РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

ФАКУЛЬТЕТ ФИЗИКО-МАТЕМАТИЧЕСКИХ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

**ОТЧЕТ**

По дисциплине: Информационная безопасность.

Лабораторная работа № 5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов.

Нгуен Чау Ки Ань

1032185287

НБИбд-01-18

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

# .**Подготовка к работе**

1/ Cредства разработки приложений

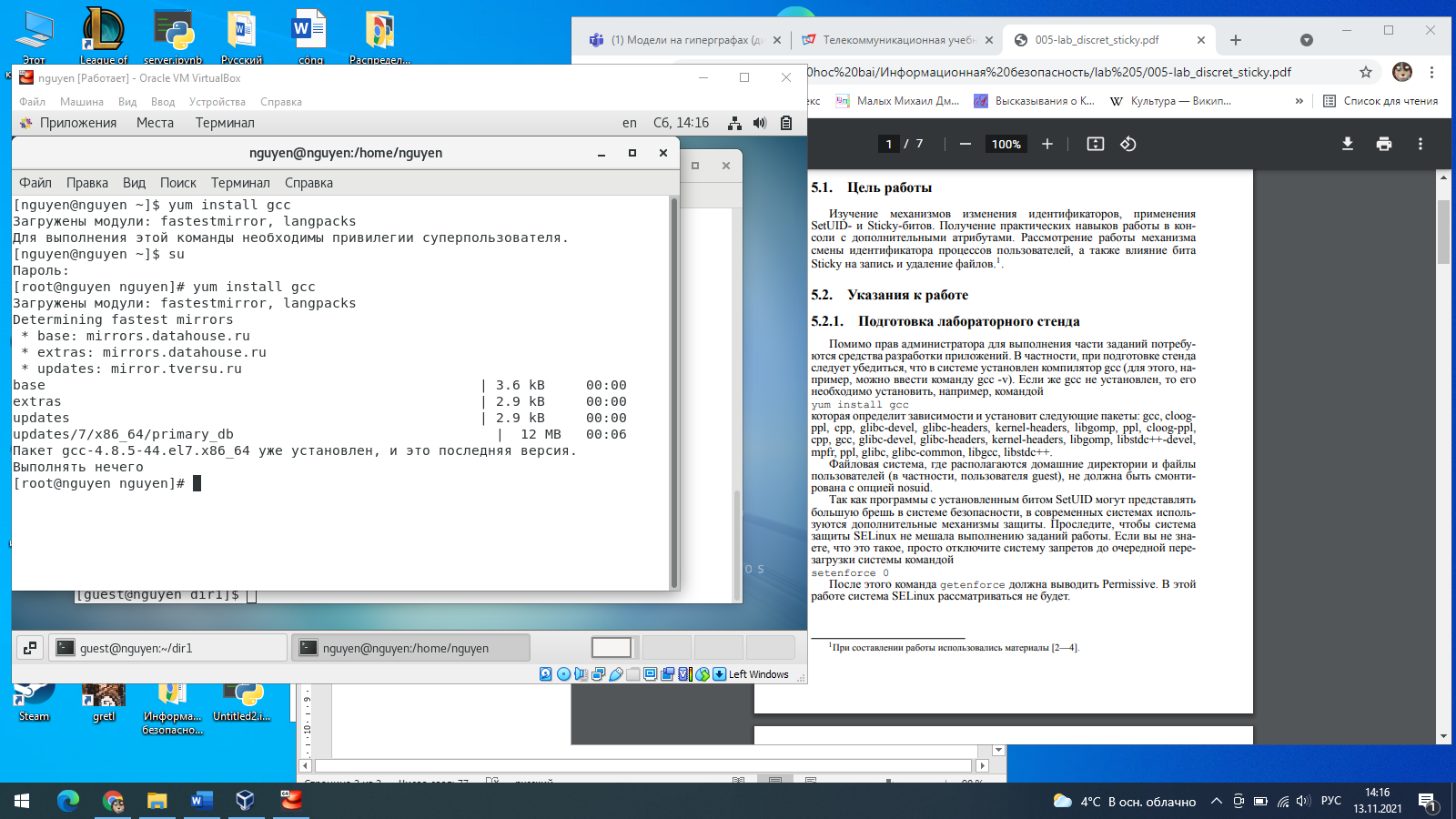


Figure 1: yum install gcc

2/ Отключить систему запретов до очередной перезагрузки системы командой setenforce 0 После этого команда getenforce должна выводить Permissive. В этой работе система SELinux рассматриваться не будет.

