Информационная безопасность.

Лабораторная работа №5.

Подмогильный Иван Александрович.

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 Задание

1. Выполнить пункты из задания по порядку.

# 3 Выполнение лабораторной работы

Установил gcc с помощью команды yum install gcc

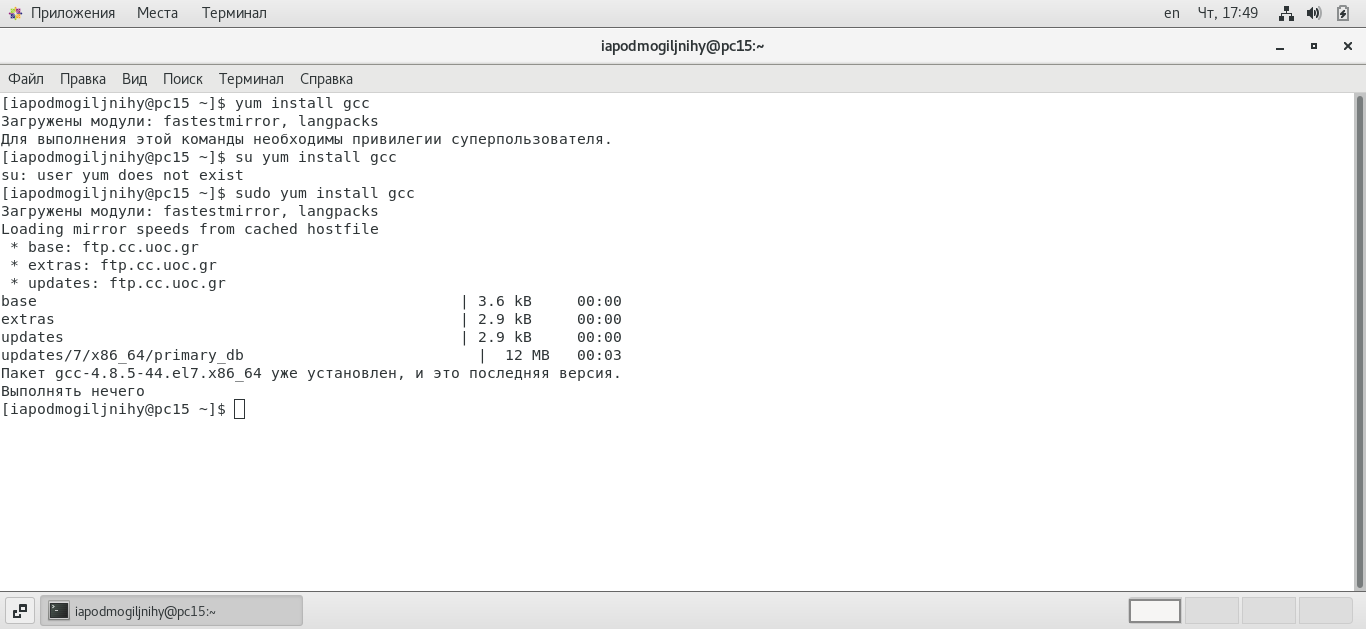


Figure : Установка gcc

Отменил на текущую сессию SELinux командой setenforce 0

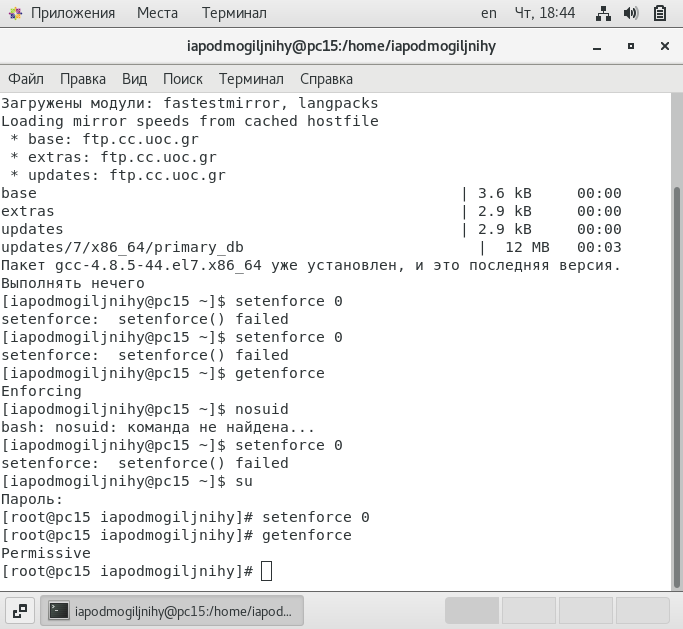


Figure : Отключение SELinux

Вошёл в систему от имени пользователя guest, создал программу simpleid.c

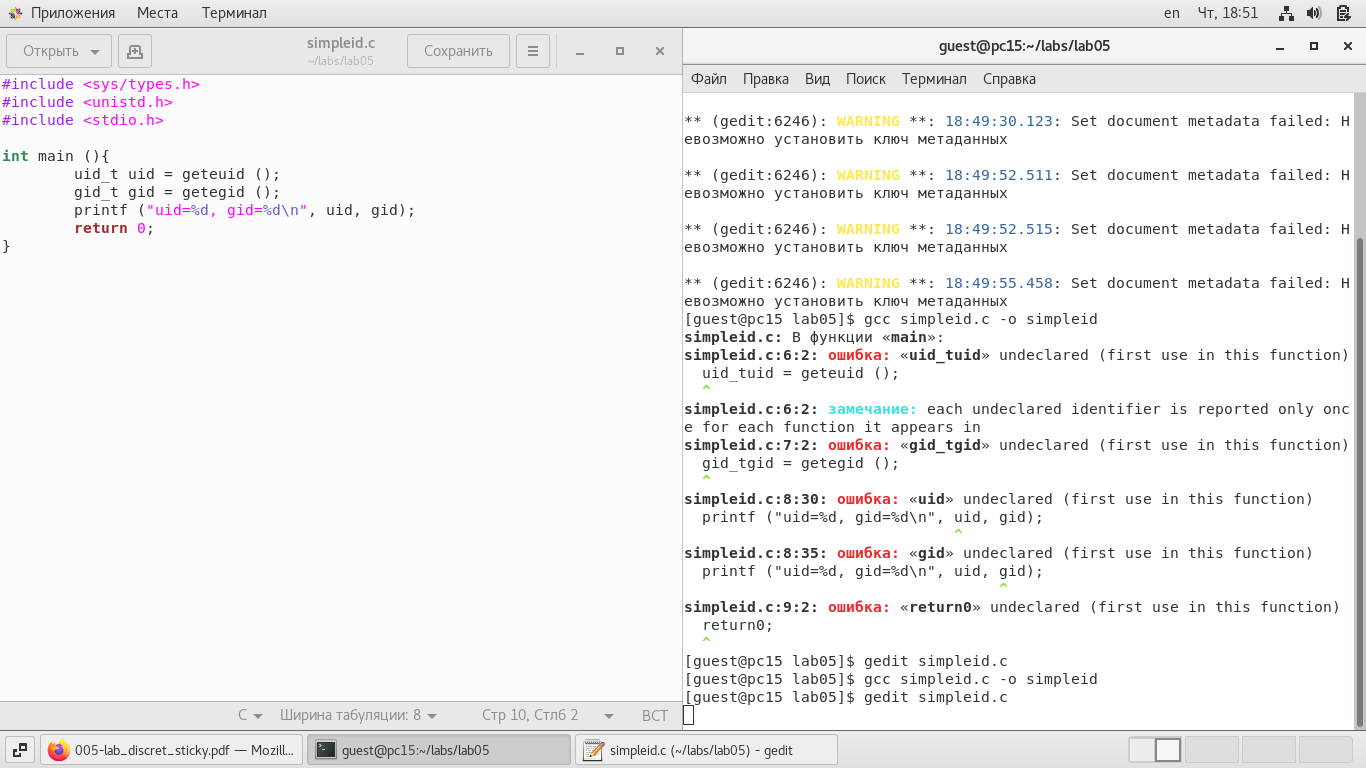


Figure : Создание файла и программы simpleid.c

Скомпилировал программу и убедился, что файл программы создан: gcc simpleid.c -o simpleid

