

# Основы информационной безопасности

---

Колчева Юлия Вячеславовна

2 Октября 2023

РУДН, Москва, Россия

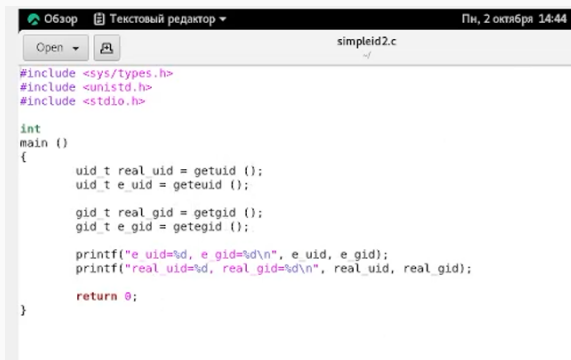
## **Лабораторная работа 5**

---

```
[yvkolcheva@yvkolcheva ~]$ whereis gcc
gcc: /usr/bin/gcc /usr/lib/gcc /usr/libexec/gcc /usr/share/man/man1/gcc.1.gz /usr/share/info/gcc.info.gz
[yvkolcheva@yvkolcheva ~]$ whereis g++
g++: /usr/bin/g++ /usr/share/man/man1/g++.1.gz
[yvkolcheva@yvkolcheva ~]$
```

Рис. 1: Просмотр

# Усложненная программа



```
#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 ();

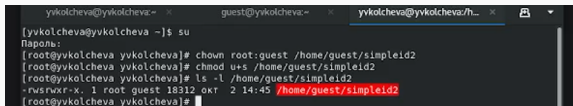
    printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);
    printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);

    return 0;
}
```

Рис. 2: Написание программы

```
[guest@yvkolcheva ~]$ gcc simpleid2.c -o simpleid2
[guest@yvkolcheva ~]$ ./simpleid2
e uid=1001, e gid=1001
real uid=1001, real gid=1001
[guest@yvkolcheva ~]$
```

Рис. 3: Вывод



A terminal window with three tabs: 'yvkolcheva@yvkolcheva:~', 'guest@yvkolcheva:~', and 'yvkolcheva@yvkolcheva:/h...'. The active tab shows the following commands and output:

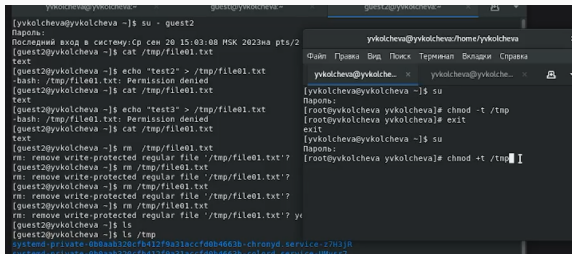
```
[yvkolcheva@yvkolcheva ~]$ su
Пароль:
[root@yvkolcheva yvkolcheva]# chown root:guest /home/guest/simpleid2
[root@yvkolcheva yvkolcheva]# chmod u+s /home/guest/simpleid2
[root@yvkolcheva yvkolcheva]# ls -l /home/guest/simpleid2
-rwsrwxr-x. 1 root guest 18312 окт  2 14:45 /home/guest/simpleid2
[root@yvkolcheva yvkolcheva]#
```

Рис. 4: Работа в терминале

```
[guest@yvkolcheva ~]$ ./simpleid2
e uid=0, e gid=1001
real uid=1001, real gid=1001
[guest@yvkolcheva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfi
ned_t:s0-s0:c0.c1023
[guest@yvkolcheva ~]$
```

Рис. 5: НОВЫЙ ВЫВОД

# Исследование Sticky-бита

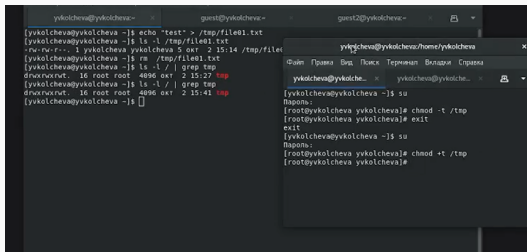


```
[yvkolcheva@yvkolcheva ~]$ su - quest2
Последний вход в систему: Ср сен 20 15:03:08 MSK 2023 на pts/2
Пароль:
[quest2@yvkolcheva ~]$ cat /tmp/file01.txt
text
[quest2@yvkolcheva ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[quest2@yvkolcheva ~]$ cat /tmp/file01.txt
text
[quest2@yvkolcheva ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Permission denied
[quest2@yvkolcheva ~]$ cat /tmp/file01.txt
text
[quest2@yvkolcheva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[quest2@yvkolcheva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[quest2@yvkolcheva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[quest2@yvkolcheva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'?
[quest2@yvkolcheva ~]$ ls
[quest2@yvkolcheva ~]$ ls /tmp
systemd-private-0b0a8b320cfb41279a31accfd0b4663b-chronyd.service-27H3JR
systemd-private-0b0a8b320cfb41279a31accfd0b4663b-colord.service-10Hys7
```

Рис. 6: Проверка доступа



# Исследование Sticky-бита



```
yvkolcheva@yvkolcheva:~$ echo "test" > /tmp/file01.txt
yvkolcheva@yvkolcheva:~$ ls -l /tmp/file01.txt
-rw-rw-r-- 1 yvkolcheva yvkolcheva 5 окт  2 15:14 /tmp/file01.txt
yvkolcheva@yvkolcheva:~$ rm /tmp/file01.txt
yvkolcheva@yvkolcheva:~$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 окт  2 15:27 tmp
yvkolcheva@yvkolcheva:~$ ls -l / | grep tmp
drwxrwxrwt. 16 root root 4096 окт  2 15:41 tmp
yvkolcheva@yvkolcheva:~$
```

The screenshot shows a terminal window with three tabs. The active tab is 'yvkolcheva@yvkolcheva:~'. The terminal displays the following sequence of commands and outputs:

- `echo "test" > /tmp/file01.txt`
- `ls -l /tmp/file01.txt` outputs: `-rw-rw-r-- 1 yvkolcheva yvkolcheva 5 окт 2 15:14 /tmp/file01.txt`
- `rm /tmp/file01.txt`
- `ls -l / | grep tmp` outputs: `drwxrwxrwt. 16 root root 4096 окт 2 15:27 tmp`
- `ls -l / | grep tmp` outputs: `drwxrwxrwt. 16 root root 4096 окт 2 15:41 tmp`

A second terminal window is open in the foreground, titled 'yvkolcheva@yvkolcheva/home/yvkolcheva'. It shows the following sequence of commands and outputs:

- `su` outputs: `Пароль:`
- `chmod -t /tmp`
- `exit` outputs: `exit`
- `su` outputs: `Пароль:`
- `chmod +t /tmp`
- `exit`

Рис. 7: Результат

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

**Спасибо за внимание!**