

# Отчёт по лабораторной работе №5

# **Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов**

# 1. Создание кода `simpleid`

Создан код `simpleid.c` (рис.1).

```
guest@vgkupatenko:~/dir1
Файл Правка Вид Поиск Терминал Справка
simpleid.c [----] 34 L: [ 1+ 9 10/ 12] *(167 / 194b) 0032 0x020 [*][X]
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf("uid = %d, gid = %d\n", uid, gid);
    return 0;
}

1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Перейти 7Поиск 8Удалить 9МенюМС 10Выход
```

Рисунок №1: simpleid.c

Проведена компиляция кода и сравнение с id  
(рис.2).

The image shows a terminal window titled "vgkupatenko [Работает] - Oracle VM VirtualBox". The window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". Below the menu bar is a toolbar with "Обзор" and "Терминал". The terminal itself has a title bar "guest@vgkupatenko:~/dir1" and a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal output shows the following commands and results:

```
[guest@vgkupatenko dir1]$ gcc simpleid.c -o simpleid
[guest@vgkupatenko dir1]$ ./simpleid
uid = 1001, gid = 1001
[guest@vgkupatenko dir1]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@vgkupatenko dir1]$
```

Рисунок №2: Компиляция simpleid.c

Модифицирован код simpleid (рис.3).

```
guest@vgkupatenko:~/dir1
Файл  Правка  Вид  Поиск  Терминал  Справка
simpleid2.c  [----]  0 L:[ 1+15 16/ 18] *(331 / 347b) 0010 0x00A [*][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);

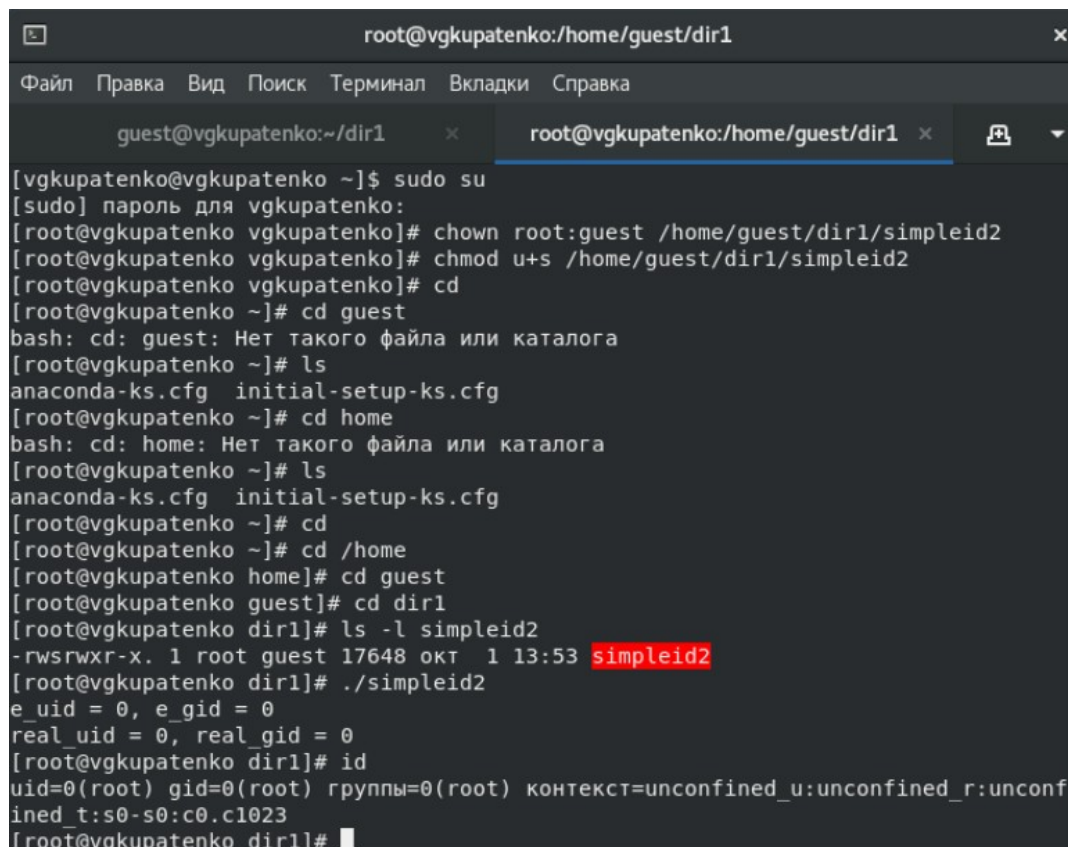
    return 0;
}

1Помощь 2Сохранить 3Блок 4Замена 5Копия 6Перейти 7Поиск 8Удалить 9МенюМС10Выход
```