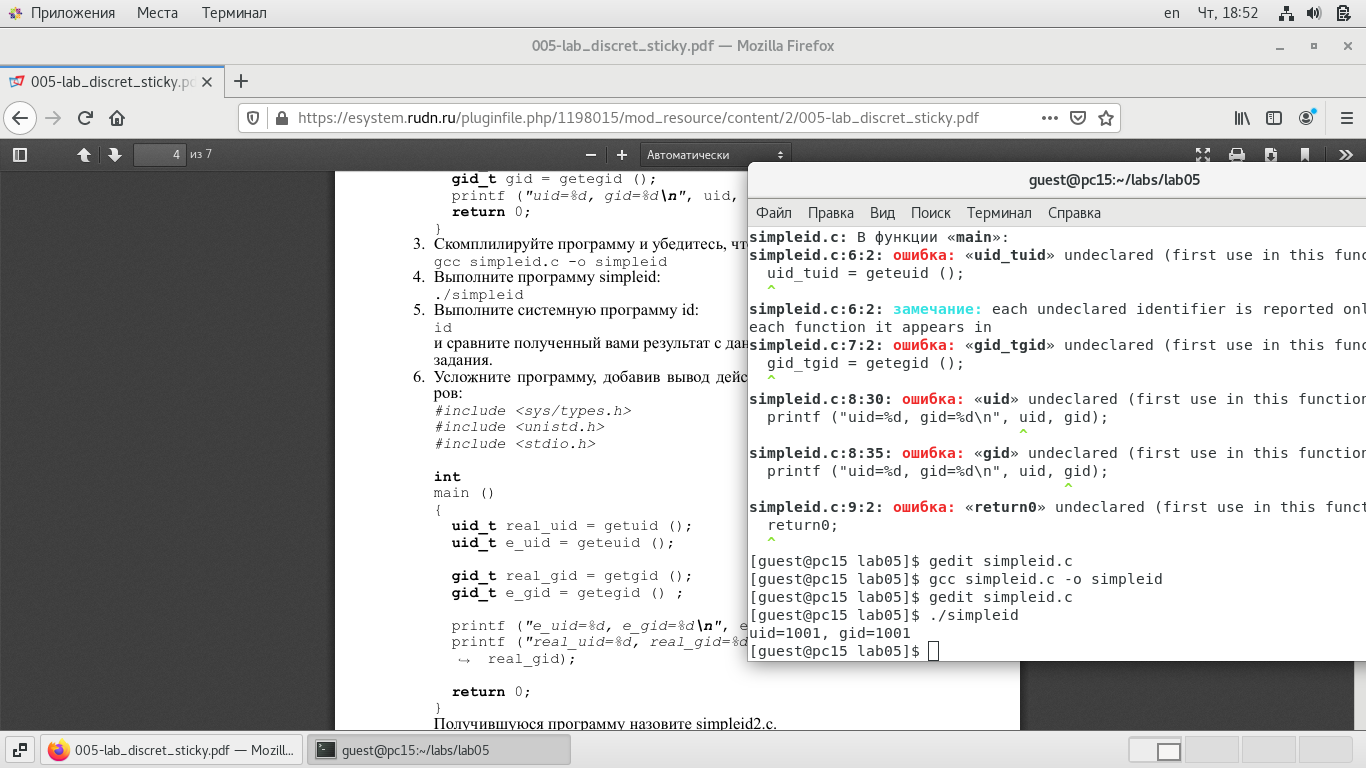


Figure : Комплирование файла

Выполнил программу simpleid: ./simpleid

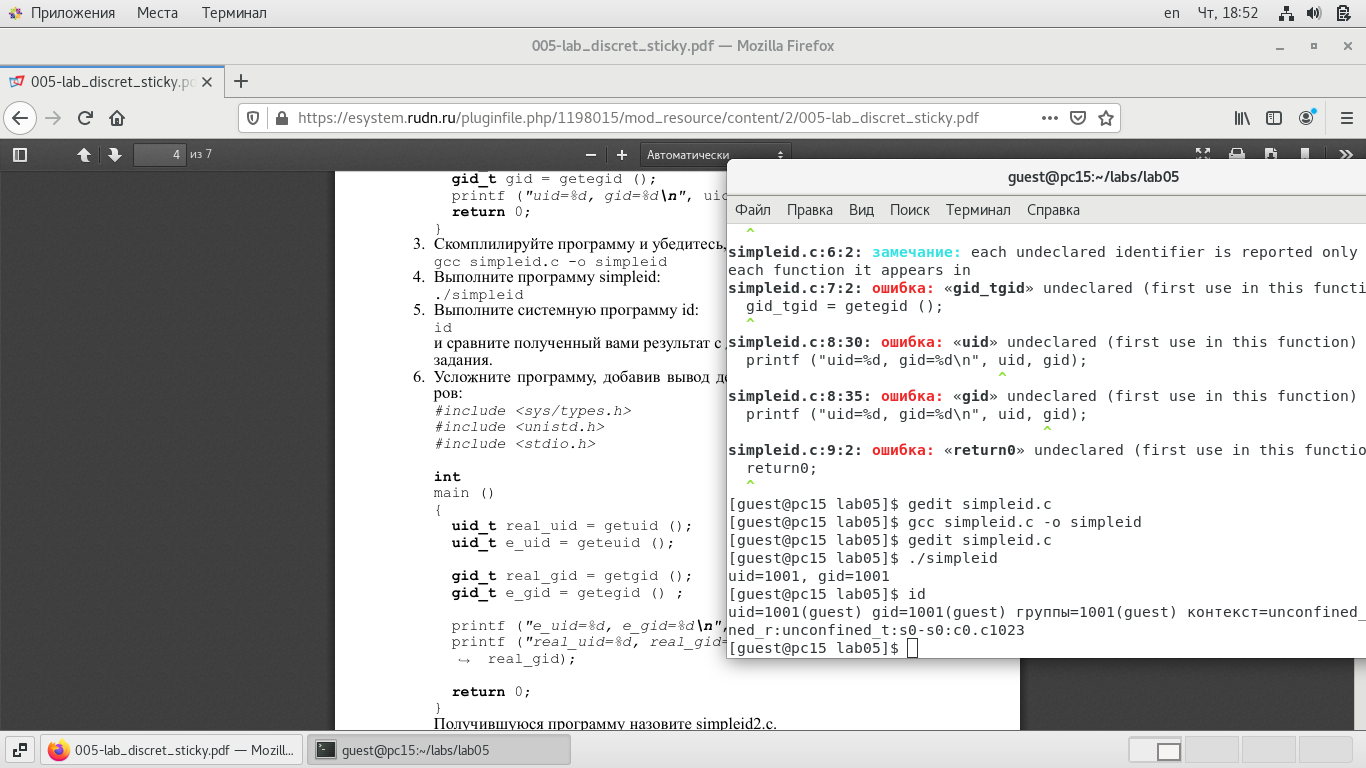


Figure : Выполнение программы simpleid

Выполнил программу id и сравнил полученный результат с данными предыдущего пункта задания. Полученные значения id совпадают

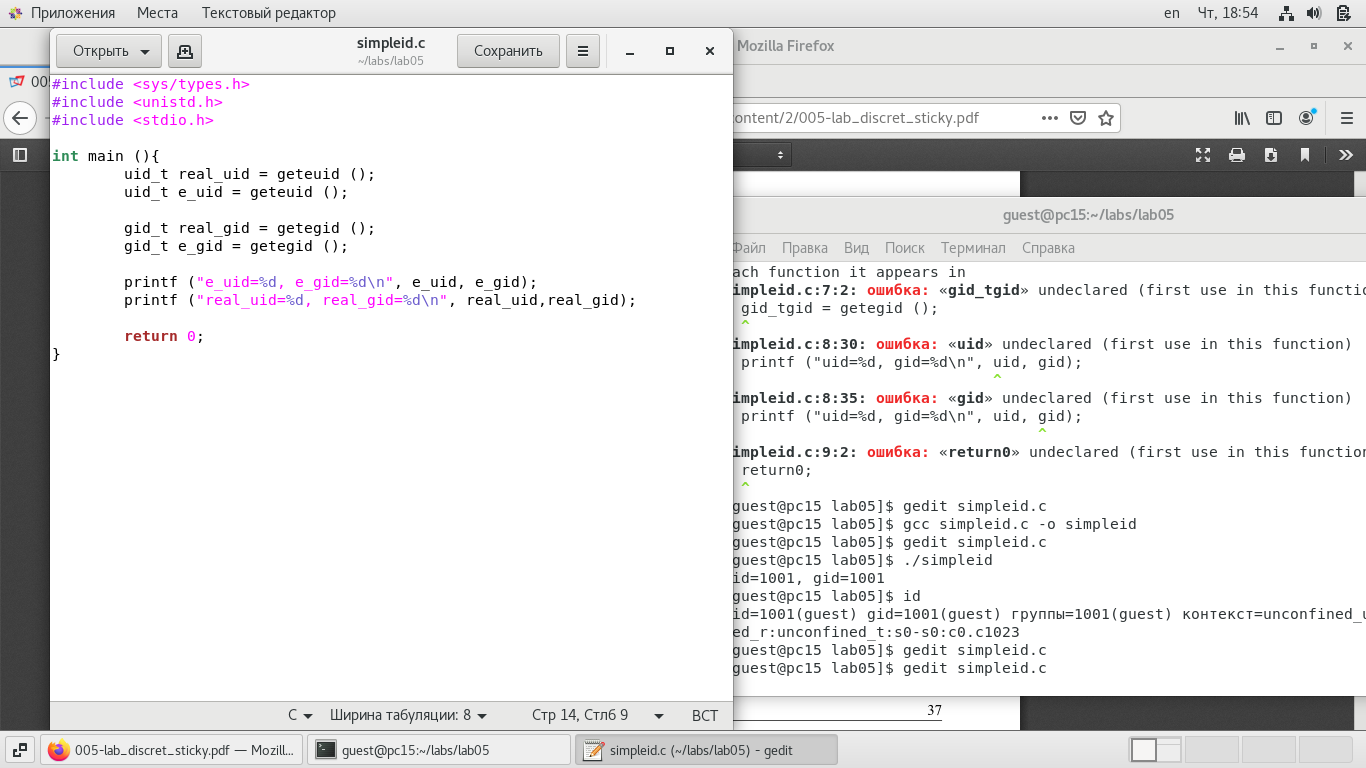


Figure : Выполнение программы id

Усложнил программу, добавив вывод действительных идентификаторов, получившуюися программу назвал simpleid2.c

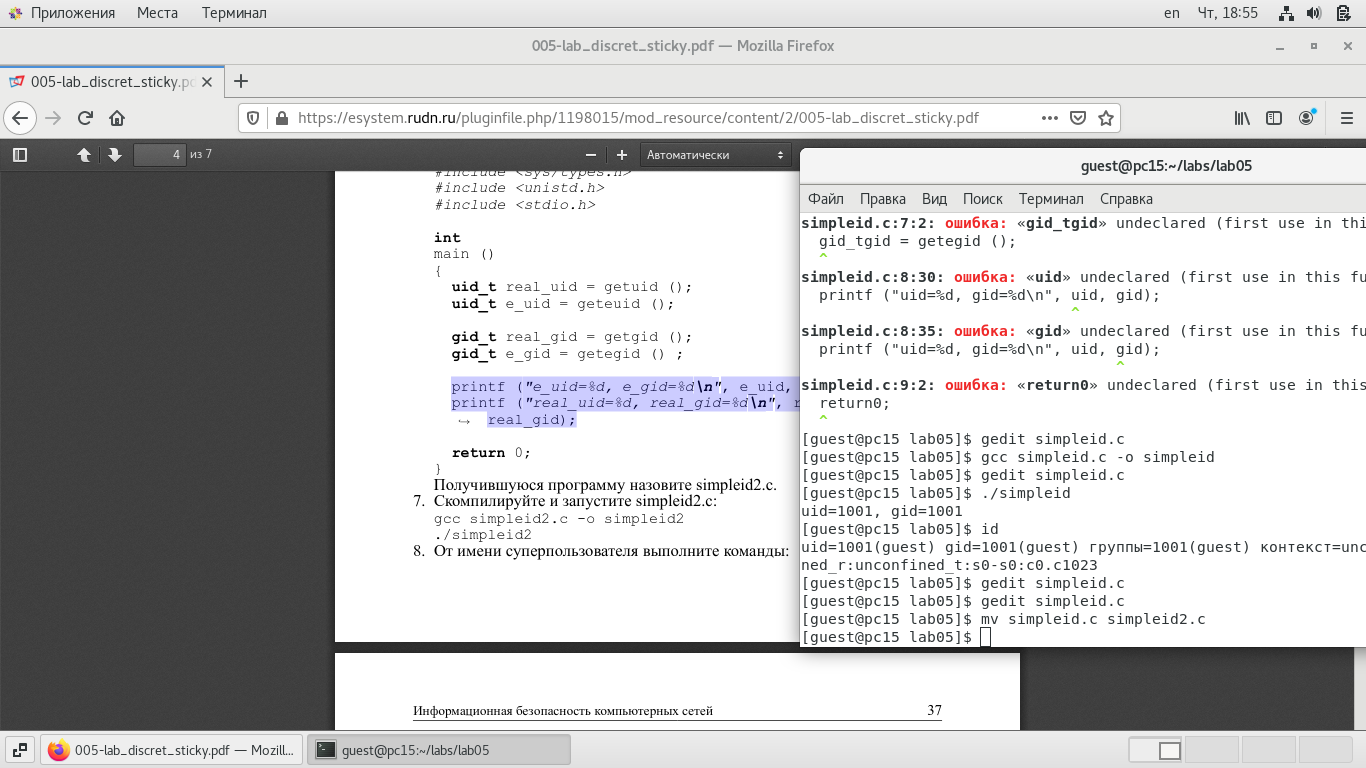


Figure : Усложнение программы

Скомпилировал и запустил simpleid2.c gcc simpleid2.c -o simpleid2, а затем ./simpleid2

