Отчет по лабораторной работе номер 5

Хамбалеев Булат Галимович

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 бита Sticky на запись и удаление файлов.

# Задание

Лабораторная работа подразумевает использование некоторых консольных команд для взаимодействия с кодом, правами и атрибутами.

# Теория

Setuid и setgid являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами владельца или группы исполняемого файла. Sticky bit — дополнительный атрибут файлов или каталогов в операционных системах семейства UNIX.

# Выполнение работы

1. Войдём в систему от имени пользователя guest. Создадим программу simpleid.c . Скомпилируем её и затем выполним. Затем выполним id.(рис 1-4)

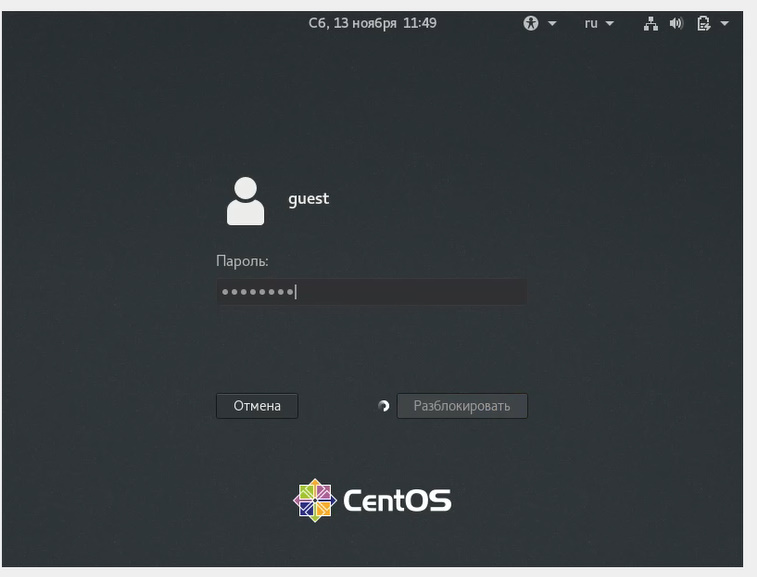


Figure 1: рис.1. Вход.

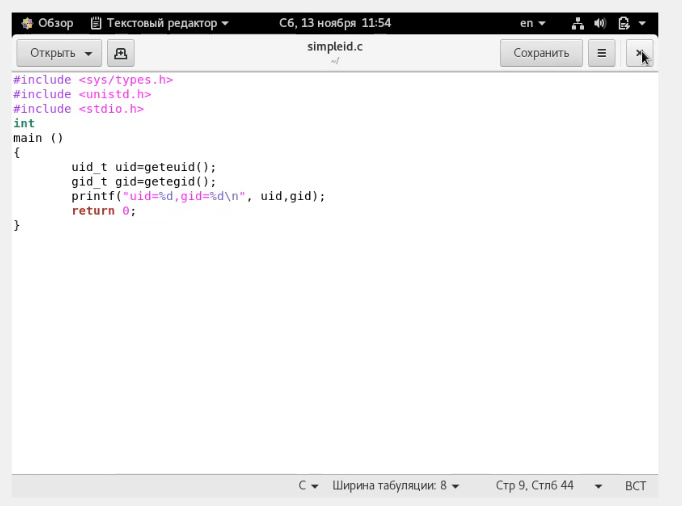


Figure 2: рис.2. Программа.

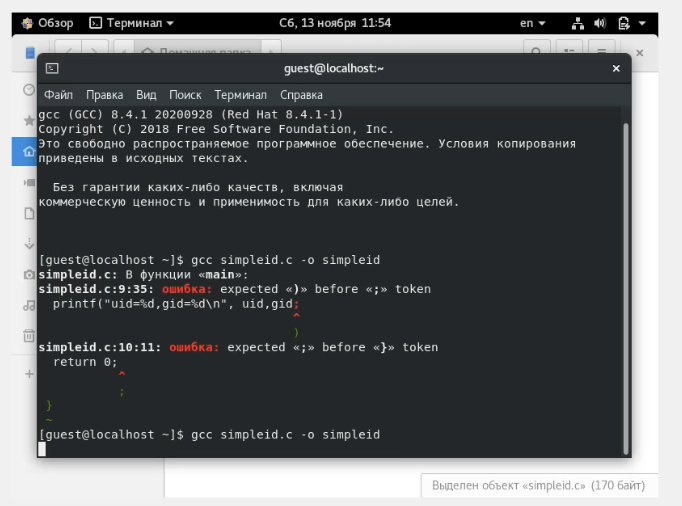


Figure 3: рис.3. Компиляция.

