Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Венчаков Никита НБИбд-01-19"

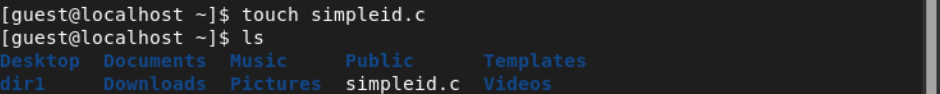
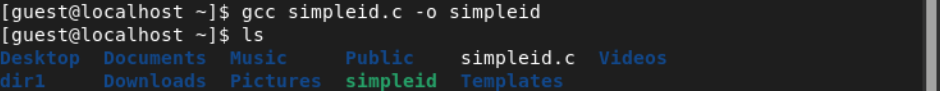
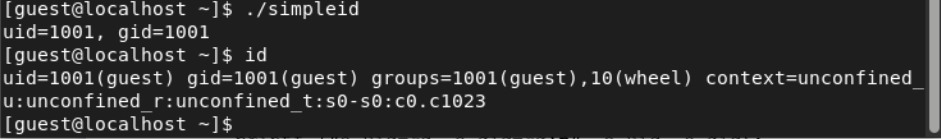
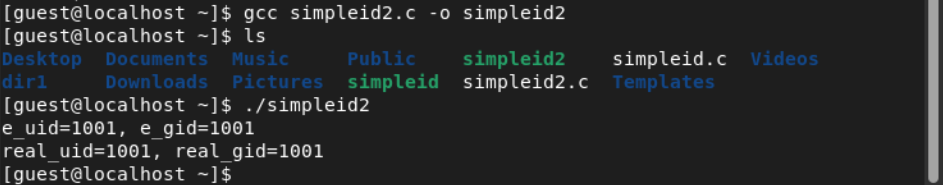
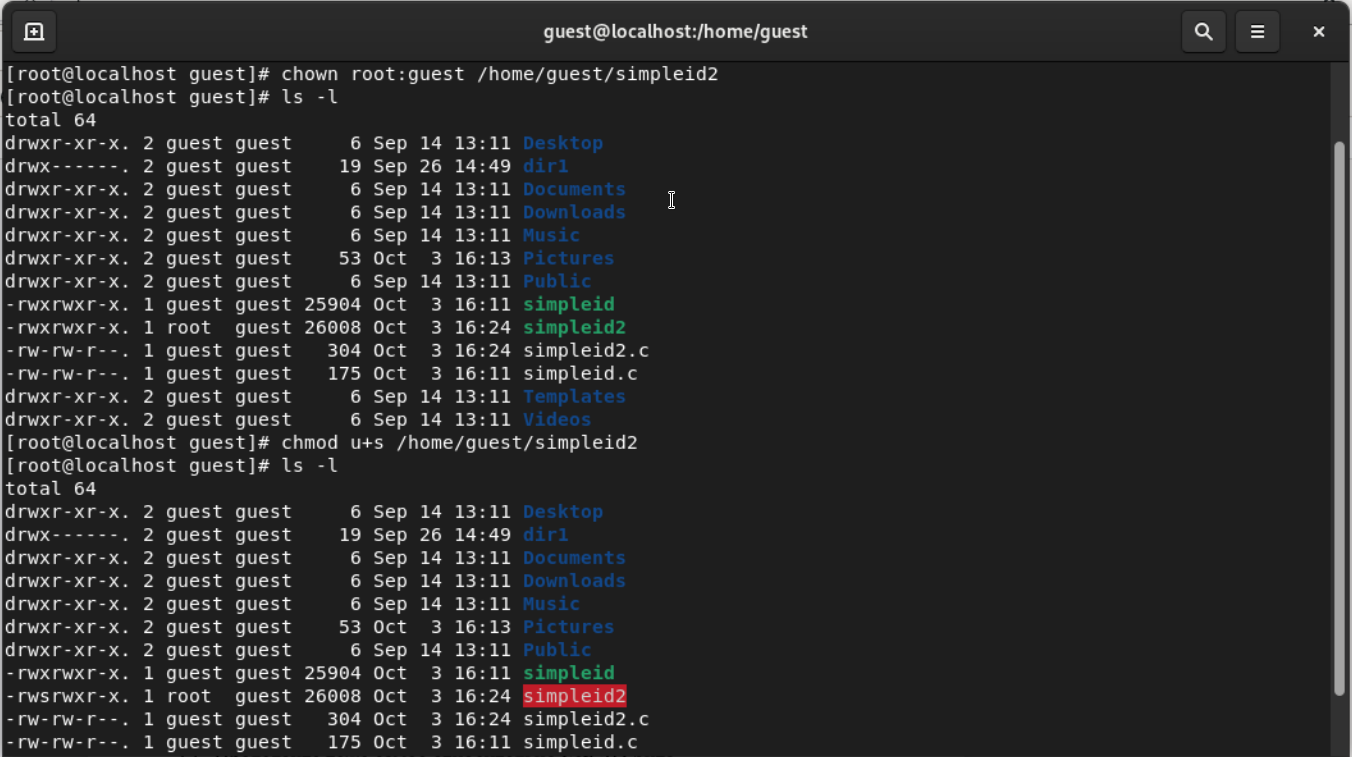
