Лабораторная работа №5

Основы информационной безопасности

Серёгина Ирина Андреевна

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.

# 2 Выполнение лабораторной работы

1. Проверяю, установлен ли у меня gcc (рис. 1).

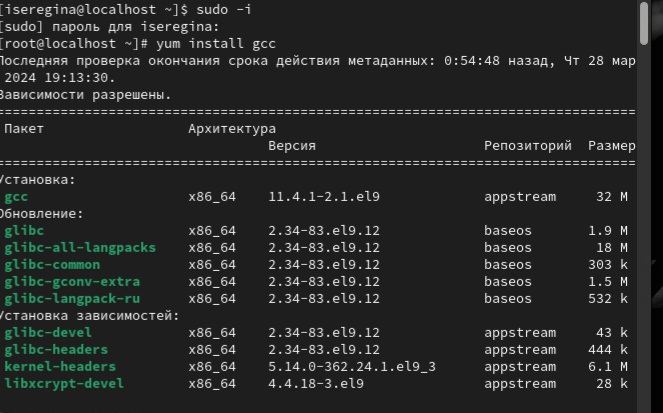


Рис. 1: gcc установлен

1. Отключаю систему запретов до следующей перезагрузки системы (рис. 2).

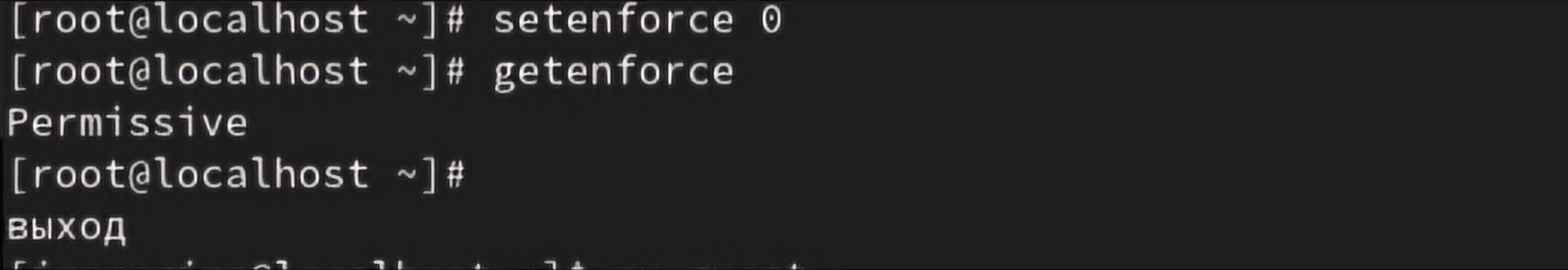


Рис. 2: отключаю систему запретов

1. Вхожу от имени пользователя guest (рис. 3).

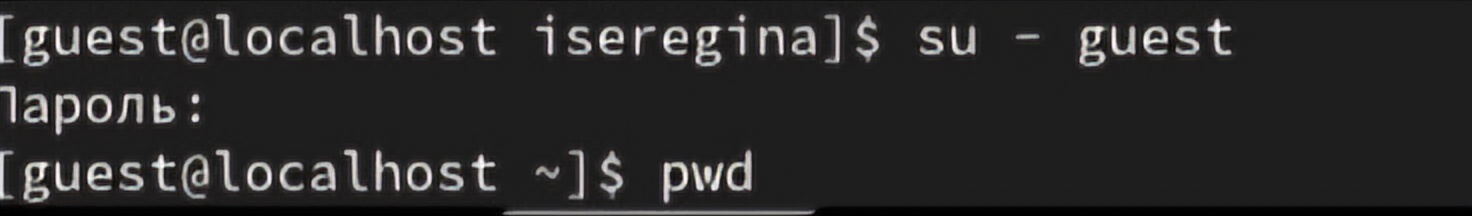


Рис. 3: пользователь guest

1. Создаю программу simpleid.c (рис. 4).

