cache] [ldb] (0x0010): ldb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:238677): [sss_cache] [ldb] (0x0010): ldb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
[root@kamaksimova kamaksimova]#
```

Figure 4.1: Рис 1.Создание нового пользователя

Рисунок 1

Задаем пароль для пользователя guest с помощью команды passwd

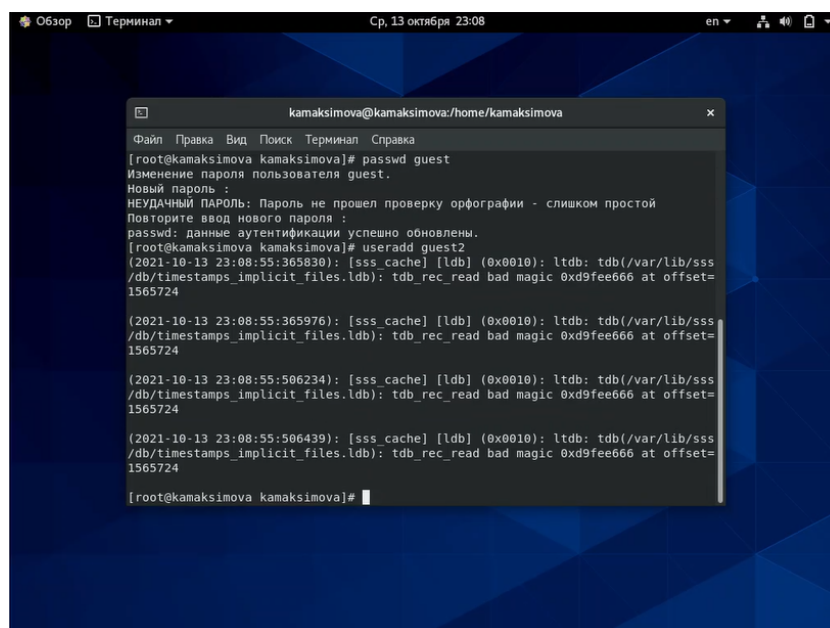


```
kamaksimova@kamaksimova/home/kamaksimova
[root@kamaksimova kamaksimova]# useradd guest
(2021-10-13 23:08:23:00450): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:000592): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:238483): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:23:238677): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