Рисунок №3: simpleid2.c



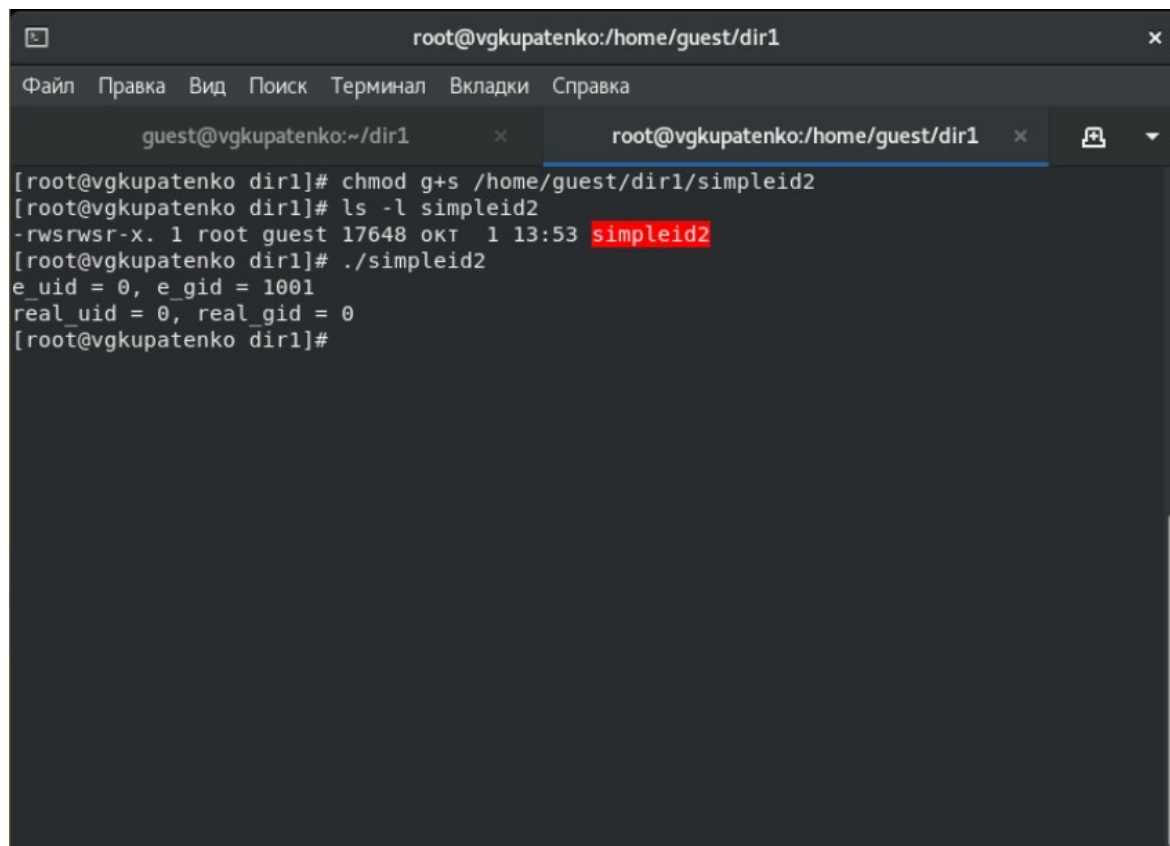
Выполнены команды с правами от имени суперпользователя. (рис. 4).



```
root@vgkupatenko:/home/guest/dir1
Файл Правка Вид Поиск Терминал Вкладки Справка
guest@vgkupatenko:~/dir1 x root@vgkupatenko:/home/guest/dir1 x
[vgkupatenko@vgkupatenko ~]$ sudo su
[sudo] пароль для vgkupatenko:
[root@vgkupatenko vgkupatenko]# chown root:guest /home/guest/dir1/simpleid2
[root@vgkupatenko vgkupatenko]# chmod u+s /home/guest/dir1/simpleid2
[root@vgkupatenko vgkupatenko]# cd
[root@vgkupatenko ~]# cd guest
bash: cd: guest: Нет такого файла или каталога
[root@vgkupatenko ~]# ls
anaconda-ks.cfg initial-setup-ks.cfg
[root@vgkupatenko ~]# cd home
bash: cd: home: Нет такого файла или каталога
[root@vgkupatenko ~]# ls
anaconda-ks.cfg initial-setup-ks.cfg
[root@vgkupatenko ~]# cd
[root@vgkupatenko ~]# cd /home
[root@vgkupatenko home]# cd guest
[root@vgkupatenko guest]# cd dir1
[root@vgkupatenko dir1]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 17648 окт 1 13:53 simpleid2
[root@vgkupatenko dir1]# ./simpleid2
e_uid = 0, e_gid = 0
real_uid = 0, real_gid = 0
[root@vgkupatenko dir1]# id
uid=0(root) gid=0(root) группы=0(root) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@vgkupatenko dir1]#
```

