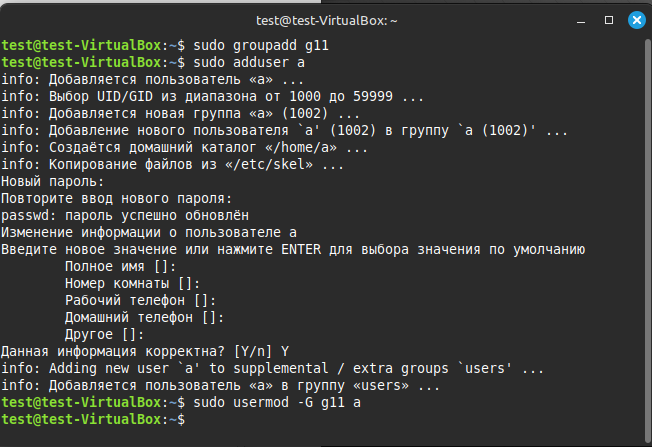
Лабораторная работа №8

Шулер М.А 1-МД-20

**2. Создать группу g11 и пользователя a в этой группе (через терминал)**



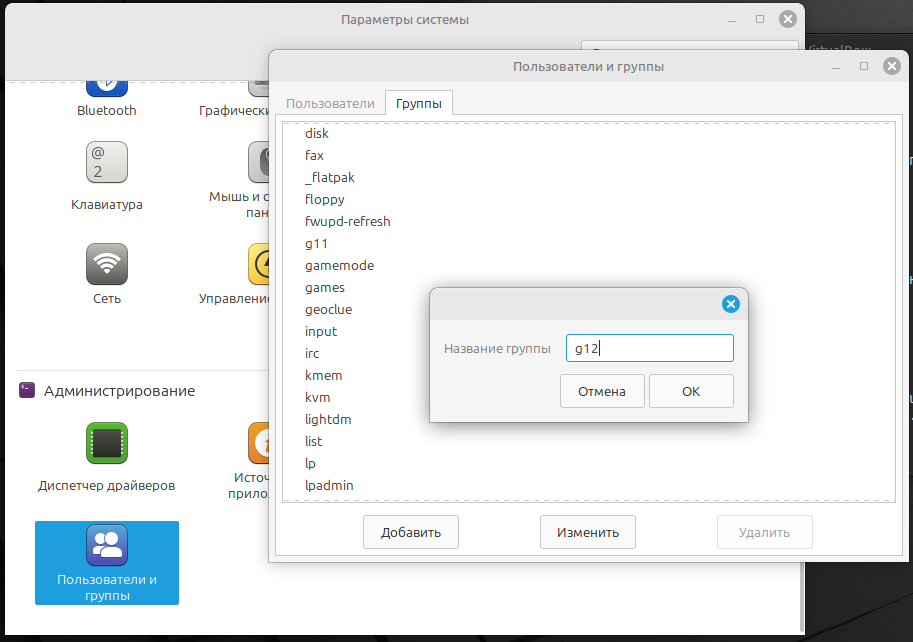
**sudo** — выполняет команду от имени администратора.

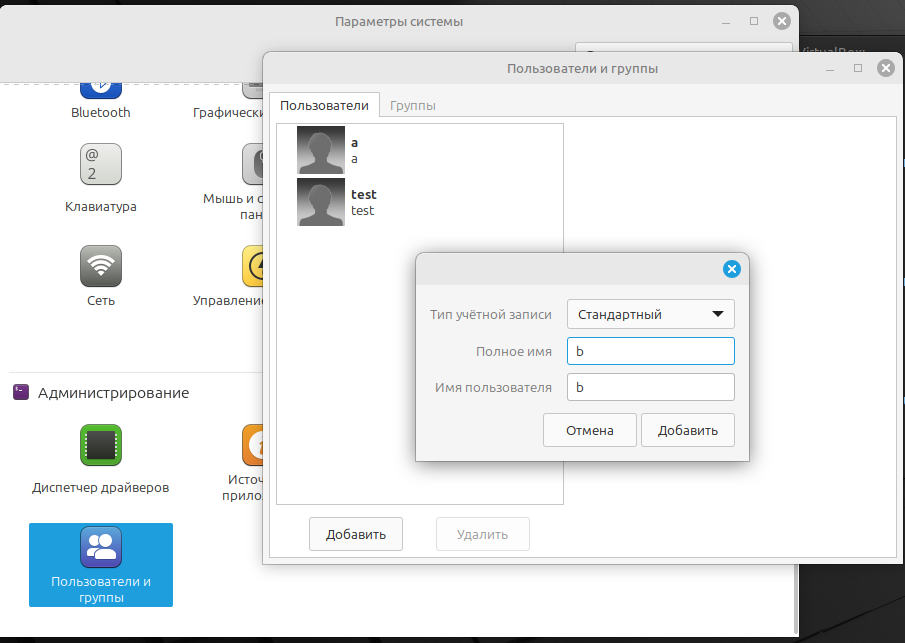
**groupadd g11** — создаёт группу с именем *g11*.

