

Лабораторная работа №5

Дискреционное разграничение прав в Linux.

Исследование влияния дополнительных атрибутов

Щербак Маргарита Романовна

НПИБд-02-21

Студ. билет: 1032216537

2024

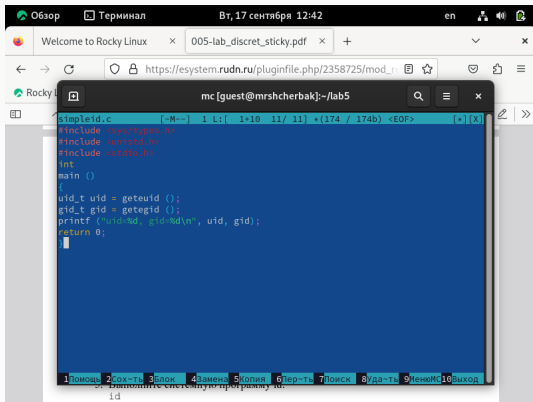
RUDN

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

Информационная безопасность представляет собой защиту данных и поддерживающей инфраструктуры от случайных или преднамеренных воздействий природного или искусственного характера, которые могут нанести ущерб владельцам или пользователям этой информации и инфраструктуры.

Выполнение лабораторной работы. Создание программы

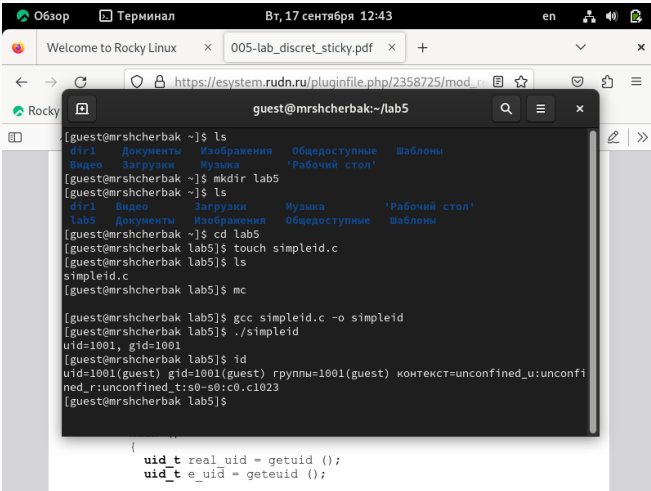
Я подготовила лабораторный стенд. У меня был установлен gcc. Я вошла в систему от имени пользователя guest. Создала программу simpleid.c.



```
simpleid.c (-M-- 1 L: 1*10 11/ 11) *(174 / 174b) <EOF> (*) [X]
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getgid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

Рис. 1: Содержимое программы simpleid.c

Выполнение лабораторной работы



The screenshot shows a terminal window titled "guest@mrshcherbak:~/lab5" with the following commands and output:

```
[guest@mrshcherbak ~]$ ls
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка  'Рабочий стол'
[guest@mrshcherbak ~]$ mkdir lab5
[guest@mrshcherbak ~]$ ls
dir1  Видео  Загрузки  Музыка  'Рабочий стол'
lab5  Документы  Изображения  Общедоступные  Шаблоны
[guest@mrshcherbak ~]$ cd lab5
[guest@mrshcherbak lab5]$ touch simpleid.c
[guest@mrshcherbak lab5]$ ls
simpleid.c
[guest@mrshcherbak lab5]$ mc