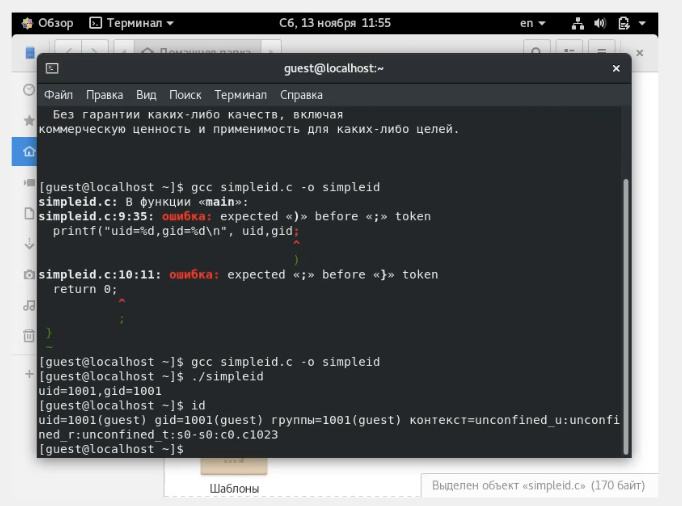


Figure 4: рис.4. id.

1. Усложним программу, добавив вывод действительных идентификаторов. Назовём программу simpleid2. Cкомпилируем и запустим. От имени суперпользователя выполним следующие команды: chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2 . Повысим права с помощью su. Выполним проверку правильности установки атрибутов и смены владельца файла simpleid2. (рис.5-8)

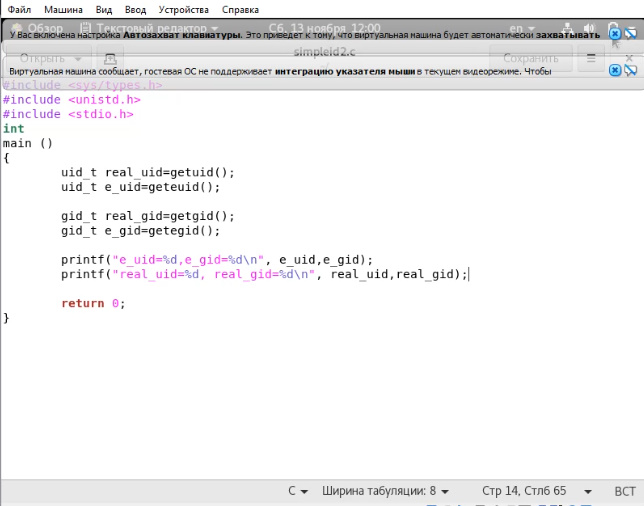


Figure 5: рис.5. Усложнённый код.

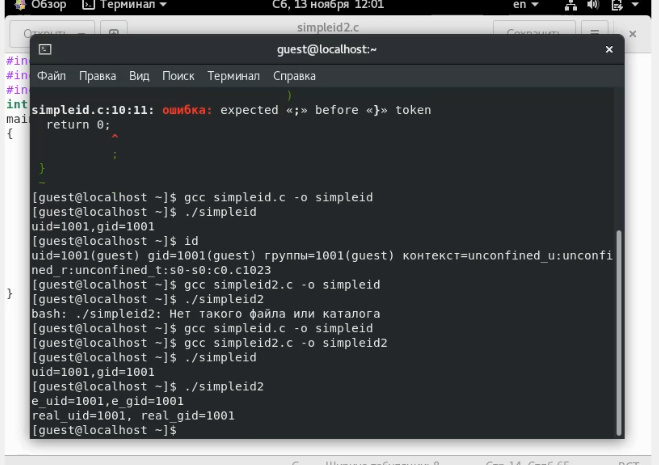


Figure 6: рис.6. Компиляция.

