

Цель работы

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.

Выполнение лабораторной работы

Часть №1

1. Вошел в систему от имени пользователя guest.
2. Создал программу simpleid.c: ([рис.№1](#))

```
[guest@localhost ~]$ touch simpleid.c
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      Templates
dir1     Downloads  Pictures   simpleid.c  Videos
```

3. Скомпилировал программу и убедился, что файл программы создан: ([рис.№2](#))

```
[guest@localhost ~]$ gcc simpleid.c -o simpleid
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      simpleid.c  Videos
dir1     Downloads  Pictures   simpleid    Templates
```

4. Выполнил программу simpleid. ([рис.№3](#))

```
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
```

5. Сравнил id пользователя и группы пользователей через команду id, при проверке с прошлым пунктом - результат одинаковый. ([рис.№4](#))

```
[guest@localhost ~]$ ./simpleid
uid=1001, gid=1001
[guest@localhost ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest),10(wheel) context=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$
```

6. Усложнил программу, добавив вывод действительных идентификаторов.
7. Скомпилировал и запустил simpleid2.c:

lsattr /home/guest/dir1/file1 ([рис.№5](#))

```
[guest@localhost ~]$ gcc simpleid2.c -o simpleid2
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      simpleid2  simpleid.c  Videos
dir1     Downloads  Pictures   simpleid    simpleid2.c  Templates
[guest@localhost ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@localhost ~]$
```

8. От имени суперпользователя выполните команды:
chown root:guest /home/guest/simpleid2, chmod u+s /home/guest/simpleid2 ([рис.№6](#))

```
guest@localhost:/home/guest

[root@localhost guest]# chown root:guest /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Desktop
drwx----- 2 guest guest 19 Sep 26 14:49 dirl
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest 53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwxrwxr-x. 1 root guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r-- 1 guest guest 304 Oct 3 16:24 simpleid2.c
-rw-rw-r-- 1 guest guest 175 Oct 3 16:11 simpleid.c
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Videos
[root@localhost guest]# chmod u+s /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Desktop
drwx----- 2 guest guest 19 Sep 26 14:49 dirl
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest 53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwsrwxr-x. 1 root guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r-- 1 guest guest 304 Oct 3 16:24 simpleid2.c
-rw-rw-r-- 1 guest guest 175 Oct 3 16:11 simpleid.c
```

9. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2: `ls -l simpleid2`.

10. Запустил simpleid2 и id. ([рис.№7](#))

```
[root@localhost guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost guest]#
```

11. Прделал тоже самое относительно SetGID-бита. ([рис.№8](#))

```
guest@localhost:/home/guest

[root@localhost guest]# chmod g+s /home/guest/simpleid2
[root@localhost guest]# ls -l
total 64
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Desktop
drwx----- 2 guest guest 19 Sep 26 14:49 dirl
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Documents
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Music
drwxr-xr-x. 2 guest guest 53 Oct 3 16:13 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Public
-rwxrwxr-x. 1 guest guest 25904 Oct 3 16:11 simpleid
-rwsrwxr-x. 1 root guest 26008 Oct 3 16:24 simpleid2
-rw-rw-r-- 1 guest guest 304 Oct 3 16:24 simpleid2.c
-rw-rw-r-- 1 guest guest 175 Oct 3 16:11 simpleid.c
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Templates
drwxr-xr-x. 2 guest guest 6 Sep 14 13:11 Videos
[root@localhost guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@localhost guest]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost guest]#
```

13. Создал программу 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;
}

```

14. Скомпилировал её. [\(рис.№9\)](#)

```

[guest@localhost ~]$ touch readfile.c
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      simpleid      simpleid2.c  Templates
dir1     Downloads  Pictures   readfile.c  simpleid2     simpleid.c   Videos
[guest@localhost ~]$ gcc readfile.c -o readfile
/usr/bin/ld: /usr/lib/gcc/x86_64-redhat-linux/11/../../../../lib64/crt1.o: in function `_start':
(.text+0x1b): undefined reference to `main'
collect2: error: ld returned 1 exit status
[guest@localhost ~]$ gcc readfile.c -o readfile
[guest@localhost ~]$ ls
Desktop  Documents  Music      Public      readfile.c    simpleid2     simpleid.c   Videos
dir1     Downloads  Pictures   readfile    simpleid      simpleid2.c  Templates
[guest@localhost ~]$

```

15. Сменил владельца у файла readfile.c на vnikikita и изменил права так, чтобы только суперпользователь мог прочитать его, а guest не мог. [\(рис.№10\)](#)

