Упражнение 1 Создание и просмотр файлов

1.

mkdir labrabota4

cd labrabota4/

2.

touch request.txt

3.

nano request.txt

4.

cat request.txt

tac request.txt

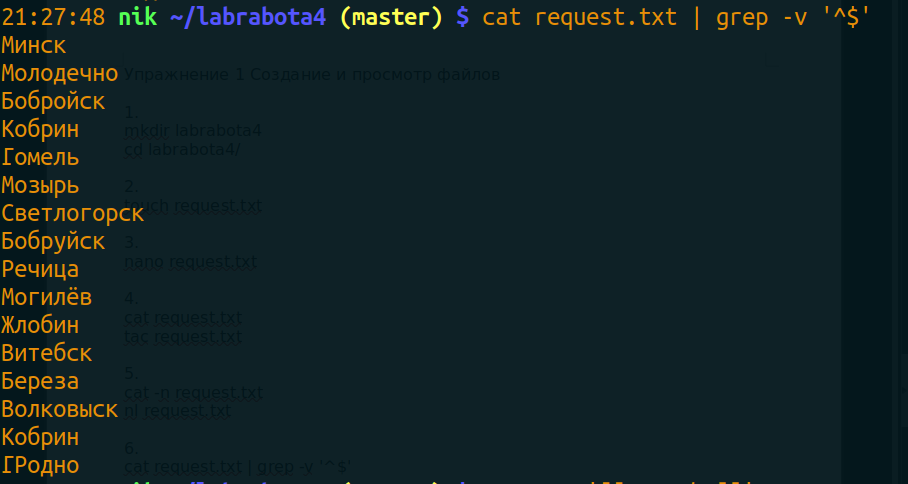
5.

cat -n request.txt

nl request.txt

6.

cat request.txt | grep -v '^$'

1

7.

grep -n '[[:graph:]]' request.txt



8.

head -n 7 request.txt

9.

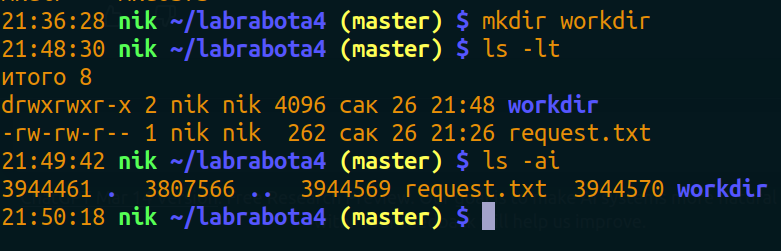
tail -n 6 request.txt

10.

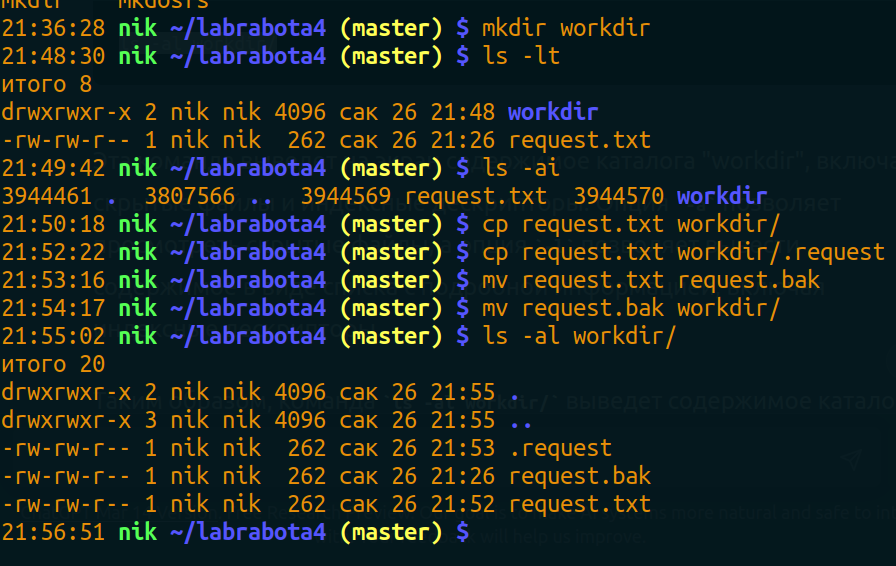
sort request.txt

sort -r request.txt

Упражнение 2 Создание и просмотр каталогов



Упражнение 3 Копирование и перемещение файлов



Упражнение 4 Работа со ссылками

2.

