

# Презентация к лабораторной работе №5

---

## Цель работы

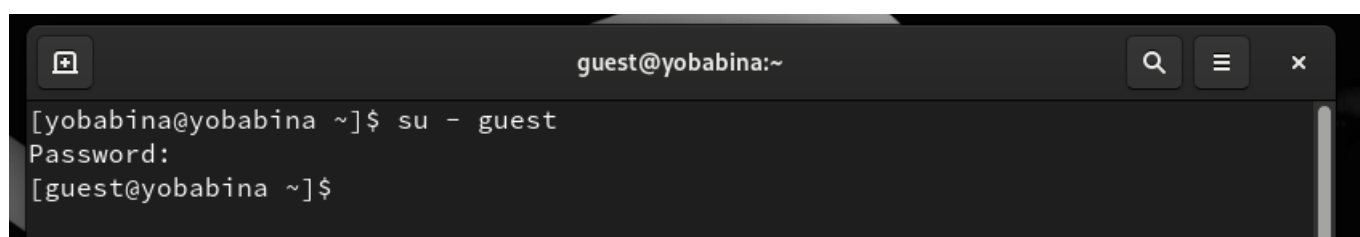
---

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 работы

---

### Вход под пользователем guest



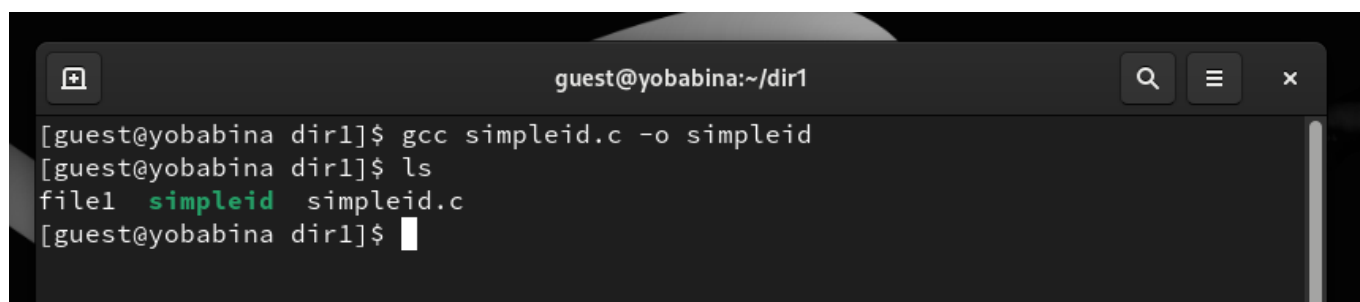
```
guest@yobabina:~  
[yobabina@yobabina ~]$ su - guest  
Password:  
[guest@yobabina ~]$
```

### Программа simpleid.c



```
GNU nano 5.6.1 simpleid.c  
#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;  
}
```

### Компиляция, выполнение и команда id



```
guest@yobabina:~/dir1  
[guest@yobabina dir1]$ gcc simpleid.c -o simpleid  
[guest@yobabina dir1]$ ls  
file1  simpleid  simpleid.c  
[guest@yobabina dir1]$
```

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./simpleid
uid=1001, gid=1001
[guest@yobabina dir1]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yobabina dir1]$
```

## Установка расширенных атрибутов файла и их проверка

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./simpleid
uid=1001, gid=1001
[guest@yobabina dir1]$
```

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./simpleid
uid=1001, gid=1001
[guest@yobabina dir1]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yobabina dir1]$
```

## Программа simpleid2.c

```
GNU nano 5.6.1 simpleid2.c Modified
#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;
}
```

## Процесс компиляции и запуск программы

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ gcc simpleid2.c -o simpleid2
[guest@yobabina dir1]$ ls
file1  simpleid  simpleid2  simpleid2.c  simpleid.c
[guest@yobabina dir1]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@yobabina dir1]$
```

## Изменение прав доступа к файлу и запуск программы

```
yobabina@yobabina:~
[yobabina@yobabina ~]$ sudo chown root:guest /home/guest/dir1/simpleid2
[sudo] password for yobabina:
[yobabina@yobabina ~]$ sudo chmod u+s /home/guest/dir1/simpleid2
[yobabina@yobabina ~]$ sudo ls -l /home/guest/dir1/simpleid2
-rwsr-xr-x. 1 root guest 17720 Oct  1 23:00 /home/guest/dir1/simpleid2
[yobabina@yobabina ~]$
```