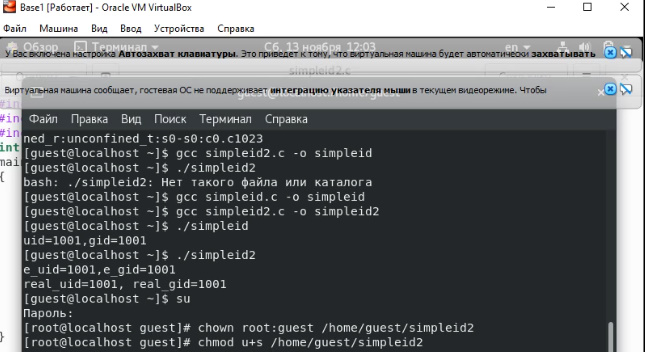


Figure 7: рис.7. Выполнение и chown root.

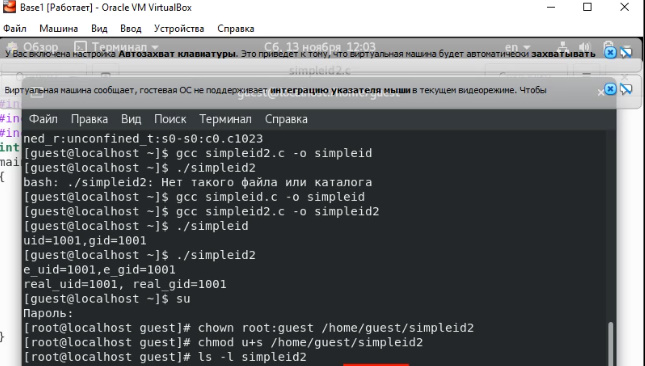


Figure 8: рис.8. Команда ls -l.

1. Запустил simpleid2 и id. Проделал тоже самое относительно SetGID-бита Создал программу readfile.c . Откомпилировал её. Сменил владельца файла readfile.c . Проверил, что пользователь guest не может прочитать файл readfile.c . Сменил у программы redfile владельца и установил SetU’D-бит.(рис.9-13)

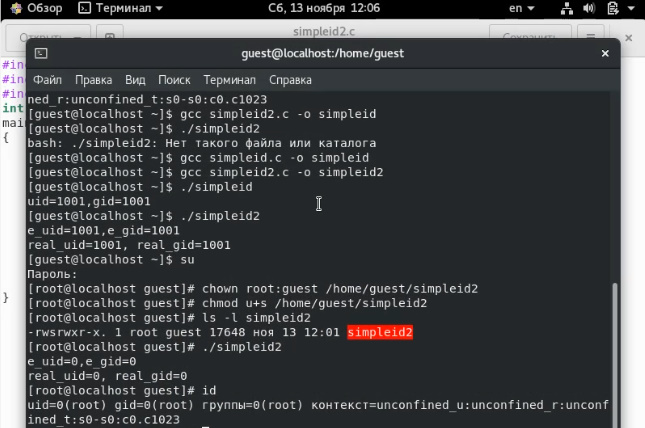


Figure 9: рис.9. Повторный запуск программы и id.

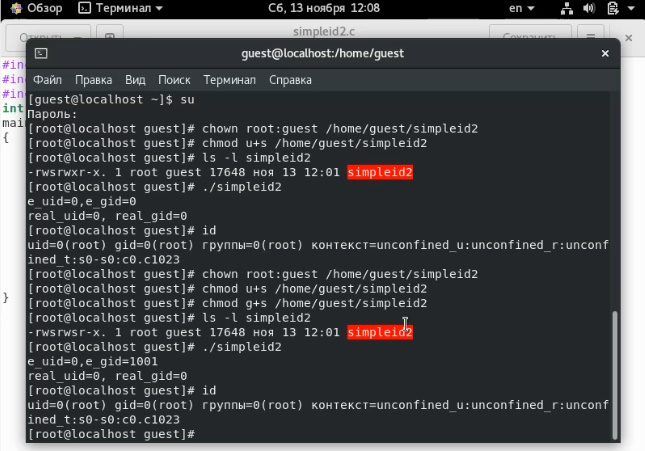


Figure 10: рис.10. Повторный запуск программы и id.