[root@kamaksimova kamaksimova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@kamaksimova kamaksimova]#
```

Figure 4.2: Рис 2.Установка пароля

Рисунок 2

Аналогично создаем второго пользователя guest2



```
kamaksimova@kamaksimova/home/kamaksimova
[root@kamaksimova kamaksimova]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@kamaksimova kamaksimova]# useradd guest2
(2021-10-13 23:08:55:365976): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:55:365830): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:55:506234): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
(2021-10-13 23:08:55:506439): [sss_cache] [ldb] (0x0010): ltdb: tdb(/var/lib/sss/db/timestamps_implicit_files.ldb): tdb_rec_read bad magic 0xd9fee666 at offset=1565724
[root@kamaksimova kamaksimova]#
```

Figure 4.3: Рис 3.Создание пользователя guest2

Рисунок 3

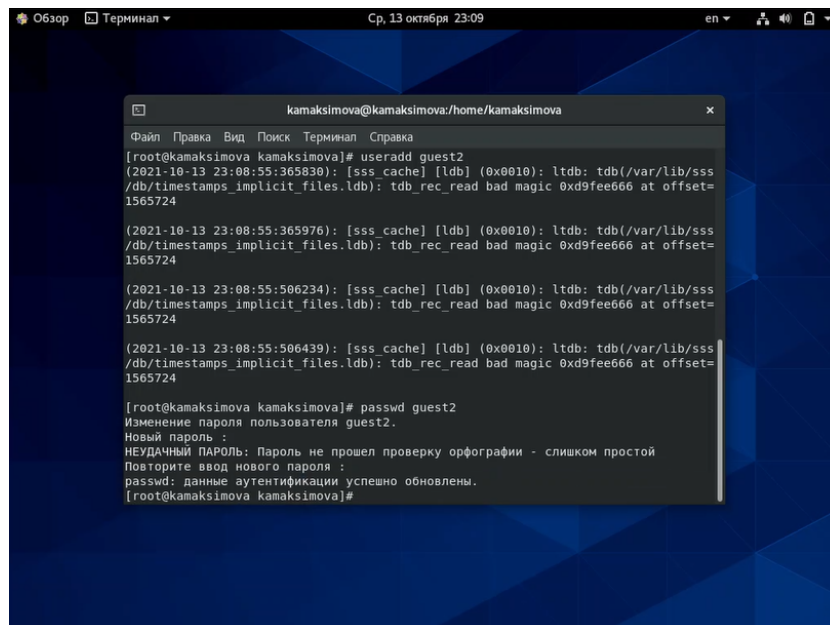


Figure 4.4: Рис 4.Задание пароля для пользователя guest2

Рисунок 4

Добавляем пользователя guest2 в группу guest

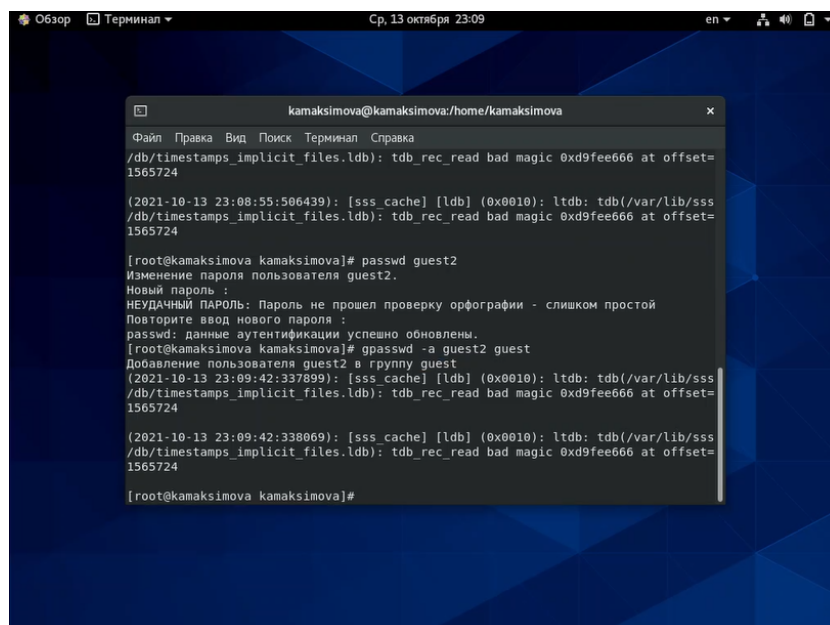


Figure 4.5: Рис 5.Добавляем пользователя guest2 в группу guest

Рисунок 5

Осуществляем вход в систему от двух пользователей на двух разных консолях:
guest на первой консоли и guest2 на второй консоли

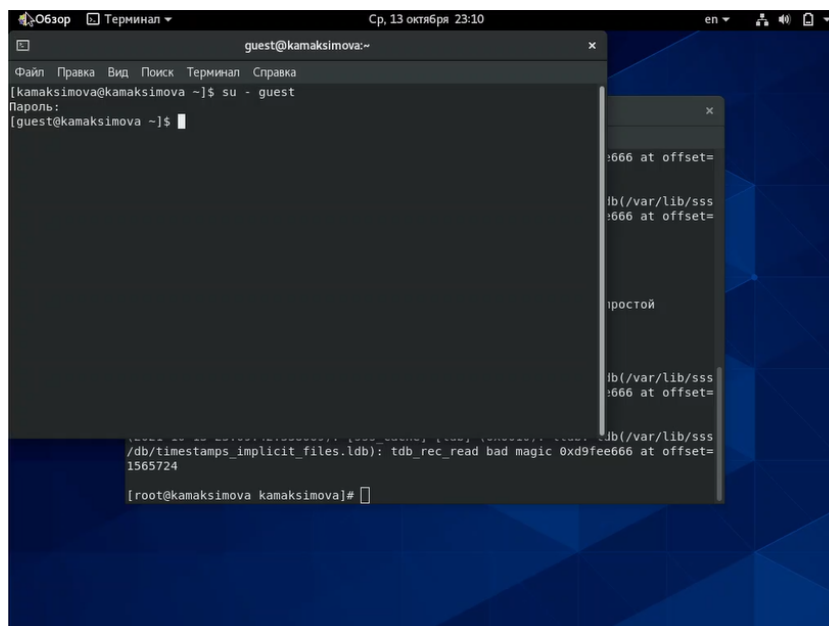


Figure 4.6: Рис 6.Осуществляем вход в систему от guest

Рисунок 6

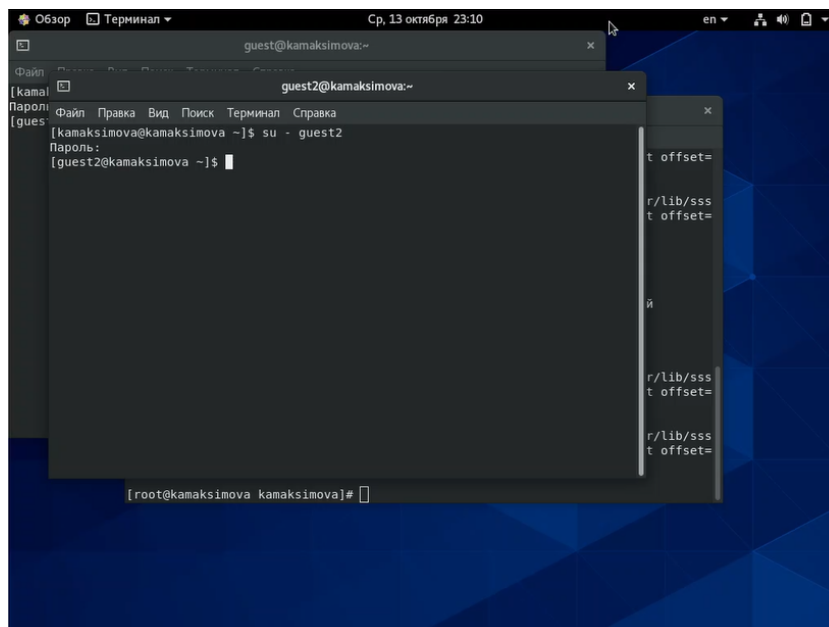


Figure 4.7: Рис 7.Осуществляем вход в систему от guest2

