Отчёт по лабораторной работе №5

Основы информационной безопасности

Ищенко Ирина НПИбд-02-22

Содержание

# 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[1].

# 2 Выполнение лабораторной работы

Войдем в систему от имени пользователя guest. Создадим программу simpleid.c (рис. 1):

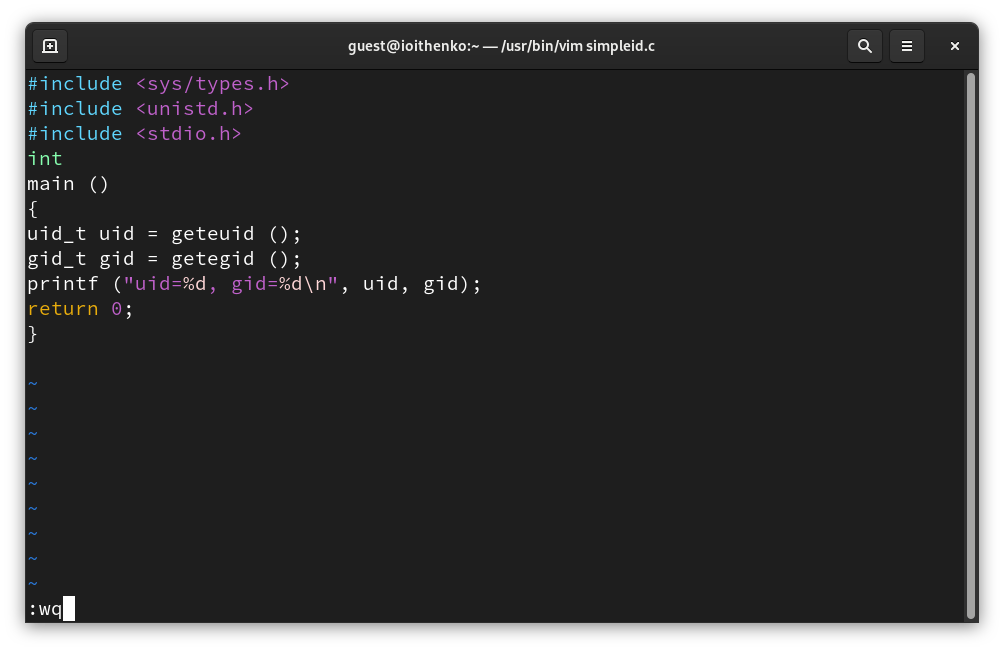


Рис. 1: simpleid.c

Скомплилируем программу и убедимся, что файл программы создан: gcc simpleid.c -o simpleid Выполним программу simpleid: ./simpleid Выполним системную программу id: id и сравним полученный вами результат с данными предыдущего пункта задания. Данные совпадают (рис. 2).