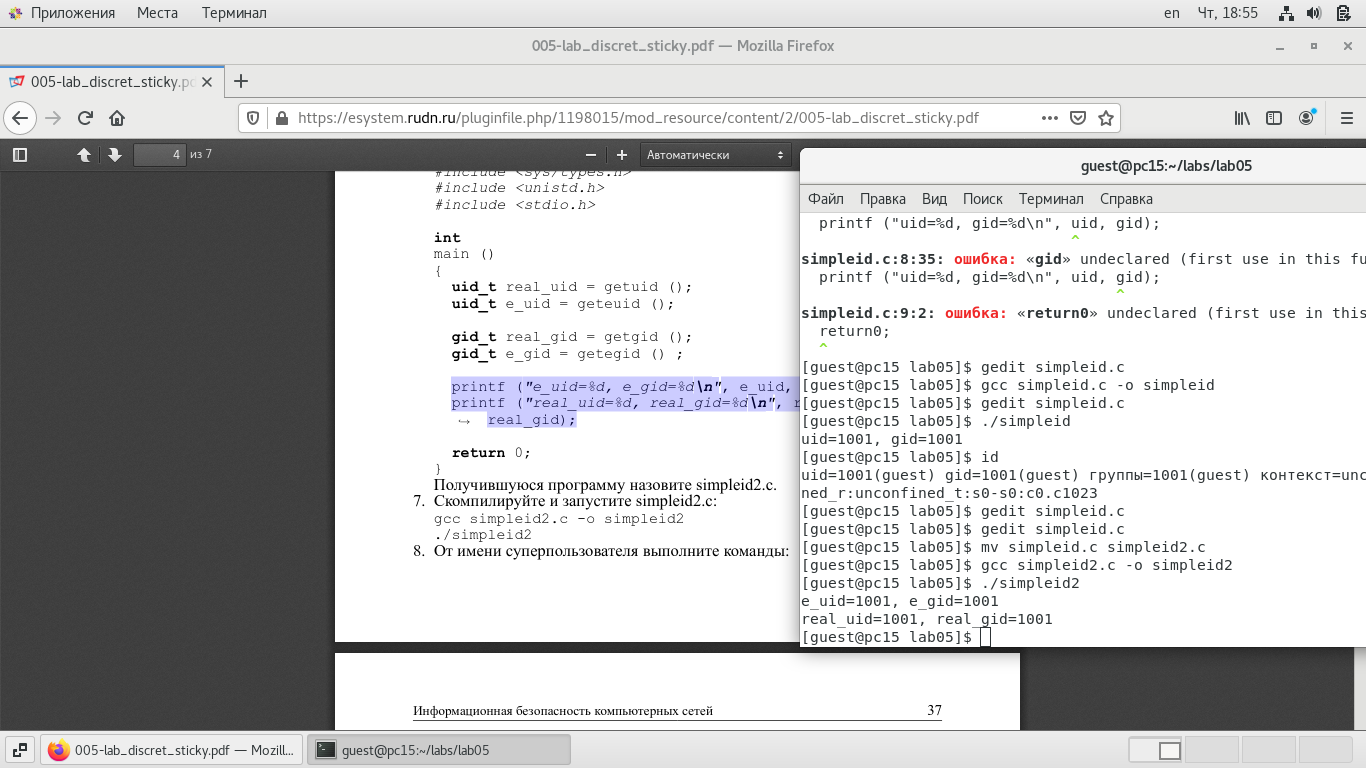


Figure : Компиляция и запуск

От имени суперпользователя выполнил команды: chown root:guest /home/guest/simpleid2, а затем chmod u+s /home/guest/simpleid2. Первая команда изменяет права на файл с guest на root. А затем устанавливает атрибут SetUID, который запускает программу не с правами пользователя, а с правами владельца файла. Затем выполнил проверку изменений с помощью команды ls -l simpleid2

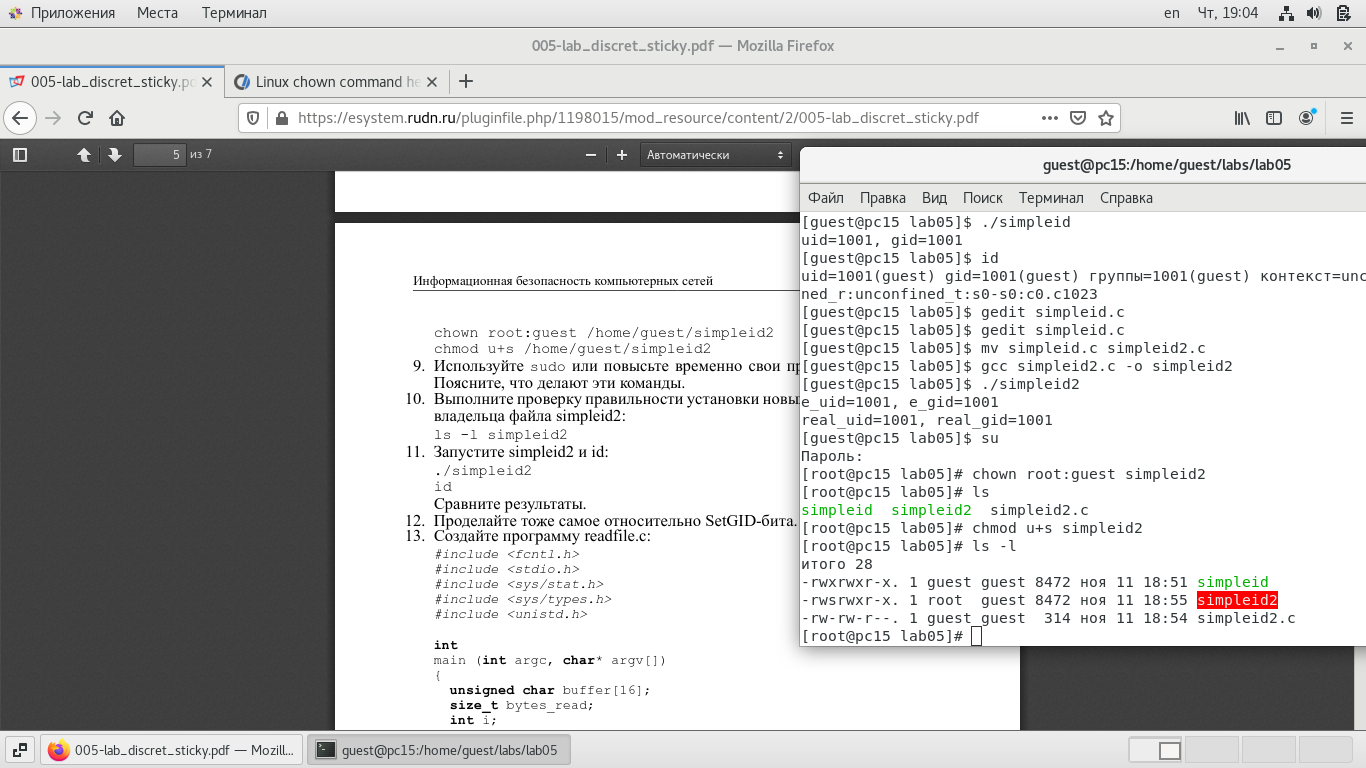


Figure : Добавление SetUID

Запустил simpleid2 и id: ./simpleid2, id. При данном запуску выводы совпадают.

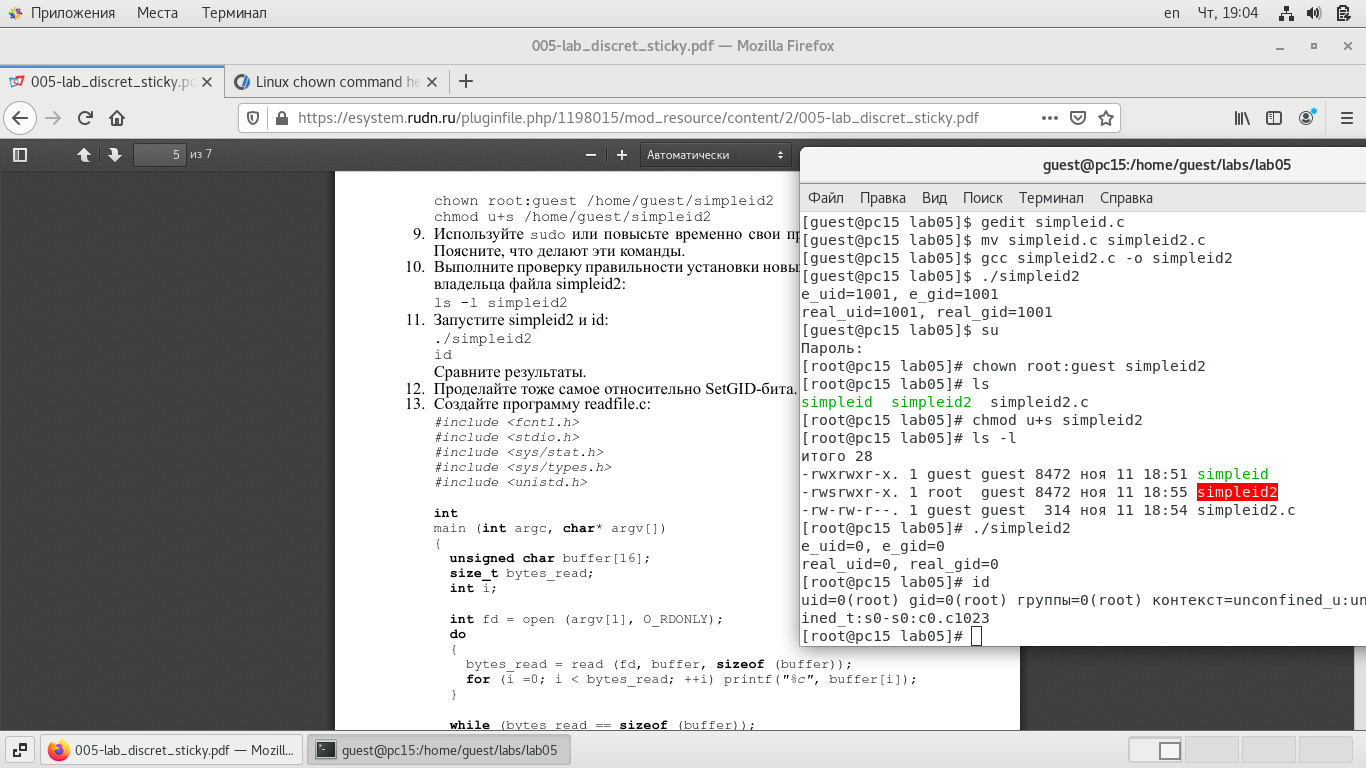


Figure : Действия над файлом.

Проделал то же самое с атрибутом SetGID (установление прав для владеющей группы).