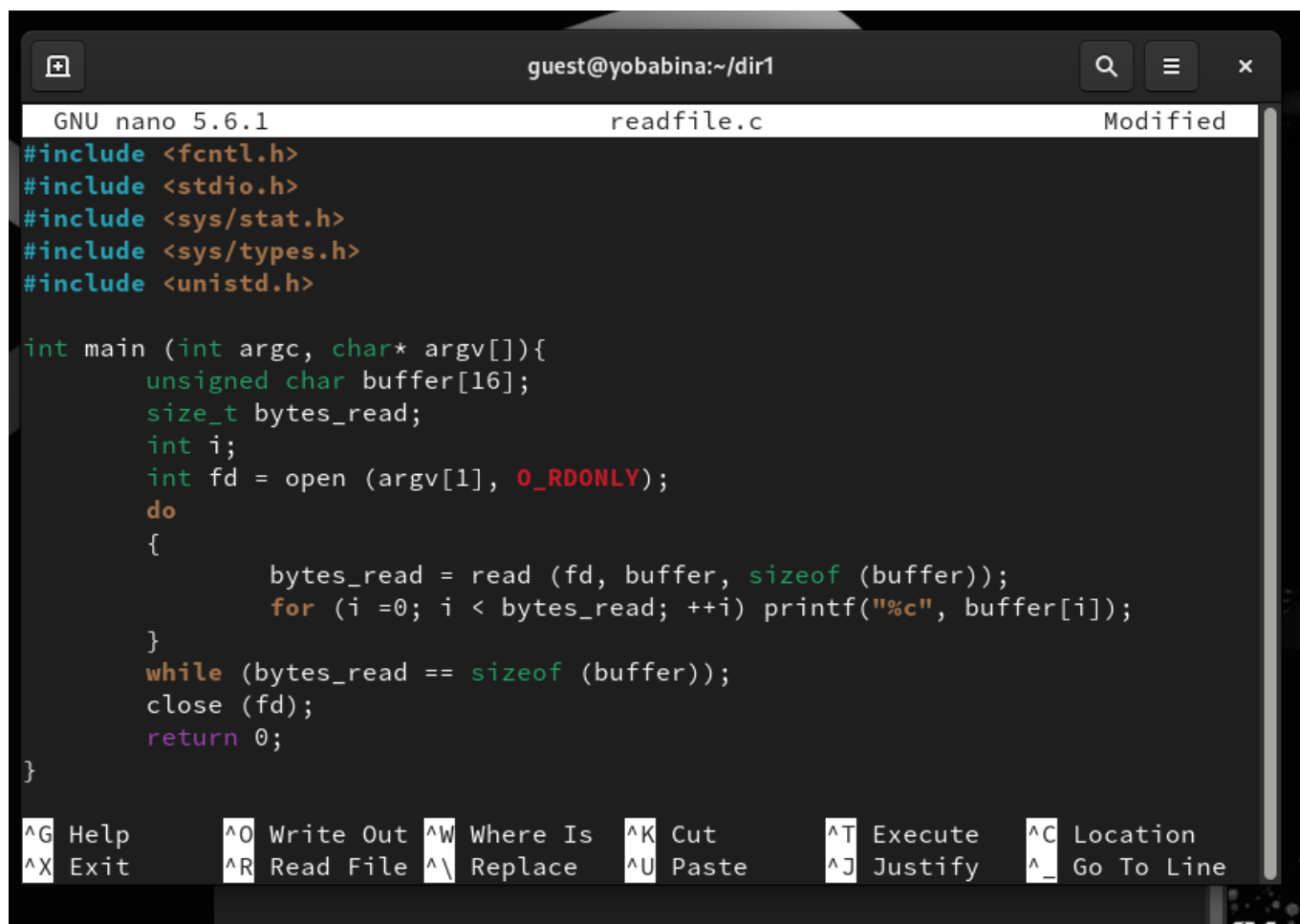
```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@yobabina dir1]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yobabina dir1]$
```

## Добавление SetGID-бита

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@yobabina dir1]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@yobabina dir1]$

yobabina@yobabina:~
[yobabina@yobabina ~]$ sudo chown root:guest /home/guest/dir1/simpleid2
[yobabina@yobabina ~]$ sudo chmod g+s /home/guest/dir1/simpleid2
[yobabina@yobabina ~]$
```

## Программа readfile.c