Рисунок №4: Опыты с правами

Повторение операции относительно GID бита  
(рис. 5).



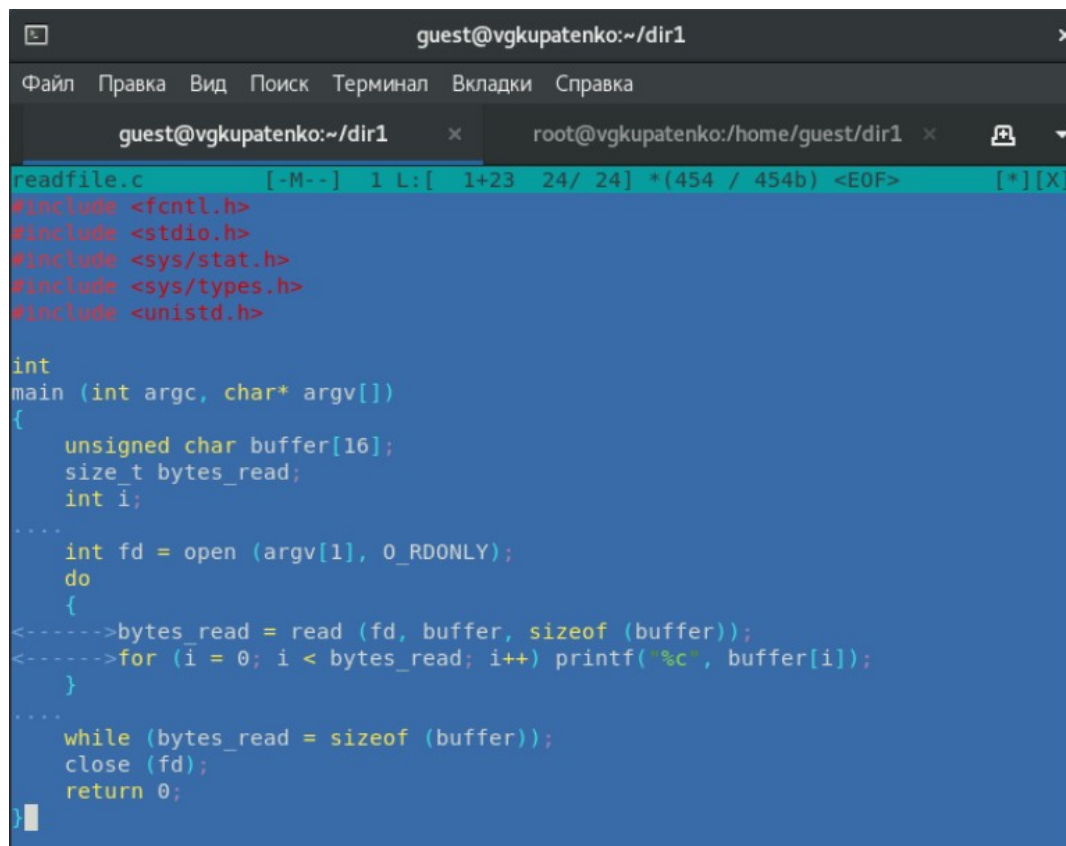
The image shows a terminal window with a dark background. The title bar at the top reads "root@vgkupatenko:/home/guest/dir1". Below the title bar is a menu bar with options: "Файл", "Правка", "Вид", "Поиск", "Терминал", "Вкладки", and "Справка". There are two tabs open: "guest@vgkupatenko:~/dir1" and "root@vgkupatenko:/home/guest/dir1", with the latter being the active tab. The terminal content shows the following commands and output:

```
[root@vgkupatenko dir1]# chmod g+s /home/guest/dir1/simpleid2
[root@vgkupatenko dir1]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 17648 окт 1 13:53 simpleid2
[root@vgkupatenko dir1]# ./simpleid2
e_uid = 0, e_gid = 1001
real_uid = 0, real_gid = 0
[root@vgkupatenko dir1]#
```

