

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Гебриал Ибрам¹

2021 Moscow, Russia

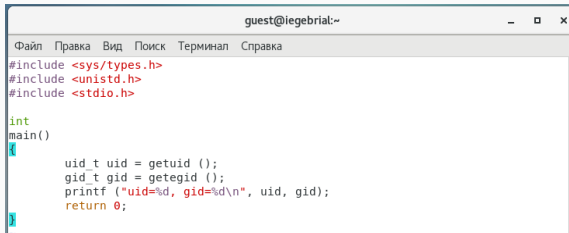
¹RUDN University, Moscow, Russian Federation

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.

Результаты

Создал программу simpleid.c. (рис. 1)

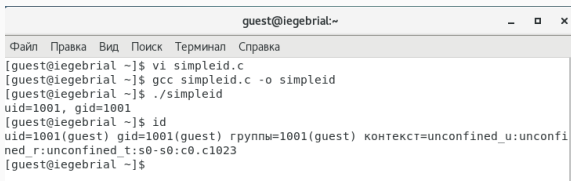
A screenshot of a code editor window titled 'guest@iegebriat:~'. The window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The code is written in C and includes headers for `<sys/types.h>`, `<unistd.h>`, and `<stdio.h>`. It defines a `main()` function that uses `getuid()` and `getegid()` to retrieve the current user and group IDs, and then prints them using `printf`.

```
#include <sys/types.h>
#include <unistd.h>
#include <stdio.h>

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

Figure 1: Создание программы simpleid.c

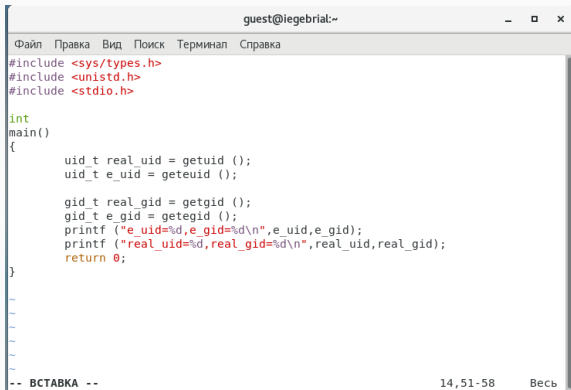
Выполнил программу simpleid и выполнил системную программу id.
(рис. 2)



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

Figure 2: Выполнение программы

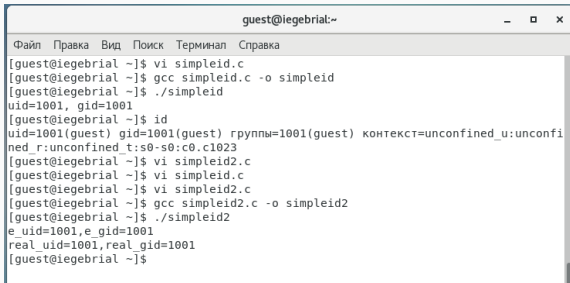
Усложнил программу, добавив вывод действительных идентификаторов. (рис. 3)



```
guest@iegebriat:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
#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;  
}  
~  
~  
~  
~  
-- ВСТАВКА -- 14, 51-58  Весь
```

Figure 3: Создание программы simpleid2.c

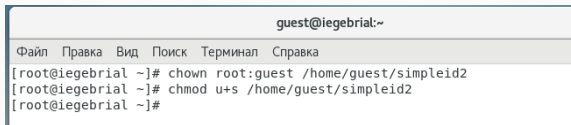
Скомпилировал и запустил simpleid2.c. (рис. 4)



```
guest@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@iegebrial ~]$ vi simpleid.c  
[guest@iegebrial ~]$ gcc simpleid.c -o simpleid  
[guest@iegebrial ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@iegebrial ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@iegebrial ~]$ vi simpleid2.c  
[guest@iegebrial ~]$ vi simpleid.c  
[guest@iegebrial ~]$ vi simpleid2.c  
[guest@iegebrial ~]$ gcc simpleid2.c -o simpleid2  
[guest@iegebrial ~]$ ./simpleid2  
e_uid=1001,e_gid=1001  
real_uid=1001,real_gid=1001  
[guest@iegebrial ~]$
```

Figure 4: Компиляция и выполнение программы

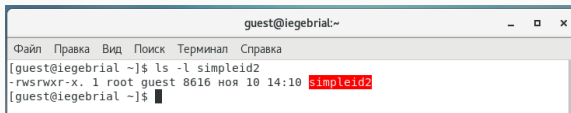
От имени суперпользователя выполнил команды. (рис. 5)

A terminal window titled 'guest@iegebrial:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows three commands executed as root: 'chown root:guest /home/guest/simpleid2', 'chmod u+s /home/guest/simpleid2', and the prompt '[root@iegebrial ~]#'.

