

0.1 Front matter

title: "Лабораторная работа №5" subtitle: "Основы информационной безопасности"
author: "Пинега Белла Александровна"

0.2 Generic options

lang: ru-RU toc-title: "Содержание"

0.3 Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

0.4 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables
fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia
polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true
polyglossia-otherlangs: name: english ## I18n babel babel-lang: russian babel-otherlangs:
english ## Fonts mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT
Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions:
Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9
Biblatex biblatex: true biblio-style: "gost-numeric" biblatexoptions: - parenttracker=true
- backend=biber - hyperref=auto - language=auto - autolang=other* - citestyle=gost-
numeric ## Pandoc-crossref LaTeX customization figureTitle: "Рис." tableTitle: "Таблица"
listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle: "Список таблиц" lolTitle:
"Листинги" ## Misc options indent: true header-includes: -

keep figures where there are in the text

– # keep figures where there are in the text

1 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

2 Задание

Загрузите в дисплейном классе операционную систему Linux. Осуществите вход в систему. Запустите терминал. Перейдите в каталог /var/tmp: cd /var/tmp Создайте каталог с именем пользователя (совпадающий с логином студента в дисплейном

классе). Для этого можно использовать команду: `mkdir /var/tmp/id -un` или непосредственно: `mkdir /var/tmp/имя_пользователя` Здесь вместо `имя_пользователя` должен быть указан ваш логин (учётная запись) в дисплейном классе. Запустите виртуальную машину, введя в командной строке:

Информационная безопасность компьютерных сетей 11 Рис. 1.6. Окно определения формата виртуального жёсткого диска Рис. 1.7. Окно определения размера виртуального динамического жёсткого диска и его расположения После завершения установки операционной системы корректно переза-пустите виртуальную машину (рис. 1.18) и при запросе примите условия лицензии (рис. 1.19–1.20). Рис. 1.8. Окно «Носители» виртуальной машины: подключение образа оптического диска Рис. 1.9. Запуск виртуальной машины В VirtualBox оптический диск должен отключиться автоматически, но если это не произошло, то необходимо отключить носитель информации с обра-зом, выбрав Свойства Носители Rocky-номер-версии.iso Удалить устройство . Информационная безопасность компьютерных сетей 13 Рис. 1.10. Установка английского языка интерфейса ОС Войдите в ОС под заданной вами при установке учётной записью. В меню Устройства виртуальной машины подключите образ диска дополнений госте-вой ОС (рис. 1.21, 1.22), при необходимости введите пароль пользователя root вашей виртуальной ОС. После загрузки дополнений нажмите Return или Enter и корректно переза-грузите виртуальную машину. 14 Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.11. Окно настройки установки образа ОС Рис. 1.12. Окно настройки установки: выбор программ 1.3.1. Установка имени пользователя и названия хоста Если при установке виртуальной машины вы задали имя пользователя или имя хоста, не удовлетворяющее соглашению об именовании (см. раздел 1.2.2), то вам необходимо исправить это. 1. Запустите виртуальную машину и залогиньтесь. 2. Запустите терминал и получите полномочия администратора: `su -` Информационная безопасность компьютерных сетей 15 Рис. 1.13. Окно настройки установки: отключение KDUMP Рис. 1.14. Окно настройки установки: место установки 3. Создайте пользователя (вместо `username` укажите ваш логин в дисплей-ном классе): `adduser -G wheel username` 4. Задайте пароль для пользователя (вместо `username` укажите ваш логин в дисплейном классе): `passwd username` 16 Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.15. Окно настройки установки: сеть и имя узла Рис. 1.16. Установка пароля для root 5. Установите имя хоста (вместо `username` укажите ваш логин в дисплейном классе): `hostnamectl set-hostname username` 6. Проверьте, что имя хоста установлено верно: `hostnamectl` Информационная безопасность компьютерных сетей 17 Рис. 1.17. Установка пароля для пользователя с правами администратора Рис. 1.18. Завершение установки ОС 1.4. Домашнее задание Дождитесь загрузки графического окружения и откройте терминал. В окне терминала проанализируйте последовательность загрузки системы, выпол-нив команду `dmesg`. Можно просто просмотреть вывод этой команды: 18 Кулябов Д. С., Королькова А. В., Геворкян М. Н. Рис. 1.19. Первоначальная настройка ОС: переход к лицензии Рис. 1.20. Первоначальная настройка ОС: лицензия `dmesg | less` Информационная безопасность компьютерных сетей 19 Рис. 1.21. Подключение образа диска дополнений гостевой ОС Рис. 1.22. Запуск образа диска дополнений гостевой ОС Можно использовать поиск с помощью `grep`: `dmesg | grep -i "то, что ищем"` Получите следующую информацию. 1. Версия ядра Linux (Linux version). 2. Частота процессора (Detected