Рисунок №5: Повторение для GID-bit

## **2. Создание кода readfile**

Создан код readfile.c (рис. 6).



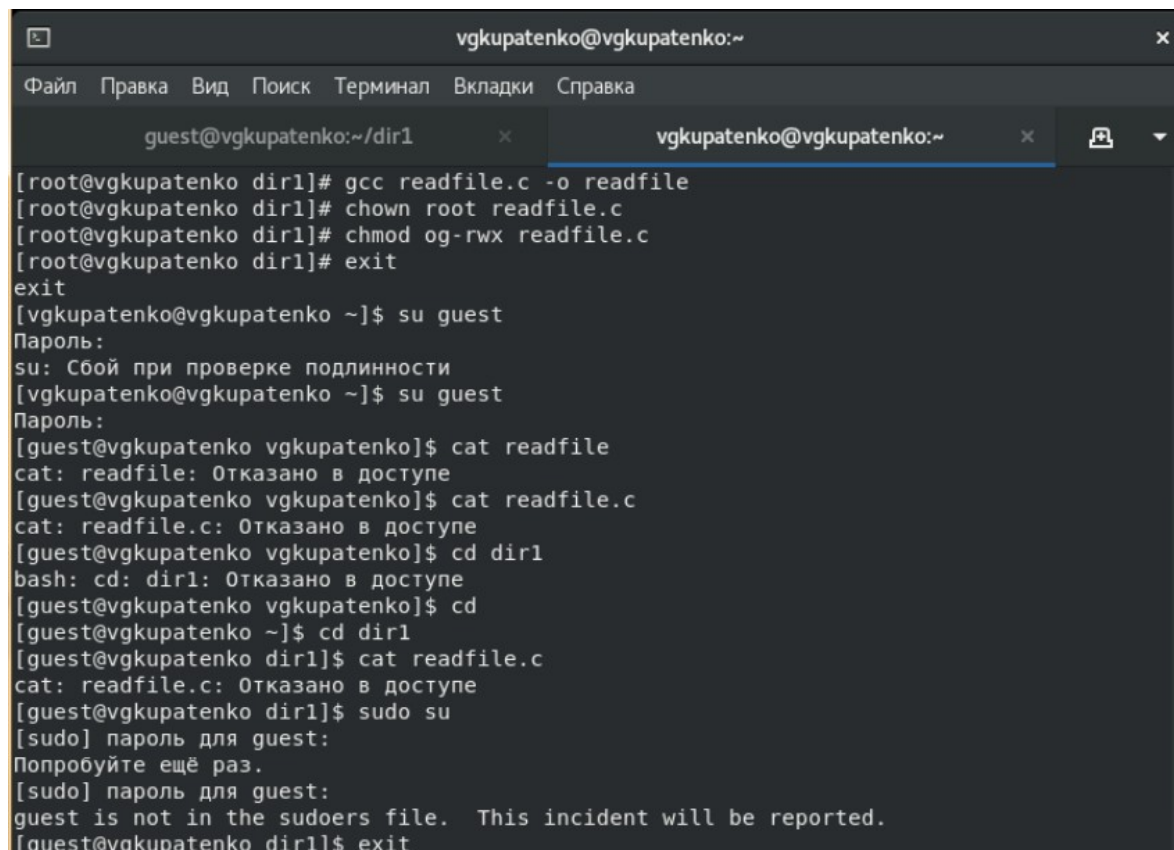
```
readfile.c [-M--] 1 L: [ 1+23 24/ 24] *(454 / 454b) <EOF> [*][X]
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

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;
}
```

