

# Отчет к лабораторной работе №7

## Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

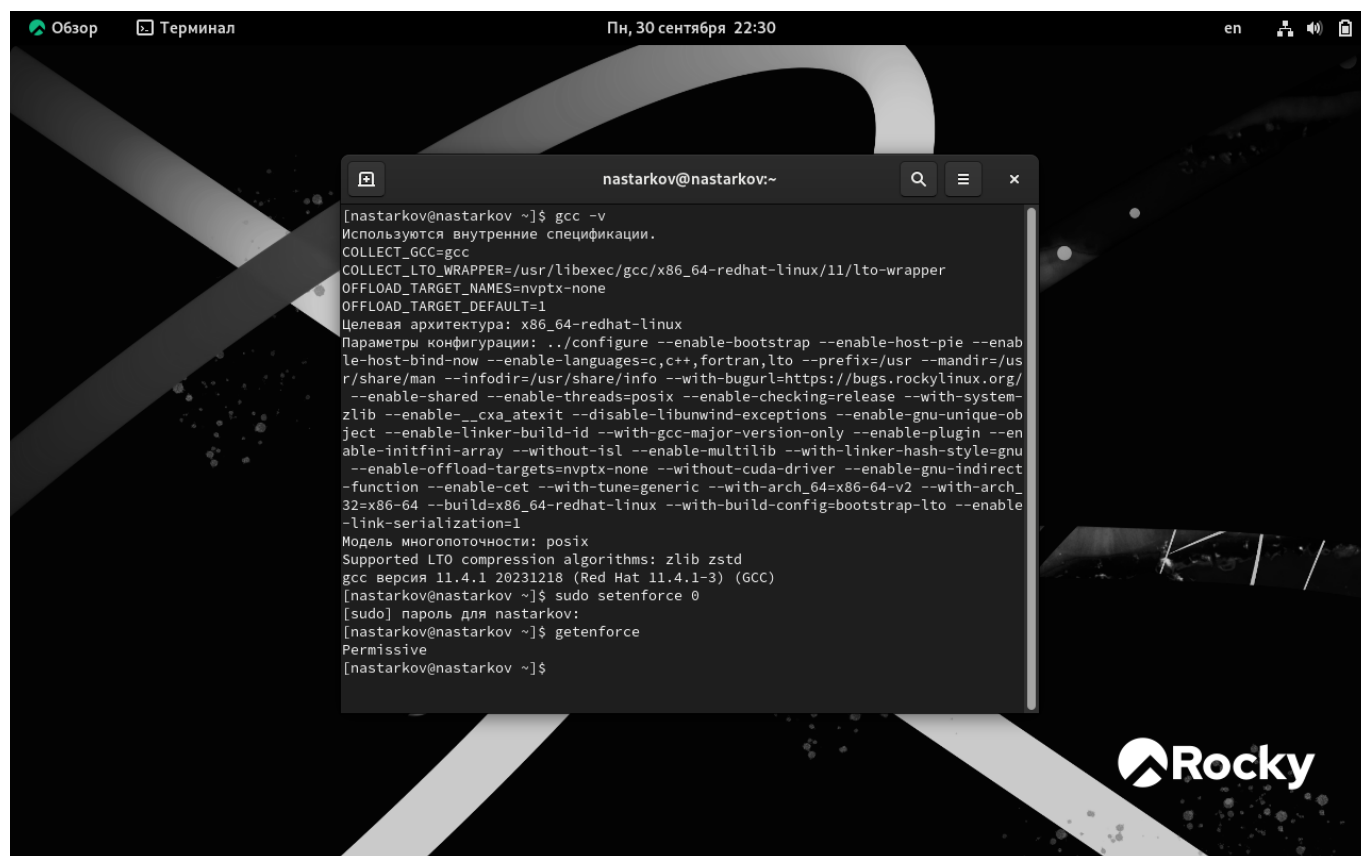
author: Старков Н.А.

## Цель работы

Освоить на практике применение режима однократного гаммирования.

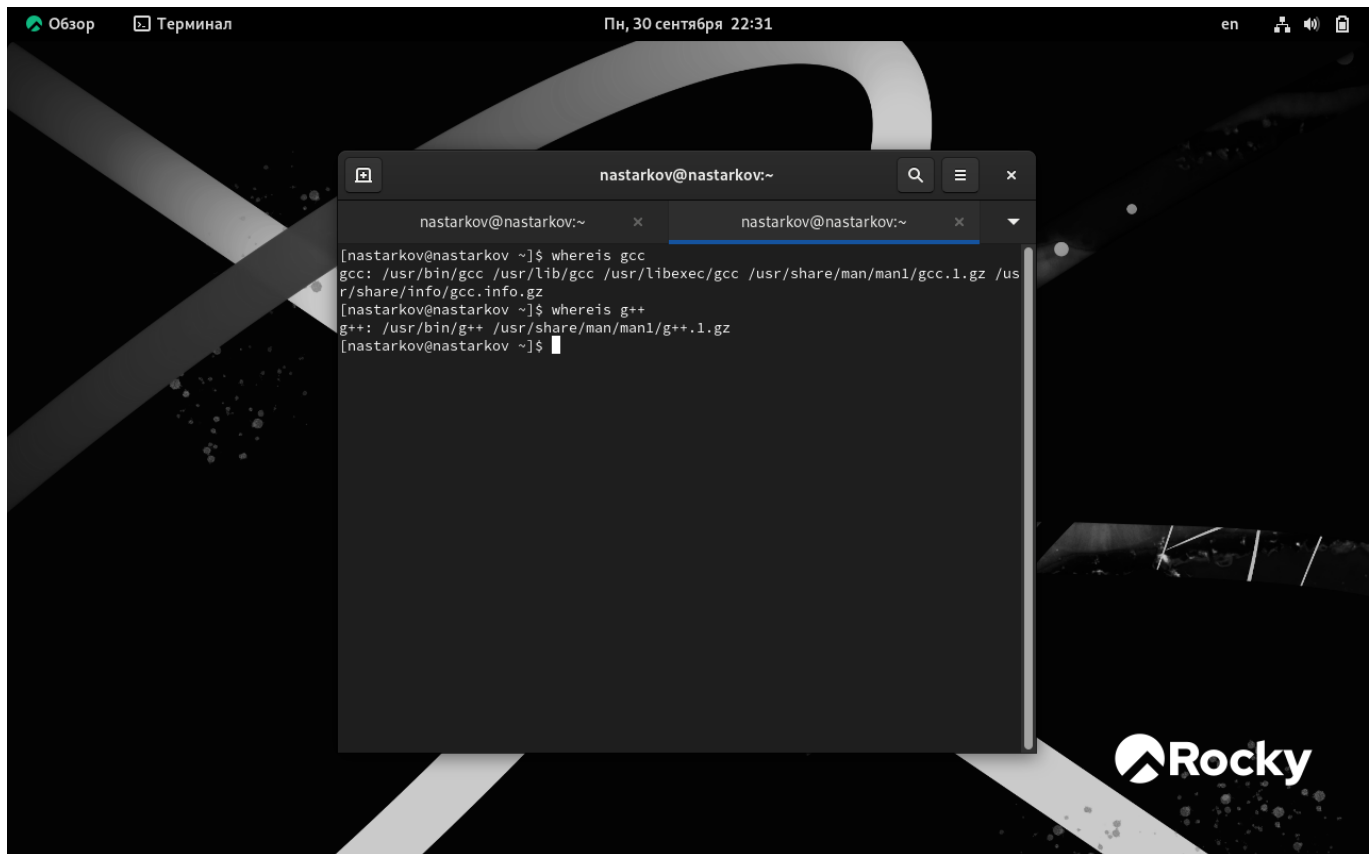
## Выполнение работы

1. Для начала я убедился, что компилятор gcc установлен, используя команду "gcc -v". Затем отключила систему запретов до очередной перезагрузки системы командой "sudo setenforce 0", после чего команда "getenforce" вывела "Permissive"

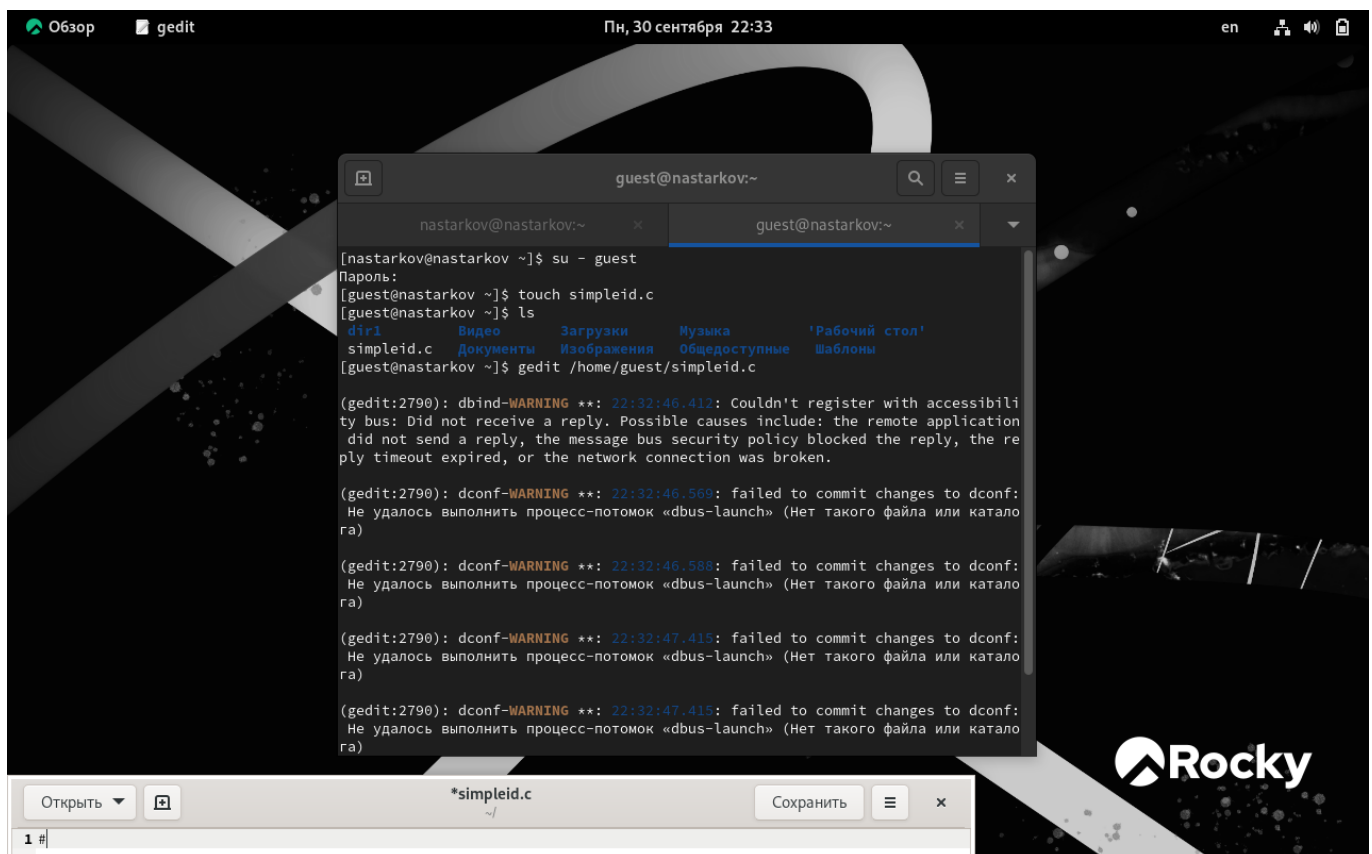


```
[nastarkov@nastarkov ~]$ gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --enable-host-pie --enable-host-bind-now --enable-languages=c,c++,fortran,lto --prefix=/usr --mandir=/usr/share/man --infodir=/usr/share/info --with-bugurl=https://bugs.rockylinux.org/ --enable-shared --enable-threads=posix --enable-checking=release --with-system-zlib --enable-_cxa_atexit --disable-libunwind-exceptions --enable-gnu-unique-object --enable-linker-build-id --with-gcc-major-version-only --enable-plugin --enable-initfini-array --without-isl --enable-multilib --with-linker-hash-style=gnu --enable-offload-targets=nvptx-none --without-cuda-driver --enable-gnu-indirect-function --enable-cet --with-tune=generic --with-arch_64=x86-64-v2 --with-arch_32=x86-64 --build=x86_64-redhat-linux --with-build-config=bootstrap-lto --enable-link-serialization=1
Модель многопоточности: posix
Supported LTO compression algorithms: zlib zstd
gcc версия 11.4.1 20231218 (Red Hat 11.4.1-3) (GCC)
[nastarkov@nastarkov ~]$ sudo setenforce 0
[sudo] пароль для nastarkov:
[nastarkov@nastarkov ~]$ getenforce
Permissive
[nastarkov@nastarkov ~]$
```