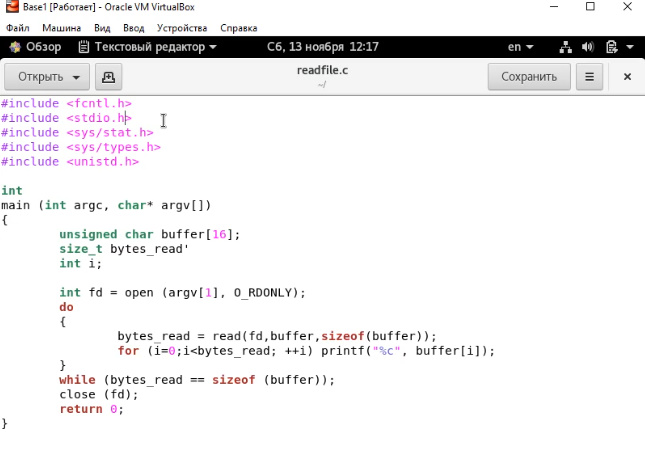


Figure 11: рис.11. Readfile.c.

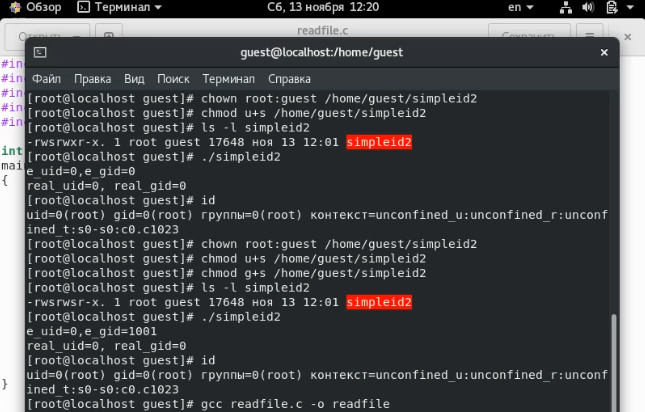


Figure 12: рис.12. Компиляция.

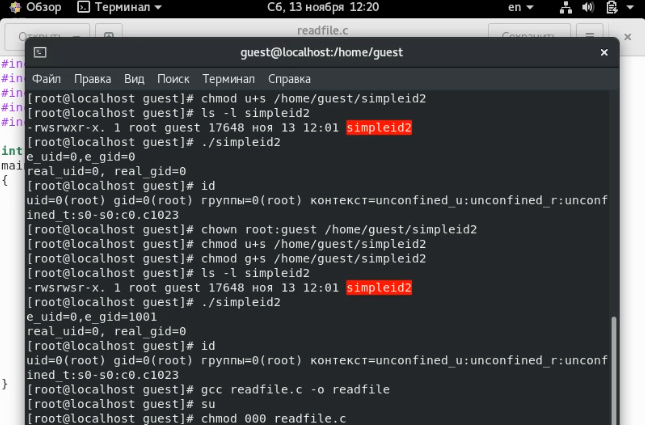


Figure 13: рис.13. Смена владельца.

1. Проверил , может ли программа readfile прочитать файл readfile.c . Может. Проверил может ли программа readfile.c прочитать файл /etc/shadow . Может.( рис.14-17)

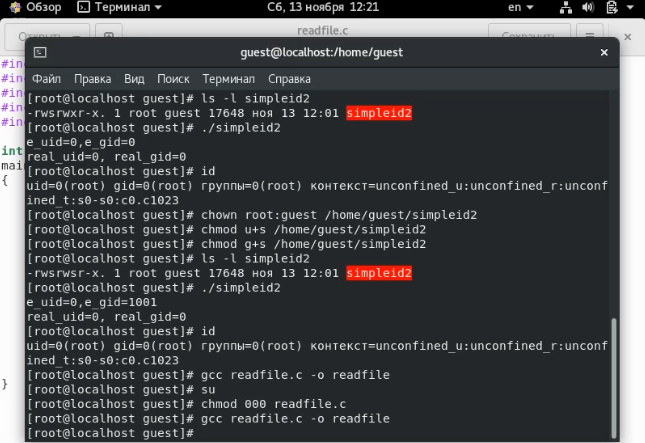


Figure 14: рис.14. Повторная компиляция.

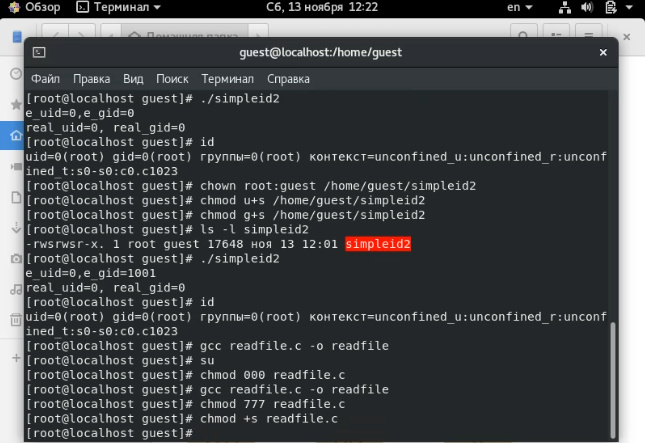


Figure 15: рис.15. Изменение прав доступа к файлу.