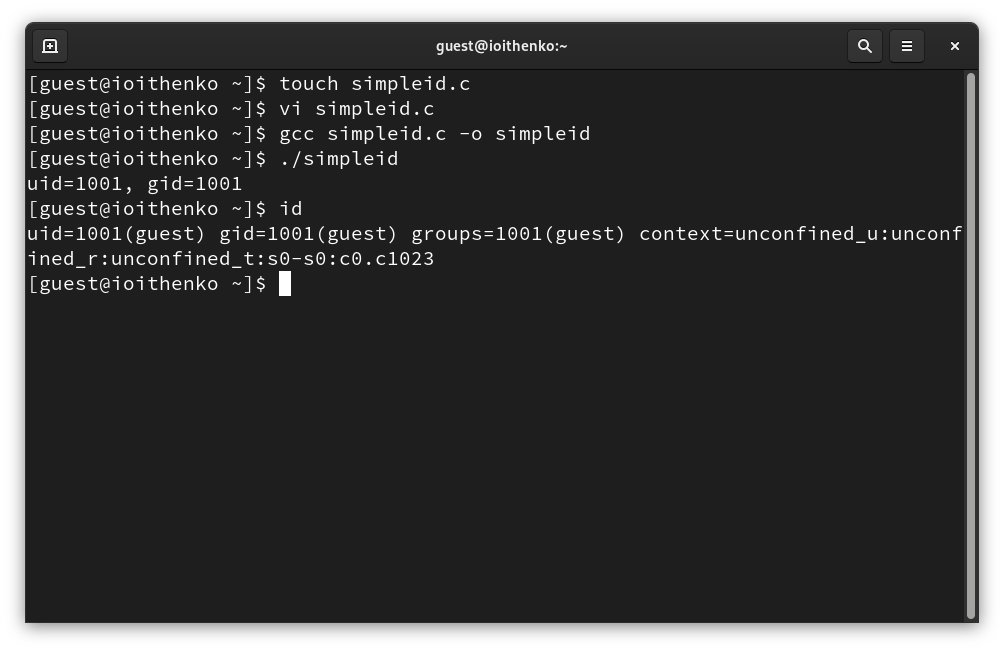


Рис. 2: Выполнение simpleid

Усложним программу, добавив вывод действительных идентификаторов (рис. 3):

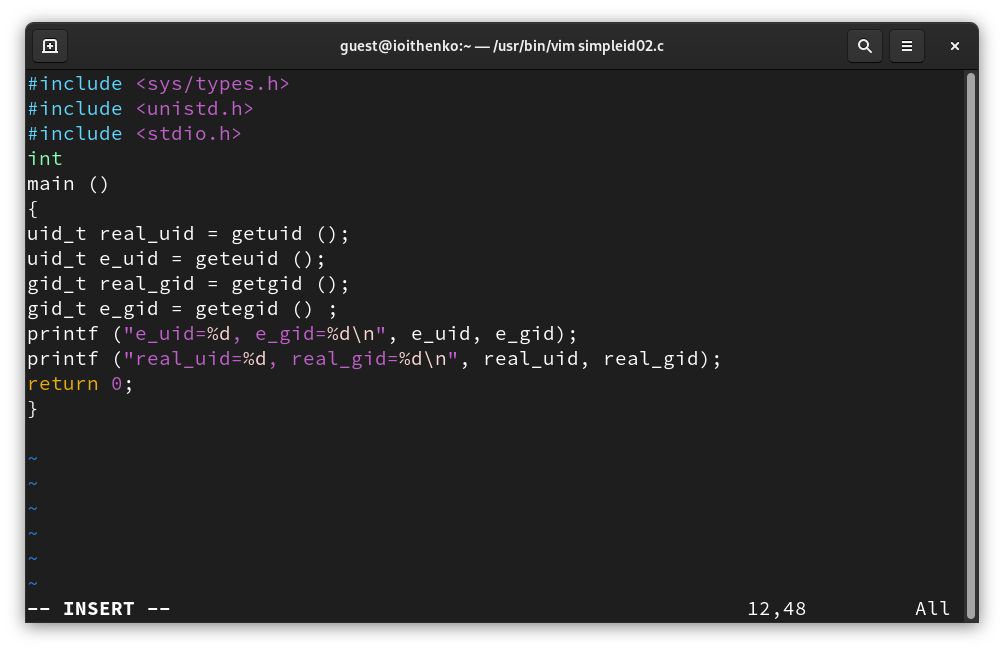


Рис. 3: simpleid02

Скомпилируем и запустим simpleid02.c: gcc simpleid02.c -o simpleid02 ./simpleid2 (рис. 4).



Рис. 4: Выполнение simpleid02

От имени суперпользователя выполниv команды: chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2 Т.е. изменяем владельца файла и добавляем атрибут.

Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid02: ls -l simpleid02 Запустим simpleid02 и id: ./simpleid02 id Сравним результаты. Данные совпадают (рис. 5).