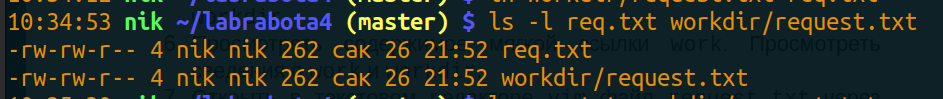
ln workdir/request.txt

3.

ln workdir/request.txt req.txt

4.

ls -l req.txt workdir/request.txt



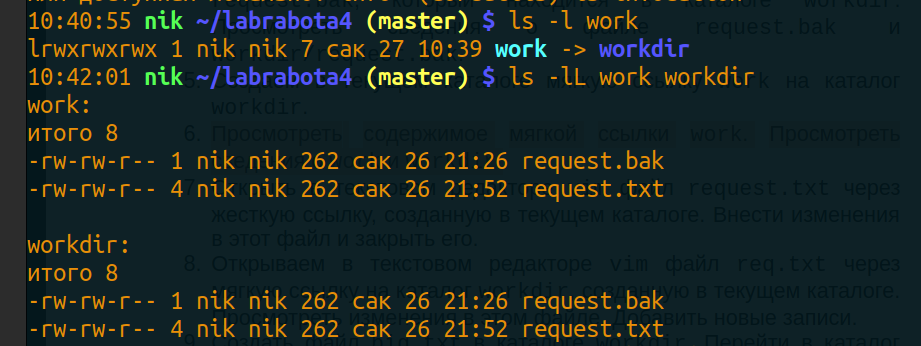
5.

ln -s workdir work

6.

ls -l work

ls -lL work workdir



7.

nano req.txt

8.

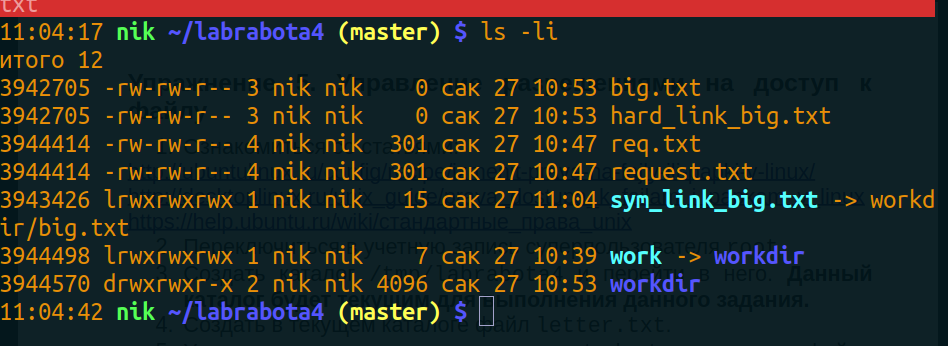
nano work/req.txt

9.

ln workdir/big.txt hard\_link\_big.txt

ln -s workdir/big.txt sym\_link\_big.txt

ls -li



10.

rm work

rm req.txt

rm hard\_link\_big.txt

rm sym\_link\_big.txt

Упражнение 5. Управление разрешениями на доступ к  
файлу

2. sudo -i

3. mkdir /tmp/labrabota4

cd /tmp/labrabota4/

4. touch letter.txt

5. useradd student

sudo chown student letter.txt

6.

sudo groupadd visitors

7.

useradd student1

sudo adduser student visitors

sudo adduser student1 visitors

8.

sudo chown :visitors letter.txt

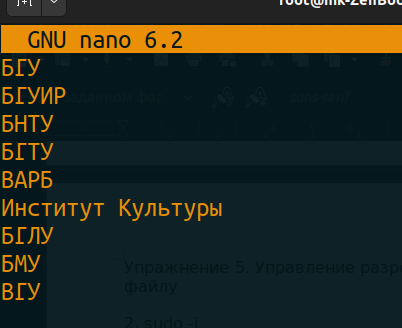
9. ls -l

chmod g+rw letter.txt

10.

sudo su student1

sudo nano letter.txt



11.

exit

12.

13.

14.

umask 0027

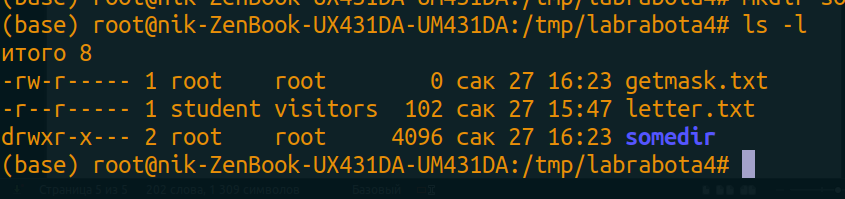
002 задают маску доступа для каталогов.