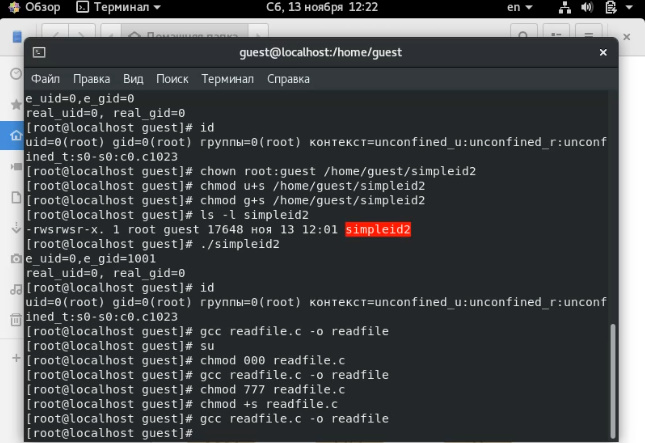


Figure 16: рис.16. Компиляция.

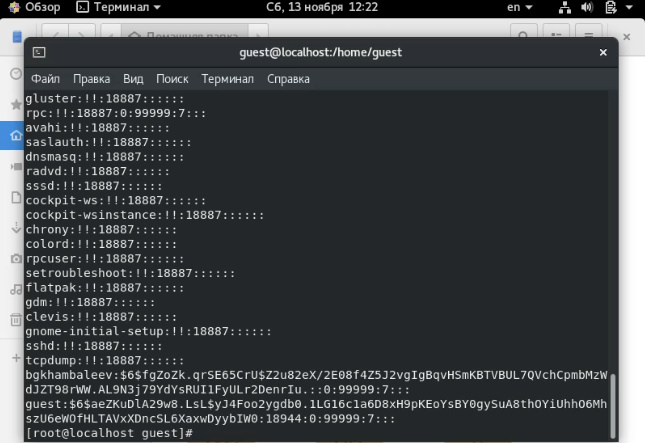


Figure 17: рис.17. Чтение файла.

1. Выяснил установлен ли атрибут Sticky на директории /tmp. Создал файл file01.txt со словом test. Разрешил чтение и запись для категории пользователей “все остальные”. Попробовал прочитать file01.txt от пользователя guest2. От пользователя guest2 попробовал дозаписать в файл file01.txt слово test2. (рис. 18-22)

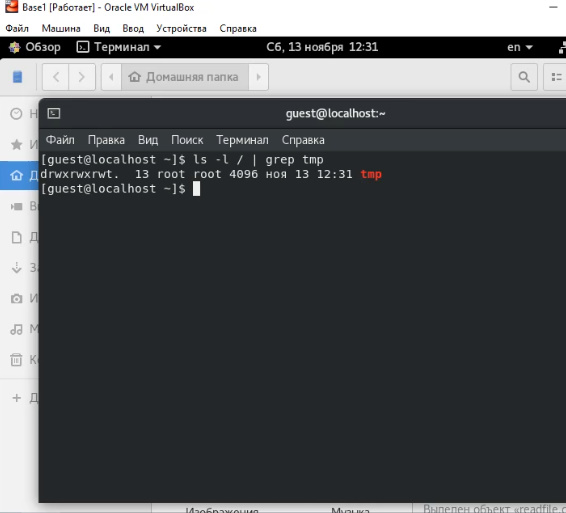


Figure 18: рис.18. Команда ls -l / | grep tmp.