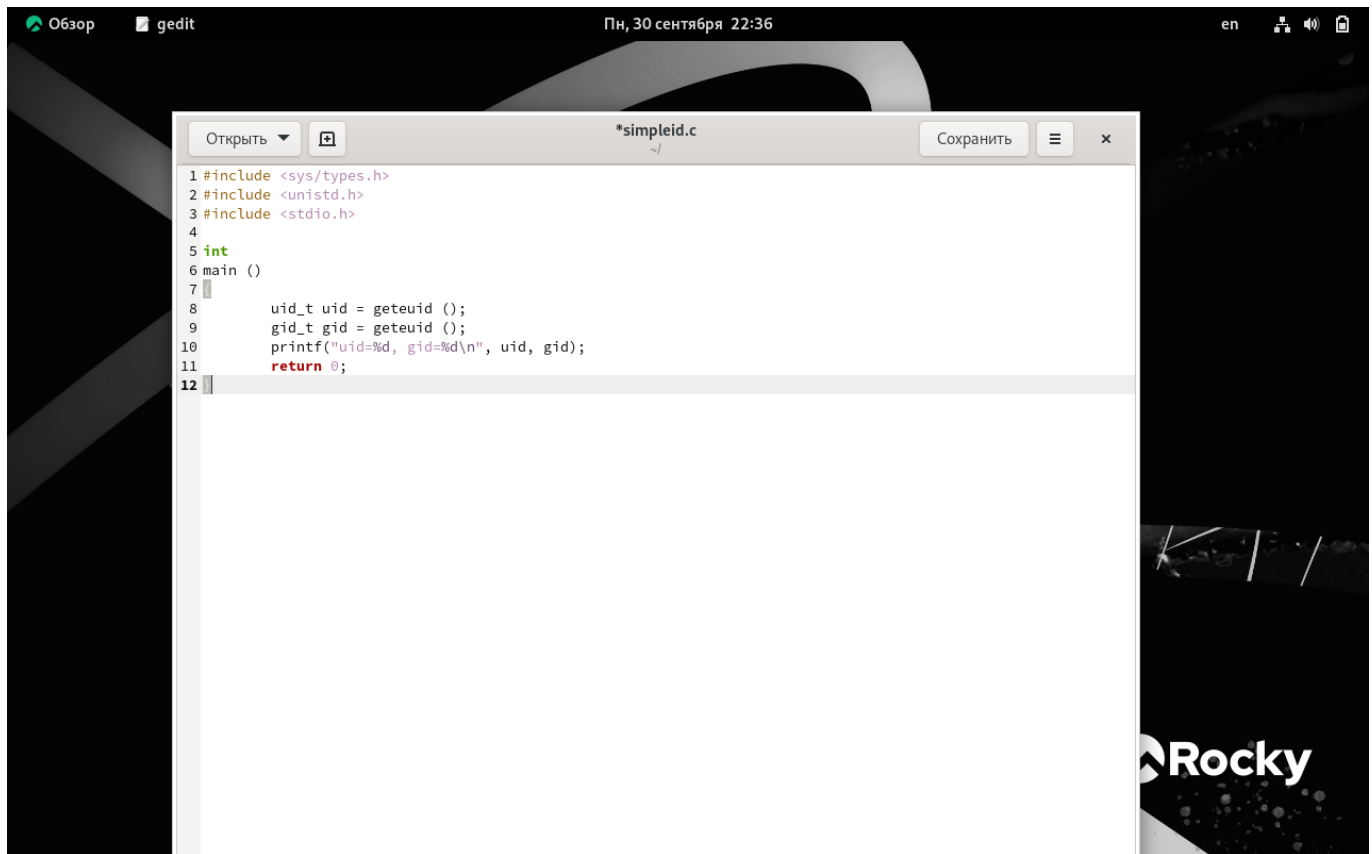
2. Проверили успешное выполнение команд "whereis gcc" и "whereis g++"



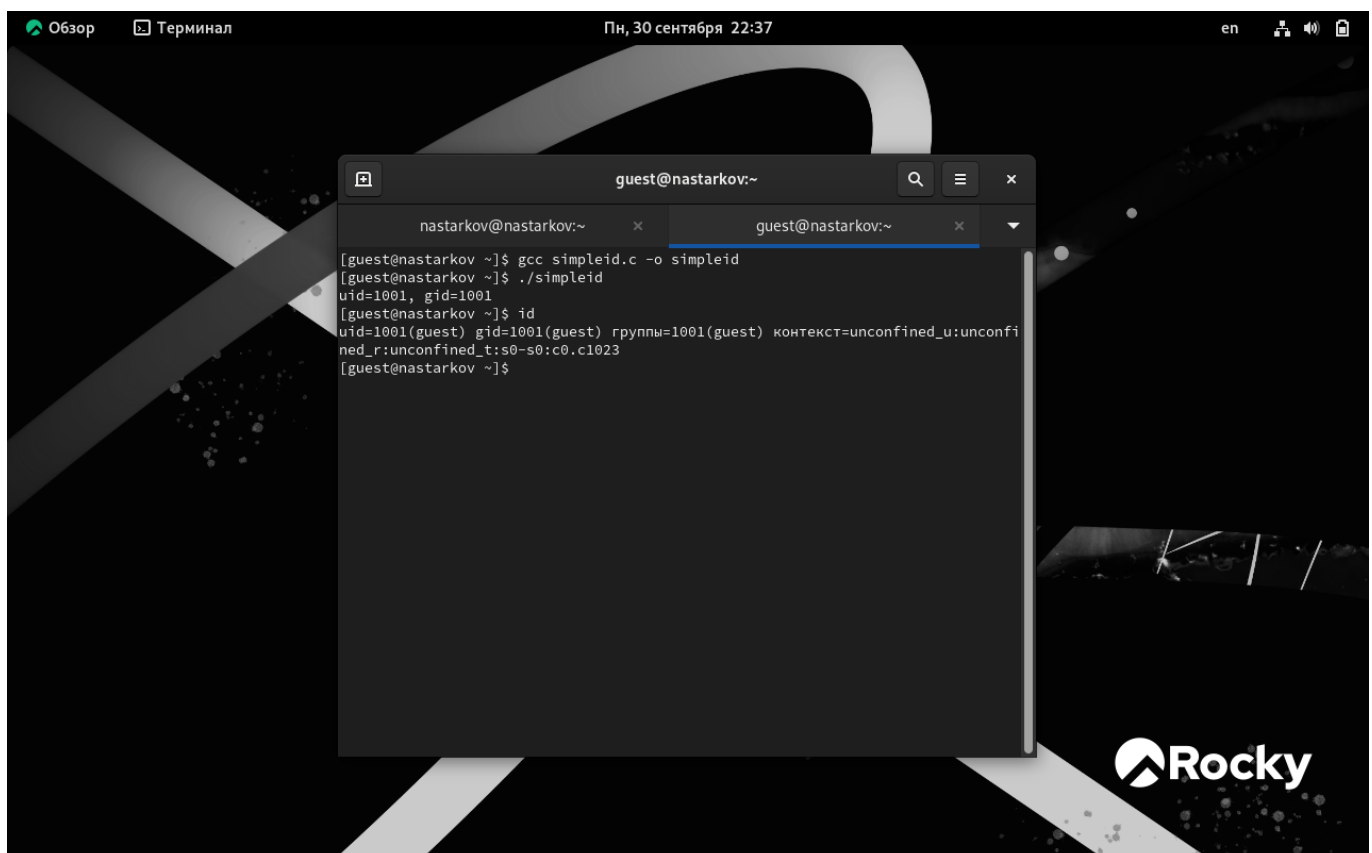
3. Вошли в систему от имени пользователя guest командой "su - guest". Создали программу simpleid.c командой "touch simpleid.c" и открыла её в редакторе командой "gedit /home/guest/simpleid.c"



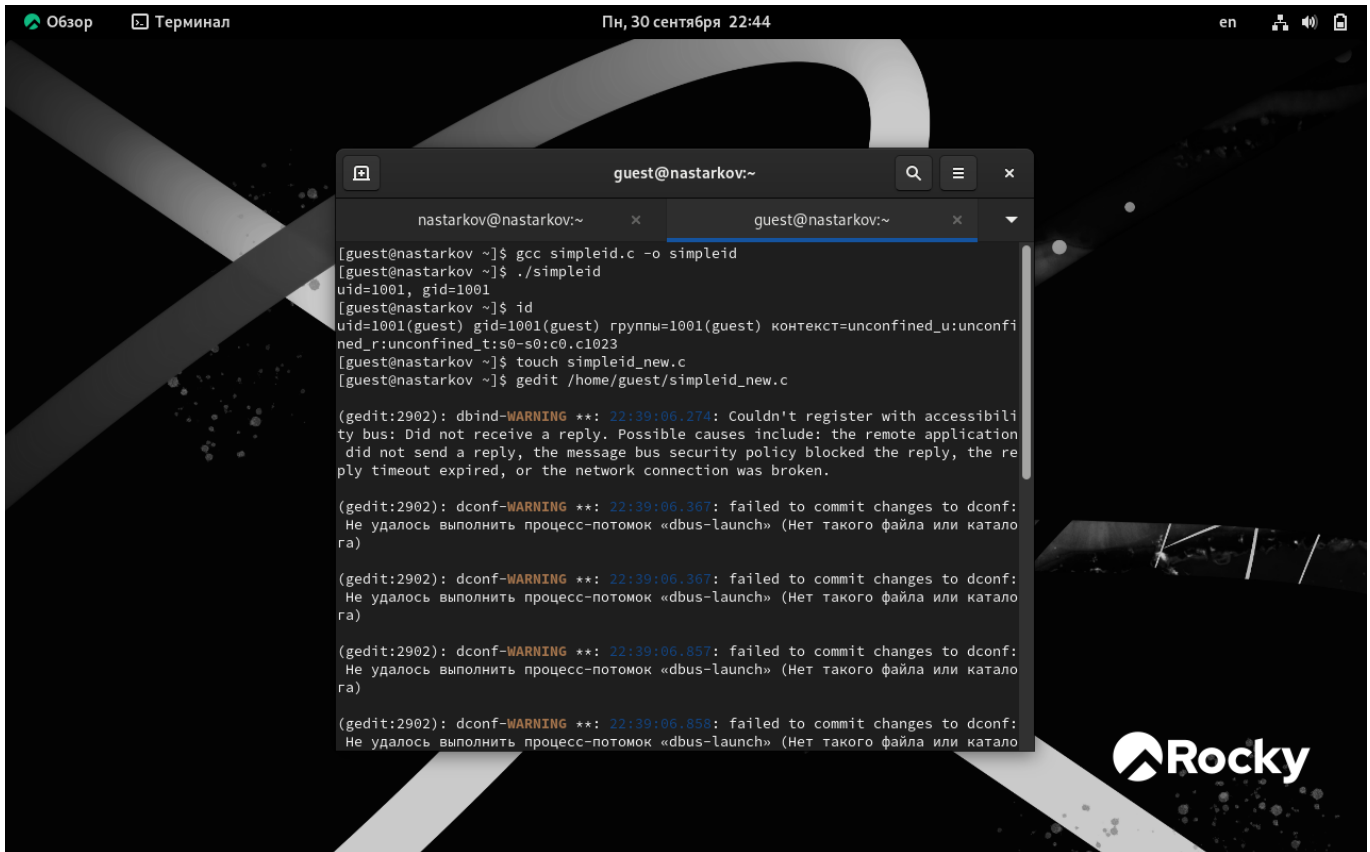
4. Написали код в созданном файле



5. Скомпилировали программу и запустили ее

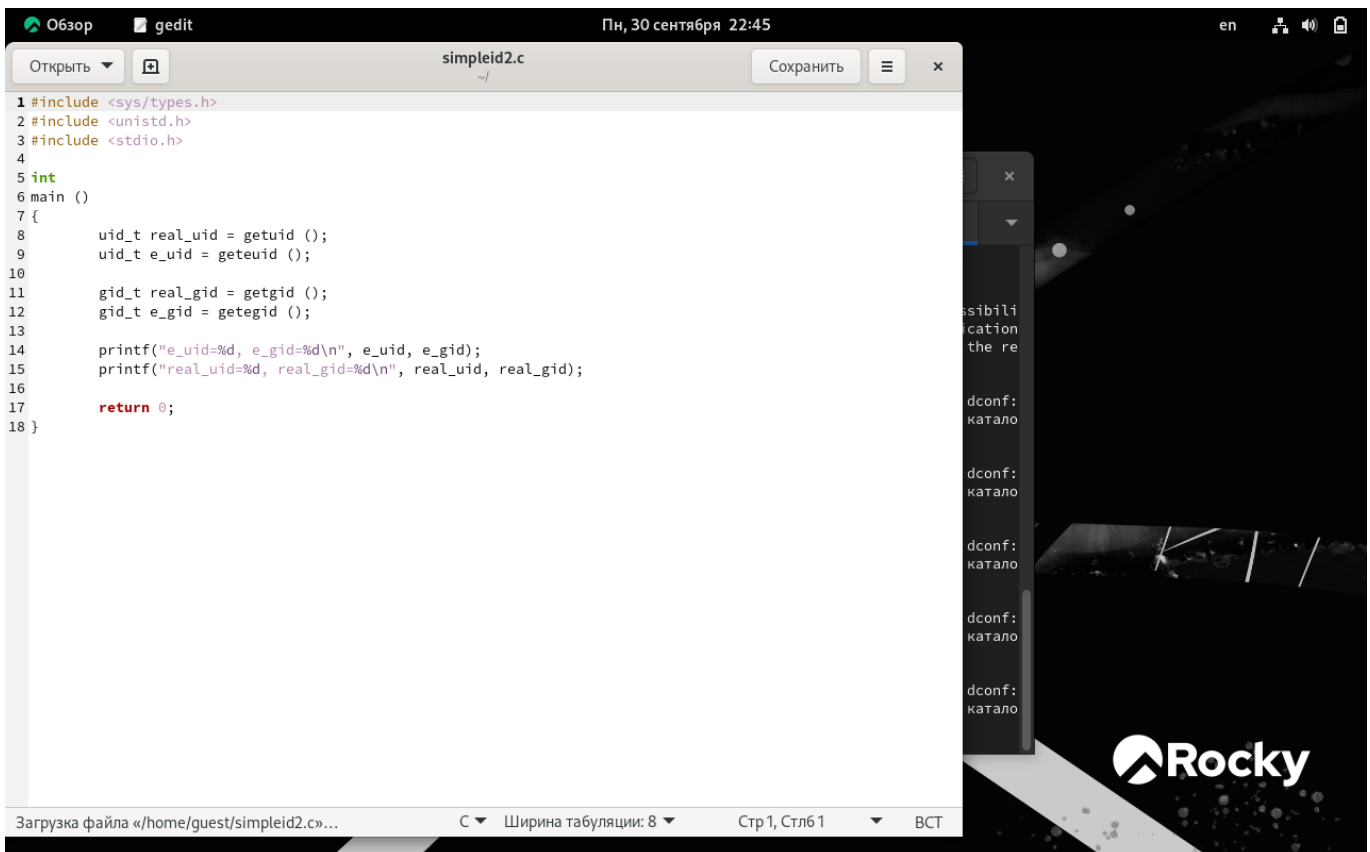


6. Создаем новый файл, там пишем более сложный код, компилируем и запускаем программу.



```
Обзор Терминал Пн, 30 сентября 22:44 en
```