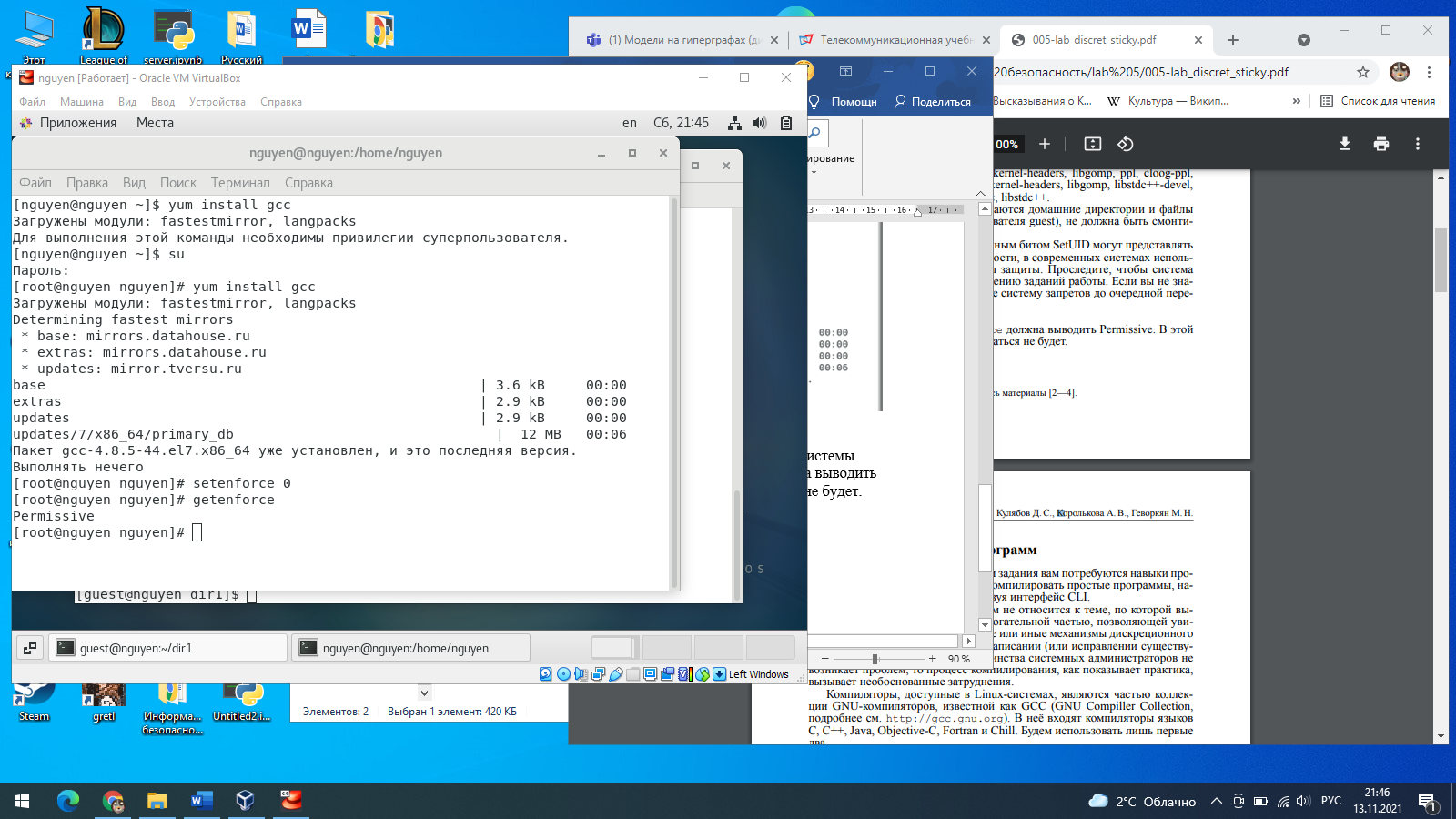


Figure 2: отключение SELinux

**2. Компилирование программ**

1. Для выполнения четвёртой части задания вам потребуются навыки программирования, а именно, умение компилировать простые программы, написанные на языке С (С++), используя интерфейс CLI.

Компилятор языка С называется gcc. Компилятор языка С++ называется g++ и запускается с параметрами почти так же, как gcc.

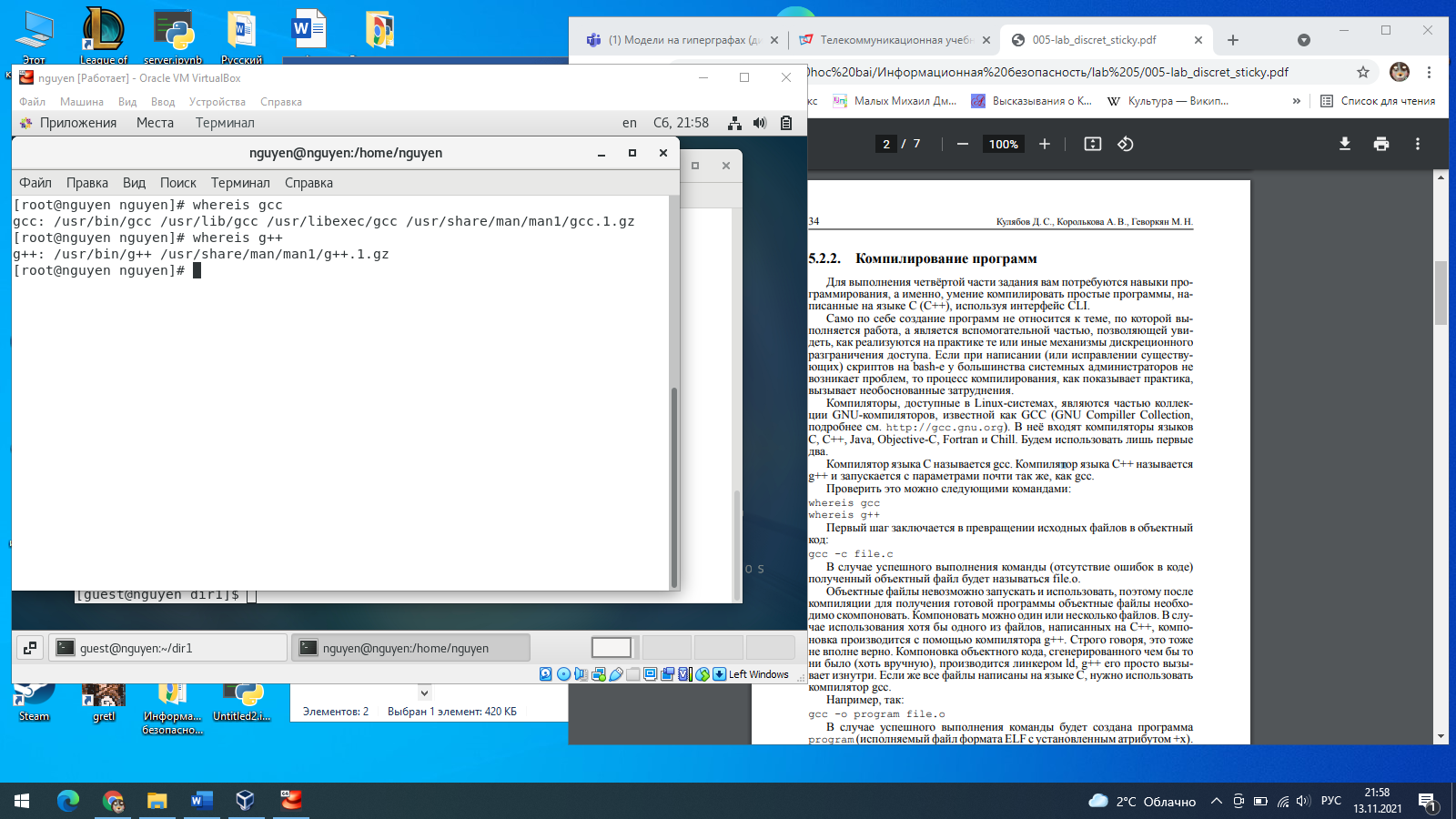


Figure 3: проверка командами whereis gcc, whereis g++

3. Порядок выполнения работы

1. Создание программы

1. Войти в систему от имени пользователя guest.