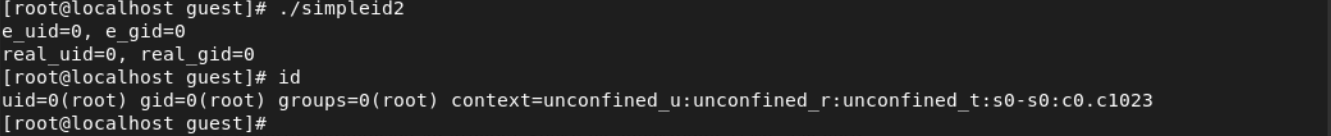
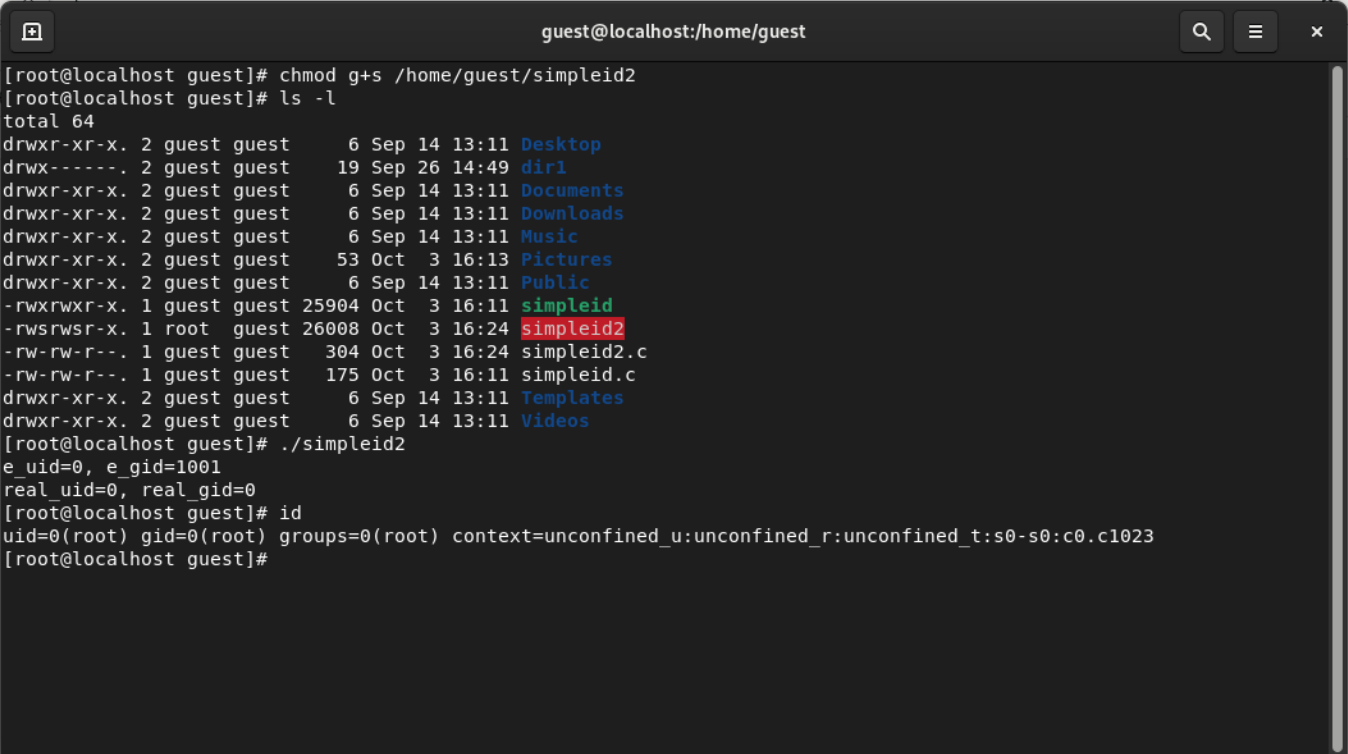
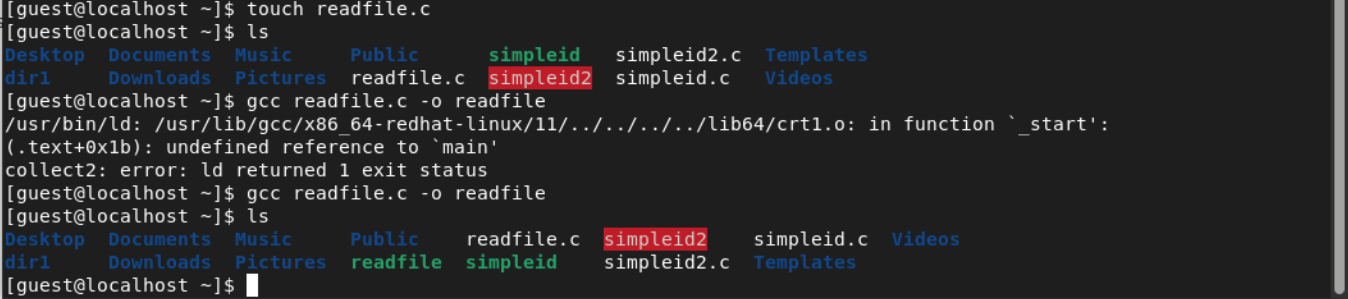