Рисунок 7

Для обоих пользователей командой `pwd` определяем директорию, в которой находимся

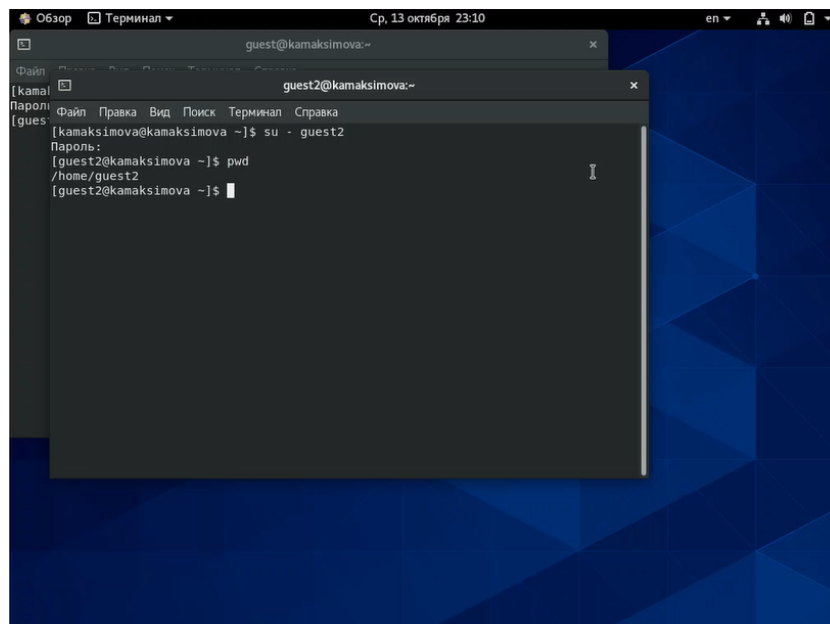


Figure 4.8: Рис 8./home/guest2

Рисунок 8

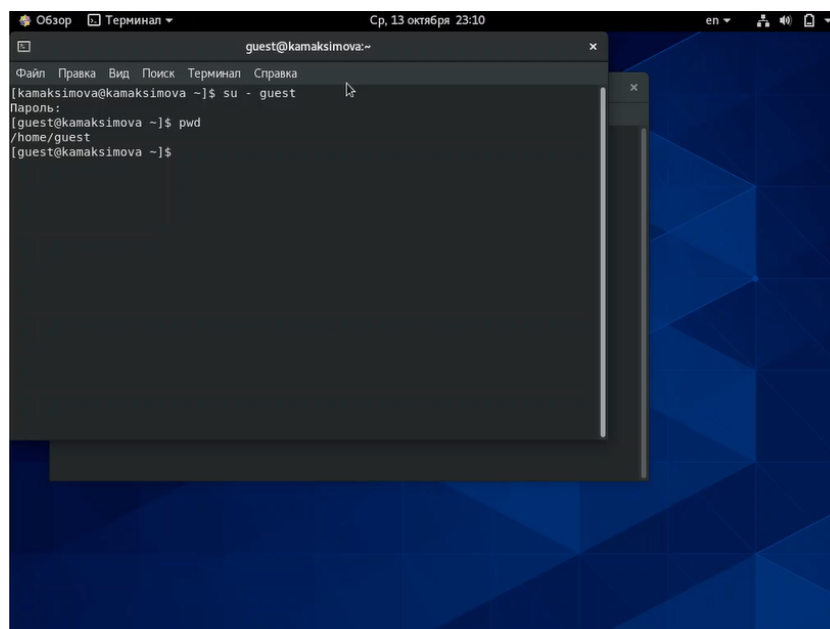
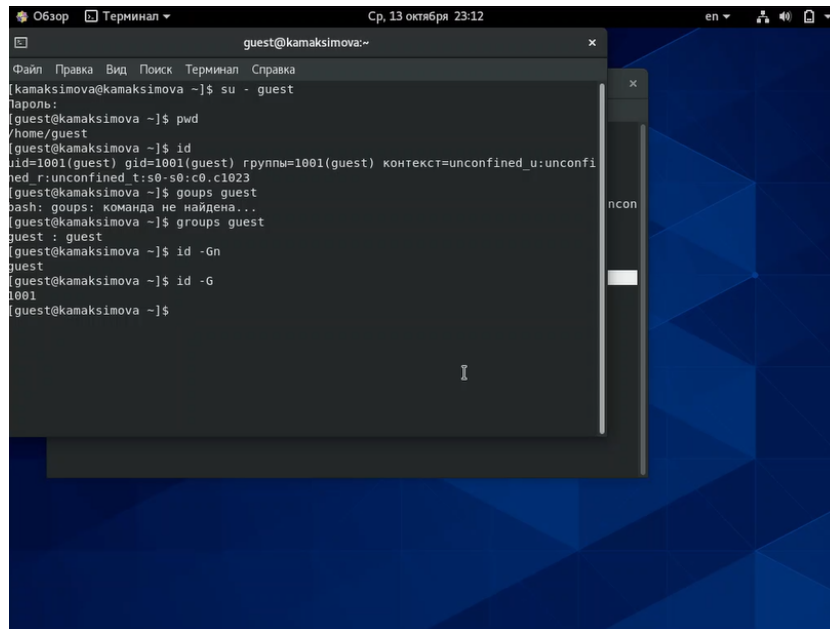


Figure 4.9: Рис 9./home/guest

Рисунок 9

Уточним имя пользователя, его группу, кто входит в неё и к каким группам принадлежит пользователь. Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`.



```
guest@kamaksimova:~  
[kamaksimova@kamaksimova ~]$ su - guest  
Пароль:  
[guest@kamaksimova ~]$ pwd  
/home/guest  
[guest@kamaksimova ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@kamaksimova ~]$ groups guest  
bash: groups: команда не найдена...  