2. Создать программу simpleid.c:

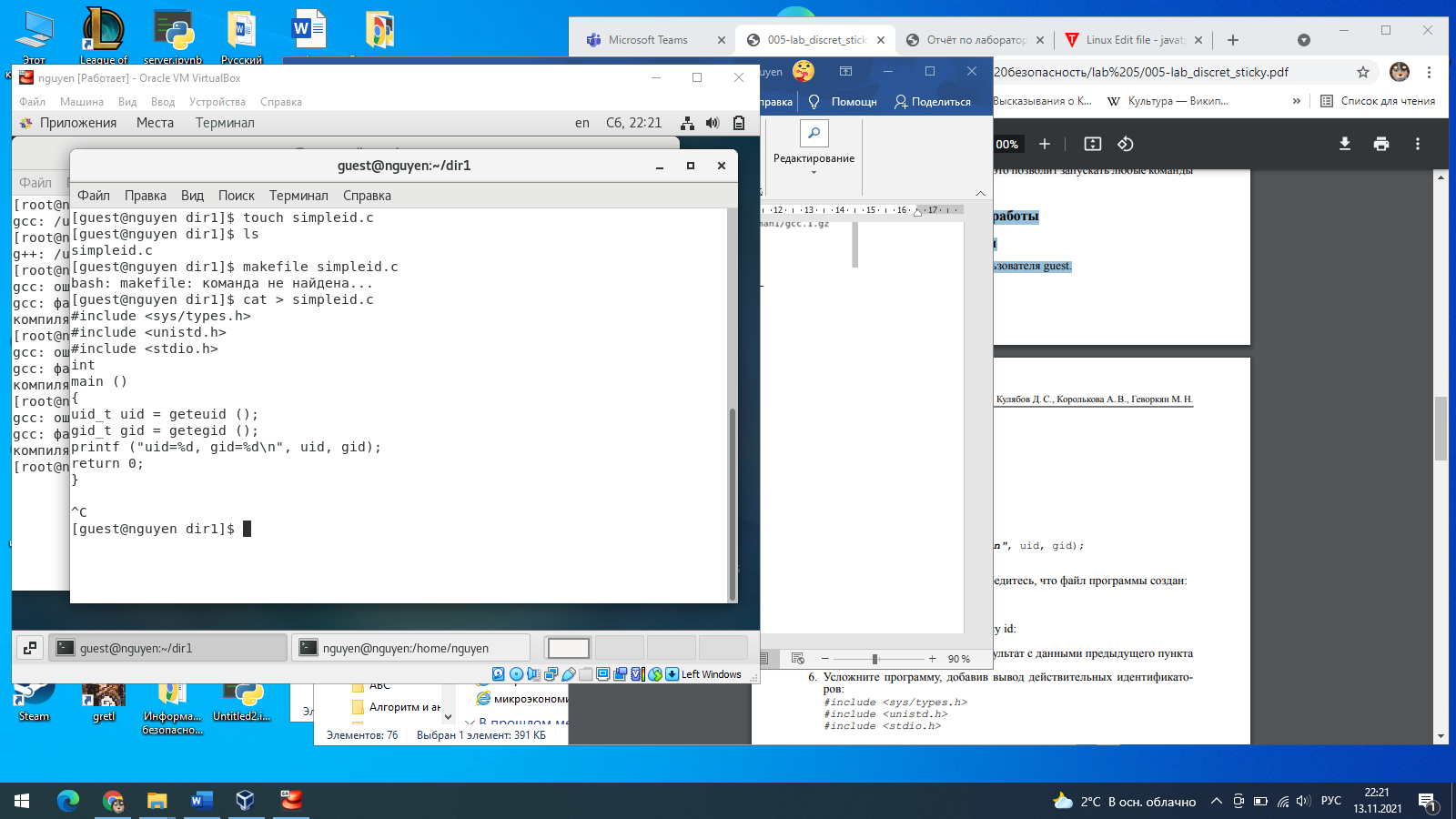


Figure 4: simpleid.c

1. Скомплилировать программу --- файл программы создан.
2. Выполнить программу simpleid.
3. Выполнить системную программу id.

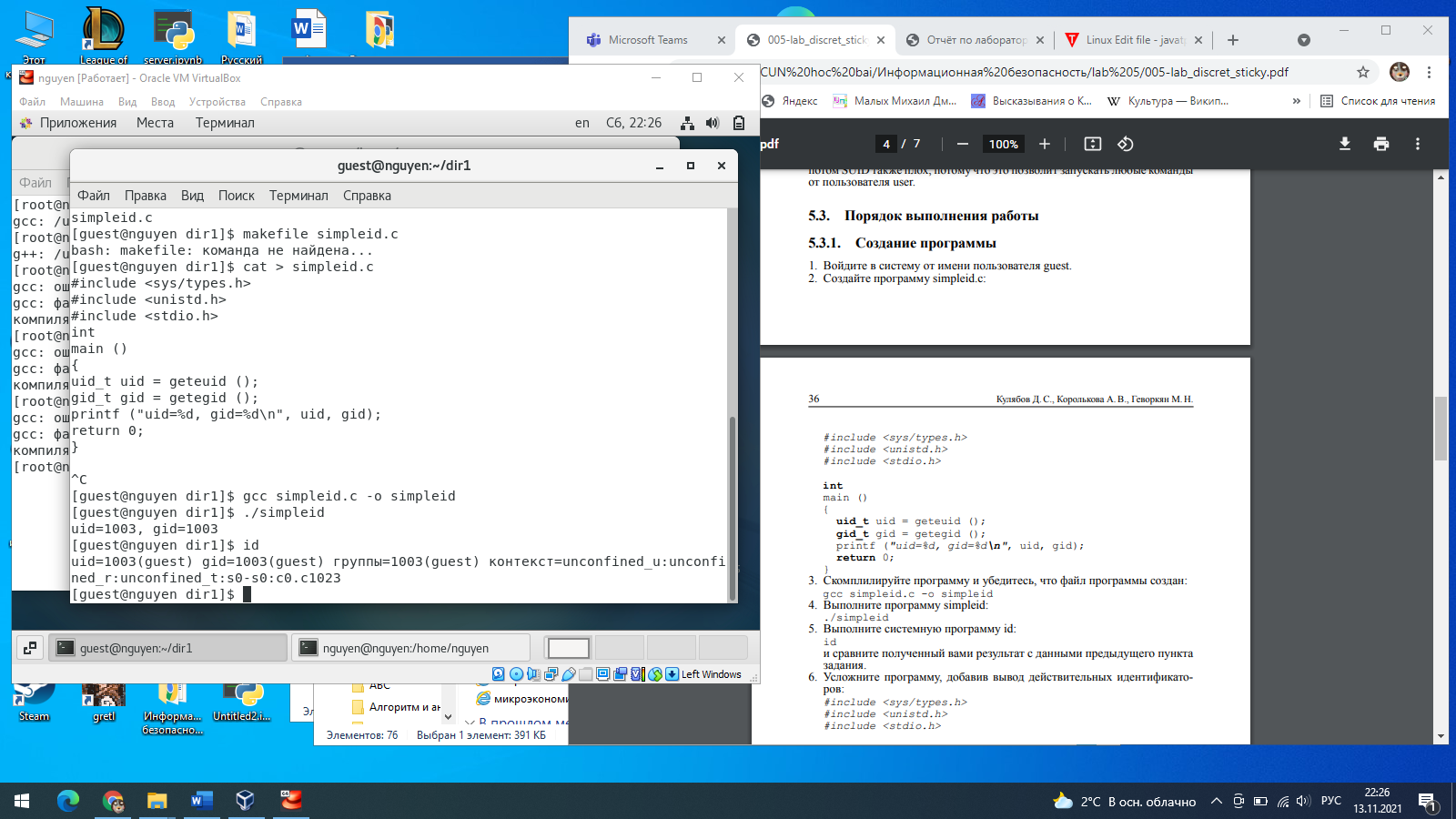


Figure 5: id

1. Усложнить программу, добавив вывод действительных идентификаторов.

