

# Отчет к лабораторной работе №5

## Common information

discipline: Основы информационной безопасности

group: НПМбд-02-21

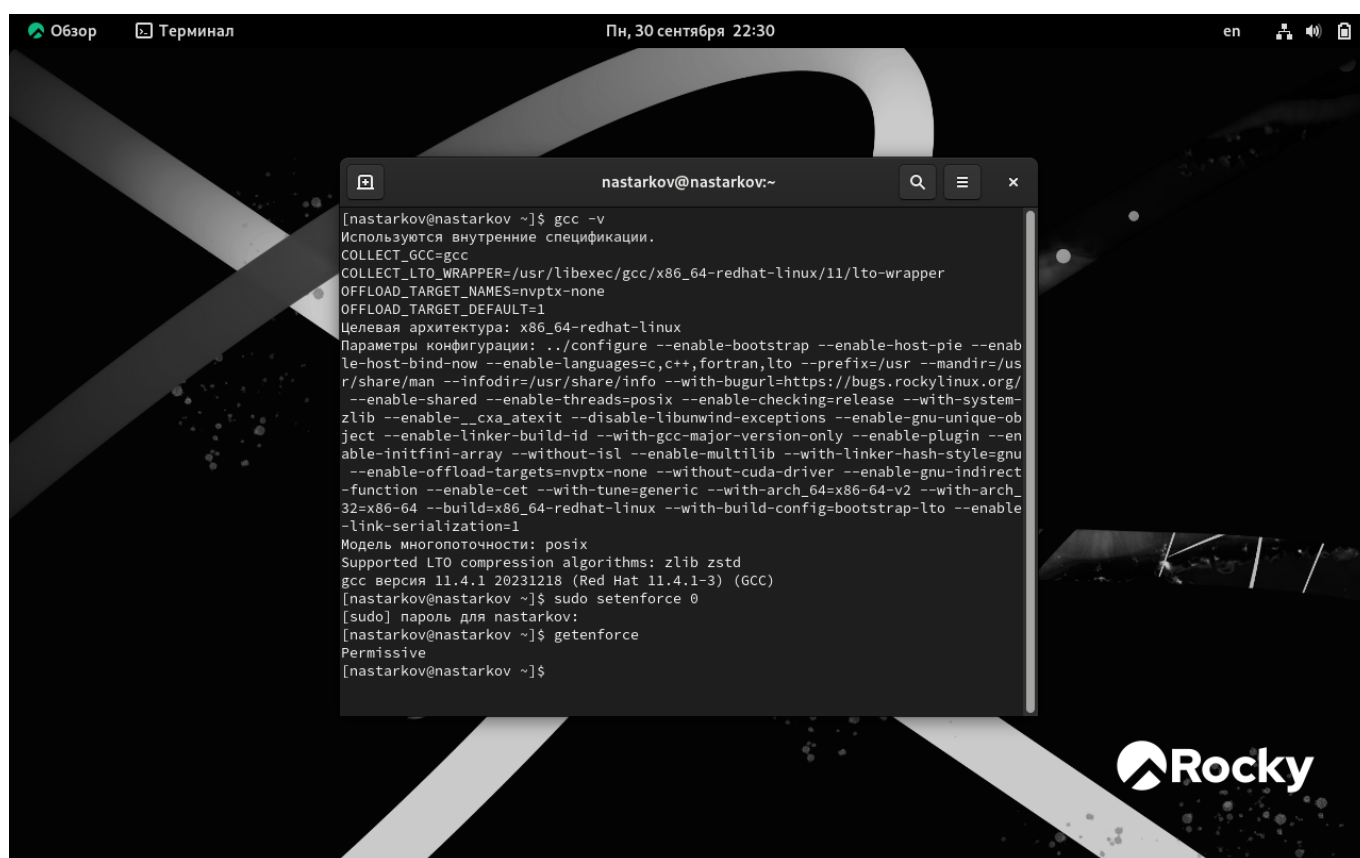
author: Старков Н.А.

## 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.

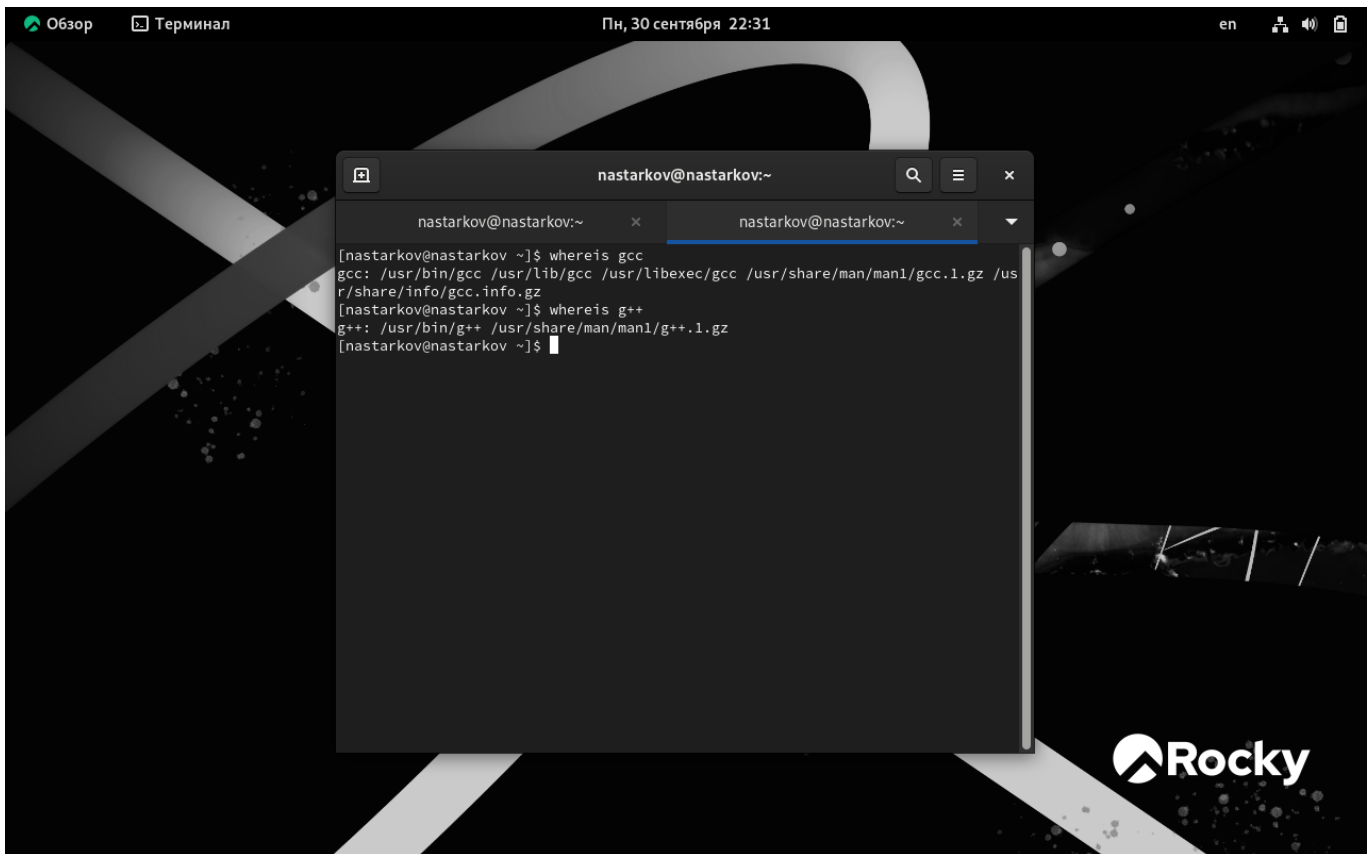
## Выполнение работы

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"

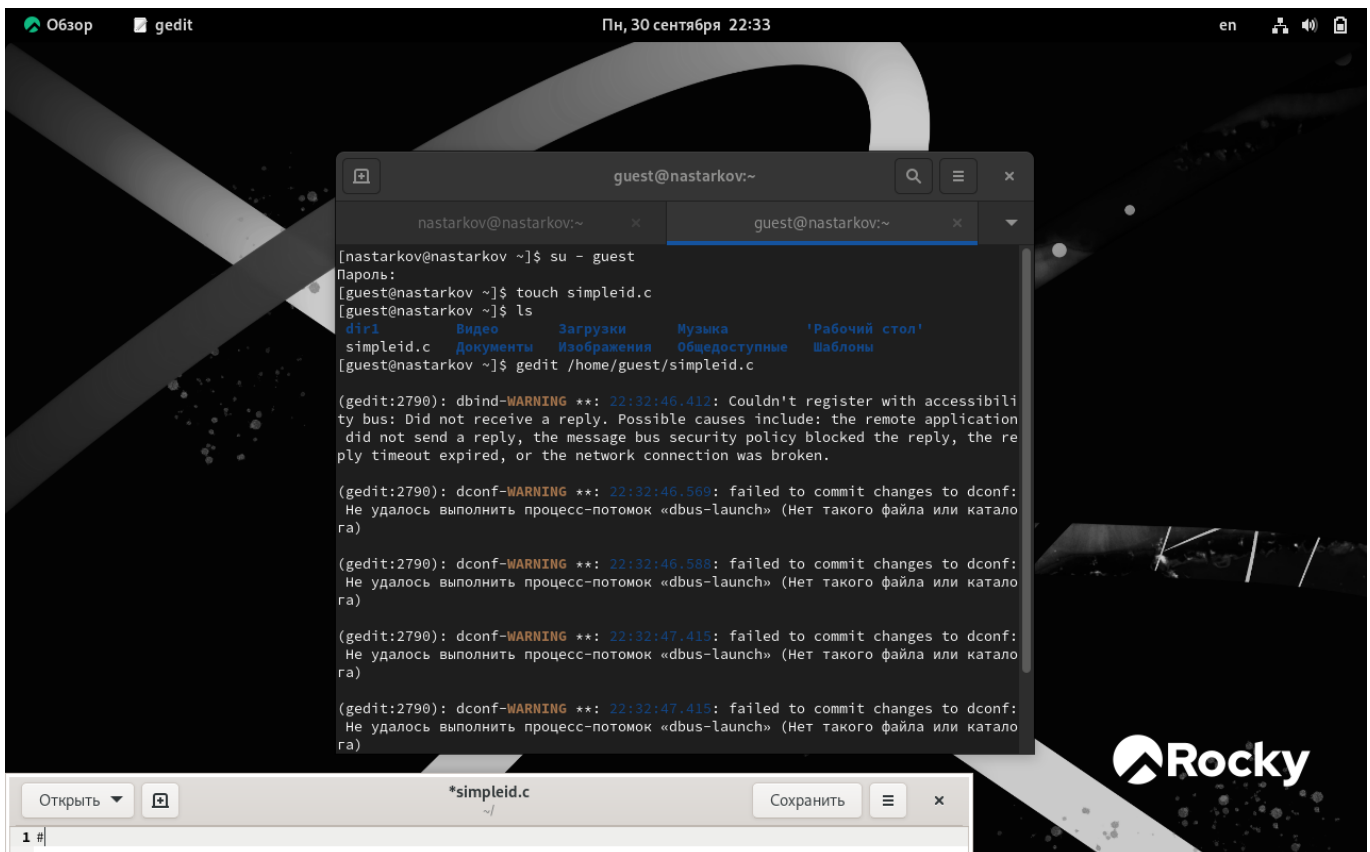


```
[nastarkov@nastarkov ~]$ gcc -v
Используются внутренние спецификации.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/libexec/gcc/x86_64-redhat-linux/11/lto-wrapper
OFFLOAD_TARGET_NAMES=nvptx-none
OFFLOAD_TARGET_DEFAULT=1
Целевая архитектура: x86_64-redhat-linux
Параметры конфигурации: ../configure --enable-bootstrap --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 ~]$
```