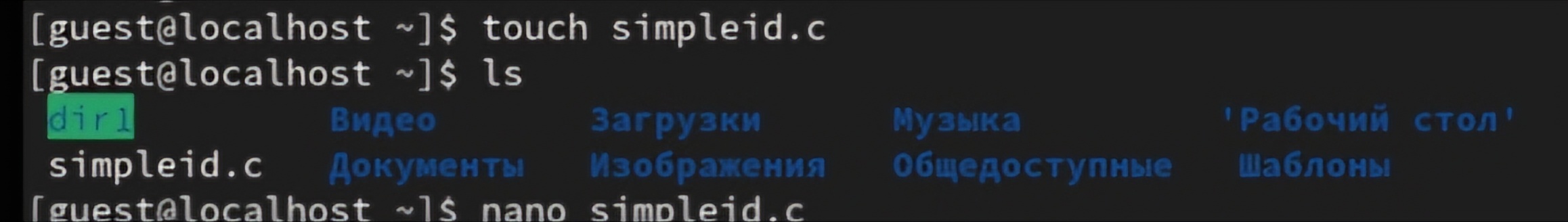


Рис. 4: создание программы

1. Заполняю программу (рис. 5).



Рис. 5: simpleid.c

1. Компилирую файл и выполняю системную программу id (рис. 6).

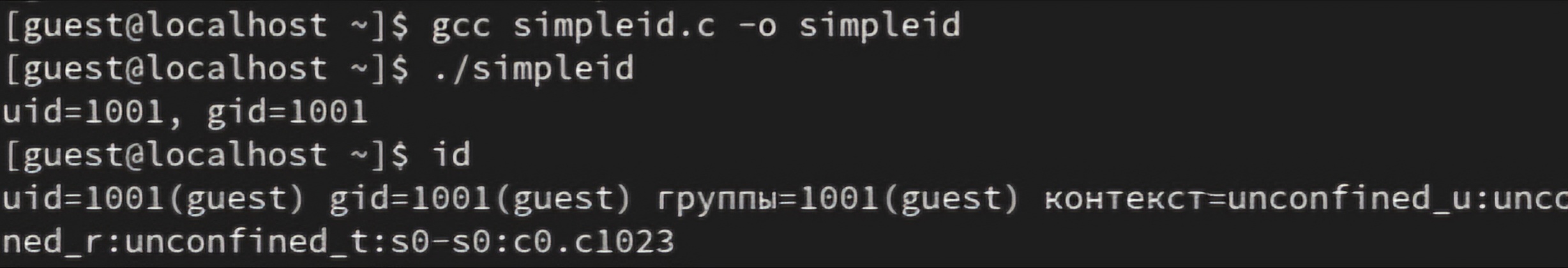


Рис. 6: запускаю программу

1. Усложняю программу (рис. 7).