[guest@mrshcherbak lab5]$ gcc simpleid.c -o simpleid
[guest@mrshcherbak lab5]$ ./simpleid
uid=1001, gid=1001
[guest@mrshcherbak lab5]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@mrshcherbak lab5]$
```

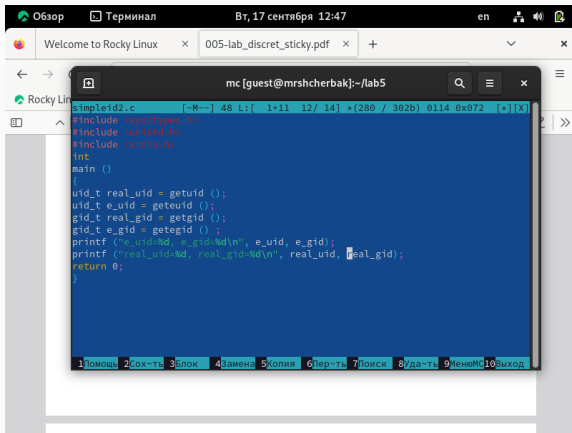
Below the terminal window, the following code snippet is visible:

```
{
    uid_t real_uid = getuid ();
    uid_t e_uid = geteuid ();
```

Рис. 2: Выполнение команд

Выполнение лабораторной работы

Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c.



```
simpleid2.c [-M--] 48 L: [ 1+11 12/ 14] *(280 / 302b) 0114 0x072 [*](X)
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>
int
main ()
{
    uid_t real_uid = getuid ();
    uid_t e_uid = geteuid ();
    gid_t real_gid = getgid ();
    gid_t e_gid = getegid ();
    printf ("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf ("real_uid=%d, real_gid=%d\n", real_uid, real_gid);
    return 0;
}
```

Рис. 3: Усложненная программа

Выполнение лабораторной работы

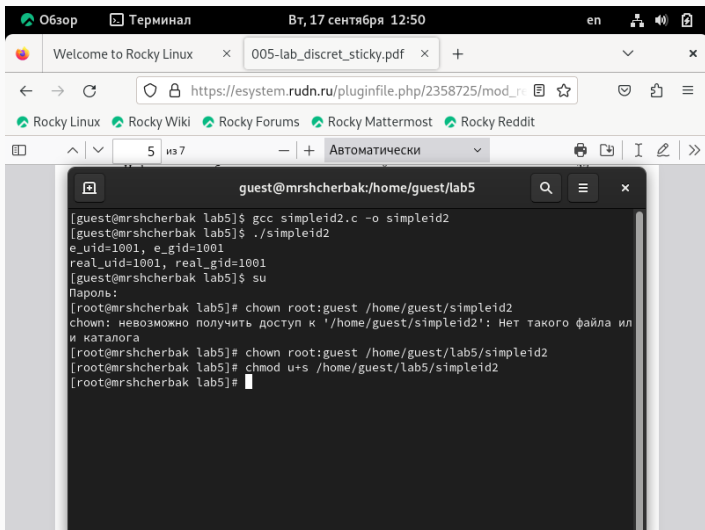
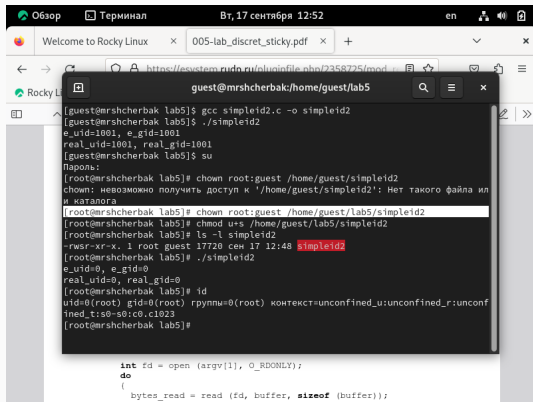


Рис. 4: Выполнение команд

Выполнение лабораторной работы

Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустила simpleid2 и id. Результаты совпадают.