```

guest@localhost:/home/guest
[root@localhost guest]# chown vnikikita readfile.c
[root@localhost guest]# ls -l readfile.c
-rw-rw-r--. 1 vnikikita guest 403 Oct  3 16:40 readfile.c
[root@localhost guest]# chmod ugo-r readfile.c
[root@localhost guest]# ls -l readfile.c
--w--w----. 1 vnikikita guest 403 Oct  3 16:40 readfile.c
[root@localhost guest]# cat 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@localhost guest]#

```

16. Сменил у программы readfile владельца и установите SetUID-бит (рис.№11)

```

[guest@localhost: /home/guest]
[guest@localhost guest]# chown vnikita readfile
[guest@localhost guest]# ls -l readfile
-rwxrwxr-x. 1 vnikita guest 25952 Oct  3 16:40 readfile
[guest@localhost guest]# chmod u+s readfile
[guest@localhost guest]# ls -l readfile
ls: cannot access '-': No such file or directory
ls: cannot access 'l': No such file or directory
readfile
[guest@localhost guest]# ls -l readfile
-rwxrwxr-x. 1 vnikita guest 25952 Oct  3 16:40 readfile
[guest@localhost guest]#

```

17. Проверил, может ли программа readfile прочитать файл readfile.c - да может. (рис.№12)

```
[root@localhost guest]# ./readfile = readfile.c
@00<10000000000P00>L@e@08c'0GGGsg'8Cv@0<>>@a00000IzR0Bc'f.00V000>lXc">@8c"0xc"0 B0>lp@0c'00@c'0ct'0nt'0p
t'0't'0t'00'00t'0u'0'0'u'0'0'0'e'0yu'00u'00u'00u'00u'00u'00u'0'v'04v'0cv'0Tv'0I'|'0c'|'0t'|'00'|'00'|'00'|'0'>0G'>0I
00>l]>'0rpe@0]'00']>'00']>'00']>'0r~>'00']>'02'0M'00'0'>'030000d@q8