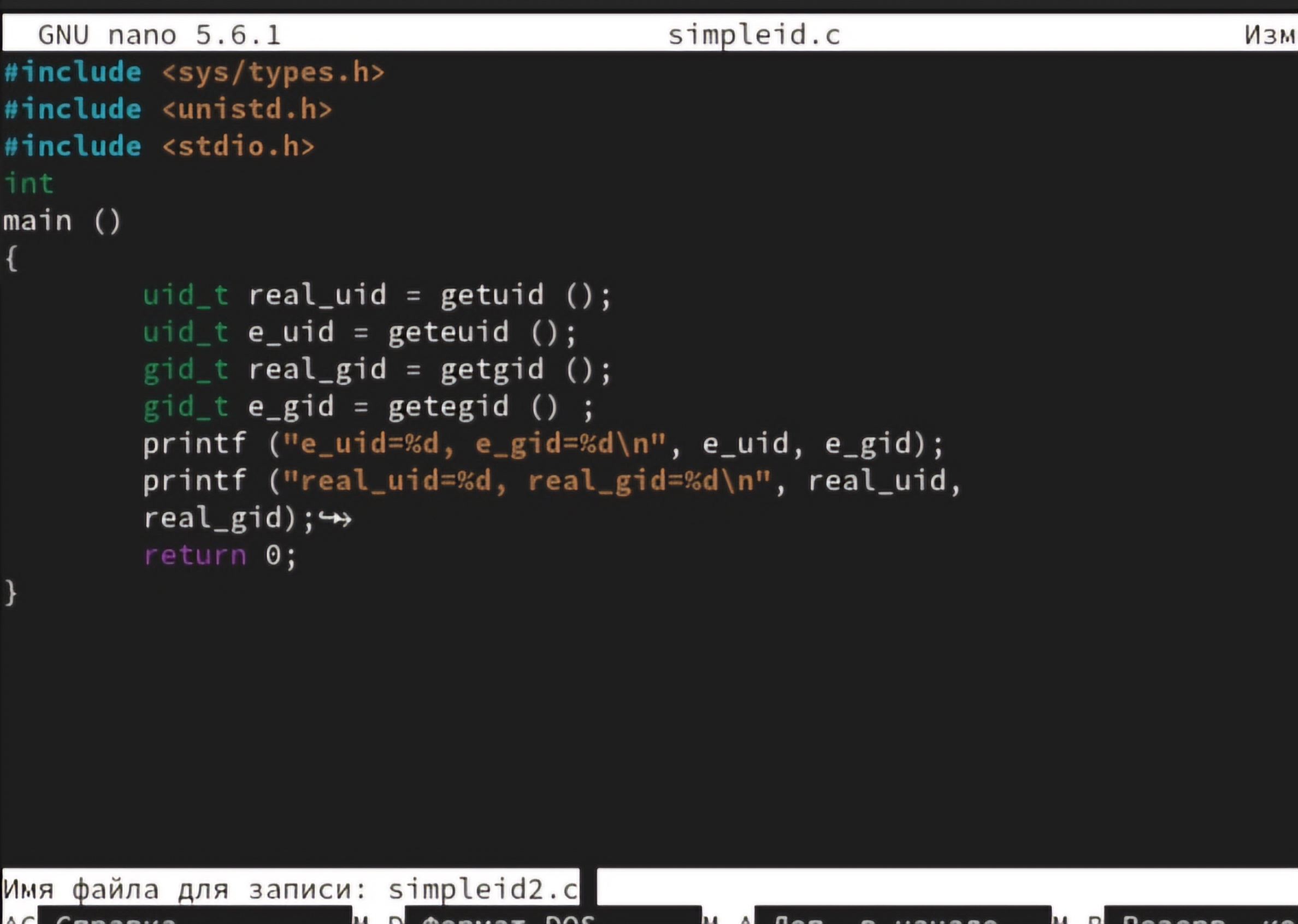


Рис. 7: измененная программа

1. Компилирую и запускаю программу (рис. 8).

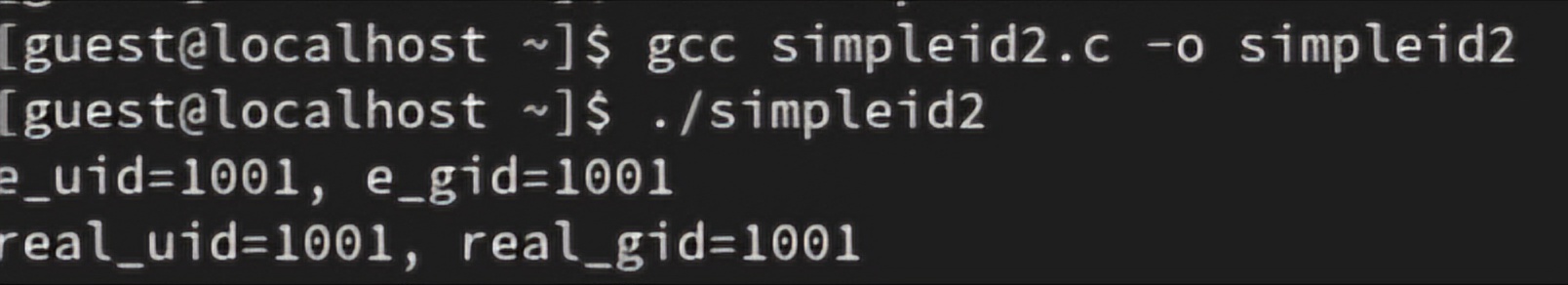


Рис. 8: запускаю программу

1. Выполняю следующие команды от лица суперпользователя, после чего выполняю проверку правильности запуска (рис. 9).