```
guest@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[root@iegebrial ~]# chown root:guest /home/guest/simpleid2  
[root@iegebrial ~]# chmod u+s /home/guest/simpleid2  
[root@iegebrial ~]#
```

Figure 5: Выполнение команды

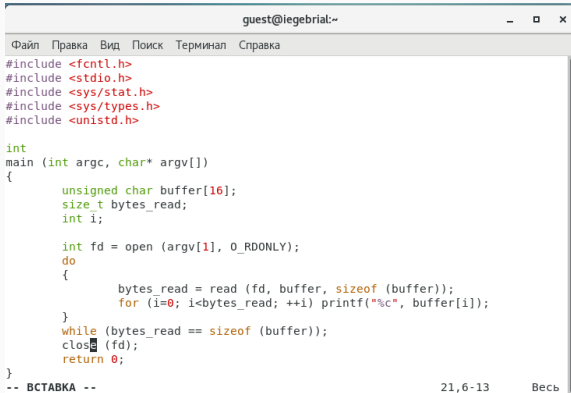
Выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2. (рис. 6)

A terminal window titled 'guest@iegebrial:~' with a menu bar containing 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal shows the command 'ls -l simpleid2' and its output: '-rwsrwxr-x. 1 root guest 8616 ноя 10 14:10 simpleid2'. The filename 'simpleid2' is highlighted in red in the original image.

```
guest@iegebrial:~  
Файл  Правка  Вид  Поиск  Терминал  Справка  
[guest@iegebrial ~]$ ls -l simpleid2  
-rwsrwxr-x. 1 root guest 8616 ноя 10 14:10 simpleid2  
[guest@iegebrial ~]$
```

Figure 6: Проверка правильности установки новых атрибутов и смены владельца файла simpleid2

Создал программу readfile.c. (рис. 7)



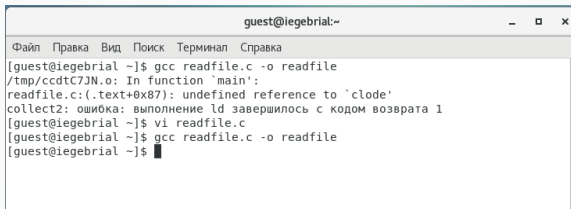
```
guest@iegebriat:~
Файл  Правка  Вид  Поиск  Терминал  Справка
#include <fcntl.h>
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

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;
}
-- ВСТАВКА --                                     21,6-13  Весь
```

Figure 7: Создание программы readfile.c

Откомпилировал её. (рис. 8)



```
guest@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@iegebrial ~]$ gcc readfile.c -o readfile  
/tmp/ccdtC7JN.o: In function 'main':  
readfile.c:(.text+0x87): undefined reference to 'close'  
collect2: ошибка: выполнение ld завершилось с кодом возврата 1  
[guest@iegebrial ~]$ vi readfile.c  
[guest@iegebrial ~]$ gcc readfile.c -o readfile  
[guest@iegebrial ~]$
```

Figure 8: Компиляция программы

Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог. (рис. 9)

```
[root@iegebr1al ~]# chown root /home/guest/readfile.c
[root@iegebr1al ~]# chmod u+x /home/guest/readfile.c
[root@iegebr1al ~]# chmod g-rw /home/guest/readfile.c
[root@iegebr1al ~]# chmod o-r /home/guest/readfile.c
[root@iegebr1al ~]#
```

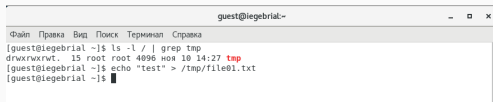
Figure 9: Изменение владельца прав у файла readfile.c

Проверил, что пользователь guest не может прочитать файл readfile.c. (рис. 10)