```
guest@yobabina:~/dir1
GNU nano 5.6.1 readfile.c Modified
#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;
}
```

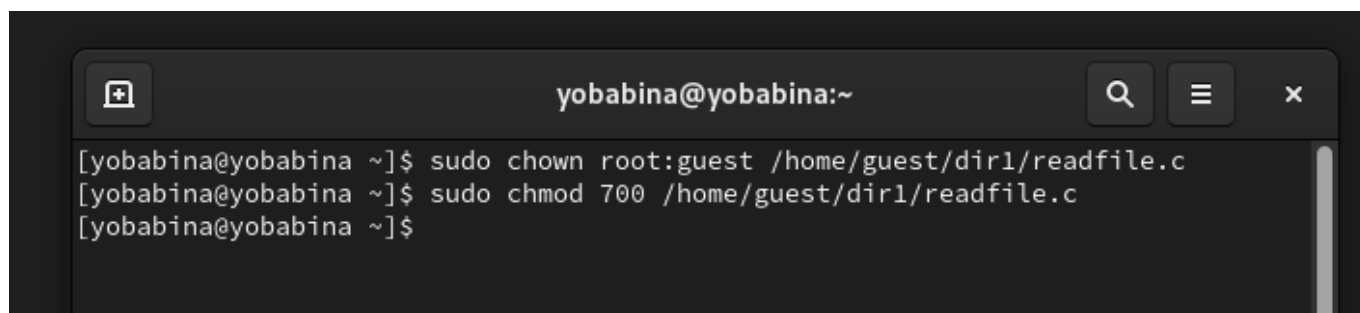
Terminal shortcuts: ^G Help, ^X Exit, ^O Write Out, ^R Read File, ^W Where Is, ^\ Replace, ^K Cut, ^U Paste, ^T Execute, ^J Justify, ^C Location, ^\_ Go To Line

## Компиляция



```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ gcc readfile.c -o readfile
[guest@yobabina dir1]$ ls
file1 readfile readfile.c simpleid simpleid2 simpleid2.c simpleid.c
[guest@yobabina dir1]$
```

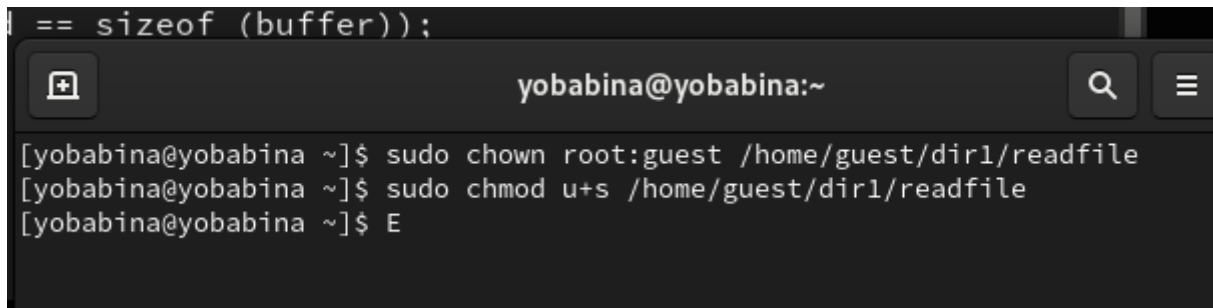
## Изменение прав доступа к файлу