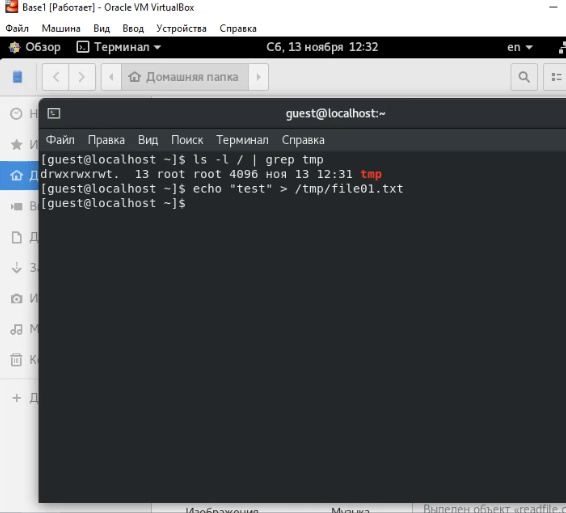


Figure 19: рис.19. Внесение слова test в файл.

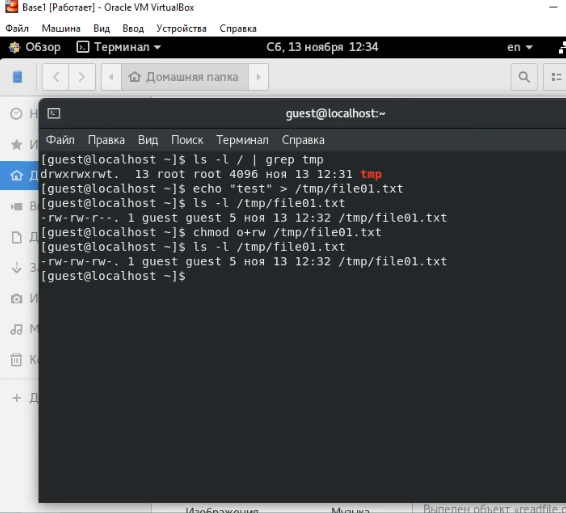


Figure 20: рис.20. Разрешил чтение и запись в файл.

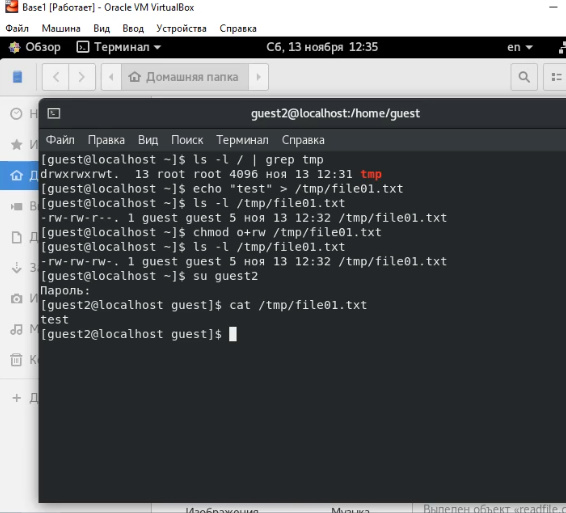


Figure 21: рис.21. Просмотр файла.

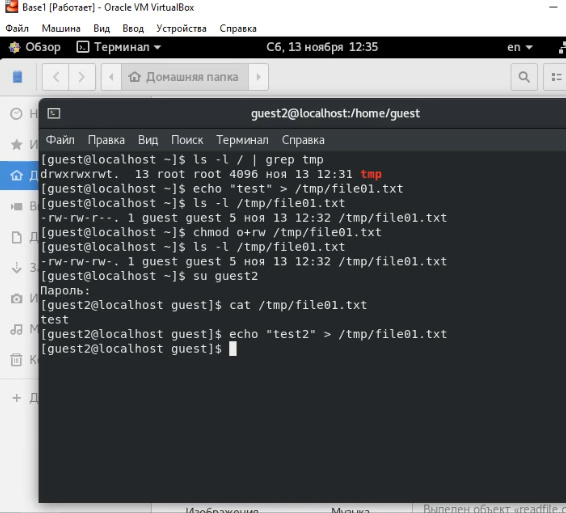


Figure 22: рис.22. Запись в файл слова test2.

