

# Отчёт по лабораторной работе №2

## Дискреционное разграничение прав в CentOS

Оразклычев Давут НФИбд-02-18

### Содержание

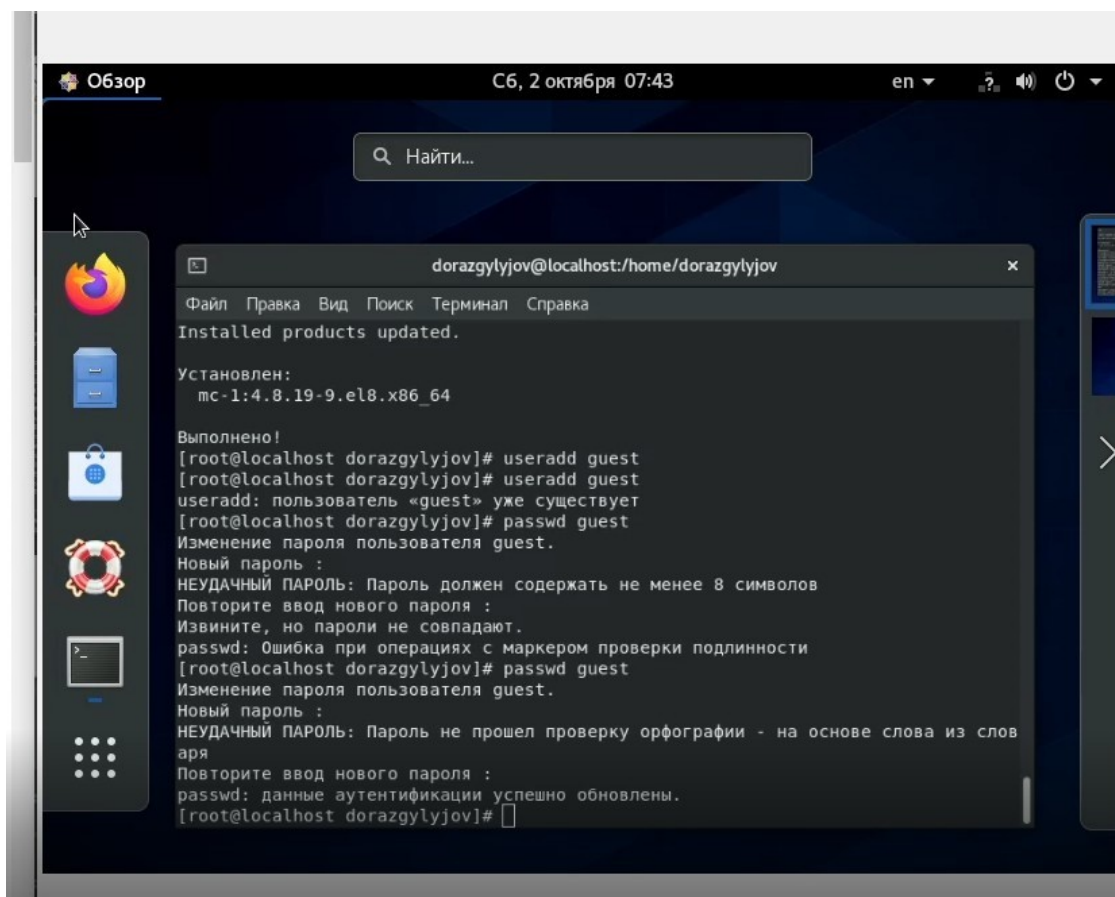
Цель работы.....	1
Выполнение лабораторной работы.....	1
Вывод.....	9

### Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе CentOS

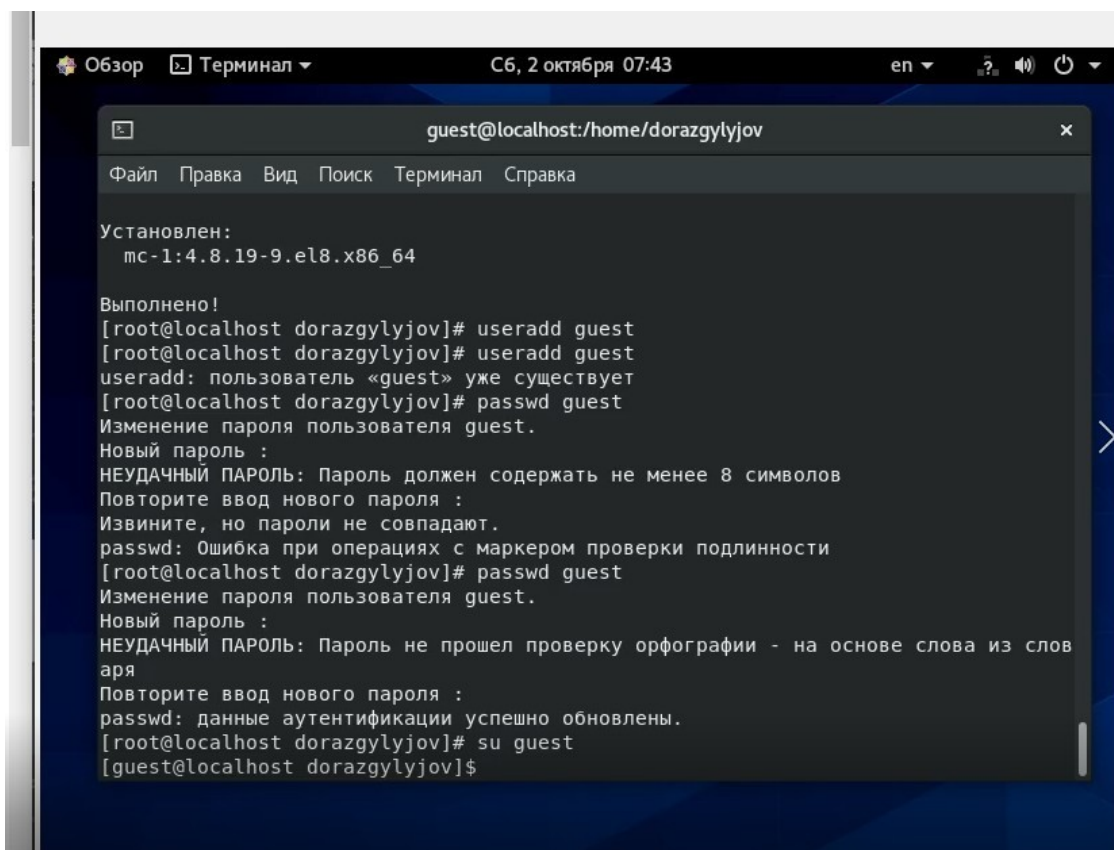
### Выполнение лабораторной работы

1. Создали учётную запись пользователя *guest* (используя учётную запись администратора) и задали ему пароль:



*Создание пользователя guest и задание пароля*

2. *Вошли в систему от имени пользователя guest*



The screenshot shows a terminal window titled "guest@localhost:/home/dorazgylyjov". The window has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal output is as follows:

```
Установлен:
  mc-1:4.8.19-9.el8.x86_64

Выполнено!
[root@localhost dorazgylyjov]# useradd guest
[root@localhost dorazgylyjov]# useradd guest
useradd: пользователь «guest» уже существует
[root@localhost dorazgylyjov]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля :
Извините, но пароли не совпадают.
passwd: Ошибка при операциях с маркером проверки подлинности
[root@localhost dorazgylyjov]# passwd guest
Изменение пароля пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - на основе слова из слов
аря
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@localhost dorazgylyjov]# su guest
[guest@localhost dorazgylyjov]$
```