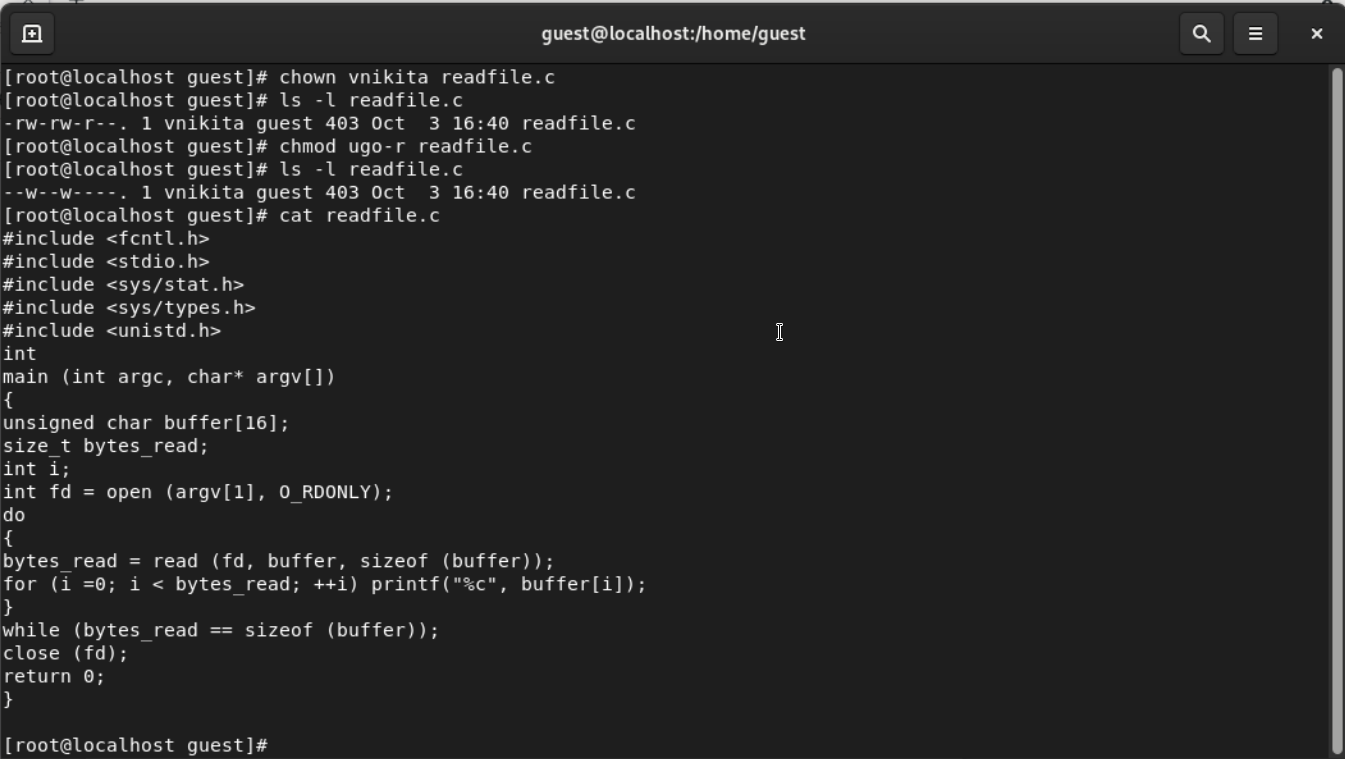
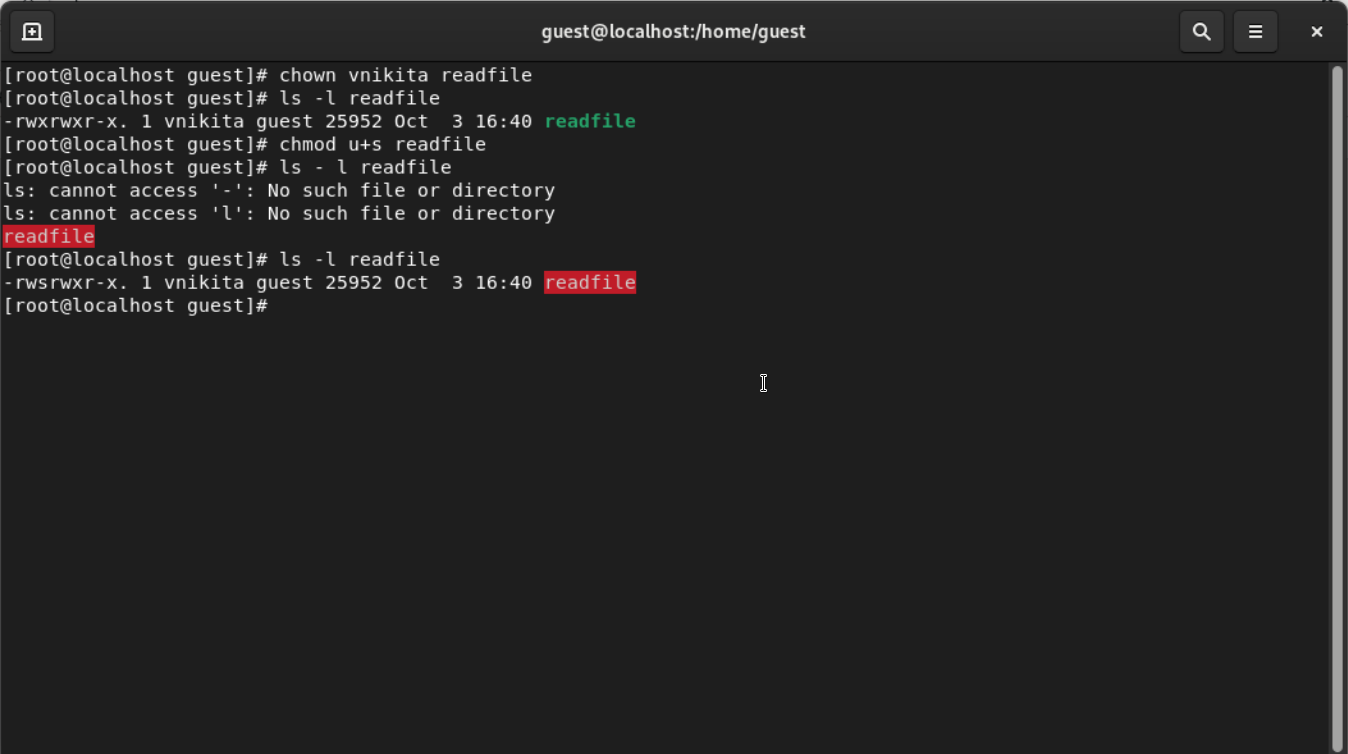
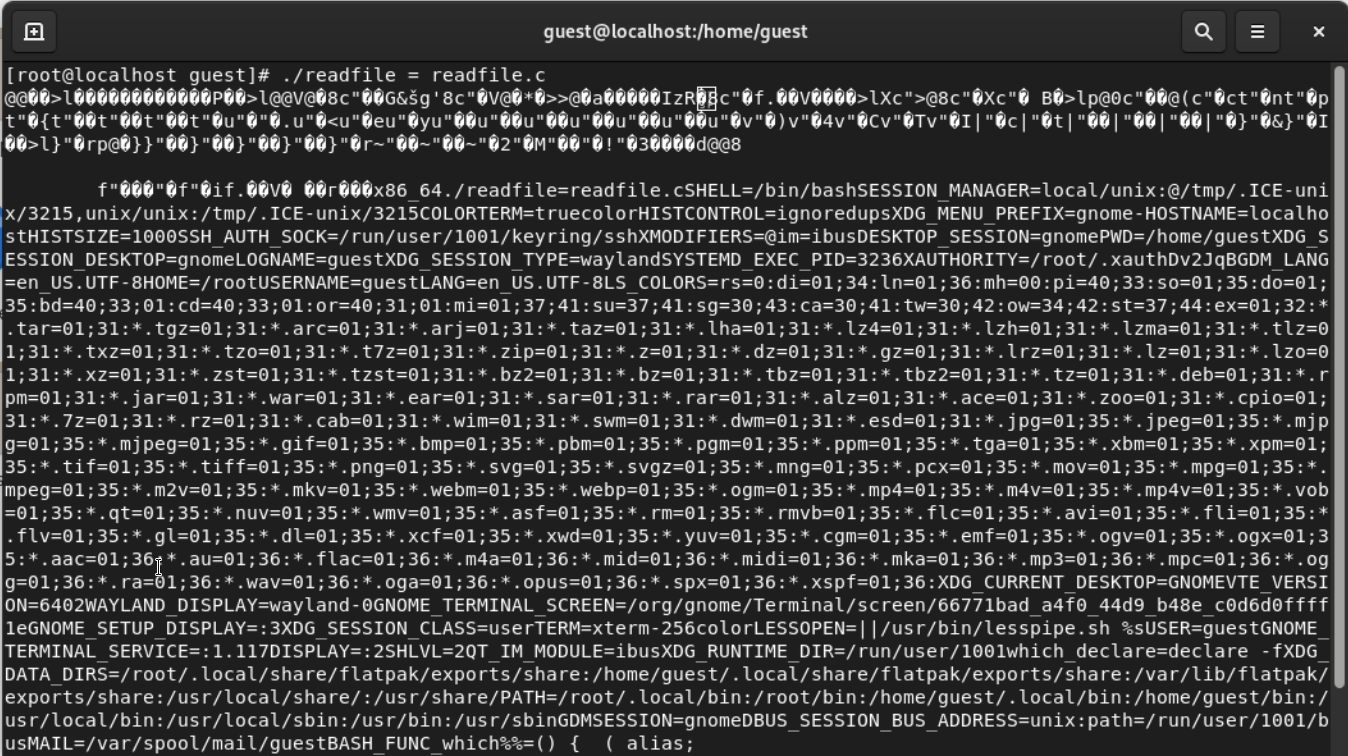
Содержание