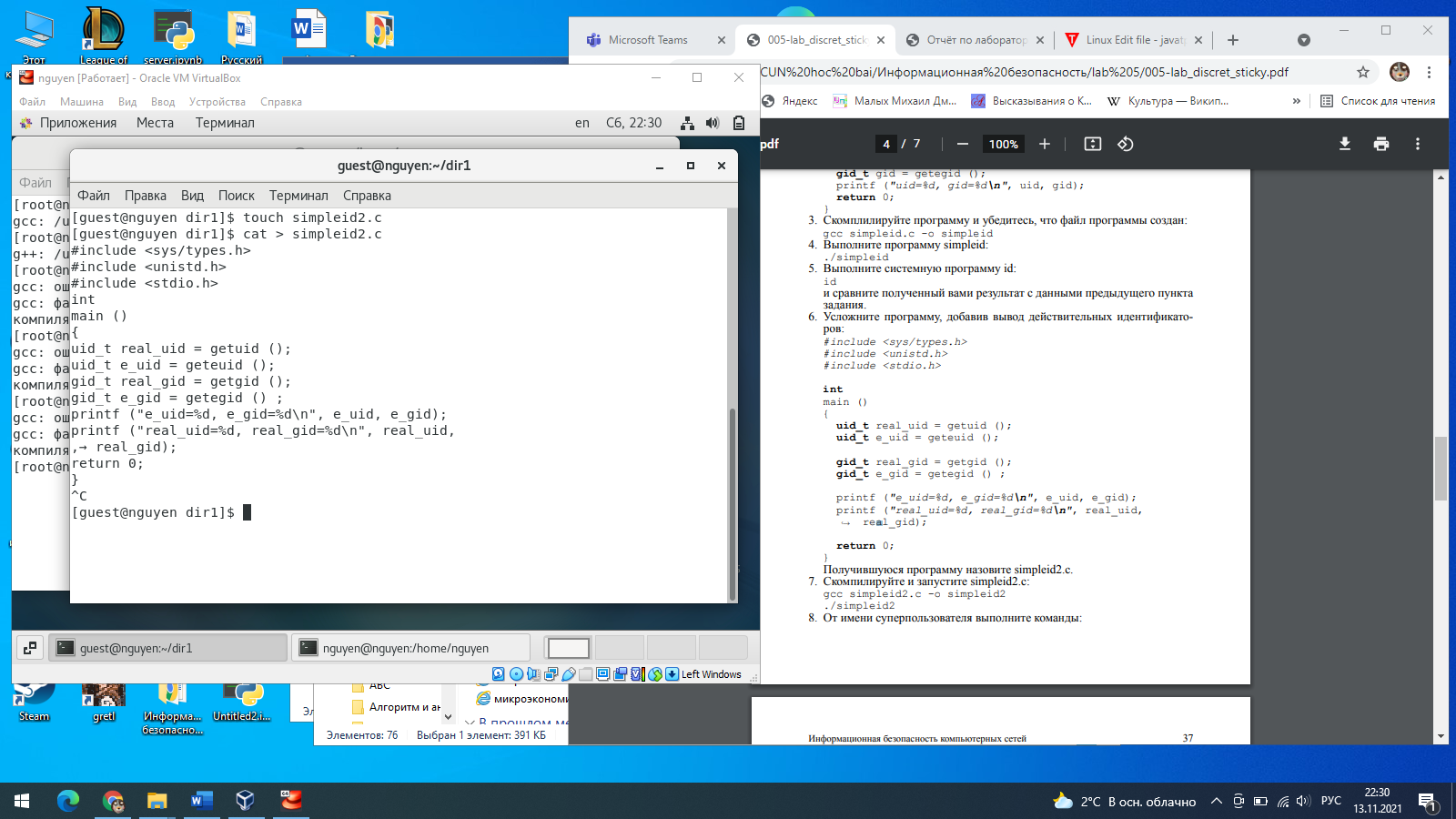


Figure 6: simpleid2.c

1. Скомпилировать и запустить simpleid2.c:

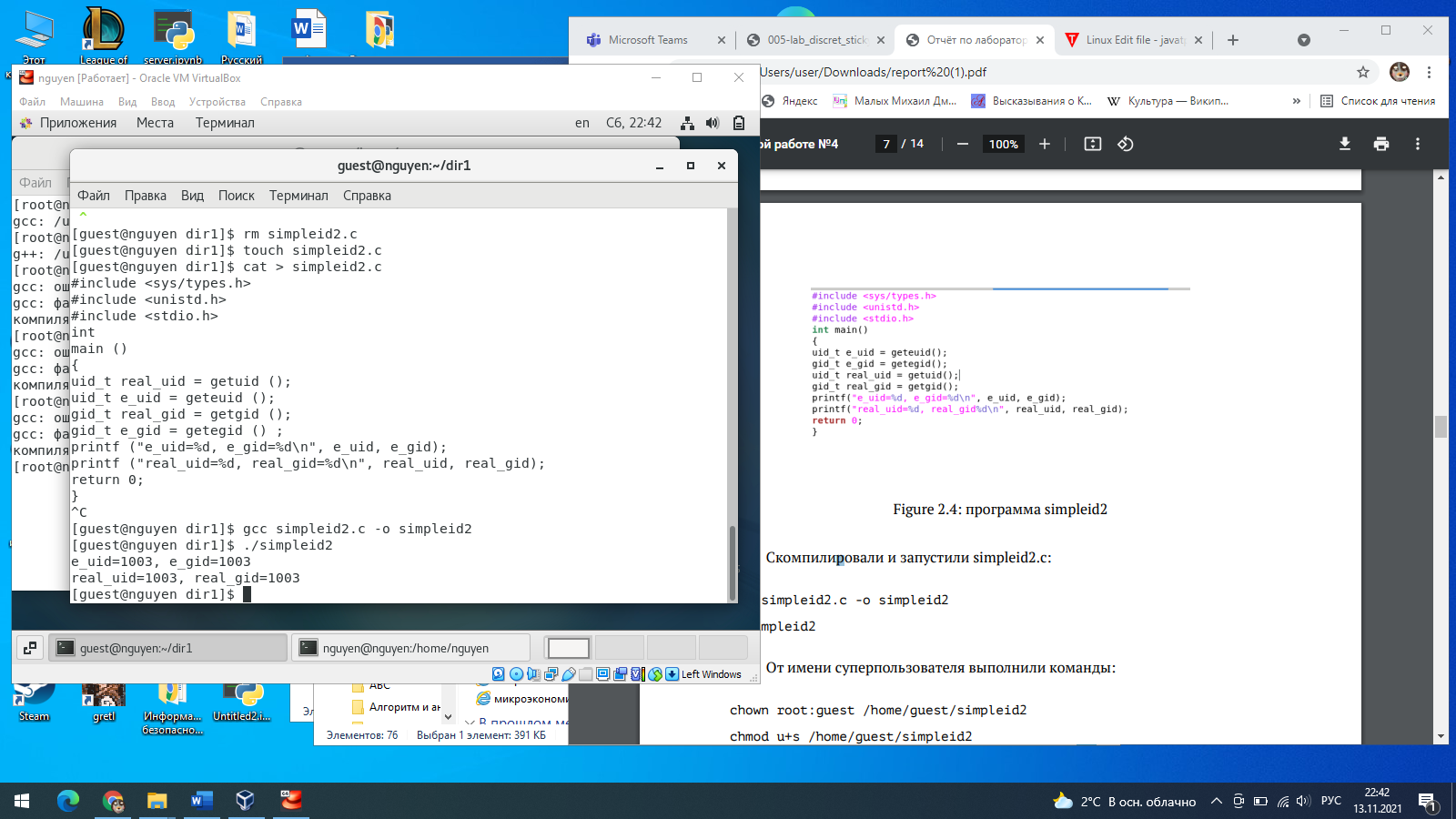


Figure 7: программа ./simpleid2

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

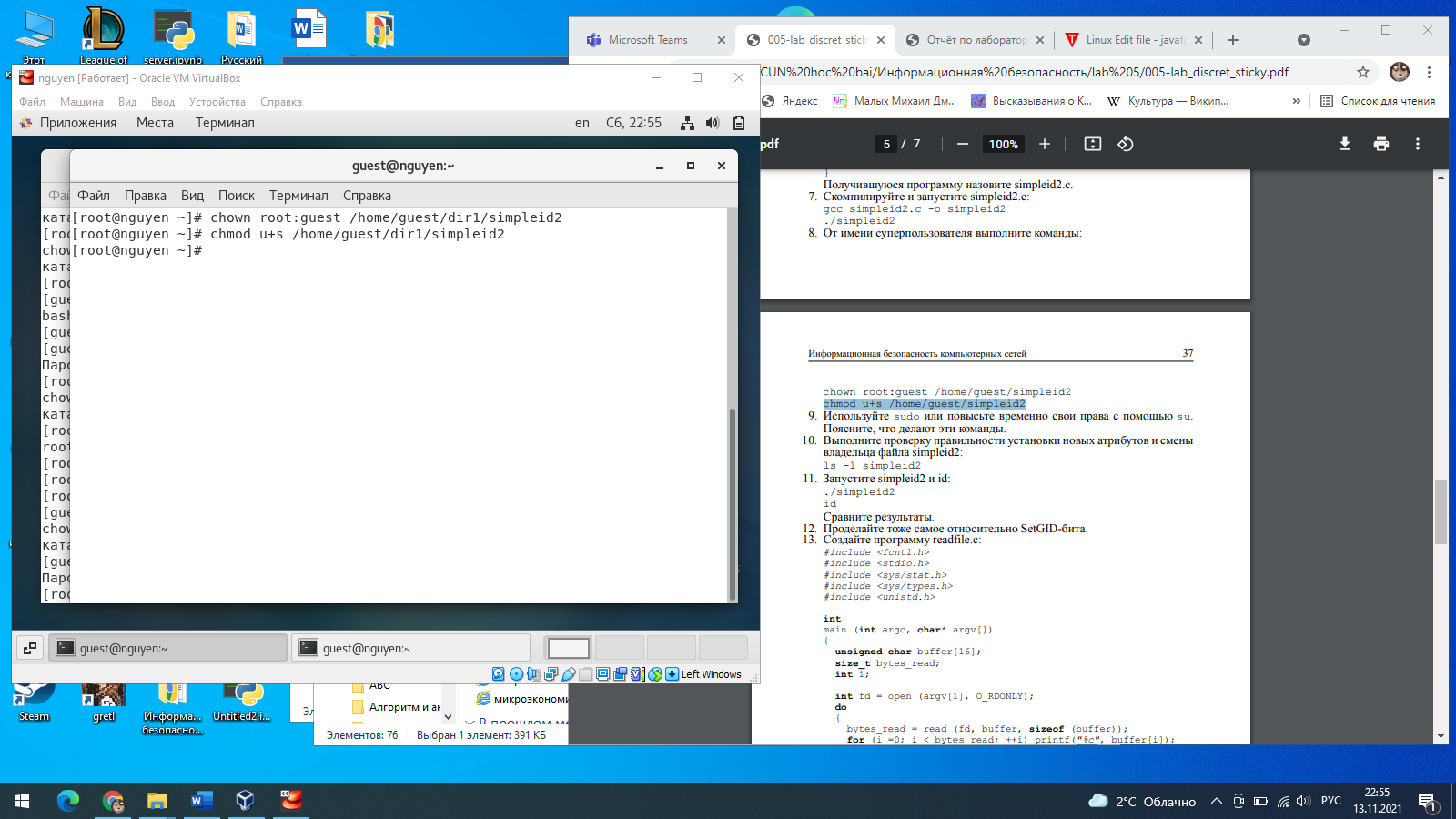


Figure 8: chown root:guest /home/guest/dir1/readfile.c

1. Использовать sudo или повысьте временно свои права с помощью su.
2. Выполнить проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