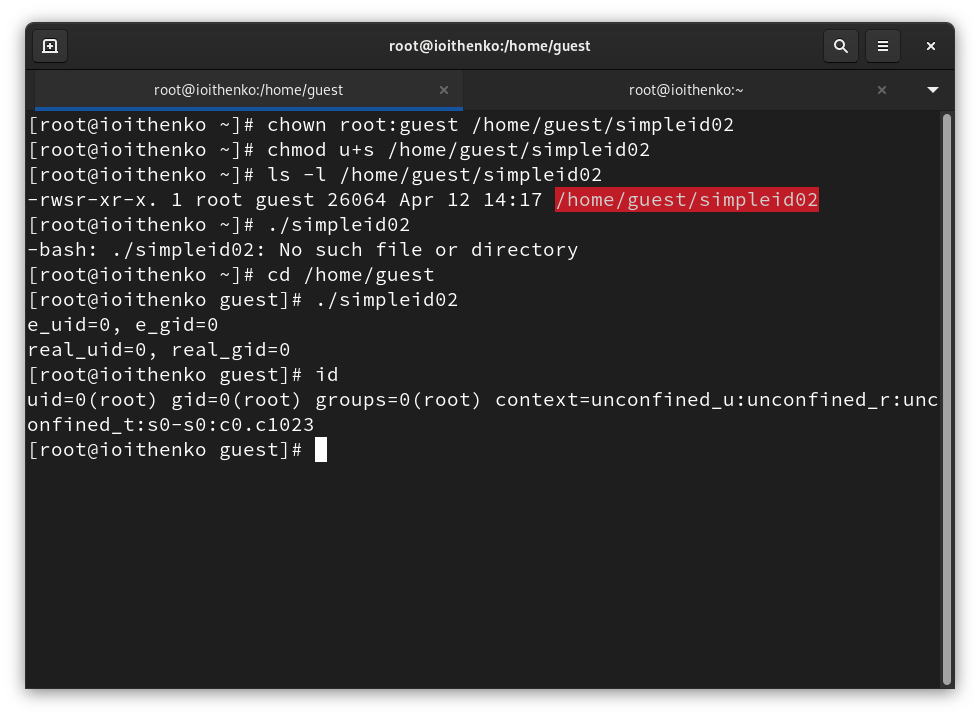


Рис. 5: Смена владельца и атрибут

Создадим программу readfile.c (рис. 6):

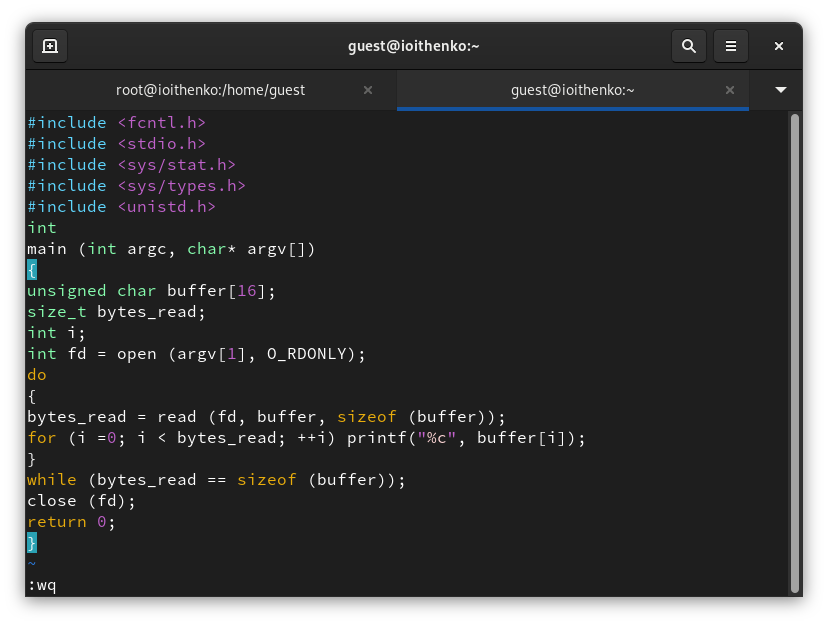


Рис. 6: readfile.c

Откомпилируем её. gcc readfile.c -o readfile

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

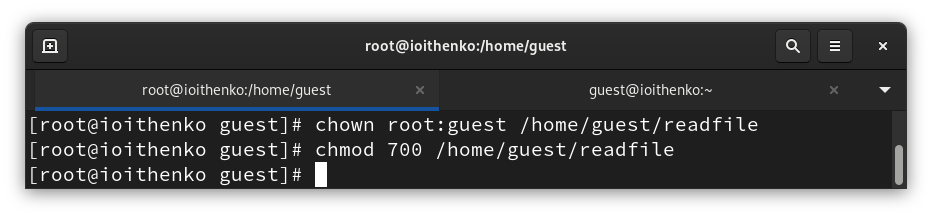


Рис. 7: Изменение владельца и прав

Проверим, что пользователь guest не может прочитать файл readfile.c (рис. 8).