1. Проверил содержимое файла командой. Попробовал записать test3 в файл от имени guest2. От пользователя guest2 попробовал удалить файл file01.txt. Удалить не удалось. Повысил права до суперпользователя и снял атрибут t. (рис. 23-27)

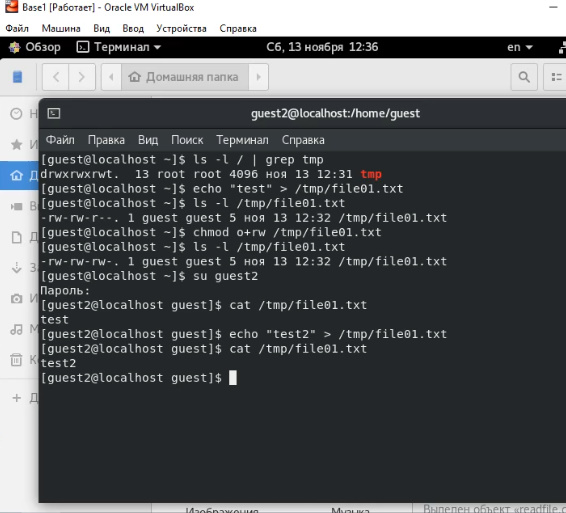


Figure 23: рис.23. Просмотр файла.

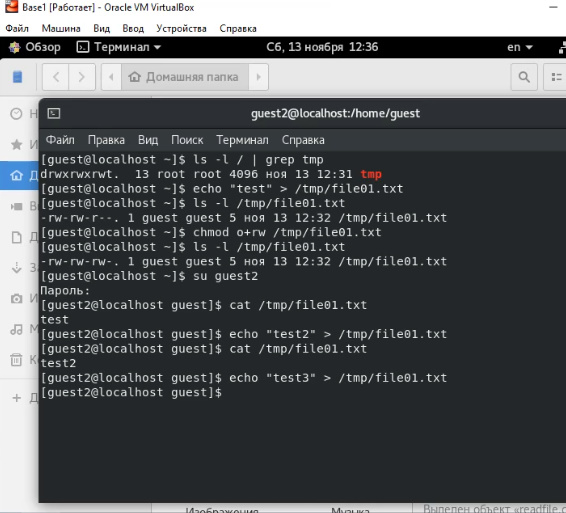


Figure 24: рис.24. Запись test3 в файл.

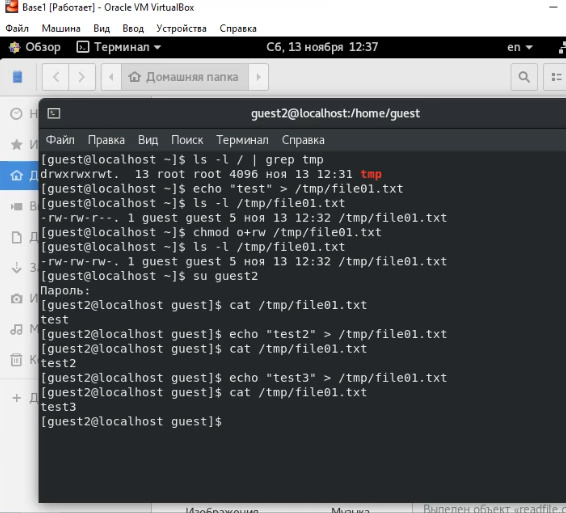


Figure 25: рис.25. Чтение файла.

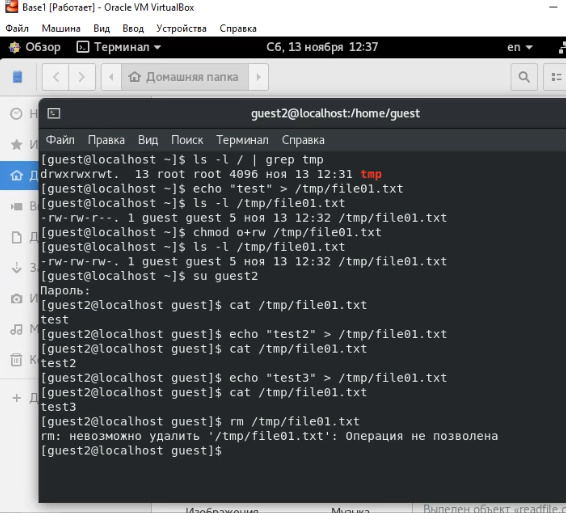


Figure 26: рис.26. Попытка удаления файла.