[guest@kamaksimova ~]$ groups guest  
guest : guest  
[guest@kamaksimova ~]$ id -Gn  
guest  
[guest@kamaksimova ~]$ id -G  
1001  
[guest@kamaksimova ~]$
```

Figure 4.10: Рис 10. Команды `id`, `groups guest`, `id -Gn` и `id -G` для `guest`

Рисунок 10

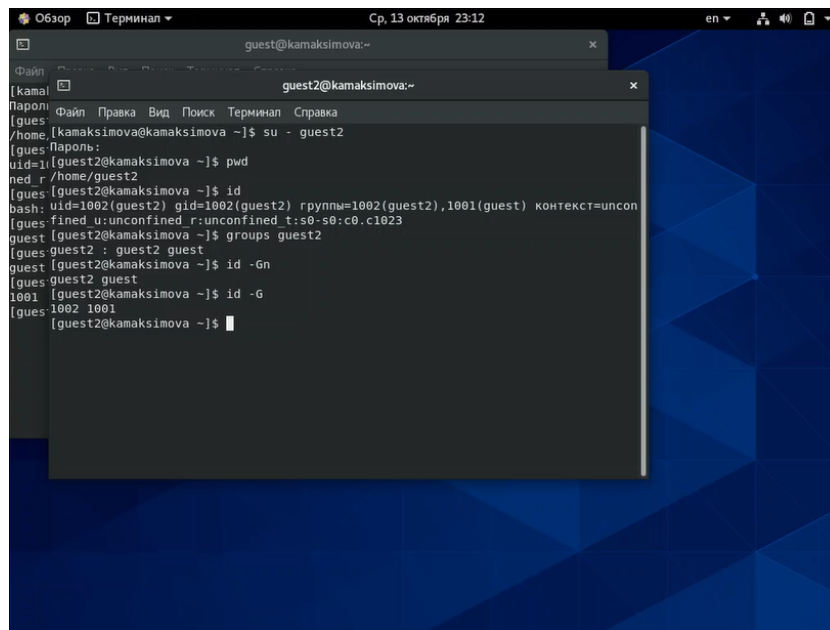


Figure 4.11: Рис 11. Команды id, groups guest, id -Gn и id -G для guest2

Рисунок 11

Просмотрим файл “/etc/group” командой cat

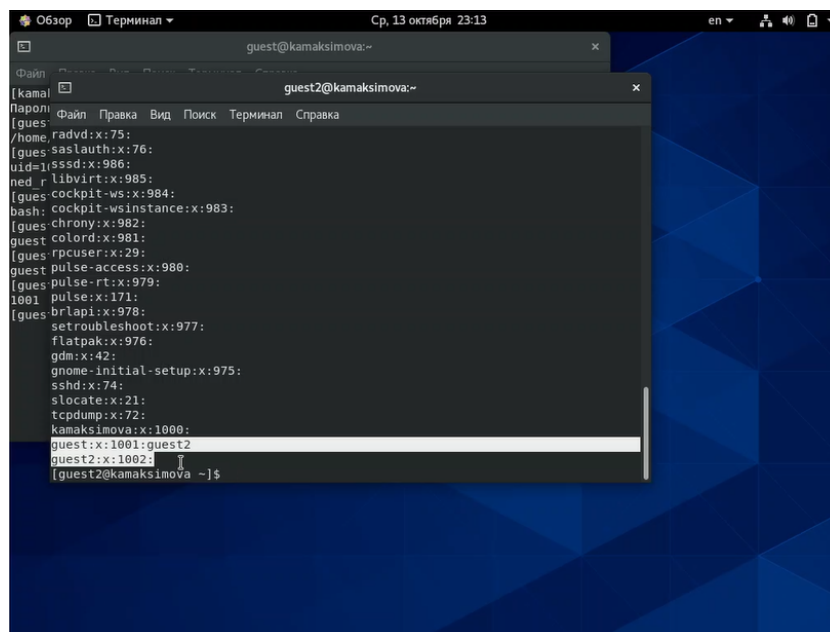