```
guest@mrshcherbak:/home/guest/lab5
[guest@mrshcherbak lab5]$ gcc simpleid2.c -o simpleid2
[guest@mrshcherbak lab5]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@mrshcherbak lab5]$ su
Пароль:
[root@mrshcherbak lab5]# chown root:guest /home/guest/simpleid2
chown: невозможно получить доступ к '/home/guest/simpleid2': Нет такого файла или каталога
[root@mrshcherbak lab5]# chown root:guest /home/guest/lab5/simpleid2
[root@mrshcherbak lab5]# chmod u+s /home/guest/lab5/simpleid2
[root@mrshcherbak lab5]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 17720 сен 17 12:48 simpleid2
[root@mrshcherbak lab5]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@mrshcherbak lab5]# id
uid=0(root) gid=0(root) rpnnyu=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@mrshcherbak lab5]#

int fd = open (argv[1], O_RDONLY);
do
{
    bytes_read = read (fd, buffer, sizeof (buffer));
    ...
```

Рис. 5: Выполнение команд

Выполнение лабораторной работы

Прodelала то же самое относительно SetGID-бита. Создала программу readfile.c.

```
readfile.c  [-M--]  1 L:  2+19  21/ 21]  +(401 / 401b)  <EOF>  [*][X]
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read (fd, buffer, sizeof (buffer));
        for (i = 0; i < bytes_read; ++i) printf ("%c", buffer[i]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
```

1.Помощь 2.Сок-ть 3.Блок 4.Замена 5.Копия 6.Пер-ть 7.Поиск 8.Уда-ть 9.Меню 10.Выход

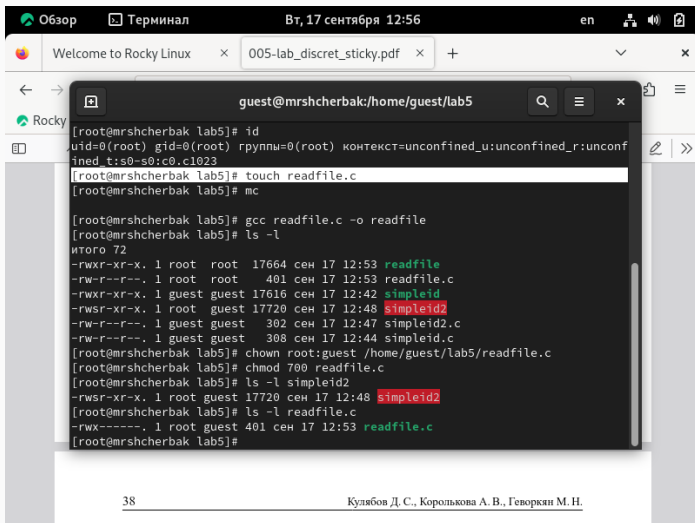
(root) мог прочитать его, а guest не мог.

16. Проверьте, что пользователь guest не может прочитать файл readfile.c.

17. Смените у программы readfile владельца и установите SetU'D-бит.

Рис. 6: Содержимое программы readfile.c

Выполнение лабораторной работы



The screenshot shows a terminal window titled "guest@mrshcherbak:/home/guest/lab5". The user is root. The terminal output is as follows:

```
[root@mrshcherbak lab5]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@mrshcherbak lab5]# touch readfile.c
[root@mrshcherbak lab5]# mc