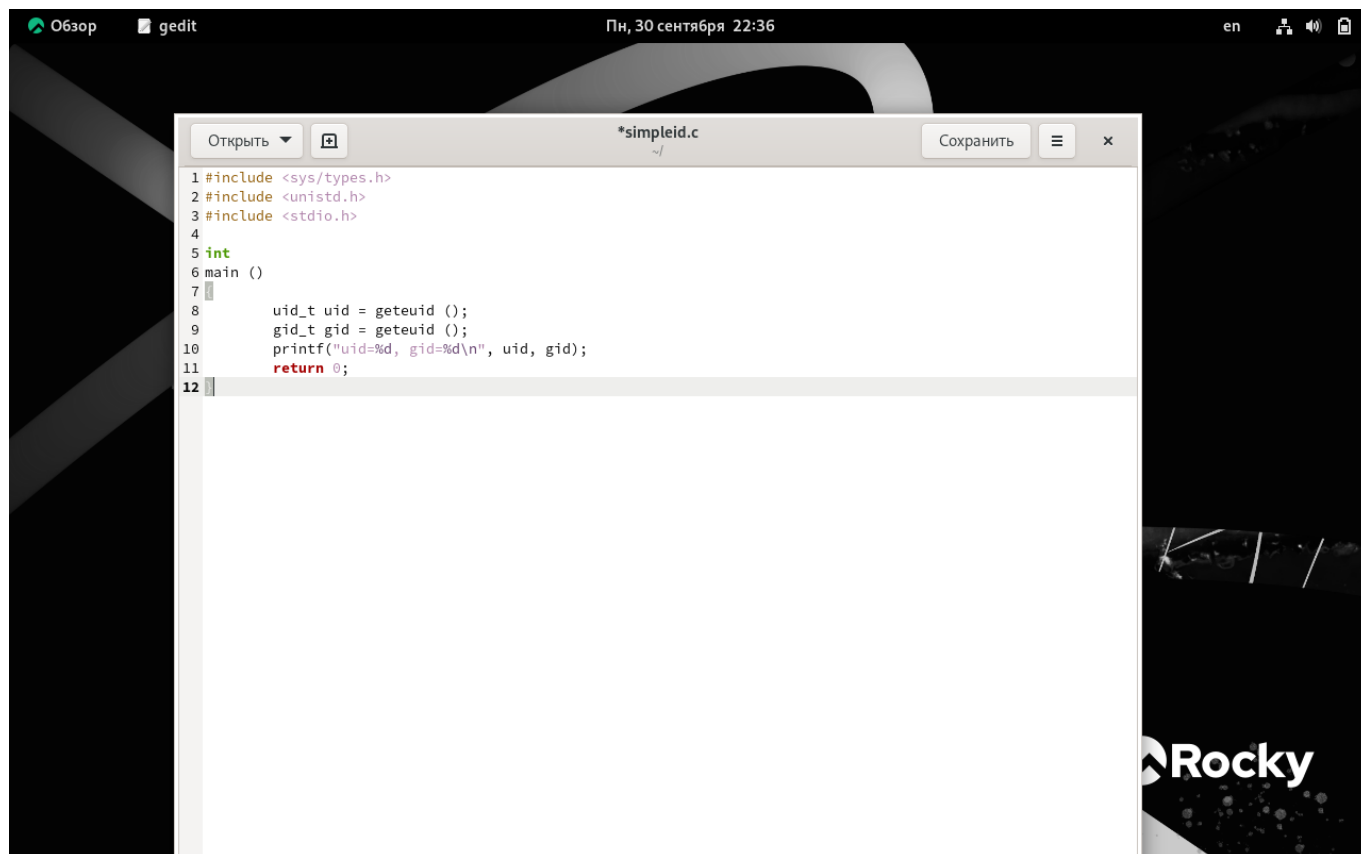
2. Проверили успешное выполнение команд "whereis gcc" и "whereis g++"



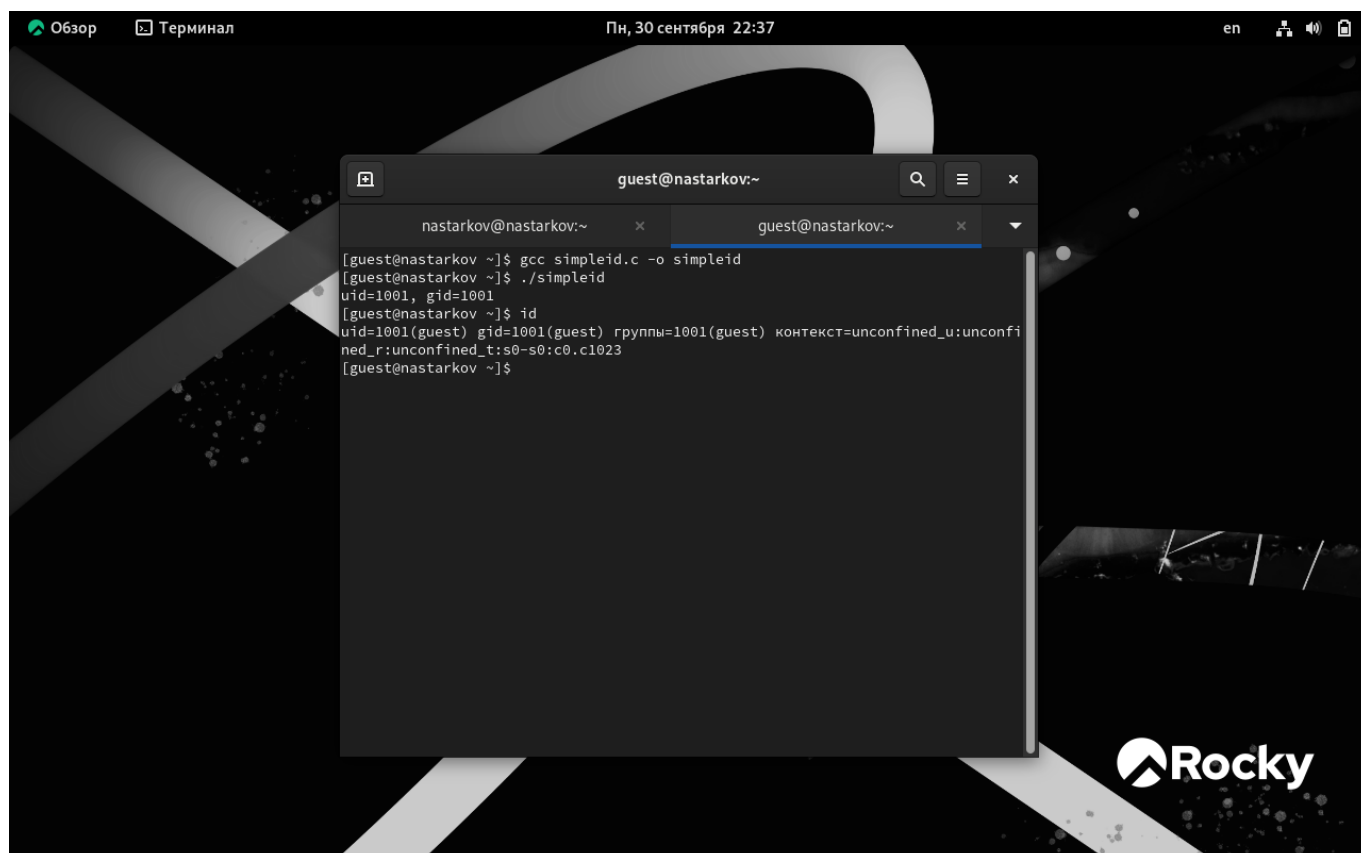
3. Вошли в систему от имени пользователя guest командой "su - guest". Создали программу simpleid.c командой "touch simpleid.c" и открыла её в редакторе командой "gedit /home/guest/simpleid.c"



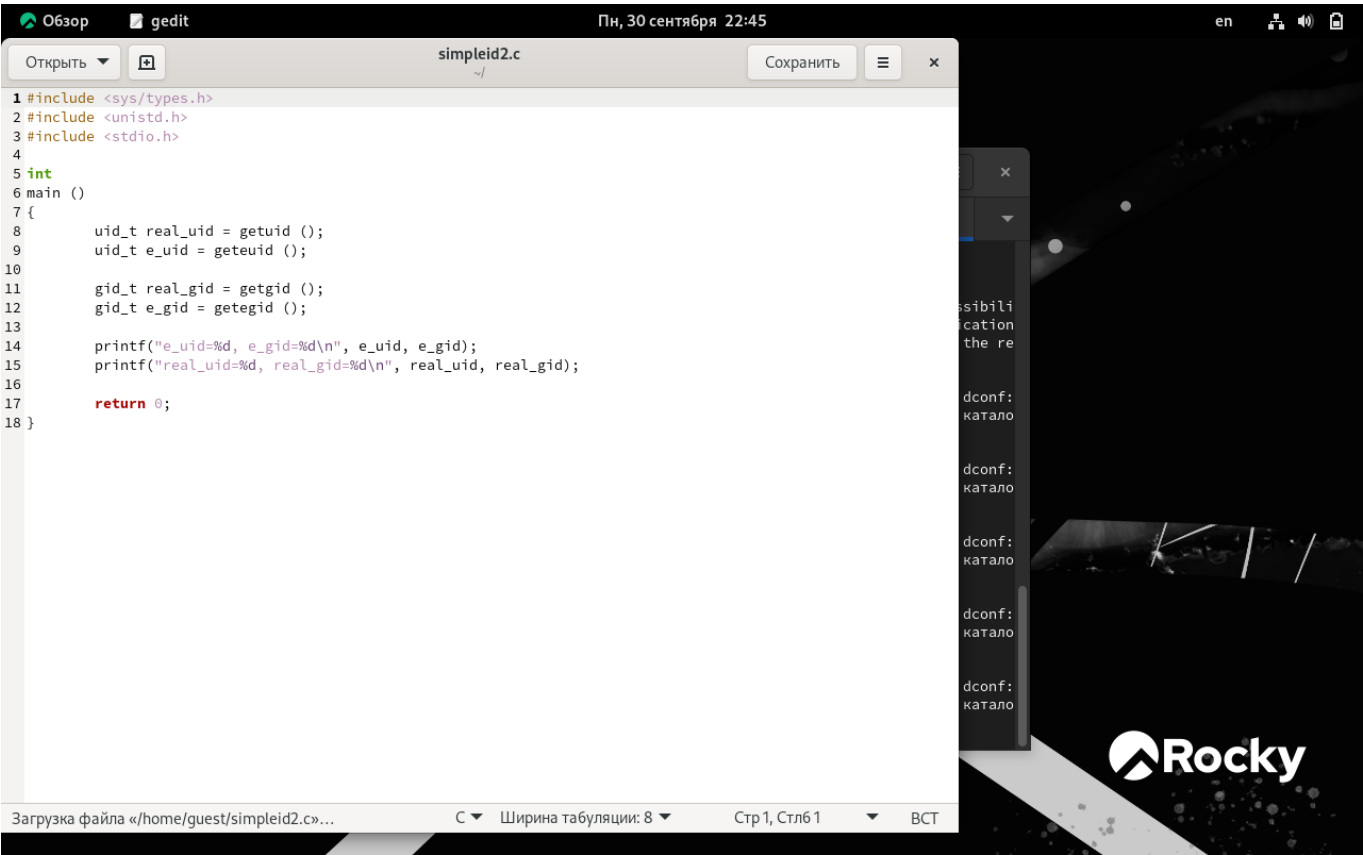
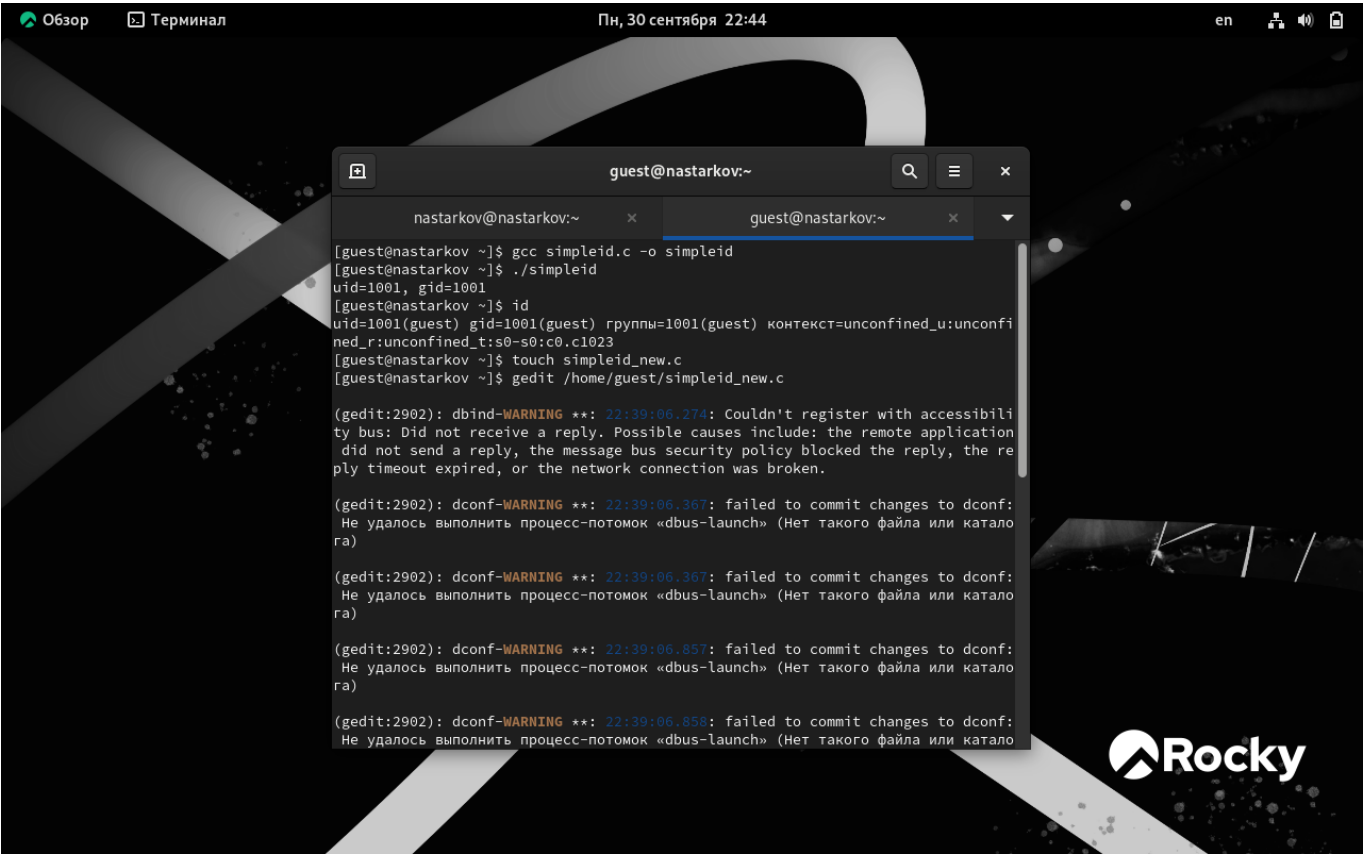
4. Написали код в созданном файле