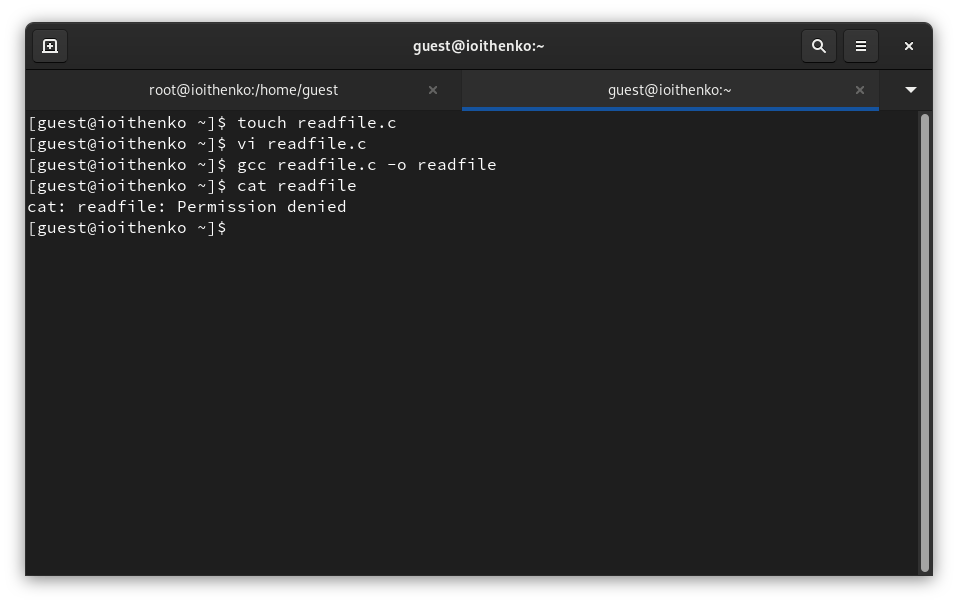


Рис. 8: Отказ в чтении

Сменим у программы readfile владельца и установим SetU’D-бит (рис. 9).