# Цель работы

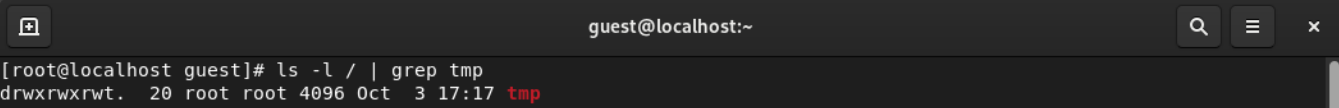
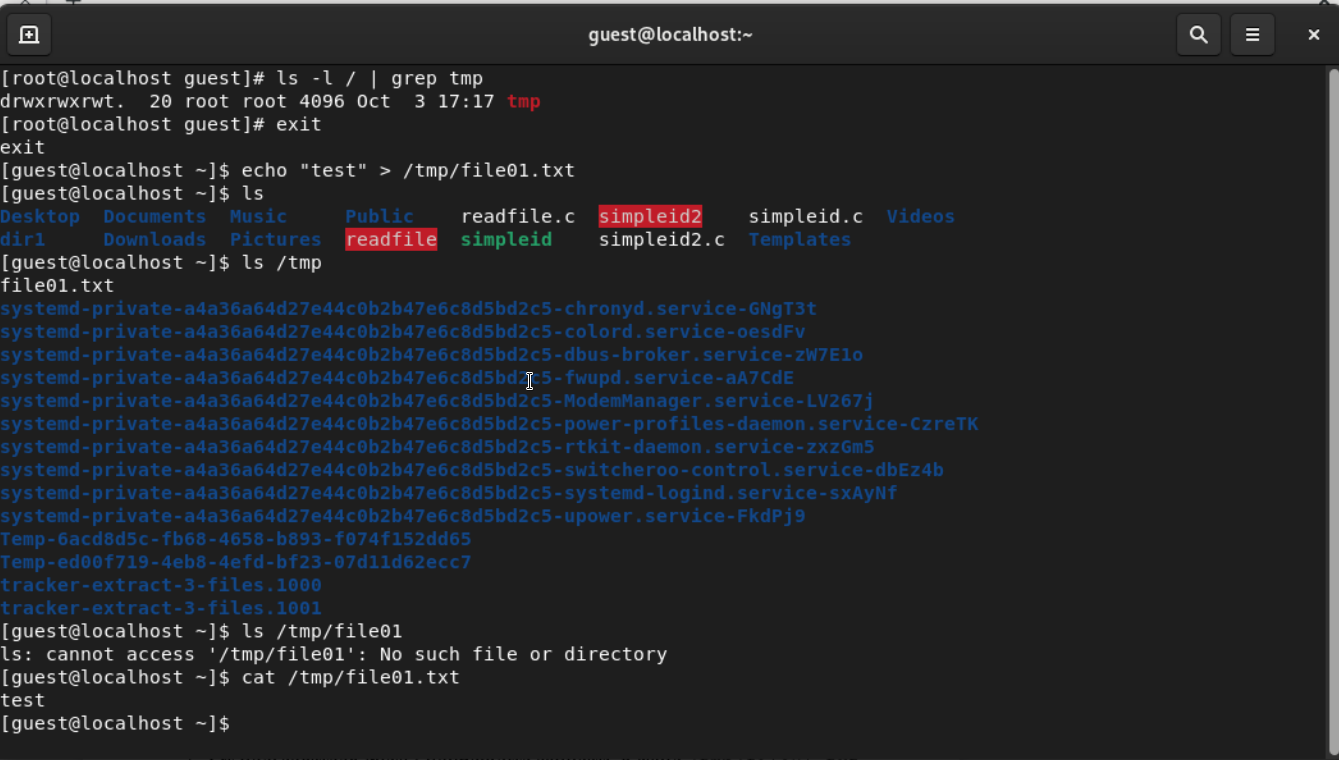
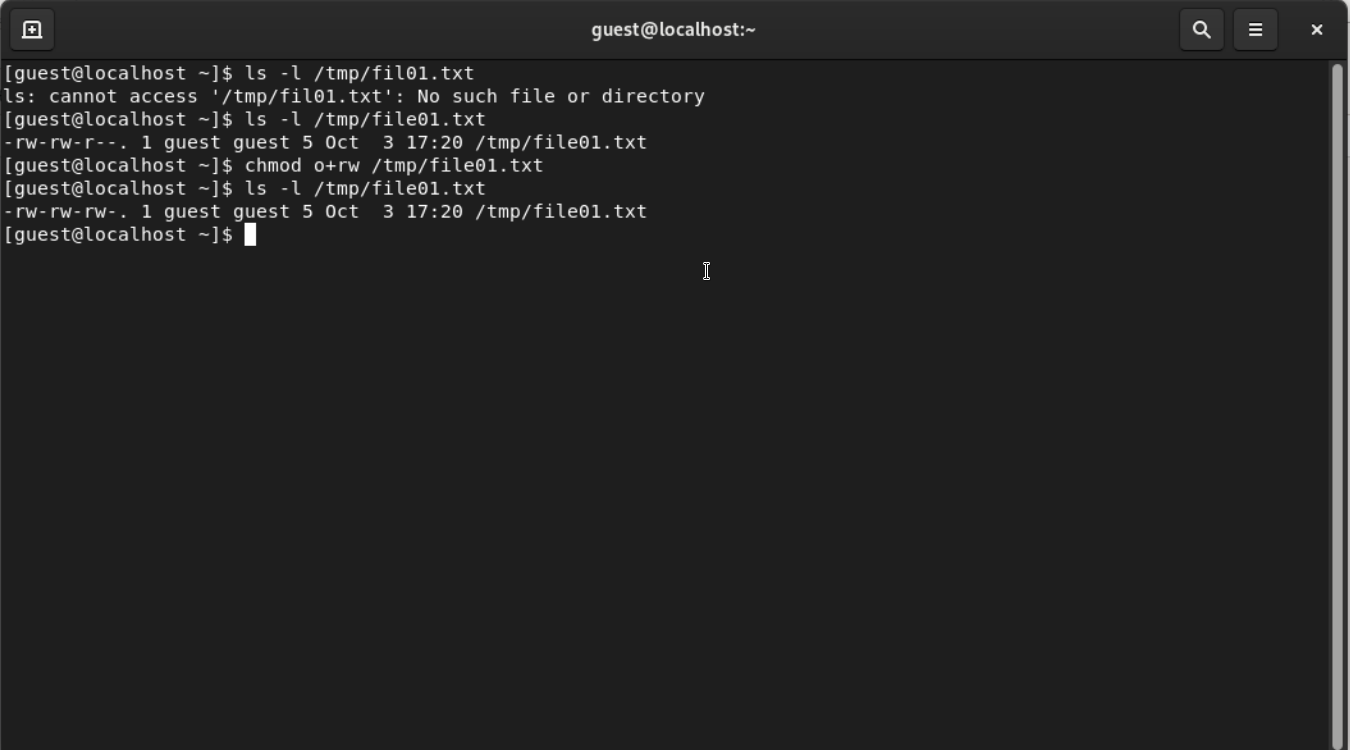