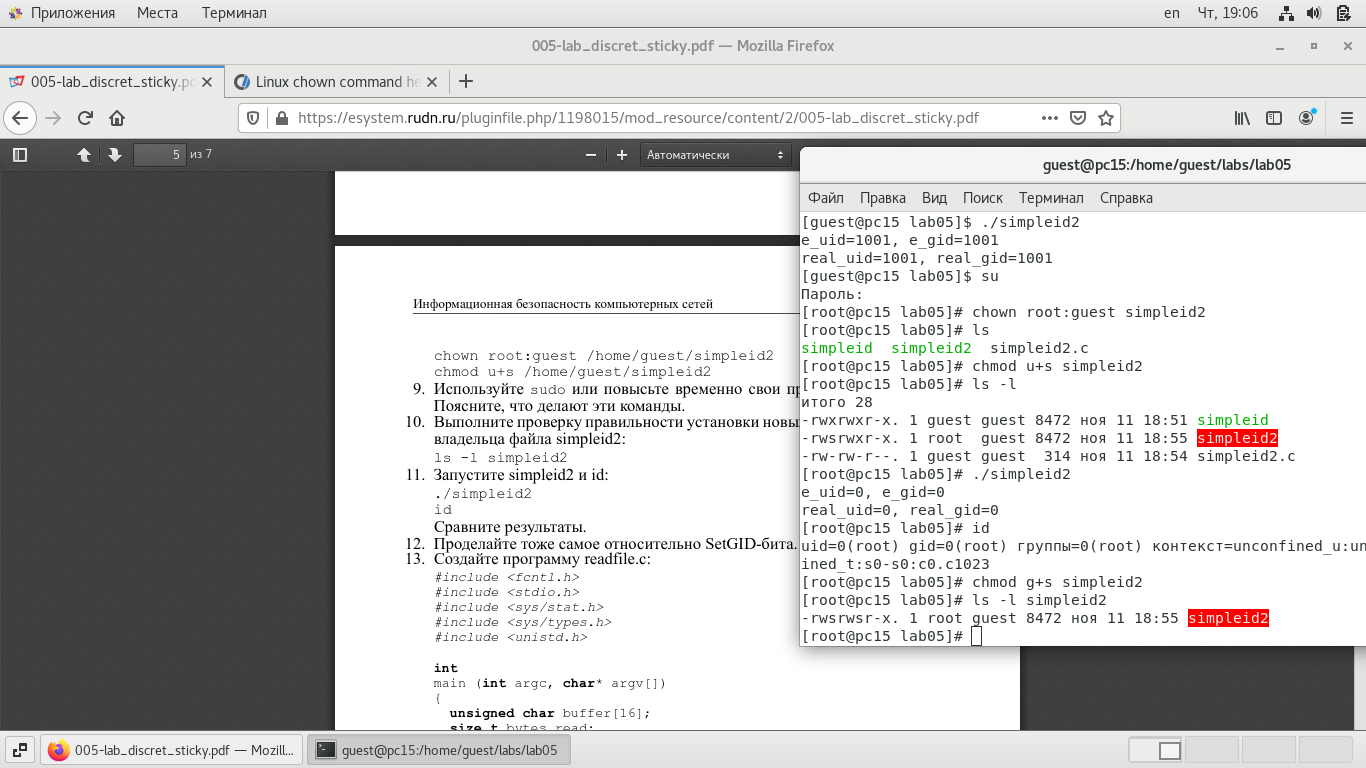


Figure : Установка SetGID

Запустил файл. Теперь выводы для группы различны.

