

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

ФИО: Жукова Виктория Юрьевна

Группа: НКНбд-01-19

Студ. билет: 1032196000

Цель выполнения лабораторной 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.

Задачи выполнения работы

1. Поработать с компиляцией си программ.
2. Поэкспериментировать со Sticky-битом.

Выполнение

```
[vyzhukova@user ~]$ su - guest
```

Пароль:

Последний вход в систему: Пт сен 23 21:13:50 MSK 2022 на pts/0

Последняя неудачная попытка входа в систему: Пт окт 7 21:40:26 М

Со времени последнего входа была 1 неудачная попытка.

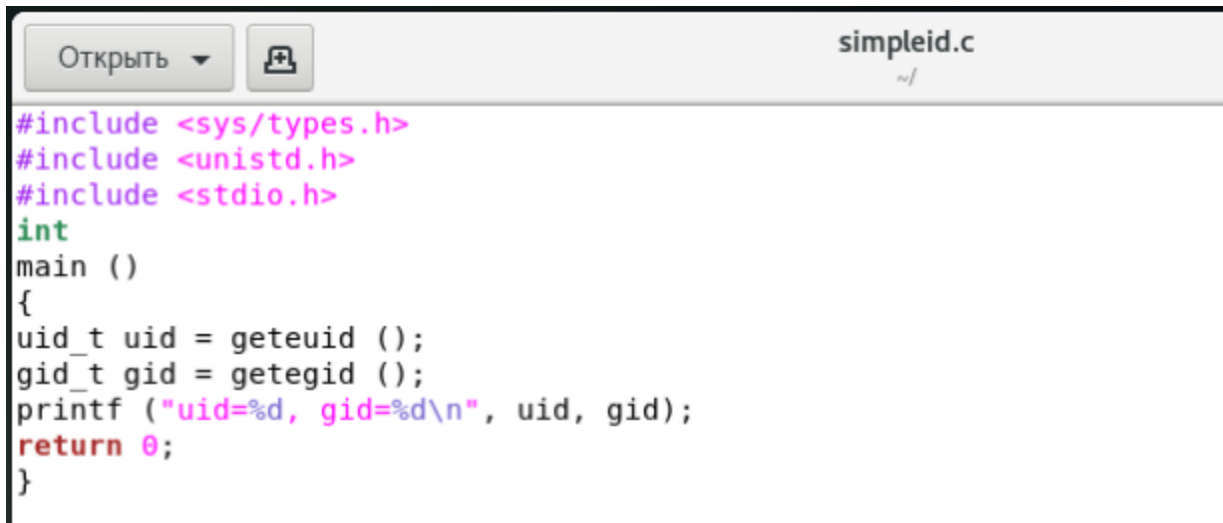
```
[guest@user ~]$ ls
```

```
dir1  Документы  Изображения  Общедоступные  Шаблоны
Видео  Загрузки  Музыка  Рабочий стол
```

```
[guest@user ~]$ touch simpleid.c
```

```
[guest@user ~]$ ls
```