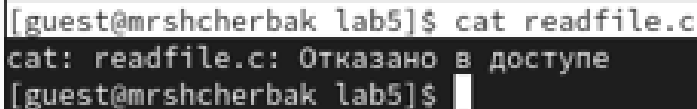
[root@mrshcherbak lab5]# gcc readfile.c -o readfile
[root@mrshcherbak lab5]# ls -l
итого 72
-rwxr-xr-x. 1 root root 17664 сен 17 12:53 readfile
-rw-r--r--. 1 root root 401 сен 17 12:53 readfile.c
-rwxr-xr-x. 1 guest guest 17616 сен 17 12:42 simpleid
-rwsr-xr-x. 1 root guest 17720 сен 17 12:48 simpleid2
-rw-r--r--. 1 guest guest 302 сен 17 12:47 simpleid2.c
-rw-r--r--. 1 guest guest 308 сен 17 12:44 simpleid.c
[root@mrshcherbak lab5]# chown root:guest /home/guest/lab5/readfile.c
[root@mrshcherbak lab5]# chmod 700 readfile.c
[root@mrshcherbak lab5]# ls -l simpleid2
-rwsr-xr-x. 1 root guest 17720 сен 17 12:48 simpleid2
[root@mrshcherbak lab5]# ls -l readfile.c
-rwx-----. 1 root guest 401 сен 17 12:53 readfile.c
[root@mrshcherbak lab5]#
```

At the bottom of the terminal window, the page number "38" is visible on the left and the authors "Кулябов Д. С., Королькова А. В., Геворкян М. Н." are listed on the right.

Рис. 7: Смена владельца

Выполнение лабораторной работы

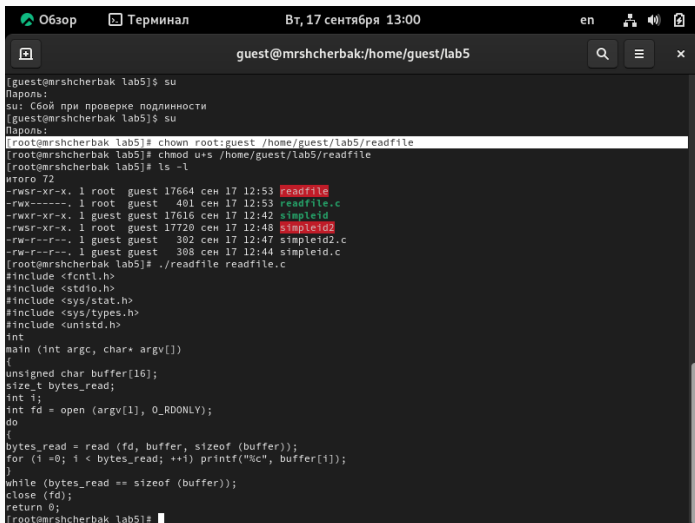
Проверила, что пользователь guest не может прочитать файл readfile.c.

A terminal window with a black background and white text. The prompt is [guest@mrshcherbak lab5]\$. The user enters 'cat readfile.c'. The output is 'cat: readfile.c: Отказано в доступе'. The prompt returns to [guest@mrshcherbak lab5]\$.

```
[guest@mrshcherbak lab5]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@mrshcherbak lab5]$
```

Рис. 8: Проверка

Выполнение лабораторной работы

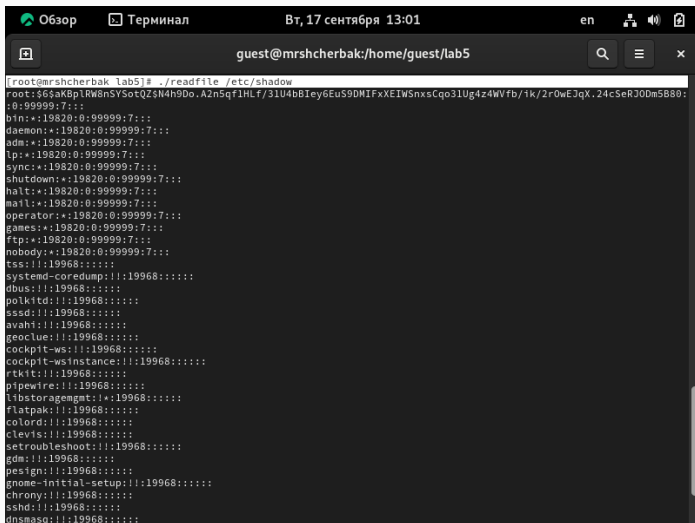