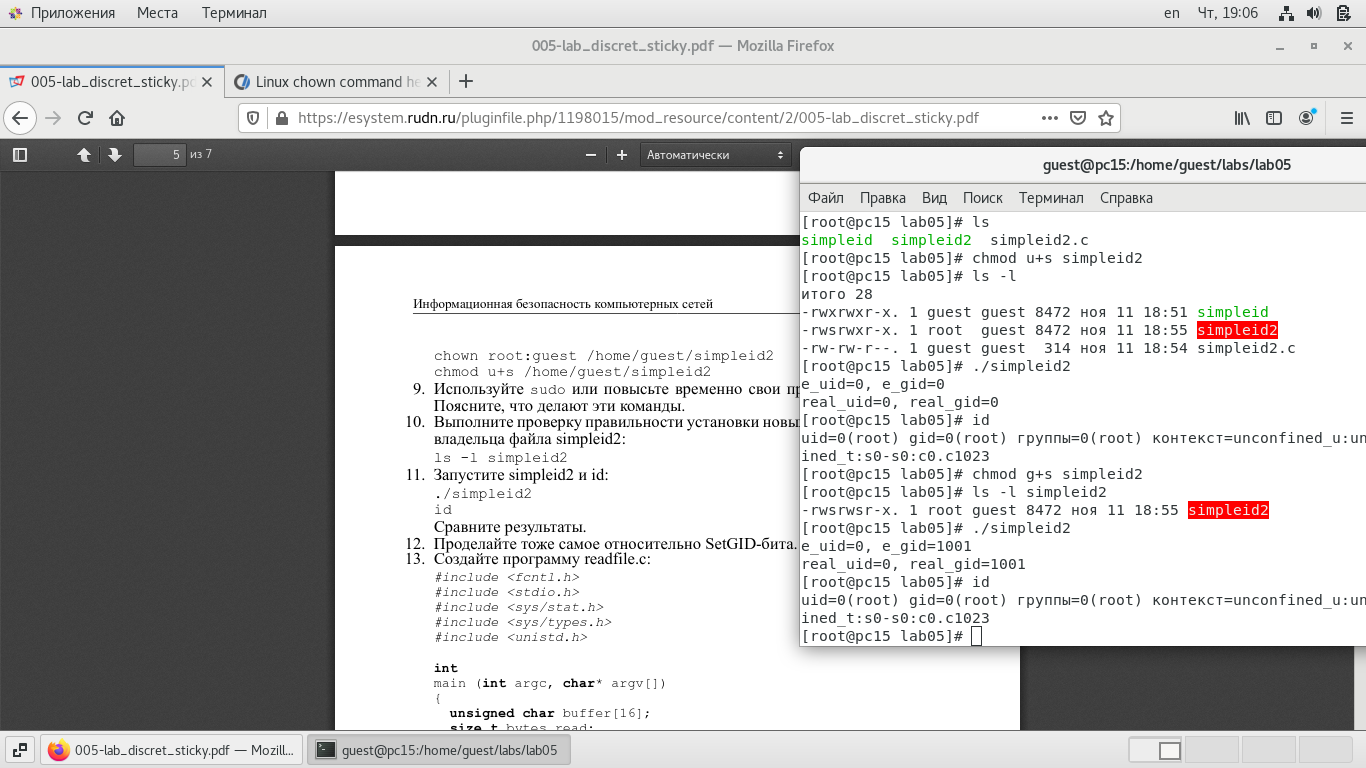


Figure : Запуск программы с установленным SetGID

Создал программу readfile.c

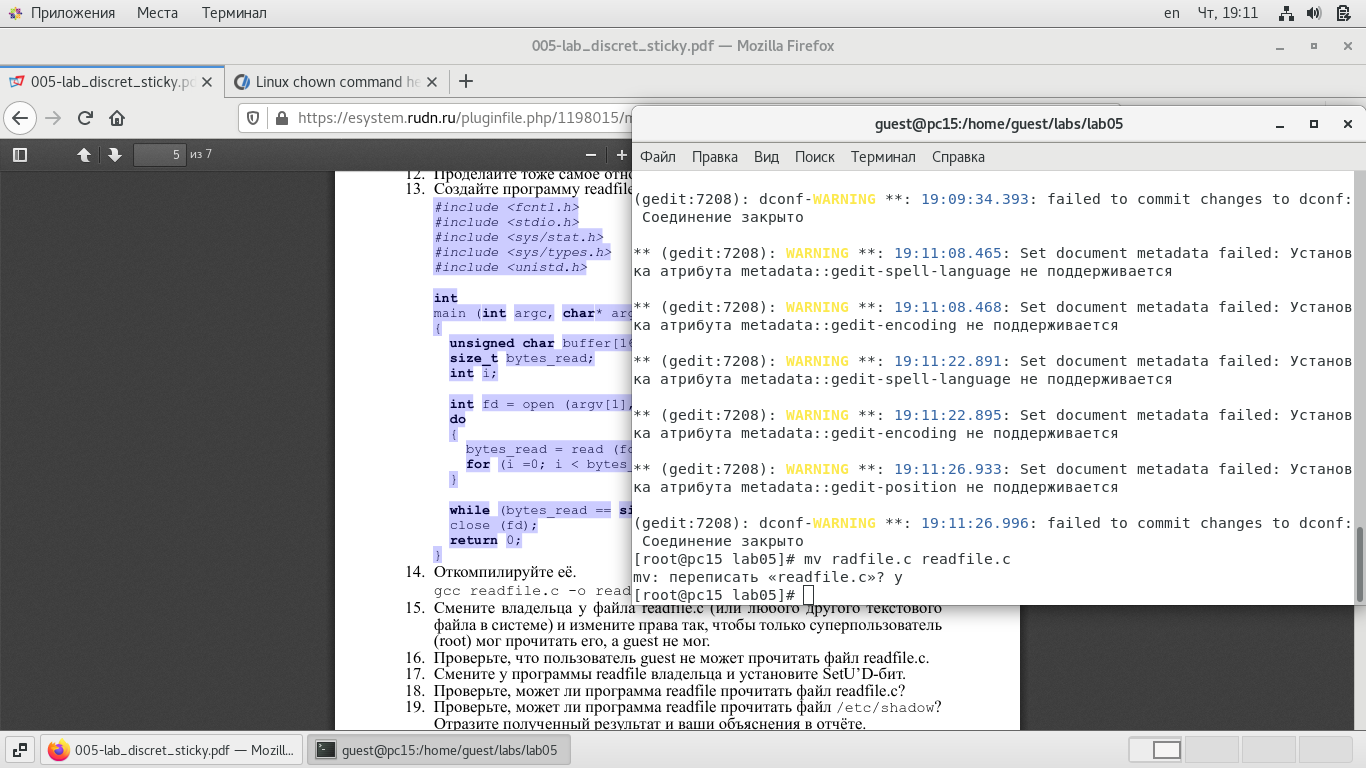


Figure : Создание программы readfile.c

Откомпилировал программу: gcc readfile.c -o readfile

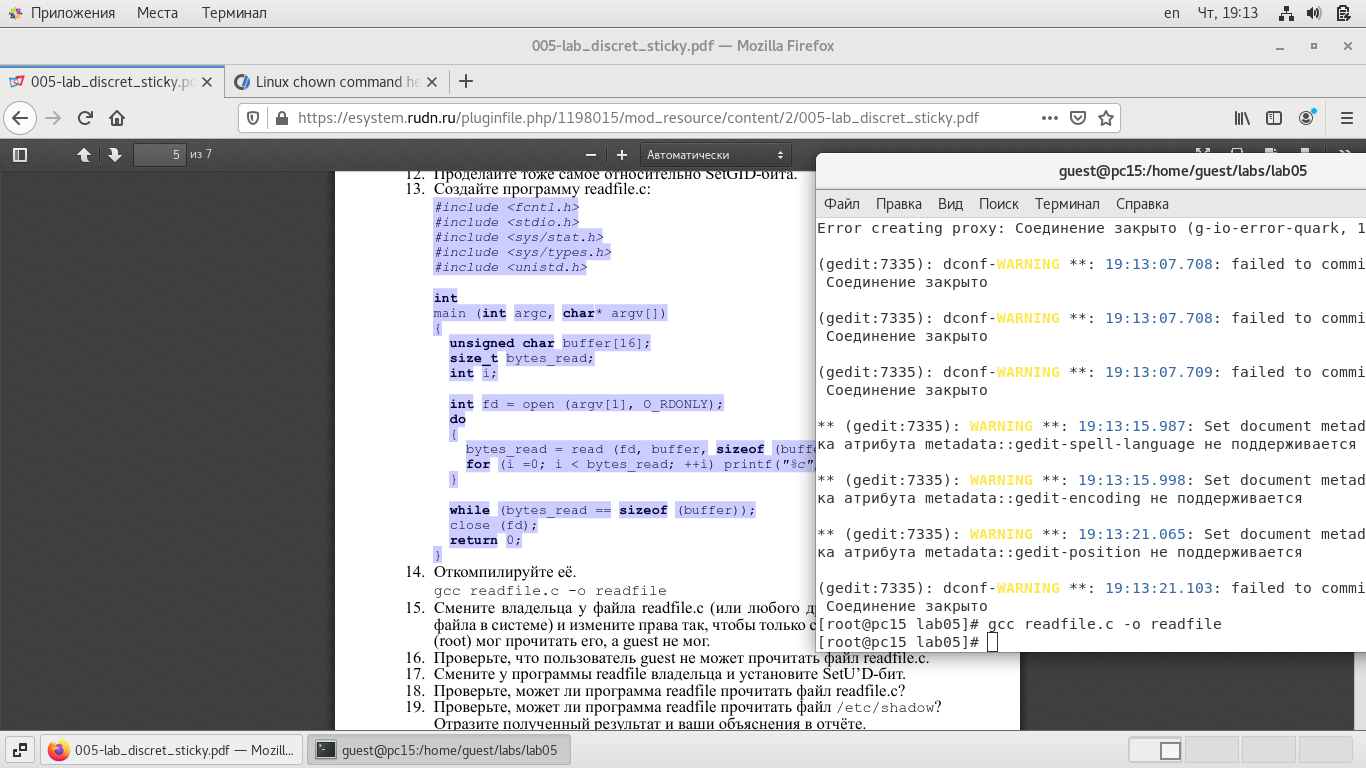


Figure : Компиляция программы

Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь(root) мог прочитать его, a guest не мог.

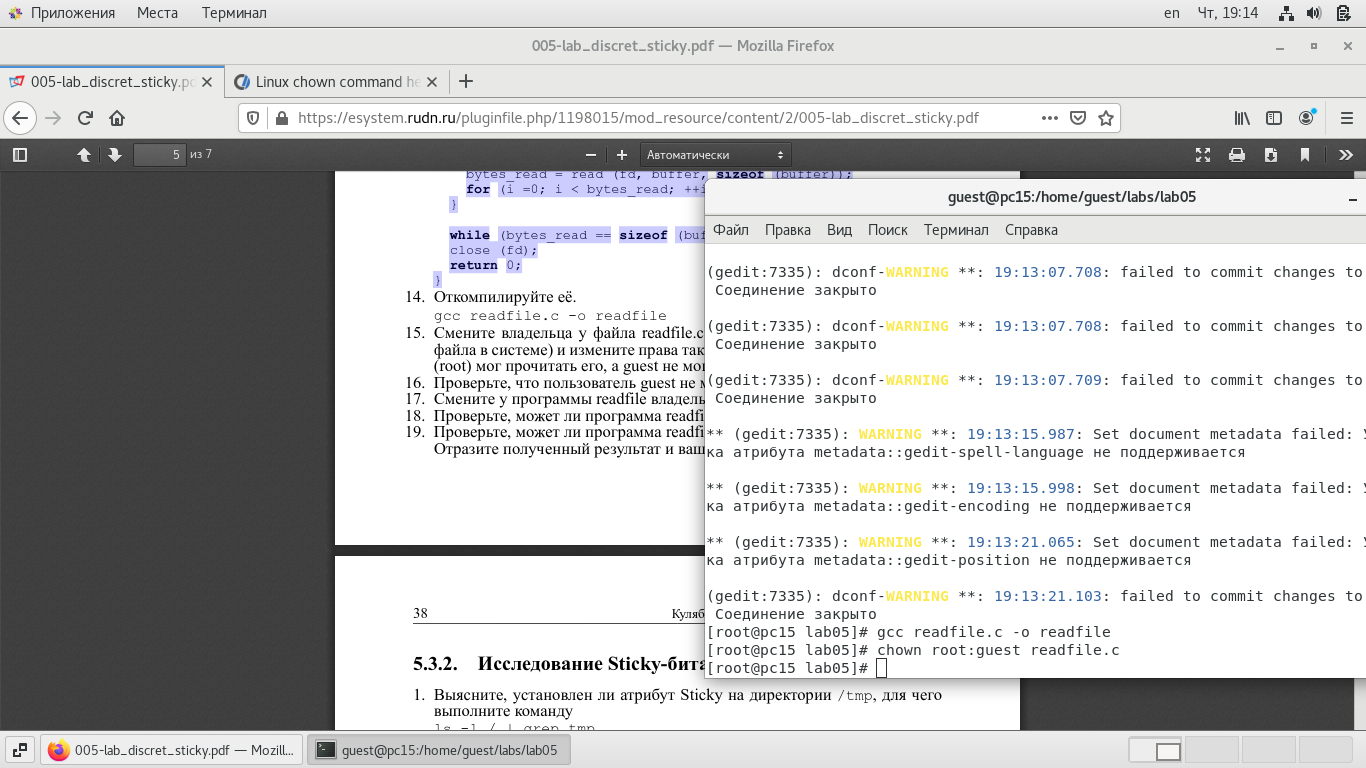


Figure : Смена владельца у файла readfile.c

Проверил, что пользователь guest не может прочитать файл readfile.с

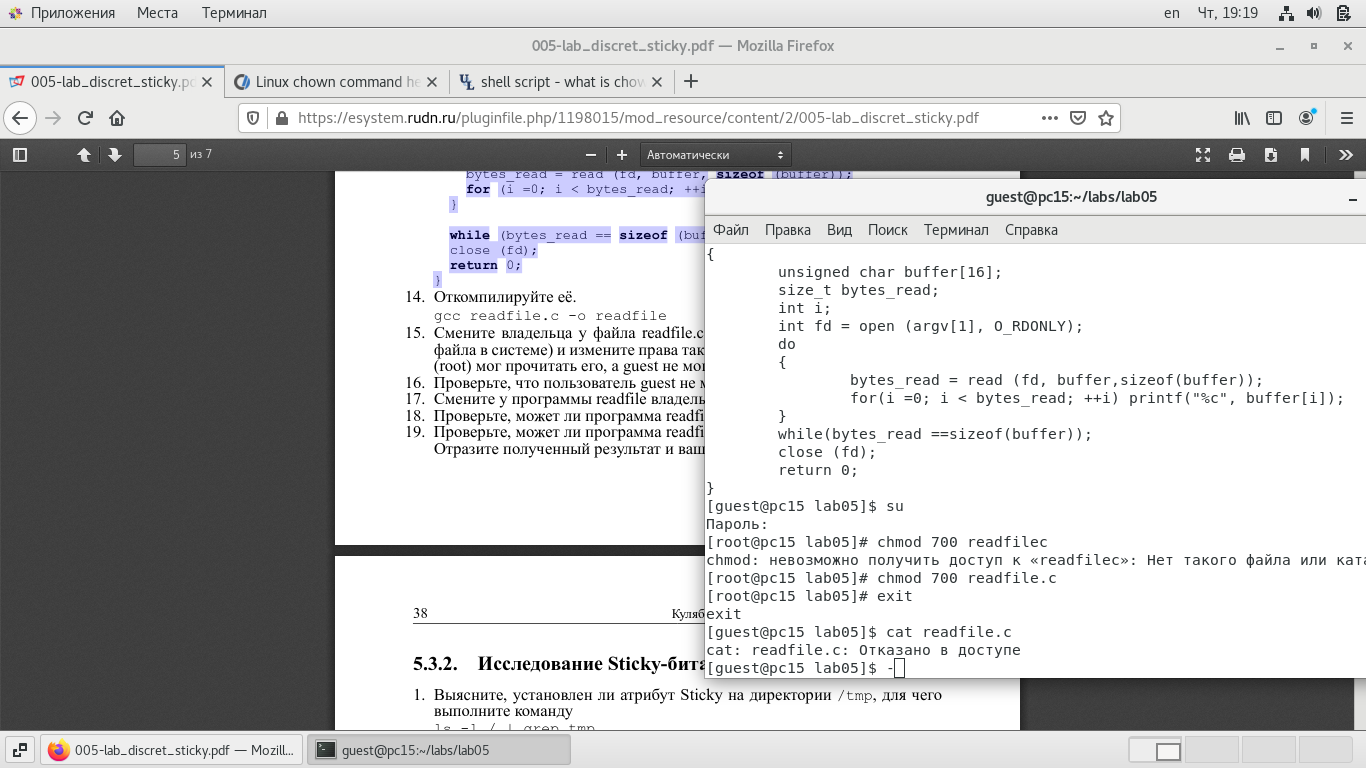


Figure : Проверка

Сменил у программы readfile владельца и установил SetU’D-бит.