Figure 4.12: Рис 12. guest2

Рисунок 12

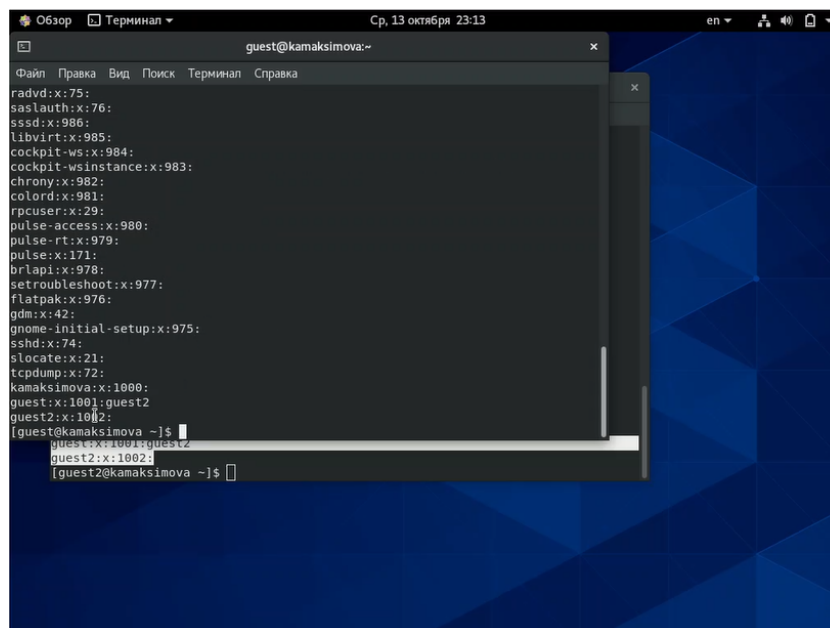


Figure 4.13: Рис 13. guest

Рисунок 13

От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest

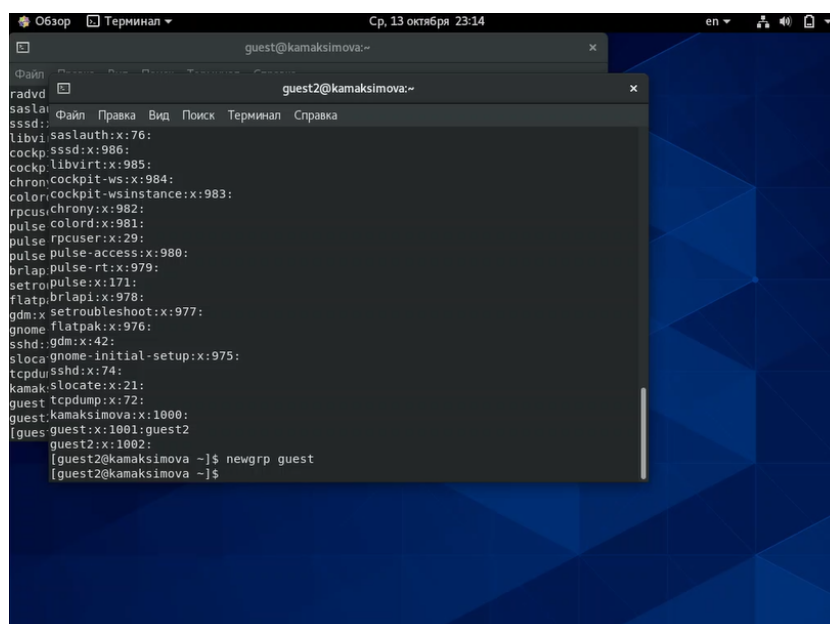


Figure 4.14: Рис 14. Регистрация пользователя guest2

Рисунок 14

От имени пользователя guest изменим права директории “/home/guest”,разре-
шив все действия для пользователей группы

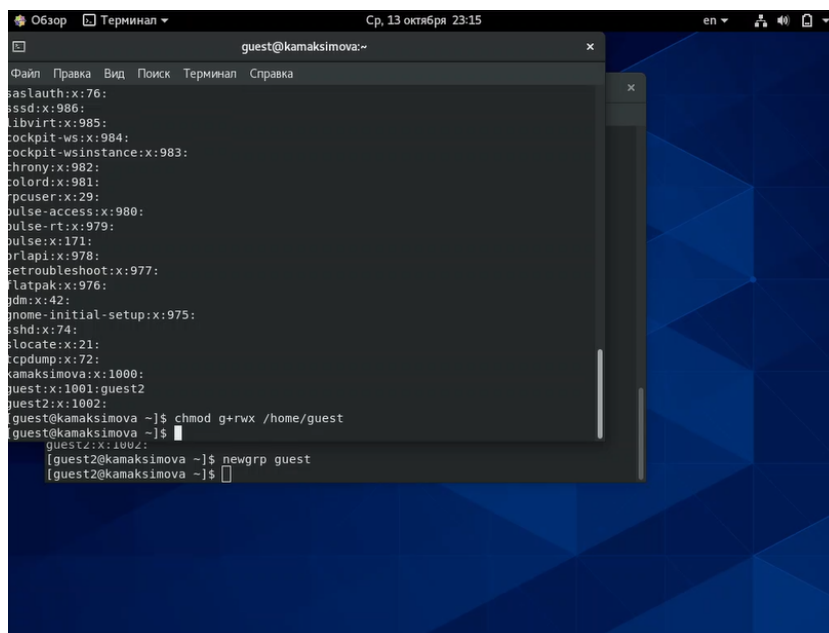