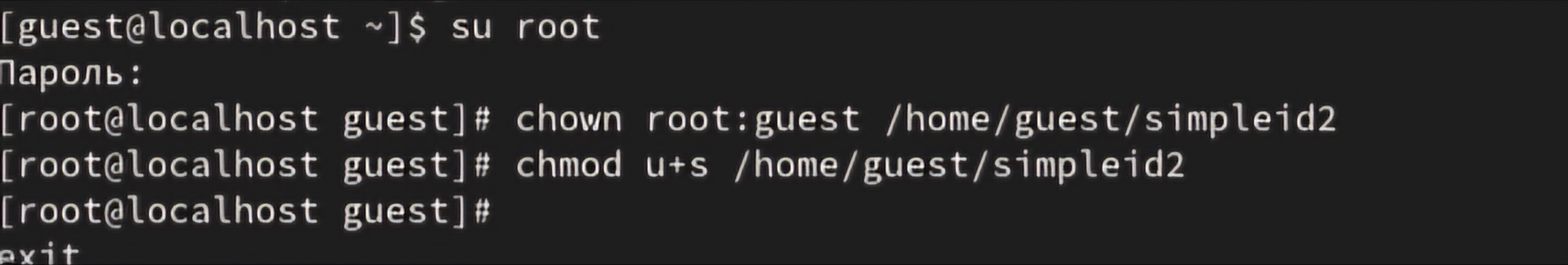


Рис. 9: выполняю команды от имени суперпользователя

1. Запускаю simpleid и id (рис. 10).

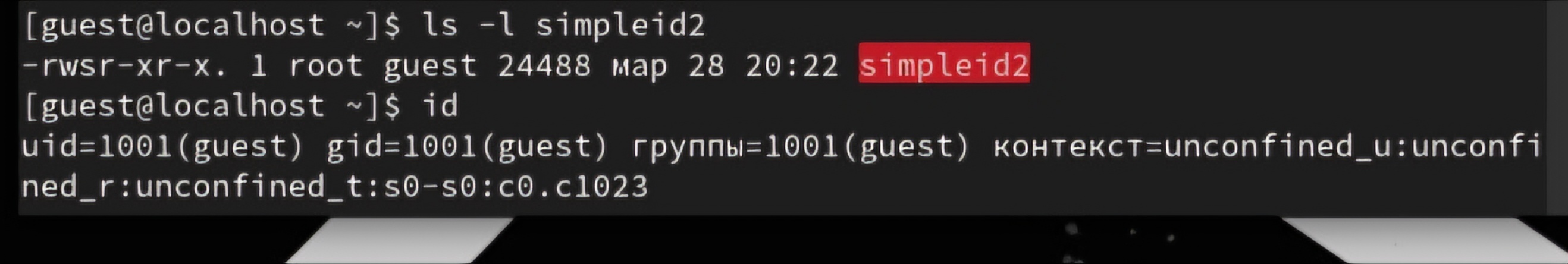


Рис. 10: simpleid.c и id

1. Создаю программу readfile.c, компилирую её (рис. 11).



Рис. 11: readfile.c

1. Меняю владельца файла, чтобы прочитать можно было только от лица суперпользователя (рис. 12).