*Вход в систему с guest*

3. Командой *pwd* определили директорию, в которой находимся
4. Уточнили имя нашего пользователя командой *whoami*
5. Уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой *id*. Сравнили вывод *id* с выводом команды *groups* - *id* выдает всю информацию *gid*, *id*, группы *т.д.*, а *groups* выводит только имя группы - *guest.gid = 1001(guest)*

```
guest@localhost:/home/dorazgylyjov
Файл Правка Вид Поиск Терминал Справка
[guest@localhost dorazgylyjov]$ pwd
/home/dorazgylyjov
[guest@localhost dorazgylyjov]$ home
bash: home: команда не найдена...
cd [guest@localhost dorazgylyjov]$ cd home
bash: cd: home: Отказано в доступе
[guest@localhost dorazgylyjov]$ su root
Пароль:
[root@localhost dorazgylyjov]# cd home
bash: cd: home: Нет такого файла или каталога
[root@localhost dorazgylyjov]# su guest
[guest@localhost dorazgylyjov]$ whoami
guest
[guest@localhost dorazgylyjov]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost dorazgylyjov]$ groups
guest
[guest@localhost dorazgylyjov]$ ls
ls: невозможно открыть каталог '.': Отказано в доступе
[guest@localhost dorazgylyjov]$ .
bash: .: требуется аргумент с именем файла
.: использование: . файл [аргументы]
[guest@localhost dorazgylyjov]$
```

Команды: *pwd*, *whoami*, *id*, *groups*

6. Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедимся, что они совпадают
7. Просмотрим файл */etc/passwd* Командой: *cat /etc/passwd*. Найдём в нём свою учётную запись. Определим *uid* пользователя. Определим *gid* пользователя. Сравним найденные значения с полученными в предыдущих пунктах.

The screenshot shows a terminal window titled 'guest@localhost:~'. The terminal displays the output of the command `cat /etc/passwd | grep guest`. The output lists system users and the 'guest' user. The 'guest' user entry is highlighted in red text: `guest:x:1001:1001::/home/guest:/bin/bash`. The terminal window has a menu bar with 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The top status bar shows 'Обзор', 'Терминал', the date 'Сб, 2 октября 07:49', and language 'en'.

```
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
sasauth:x:992:76:Sasauthd user:/run/sasauthd:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/sbin/nologin
sssd:x:984:984:User for sssd:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980::/var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
dorazgylyjov:x:1000:1000:dorazgylyjov:/home/dorazgylyjov:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@localhost ~]$
```

Команда `cat /etc/passwd` с фильтром и без

8. Определим существующие в системе директории командой `ls -l /home/`
9. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.
10. Создали в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1`.
11. Сняли с директории `dir1` все атрибуты командой `chmod 000 dir1` и проверили с помощью `ls -l` правильность выполнения команды `chmod`.

```
Обзор Терминал Сб, 2 октября 09:35 en ? ? ?
guest@localhost:~
Файл Правка Вид Поиск Терминал Справка
[guest@localhost ~]$ cd home
bash: cd: home: Нет такого файла или каталога
[guest@localhost ~]$ cd ~
[guest@localhost ~]$ pwd
/home/guest
[guest@localhost ~]$ mkdir dir1
[guest@localhost ~]$ ls
dir1
[guest@localhost ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest guest 6 окт  2 07:52 dir1
[guest@localhost ~]$ lsattr
----- ./dir1
[guest@localhost ~]$ chmod 000 dir1
[guest@localhost ~]$ ls -l
итого 0
d----- . 2 guest guest 6 окт  2 07:52 dir1
[guest@localhost ~]$ echo 'test' > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@localhost ~]$ echo 'test' /home/guest/dir1/file1
test /home/guest/dir1/file1
[guest@localhost ~]$ ls
dir1
[guest@localhost ~]$ cd dir`
```

Правильность выполнения команды

12. Попытались создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1`. Однако получили отказ из-за недостатка прав

```
[guest@localhost ~]$ echo 'test' > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
```

Попытка создать файл в директории

13. Заполним таблицу «Установленные права и разрешённые действия». Выполняем от лица пользователя `guest` (т.е. от создателя директории). Нужно проверить все 64 варианта атрибутов на различные права в директориях и файлах

Права для всех 64 вариантов атрибутов

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
000	000	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	+
200	000	-	-	-	-	-	-	-	-
300	000	+	+	-	-	+	-	+	+
400	000	-	-	-	-	-	-	-	-