```
yobabina@yobabina:~
[yobabina@yobabina ~]$ sudo chown root:guest /home/guest/dir1/readfile.c
[yobabina@yobabina ~]$ sudo chmod 700 /home/guest/dir1/readfile.c
[yobabina@yobabina ~]$
```

## Добавление SetUID-бит

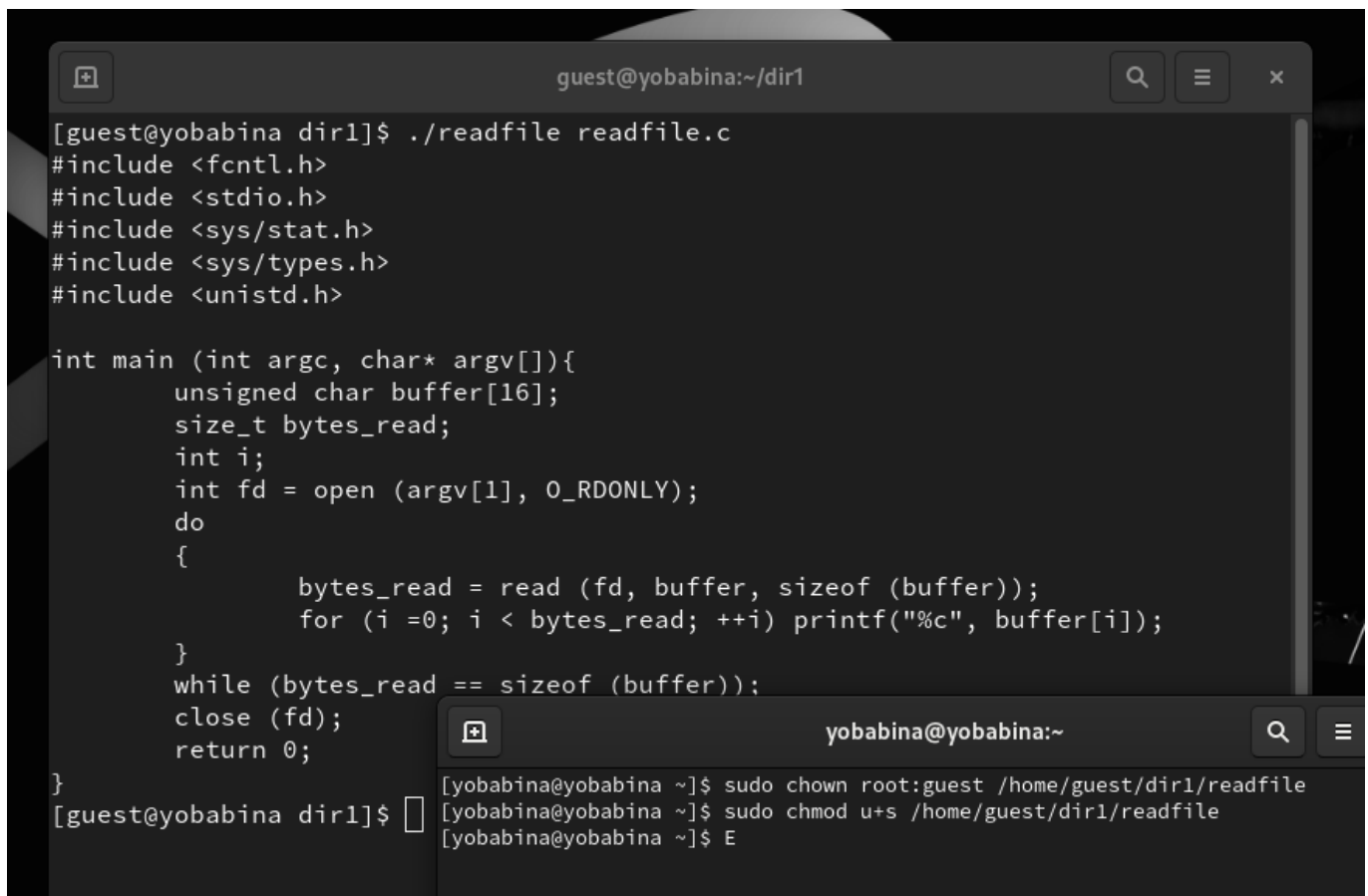
```
== sizeof (buffer));
```



A terminal window titled 'yobabina@yobabina:~' with search and menu icons. It shows the execution of two sudo commands to set permissions on a file named 'readfile' in the directory '/home/guest/dir1'. The first command sets ownership to root:guest, and the second sets permissions to u+s. The prompt returns to the user after each command.

```
yobabina@yobabina:~$ sudo chown root:guest /home/guest/dir1/readfile
yobabina@yobabina:~$ sudo chmod u+s /home/guest/dir1/readfile
yobabina@yobabina:~$ E
```

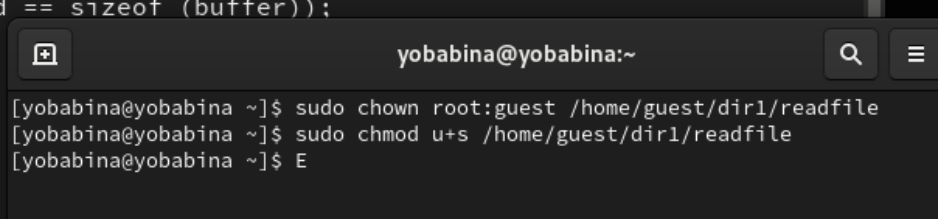
## Чтение файлов



A terminal window titled 'guest@yobabina:~/dir1' with search, menu, and close icons. It shows the execution of a C program named 'readfile.c'. The code includes headers for fcntl, stdio, sys/stat, sys/types, and unistd. The main function opens a file in read-only mode, reads it in 16-byte chunks, and prints each byte. The prompt returns to the user after the program execution.