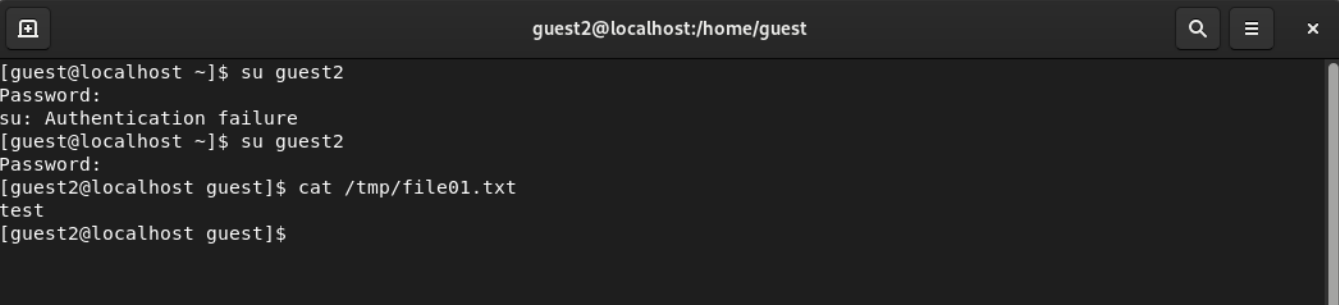
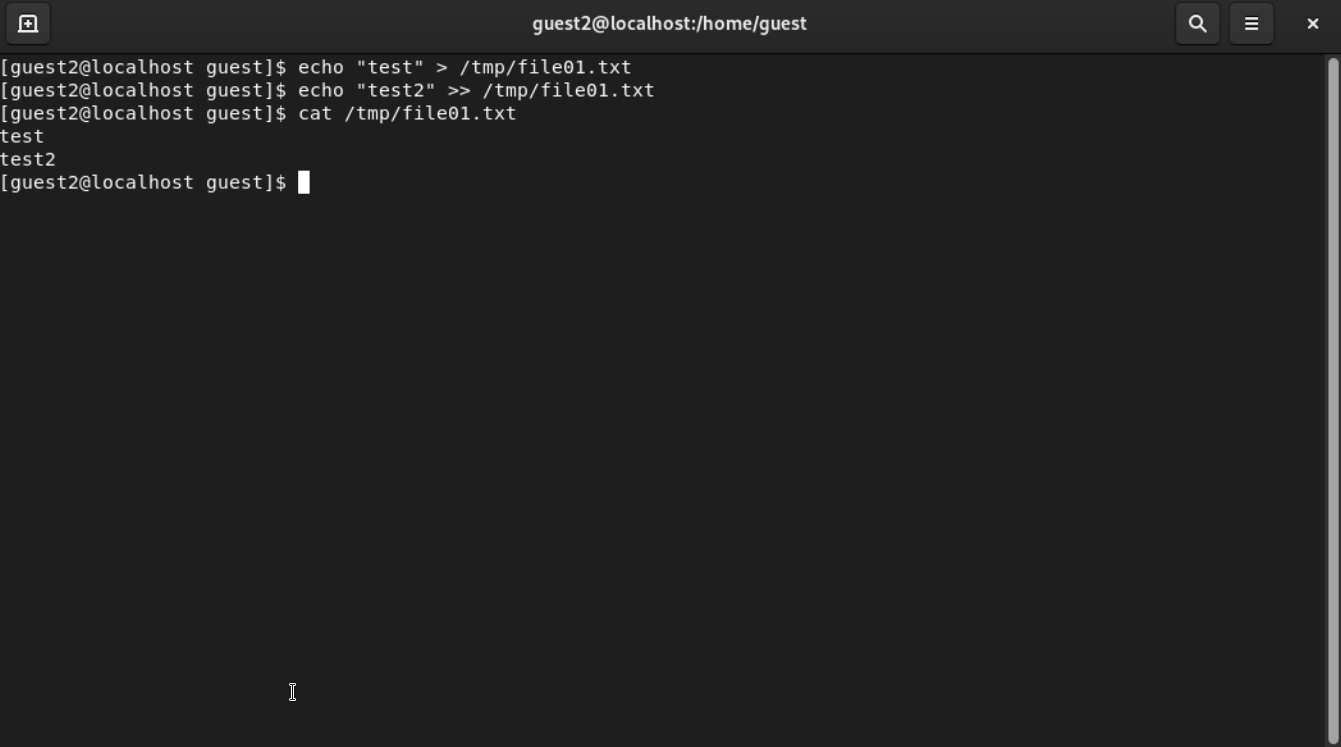
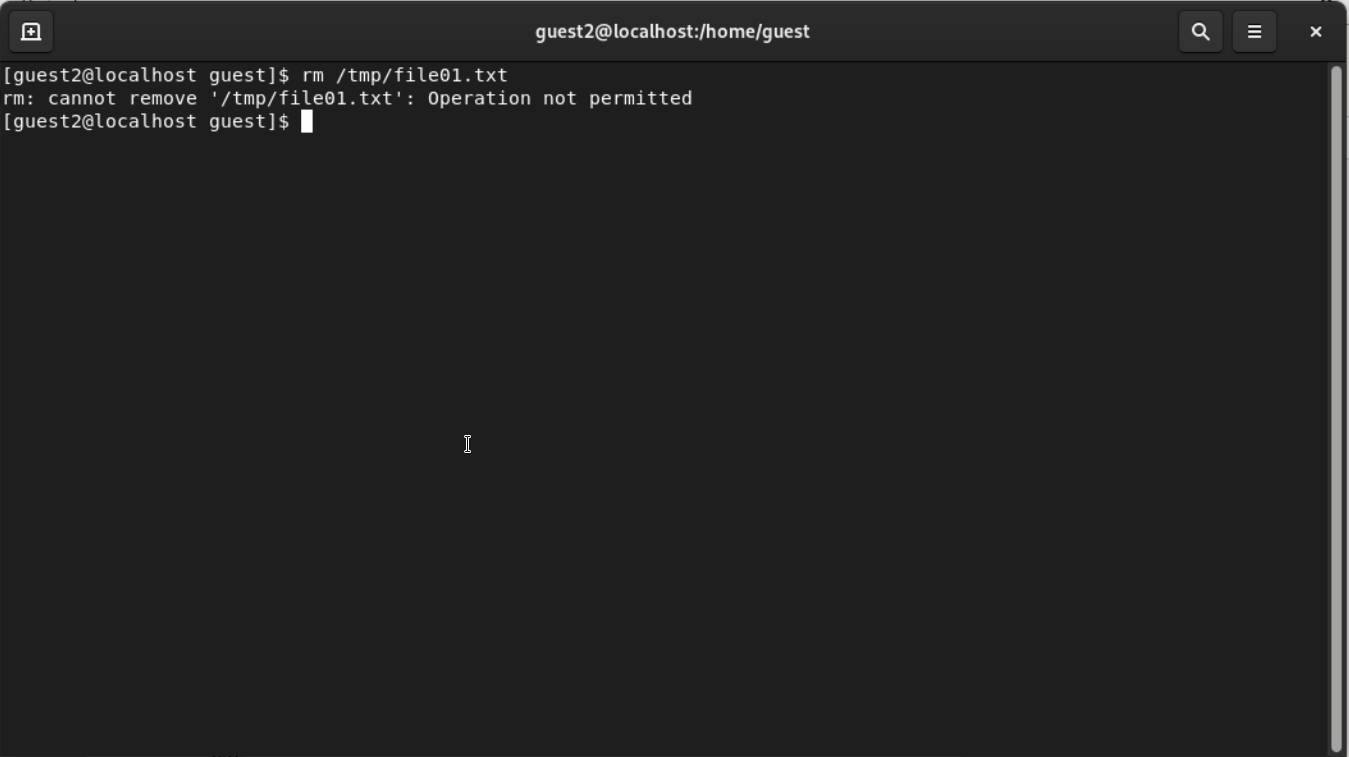