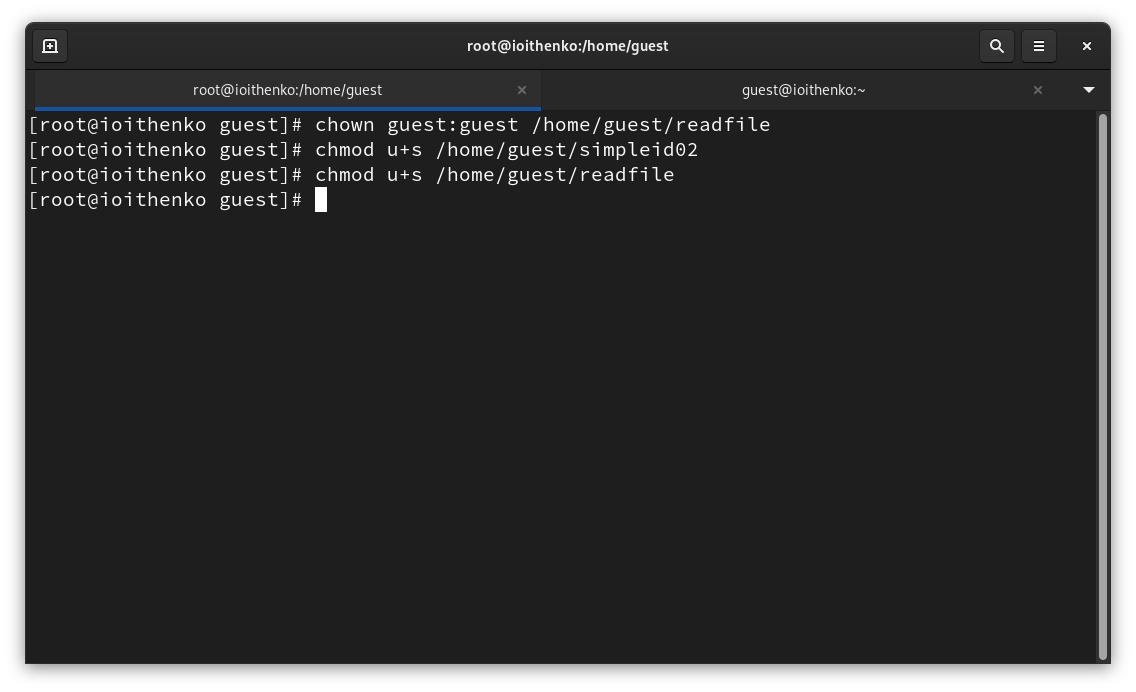


Рис. 9: Смена владельца и атрибута

Проверим, может ли программа readfile прочитать файл readfile.c? Может (рис. 10).

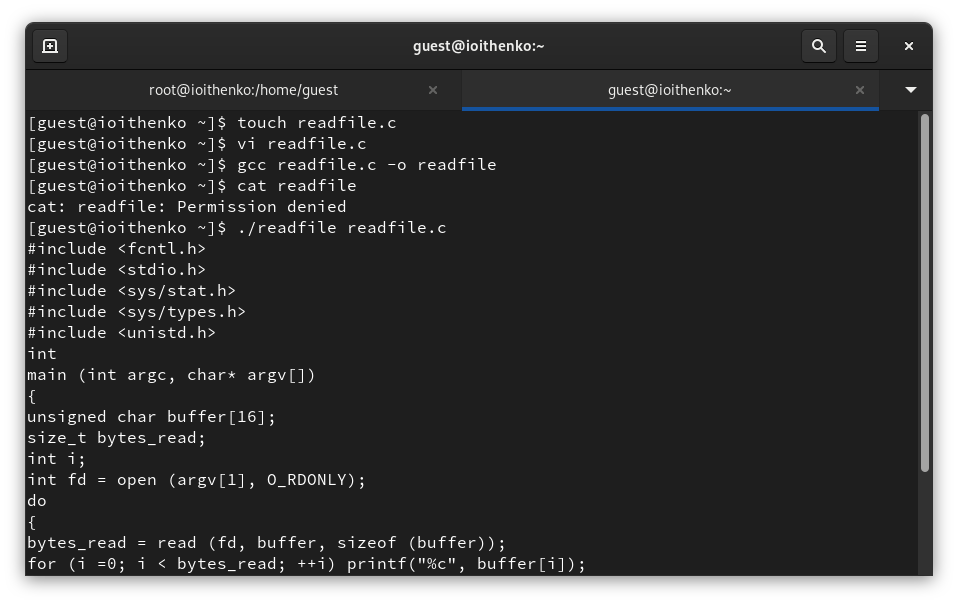


Рис. 10: Выполнение проверки

Проверим, может ли программа readfile прочитать файл /etc/shadow? Может (рис. 11).