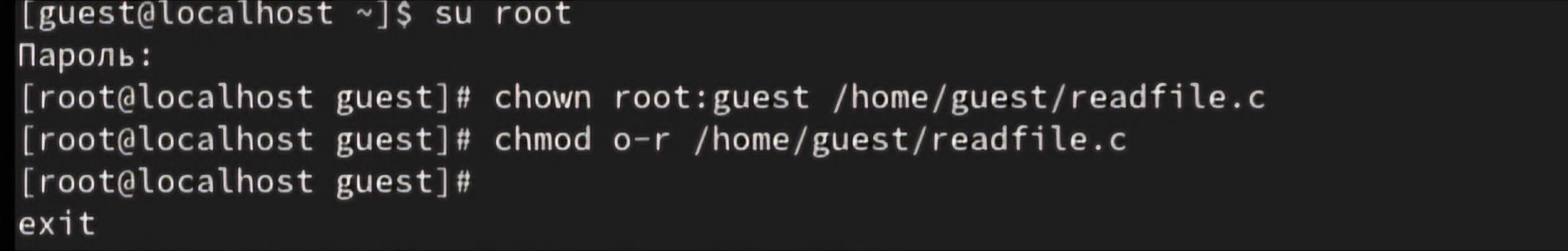


Рис. 12: меняю владельца файла

1. Readfile может прочитать файл /etc/shadow (рис. 13).

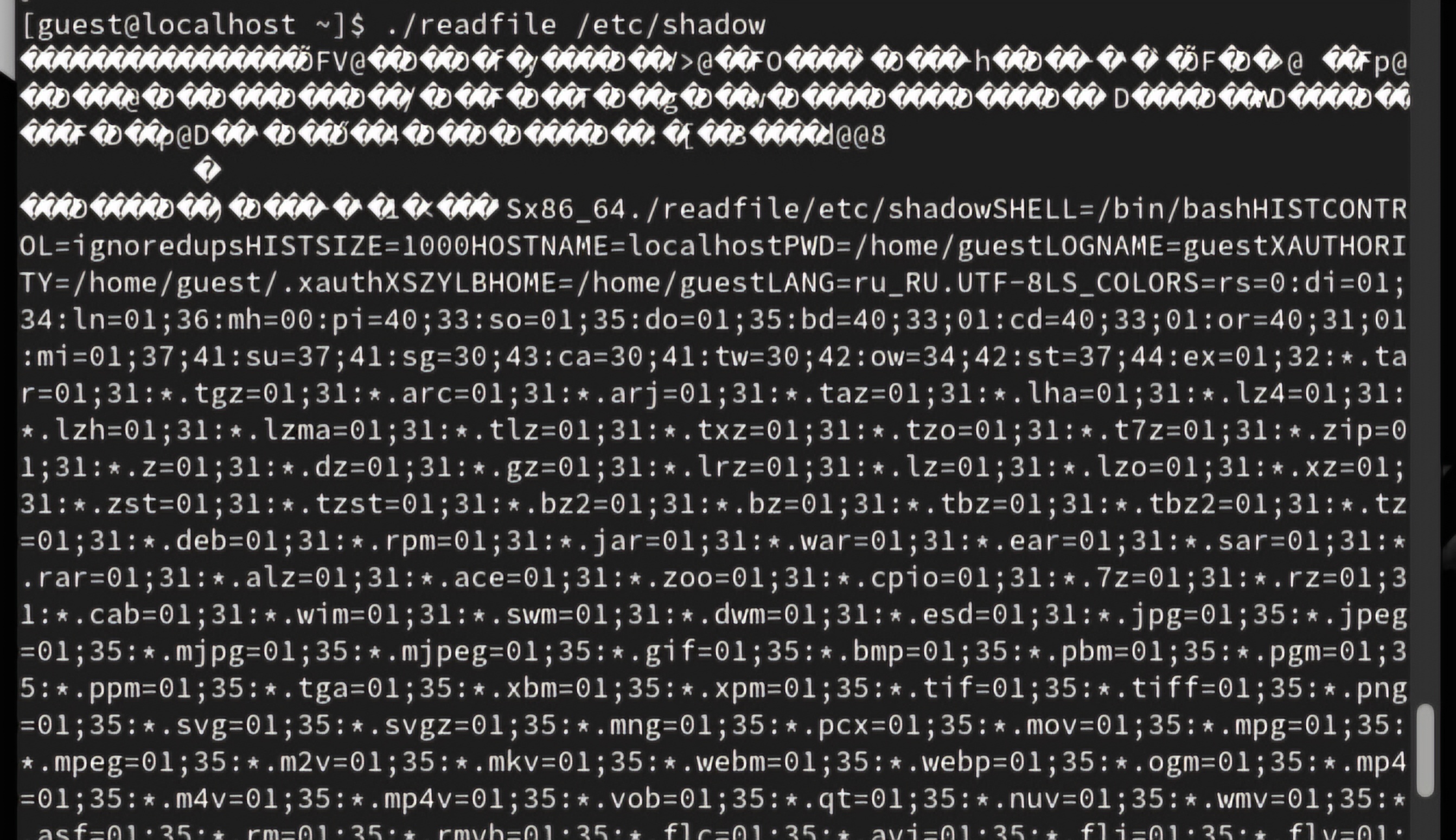


Рис. 13: /etc/shadow

1. Выясняю, установлен ли атрибут sticky на /tmp, создаю файл file01.txt, просматриваю его атрибуты (рис. 14).