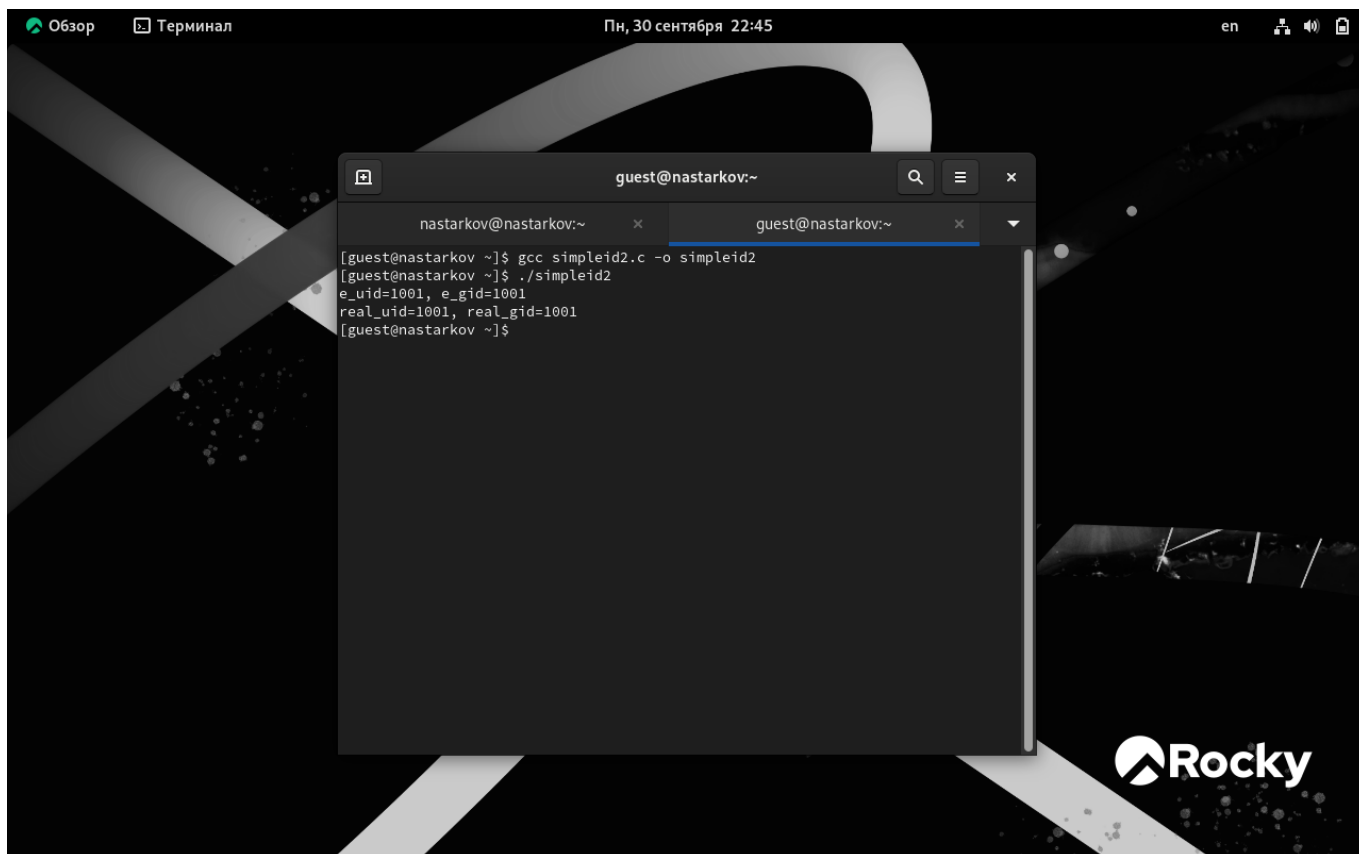
```
guest@nastarkov:~  
nastarkov@nastarkov:~ x guest@nastarkov:~ x  
[guest@nastarkov ~]$ gcc simpleid.c -o simpleid  
[guest@nastarkov ~]$ ./simpleid  
uid=1001, gid=1001  
[guest@nastarkov ~]$ id  
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi  
ned_r:unconfined_t:s0-s0:c0.c1023  
[guest@nastarkov ~]$ touch simpleid_new.c  
[guest@nastarkov ~]$ gedit /home/guest/simpleid_new.c  
  
(gedit:2902): dbind-WARNING **: 22:39:06.274: Couldn't register with accessibili  
ty bus: Did not receive a reply. Possible causes include: the remote application  
did not send a reply, the message bus security policy blocked the reply, the re  
ply timeout expired, or the network connection was broken.  
  
(gedit:2902): dconf-WARNING **: 22:39:06.367: failed to commit changes to dconf:  
Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или катало  
га)  
  
(gedit:2902): dconf-WARNING **: 22:39:06.367: failed to commit changes to dconf:  
Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или катало  
га)  
  
(gedit:2902): dconf-WARNING **: 22:39:06.857: failed to commit changes to dconf:  
Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или катало  
га)  
  
(gedit:2902): dconf-WARNING **: 22:39:06.858: failed to commit changes to dconf:  
Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или катало
```



```
Обзор gedit Пн, 30 сентября 22:45 en
```

```
Открыть simpleid2.c Сохранить x  
1 #include <sys/types.h>  
2 #include <unistd.h>  
3 #include <stdio.h>  
4  
5 int  
6 main ()  
7 {  
8     uid_t real_uid = getuid ();  
9     uid_t e_uid = geteuid ();  
10  
11     gid_t real_gid = getgid ();  
12     gid_t e_gid = getegid ();  
13  
14     printf("e_uid=%d, e_gid=%d\n", e_uid, e_gid);  
15     printf("real_uid=%d, real_gid=%d\n", real_uid, real_gid);  
16  
17     return 0;  
18 }
```

Загрузка файла «/home/guest/simpleid2.c»... С Ширина табуляции: 8 Стр 1, Стлб 1 ВСТ

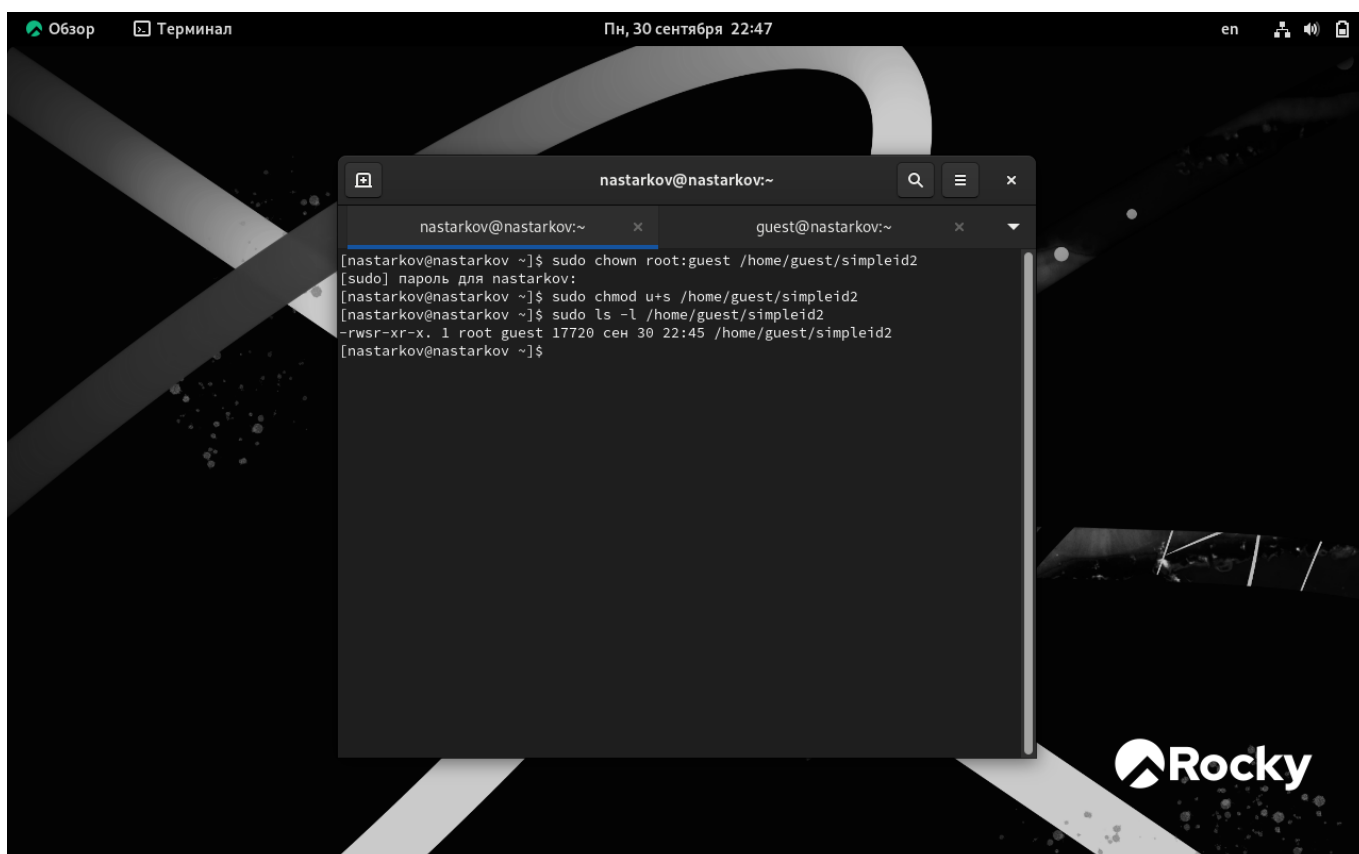


The image shows a terminal window titled "guest@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The active tab is "guest@nastarkov:~". The terminal output is as follows:

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

The background of the terminal window shows a desktop environment with a "Rocky" logo in the bottom right corner.

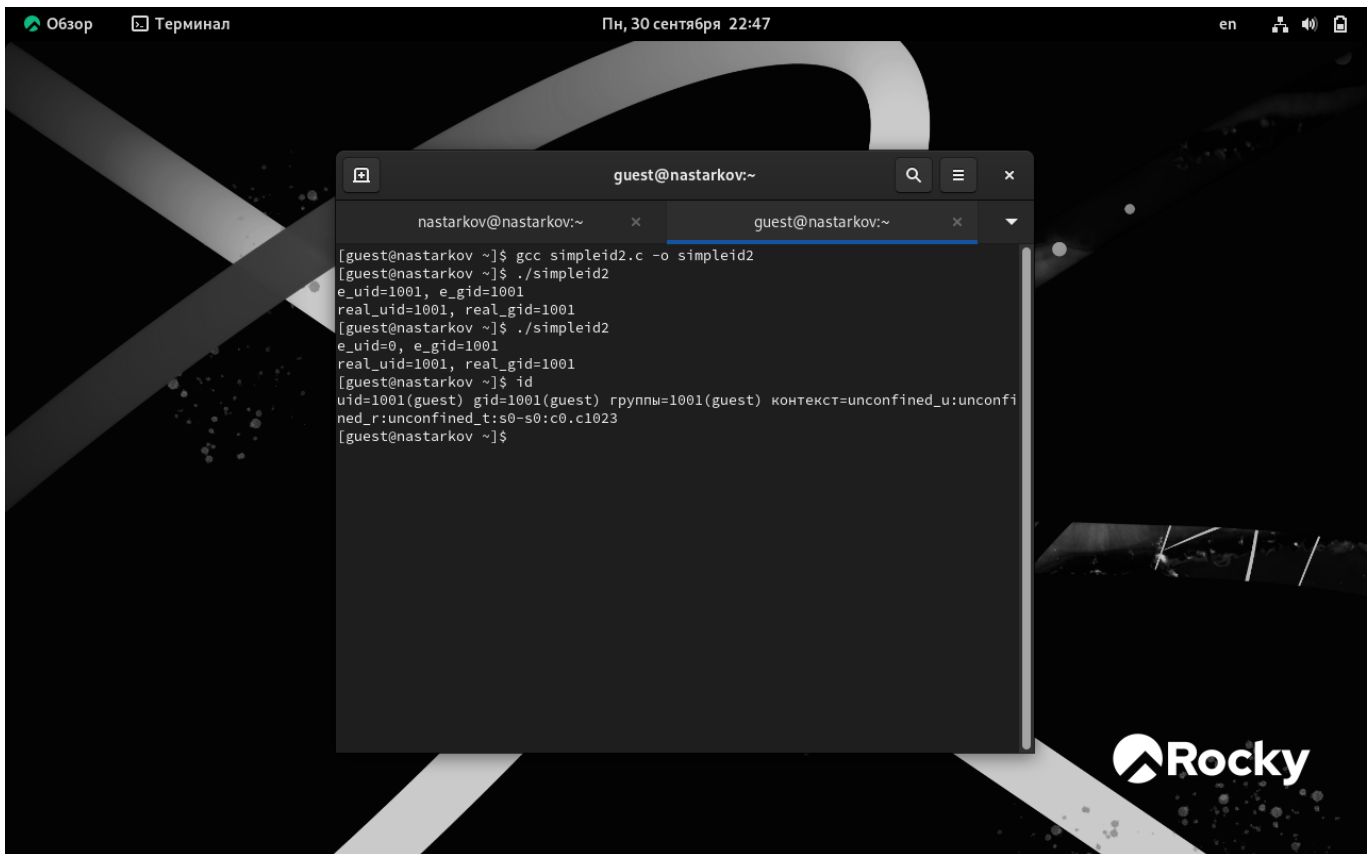
7. От имени суперпользователя выполнили команды "sudo chown root:guest/home/guest/simpleid2" и "sudo chmod u+s /home/guest/simpleid2", затем выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой "sudo ls -l /home/guest/simpleid2". Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит.