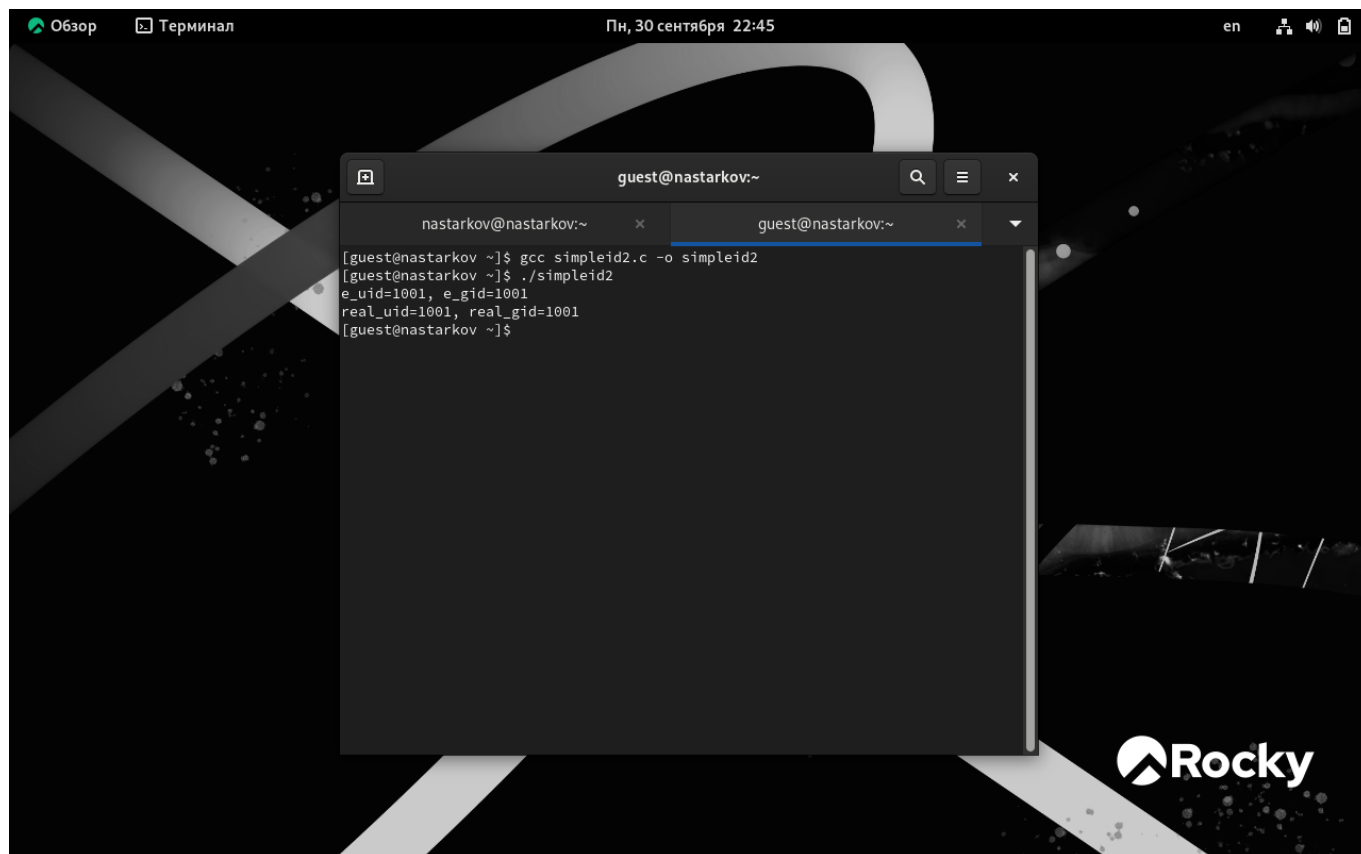


5. Скомпилировали программу и запустили ее



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



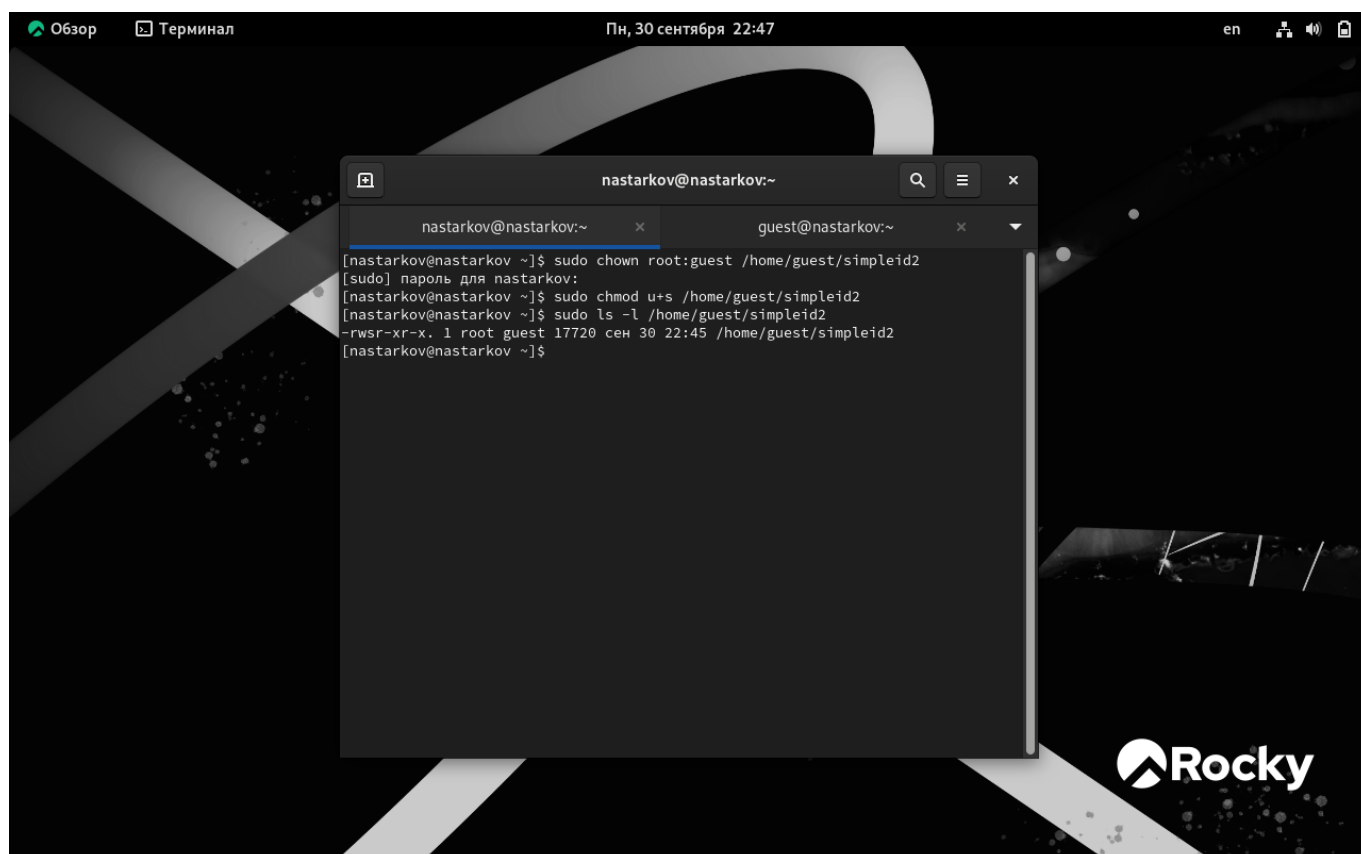


```
Обзор Терминал Пн, 30 сентября 22:45 en
```

```
guest@nastarkov:~  
nastarkov@nastarkov:~ x guest@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 ~]$
```

Rocky

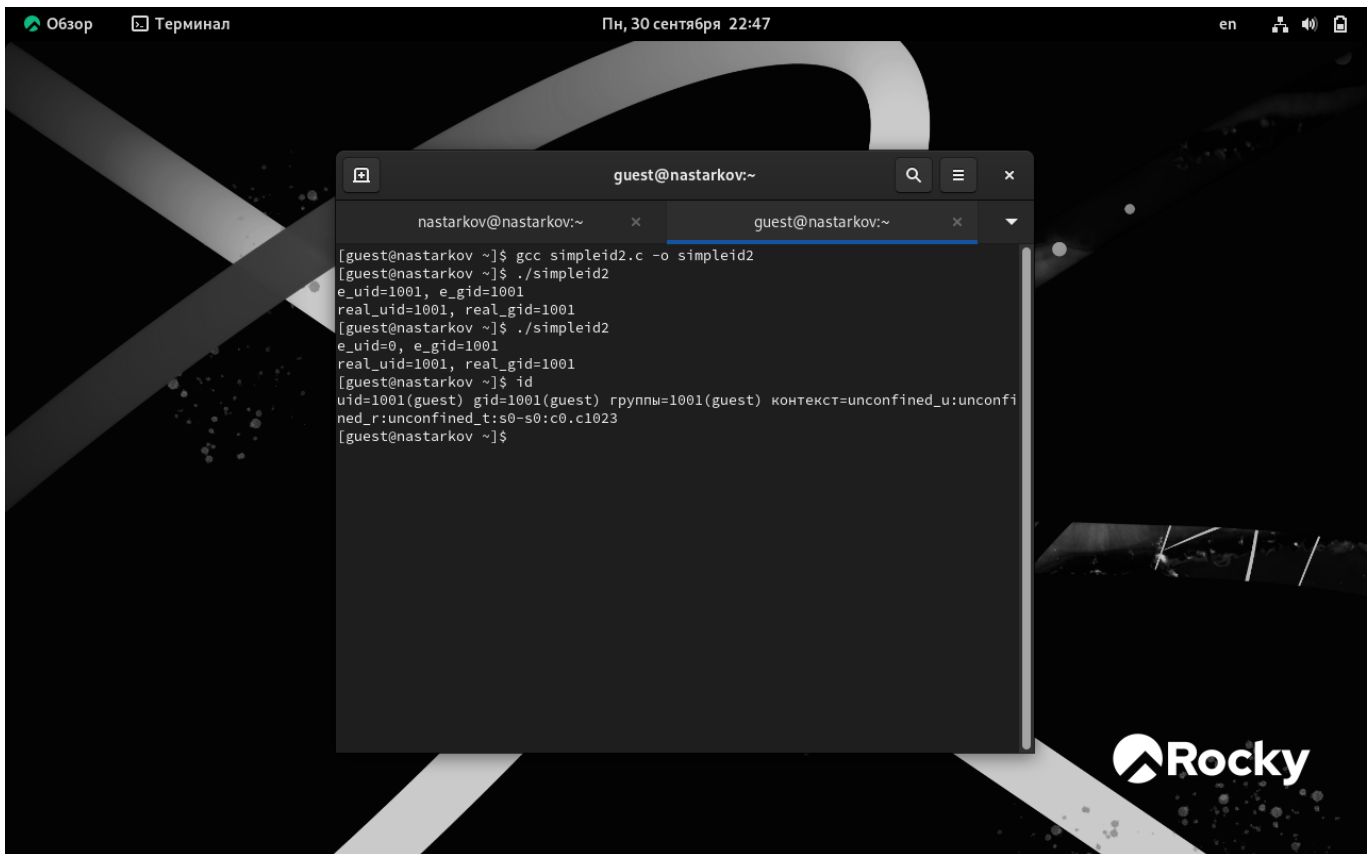
7. От имени суперпользователя выполнили команды "sudo chown root:guest/home/guest/simpleid2" и "sudo chmod u+s /home/guest/simpleid2", затем выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой "sudo ls -l /home/guest/simpleid2". Этими командами была произведена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



```
Обзор Терминал Пн, 30 сентября 22:47 en
```

```
nastarkov@nastarkov:~  
nastarkov@nastarkov:~ x guest@nastarkov:~  
[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 ~]$
```