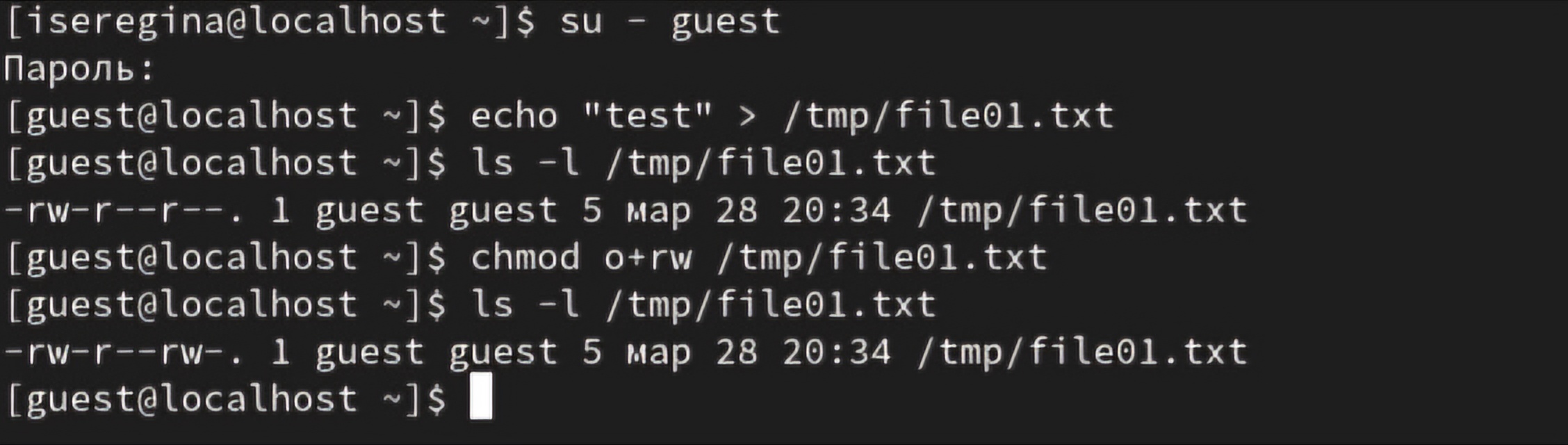


Рис. 14: проверяю наличие атрибута

1. От имени пользователя, не являющегося владельцем пробую прочитать и изменить файл. Не могу также удалить его (рис. **¿fig:015?**).

пробую выполнить действия с файлом

1. От имени суперпользователя убираю атрибут t с директории (рис. 15).

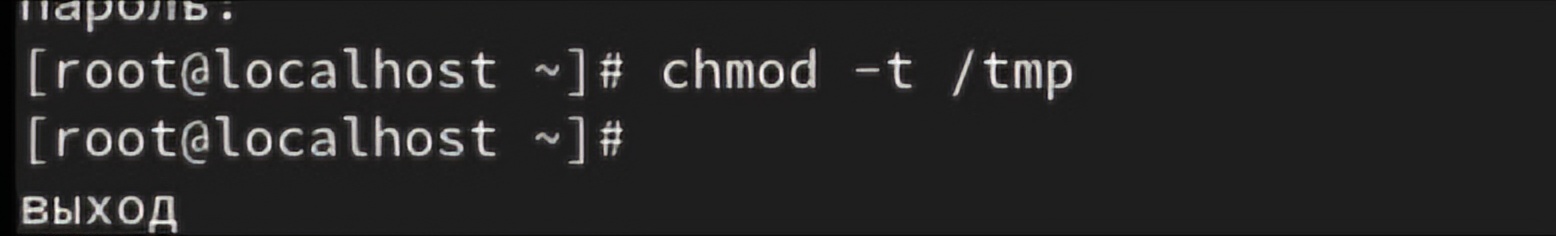


Рис. 15: убираю атрибут с директории

1. Файл удалился (рис. 16).