```
Обзор Терминал Вт, 17 сентября 13:00 en
guest@mrshcherbak:/home/guest/lab5

[guest@mrshcherbak lab5]$ su
Пароль:
su: Сбой при проверке подлинности
[guest@mrshcherbak lab5]$ su
Пароль:
[root@mrshcherbak lab5]# chown root:guest /home/guest/lab5/readfile
[root@mrshcherbak lab5]# chmod u+s /home/guest/lab5/readfile
[root@mrshcherbak lab5]# ls -l
итого 72
-rwsr-xr-x. 1 root guest 17664 сен 17 12:53 readfile
-rwx----- 1 root guest 401 сен 17 12:53 readfile.c
-rwxr-xr-x. 1 guest guest 17616 сен 17 12:42 simpleid
-rwsr-xr-x. 1 root guest 17720 сен 17 12:48 simpleid2
-rw-r--r--. 1 guest guest 302 сен 17 12:47 simpleid2.c
-rw-r--r--. 1 guest guest 308 сен 17 12:44 simpleid.c
[root@mrshcherbak lab5]# ./readfile readfile.c
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
int
main (int argc, char* argv[])
{
    unsigned char buffer[16];
    size_t bytes_read;
    int i;
    int fd = open (argv[1], O_RDONLY);
    do
    {
        bytes_read = read (fd, buffer, sizeof (buffer));
        for (i = 0; i < bytes_read; ++i) printf("%c", buffer[i]);
    }
    while (bytes_read == sizeof (buffer));
    close (fd);
    return 0;
}
[root@mrshcherbak lab5]#
```

Рис. 9: Проверка

Выполнение лабораторной работы

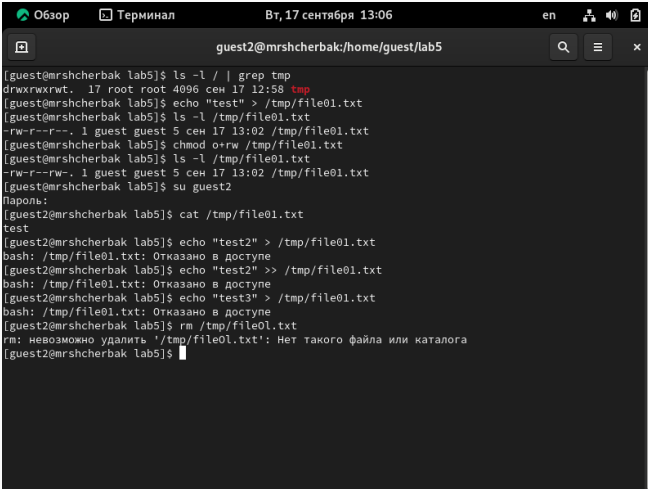


The screenshot shows a terminal window with a dark theme. The title bar at the top indicates the current view is 'Обзор' (Overview) and the active window is 'Терминал' (Terminal). The system time is 'Вт, 17 сентября 13:01' (Tuesday, September 17, 13:01). The user is logged in as 'en'. The terminal address bar shows the current directory as 'guest@mrshcherbak:/home/guest/lab5'. The terminal content shows the command `cat /etc/shadow` being executed, displaying the shadow file's contents. The output lists system users and their password hashes, all using the `!$` hash, indicating they are inactive or disabled accounts. The users listed include `bin`, `daemon`, `adm`, `lp`, `sync`, `shutdown`, `halt`, `mail`, `operator`, `games`, `ftp`, `nobody`, `tss`, `systemd-coredump`, `dbus`, `polkitd`, `sssd`, `avahi`, `geoclue`, `cockpit-ws`, `cockpit-wsinstance`, `rtkit`, `pipewire`, `libstoragemgmt`, `flatpak`, `colord`, `cleviis`, `setroubleshoot`, `gdm`, `pesign`, `gnome-initial-setup`, `chrony`, `sshd`, and `dnsmasq`.