```
[guest@yobabina dir1]$ ./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;
}
[guest@yobabina dir1]$
```



A terminal window titled 'yobabina@yobabina:~' with search and menu icons. It shows the execution of two sudo commands to set permissions on a file named 'readfile' in the directory '/home/guest/dir1'. The first command sets ownership to root:guest, and the second sets permissions to u+s. The prompt returns to the user after each command.

```
yobabina@yobabina:~$ sudo chown root:guest /home/guest/dir1/readfile
yobabina@yobabina:~$ sudo chmod u+s /home/guest/dir1/readfile
yobabina@yobabina:~$ E
```

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ./readfile /etc/shadow
root:$6$8m6DK1DRkS7KeMCe$LQGA9Xaywq0LZpRepsNmK/qd463oGhGv.IX2/pquukeHVLDJEMkcP2
OTDvd5DFdwn91jbrMJyzzKXPn5.N4k0::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:::
systemd-coredump:!!:19975:::::::
dbus:!!:19975:::::::
polkitd:!!:19975:::::::
avahi:!!:19975:::::::
rtkit:!!:19975:::::::
pipewire:!!:19975:::::::
sssd:!!:19975:::::::
libstoragemgmt:!*:19975:::::::
tss:!!:19975:::::::
```

## Sticky-бит

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 Oct  1 23:14 tmp
[guest@yobabina dir1]$
```

## Файл file01.txt

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ echo "test" > /tmp/file01.txt
[guest@yobabina dir1]$ ls /tmp
file01.txt
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-chrond.service-LL14MI
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-colord.service-NVwCcV
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-dbus-broker.service-AhQ3Su
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-fwupd.service-07BCRi
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-geoclue.service-mRmv2o
```

## Предоставление прав доступа

```
guest@yobabina:~/dir1
[guest@yobabina dir1]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 Oct  1 23:22 /tmp/file01.txt
[guest@yobabina dir1]$ chmod o+rw /tmp/file01.txt
[guest@yobabina dir1]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 Oct  1 23:22 /tmp/file01.txt
[guest@yobabina dir1]$
```

## Другие операции с файлом

```
guest2@yobabina:~
[yobabina@yobabina ~]$ su - guest2
Password:
[guest2@yobabina ~]$ cat /tmp/file01.txt
test
[guest2@yobabina ~]$
```

```
guest2@yobabina:~
[guest2@yobabina ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[guest2@yobabina ~]$ cat /tmp/file01.txt
test
[guest2@yobabina ~]$
```

```
guest2@yobabina:~
[guest2@yobabina ~]$ rm /tmp/file01.txt
rm: cannot remove '/tmp/file01.txt': No such file or directory
[guest2@yobabina ~]$ ls /tmp
file01.txt
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-chronyd.service-LL14MI
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-colord.service-NVwCcV
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-dbus-broker.service-AhQ3Su
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-fwupd.service-07BCRi
```

## Снятие Sticky-бита

```
yobabina@yobabina:~
[yobabina@yobabina ~]$ su -
Password:
[root@yobabina ~]# chmod -t /tmp
[root@yobabina ~]# exit
logout
[yobabina@yobabina ~]$
```

## Повторение команд

```
guest2@yobabina:~  
[guest2@yobabina ~]$ ls -l / | grep tmp  
drwxrwxrwx. 20 root root 4096 Oct  1 23:31 tmp  
[guest2@yobabina ~]$ cat /tmp/file01.txt  
test  
[guest2@yobabina ~]$ echo "test2" > /tmp/file01.txt  
-bash: /tmp/file01.txt: Permission denied  
[guest2@yobabina ~]$ cat /tmp/file01.txt  
test  
[guest2@yobabina ~]$ echo "test3" > /tmp/file01.txt  
-bash: /tmp/file01.txt: Permission denied  
[guest2@yobabina ~]$ cat /tmp/file01.txt  
test  
[guest2@yobabina ~]$ rm /tmp/file01.txt  
rm: cannot remove '/tmp/file01.txt': No such file or directory  
[guest2@yobabina ~]$ ls /tmp  
file01.txt  
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-chrond.service-LL14MI  
systemd-private-0d9fb928478e40e1ae70fde386be2ea0-colord.service-MVwCcV
```

## Возвращение Sticky-бита

```
yobabina@yobabina:~  
[yobabina@yobabina ~]$ su -  
Password:  
[root@yobabina ~]# chmod +t /tmp  
[root@yobabina ~]# exit  
logout  
[yobabina@yobabina ~]$
```

## Вывод

В рамках выполнения данной лабораторной работы я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов.

Получила практические навыки работы в консоли с дополнительными атрибутами.

Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.