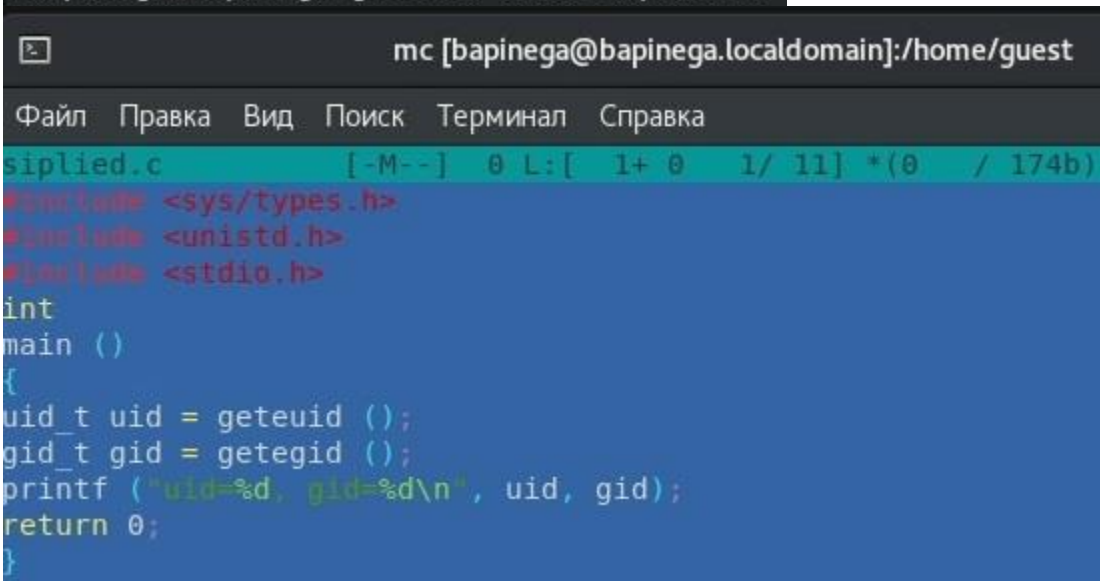
Mhz processor). 3. Модель процессора (CPU0). 4. Объем доступной оперативной памяти (Memory available). 5. Тип обнаруженного гипервизора (Hypervisor detected). 6. Тип файловой системы корневого раздела. 20 Кулябов Д. С., Королькова А. В., Геворкян М. Н. 7. Последовательность монтирования файловых систем # Теоретическое введение

1.2.1. Техническое обеспечение Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (<https://www.virtualbox.org/>) операционной системы Linux (дистрибутив Rocky (<https://rockylinux.org/>)). Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками: – Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 20 GB свободного места на жёстком диске; – ОС Linux Gentoo (<http://www.gentoo.ru/>); – VirtualBox верс. 6.1 или старше; – каталог с образами ОС для работающих в дисплейном классе: [/afs/dk.sci.pfu.edu.ru/common/files/iso/](http://afs/dk.sci.pfu.edu.ru/common/files/iso/). 1.2.2. Соглашения об именовании При выполнении работ следует придерживаться следующих правил именования: имя виртуальной машины, имя хоста вашей виртуальной машины, пользователь внутри виртуальной машины должны совпадать с логином студента, выполняющего лабораторную работу. Вы можете посмотреть ваш логин, набрав в терминале ОС типа Linux команду `id -un`.

3 Выполнение лабораторной работы

1. Войду в систему от имени пользователя guest. Создам программу `simpleid.c`:

```
[bapinega@bapinega ~]$ cd /home/guest
[bapinega@bapinega guest]$ touch siplied.c
```



The screenshot shows a terminal window titled "mc [bapinega@bapinega.localdomain]:/home/guest". The terminal has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The file "siplied.c" is open, showing its metadata as "[-M--] 0 L:[1+ 0 1/ 11] *(0 / 174b)". The code content is as follows:

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

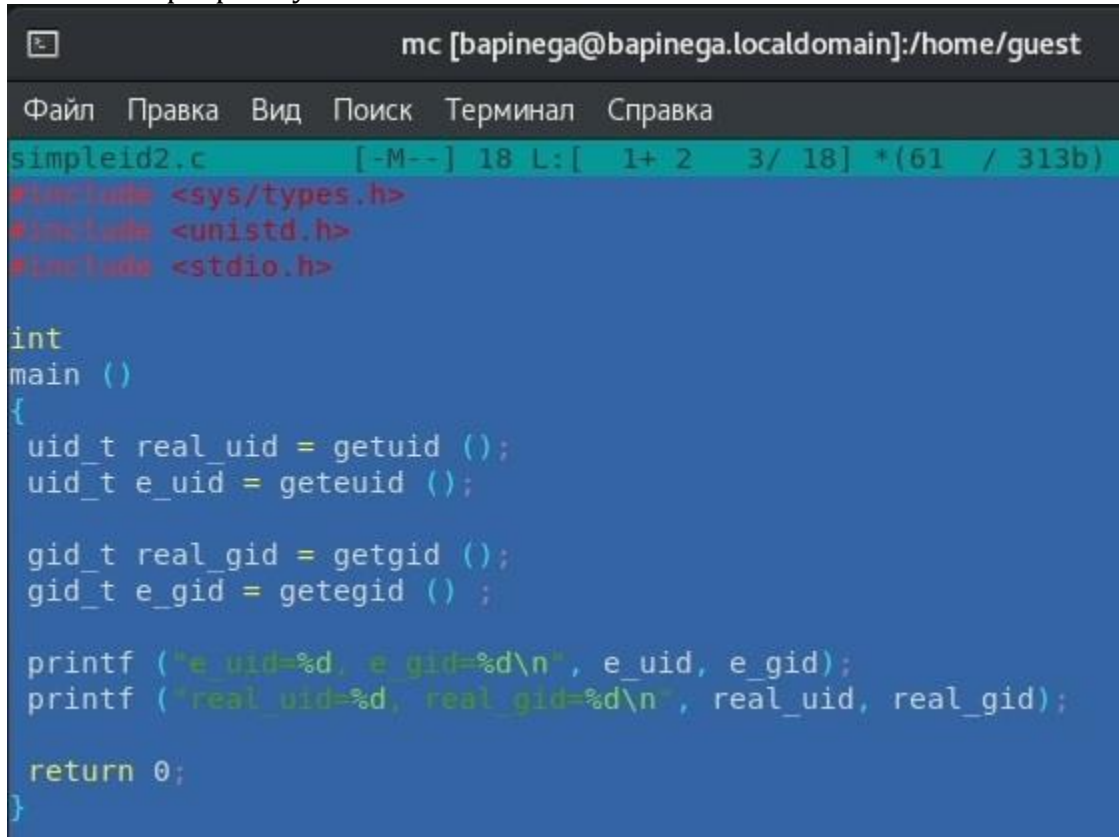
int
main ()
{
    uid_t uid = geteuid ();
    gid_t gid = getegid ();
    printf ("uid=%d, gid=%d\n", uid, gid);
    return 0;
}
```

2. Скомпилирую программу. Успешно. Выполню системную программу id:

```
[bapinega@bapinega guest]$ mv siplied.c simpleid.c
[bapinega@bapinega guest]$ gcc simpleid.c -o simpleid
[bapinega@bapinega guest]$ ls
dir1 simpleid simpleid.c
[bapinega@bapinega guest]$ ./sipleid
bash: ./sipleid: Нет такого файла или каталога
[bapinega@bapinega guest]$ ./simpleid
uid=1000, gid=1000
[bapinega@bapinega guest]$ id
uid=1000(bapinega) gid=1000(bapinega) группы=1000(bapinega),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Во второй команде результат более детальный, но uid и gid совпадают

3. Усложню программу



```
mc [bapinega@bapinega.localdomain]:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
simpleid2.c  [-M--] 18 L: [ 1+ 2 3/ 18] *(61 / 313b)
#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;
}
```

Получившуюся программу назову simpleid2.c. Скомпилирую и запущу

```
[bapinega@bapinega guest]$ gcc simpleid2.c -o simpleid2
[bapinega@bapinega guest]$ ./simpleid2
e_uid=1000, e_gid=1000
real uid=1000, real gid=1000
```