027 задают маску доступа для файлов.

15.

touch getmask.txt

mkdir somedir



16.

umask 0022

17.

touch file1 file2 file3 file4

chmod 700 file1

chmod 640 file2

chmod 310 file3

chmod 270 file4

18.

touch file5 file6 file7 file8

chmod u=rwx,g=---,o=--- file5

chmod u=rw-,g=r--,o=rwx file6

chmod u=-wx,g=---,o=r-- file7

chmod u=-w-,g=rwx,o=--w file8

19.

echo "obase=8; 2039027" | bc для перевода

touch file761

touch file363

chmod 761 file761 chmod u=rwx, g= rw-, o=--x для users полные права; для group чтение и запись файла; для others выполнение файла

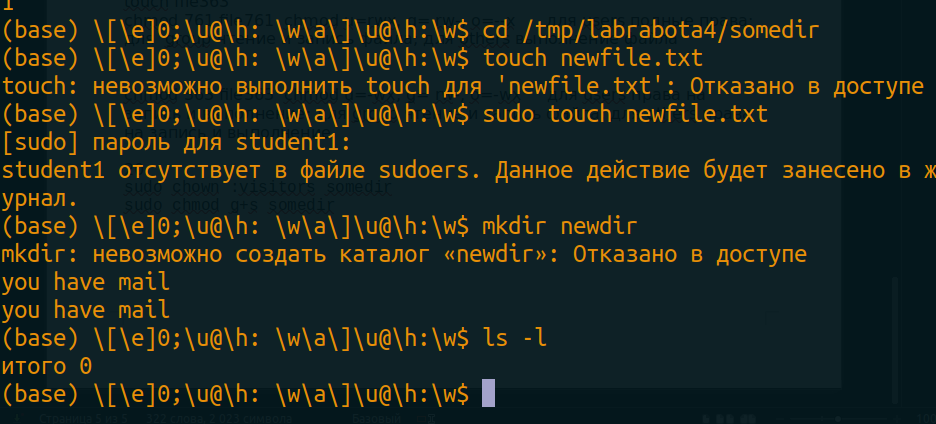
chmod 363 file363 chmod u=-wx, g= rw-, o=-wx для users права на запись и выполнение; для group чтение и запись файла; для others права на запись и выполнение.

20.

sudo chown :visitors somedir

sudo chmod g+s somedir

21.



22.

exit

Упражнение 6. Управление разрешениями на доступ к  
файлу с помощью списков контроля доступа

2. mkdir -p /tmp/labrabota4/example-acl

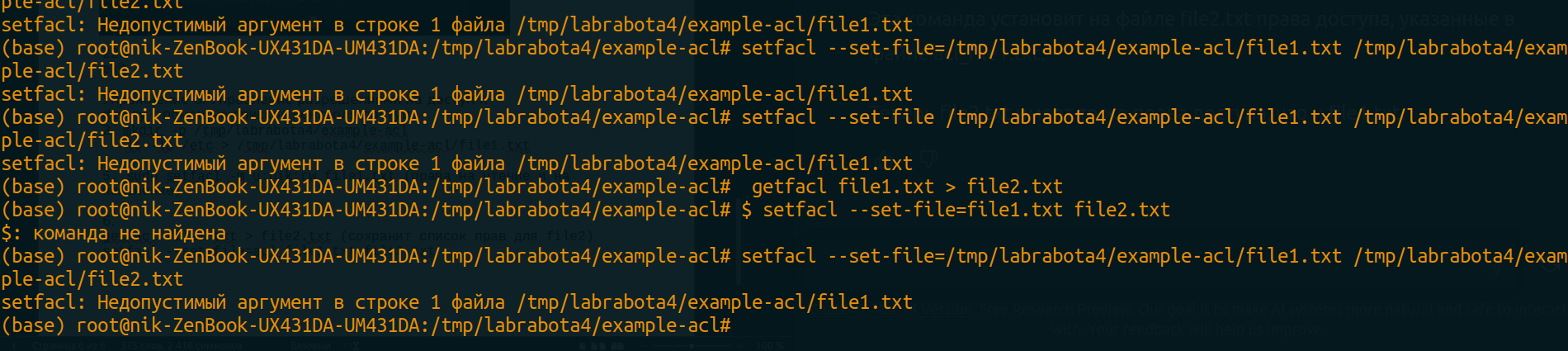
ls -la /etc > /tmp/labrabota4/example-acl/file1.txt