Рисунок №6: readfile.c

Компиляция кода readfile и работа с правами  
(рис. 7).



```
vgkupatenko@vgkupatenko:~  
Файл Правка Вид Поиск Терминал Вкладки Справка  
guest@vgkupatenko:~/dir1 x vgkupatenko@vgkupatenko:~ x  
[root@vgkupatenko dir1]# gcc readfile.c -o readfile  
[root@vgkupatenko dir1]# chown root readfile.c  
[root@vgkupatenko dir1]# chmod og-rwx readfile.c  
[root@vgkupatenko dir1]# exit  
exit  
[vgkupatenko@vgkupatenko ~]$ su guest  
Пароль:  
su: Сбой при проверке подлинности  
[vgkupatenko@vgkupatenko ~]$ su guest  
Пароль:  
[guest@vgkupatenko vgkupatenko]$ cat readfile  
cat: readfile: Отказано в доступе  
[guest@vgkupatenko vgkupatenko]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@vgkupatenko vgkupatenko]$ cd dir1  
bash: cd: dir1: Отказано в доступе  
[guest@vgkupatenko vgkupatenko]$ cd  
[guest@vgkupatenko ~]$ cd dir1  
[guest@vgkupatenko dir1]$ cat readfile.c  
cat: readfile.c: Отказано в доступе  
[guest@vgkupatenko dir1]$ sudo su  
[sudo] пароль для guest:  
Попробуйте ещё раз.  
[sudo] пароль для guest:  
guest is not in the sudoers file. This incident will be reported.  
[guest@vgkupatenko dir1]$ exit
```

Рисунок №7: Компиляция readfile.c



Сменил владельца у файла `readfile.c` и изменил права так, чтобы только суперпользователь (`root`) мог прочитать его, а `guest` не мог. Проверил, что пользователь `guest` не может прочитать файл `readfile.c`. Сменил у программы `readfile` владельца и установил SetU'D-бит. Проверил, может ли программа `readfile` прочитать файл `readfile.c` (рис. 8).

```

exit
[vgkupatenko@vgkupatenko ~]$ sudo su
[sudo] пароль для vgkupatenko:
[root@vgkupatenko vgkupatenko]# cd
[root@vgkupatenko ~]# cd /home
[root@vgkupatenko home]# cd guest
[root@vgkupatenko guest]# cd dir1
[root@vgkupatenko dir1]# chmod u+s readfile
[root@vgkupatenko dir1]# ./readfile
0000@'0[00]y[00]K[00]X[00]y[00]gRL[00]X[00]0[00]5Lf000*f00@'0[00]^@0&0[00] 0Lf0[00]60[00]60[00]60[00]=0[00]=0[00]=0[00]=0[00]=0[00]
00=0[00]0[00]0[00]0[00]0[00],>0[00]6>0[00]K>0[00]~>0[00]>0[00]>0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]
?0[00]0[00]?0[00]0[00]?0[00]100[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]0[00]
) f0 0@

)0[00]0[00]?0[00]9)0[00]k000[00]0[00]000000Sxx66_64./readfileLS_COLORS=rs=0:di=38;5;33:ln=38;5;51:
mh=00:pi=40;38;5;11:so=38;5;13:do=38;5;5:bd=48;5;232;38;5;11:cd=48;5;232;38;5;3:or=48;5
;232;38;5;9:mi=01;05;37;41:su=48;5;196;38;5;15:sg=48;5;11;38;5;16:ca=48;5;196;38;5;226:
tw=48;5;10;38;5;16:ow=48;5;10;38;5;21:st=48;5;21;38;5;15:ex=38;5;40:*.tar=38;5;9:*.tgz=
38;5;9:*.arc=38;5;9:*.arj=38;5;9:*.taz=38;5;9:*.lha=38;5;9:*.lz4=38;5;9:*.lzh=38;5;9:*.
lzma=38;5;9:*.tlz=38;5;9:*.txz=38;5;9:*.tzo=38;5;9:*.t7z=38;5;9:*.zip=38;5;9:*.z=38;5;9
:*.dz=38;5;9:*.gz=38;5;9:*.lrz=38;5;9:*.lz=38;5;9:*.lzo=38;5;9:*.xz=38;5;9:*.zst=38;5;9
:*.tzst=38;5;9:*.bz2=38;5;9:*.bz=38;5;9:*.tbz=38;5;9:*.tbz2=38;5;9:*.tz=38;5;9:*.deb=38
;5;9:*.rpm=38;5;9:*.jar=38;5;9:*.war=38;5;9:*.ear=38;5;9:*.sar=38;5;9:*.rar=38;5;9:*.al
z=38;5;9:*.ace=38;5;9:*.zoo=38;5;9:*.cpio=38;5;9:*.7z=38;5;9:*.rz=38;5;9:*.cab=38;5;9:*
.wim=38;5;9:*.swm=38;5;9:*.dwm=38;5;9:*.esd=38;5;9:*.jpg=38;5;13:*.jpeg=38;5;13:*.mjpg=
38;5;13:*.mjpeg=38;5;13:*.gif=38;5;13:*.bmp=38;5;13:*.pbm=38;5;13:*.pgm=38;5;13:*.ppm=3
8;5;13:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;13:*.tif=38;5;13:*.tiff=38;5;13:*.png=38;