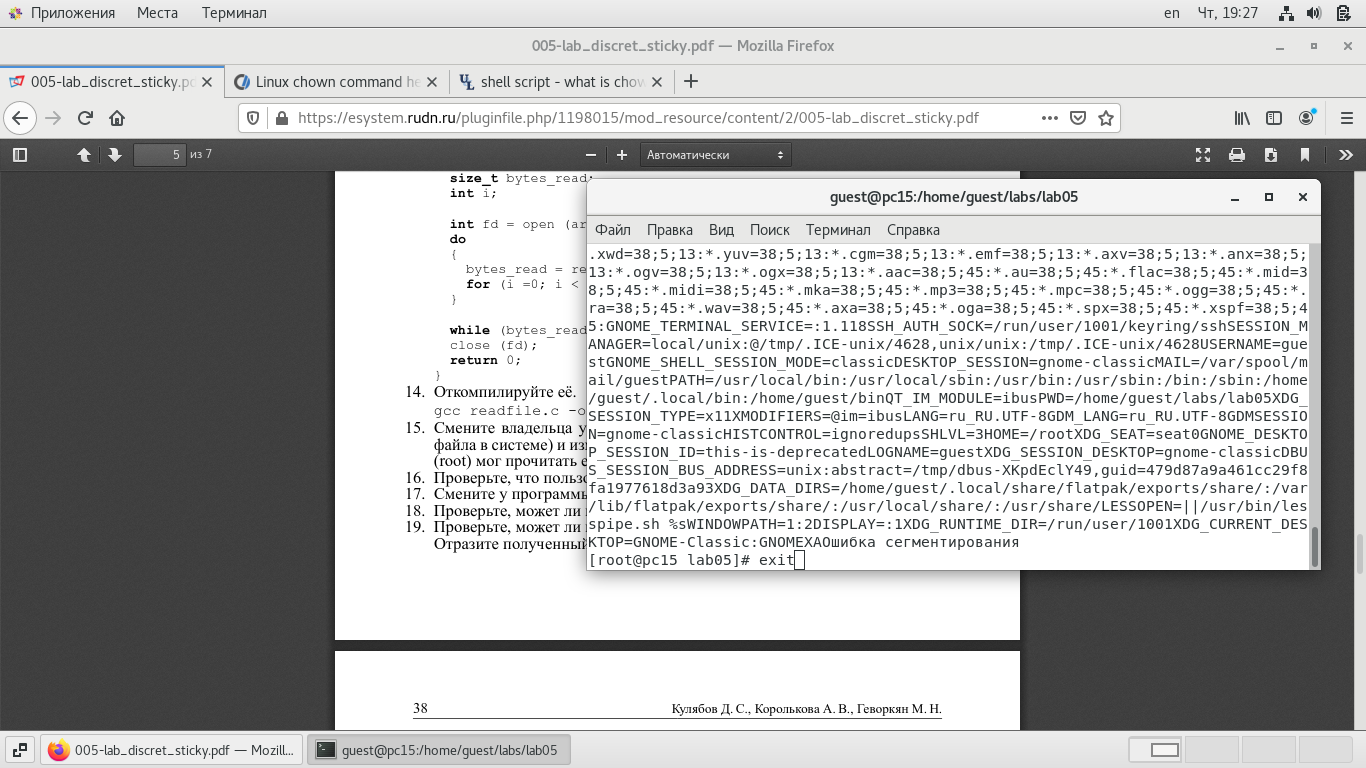


Figure : Установил SetU’D бит

Проверил, может ли программа readfile прочитать файл readfile.c. Может.

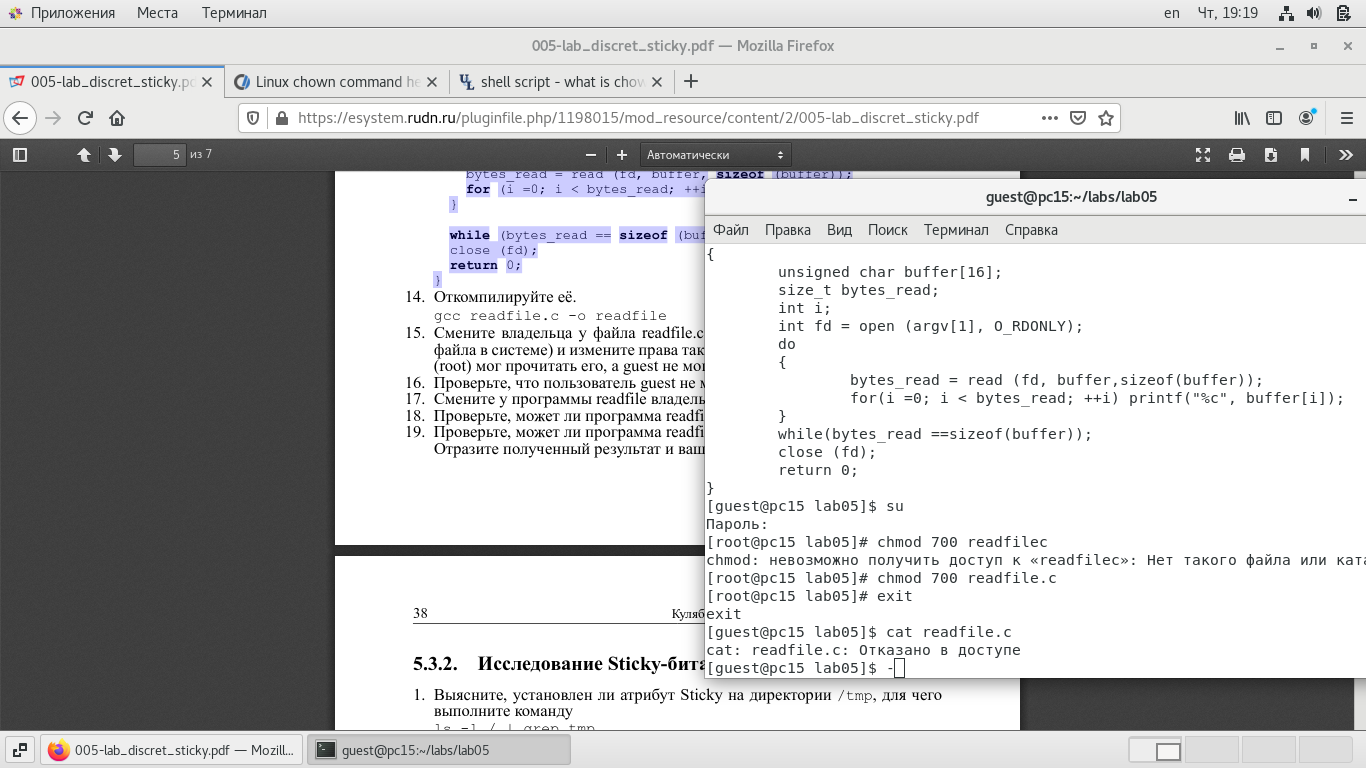


Figure : Проверка

Проверил, может ли программа readfile прочитать файл /etc/shadow. Может

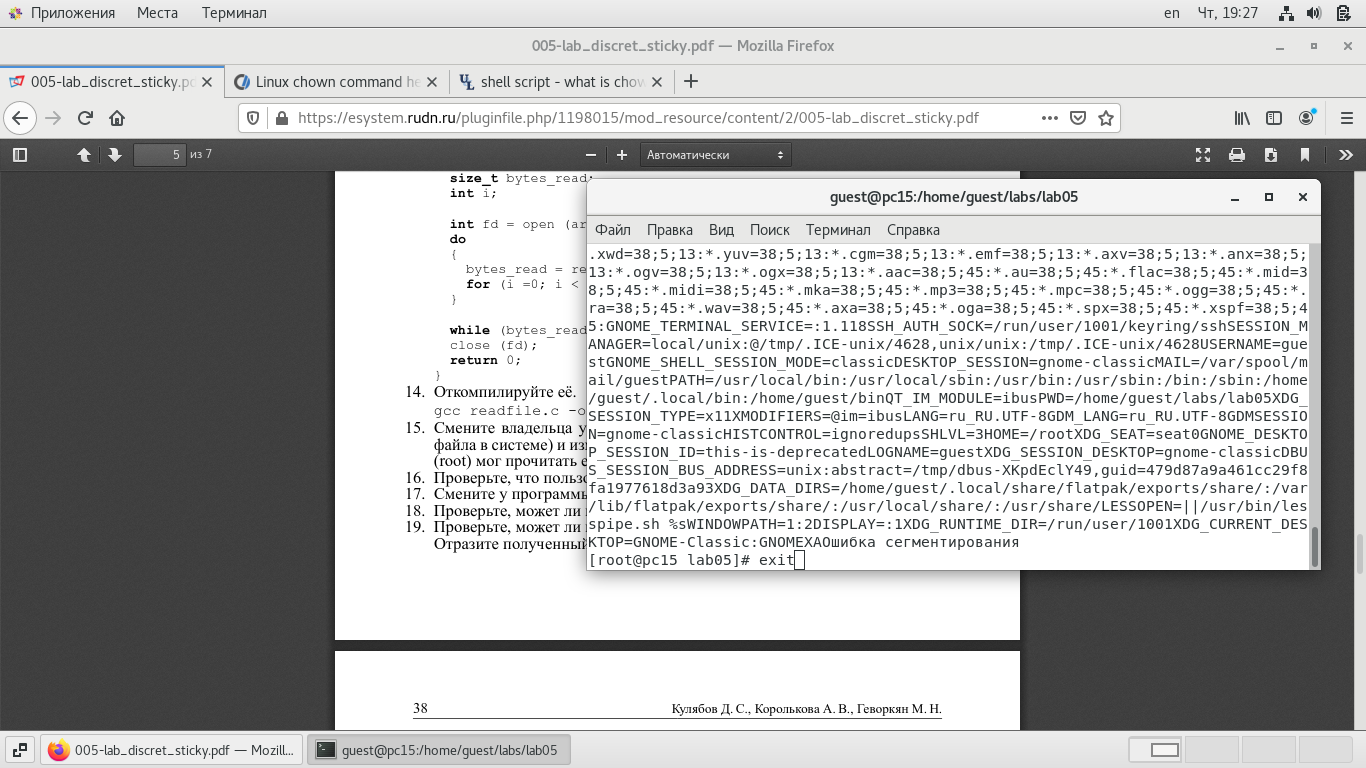


Figure : Проверка

Исследование Sticky-бита. Узнал, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду ls -l / | grep tmp

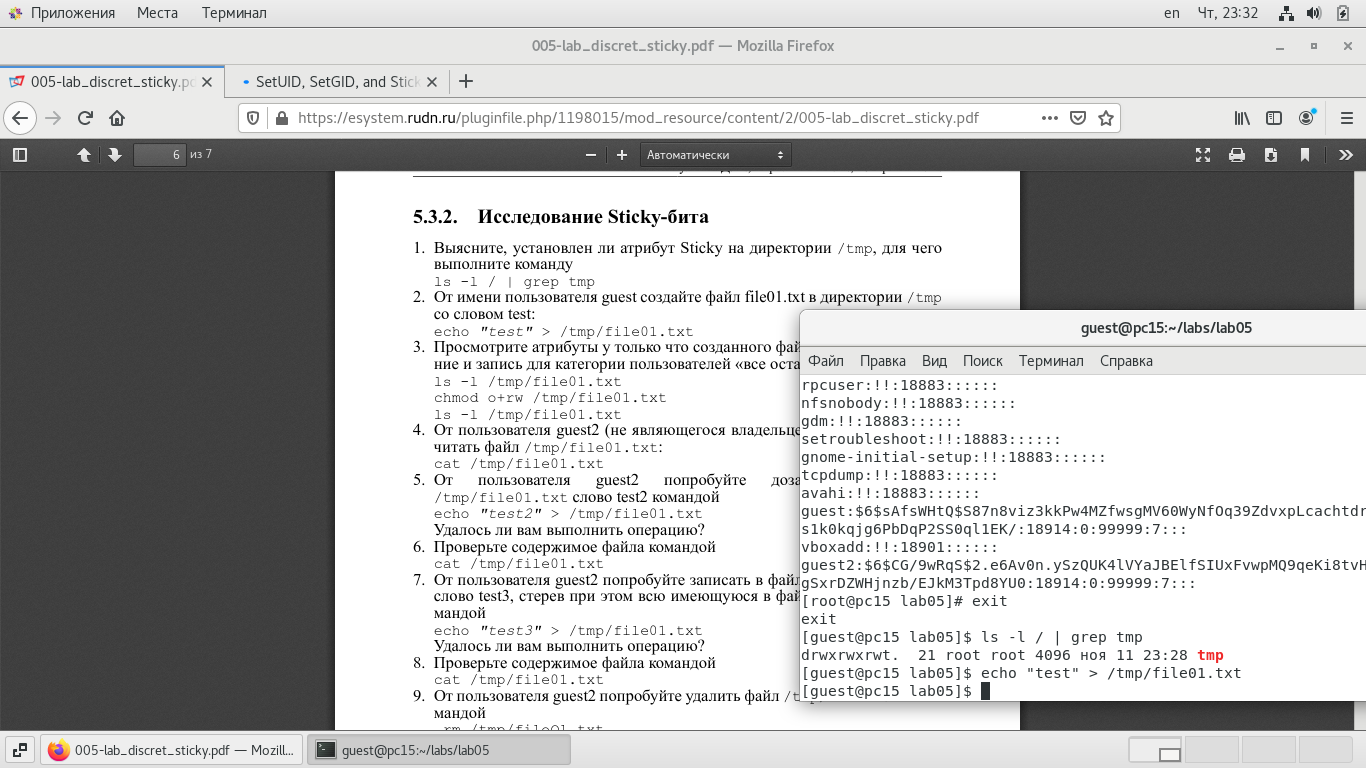


Figure : Sticky бит на папке tmp

От имени пользователя guest создал файл file01.txt в директории /tmp со словом test echo "test" > /tmp/file01.txt