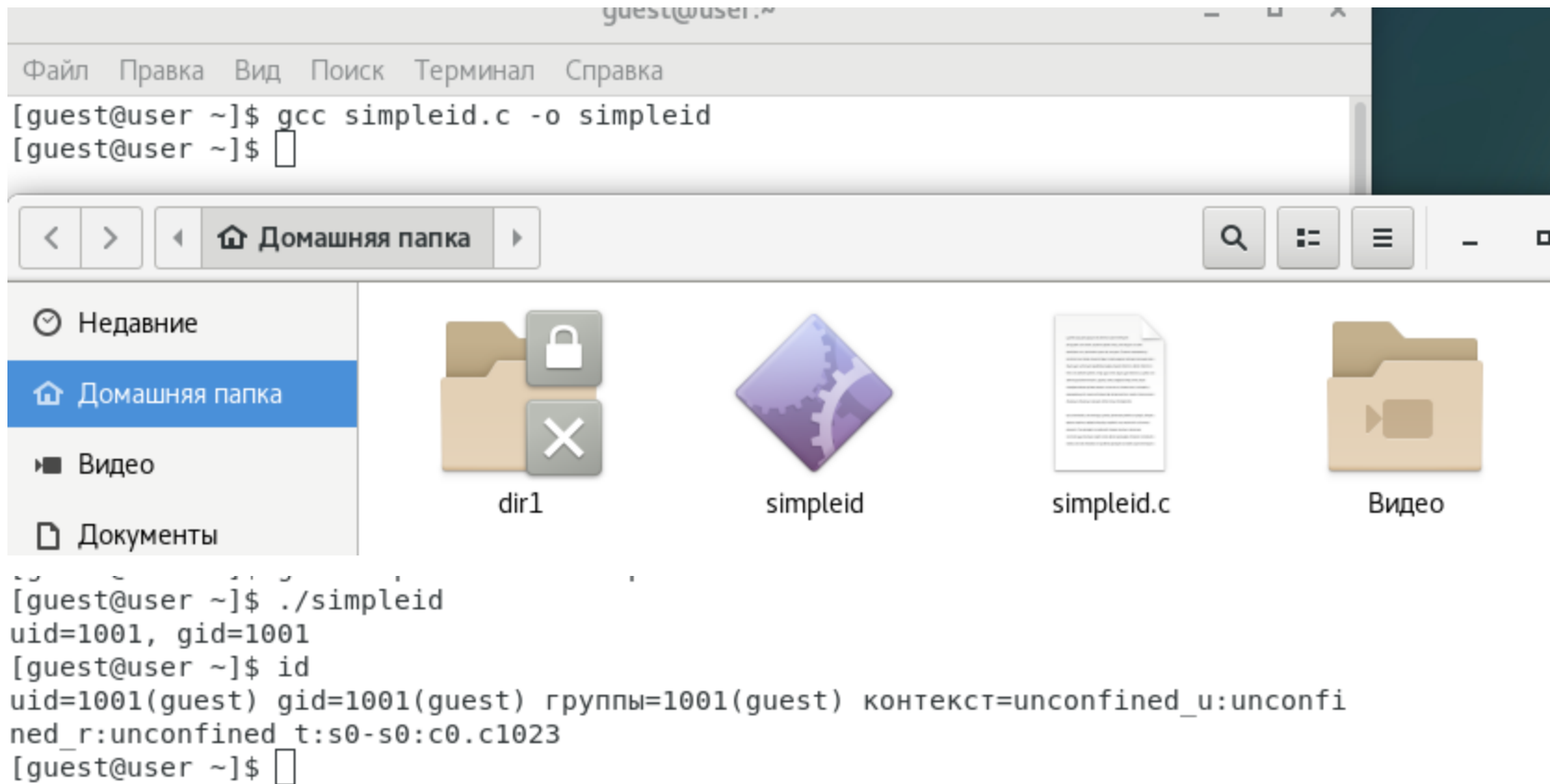
```
dir1      Видео      Загрузки      Музыка      Рабочий стол
simpleid.c Документы  Изображения  Общедоступные  Шаблоны
```



```
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;
}
```

Выполнение

```
guest@user.~  
Файл Правка Вид Поиск Терминал Справка  
[guest@user ~]$ gcc simpleid.c -o simpleid  
[guest@user ~]$  
[guest@user ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@user ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined t:s0-s0:c0.c1023  
[guest@user ~]$
```



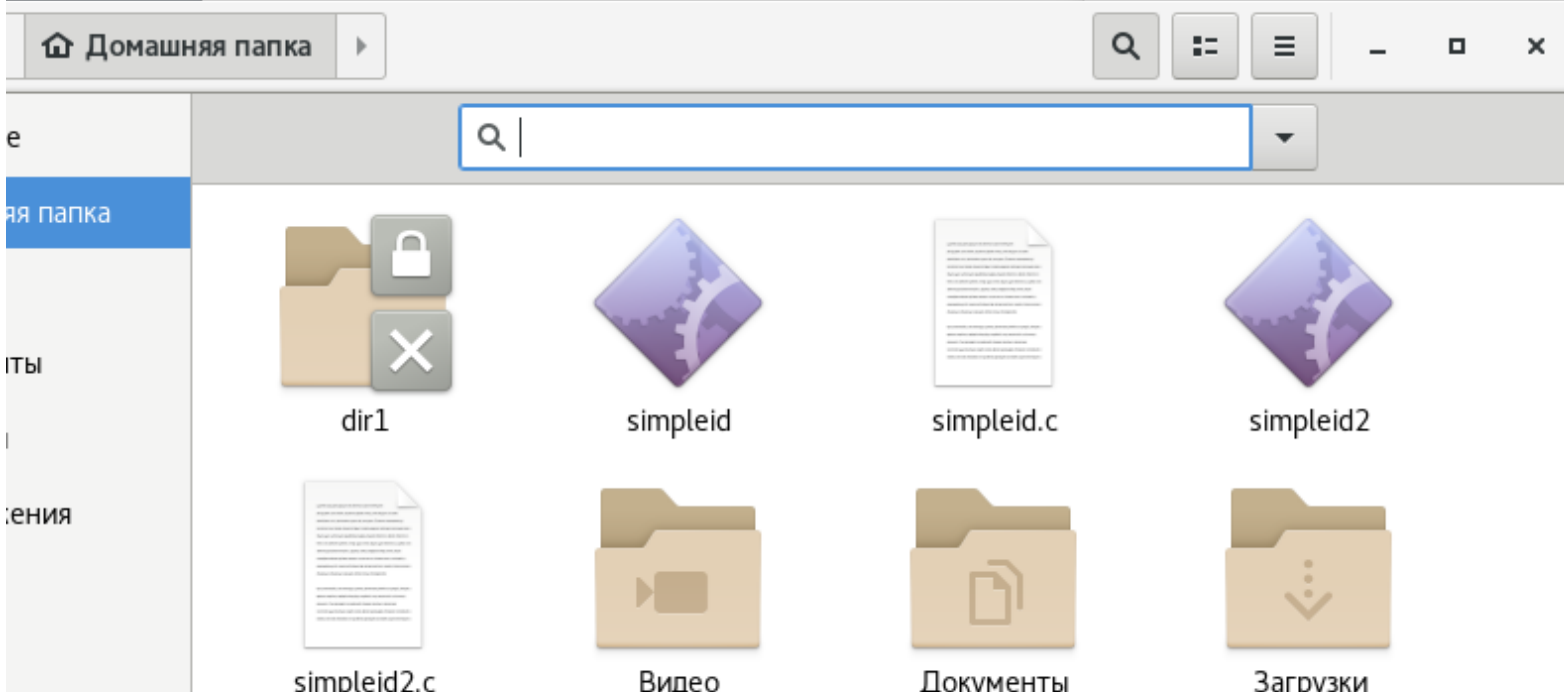
```
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@user ~]$ gcc simpleid2.c -o simpleid2
simpleid2.c: В функции «main»:
simpleid2.c:13:1: ошибка: expected expression before
^, → real_gid);

simpleid2.c:13:1: ошибка: в программе обнаружен не
simpleid2.c:13:1: ошибка: в программе обнаружен не
simpleid2.c:13:1: ошибка: в программе обнаружен не
[guest@user ~]$ gcc simpleid2.c -o simpleid2
[guest@user ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@user ~]$
```