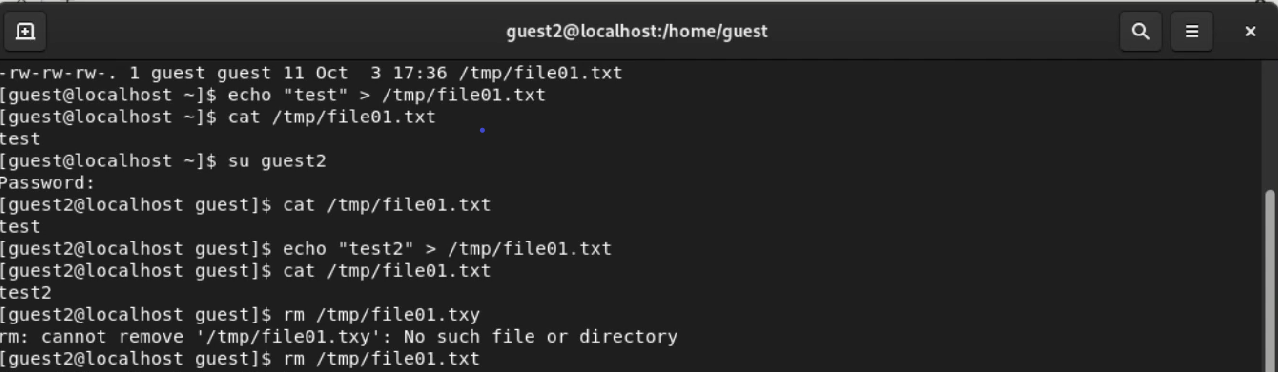
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние битаSticky на запись и удаление файлов.