Rocky

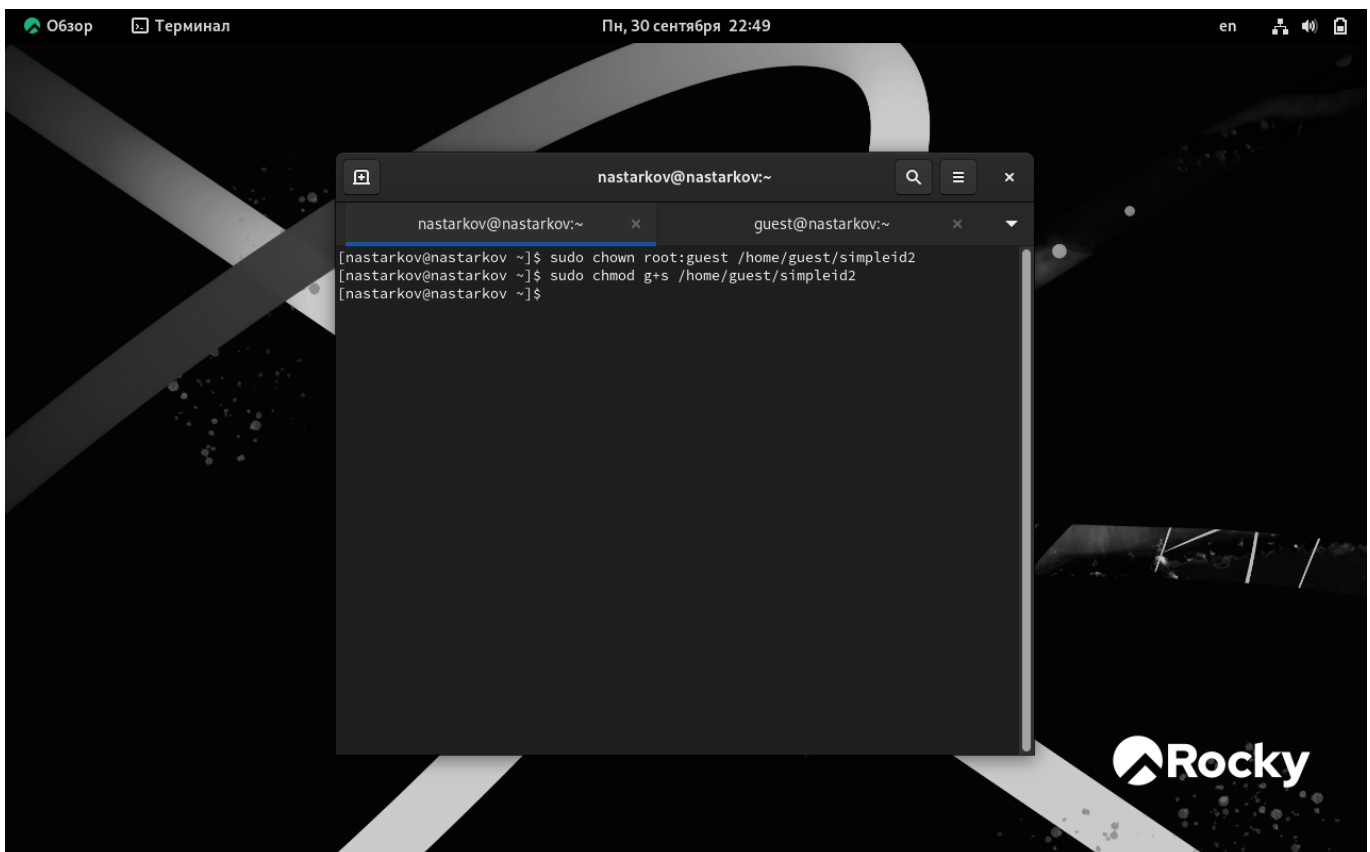


The screenshot shows a terminal window titled "guest@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The terminal output is as follows:

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

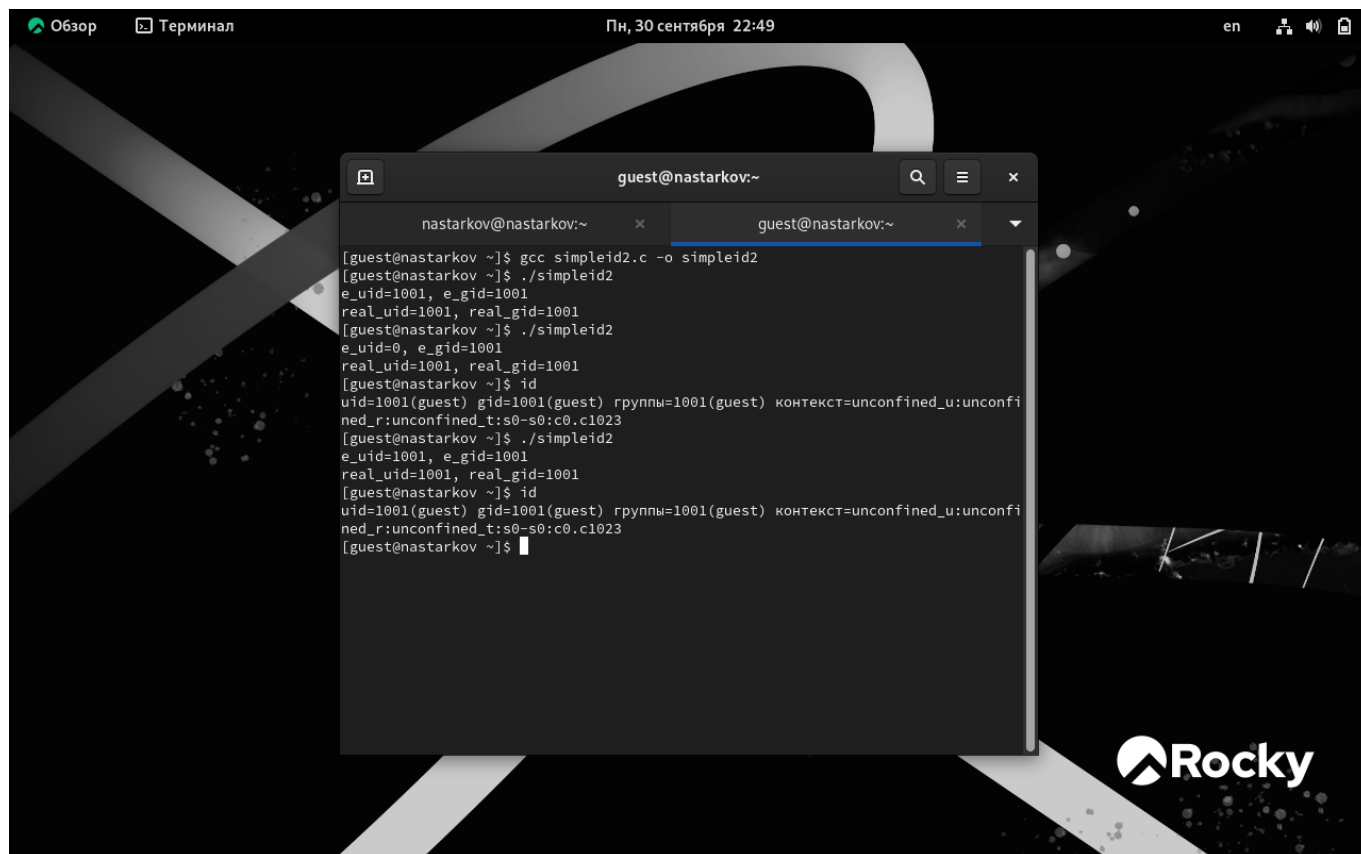
Запустил программы simpleid2 и id. Теперь появились различия в uid

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



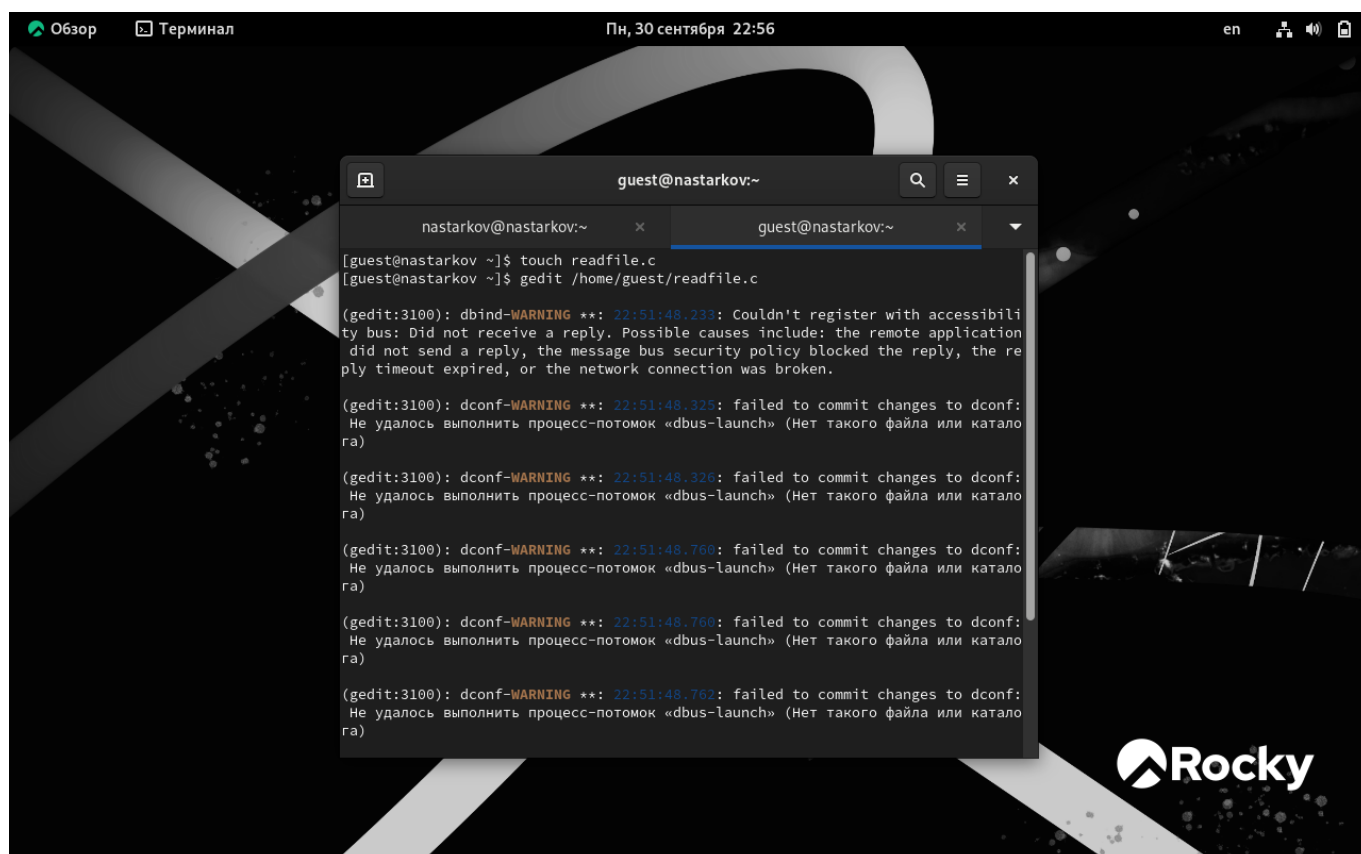
The screenshot shows a terminal window titled "nastarkov@nastarkov:~" with two tabs: "nastarkov@nastarkov:~" and "guest@nastarkov:~". The terminal output is as follows:

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

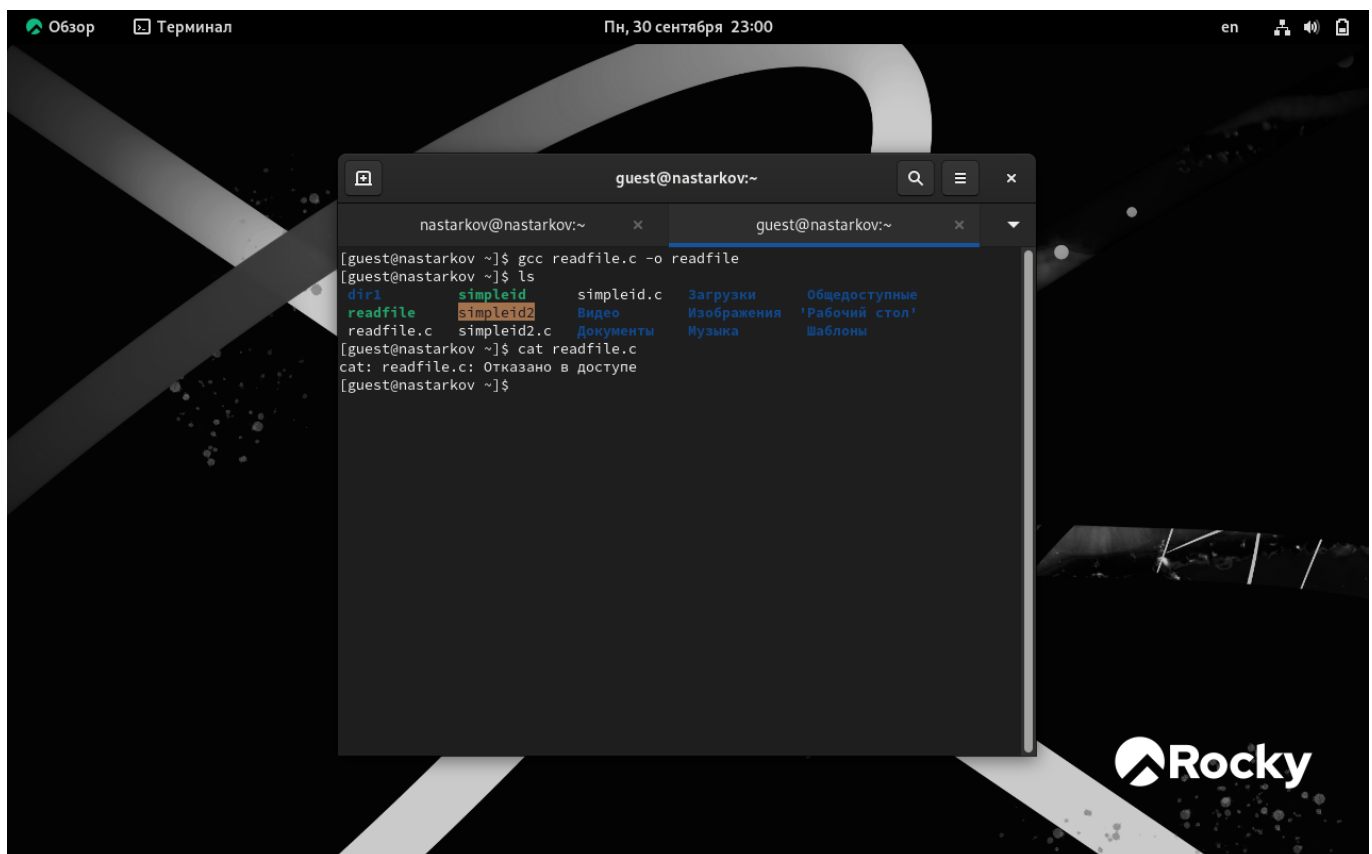
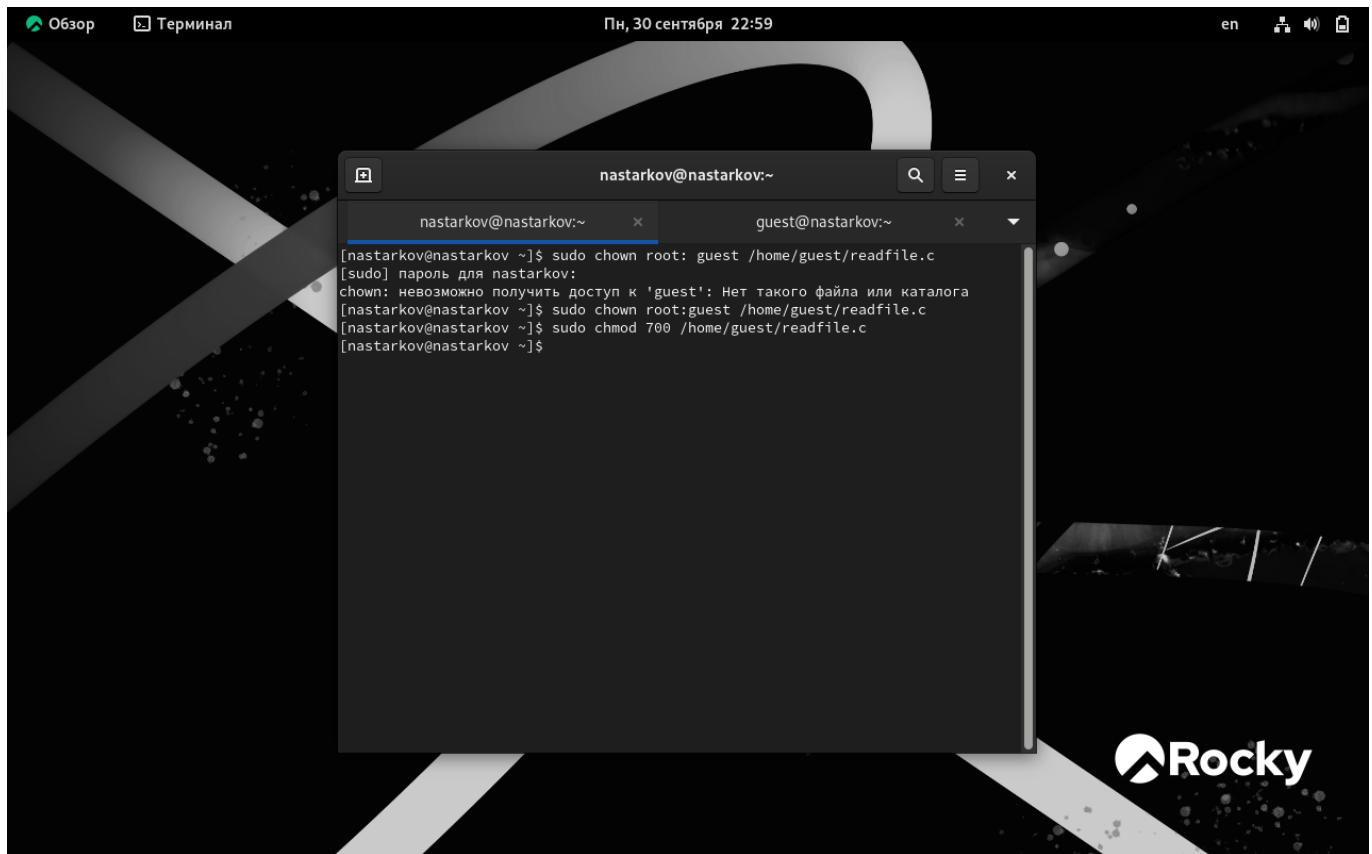


```
guest@nastarkov:~  
nastarkov@nastarkov:~  
[guest@nastarkov ~]$ gcc simpleid2.c -o simpleid2  
[guest@nastarkov ~]$ ./simpleid2  
e_uid=1001, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@nastarkov ~]$ ./simpleid2  
e_uid=0, e_gid=1001  
real_uid=1001, real_gid=1001  
[guest@nastarkov ~]$ id  
uid=1001(guest) gid=1001(guest) грппны=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) грппны=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.

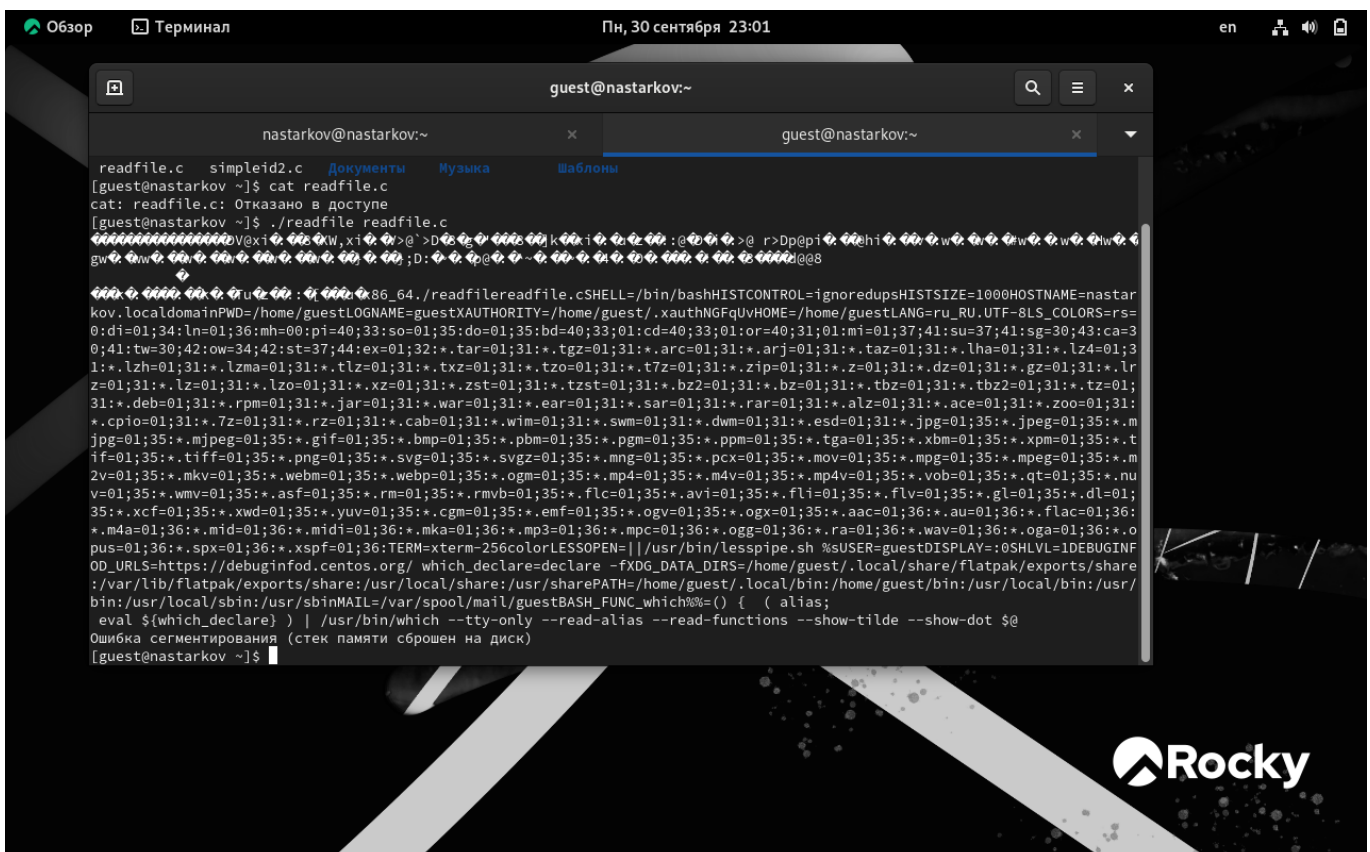
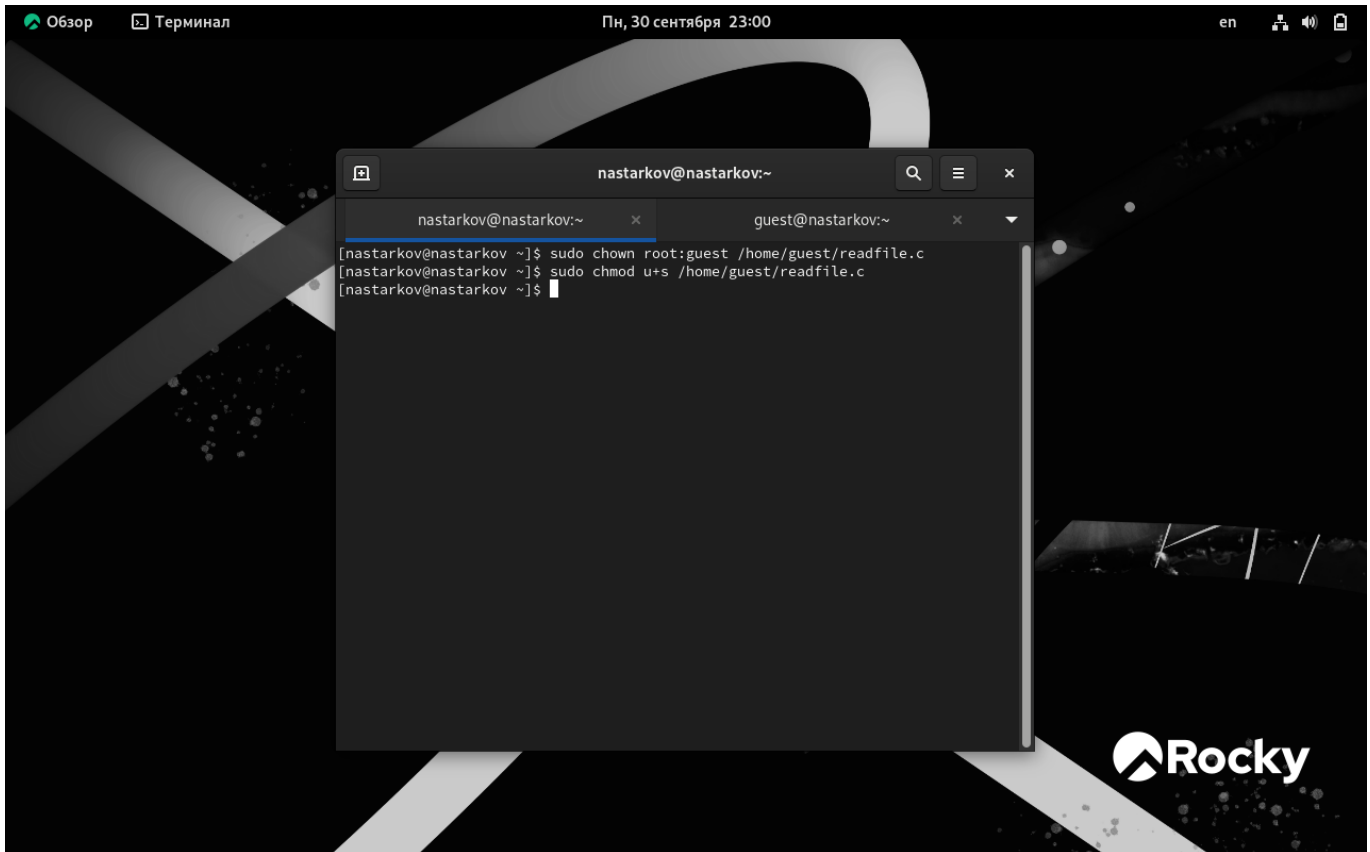