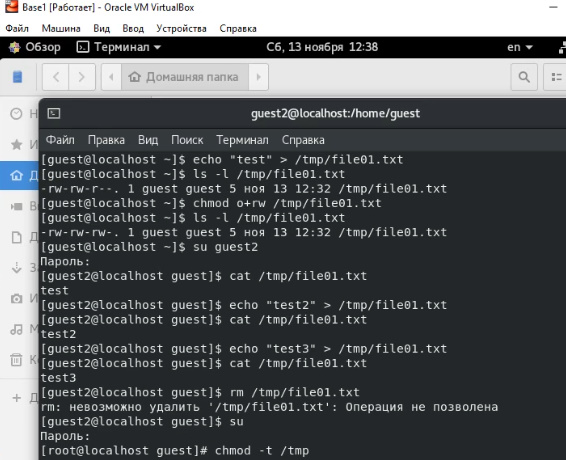


Figure 27: рис.27. Снятие атрибута t.

1. Покинул режим суперпользователя командой exit. Проверил наличие атрибута t. Повторил предыдущие шаги, на этот раз получилось удалить файл. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp.(рис. 28-30).

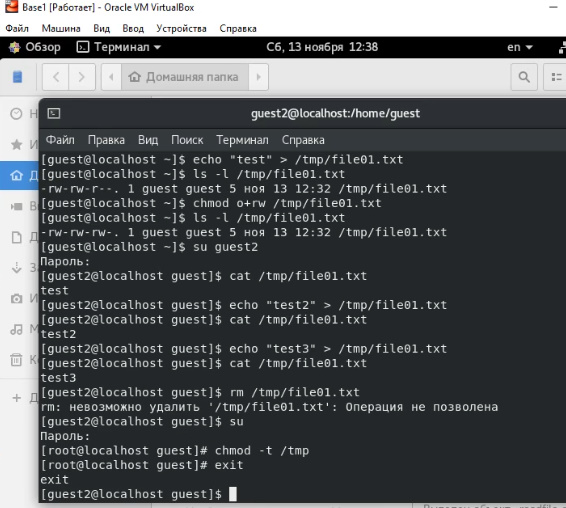


Figure 28: рис.28. Выход из режима суперпользователя.

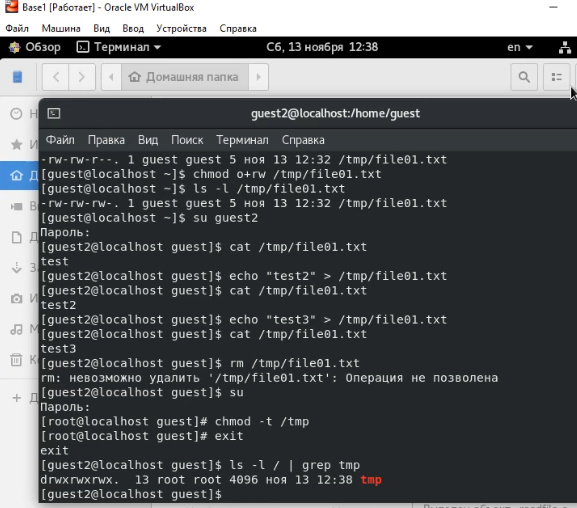


Figure 29: рис.29. Команда ls -l.

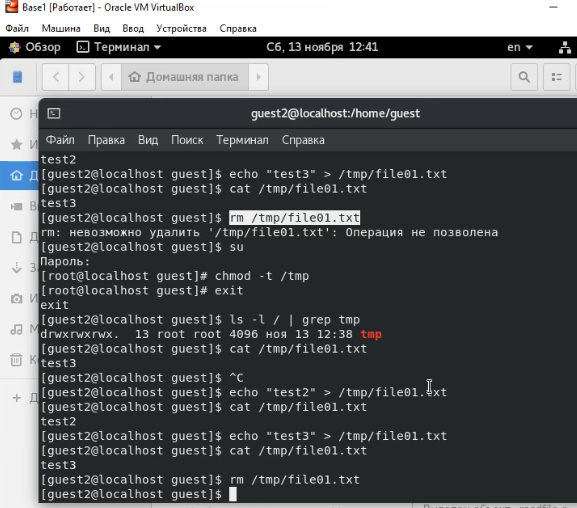


Figure 30: рис.30. Повторный набор команд и повторная попытка удаления(успешная).

# Библиография

1. ТУИС РУДН
2. Статья на сайте “https://ru.wikipedia.org/wiki/Sticky\_bit”
3. Статья на сайте “https://ru.wikipedia.org/wiki/Suid”

# Выводы

Во время выполнения лабораторной работы я получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификаторов процессов пользователей. Изучил механизмы изменения идентификаторов.