The image shows a terminal window titled "nastarkov@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The active tab is "nastarkov@nastarkov:~". The terminal output is as follows:

```
[nastarkov@nastarkov ~]$ sudo chown root:guest /home/guest/simpleid2
[sudo] пароль для nastarkov:
[nastarkov@nastarkov ~]$ sudo chmod u+s /home/guest/simpleid2
[nastarkov@nastarkov ~]$ sudo ls -l /home/guest/simpleid2
-rwsr-xr-x. 1 root guest 17720 сен 30 22:45 /home/guest/simpleid2
[nastarkov@nastarkov ~]$
```

The background of the terminal window shows a desktop environment with a "Rocky" logo in the bottom right corner.

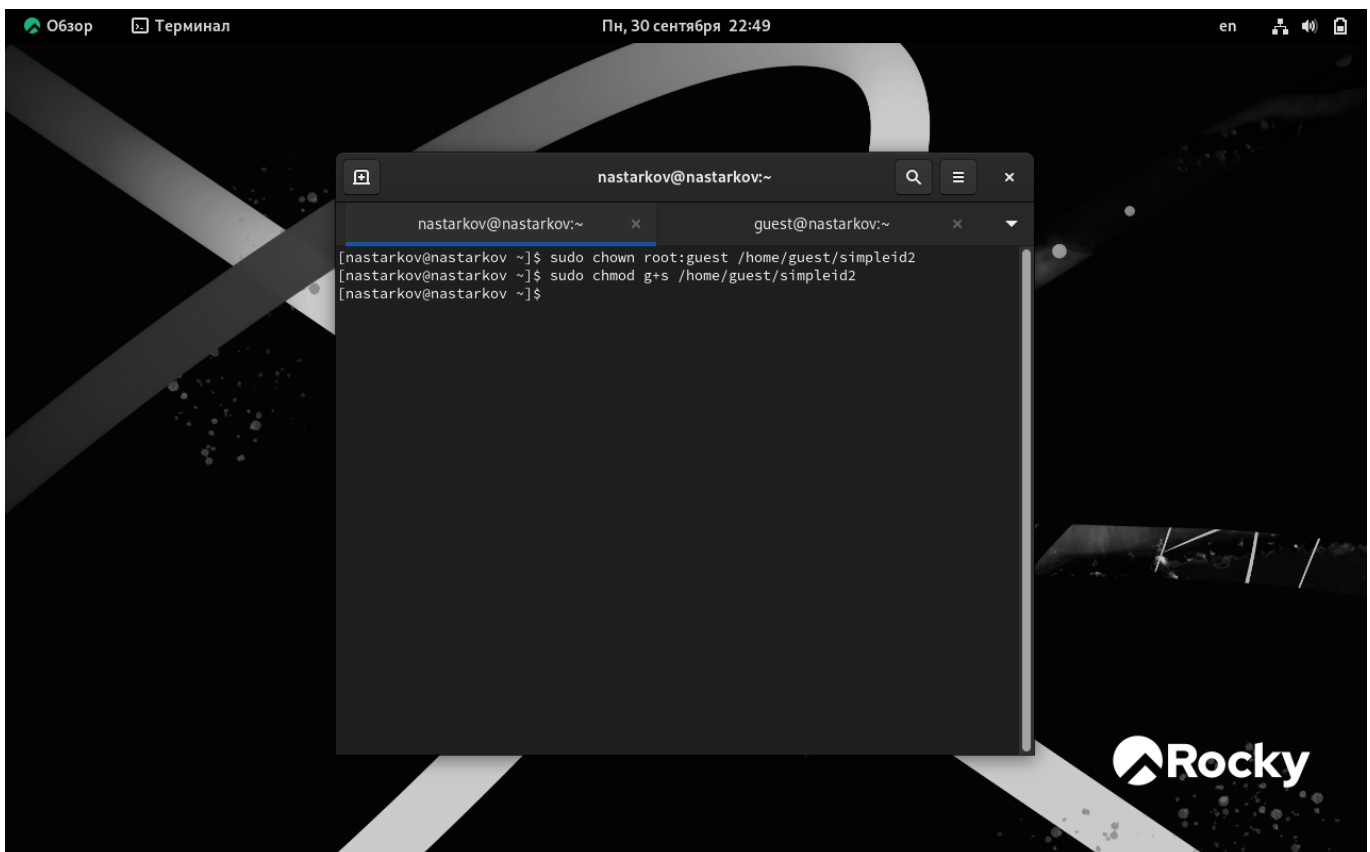


The screenshot shows a terminal window titled "guest@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The "guest" tab is active. The terminal output is as follows:

```
[guest@nastarkov ~]$ gcc simpleid2.c -o simpleid2
[guest@nastarkov ~]$ ./simpleid2
e_uid=1001, e_gid=1001
real_uid=1001, real_gid=1001
[guest@nastarkov ~]$ ./simpleid2
e_uid=0, e_gid=1001
real_uid=1001, real_gid=1001
[guest@nastarkov ~]$ id
uid=1001(guest) gid=1001(guest) грппны=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@nastarkov ~]$
```

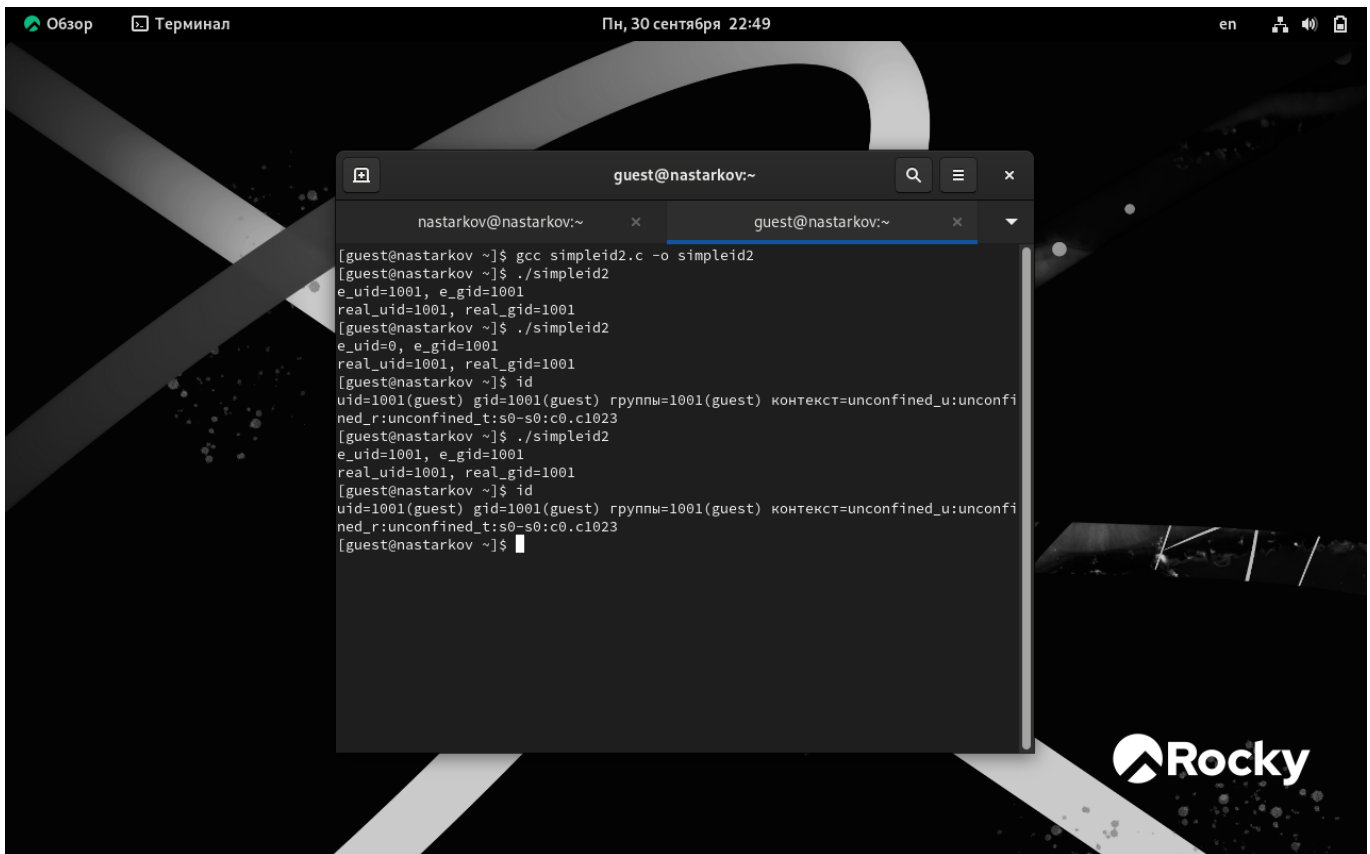
Запустил программы simpleid2 и id. Теперь появились различия в uid

8. Прodelал тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом.



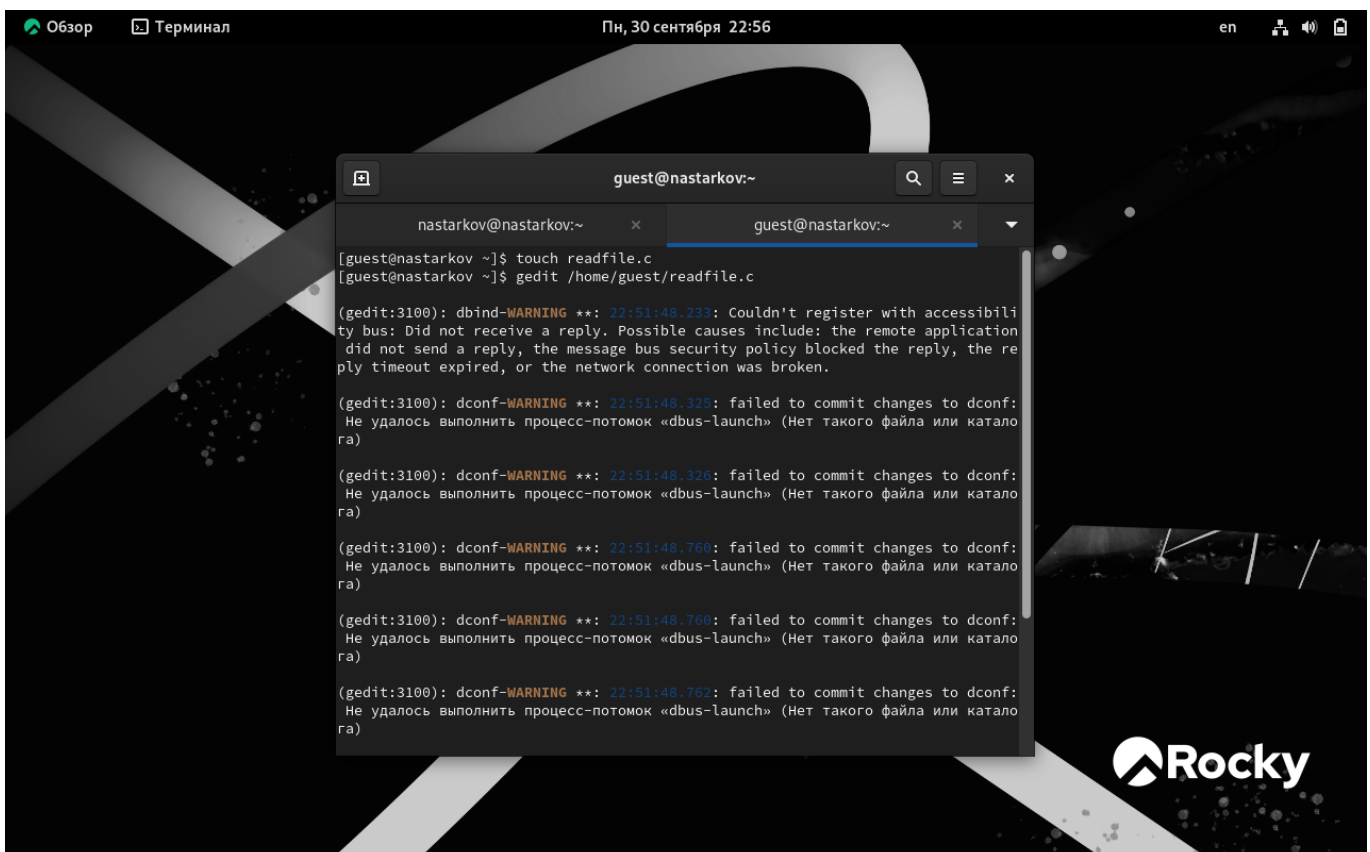
The screenshot shows a terminal window titled "nastarkov@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The "nastarkov" tab is active. The terminal output is as follows:

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

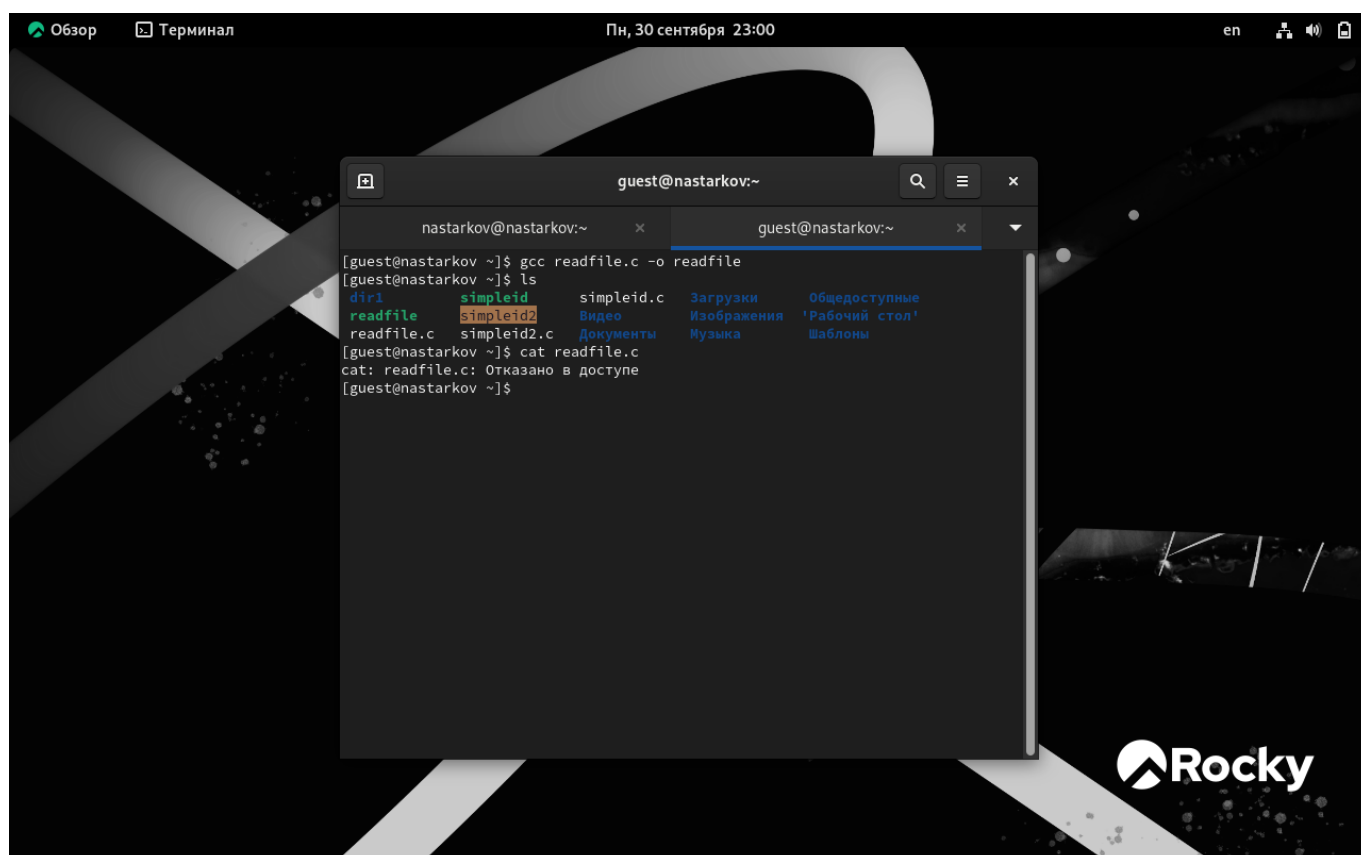
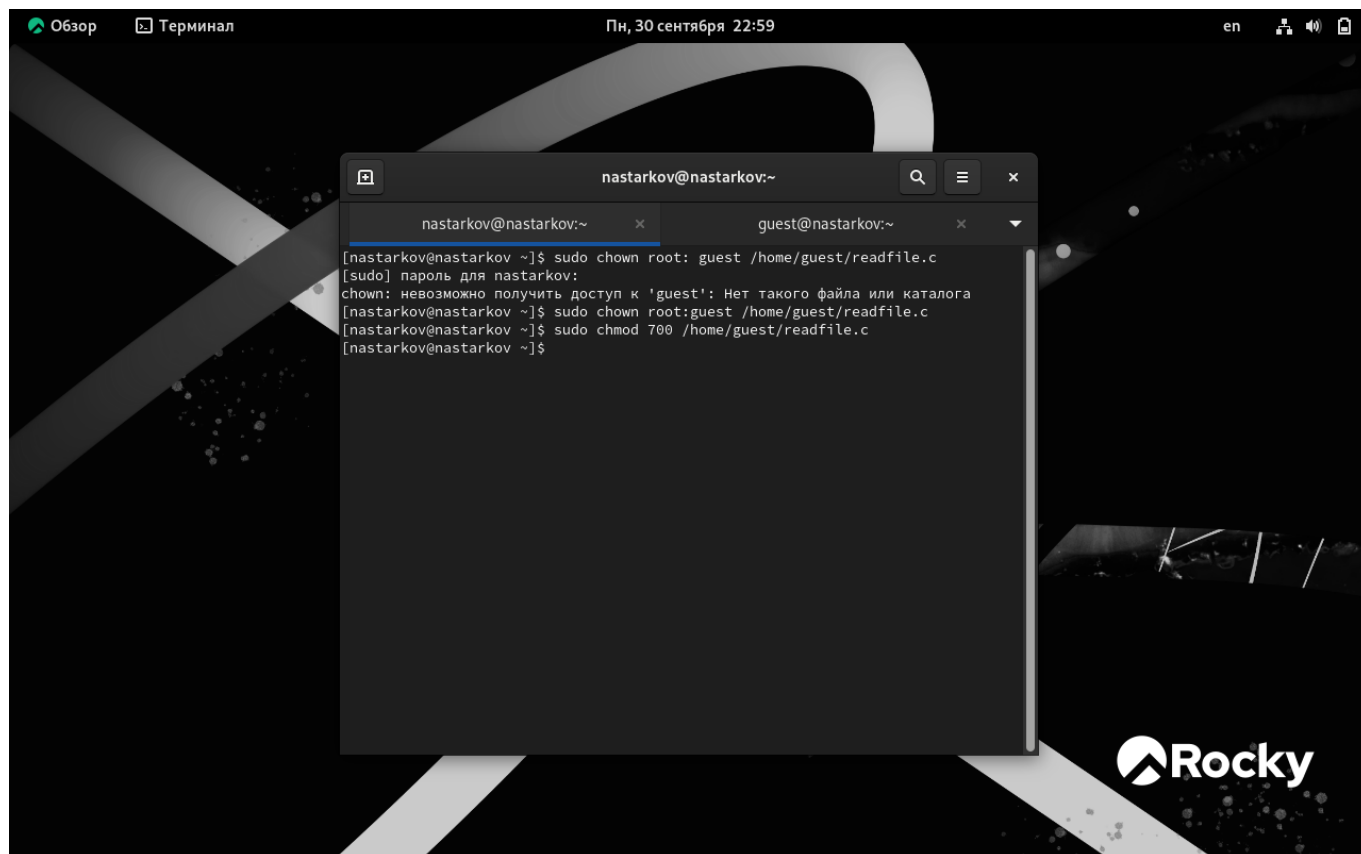


```
guest@nastarkov:~  
nastarkov@nastarkov:~  
[guest@nastarkov ~]$ gcc simpleid2.c -o simpleid2  
[guest@nastarkov ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@nastarkov ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@nastarkov ~]$ id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

9. Создаем новый файл readfile. Скомпилировали созданную программу командой "gcc readfile.c -o readfile". Сменили владельца у файла readfile.c командой "sudo chown root:guest/home/guest/readfile.c" и поменяли права так, чтобы только суперпользователь мог прочитать его, а guest не мог, с помощью команды "sudo chmod 700/home/guest/readfile.c". Теперь убедились, что пользователь guest не может прочитать файл readfile.c командой "cat readfile.c", получив отказ в доступе.

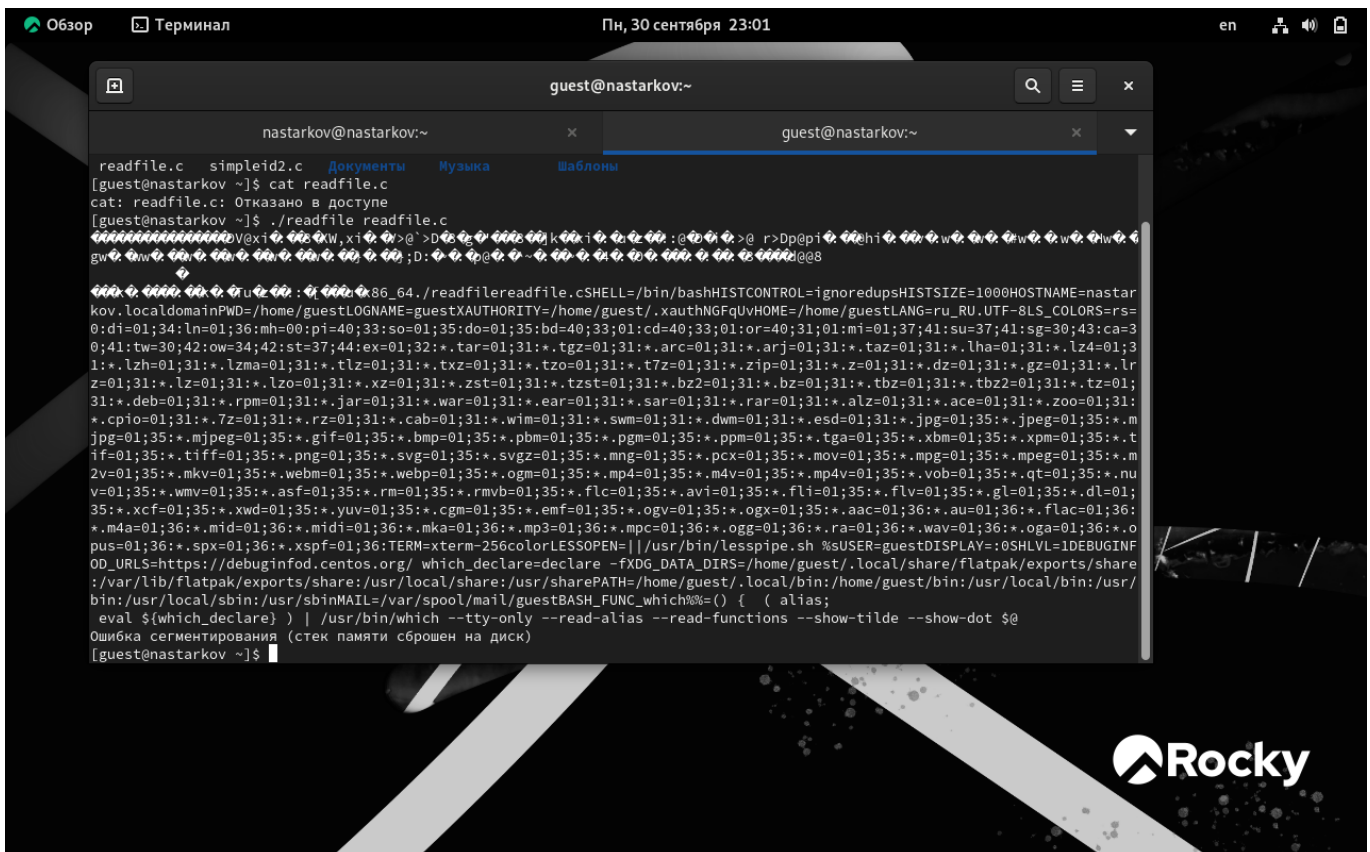
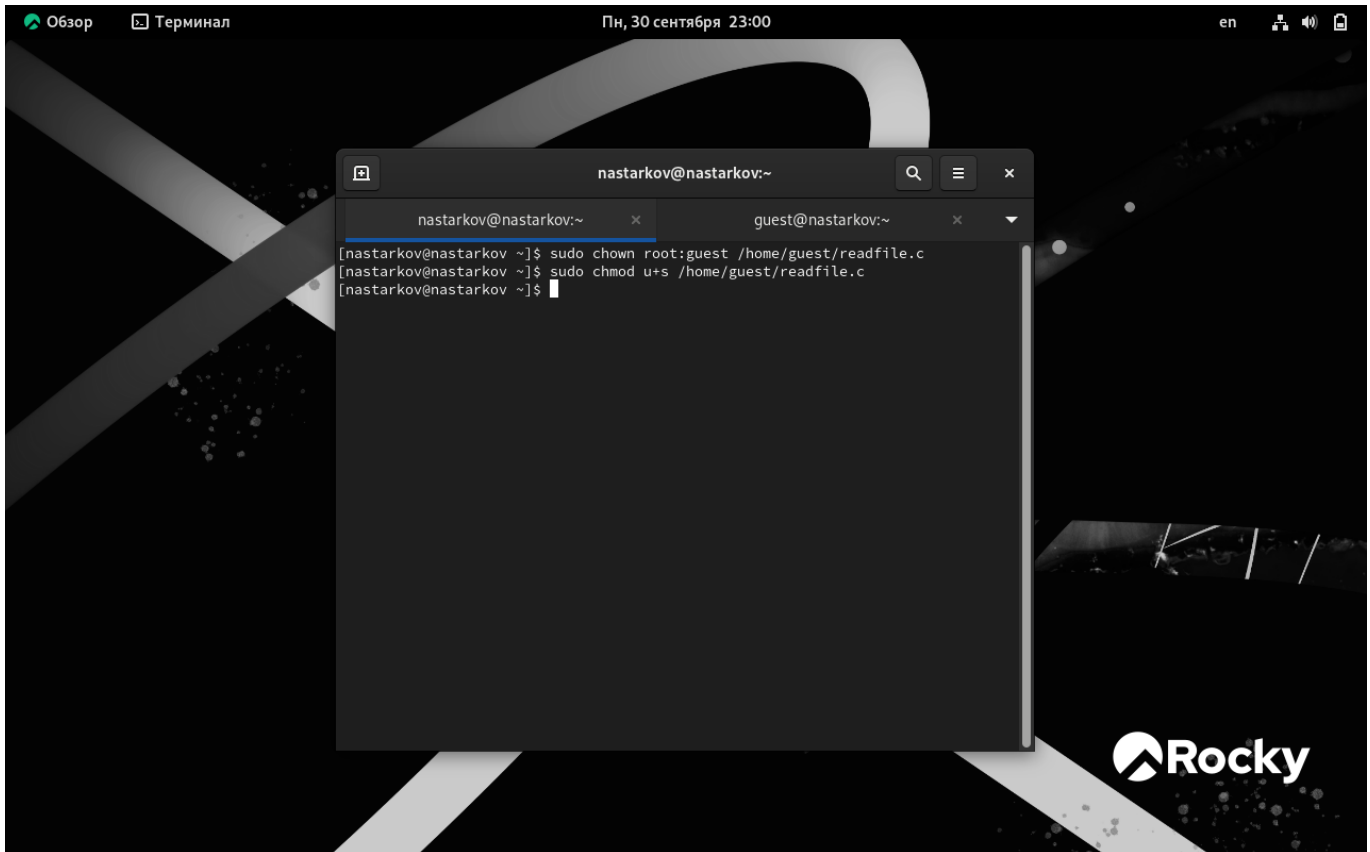