```
[guest@iegebr1al ~]$ ls -l readfile.c
-rwx----- 1 root guest 416 ноя 10 14:26 readfile.c
[guest@iegebr1al ~]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[guest@iegebr1al ~]$
```

Figure 10: Проверка, что пользователь guest не может прочитать файл readfile.c

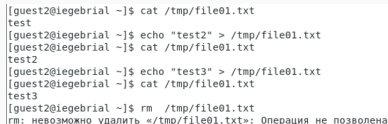
Выяснил, установлен ли атрибут Sticky на директории /tmp и От имени пользователя guest создал файл file01.txt (рис. 11)



```
guest@iegebrial:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@iegebrial ~]$ ls -l / | grep tmp  
drwxrwxrwt. 15 root root 4096 ноя 10 14:27 tmp  
[guest@iegebrial ~]$ echo "test" > /tmp/file01.txt  
[guest@iegebrial ~]$
```

Figure 11: Создание файла file01.txt в директории /tmp со словом test

От пользователя guest2 попробовал дозаписи в файла, записи, удаления файла и проверка.(рис. 12)



```
[guest2@iegebrial ~]$ cat /tmp/file01.txt  
test  
[guest2@iegebrial ~]$ echo "test2" > /tmp/file01.txt  
[guest2@iegebrial ~]$ cat /tmp/file01.txt  
test2  
[guest2@iegebrial ~]$ echo "test3" > /tmp/file01.txt  
[guest2@iegebrial ~]$ cat /tmp/file01.txt  
test3  
[guest2@iegebrial ~]$ rm /tmp/file01.txt  
rm: невозможно удалить «/tmp/file01.txt»: Операция не позволена
```

Figure 12: попытка дозаписи в файла, записи, удаления файла и проверка.

Повысил свои права до суперпользователя и выполнил после этого команду, снимающую атрибут t (Sticky-бит). (рис. 13)

```
[root@iegebrial ~]# chmod -t /tmp
[root@iegebrial ~]# exit
logout
```

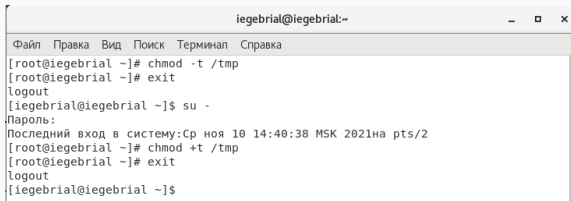
Figure 13: Снятие атрибута "t" с директории /tmp.

Повторил предыдущие шаги. Получилось удалить файл . (рис. 14)

```
[guest2@iegebrial ~]$ cat /tmp/file01.txt
test3
[guest2@iegebrial ~]$ echo "test2" >> /tmp/file01.txt
[guest2@iegebrial ~]$ cat /tmp/file01.txt
test3
test2
[guest2@iegebrial ~]$ echo "test4" > /tmp/file01.txt
[guest2@iegebrial ~]$ cat /tmp/file01.txt
test4
[guest2@iegebrial ~]$ rm /tmp/file01.txt
[guest2@iegebrial ~]$ cat /tmp/file01.txt
cat: /tmp/file01.txt: Нет такого файла или каталога
[guest2@iegebrial ~]$
```

Figure 14: Повторение предыдущих шагов.

Повысил свои права до суперпользователя и вернул атрибут `t` на директорию `/tmp`. (рис. 15)



```
iegebr1al@iegebr1al:~  
Файл Правка Вид Поиск Терминал Справка  
[root@iegebr1al ~]# chmod -t /tmp  
[root@iegebr1al ~]# exit  
logout  
[iegebr1al@iegebr1al ~]$ su -  
.Пароль:  
Последний вход в систему: Ср ноя 10 14:40:38 MSK 2021 на pts/2  
[root@iegebr1al ~]# chmod +t /tmp  
[root@iegebr1al ~]# exit  
logout  
[iegebr1al@iegebr1al ~]$
```

Figure 15: Добавление атрибута “t” на директорию `/tmp`

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

Спасибо за внимание