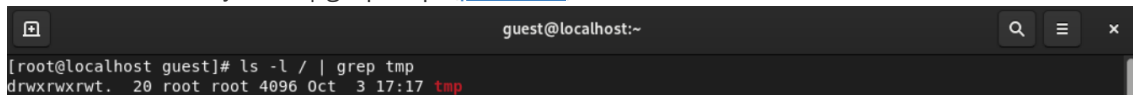
f'000'0'0'if.00V0 00R000x86 64./readfile=readfile.cSHELL=/bin/bashSESSION_MANAGER=local/unix:@tmp/.ICE-uni
x/3215,unix/unix:/tmp/.ICE-unix/3215COLORTERM=truecolorHISTCONTROL=ignoredupsXDG_MENU_PREFIX=gnome-HOSTNAME=localhost
stHISTSIZ=1000SSH_AUTH_SOCK=/run/user/1001/keyring/sshXMODIFIERS=@im=ibusDESKTOP_SESSION=gnomePWD=home/guestXDG_S
SSION_DESKTOP=gnomeLOGNAME=guestXDG_SESSION_TYPE=waylandSYSTEMD_EXEC_PID=3236XAUTHORITY=/root/.authdV2jgBGDM LANG
=en_US.UTF-8HOME=/rootUSERNAME=guestLANG=en_US.UTF-8_COLORS=rs=0:di=0:1:34:ln=0:1:36:mh=0:0:pi=40:40:33:so=0:1:35:do=0:1
:33:bd=40:33:01:cd=40:33:01:or=40:31:01:mi=0:1:37:41:su=37:41:sg=30:43:ca=30:41:tw=30:42:ow=34:42:st=37:44:ex=0:1:32:*
.tar=01:31:*.tgz=01:31:*.arc=01:31:*.arj=01:31:*.taz=01:31:*.lha=01:31:*.lz4=01:31:*.lzh=01:31:*.lma=01:31:*.tlz=0
1:31:*.txz=01:31:*.tzo=01:31:*.t7z=01:31:*.zip=01:31:*.z=01:31:*.dz=01:31:*.gz=01:31:*.lrz=01:31:*.lz=01:31:*.lzo=0
1:31:*.xz=01:31:*.zst=01:31:*.tzst=01:31:*.bz2=01:31:*.bz=01:31:*.tbz=01:31:*.tbz2=01:31:*.tzi=01:31:*.deb=01:31:*.r
pm=01:31:*.jar=01:31:*.war=01:31:*.ear=01:31:*.sar=01:31:*.rar=01:31:*.alz=01:31:*.ace=01:31:*.zoo=01:31:*.cpio=01:
31:*.7z=01:31:*.rz=01:31:*.cab=01:31:*.wim=01:31:*.swm=01:31:*.dwm=01:31:*.esd=01:31:*.jpg=01:35:*.jpeg=01:35:*.mjp
g=01:35:*.mjpeg=01:35:*.gif=01:35:*.bmp=01:35:*.pbm=01:35:*.pgm=01:35:*.ppm=01:35:*.tga=01:35:*.xbm=01:35:*.xpm=01:
35:*.tif=01:35:*.tiff=01:35:*.png=01:35:*.svg=01:35:*.svgz=01:35:*.mng=01:35:*.pcx=01:35:*.mov=01:35:*.mpg=01:35:*.
mpeg=01:35:*.m2v=01:35:*.mkv=01:35:*.webm=01:35:*.webp=01:35:*.ogm=01:35:*.mp4=01:35:*.m4v=01:35:*.mp4v=01:35:*.vo
=01:35:*.qt=01:35:*.nuv=01:35:*.wmv=01:35:*.asf=01:35:*.rm=01:35:*.rmvb=01:35:*.flc=01:35:*.avi=01:35:*.fli=01:35:*
.flv=01:35:*.gl=01:35:*.dl=01:35:*.xcf=01:35:*.xwd=01:35:*.yuv=01:35:*.cgm=01:35:*.emf=01:35:*.ogv=01:35:*.ogx=01:
5:*.aac=01:36:*.au=01:36:*.flac=01:36:*.m4a=01:36:*.mid=01:36:*.midi=01:36:*.mka=01:36:*.mp3=01:36:*.mpe=01:36:*.o
g=01:36:*.ra=01:36:*.wav=01:36:*.oga=01:36:*.opus=01:36:*.spx=01:36:*.xspf=01:36:XDG_CURRENT_DESKTOP=GNOMEVE TERMINAL
ON=6402WAYLAND_DISPLAY=wayland-0GNOME_TERMINAL_SCREEN=/org/gnome/terminal/screen/66771bad a4f0 44d9 b48e c0dd60ffff
leGNOME_SETUP_DISPLAY=:XDG_SESSION_CLASS=userTERM=xterm-256colorLESSOPEN=||/usr/bin/lesspipe.sh %sUSER=guestGNOME
TERMINAL_SERVICE=:1.117DISPLAY=:2SHLV=2QT_IM_MODULE=ibusXDG_RUNTIME_DIR=/run/user/1001which declare-declare -FXDG
DATA_DIRS=/root/.local/share/flatpak/exports/share:/home/guest/.local/share/flatpak/exports/share:/var/lib/flatpak/
exports/share:/usr/local/share:/usr/share/PATH=/root/.local/bin:/root/bin:/home/guest/.local/bin:/home/guest/bin:/
usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/usr/binXDG_SESSION_NAME=gnomeBUS_ADDRESS=unix:path=/run/user/1001/b
```

18. Проверил, может ли программа readfile прочитать файл /etc/shadow - да может. (рис.№13)

[illegible]

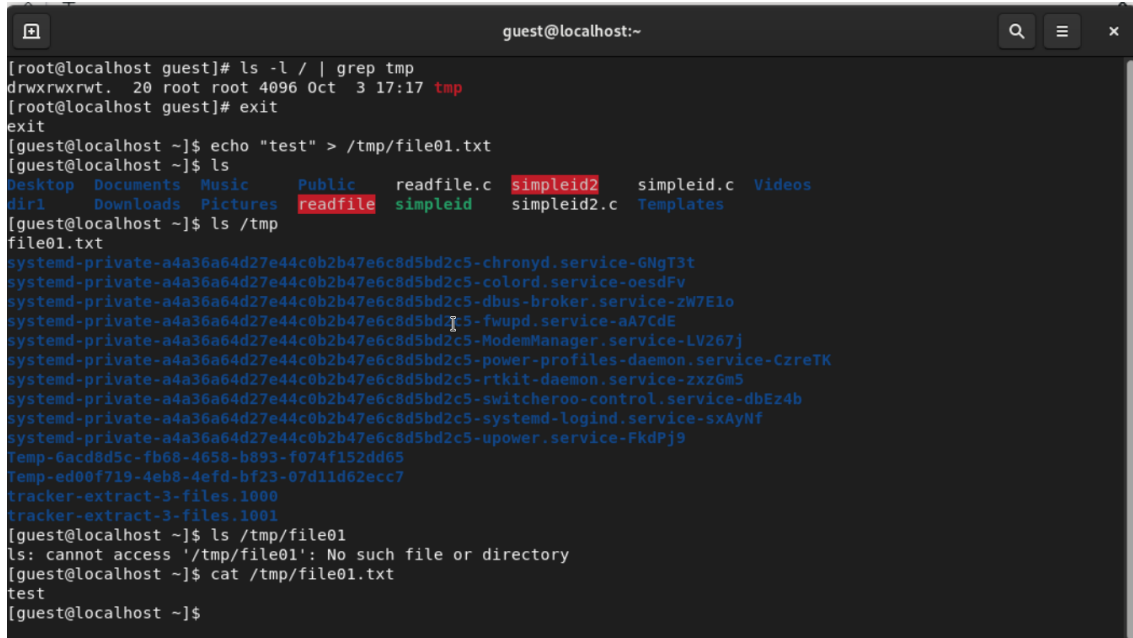
Часть №2

1. Выяснил, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду `ls -l / | grep tmp`. ([рис.№14](#))



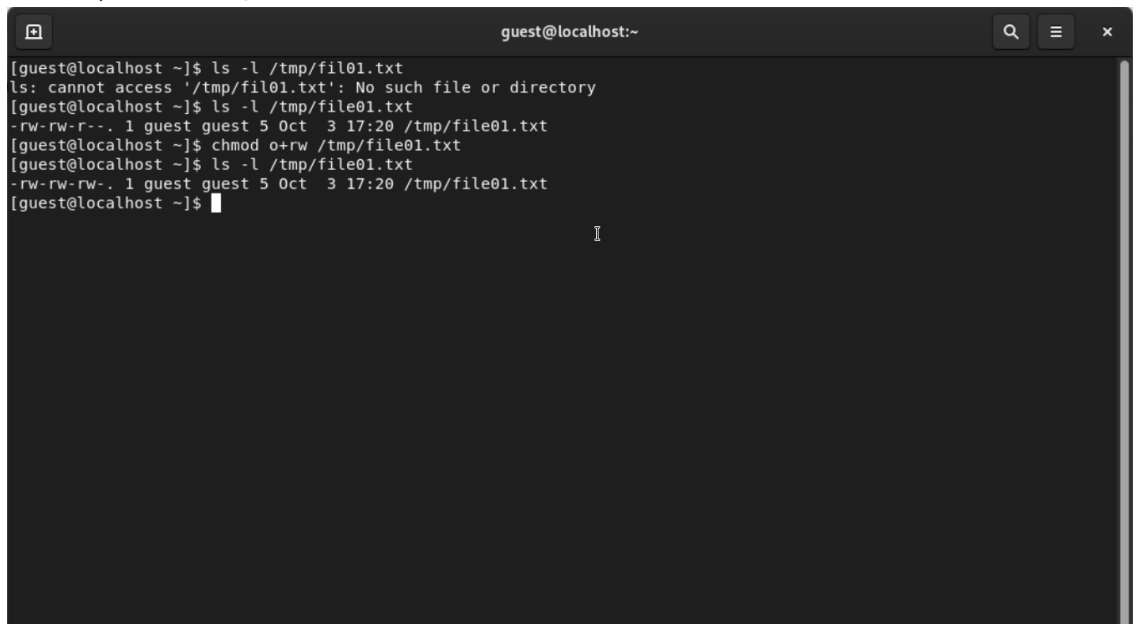
```
guest@localhost:~  
[root@localhost guest]# ls -l / | grep tmp  
drwxrwxrwt. 20 root root 4096 Oct 3 17:17 tmp
```

2. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test: ([рис.№15](#))