```
guest@nastarkov:~  
nastarkov@nastarkov:~  
[guest@nastarkov ~]$ touch readfile.c  
[guest@nastarkov ~]$ gedit /home/guest/readfile.c  
(gedit:3100): dbind-WARNING **: 22:51:48.233: Couldn't register with accessibility bus: Did not receive a reply. Possible causes include: the remote application 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)
```

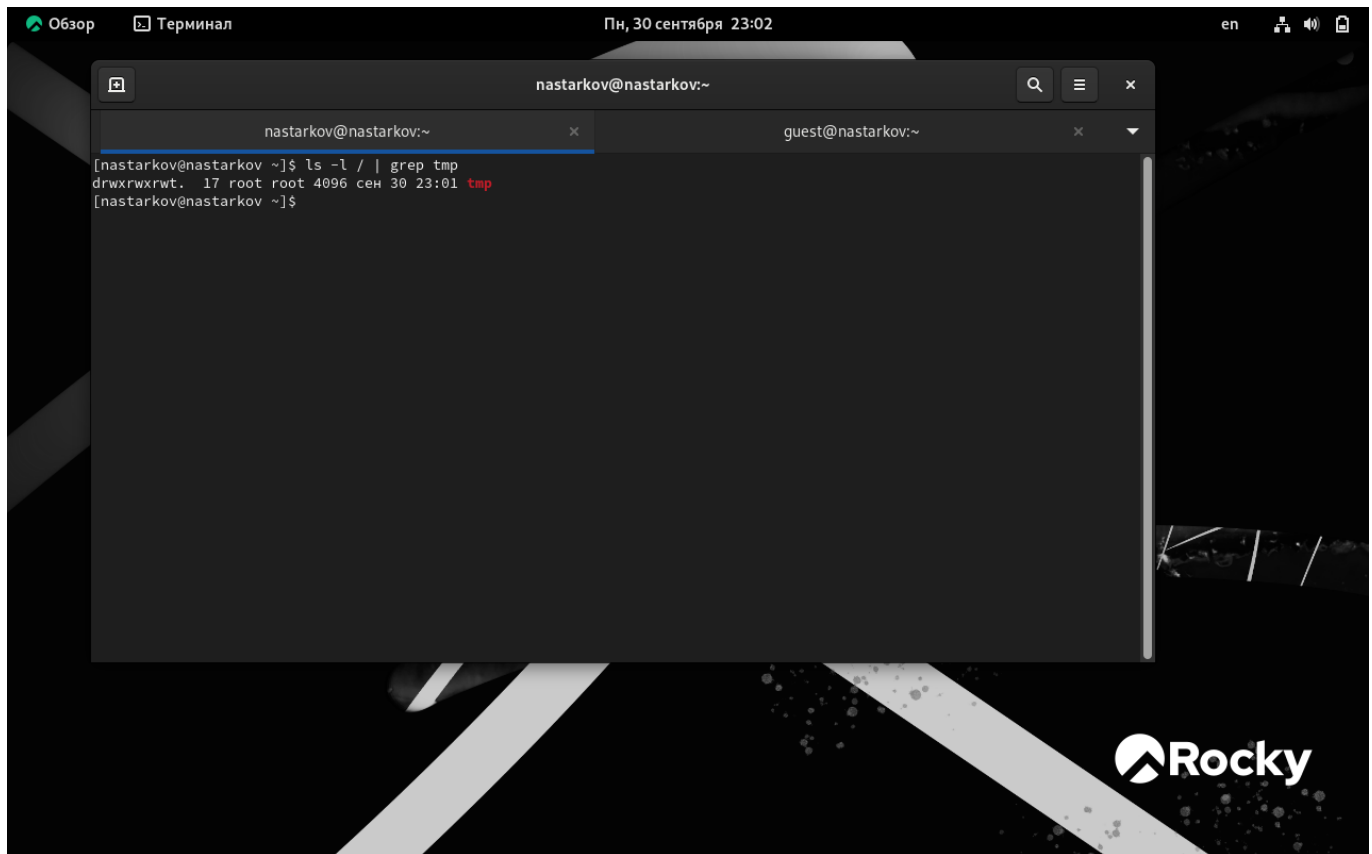


10. Поменяли владельца у программы readfile и установила SetUID. Проверили, может ли программа readfile прочитать файл readfile.c командой `./readfile readfile.c`. Прочитать удалось. Аналогично проверили, можно ли прочитать файл `/etc/shadow`. Прочитать удалось





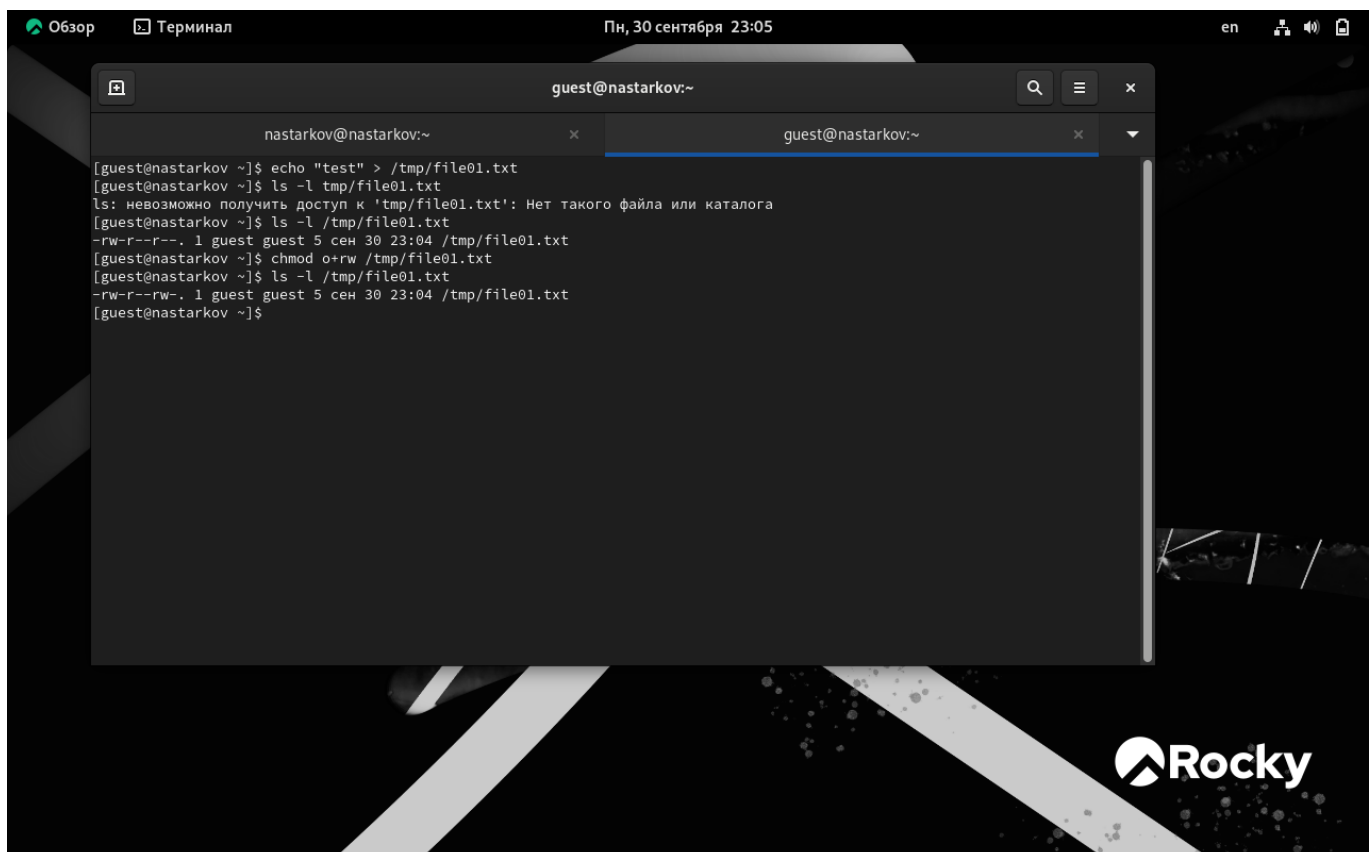
11. Командой "ls -l | grep tmp" убедились, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test командой "echo test" > /tmp/file01.txt". Просмотрели атрибуты у только что созданного файла и разрешаем чтение и запись для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

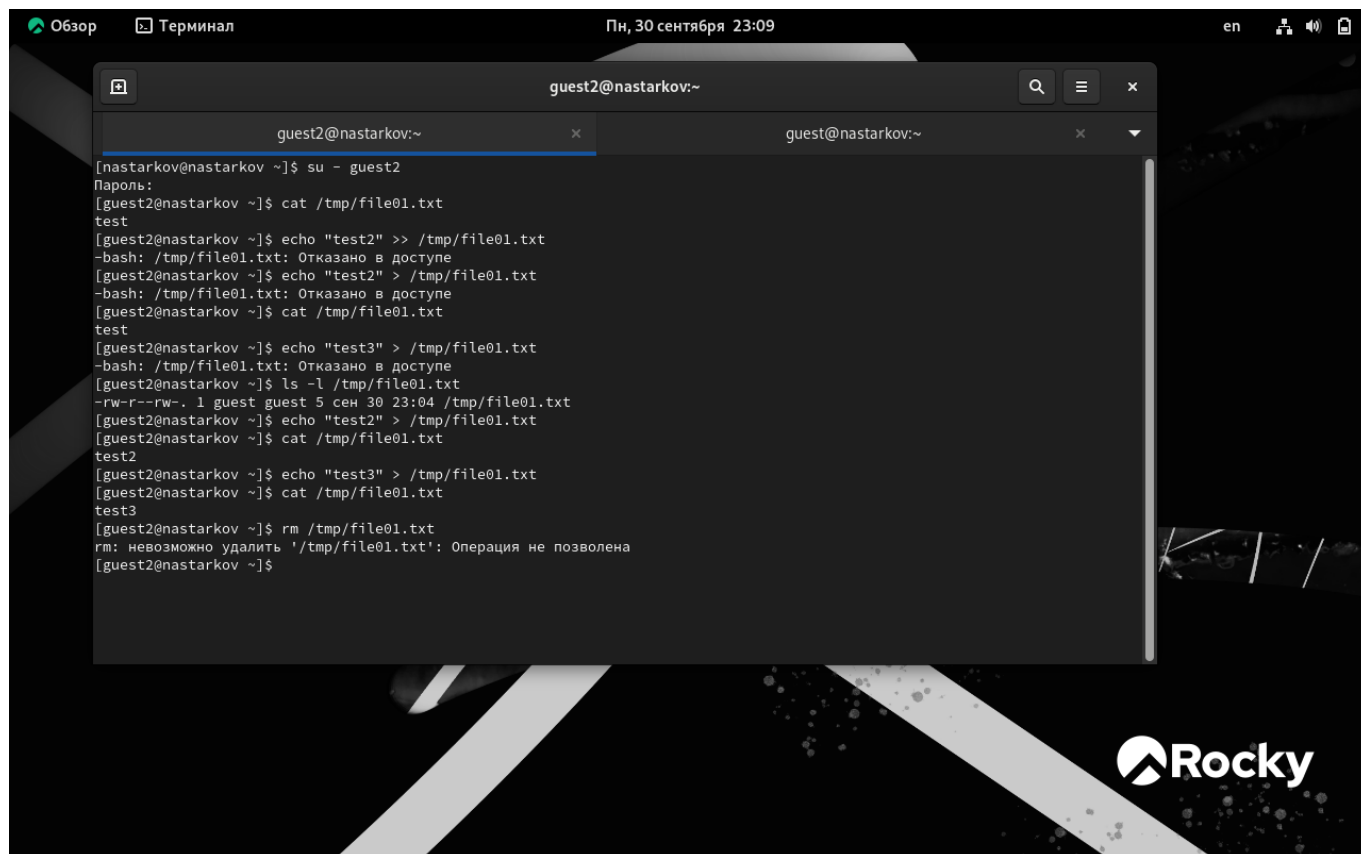


Обзор Терминал Пн, 30 сентября 23:05 en