simpleid2.c

Открыть

```
#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;
}
```



Выполнение

```
[vyzhukova@user ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для vyzhukova:
[vyzhukova@user ~]$ sudo chmod u+s /home/guest/simpleid2

[vyzhukova@user ~]$ sudo ls -l /home/guest/simpleid2
-rwsrwxr-x. 1 root guest 8576 окт  7 21:52 /home/guest/simpleid2
[vyzhukova@user ~]$

[root@user home]# cd guest
[root@user guest]# ./simpleid2
e_uid=0, e_gid=0
real_uid=0, real_gid=0
```

Выполнение

```
[root@user guest]# chmod g+s simpleid2
[root@user guest]# ls -l simpleid2
-rwsrwsr-x. 1 root guest 8576 окт  7 21:52 simpleid2
[root@user guest]# ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=0
[root@user guest]# █
```

{ #fig:008 width=70% }


```
vyzhukova@user:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
boot  etc  lib  media  opt  root  sbin  sys  usr  
[root@user /]# cd home  
[root@user home]# ls  
guest  guest2  vyzhukova  
[root@user home]# cd guest  
[root@user guest]# ./simpleid2  
e_uid=0, e_gid=0  
real_uid=0, real_gid=0  
[root@user guest]# chmod g+s simpleid2  
[root@user guest]# ls -l simpleid2  
-rwsrwsr-x. 1 root guest 8576 окт  7 21:52 simpleid2  
[root@user guest]# ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=0, real_gid=0  
[root@user guest]# su - guest  
Последний вход в систему:Пт окт  7 21:46:15 MSK 2022на :1  
[guest@user ~]$ su - vyzhukova  
Пароль:  
Последний вход в систему:Пт окт  7 22:15:28 MSK 2022на :0  
[vyzhukova@user ~]$ pwd  
/home/vyzhukova  
[vyzhukova@user ~]$ touch  readfile.c  
[vyzhukova@user ~]$ gcc readfile.c -o readfile  
[vyzhukova@user ~]$
```

```
Открыть  +  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;  
}
```



Выполнение

```
[root@user ~]# chown root:vyzhukova /home/vyzhukova/readfile.c
[root@user ~]# chmod 700 /home/vyzhukova/readfile.c
[root@user ~]# su - vyzhukova
Последний вход в систему:Пт окт  7 22:41:23 MSK 2022на pts/0
[vyzhukova@user ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[vyzhukova@user ~]$ █
```

По команде «`chmod --help`» можно получить дополнительную информацию.

```
[root@user ~]# chmod u+s /home/vyzhukova/readfile
```

```

@K0Y0[0.0] @000000e000gro000Z^0P[0.0] ^0[0.0] @000Ia[0.0]0000000&0000&0000&00'000'0003'000C'000w'000e'000o'000'.000;.000I.000w.0000.0000.0000.0