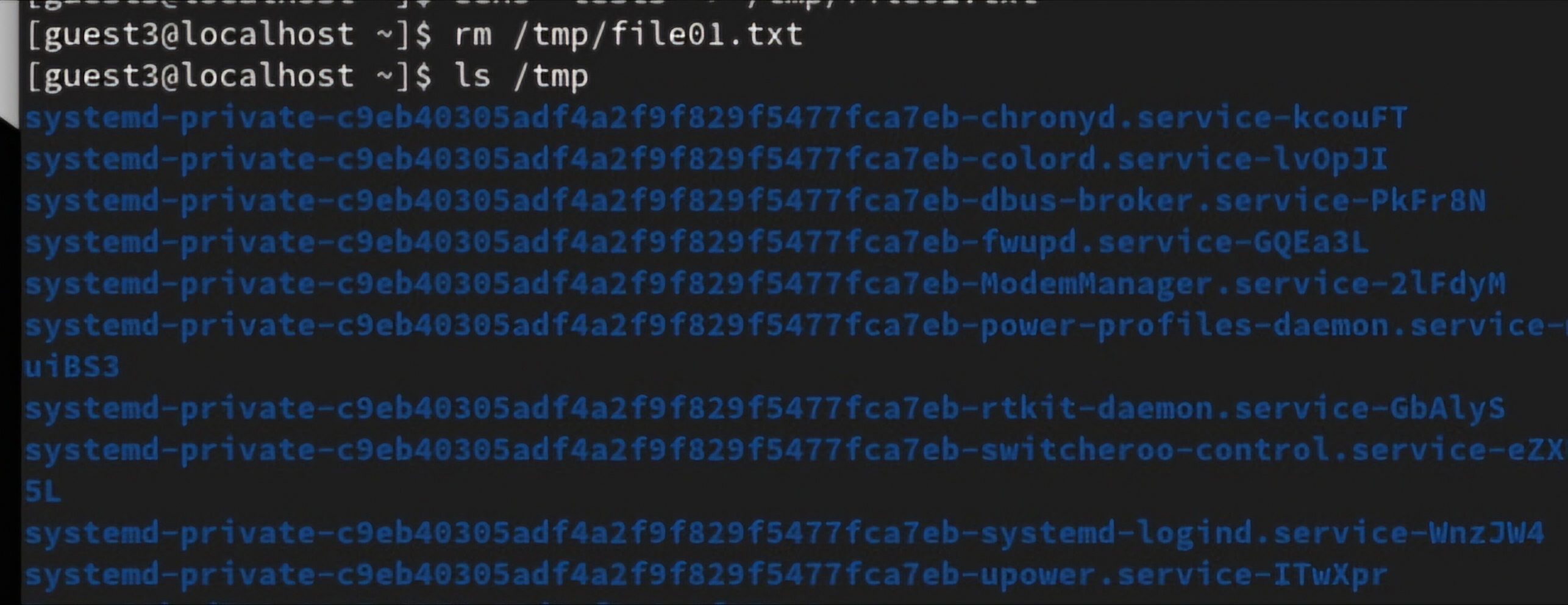


Рис. 16: файл удален

1. Возвращаю атрибут t (рис. 17).

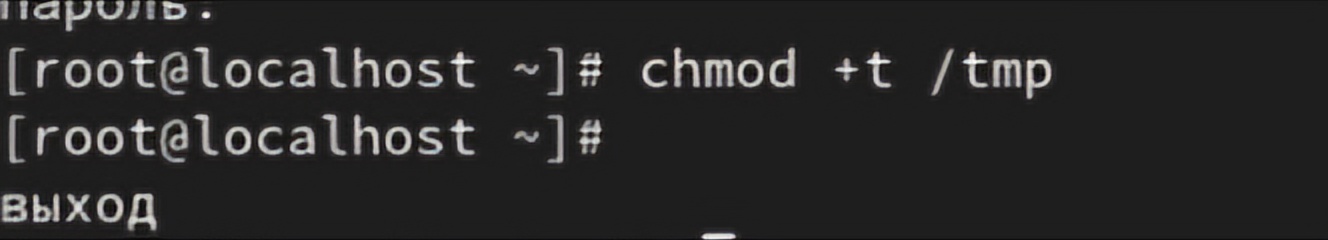


Рис. 17: возвращаю атрибут

# 3 Выводы

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки 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