ls -l simpleid2

1. Запустить simpleid2 и id: ./simpleid2

id

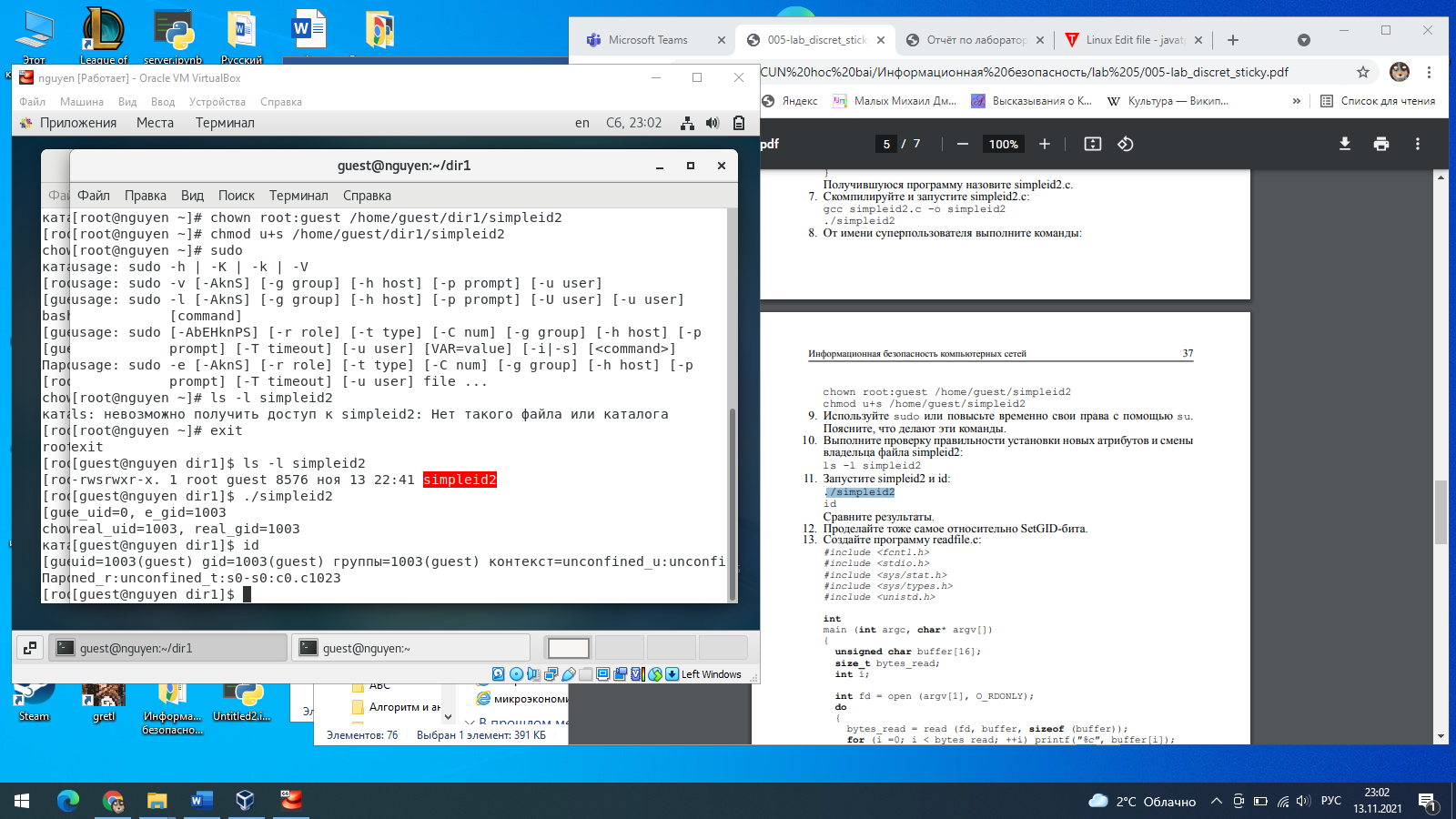
1. Проделать тоже самое относительно SetGID-бита.

Figure 9: ./simpleid2

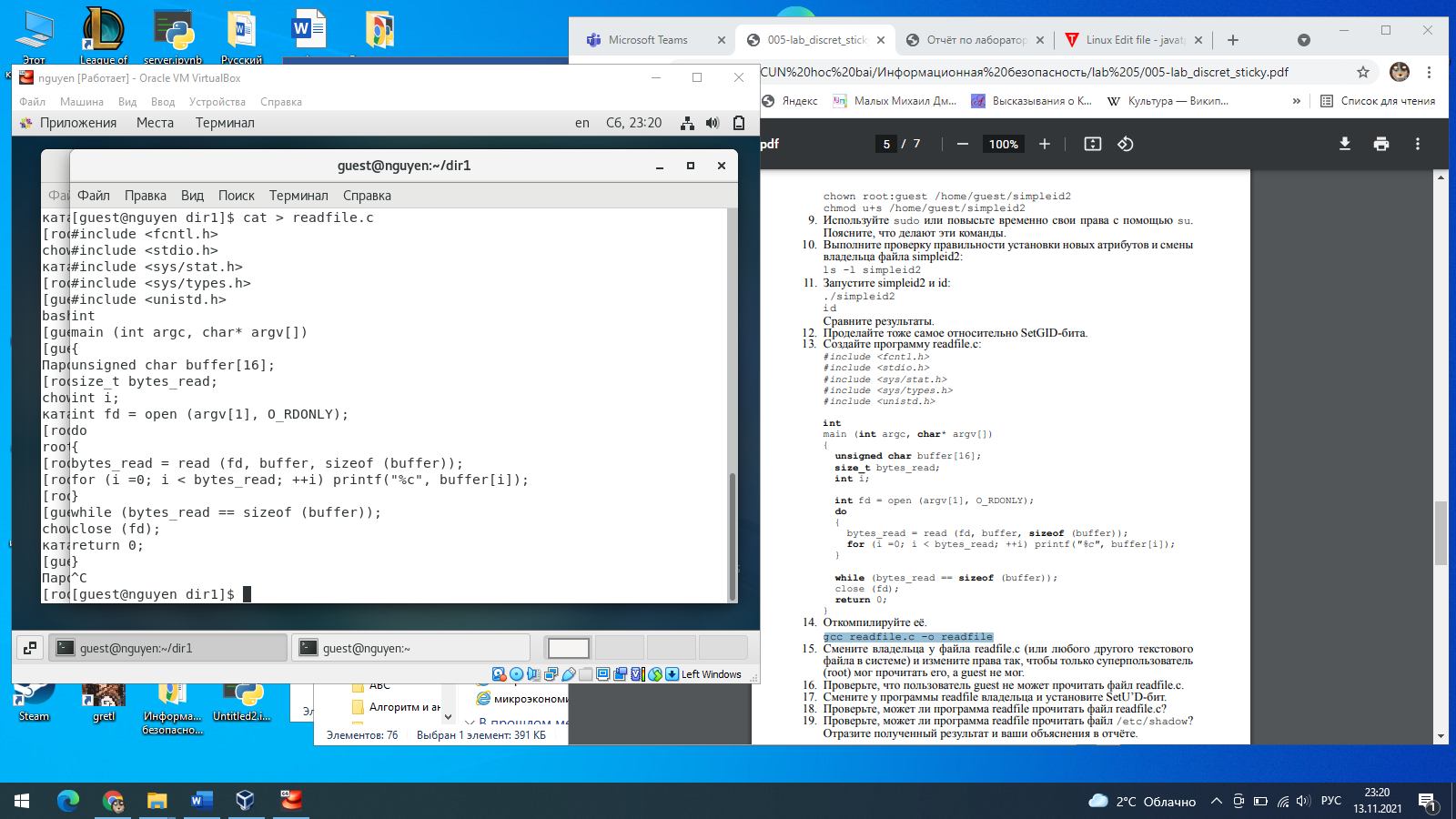
13. Создать программу readfile.c: 

Figure 10: readfile.c

14. Откомпилировать её. gcc readfile.c -o readfile

15. Сменить владельца у файла readfile.c и изменить права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. chown root:guest /home/guest/readfile.c chmod 700 /home/guest/readfile.c

16. Проверить, что пользователь guest не может прочитать файл readfile.c.