```

```
00000000/0000j000^0B000000.猿40x86 64./readfilereadfile.cXDG_VTNR=1XDG_SESSION_ID=1HOSTNAME=user.localdomainSHELL=/bin/bashTERM=xterm
```

```
[root@user vyzhukova]# ./readfile /etc/shadow
```

[illegible]

```
09:06x86_64./readfile/etc/shadowXDG_VNOR=1XDG_SESSION_ID=1HOSTNAME=user.localdomainSHELL=/bin/bashTERM=xterm-256colorHISTSIZE=1000USER=ro
```

```
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=05;48;5;232;38;5;15:su=48;5;196;38;5;15:sg=48;5;11;38;5;16:ca=
ex=38;5;34:*.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=3
;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:*.bz2=38;5;9:*.bz=38;5;9:*.tbz=38;5;9:*.tbz2=38;5;9:*.tz=
ar=38;5;9:*.rar=38;5;9:*.alz=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:*.jpg=38;5;13:*.jpeg=38
:*.tga=38;5;13:*.xbm=38;5;13:*.xpm=38;5;13:*.tif=38;5;13:*.tiff=38;5;13:*.png=38;5;13:*.svg=38;5;13:*.svgz=38;5;13:*.mng=38;5;13:*.pcx=3
13:*.webm=38;5;13:*.ogm=38;5;13:*.mp4=38;5;13:*.m4v=38;5;13:*.mp4v=38;5;13:*.vob=38;5;13:*.qt=38;5;13:*.nuv=38;5;13:*.wmv=38;5;13:*.asf=
13:*.flv=38;5;13:*.gl=38;5;13:*.dl=38;5;13:*.xcf=38;5;13:*.xwd=38;5;13:*.yuv=38;5;13:*.cgm=38;5;13:*.emf=38;5;13:*.axv=38;5;13:*.anx=38;
```

```
[root@user vyzhukova]#
```

Выполнение

Файл Правка Вид Поиск Терминал Справка

```
[vyzhukova@user ~]$ ls -l / | grep tmp
drwxrwxrwt. 18 root root 4096 окт  7 23:01 tmp
[vyzhukova@user ~]$ su - guest
Пароль:
Последний вход в систему:Пт окт  7 22:41:00 MSK 2022на pts/0
[guest@user ~]$ echo "test" > /tmp/file01.txt
[guest@user ~]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 guest guest 5 окт  7 23:05 /tmp/file01.txt
[guest@user ~]$ chmod o+rw /tmp/file01.txt
[guest@user ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  7 23:05 /tmp/file01.txt
[guest@user ~]$ su - guest2
Пароль:
Последний вход в систему:Пт сен 23 21:14:16 MSK 2022на pts/1
[guest2@user ~]$ cat /tmp/file01.txt
test
[guest2@user ~]$ echo "test2" > /tmp/file01.txt
[guest2@user ~]$ cat /tmp/file01.txt
test2
[guest2@user ~]$ echo "test3" > /tmp/file01.txt
[guest2@user ~]$ cat /tmp/file01.txt
test3
[guest2@user ~]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Нет такого файла или каталога
```

Выполнение

```
cat /etc/passwd | grep pts/0
[guest2@user ~]$ su - vyzhukova
Пароль:
Последний вход в систему:Пт окт  7 22:47:38 MSK 2022на pts/0
[vyzhukova@user ~]$ sudo -i
[sudo] пароль для vyzhukova:
[root@user ~]# chmod -t /tmp
[root@user ~]# su - guest2
Последний вход в систему:Пт окт  7 23:06:00 MSK 2022на pts/0
[guest2@user ~]$ ls -l / | grep tmp
drwxrwxrwx. 18 root root 4096 окт  7 23:11 tmp
[guest2@user ~]$ echo "test" > /tmp/file01.txt
[guest2@user ~]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 guest guest 5 окт  7 23:13 /tmp/file01.txt
[guest2@user ~]$ chmod o+rw /tmp/file01.txt
chmod: изменение прав доступа для «/tmp/file01.txt»: Операция не позволена
[guest2@user ~]$ cat /tmp/file01.txt
test
[guest2@user ~]$ echo "test2" > /tmp/file01.txt
[guest2@user ~]$ cat /tmp/file01.txt
test2
[guest2@user ~]$ echo "test3" > /tmp/file01.txt
[guest2@user ~]$ cat /tmp/file01.txt
test3
[guest2@user ~]$ rm /tmp/file01.txt
rm: невозможно удалить «/tmp/file01.txt»: Нет такого файла или каталога
[guest2@user ~]$ su - vyzhukova
Пароль:
Последний вход в систему:Пт окт  7 23:11:18 MSK 2022на pts/0
[vyzhukova@user ~]$ sudo -i
[root@user ~]# chmod +t /tmp
[root@user ~]#
```

Вывод

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.