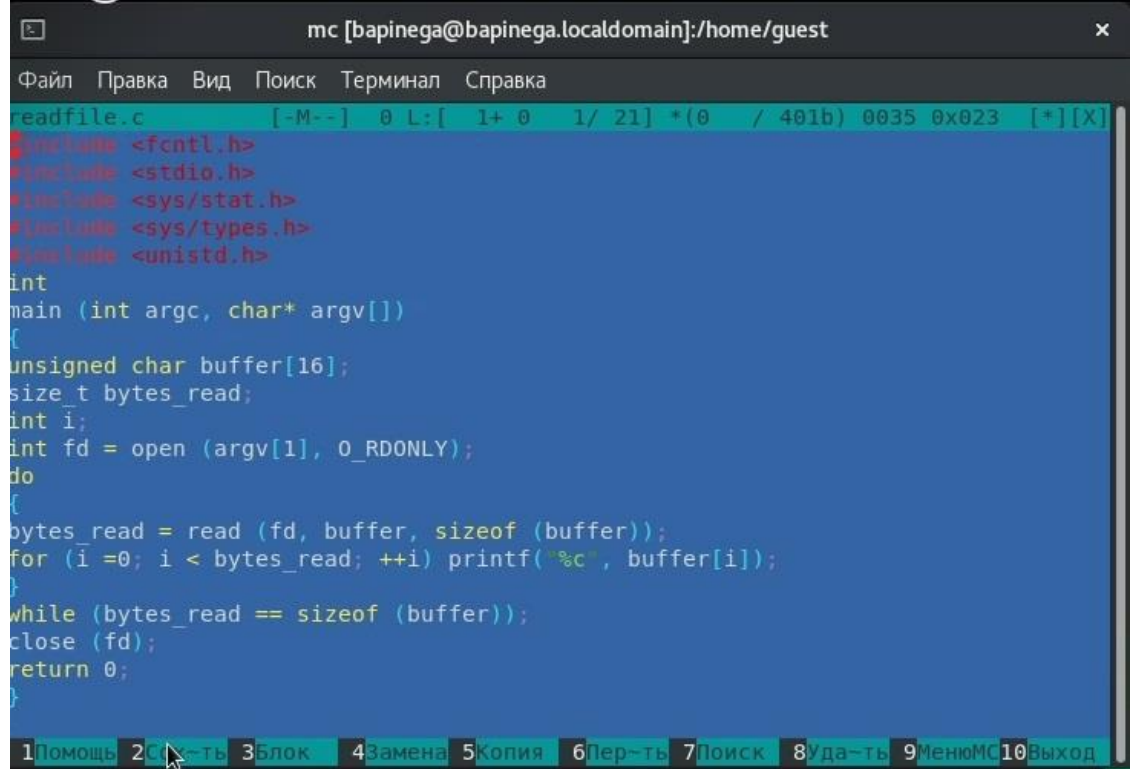
4. От имени суперпользователя выполню команды

```
[bapinega@bapinega guest]$ su
Пароль:
[root@bapinega guest]# chown root:guest /home/guest/simpleid2
[root@bapinega guest]# chmod u+s /home/guest/simpleid2
```

5. Выполню проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls -l simpleid2 Запущу simpleid2 и id Прделаю тоже

самое относительно SetGID-бита. Создам программу readfile.c:

```
[root@bapinega guest]# ls -l simpleid2
-rwsrwxr-x. 1 root guest 18256 фев 21 17:08 simpleid2
[root@bapinega guest]# exit
exit
[bapinega@bapinega guest]$ ./simpleid2
e_uid=0, e_gid=1000
real_uid=1000, real_gid=1000
[bapinega@bapinega guest]$ id
uid=1000(bapinega) gid=1000(bapinega) группы=1000(bapinega),10(wheel) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[bapinega@bapinega guest]$ touch readfile.c
[bapinega@bapinega guest]$ mc
```



```
mc [bapinega@bapinega.localdomain]:/home/guest
Файл  Правка  Вид  Поиск  Терминал  Справка
readfile.c  [-M--]  0 L:[ 1+ 0  1/ 21]  *(0  / 401b) 0035 0x023  [*][X]
#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;
}
```

6. откомпилирую ее

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

7. Сменю владельца у файла readfile.c (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (root) мог прочитать его, а guest не мог.


```

}[bapinega@bapinega guest]$ su
Пароль:
[root@bapinega guest]# chown root:root readfile
[root@bapinega guest]# chmod -rwx readfile.c
chmod: readfile.c: новые права доступа ----w----, а не -----
[root@bapinega guest]# chmod u+s readfile
[root@bapinega guest]# exit
exit
[bapinega@bapinega guest]$ cat readfile.c
cat: readfile.c: Отказано в доступе
[bapinega@bapinega guest]$ ./readfile readfile.c
bash: ./readfile: Отказано в доступе
[bapinega@bapinega guest]$ su
Пароль:
[root@bapinega guest]# chown root:guest /home/guest/readfile/c
chown: невозможно получить доступ к '/home/guest/readfile/c': Это не каталог
[root@bapinega guest]# chown root:guest /home/guest/readfile.c
[root@bapinega guest]# chmod 700 readfile.c
[root@bapinega guest]# ./readfile 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;
}