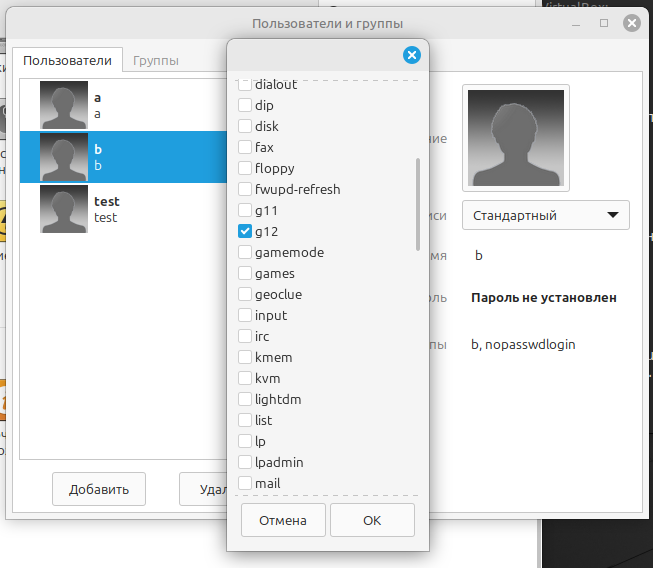
**adduser** — добавляет пользователя.

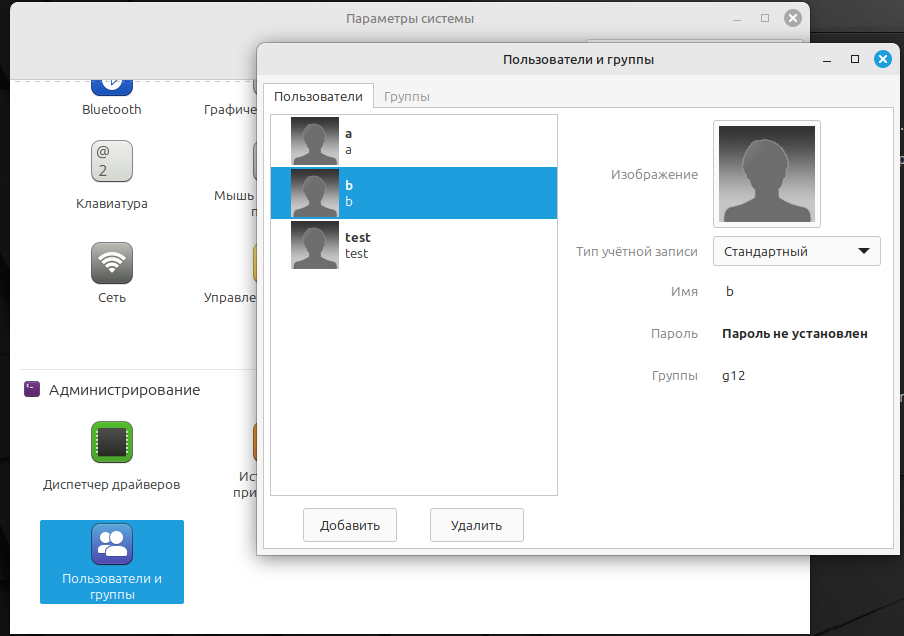
**Usermod -G g11 a** — добавляет пользователя *а* в группа *g11* и заменяет список групп, если такие были

**3. Создать группу g12 и пользователя b (через GUI)**

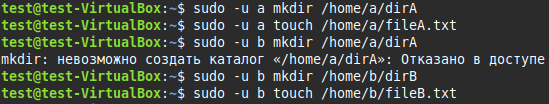


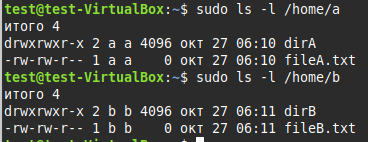






**4. В домашнем каталоге создать каталог и файл для каждого пользователя**





**sudo -u имя** — выполнить команду от имени конкретного пользователя.

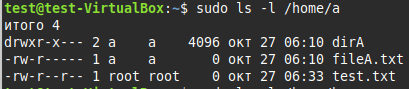
**mkdir** — создать каталог.