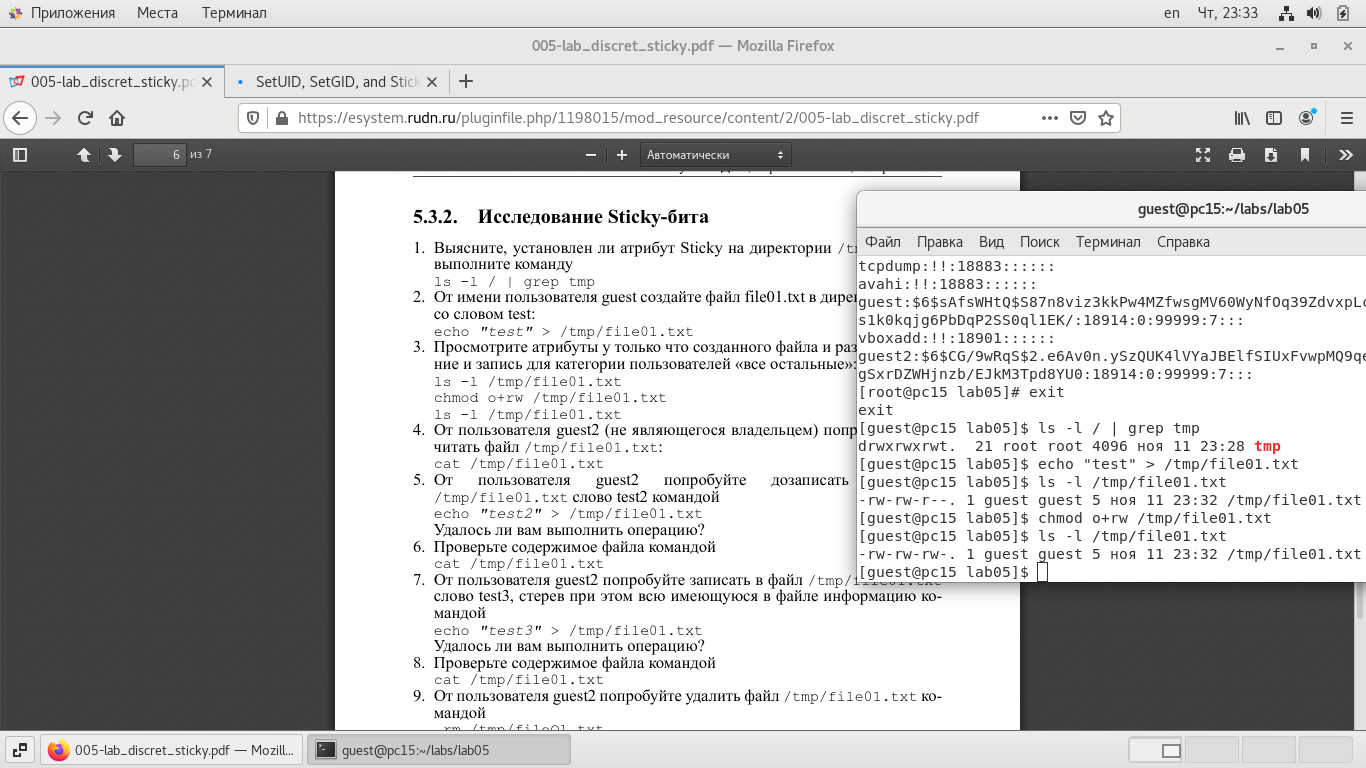


Figure : Создание файла

Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt, chmod o+rw /tmp/file01.txt, ls -l /tmp/file01.txt

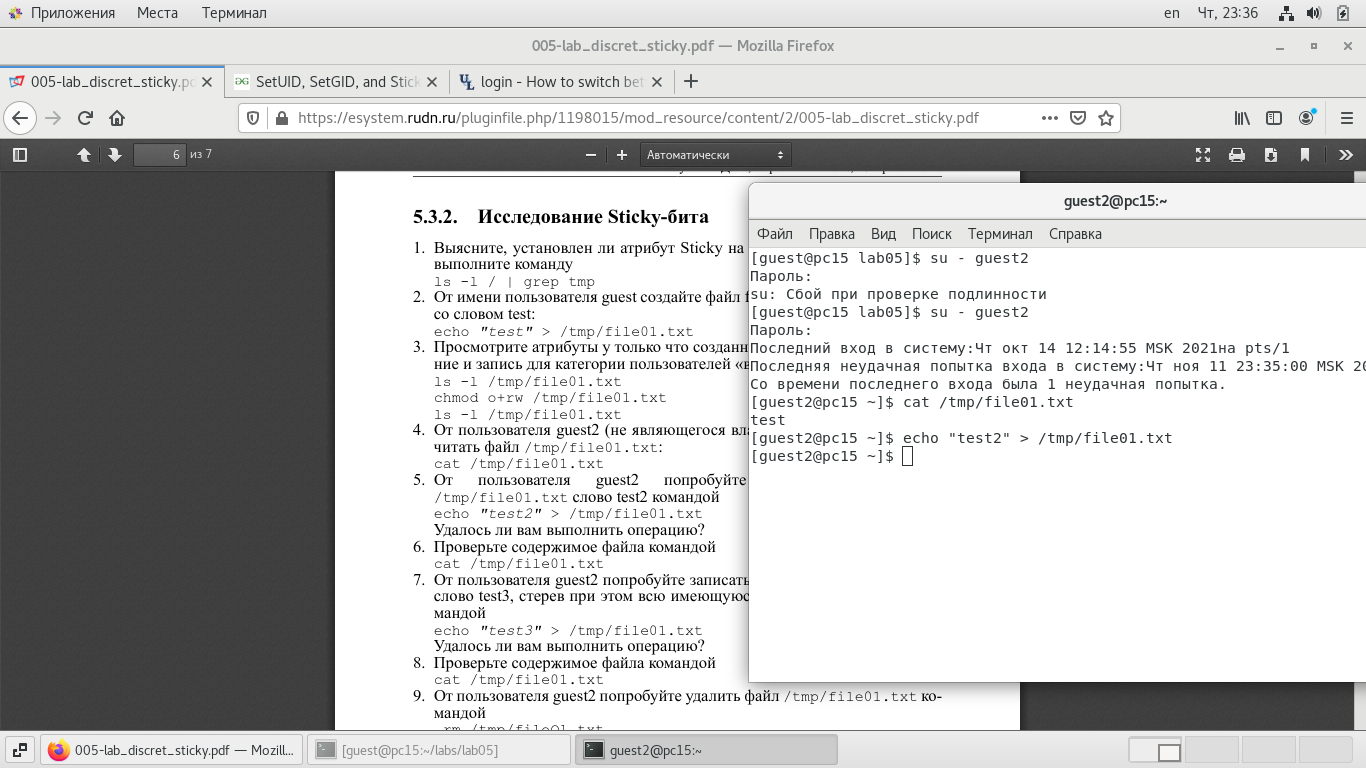


Figure : Просмотр атрибутов

От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt: cat /tmp/file01.txt

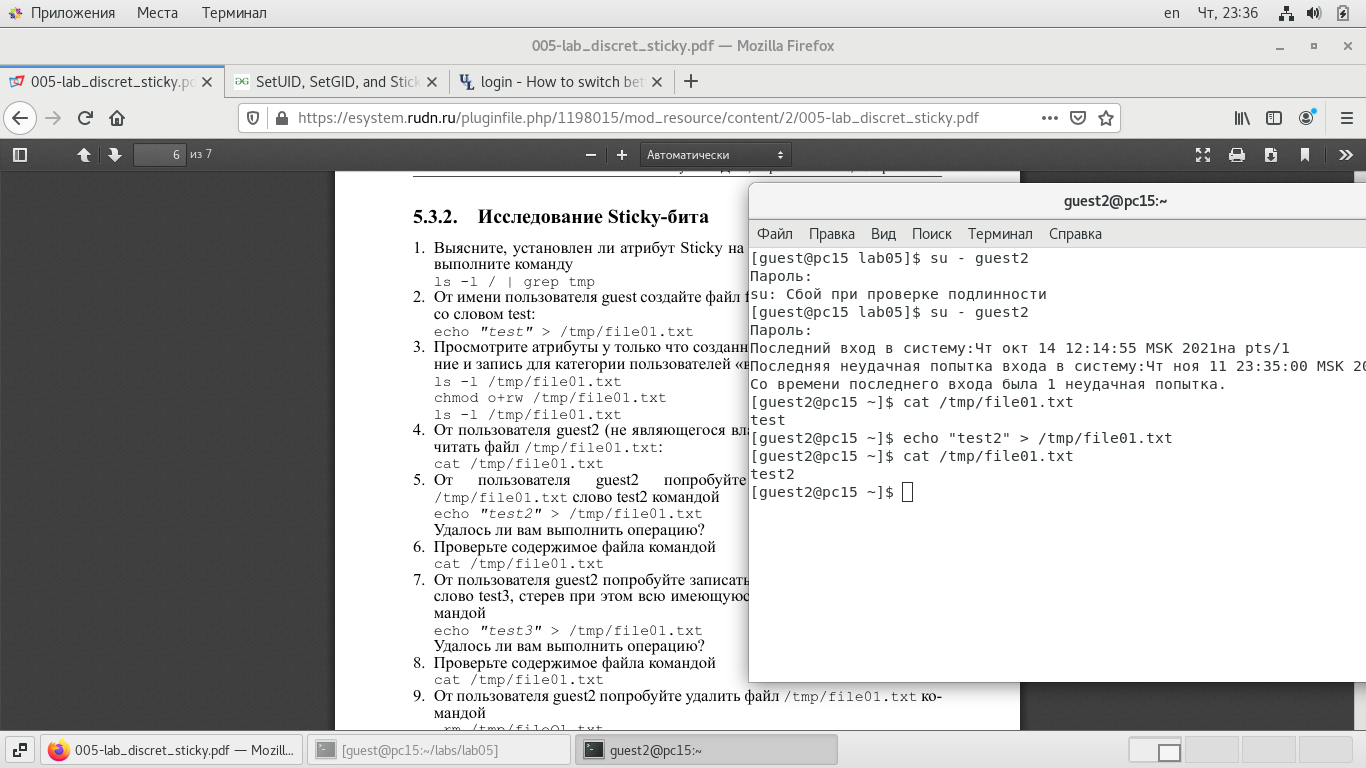


Figure : Чтение файла

От пользователя guest2 попробовал записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo "test3" > /tmp/file01.txt