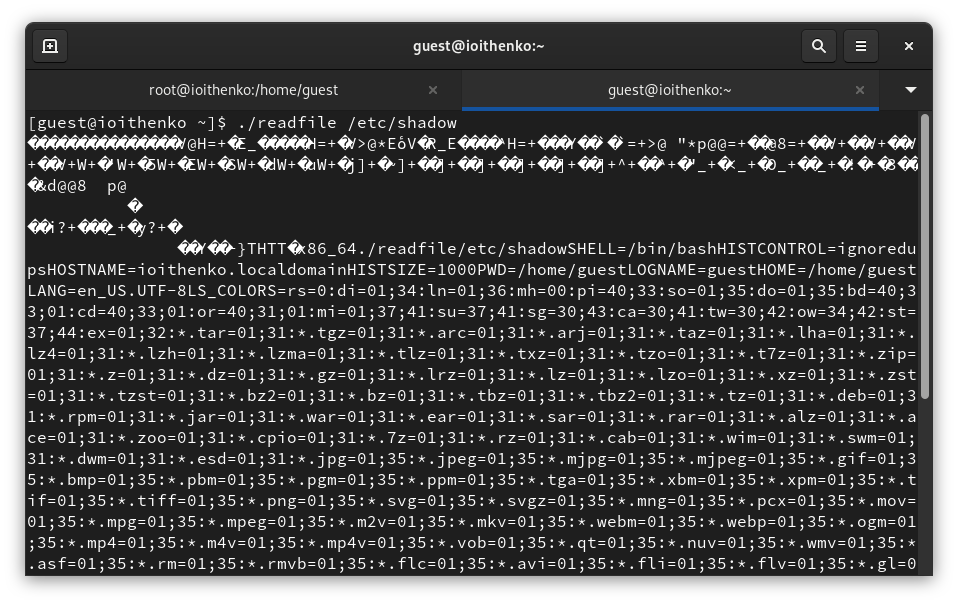


Рис. 11: Выполнение проверки

Выясним, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test: echo “test” > /tmp/file01.txt Просмотрим атрибуты у только что созданного файла и разрешим 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. 12).

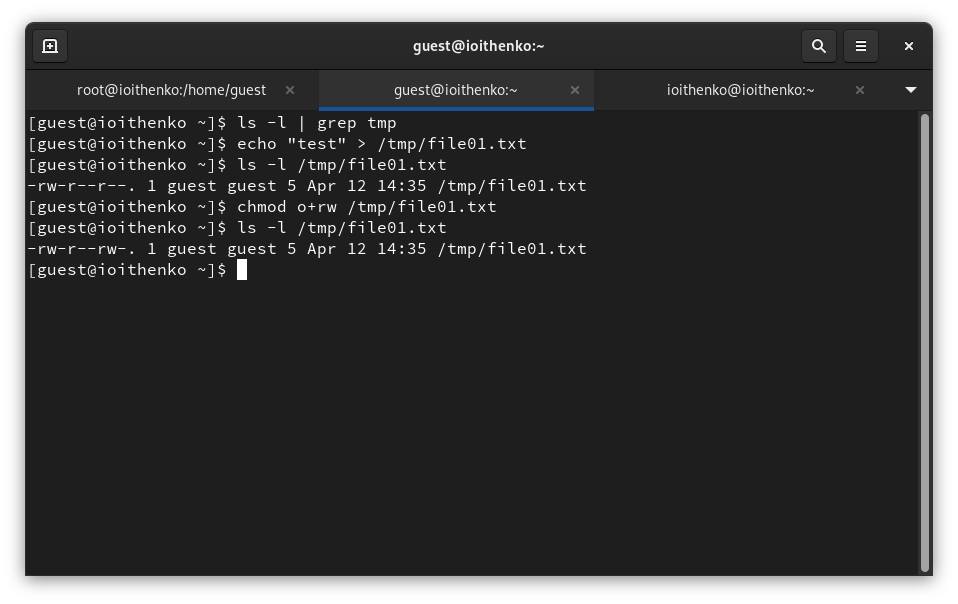


Рис. 12: Права на файл

От пользователя guest2 (не являющегося владельцем) попробуем прочитать файл /tmp/file01.txt: cat /tmp/file01.txt От пользователя guest2 попробуем дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” >> /tmp/file01.txt Удалось ли вам выполнить операцию? Не удалось. Проверим содержимое файла командой cat /tmp/file01.txt От пользователя guest2 попробуем записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt Удалось ли вам выполнить операцию? Не удалось. Проверим содержимое файла командой cat /tmp/file01.txt От пользователя guest2 попробуем удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt Удалось ли вам удалить файл? Не удалось (рис. 13).