# Выполнение лабораторной работы

## Часть №1

1. Вошел в систему от имени пользователя guest.
2. Создал программу simpleid.c: ([рис.№1](Скриншоты выполнения\Создание файла simpleid.png))  
   
3. Скомплилировал программу и убедился, что файл программы создан: ([рис.№2](Скриншоты выполнения\Компилирование simpleid.png))  
   
4. Выполнил программу simpleid. ([рис.№3](Скриншоты выполнения\ Выполнение simpleid.png))  
   fig:
5. Сравнил id пользователя и группы пользователей через команду id, при проверке с прошлым пунтком - результат одинаковый. ([рис.№4](Скриншоты выполнения\Сравнение id.png))  
   
6. Усложнил программу, добавив вывод действительных идентификаторов.
7. Скомпилировал и запустил simpleid2.c:  
   lsattr /home/guest/dir1/file1 ([рис.№5](Скриншоты выполнения\Компилирование и выполнение simpleid2.png))  
   
8. От имени суперпользователя выполните команды:   
   chown root:guest /home/guest/simpleid2, chmod u+s /home/guest/simpleid2 ([рис.№6](Скриншоты выполнения\Изменение прав simpleid2.png))  
   
9. Выполните проверку правильности установки новых атрибутов и смены  
   владельца файла simpleid2: ls -l simpleid2.
10. Запустил simpleid2 и id. ([рис.№7](Скриншоты выполнения\Выполнение simpleid2 от суперпользователя.png))  
    
11. Проделал тоже самое относительно SetGID-бита. ([рис.№8](Скриншоты выполнения\SETGid.png))  
    
12. Создал программу 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;  
    }
13. Скомпилировал её.([рис.№9](Скриншоты выполнения\readfile.png))  
    
14. Сменил владельца у файла readfile.c на vnikikita и изменил права так, чтобы только суперпользователь мог прочитать его, a guest не мог.([рис.№10](Скриншоты выполнения\Смена пользователя readfile.png))  
    
15. Сменил у программы readfile владельца и установил SetUID-бит ([рис.№11](Скриншоты выполнения\SETUID readfile.png))  
    
16. Проверил, может ли программа readfile прочитать файл readfile.c - да может. ([рис.№12](Скриншоты выполнения\Выполнение readfile.png))  
    
17. Проверил, может ли программа readfile прочитать файл /etc/shadow - да может. ([рис.№13](Скриншоты выполнения\Чтение shadow.png))  
    

## Часть №2

1. Выяснил, установлен ли атрибут Sticky на директории /tmp, для чего  
   выполнил команду ls -l / | grep tmp. ([рис.№14](Скриншоты выполнения\Просмотр sticky.png))  
   
2. От имени пользователя guest создал файл file01.txt в директории /tmp  
   со словом test: ([рис.№15](Скриншоты выполнения\Запись в tmp.png))  
   
3. Просмотрел атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt  
   chmod o+rw /tmp/file01.txt  
   ls -l /tmp/file01.txt ([рис.№16](Скриншоты выполнения\Изменение прав readfile.png))  
   
4. От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt: cat /tmp/file01.txt ([рис.№17](Скриншоты выполнения\Чтение file01 от guest2.png))  
   
5. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2 командой echo "test2" >> /tmp/file01.txt. ([рис.№18](Скриншоты выполнения\Дозаписывание text2 в file01.png))  
   
6. От пользователя guest2 попробовал удалить файл /tmp/file01.txt командой  
   rm /tmp/fileOl.txt. Удалить файл не удалось.([рис.№19](Скриншоты выполнения\Попытка удаления file01.png))  
   
7. Повторил предыдущие шаги без без sticky-бита(без атрибута t) ([рис.№20](Скриншоты выполнения\Часть 2 без sticky.png))  
   
8. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp:  
   su -  
   chmod +t /tmp

# Вывод

Получил практические навыки работы в консоли с расширенными атрибутами файлов.