Проверил содержимое файла командой cat /tmp/file01.txt

От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2 командой echo "test2" >> /tmp/file01.txt

Проверил содержимое файла командой cat /tmp/file01.txt

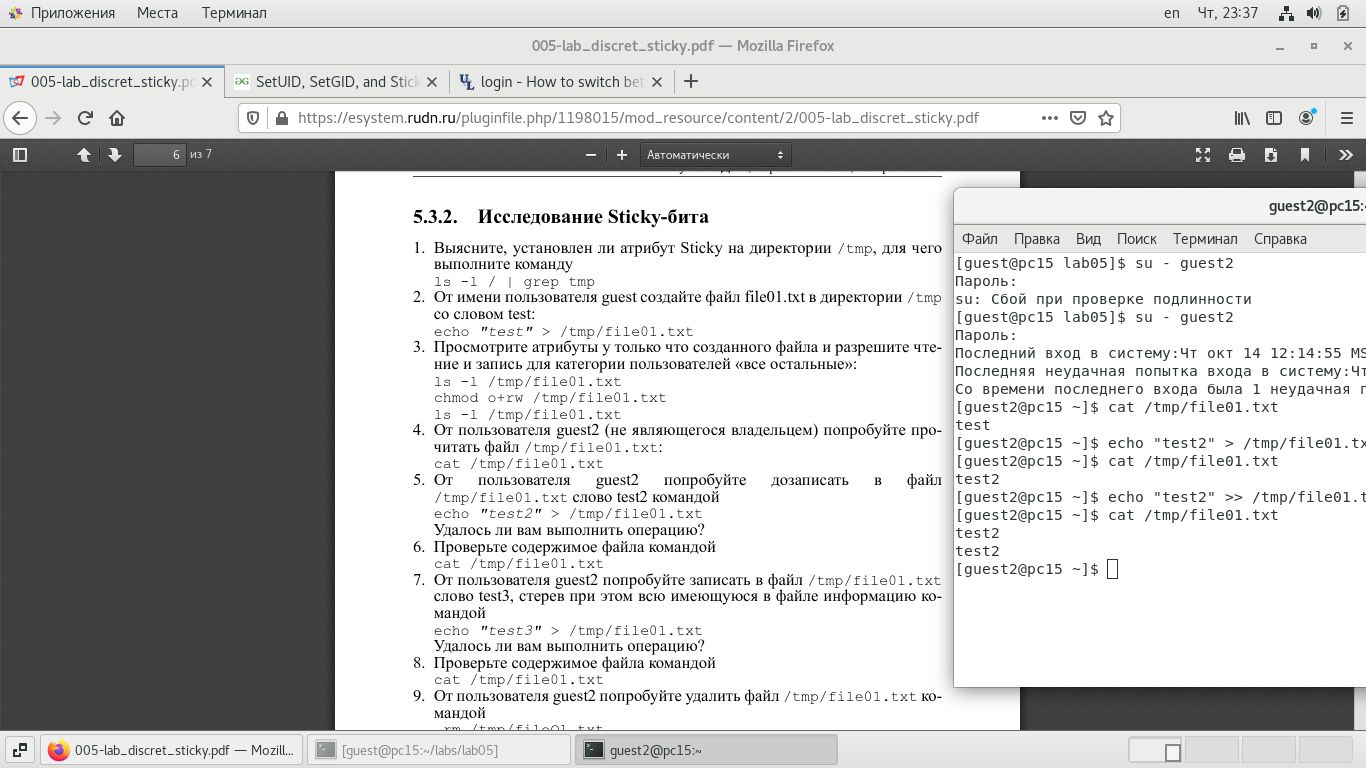


Figure : Запись и дозапись

От пользователя guest2 попробовал удалить файл /tmp/file01.txt командой rm /tmp/file01.txt Файл удалить не удалось.

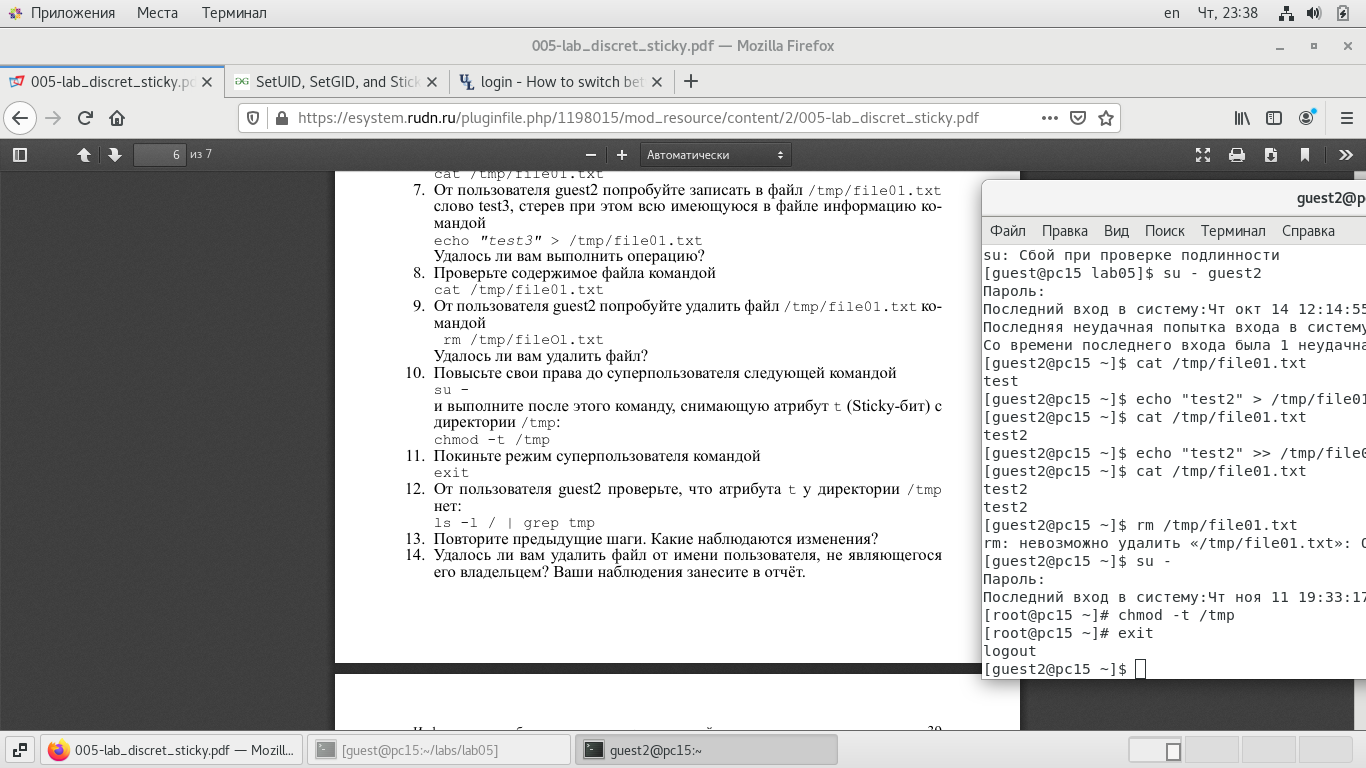


Figure : Попытка удалить файл

Повысил свои права до суперпользователя следующей командой su - и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp



Figure : Снятие Sticky атрибута

Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp: su -, chmod +t /tmp, exit

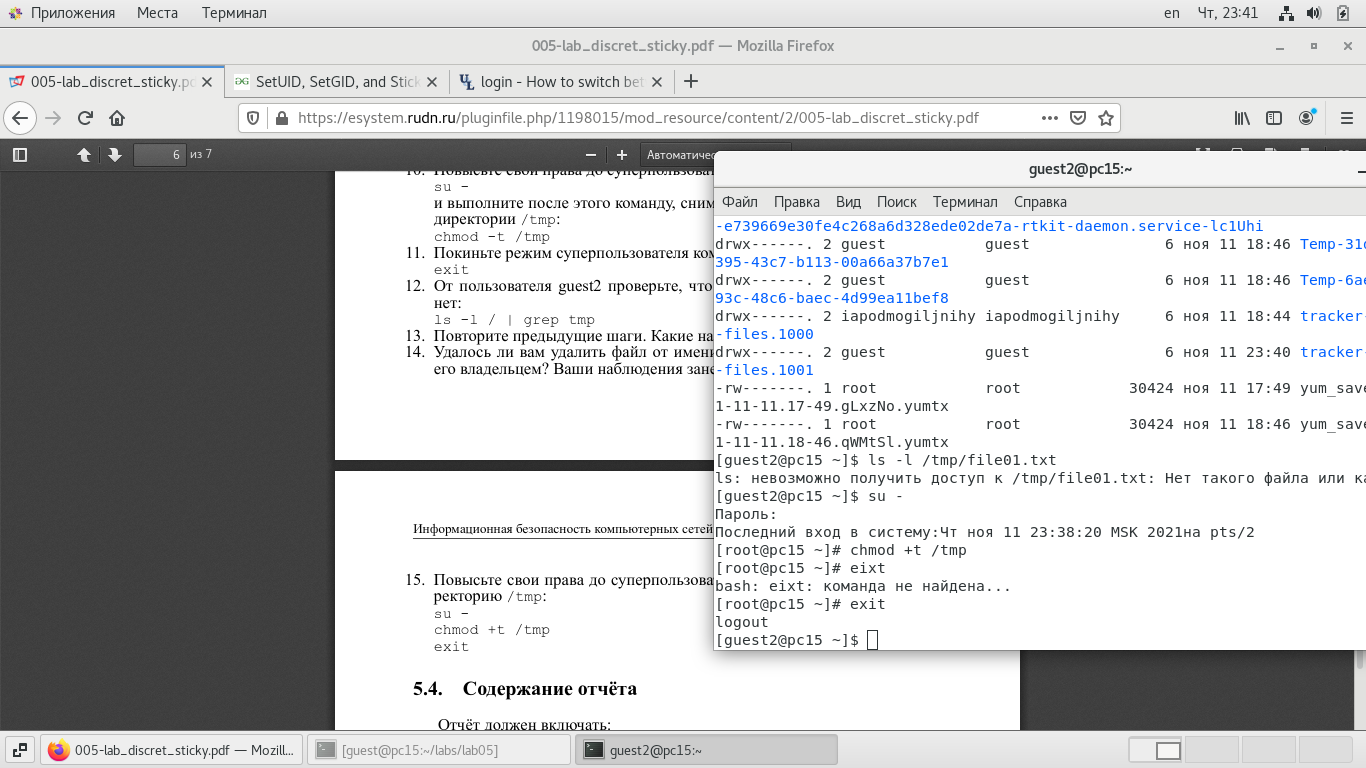


Figure : Выход из суперпользователя

# 4 Выводы

Изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.