**touch** — создать пустой файл.

**5. Установка прав в 8-ричной форме и через маску**







**chmod** — изменить права доступа.

**umask(777 - 750 = 027)** - маску прав, чтобы при создании новых файлов и папок автоматически применялись такие же ограничения.

640 (файл):

* Владелец: rw- (чтение и запись)
* Группа: r-- (только чтение)
* Остальные: --- (никаких прав)

750 (каталог):

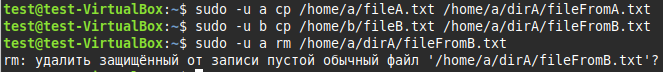
* Владелец: rwx (всё)
* Группа: r-x (чтение и выполнение)
* Остальные: ---

**6. Установить sticky-бит на один каталог**



**Sticky-бит (+t)** — запрещает пользователям удалять чужие файлы в этом каталоге.

**7. Проверить sticky-бит**

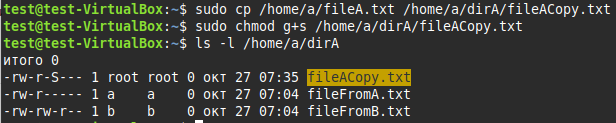


**cp** — копировать файл.

**rm** — удалить файл.

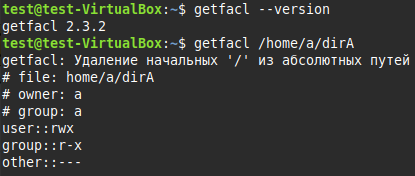
**sudo -u** — выполняем как другой пользователь, чтобы проверить права.

**8. Установка SGID на файл**



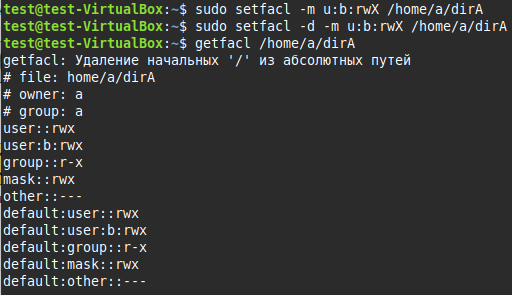
**chmod g+s** - Установить SGID-бит на этот файл

**9. Проверка поддержки ACL**



Поддержка есть

**10. Установка ACL и проверка**



**setfacl** - Установка ACL для конкретного пользователя

**-m** - modify (изменить ACL)

**-d** - default (по умолчанию для новых объектов)

**u:b:rwX** - для пользователя b права:

* r = чтение
* w = запись
* X = выполнение

**11. Контрольные вопросы**

1. **Группы пользователей** – объединяют пользователей для удобного управления правами; создаются командой groupadd, используются при назначении прав.
2. **Типы файлов ext3fs** – обычный файл, каталог, символическая ссылка, устройство, сокет, FIFO.
3. **Управление доступом** – через права чтения (r), записи (w), выполнения (x) для владельца, группы, остальных.
4. **Команда просмотра прав** – ls -l.
5. **Стандартные права** – rwx для владельца, группы и остальных; запись: буквами (rwx) или в 8-ричной системе (например, 755).
6. **Установка прав** – chmod [опции] [права] [файл/каталог], буквами или цифрами.
7. **SUID/SGID** – SUID: программа выполняется с правами владельца; SGID: файл – с правами группы, каталог – новые файлы наследуют группу каталога.
8. **Sticky** – предотвращает удаление файлов другими пользователями в каталоге.
9. **Установка битов** – chmod u+s file (SUID), chmod g+s file/dir (SGID), chmod +t dir (Sticky).
10. **ACL-списки** – дают гибкий контроль доступа, больше чем rwx.
11. **Недостатки ACL** – сложнее управление, не всегда совместимо со всеми инструментами.
12. **Виды ACL** – обычные и default; содержат пользователя/группу, права (rwx), маску.
13. **Подключение ACL** – файловая система монтируется с поддержкой acl (например, /etc/fstab опция acl).
14. **getfacl/setfacl** – просмотр и установка ACL.
15. **Проверка ACL** – getfacl filename.
16. **Маска эффективных прав** – ограничивает максимальные права группы и дополнительных пользователей.
17. **Правила по умолчанию** – задаются setfacl -d, новые файлы/каталоги наследуют права.
18. **Копирование ACL** – getfacl file | setfacl --set-file=- target.
19. **Создание пользователя в CLI** – sudo adduser username.
20. **Создание пользователя GUI** – через “Users and Groups” в Mint, можно менять группы и права.