```
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

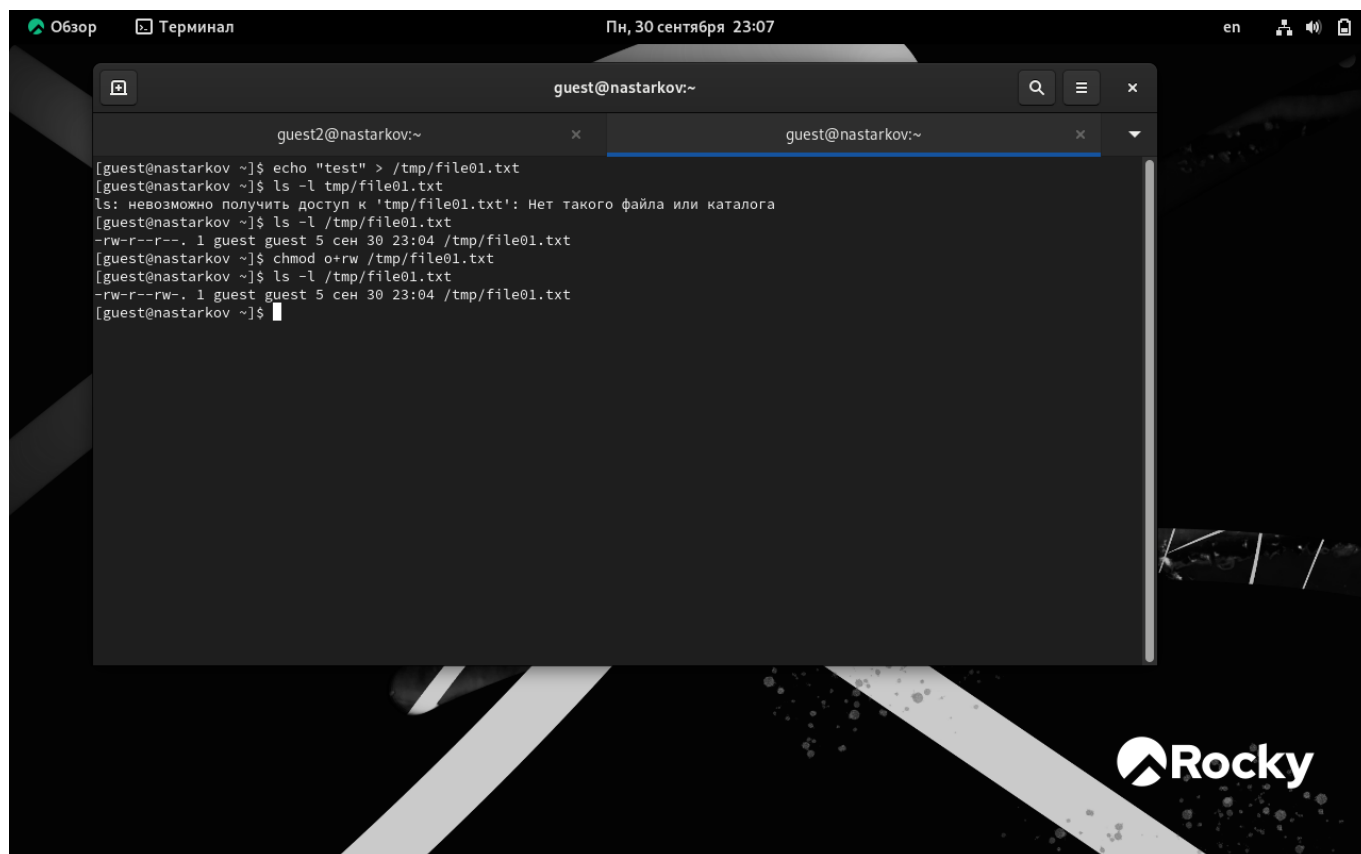
12. От имени пользователя guest2 попробовали прочитать файл командой "cat/tmp/file01.txt" - это удалось. Далее попытались дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в 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:~
```

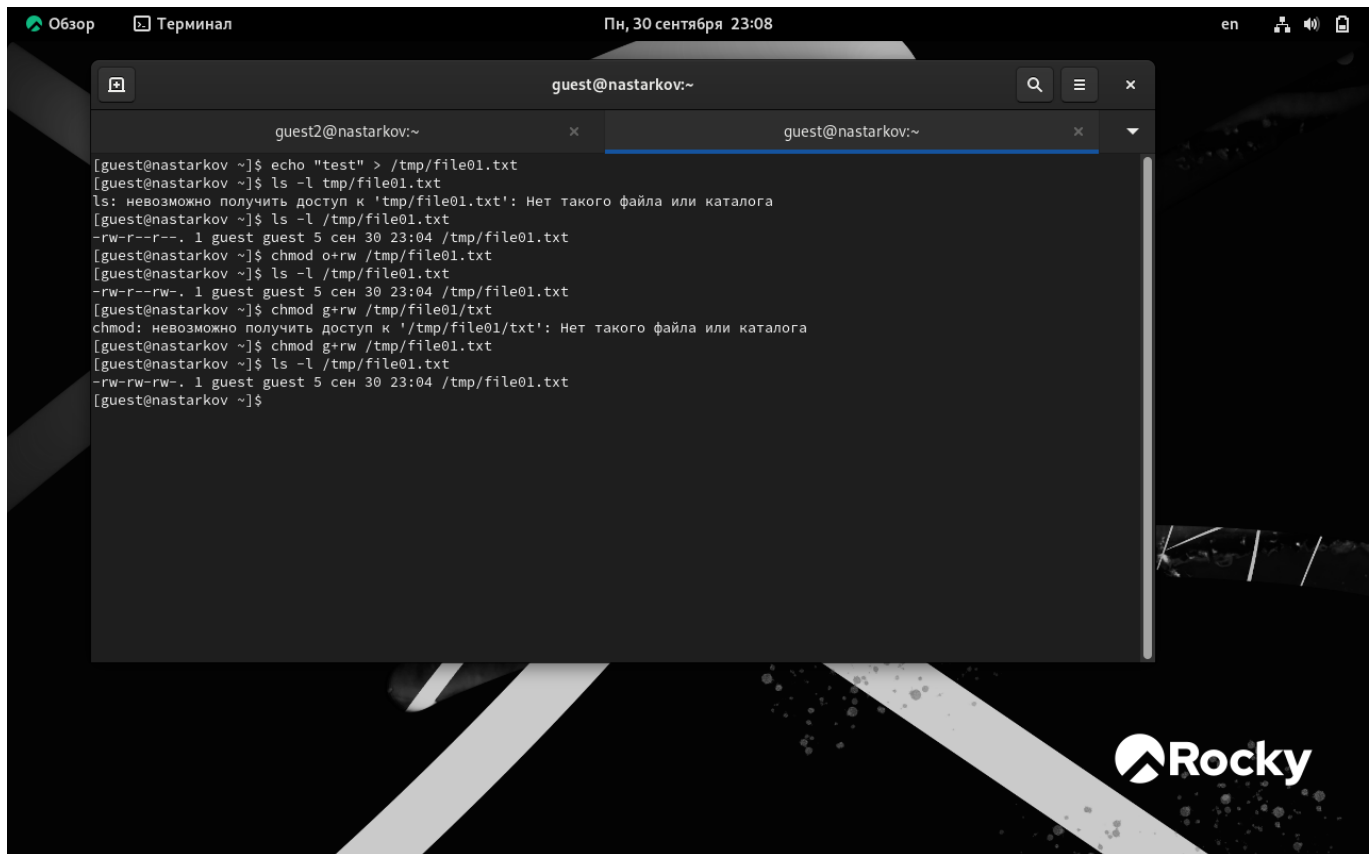
```
[nastarkov@nastarkov ~]$ su - guest2
Пароль:
[guest2@nastarkov ~]$ cat /tmp/file01.txt
test
[guest2@nastarkov ~]$ echo "test2" >> /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@nastarkov ~]$ echo "test2" > /tmp/file01.txt
-bash: /tmp/file01.txt: Отказано в доступе
[guest2@nastarkov ~]$ 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:~
```

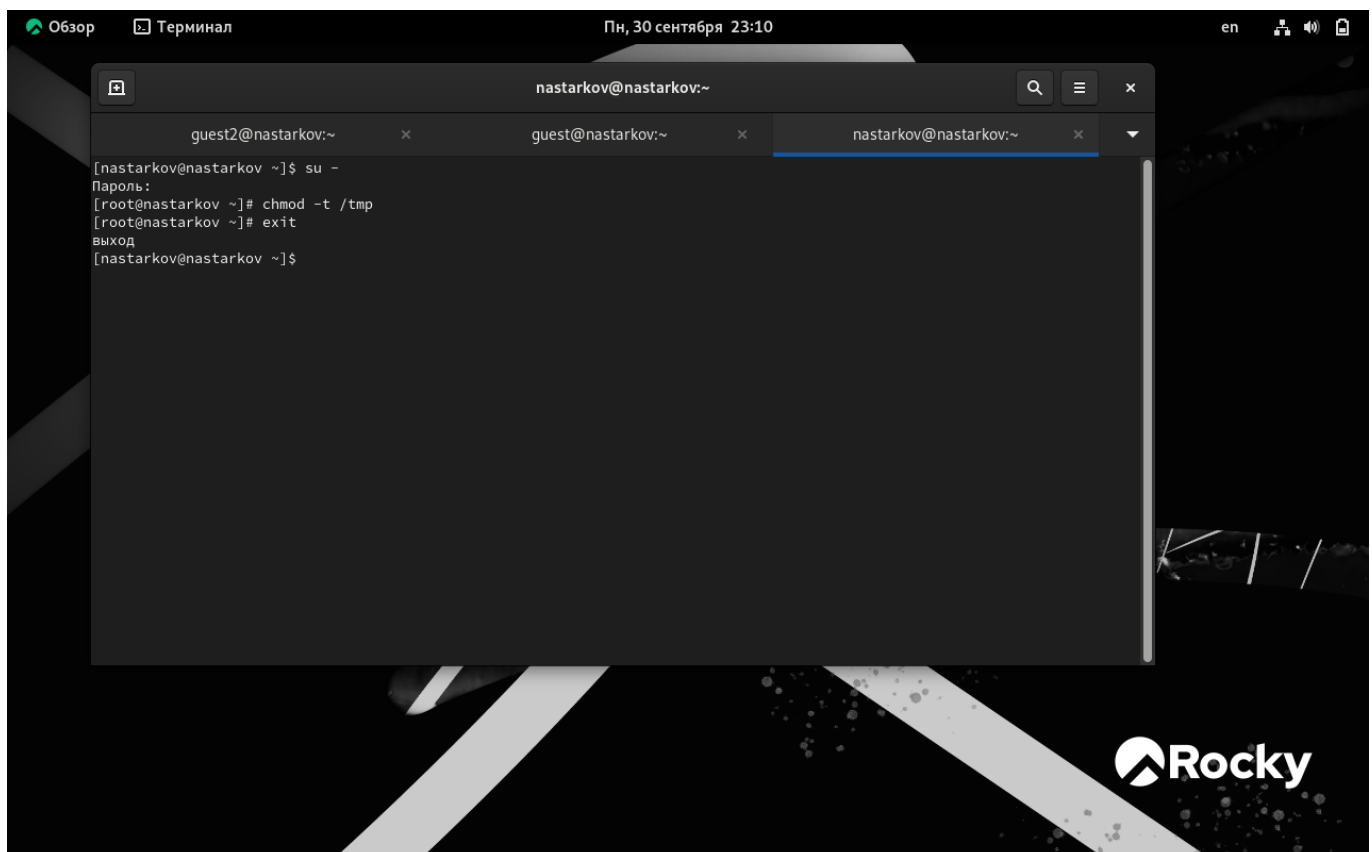
```
[guest2@nastarkov ~]$ echo "test" > /tmp/file01.txt
[guest@nastarkov ~]$ ls -l tmp/file01.txt
ls: невозможно получить доступ к 'tmp/file01.txt': Нет такого файла или каталога
[guest@nastarkov ~]$ ls -l /tmp/file01.txt
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt
[guest@nastarkov ~]$ chmod 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 user named 'guest' at a machine named 'nastarkov'. The user creates a file 'test' in the directory '/tmp/file01.txt' using the command 'echo "test" > /tmp/file01.txt'. They then use 'ls -l' to check the file's permissions, which are '-rw-r--r--'. The user attempts to change permissions to 'o+rw' but receives an error: 'chmod: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога'. They then try to change permissions to 'g+rw' and receive another error: 'chmod: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога'. Finally, they use 'chmod g+rw /tmp/file01.txt' successfully, and 'ls -l' shows the permissions as '-rw-rw-rw-'. The background of the terminal window features the Rocky Linux logo.