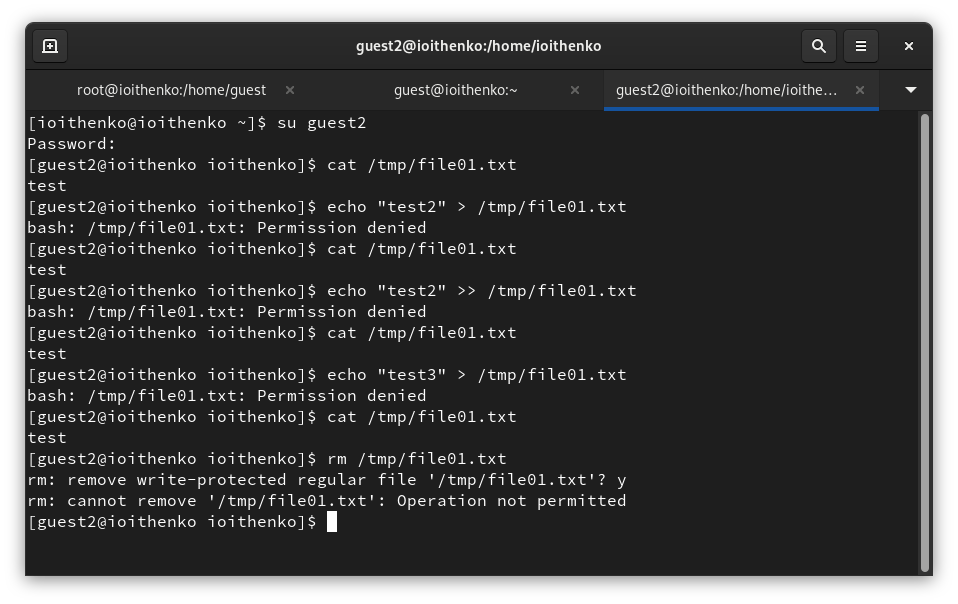


Рис. 13: Проверка атрибута

Повысим свои права до суперпользователя следующей командой su - и выполним после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp Покинем режим суперпользователя командой exit От пользователя guest2 проверим, что атрибута t у директории /tmp нет: ls -l / | grep tmp Повторим предыдущие шаги. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Удалось выполнить только удаление файла, записать и дозаписать не получилось. Повысим свои права до суперпользователя и вернем атрибут t на директорию /tmp (рис. 14): su - chmod +t /tmp exit

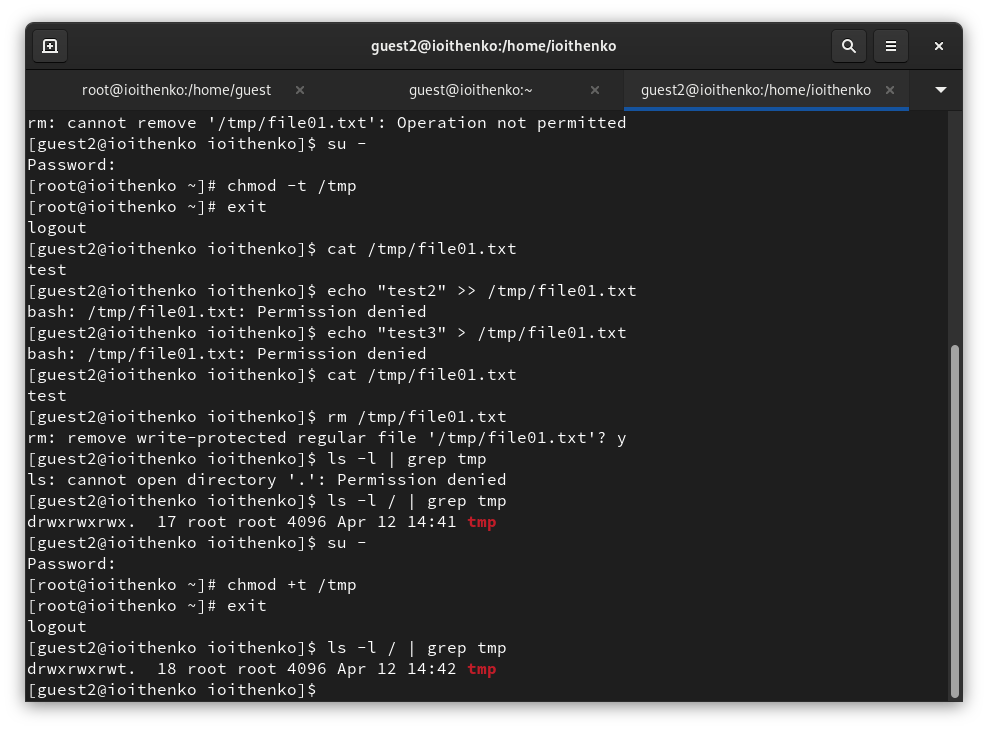


Рис. 14: Проверка снятия атрибута

# 3 Выводы

В ходе лабораторной работы я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыков работы в консоли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. Кулябов Д.С., Королькова А.В., Геворкян М.Н. Информационная безопасность компьютерных сетей. Лабораторные работы, учебное пособие. Москва: РУДН, 2015. 64 с.