```
guest@nastarkov:~  
nastarkov@nastarkov:~  
[guest@nastarkov ~]$ touch readfile.c  
[guest@nastarkov ~]$ gedit /home/guest/readfile.c  
(gedit:3100): dbind-WARNING **: 22:51:48.233: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.  
(gedit:3100): dconf-WARNING **: 22:51:48.325: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)  
(gedit:3100): dconf-WARNING **: 22:51:48.326: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)  
(gedit:3100): dconf-WARNING **: 22:51:48.760: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)  
(gedit:3100): dconf-WARNING **: 22:51:48.760: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)  
(gedit:3100): dconf-WARNING **: 22:51:48.762: failed to commit changes to dconf: Не удалось выполнить процесс-потомок «dbus-launch» (Нет такого файла или каталога)
```

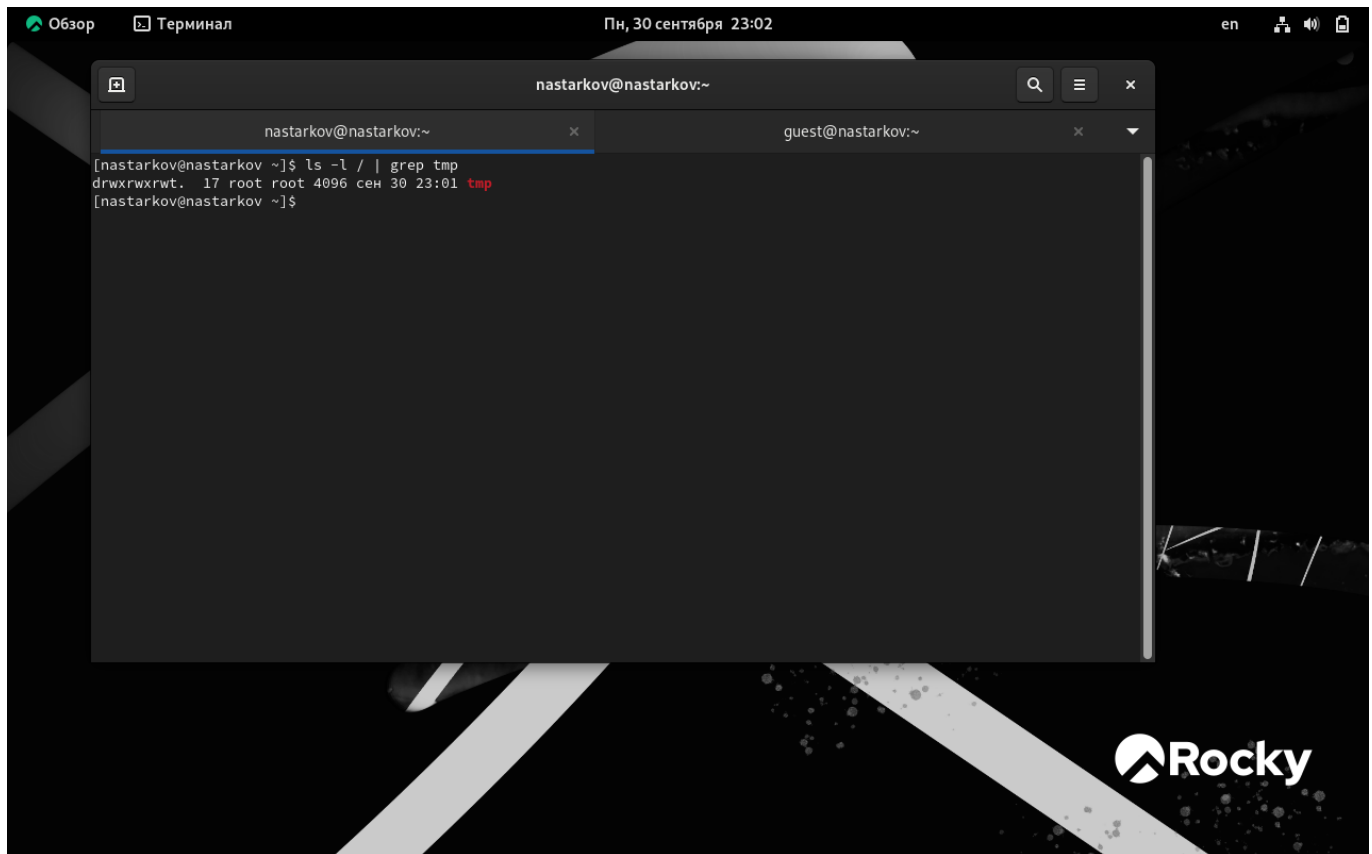


10. Поменяли владельца у программы readfile и установила SetUID. Проверили, может ли программа readfile прочитать файл readfile.c командой `./readfile readfile.c`. Прочитать удалось. Аналогично проверили, можно ли прочитать файл `/etc/shadow`. Прочитать удалось





11. Командой "ls -l | grep tmp" убежились, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test командой "echo test" > /tmp/file01.txt". Просмотрели атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей "все остальные" командами "ls -l /tmp/file01.txt" и "chmod o+rw /tmp/file01.txt"

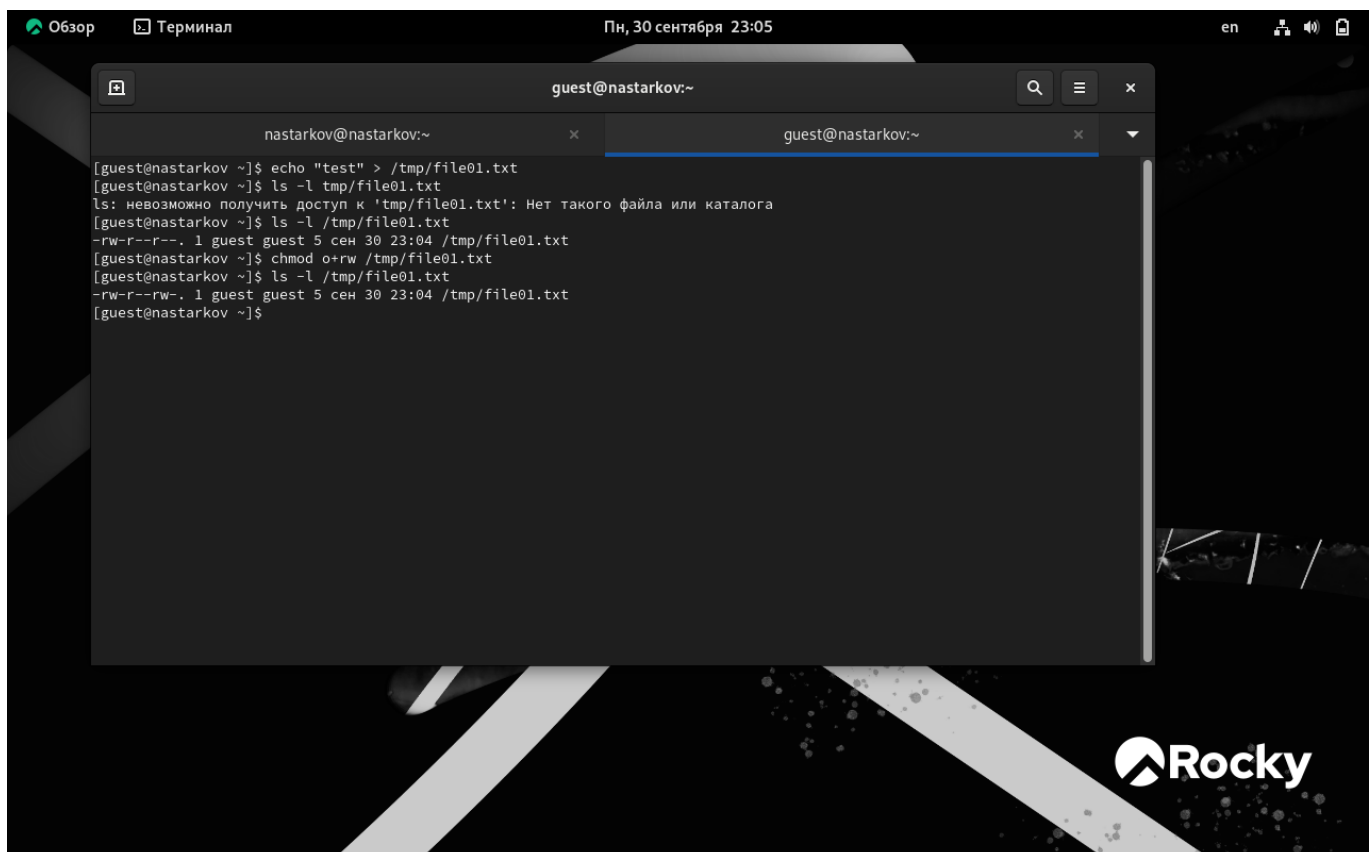


Обзор Терминал Пн, 30 сентября 23:02 en

nastarkov@nastarkov:~

```
nastarkov@nastarkov:~$ ls -l / | grep tmp
drwxrwxrwt. 17 root root 4096 сен 30 23:01 tmp
nastarkov@nastarkov:~$
```

Rocky



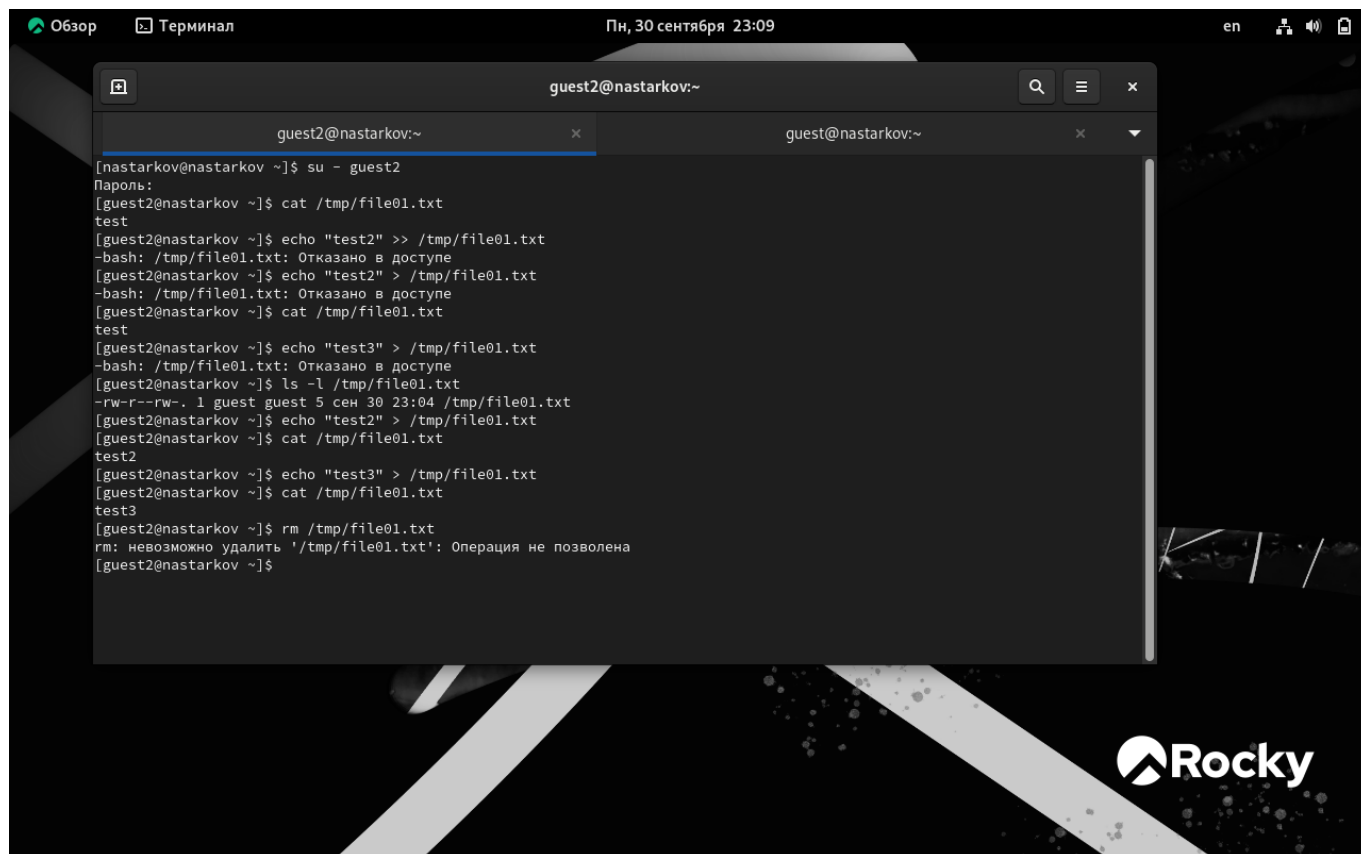
Обзор Терминал Пн, 30 сентября 23:05 en

guest@nastarkov:~