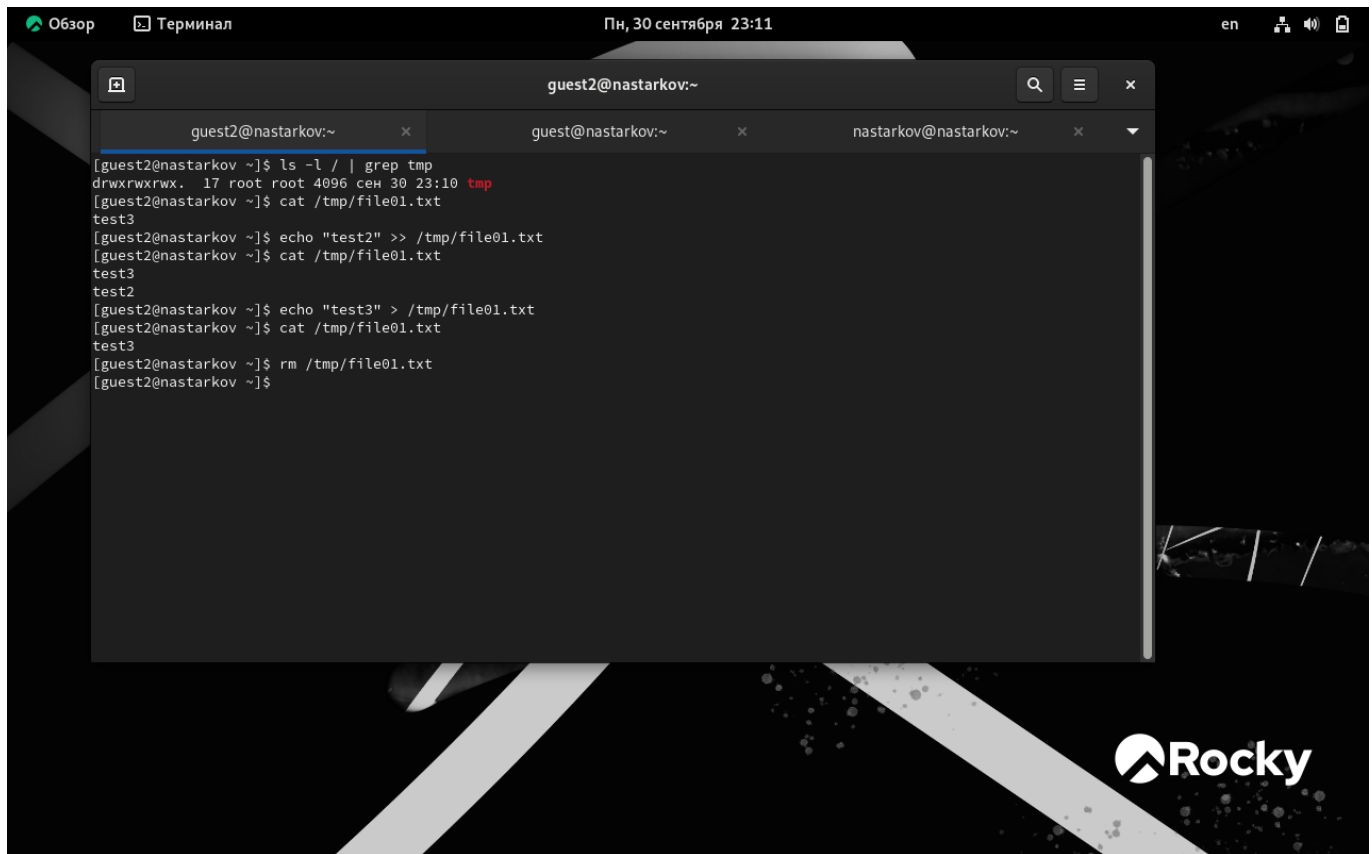
```
guest@nastarkov:~  
[guest@nastarkov ~]$ echo "test" > /tmp/file01.txt  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
ls: невозможно получить доступ к '/tmp/file01.txt': Нет такого файла или каталога  
[guest@nastarkov ~]$ ls -l /tmp/file01.txt  
-rw-r--r--. 1 guest guest 5 сен 30 23:04 /tmp/file01.txt  
[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' at the machine 'nastarkov'. They use 'su -' to switch to the root user. The prompt changes from '[nastarkov@nastarkov ~]' to '[root@nastarkov ~]'. The user then runs 'chmod -t /tmp' to remove the sticky bit from the /tmp directory. After that, they type 'exit' to return to the guest user. The prompt returns to '[nastarkov@nastarkov ~]'. 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 ~]$
```

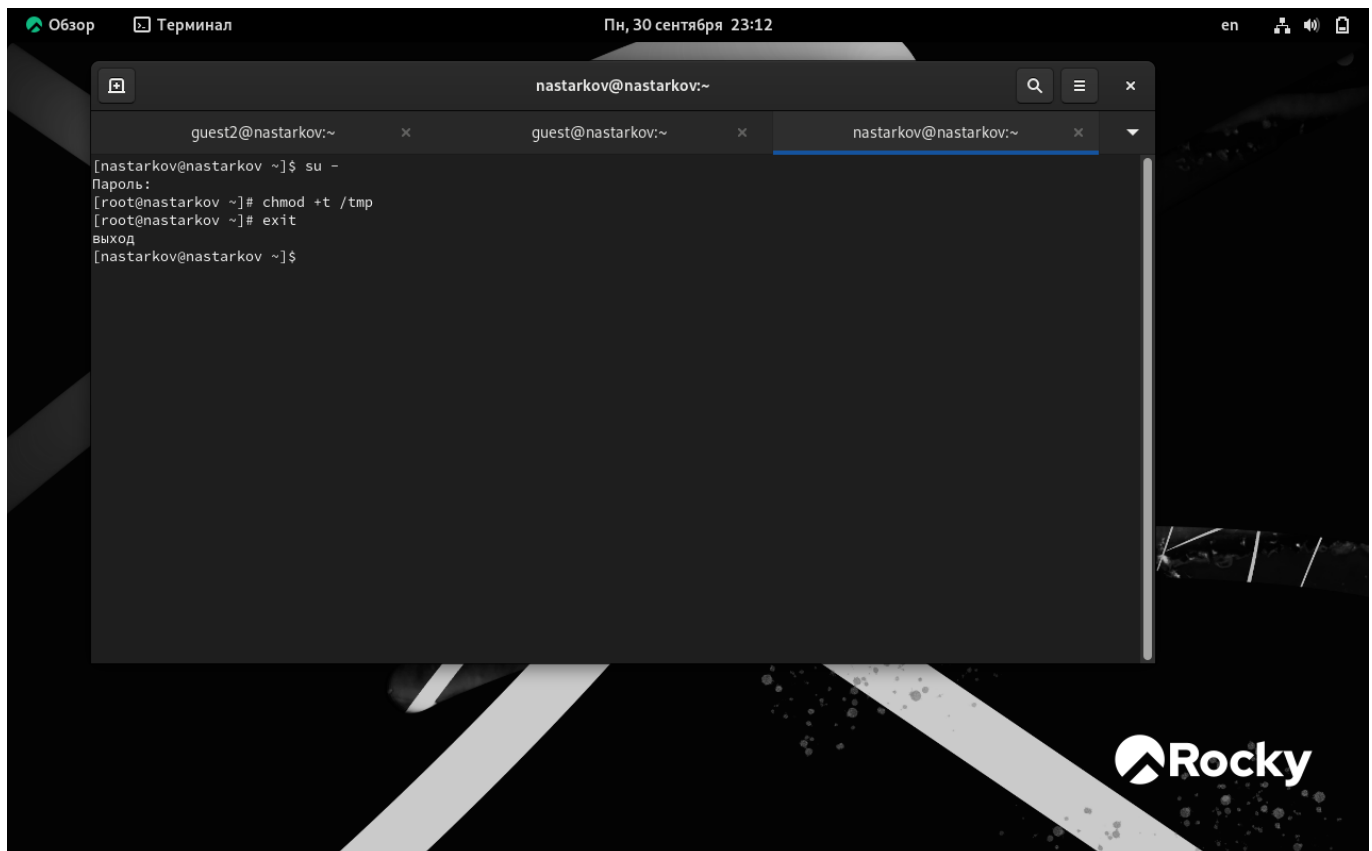


A terminal window titled "guest2@nastarkov:~" is shown. The window has a dark background with a light gray border. The terminal output shows the following commands and results:

```
[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 ~]$
```

The background of the terminal window shows a dark, abstract image with the "Rocky" logo in the bottom right corner.

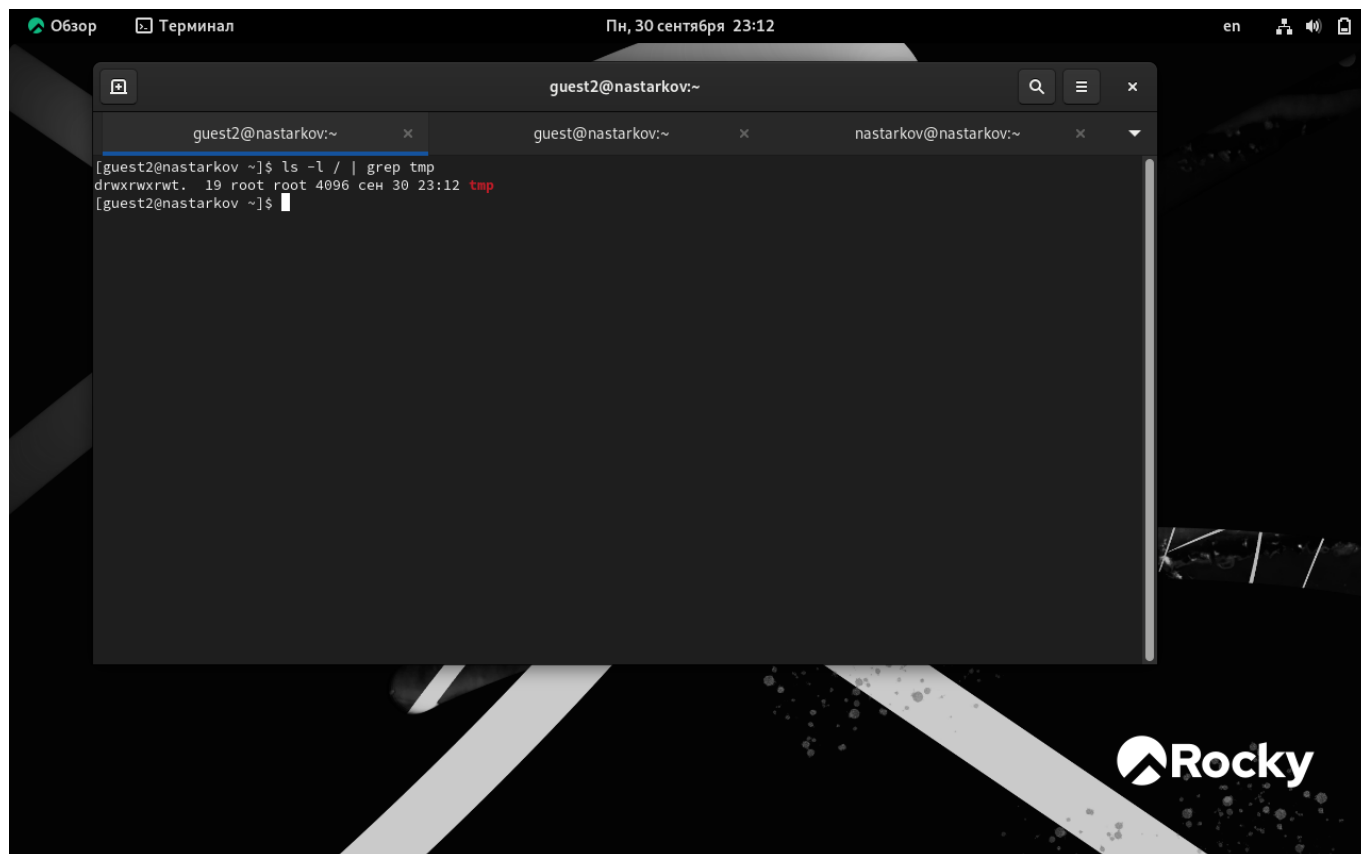
#### 14. Вернули атрибут t+



A terminal window titled "nastarkov@nastarkov:~" is shown. The window has a dark background with a light gray border. The terminal output shows the following commands and results:

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

The background of the terminal window shows a dark, abstract image with the "Rocky" logo in the bottom right corner.



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

```
guest2@nastarkov:~  
[guest2@nastarkov ~]$ ls -l | grep tmp  
drwxrwxrwt. 19 root root 4096 сеп 30 23:12 tmp  
[guest2@nastarkov ~]$
```

## Вывод

В ходе выполнения лабораторной работы №5 я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.