```
guest@localhost:~  
[root@localhost guest]# ls -l / | grep tmp  
drwxrwxrwt. 20 root root 4096 Oct 3 17:17 tmp  
[root@localhost guest]# exit  
exit  
[guest@localhost ~]$ echo "test" > /tmp/file01.txt  
[guest@localhost ~]$ ls  
Desktop Documents Music Public readfile.c simpleid2 simpleid.c Videos  
dir1 Downloads Pictures readfile simpleid simpleid2.c Templates  
[guest@localhost ~]$ ls /tmp  
file01.txt  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-chrond.service-GNgT3t  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-color.service-oesdFv  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-dbus-broker.service-zw7E1o  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-fwupd.service-aA7CdE  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-ModemManager.service-LV267j  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-power-profiles-daemon.service-CzreTK  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-rtkit-daemon.service-zxzGm5  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-switcheroo-control.service-dbEz4b  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-systemd-logind.service-sxAyNf  
systemd-private-a4a36a64d27e44c0b2b47e6c8d5bd2c5-upower.service-FkdPJ9  
Temp-6acd8d5c-fb68-4658-b893-f074f152dd65  
Temp-ed00f719-4eb8-4efd-bf23-07d11d62ecc7  
tracker-extract-3-files.1000  
tracker-extract-3-files.1001  
[guest@localhost ~]$ ls /tmp/file01  
ls: cannot access '/tmp/file01': No such file or directory  
[guest@localhost ~]$ cat /tmp/file01.txt  
test  
[guest@localhost ~]$
```

3. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: `ls -l /tmp/file01.txt`
`chmod o+rw /tmp/file01.txt`
`ls -l /tmp/file01.txt` ([рис.№16](#))