3. sudo setfacl -m u:nik:rw file1.txt (права на чтение и на изменение)

5

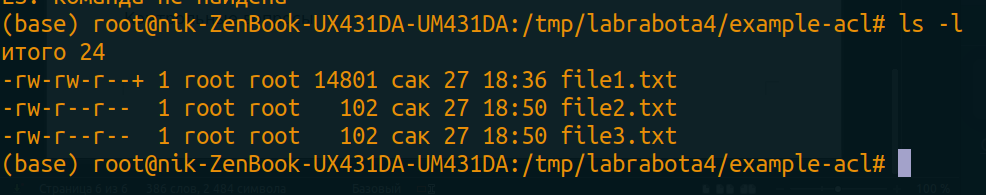
getfacl file1.txt > file2.txt (сохранит список прав для file2)

setfacl --set-file=acl\_file1.txt file2.txt (установит права для file3)



6.

cp --preserve=acl file2.txt file3.txt

7.

8. sudo setfacl -m g:visitors:rwx example-acl/

Добавит права rwx для группы visitors на каталог example-acl

9. cat /tmp/labrabota4/letter.txt >/tmp/labrabota4/example-acl/file5.txt

10.

ls -li file5.txt

11.

ls — l file1-5.txt

12.

rm -r /tmp/labrabota4

Контрольные вопросы

1. Чем о`тличается вывод команд ls -F и ls -Fla?

ls -F добавляет к каждому элементу вывода символ, указывающий на тип файла или каталога.

ls -Fla добавляет к каждому элементу вывода символ, указывающий на тип файла или каталога, а также выводит дополнительную информацию о файлах, включая права доступа, количество ссылок, владельца и группу

2. Что такое «жёсткая ссылка»

Синонимом для файла. Дополнительный указатель на файл, имеет тот же inode, что и файл

3. Что такое «символическая ссылка»?

Ссылка на файл, имеет иной inode.

4. Сравните права доступа к директориям /bin и /tmp. Какие  
операции сможет совершать в них простой пользователь?

bin - rwxrwxrwx - обычный пользователь (не владелец) обладает полными правами (чтение, запись, исполнение)

tmp - rwxrwxrwt - обычный пользователь не может удалить файлы, созданные другими пользователями

5. Какой командой необходимо задать права на текстовый файл  
таким образом, чтобы он мог просматриваться только владельцем  
и никем не мог редактироваться?

chmod 400 file\_name

6. Что смогут делать другие пользователями с файлами в домашней  
директории пользователя, если он задаст всем остальным  
пользователям право на запись в директорию, но удалит право  
исполнения на неё?

Смогут создавать файлы, директории, но не смогут зайти или посмотреть файлы в директории

7.Какие права установлены на файлы в Вашем домашнем каталоге?  
Сможет ли другой пользователь его просматривать? Изменять?

-rw-rw-r--, для других пользователей только чтение.

8. Какое значение имеет право на запись для каталога?

Создание файлов/каталогов

9. Какое значение имеет право на исполнение для каталога?

Возможность войти/посмотреть содержимое каталога

10. Как добавить программе флаг исполнения?

chmod +x file

11. Что такое бит suid? Что он делает?

Бит смены идентификатора пользователя (файлу при исполнении назначаются права его владельца)

12. Зачем нужны uid и gid?

Для идентификаторы пользователя и группы

13. Почему uid пользователя задаётся 1000 или более?

Это связано с тем, что многие системы Linux предназначены для многопользовательской работы, и первые UID (от 0 до 999) могут быть зарезервированы для системных процессов и служб.

14. С помощью какой команды можно найти все исполняемые  
файлы с установленным suid-битом?

find . -perm /4000

15. Какая маска разрешений задана по умолчанию? В каком  
файле задается значение системной маски разрешений? Можно ли  
его изменить?

022что означает, что пользователь имеет права на чтение и запись, а группа и остальные - только на чтение.

Хранится /etc/profile

С помощью umask

16.Будут ли утеряны права ACL при перемещении файлов с  
помощью команды mv?

Нет, если использовать -а для сохранение атрибутов файла, включая ACL

16. С каким ключом необходимо выполнять команду cp, чтобы не  
потерялись права ACL?

-p