Figure 4.15: Рис 15. Изменение прав директории

Рисунок 15

От имени пользователя guest снимаем с директории “/home/guest/dir1” все
атрибуты

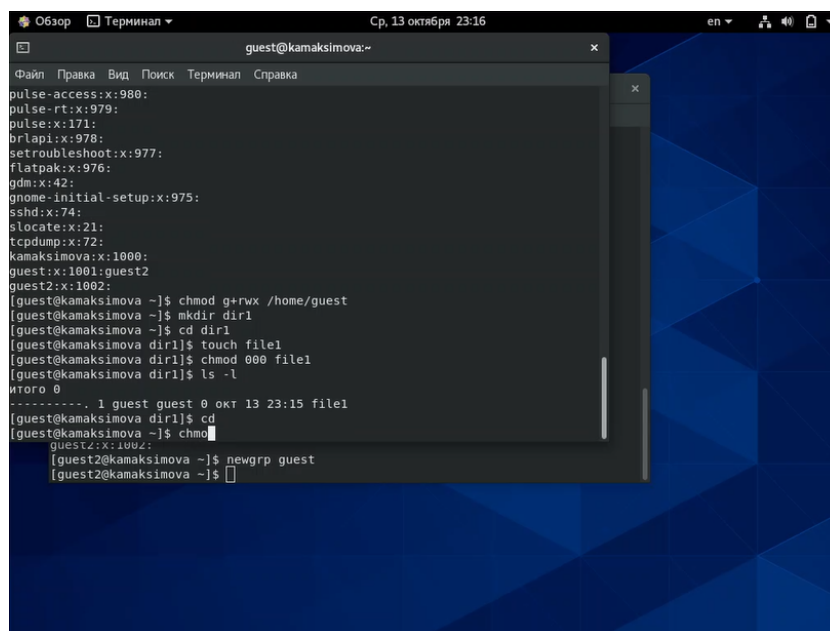


Figure 4.16: Рис 16. Снимаем все права

Рисунок 16

Меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, заполнила таблицу “Разрешенные права и действия для пользователей групп” определив опытным путём, какие операции разрешены, а какие нет.