```

Рисунок №8: Изменение прав readfile

### 3. Исследование Sticky-bit

Выяснил, установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создал файл file01.txt в директории/tmp со словом test. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» (рис. 9).

```
guest2@vgkupatenko:/home/vgkupatenko x root@vgkupatenko:/home/guest/dir1 x
guest@vgkupatenko ~]$ ls -l / | grep tmp
-rwxrwxrwt. 12 root root 4096 окт 1 14:52 tmp
guest@vgkupatenko ~]$ echo > "test" >/tmp/file01.txt
guest@vgkupatenko ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 1 окт 1 14:54 /tmp/file01.txt
guest@vgkupatenko ~]$ chmod o+rw /tmp/file01.txt
guest@vgkupatenko ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 1 окт 1 14:54 /tmp/file01.txt
guest@vgkupatenko ~]$ exit
exit
vgkupatenko@vgkupatenko ~]$ su guest2
пароль:
guest2@vgkupatenko vgkupatenko]$ cat /tmp/file01.txt

guest2@vgkupatenko vgkupatenko]$ echo "test2" > /tmp/file01.txt
guest2@vgkupatenko vgkupatenko]$ cat /tmp/file01.txt
test2
guest2@vgkupatenko vgkupatenko]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
guest2@vgkupatenko vgkupatenko]$ su -
пароль:
root@vgkupatenko ~]# chmod -t /tmp
root@vgkupatenko ~]# exit
выход
guest2@vgkupatenko vgkupatenko]$ ls -l / | grep tmp
-rwxrwxrwt. 12 root root 4096 окт 1 15:00 tmp
```

Рисунок №9: Исследование Sticky-bit

От пользователя guest2 попробовал прочитать файл /tmp/file01.txt. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию. Удалось выполнить операцию. Проверил содержимое файла. От пользователя guest2 попробовал удалить

```
[guest2@vgkupatenko vgkupatenko]$ ls -l / | grep tmp
drwxrwxrwx. 12 root root 4096 окт  1 15:00 tmp
[guest2@vgkupatenko vgkupatenko]$ echo "test2" > /tmp/file01.txt
[guest2@vgkupatenko vgkupatenko]$ cat /tmp/file01.txt
test2
[guest2@vgkupatenko vgkupatenko]$ rm /tmp/file01.txt
[guest2@vgkupatenko vgkupatenko]$ su -
Пароль:
[root@vgkupatenko ~]# chmod +t /tmp
[root@vgkupatenko ~]# exit
выход
[guest2@vgkupatenko vgkupatenko]$
```

Рисунок №10: Возвращение атрибута t

# Выводы

Были изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрены работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.