```
guest@nastarkov:~$ echo "test" > /tmp/file01.txt
guest@nastarkov:~$ ls -l tmp/file01.txt
ls: невозможно получить доступ к 'tmp/file01.txt': Нет такого файла или каталога
guest@nastarkov:~$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
guest@nastarkov:~$ chmod o+rw /tmp/file01.txt
guest@nastarkov:~$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
guest@nastarkov:~$
```

Rocky

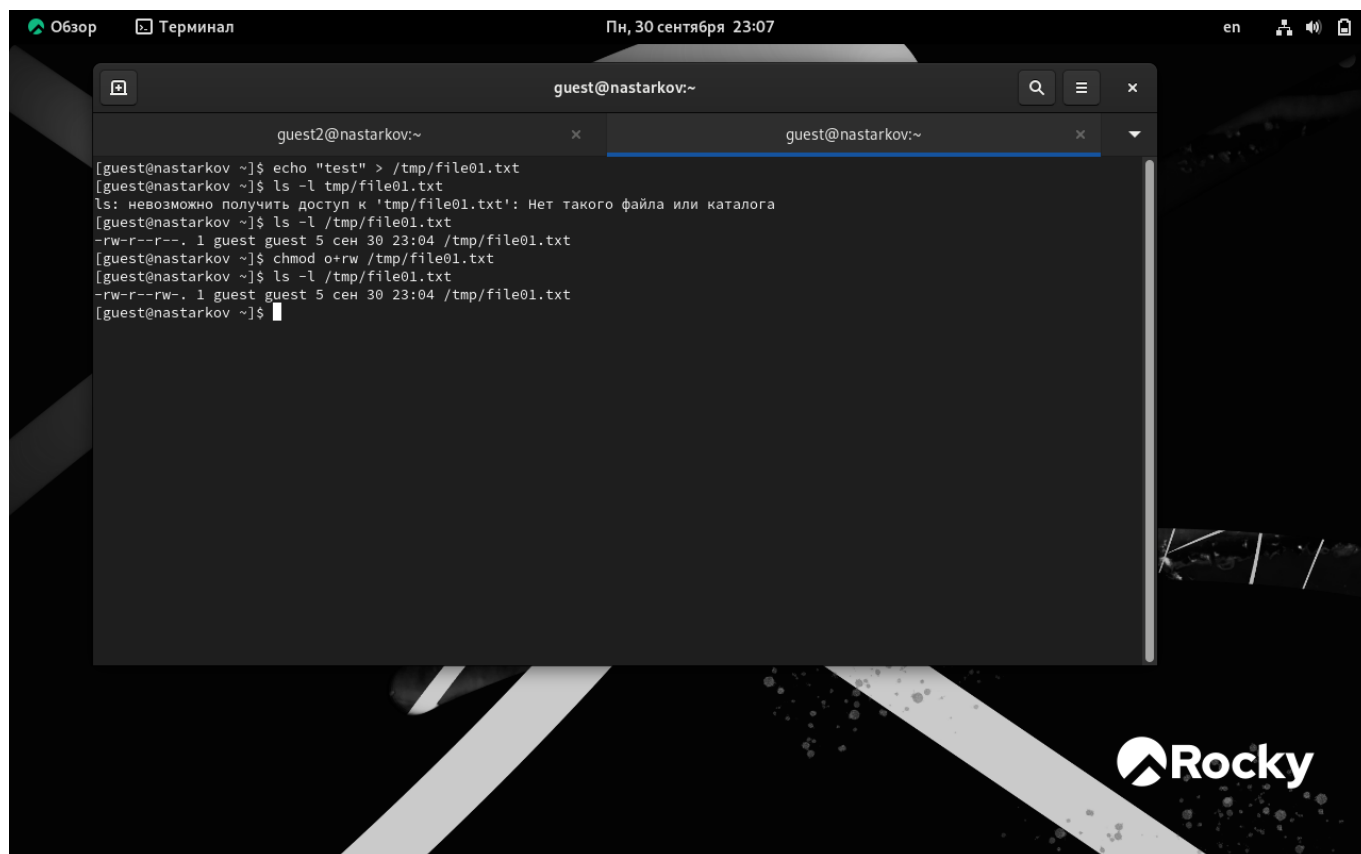

12. От имени пользователя guest2 попробовали прочитать файл командой "cat/tmp/file01.txt" - это удалось. Далее попытались дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой "chmod g+rw /tmp/file01.txt". От имени пользователя guest2 попробовала удалить файл - это не удастся ни в каком из случаев, возникает ошибка



```
Обзор Терминал Пн, 30 сентября 23:09 en
```

```
guest2@nastarkov:~
```

```
[nastarkov@nastarkov ~]$ su - guest2
Пароль:
[guest2@nastarkov ~]$ cat /tmp/file01.txt
test
[guest2@nastarkov ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@nastarkov ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@nastarkov ~]$ cat /tmp/file01.txt
test
[guest2@nastarkov ~]$ echo "test3" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@nastarkov ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
[guest2@nastarkov ~]$ echo "test2" > /tmp/file01.txt
[guest2@nastarkov ~]$ cat /tmp/file01.txt
test2
[guest2@nastarkov ~]$ echo "test3" > /tmp/file01.txt
[guest2@nastarkov ~]$ cat /tmp/file01.txt
test3
[guest2@nastarkov ~]$ rm /tmp/file01.txt
rm: невозможно удалить '/tmp/file01.txt': Операция не позволена
[guest2@nastarkov ~]$
```




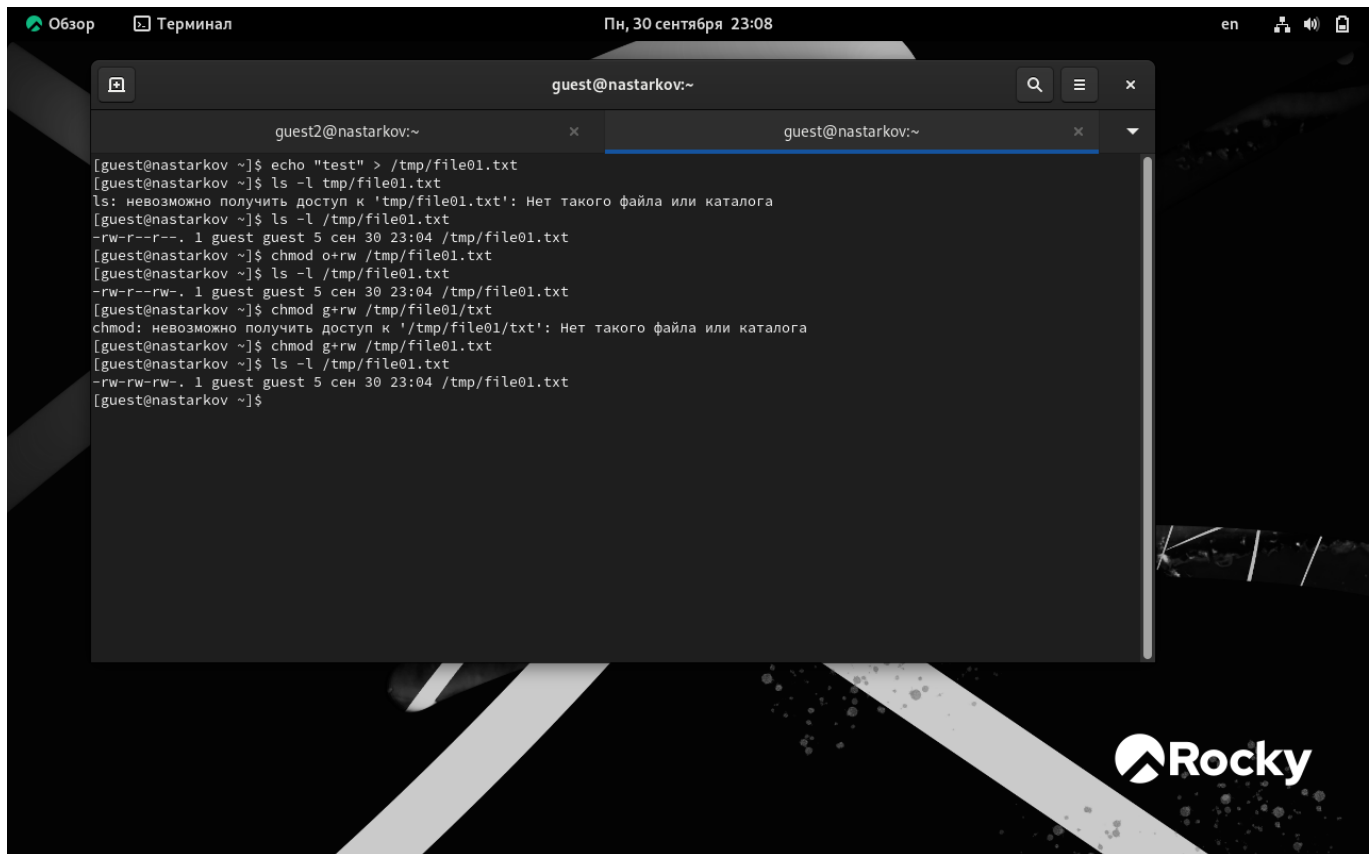
```
Обзор Терминал Пн, 30 сентября 23:07 en
```

