

# Отчет по лабораторной работе № 5

## Основы информационной безопасности

---

Маметкадыров Ынтымак

Российский университет дружбы народов, Москва, Россия

НПМбд-02-20

# **Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов**

---

## Цель лабораторной работы

- Изучить особенности работы с дополнительными атрибутами SetUID, SetGID и Sticky.
- Изучить механизмы изменения идентификаторов.

## Задачи лабораторной работы

- Создать программу, выводящую uid и gid, и посмотреть на вывод после добавления SetUID и SetGID битов.
- Создать программу для чтения файлов и проверить вывод после добавления SetUID бита.
- На примере папки /tmp изучить влияние Sticky бита на запись и удаление файлов.

## **Ход лабораторной работы**

---

## Создание файла

Создаём файл `simpleid2.c`, который будет выводить `uid` и `gid`. При отсутствии дополнительных битов, она выводит информацию, совпадающую с выводом команды `id`.

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

**Figure 1:** Результат работы `simpleid2`

## Установка SetUID-бита

С помощью команды `chown` меняем владельца файла на `root` и устанавливаем SetUID командой `chmod u+s`.

```
[itmametskadihrov@itmametskadihrov ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для itmametskadihrov:
[itmametskadihrov@itmametskadihrov ~]$ sudo chmod u+s /home/guest/simpleid2
[itmametskadihrov@itmametskadihrov ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 26016 окт  6 18:27 /home/guest/simpleid2  I
[itmametskadihrov@itmametskadihrov ~]$
```

**Figure 2:** Установка SetUID-бита

## Запуск simpleid2

После запуска видим, что uid сменилось на 0 (для root), в то время как в команде id uid всё ещё остался 1001.

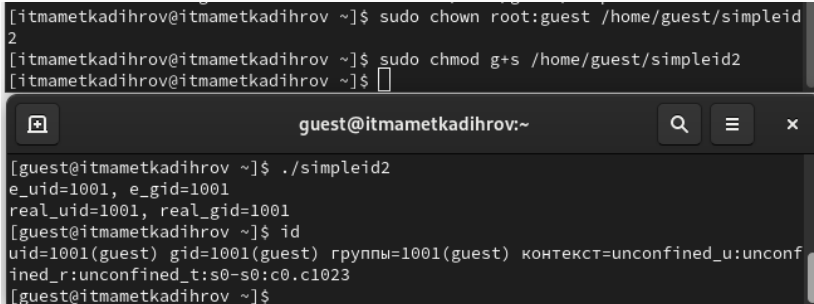
```
[guest@itmametkadihrov ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=0, real_gid=1001
[guest@itmametkadihrov ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@itmametkadihrov ~]$
```

**Figure 3:** Результат работы simpleid2

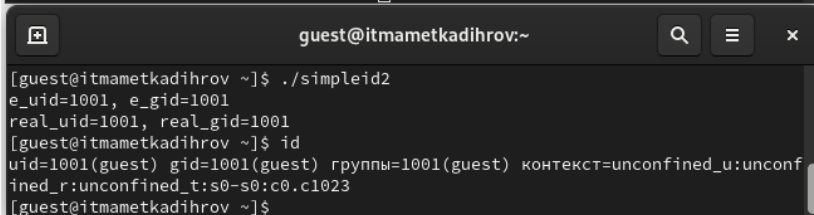


## Установка SetGID-бита

С помощью команды `chown` меняем группу для файла и устанавливаем SetGID командой `chmod g+s`. Видим, что при запуске программы изменился вывод `gid`.



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

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

Figure 4: Установка setGID-бита

## Наличие Sticky-бита

Проводим над файлом file01.txt следующие действия: читаем его, дозаписываем и перезаписываем информацию, переименовываем. Эти действия проходят без ошибок. При попытке удаления возникает ошибка.

```
[itmametskadihrov@itmametskadihrov ~]$ su - guest2
Пароль:
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
rm: удалить защищённый от записи обычный файл '/tmp/file01.txt'?
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
```

**Figure 5:** Действия над файлом

## Изменение Sticky-бита

От имени суперпользователя удаляем sticky-бит командой `chmod -t`.

```
[root@itmametskadihrov ~]# chmod -t /tmp
[root@itmametskadihrov ~]# exit
выход
[itmametskadihrov@itmametskadihrov ~]$
```

**Figure 6:** Удаление Sticky-бита

## Отсутствие Sticky-бита

Повторяем описанные ранее действия над файлом file01.txt. Теперь пользователь может удалить не принадлежащий ему файл.

```
[guest2@itmametskadihrov ~]$ ls -l / | grep tmp
drwxrwxrwx. 17 root root 4096 окт  6 18:10 tmp
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
[guest2@itmametskadihrov ~]$ echo "test2" >> /tmp/file01.txt
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test
test2
[guest2@itmametskadihrov ~]$ echo "test3" > /tmp/file01.txt
[guest2@itmametskadihrov ~]$ cat /tmp/file01.txt
test3
[guest2@itmametskadihrov ~]$ rm /tmp/file01.txt
[guest2@itmametskadihrov ~]$
```

**Figure 7:** Действия над файлом

- Изучили механизмы изменения идентификаторов.
- Получили практические навыки по работе с дополнительными атрибутами.