	A	B	C	D	E	F	G	H	I	J
	Права директории	Права файла	Создание файла (touch)	Удаление файла (rm)	Запись в файл (echo)	Чтение файла (cat)	Смена директории (cd)	Просмотр файлов в директории (ls)	Переименование файла (mv)	Смена атрибута в файла (chmod)
1	(000) d-----	(000) d-----	-	-	-	-	-	-	-	-
2	(010) d-----x		-	-	-	-	+	-	-	-
3	(020) d-----w		-	-	-	-	-	-	-	-
4	(030) d-----wx		+	+	-	-	+	-	-	+
5	(040) d-----f		-	-	-	-	-	-	-	-
6	(050) d-----fx		-	-	-	-	+	+	-	-
7	(060) d-----f-w		-	-	-	-	-	-	-	-
8	(070) d-----f-wx		+	+	+	+	+	+	+	+
9	(000) d-----	(010) d-----x	-	-	-	-	-	-	-	-
10	(010) d-----x		-	-	-	-	+	-	-	+
11	(020) d-----w		-	-	-	-	-	-	-	-
12	(030) d-----wx		+	+	+	+	+	-	+	+
13	(040) d-----f		-	-	-	-	-	-	-	-
14	(050) d-----fx		+	-	-	-	+	+	-	+
15	(060) d-----f-w		-	-	-	-	-	-	-	-
16	(070) d-----f-wx		+	+	-	-	+	+	+	+
17	(000) d-----	(020) d-----w	-	-	-	-	-	-	-	-
18	(010) d-----x		-	-	-	-	+	-	-	-
19	(020) d-----w		-	-	-	-	-	-	-	-
20	(030) d-----wx		+	+	-	-	+	-	+	+
21	(040) d-----f		-	-	-	-	-	-	-	-
22	(050) d-----fx		+	-	-	-	+	+	-	+
23	(060) d-----f-w		-	-	-	-	-	-	-	-
24	(070) d-----f-wx		+	+	+	+	+	+	+	+
25	(000) d-----	(030) d-----wx	-	-	-	-	-	-	-	-
26	(010) d-----x		+	-	-	-	+	-	-	-
27	(020) d-----w		-	-	-	-	-	-	-	-
28	(030) d-----wx		+	+	-	-	+	-	+	+
29	(040) d-----f		-	-	-	-	-	-	-	-
30	(050) d-----fx		-	-	-	-	+	+	-	+
31	(060) d-----f-w		-	-	-	-	-	-	-	-
32	(070) d-----f-wx		+	+	+	+	+	+	+	+
33	(000) d-----	(040) d-----f	-	-	-	-	-	-	-	-
34	(010) d-----x		-	-	-	-	+	+	-	+
35	(020) d-----w		-	-	-	-	-	-	-	-
36	(030) d-----wx		+	+	-	-	+	-	+	+
37	(040) d-----f		-	-	-	-	-	-	-	-
38	(050) d-----fx		+	-	-	-	+	+	-	+
39	(060) d-----f-w		-	-	-	-	-	-	-	-
40	(070) d-----f-wx		+	+	+	+	+	+	+	+
41	(000) d-----	(050) d-----fx	-	-	-	-	-	-	-	-
42	(010) d-----x		-	-	-	-	+	-	-	-
43	(020) d-----w		-	-	-	-	-	-	-	-
44	(030) d-----wx		+	+	-	-	+	-	+	+
45	(040) d-----f		-	-	-	-	-	-	-	-
46	(050) d-----fx		-	-	-	-	+	+	-	+
47	(060) d-----f-w		-	-	-	-	-	-	-	-
48	(070) d-----f-wx		+	+	+	+	+	+	+	+
49	(000) d-----	(060) d-----f-w	-	-	-	-	-	-	-	-
50	(010) d-----x		-	-	-	-	+	+	-	+
51	(020) d-----w		-	-	-	-	-	-	-	-
52	(030) d-----wx		+	+	-	-	+	-	+	+
53	(040) d-----f		-	-	-	-	-	-	-	-
54	(050) d-----fx		-	-	-	-	+	+	-	+
55	(060) d-----f-w		-	-	-	-	-	-	-	-
56	(070) d-----f-wx		+	+	+	+	+	+	+	+

Figure 4.17: Рис 17. Таблица “Разрешенные права и действия для пользователей групп”

Рисунок 17

На основании заполненной таблицы определила те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1

1	Операция	Минимальные права на директорию	Минимальные права на файл
2	Создание файла	'(030)	'(000)
3	Удаление файла	'(030)	'(000)
4	Чтение файла	'(070)	'(000)
5	Запись в файл	'(070)	'(000)
6	Переименование файла	'(030)	'(000)
7	Создание поддиректории	-	-
8	Удаление поддиректории	-	-
9			
10			

Figure 4.18: Рис 18. Таблица “Минимальные права для совершения операций”

Рисунок 18

5 Выводы

В ходе лабораторной работы были установлены разрешенные действия для файла и директории для пользователей групп, а так же были установлены минимально необходимые права для совершения тех или иных действий.

Список литературы

1. Права доступа к файлам в Linux
2. Терминал Linux
3. Разграничение прав доступа