```
guest@localhost:~  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
ls: cannot access '/tmp/file01.txt': No such file or directory  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-r--. 1 guest guest 5 Oct 3 17:20 /tmp/file01.txt  
[guest@localhost ~]$ chmod o+rw /tmp/file01.txt  
[guest@localhost ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 Oct 3 17:20 /tmp/file01.txt  
[guest@localhost ~]$
```

4. От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt: `cat /tmp/file01.txt` ([рис.№17](#))

```
guest2@localhost:/home/guest
[guest@localhost ~]$ su guest2
Password:
su: Authentication failure
[guest@localhost ~]$ su guest2
Password:
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$
```

5. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2 командой `echo "test2" >> /tmp/file01.txt`. (рис.№18)

```
guest2@localhost:/home/guest
[guest2@localhost guest]$ echo "test" > /tmp/file01.txt
[guest2@localhost guest]$ echo "test2" >> /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test
test2
[guest2@localhost guest]$
```

6. От пользователя guest2 попробовал удалить файл /tmp/file01.txt командой `rm /tmp/file01.txt`. Удалить файл не удалось. (рис.№19)

```
guest2@localhost:/home/guest
[guest2@localhost guest]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': Operation not permitted
[guest2@localhost guest]$
```

7. Повторил предыдущие шаги без без sticky-бита(без атрибута t) (рис.№20)

```
guest2@localhost:/home/guest
-rw-rw-rw-. 1 guest guest 11 Oct  3 17:36 /tmp/file01.txt
[guest@localhost ~]$ echo "test" > /tmp/file01.txt
[guest@localhost ~]$ cat /tmp/file01.txt
test
[guest@localhost ~]$ su guest2
Password:
[guest2@localhost guest]$ cat /tmp/file01.txt
test
[guest2@localhost guest]$ echo "test2" > /tmp/file01.txt
[guest2@localhost guest]$ cat /tmp/file01.txt
test2
[guest2@localhost guest]$ rm /tmp/file01.txy
rm: cannot remove '/tmp/file01.txy': No such file or directory
[guest2@localhost guest]$ rm /tmp/file01.txt
```

8. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp:

```
su -
```

```
chmod +t /tmp
```

Вывод

Получил практические навыки работы в консоли с расширенными атрибутами файлов.