```
guest@nastarkov:~
```

```
guest2@nastarkov:~
```

```
[guest@nastarkov ~]$ echo "test" > /tmp/file01.txt
[guest@nastarkov ~]$ ls -l tmp/file01.txt
ls: невозможно получить доступ к 'tmp/file01.txt': Нет такого файла или каталога
[guest@nastarkov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
[guest@nastarkov ~]$ chmod o+rw /tmp/file01.txt
[guest@nastarkov ~]$ ls -l /tmp/file01.txt
-rw-r--rw-. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
[guest@nastarkov ~]$
```

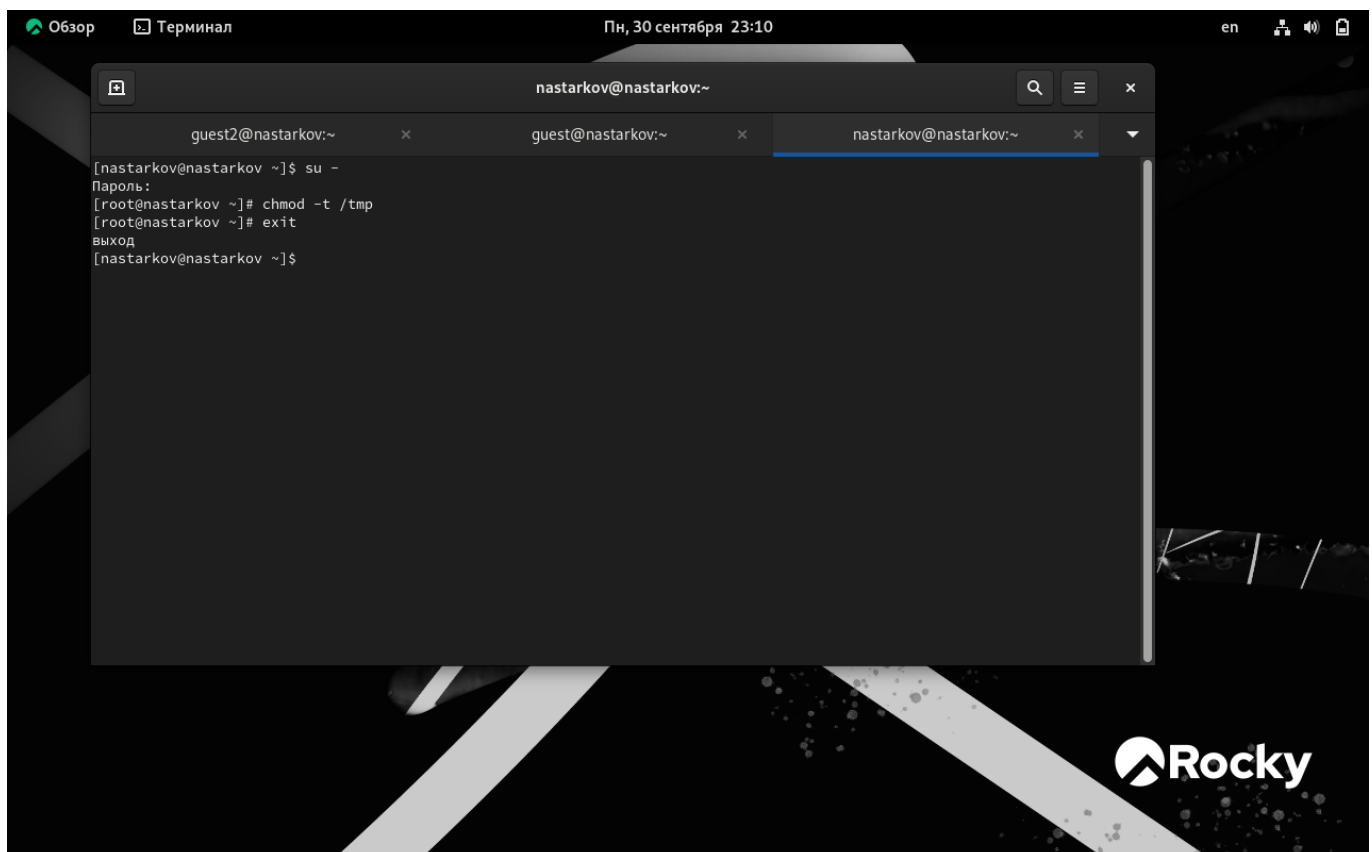




The terminal window shows a series of commands and their outputs. The user 'guest' creates a file 'test' in '/tmp/file01.txt'. They then check permissions, which are 'rw-r--r--'. They attempt to change permissions to 'o+rw' but fail because the directory '/tmp/file01.txt' does not exist. They then create the directory and change permissions to 'g+rw', which succeeds. Finally, they check permissions again, which are 'rw-rw-rw-'. The background of the terminal window features the Rocky Linux logo.

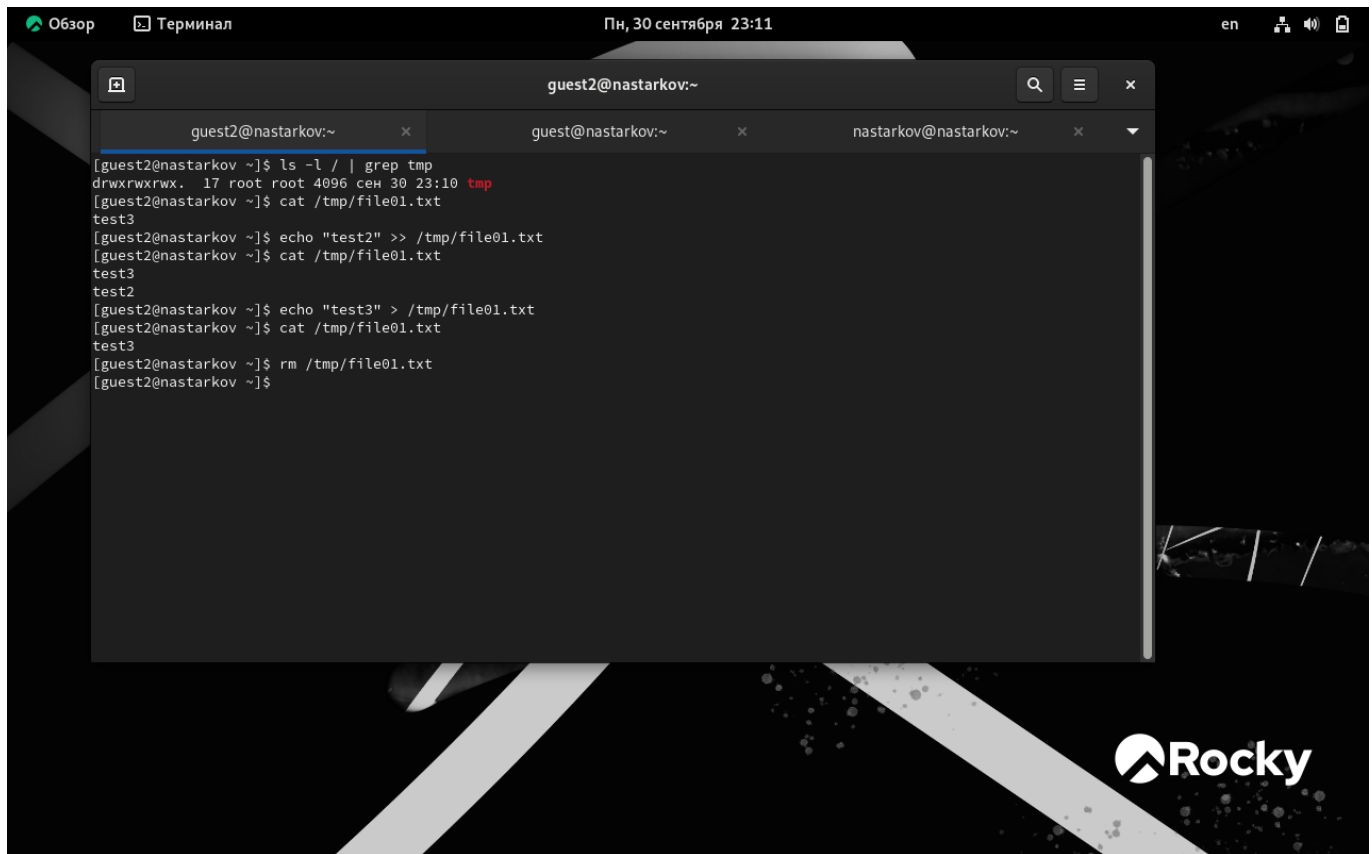
```
guest@nastarkov:~  
[guest@nastarkov ~]$ echo "test" > /tmp/file01.txt  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
ls: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt  
[guest@nastarkov ~]$ chmod o+rw /tmp/file01.txt  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt  
[guest@nastarkov ~]$ chmod g+rw /tmp/file01/txt  
chmod: невозможно получить доступ к '/tmp/file01/txt': Нет такого файла или каталога  
[guest@nastarkov ~]$ chmod g+rw /tmp/file01.txt  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
-rw-rw-rw-. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt  
[guest@nastarkov ~]$
```

13. Повысили права до суперпользователя командой "su -" и выполнили команду, снимающую атрибут t с директории /tmp "chmod -t /tmp". После чего покинули режим суперпользователя командой "exit". Повторили предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем



The terminal window shows the user 'nastarkov' switching to root using 'su -'. They then execute 'chmod -t /tmp' to remove the sticky bit from the /tmp directory. After exiting root mode with 'exit', they are back at the prompt. The background of the terminal window features the Rocky Linux logo.

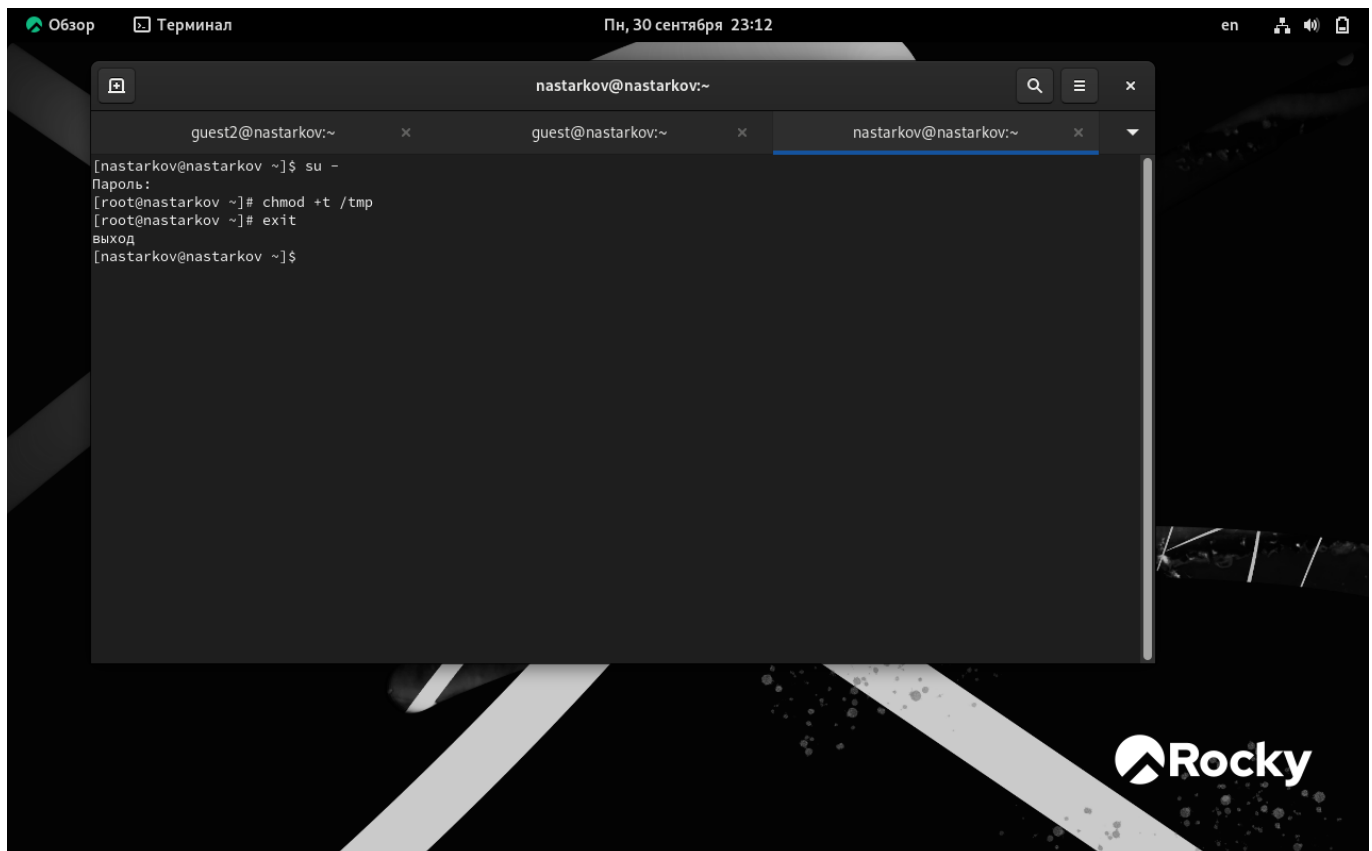
```
nastarkov@nastarkov:~  
[nastarkov@nastarkov ~]$ su -  
Пароль:  
[root@nastarkov ~]# chmod -t /tmp  
[root@nastarkov ~]# exit  
выход  
[nastarkov@nastarkov ~]$
```



The terminal window shows a series of commands executed by the user 'guest2' on the host 'nastarkov'. The commands are: `ls -l / | grep tmp`, `cat /tmp/file01.txt`, `echo "test2" >> /tmp/file01.txt`, `cat /tmp/file01.txt`, `echo "test3" > /tmp/file01.txt`, `cat /tmp/file01.txt`, and `rm /tmp/file01.txt`. The output shows the file permissions and content changes. The terminal is titled 'guest2@nastarkov:~' and the window title bar shows 'Обзор Терминал' and the date 'Пн, 30 сентября 23:11'.

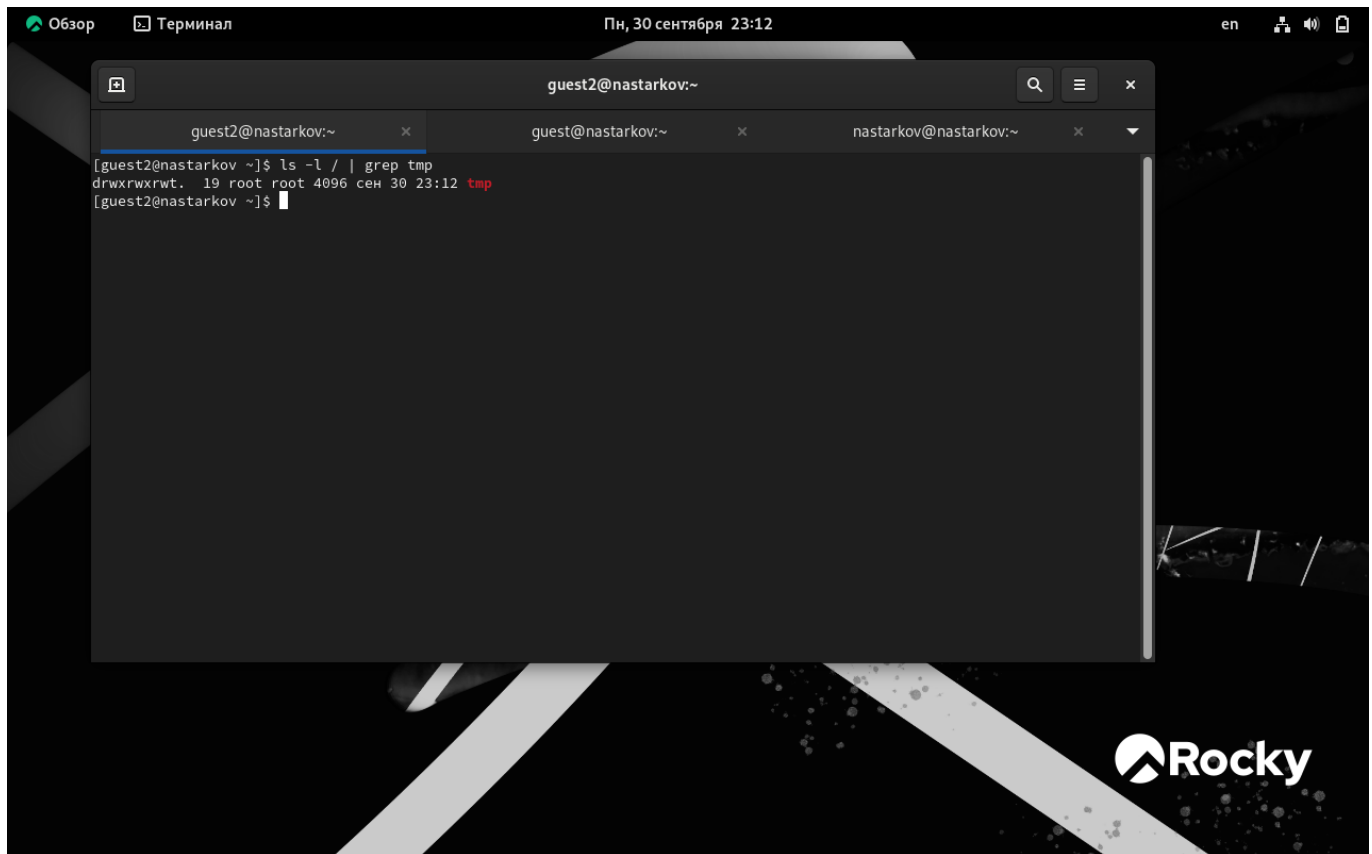
```
guest2@nastarkov:~  
[guest2@nastarkov ~]$ ls -l / | grep tmp  
drwxrwxrwx. 17 root root 4096 сен 30 23:10 tmp  
[guest2@nastarkov ~]$ cat /tmp/file01.txt  
test3  
[guest2@nastarkov ~]$ echo "test2" >> /tmp/file01.txt  
[guest2@nastarkov ~]$ cat /tmp/file01.txt  
test3  
test2  
[guest2@nastarkov ~]$ echo "test3" > /tmp/file01.txt  
[guest2@nastarkov ~]$ cat /tmp/file01.txt  
test3  
[guest2@nastarkov ~]$ rm /tmp/file01.txt  
[guest2@nastarkov ~]$
```

#### 14. Вернули атрибут t+



The terminal window shows the user 'nastarkov' switching to root using `su -`. The root user then executes `chmod +t /tmp` and `exit` to return to the guest user. The terminal is titled 'nastarkov@nastarkov:~' and the window title bar shows 'Обзор Терминал' and the date 'Пн, 30 сентября 23:12'.

```
nastarkov@nastarkov:~  
[nastarkov@nastarkov ~]$ su -  
Пароль:  
[root@nastarkov ~]# chmod +t /tmp  
[root@nastarkov ~]# exit  
выход  
[nastarkov@nastarkov ~]$
```



```
Обзор Терминал Пн, 30 сентября 23:12 en
```

```
guest2@nastarkov:~
```

```
guest2@nastarkov:~]$ ls -l / | grep tmp
```

```
drwxrwxrwt. 19 root root 4096 сен 30 23:12 tmp
```

```
guest2@nastarkov:~]$
```

## Вывод

В ходе выполнения лабораторной работы №7 я развил навыки применения режима однократного гаммирования.