```

8. Сменю у программы readfile владельца и установлю SetU'D-бит

9. Программа readfile может прочитать файл /etc/shadow

```
[root@bapinega guest]# ./readfile /etc/shadow
root:$6$PAbFRHdtXhKqS6Ra$Sx9H51lwR/XHg20t9wWBH7J3AFP7ugdascT60oIxnMbLC6
n0qjc20ZoN2n3o7PBg6GE2/4G127030::0:99999:7:::
bin:!:19326:0:99999:7:::
daemon:!:19326:0:99999:7:::
adm:!:19326:0:99999:7:::
lp:!:19326:0:99999:7:::
sync:!:19326:0:99999:7:::
shutdown:!:19326:0:99999:7:::
halt:!:19326:0:99999:7:::
mail:!:19326:0:99999:7:::
operator:!:19326:0:99999:7:::
games:!:19326:0:99999:7:::
ftp:!:19326:0:99999:7:::
nobody:!:19326:0:99999:7:::
dbus:!!:19768:::
systemd-coredump:!!:19768:::
systemd-resolve:!!:19768:::
tss:!!:19768:::
polkitd:!!:19768:::
geoclue:!!:19768:::
unbound:!!:19768:::
rtkit:!!:19768:::
pipewire:!!:19768:::
dnsmasq:!!:19768:::
clevis:!!:19768:::
usbmuxd:!!:19768:::
gluster:!!:19768:::
rpc:!!:19768:0:99999:7:::
chrony:!!:19768:::
avahi:!!:19768:::
saslauth:!!:19768:::
libstoragemgmt:!!:19768:::
sssd:!!:19768:::
qemu:!!:19768:::
cockpit-ws:!!:19768:::
cockpit-wsinstance:!!:19768:::
colord:!!:19768:::
rpcuser:!!:19768:::
pulse:!!:19768:::
setroubleshoot:!!:19768:::
flatpak:!!:19768:::
gdm:!!:19768:::
gnome-initial-setup:!!:19768:::
pesign:!!:19768:::
sshd:!!:19768:::
tcpdump:!!:19768:::
```

{#fig:012width=70%}

10. Выясню, установлен ли атрибут Sticky на директории. После от имени пользователя guest создам файл file01.txt в директории /tmp со словом test. Просмотрю атрибуты у только что созданного файла и разрешу чтение и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt

chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt Все операции выполнить не от имени гость2 не удалось. А от владельца удалось.

```
[bapinega@bapinega guest]$ ls -l / | grep tmp
drwxrwxrwt. 14 root root 4096 фев 21 18:34 tmp
[bapinega@bapinega guest]$ echo "test" > /tmp/file01.txt
[bapinega@bapinega guest]$ ls -l /tmp/file01.txt
-rw-rw-r--. 1 bapinega bapinega 5 фев 21 18:37 /tmp/file01.txt
[bapinega@bapinega guest]$ chmod o+rw /tmp/file01.txt
[bapinega@bapinega guest]$ ls -l /tmp/file01.txt
-rw-rw-rw-. 1 bapinega bapinega 5 фев 21 18:37 /tmp/file01.txt
[bapinega@bapinega guest]$ cd /home/guest2
[bapinega@bapinega guest2]$ cat /tmp/file01.txt
test
[bapinega@bapinega guest2]$ echo "test2" > /tmp/file01.txt
[bapinega@bapinega guest2]$ cat /tmp/file01.txt
test2
[bapinega@bapinega guest2]$ echo "test3" > /tmp/file01.txt
```

11. Все операции выполнить не от имени гость2 удалось.

```
[bapinega@bapinega guest2]$ cat /tmp/file01.txt
test3
[bapinega@bapinega guest2]$ rm /tmp/file01.txt
[bapinega@bapinega guest2]$ su -
Пароль:
[root@bapinega ~]# chmod -t /tmp
[root@bapinega ~]# exit
выход
[bapinega@bapinega guest2]$ ls -l / | grep tmp
drwxrwxrwx. 14 root root 4096 фев 21 18:41 tmp
[bapinega@bapinega guest2]$ echo "test3" > /tmp/file01.txt
[bapinega@bapinega guest2]$ cat /tmp/file01.txt
test3
[bapinega@bapinega guest2]$ rm /tmp/file01.txt
[bapinega@bapinega guest2]$ su -
Пароль:
[root@bapinega ~]# chmod +t /tmp
[root@bapinega ~]# exit
выход
```

4 Выводы

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в кон- соли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов

Список литературы