```
root@mrshcherbak lab5]# ./readfile /etc/shadow
root:$6$aKBPiRW8nSVSotQZ$N4h9Do.Azn5qfIHLf/3lU4b8Iey6EuS9DMIFxXEIWSnxsCqo3lUg4z4wVfb/1k/2r0wEJqX.24cSeR30Dm5B80:
0:99999:7:::
bin:!:19820:0:99999:7:::
daemon:!:19820:0:99999:7:::
adm:!:19820:0:99999:7:::
lp:!:19820:0:99999:7:::
sync:!:19820:0:99999:7:::
shutdown:!:19820:0:99999:7:::
halt:!:19820:0:99999:7:::
mail:!:19820:0:99999:7:::
operator:!:19820:0:99999:7:::
games:!:19820:0:99999:7:::
ftp:!:19820:0:99999:7:::
nobody:!:19820:0:99999:7:::
tss:!:19968:!!!!:
systemd-coredump:!:19968:!!!!:
dbus:!:19968:!!!!:
polkitd:!:19968:!!!!:
sssd:!:19968:!!!!:
avahi:!:19968:!!!!:
geoclue:!:19968:!!!!:
cockpit-ws:!:19968:!!!!:
cockpit-wsinstance:!:19968:!!!!:
rtkit:!:19968:!!!!:
pipewire:!:19968:!!!!:
libstoragemgmt:!:19968:!!!!:
flatpak:!:19968:!!!!:
colord:!:19968:!!!!:
cleviis:!:19968:!!!!:
setroubleshoot:!:19968:!!!!:
gdm:!:19968:!!!!:
pesign:!:19968:!!!!:
gnome-initial-setup:!:19968:!!!!:
chrony:!:19968:!!!!:
sshd:!:19968:!!!!:
dnsmasq:!:19968:!!!!:
```

Рис. 10: Проверка

Выполнение лабораторной работы. Исследование Sticky-бита



```
Обзор Терминал Вт, 17 сентября 13:06 en
guest2@mrshcherbak:/home/guest/lab5

[guest@mrshcherbak lab5]$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 сен 17 12:58 tmp
[guest@mrshcherbak lab5]$ echo "test" > /tmp/file01.txt
[guest@mrshcherbak lab5]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 17 13:02 /tmp/file01.txt
[guest@mrshcherbak lab5]$ chmod o+rw /tmp/file01.txt
[guest@mrshcherbak lab5]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 17 13:02 /tmp/file01.txt
[guest@mrshcherbak lab5]$ su guest2
Пароль:
[guest2@mrshcherbak lab5]$ cat /tmp/file01.txt
test
[guest2@mrshcherbak lab5]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@mrshcherbak lab5]$ echo "test2" >> /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@mrshcherbak lab5]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Отказано в доступе
[guest2@mrshcherbak lab5]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Нет такого файла или каталога
[guest2@mrshcherbak lab5]$
```

Рис. 11: Выполнение команд

Выполнение лабораторной работы

```
[guest2@mrshcherbak lab5]$ su -  
Пароль:  
[root@mrshcherbak ~]# chmod -t /tmp  
[root@mrshcherbak ~]# exit  
выход  
[guest2@mrshcherbak lab5]$ ls -l / | grep tmp  
drwxrwxrwx. 18 root root 4096 сен 17 13:07 tmp  
[guest2@mrshcherbak lab5]$
```

Рис. 12: Снятие Sticky-бита

Выполнение лабораторной работы

Повторила предыдущие шаги. Повысила свои права до суперпользователя и вернула атрибут `t` на директорию `/tmp`.

```
[guest2@mrshcherbak guest]$ cat /tmp/file01.txt
test
[guest2@mrshcherbak guest]$ echo "test2" >>/tmp/file01.txt
[guest2@mrshcherbak guest]$ cat /tmp/file01.txt
test
test2
[guest2@mrshcherbak guest]$ echo "test3" >/tmp/file01.txt
[guest2@mrshcherbak guest]$ cat /tmp/file01.txt
test3
[guest2@mrshcherbak guest]$ rm /tmp/file01.txt
[guest2@mrshcherbak guest]$ su -
Пароль:
[root@mrshcherbak ~]# chmod +t /tmp
[root@mrshcherbak ~]# exit
выход
[guest2@mrshcherbak guest]$
```

Рис. 13: Возвращение Sticky-бита

Таким образом, в ходе ЛРН№5 я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

1. Методические материалы курса.
2. Chmod. [Электронный ресурс]. М. URL: Файловая система (Дата обращения: 17.09.2024).