17. Сменить у программы readfile владельца и установить SetU’D-бит.

18. Проверить, может ли программа readfile прочитать файл readfile.c

19. Проверить, может ли программа readfile прочитать файл /etc/shadow

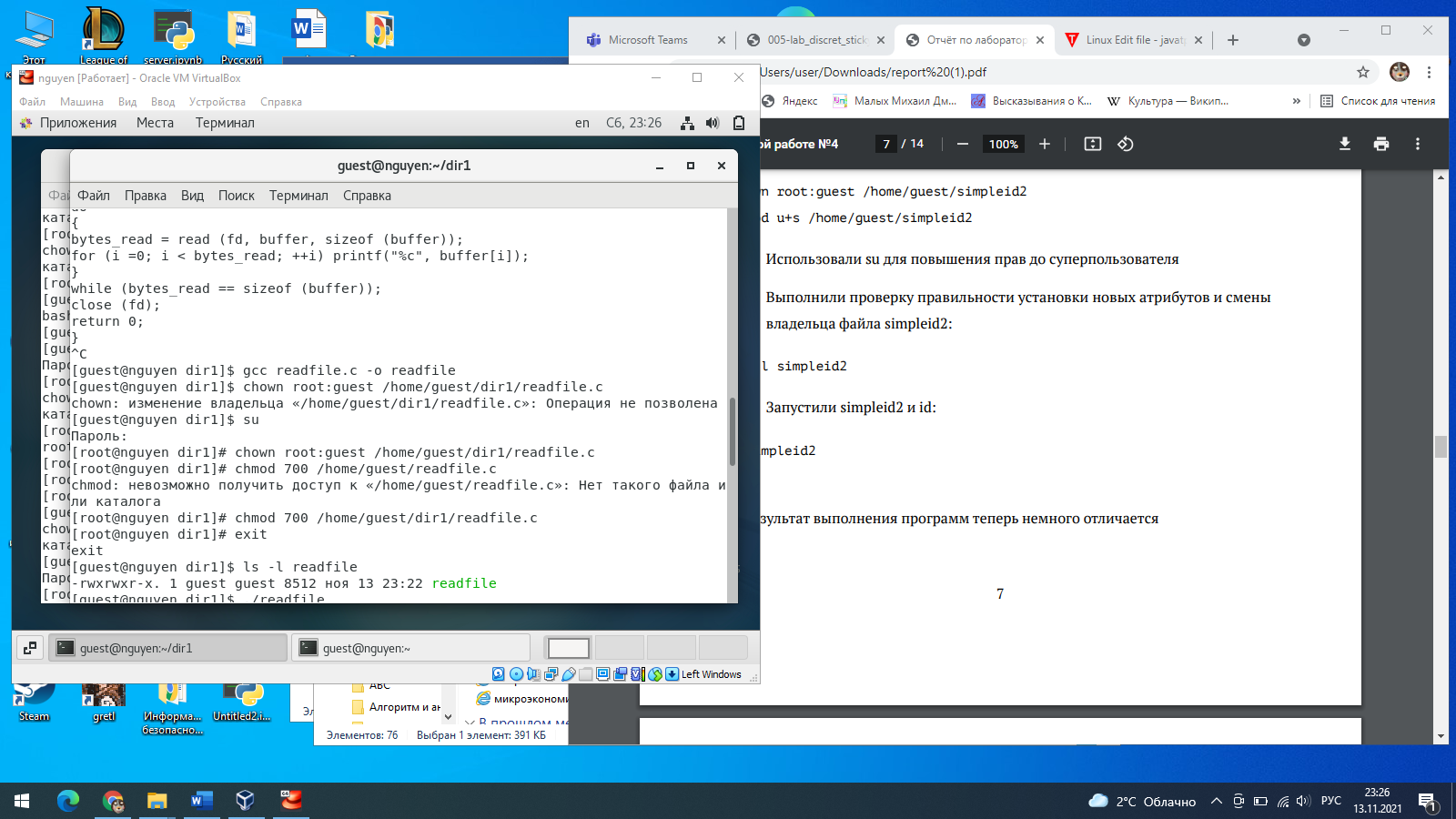


Figure 11: результат программы readfile

**3. Исследование Sticky-бита**

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего

выполните команду

ls -l / | grep tmp

2. От имени пользователя guest создайте файл file01.txt в директории /tmp

со словом test:

echo "test" > /tmp/file01.txt

3. Просмотрите 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

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

cat /tmp/file01.txt

5. От пользователя guest2 попробуйте дозаписать в файл

/tmp/file01.txt слово test2 командой

echo "test2" > /tmp/file01.txt

Удалось ли вам выполнить операцию?

6. Проверьте содержимое файла командой

cat /tmp/file01.txt

7. От пользователя guest2 попробуйте 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?

8. Проверьте содержимое файла командой

cat /tmp/file01.txt

9. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой

rm /tmp/fileOl.txt

Удалось ли вам удалить файл?

10. Повысьте свои права до суперпользователя следующей командой

su -

и выполните после этого команду, снимающую атрибут t (Sticky-бит) с

директории /tmp:

chmod -t /tmp

11. Покиньте режим суперпользователя командой

Exit

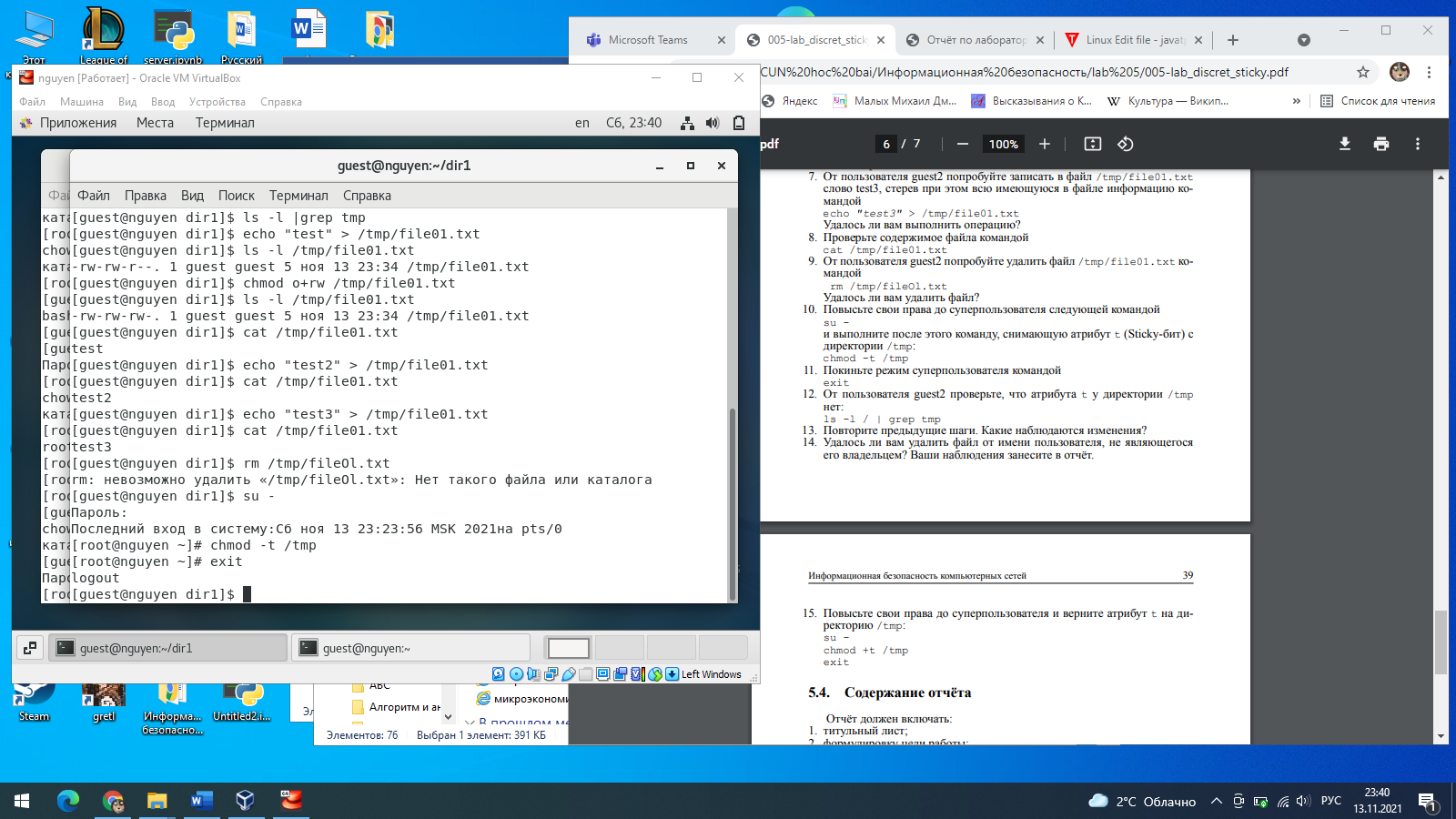


Figure 13: исследование

12. От пользователя guest2 проверьте, что атрибута t у директории /tmp

нет:

ls -l / | grep tmp

13. Повторите предыдущие шаги. Какие наблюдаются изменения?

14. Удалось ли вам удалить файл от имени пользователя, не являющегося

его владельцем? Ваши наблюдения занесите в отчёт.

Информационная безопасность компьютерных сетей 39

15. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp:

su -

chmod +t /tmp

exit

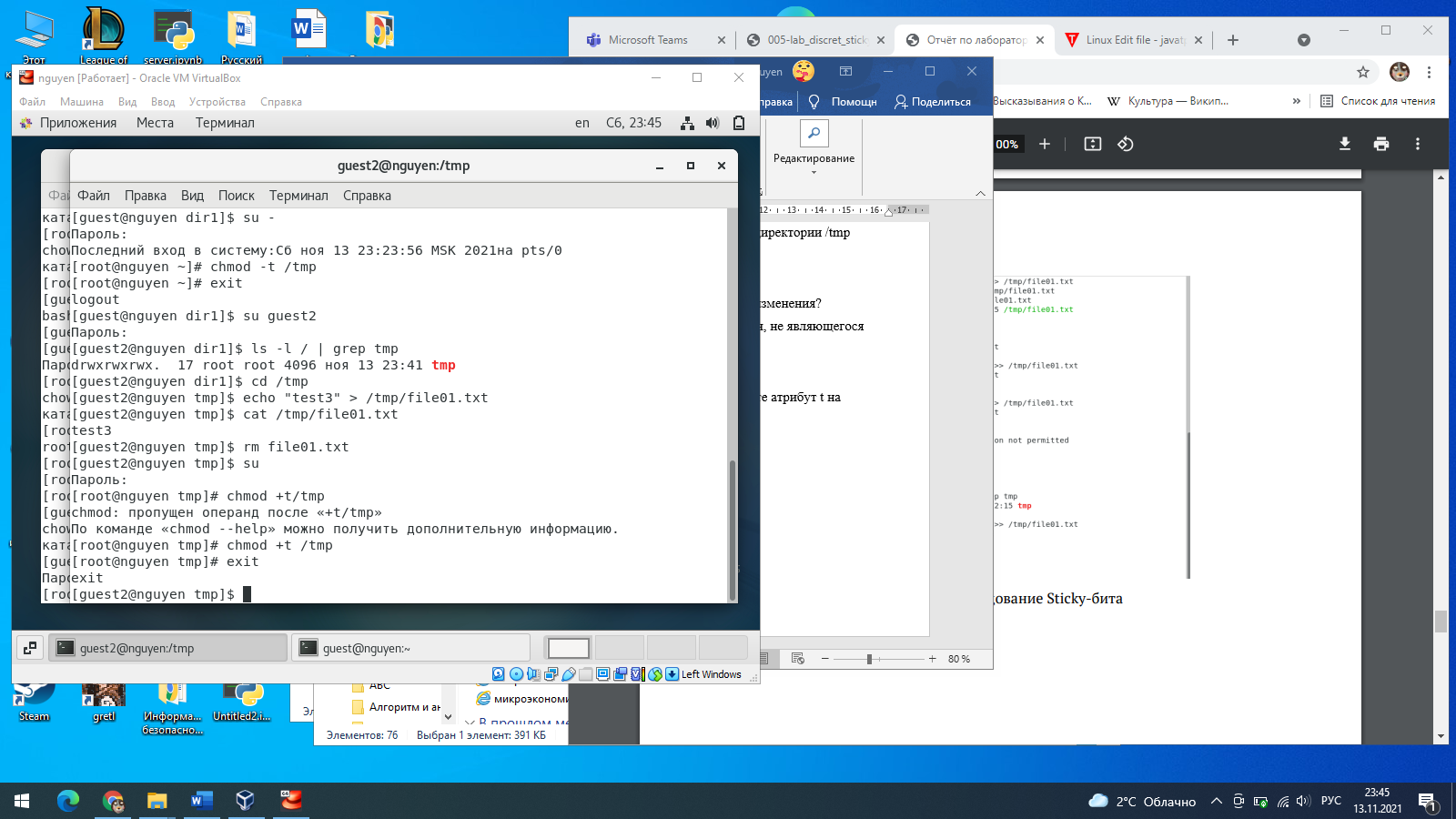


Figure 14: исследование Sticky-бита

**4. Вывод**

Изучили механизмы изменения идентификаторов, применения SetUID- и Stickyбитов. Получили практические навыки работы в консоли с дополнительными атрибутами. Также мы рассмотрели работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.