

# Перезентация по лабораторной работе 5

---

Неустроева И.Н.

19.04.25

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов
- <https://inneustroeva.github.io/ru/>

# Вводная часть

---

Навыки работы с атрибутами, а также компиляции программных файлов и их исполнение- важные умения специалиста в области информационной безопасности.

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

- Процессор pandoc для входного формата Markdown
- Результирующие форматы
  - pdf
  - html
- Автоматизация процесса создания: Makefile

# Создание презентации

---



## Создание программы simpleid.c

Вошли в систему от имени пользователя guest и создали программу simpleid.c



```
guest@inneustroeva:~ — nano 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 программы и проверка на создание файла

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

Скомпилировали программу и убедились, что файл программы создан

```
[guest@inneustroeva ~]$ gcc simpleid.c -o simpleid
[guest@inneustroeva ~]$ ls
1.jpg  dir1  Downloads  Music  Public  simpleid.c  Videos
Desktop  Documents  file3  Pictures  simpleid  Templates
[guest@inneustroeva ~]$
```


# Выполнение программ simpleid и id

Выполнили программу simpleid.c и программу id. Вывод программ одинаковый

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

# Создание программы simpleid2.c

Создали новую программу simpleid2.c, добавили вывод действительных идентификаторов



```
guest@inneustroeva:~ — nano s
GNU nano 5.6.1 simpleid2.c
#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,
```

## Запуск программы simpleid2.c

Скомпилировали и запустили simpleid2.c

```
[guest@inneustroeva ~]$ gcc simpleid2.c -o simpleid2
[guest@inneustroeva ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@inneustroeva ~]$
```

От имени суперпользователя выполнили команды

```
[root@inneustroeva ~]# chown root:guest /home/guest/simpleid2  
[root@inneustroeva ~]# chmod u+s /home/guest/simpleid2  
[root@inneustroeva ~]#
```

## Проверка правильности установки атрибутов и смены владельца файла. Запуск simpleid2 и id

Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустили simpleid2 и id

```
[guest@inneustroeva ~]$ ls -l simpleid2
-rwsr-xr-x. 1 root guest 17656 Apr 19 16:11 simpleid2
[guest@inneustroeva ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@inneustroeva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@inneustroeva ~]$
```

# Создание программы readfile.c

## Создали программу readfile.c

```
GNU nano 5.6.1                                readfile.c
#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;
```



# Откомпилировали программу

Откомпилировали программу

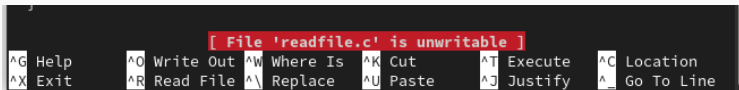
```
[guest@inneustroeva ~]$ gcc readfile.c -o readfile  
[guest@inneustroeva ~]$
```

## Смена владельца у файла readfile.c

Сменили владельца у файла readfile.c и изменили права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог

```
[root@inneustroeva ~]# chown root:guest /home/guest/readfile.c  
[root@inneustroeva ~]# chmod u+s /home/guest/readfile.c  
[root@inneustroeva ~]#
```

Проверили, что пользователь guest не может прочитать файл readfile.c



A screenshot of a terminal window with a dark background. A red error message is displayed in the center: "[ File 'readfile.c' is unwritable ]". Below the message is a menu of keyboard shortcuts arranged in two rows. The first row contains: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, and ^C Location. The second row contains: ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, and ^\_ Go To Line.

```
[ File 'readfile.c' is unwritable ]
```

<b>^G</b>	Help	<b>^O</b>	Write Out	<b>^W</b>	Where Is	<b>^K</b>	Cut	<b>^T</b>	Execute	<b>^C</b>	Location
<b>^X</b>	Exit	<b>^R</b>	Read File	<b>^\ ^_</b>	Replace	<b>^U</b>	Paste	<b>^J</b>	Justify	<b>^_</b>	Go To Line

## Попытка прочесть файл

Проверили, что программа readfile прочитать файл /etc/shadow не может

[illegible]

## Проверка на установку атрибута

Выяснили, что атрибут Sticky на директории /tmp установлен

```
[root@inneustroeva ~]# ls -l / | grep tmp
drwxrwxrwt. 21 root root 4096 Apr 19 17:03 tmp
[root@inneustroeva ~]#
```

## Создание файла с текстом внутри

От имени пользователя guest создали файл file01.txt в директории /tmp со словом test

```
[guest@inneustroeva ~]$ echo "test" > /tmp/file01.txt  
[guest@inneustroeva ~]$
```

## Разрешение в доступе на чтение и запись для каткгории все остальные

Просмотрели атрибуты у только что созданного файла и разрешили доступ на чтение и запись для категории пользователей все остальные

```
[guest@inneustroeva ~]$ ls -l /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 Apr 19 17:07 /tmp/file01.txt  
[guest@inneustroeva ~]$ chmod o+rw /tmp/file01.txt  
[guest@inneustroeva ~]$ ls -l /tmp/file01.txt  
-rw-r--rw-. 1 guest guest 5 Apr 19 17:07 /tmp/file01.txt  
[guest@inneustroeva ~]$
```

## Попытки от пользователя guest2 прочитать, дозаписать и удалить файл

От пользователя guest2 (не являющегося владельцем) получилось прочитать файл /tmp/file01.txt. Дозаписать в файл /tmp/file01.txt слово test2 не удалось. Не получилось записать в файл /tmp/file01.txt слово test3. Не удалось удалить файл /tmp/file01.txt.

```
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
rm: cannot remove '/tmp/file01.txt': Operation not permitted
```



Повысили свои права до суперпользователя и сняли атрибут t (Sticky-бит) с директории /tmp. Покинули режим суперпользователя командой

```
[guest2@inneustroeva ~]$ su -  
Password:  
[root@inneustroeva ~]# chmod -t /tmp  
[root@inneustroeva ~]# exit  
logout  
[guest2@inneustroeva ~]$
```

От пользователя guest2 проверили, что атрибута t нет у директории /tmp

```
[guest2@inneustroeva ~]$ ls -l / | grep tmp  
drwxrwxrwx. 21 root root 4096 Apr 19 17:26 tmp  
[guest2@inneustroeva ~]$
```

## Повторение предыдущих шагов

Повторили предыдущие шаги и выяснили, что можем только прочитать файл и удалить его.

```
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ echo "test2" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ echo "test3" > /tmp/file01.txt
bash: /tmp/file01.txt: Permission denied
[guest2@inneustroeva ~]$ cat /tmp/file01.txt
test
[guest2@inneustroeva ~]$ rm /tmp/file01.txt
rm: remove write-protected regular file '/tmp/file01.txt'? y
[guest2@inneustroeva ~]$
```

## Повысили свои права до суперпользователя и вернули атрибут

Повысили свои права до суперпользователя и вернули атрибут `t` на директорию `/tmp`:

```
rm: remove write-protected regular file  
[guest2@inneustroeva ~]$ su -  
Password:  
[root@inneustroeva ~]# chmod +t /tmp  
[root@inneustroeva ~]# exit  
logout  
[guest2@inneustroeva ~]$
```

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

...