<i>Права директ ории</i>	<i>Пра ва фай ла</i>	<i>Созда ние файл а</i>	<i>Удале ние файла</i>	<i>Зап ись в фай л</i>	<i>Чте ние фай ла</i>	<i>Смена директ ории</i>	<i>Просмо тр файлов в директ ории</i>	<i>Переимено вание файла</i>	<i>Смена атриб утов файла</i>
500	000	-	-	-	-	+	+	-	+
600	000	-	-	-	-	-	-	-	-
700	000	+	+	-	-	+	+	+	+
000	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	+
400	100	-	-	-	-	-	-	-	-
500	100	-	-	-	-	+	+	-	+
600	100	-	-	-	-	-	-	-	-
700	100	+	+	-	-	+	+	+	+
000	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	200	+	+	+	-	+	-	+	+
400	200	-	-	-	-	-	-	-	-
500	200	-	-	+	-	+	+	-	+
600	200	-	-	-	-	-	-	-	-
700	200	+	+	+	-	+	+	+	+
000	300	-	-	-	-	-	-	-	-
100	300	-	-	+	-	+	-	-	+
200	300	-	-	-	-	-	-	-	-
300	300	+	+	+	-	+	-	+	+
400	300	-	-	-	-	-	-	-	-
500	300	-	-	+	-	+	+	-	+
600	300	-	-	-	-	-	-	-	-
700	300	+	+	+	-	+	+	+	+
000	400	-	-	-	-	-	-	-	-
100	400	-	-	-	+	+	-	-	+
200	400	-	-	-	-	-	-	-	-
300	400	+	+	-	+	+	-	+	+
400	400	-	-	-	-	-	-	-	-
500	400	-	-	-	+	+	+	-	+

<i>Права директ ории</i>	<i>Пра ва фай ла</i>	<i>Созда ние файл а</i>	<i>Удале ние файла</i>	<i>Зап ись в фай л</i>	<i>Чте ние фай ла</i>	<i>Смена директ ории</i>	<i>Просмо тр файлов в директ ории</i>	<i>Переимено вание файла</i>	<i>Смена атриб утов файла</i>
600	400	-	-	-	-	-	-	-	-
700	400	+	+	-	+	+	+	+	+
000	500	-	-	-	-	-	-	-	-
100	500	-	-	-	+	+	-	-	+
200	500	-	-	-	-	-	-	-	-
300	500	+	+	-	+	+	-	+	+
400	500	-	-	-	-	-	-	-	-
500	500	-	-	-	+	+	+	-	+
600	500	-	-	-	-	-	-	-	-
700	500	+	+	-	+	+	+	+	+
000	600	-	-	-	-	-	-	-	-
100	600	-	-	+	+	+	-	-	+
200	600	-	-	-	-	-	-	-	-
300	600	+	+	+	+	+	-	+	+
400	600	-	-	-	-	-	-	-	-
500	600	-	-	+	+	+	+	-	+
600	600	-	-	-	-	-	-	-	-
700	600	+	+	+	+	+	+	+	+
000	700	-	-	-	-	-	-	-	-
100	700	-	-	+	+	+	-	-	+
200	700	-	-	-	-	-	-	-	-
300	700	+	+	+	+	+	-	+	+
400	700	-	-	-	-	-	-	-	-
500	700	-	-	+	+	+	+	-	+
600	700	-	-	-	-	-	-	-	-
700	700	+	+	+	+	+	+	+	+

*Для заполнения последних двух строк опытным путем проверили минимальные права.*

*Список минимальных прав для указанных операций*

<i>Операция</i>	<i>Права на директорию</i>	<i>Права на файл</i>
<i>Создание файла</i>	<i>300</i>	<i>000</i>
<i>Удаление файла</i>	<i>300</i>	<i>000</i>



<i>Операция</i>	<i>Права на директорию</i>	<i>Права на файл</i>
<i>Чтение файла</i>	<i>100</i>	<i>400</i>
<i>Запись в файл</i>	<i>100</i>	<i>200</i>
<i>Переименование файла</i>	<i>300</i>	<i>000</i>
<i>Создание поддиректории</i>	<i>300</i>	<i>000</i>
<i>Удаление поддиректории</i>	<i>300</i>	<i>000</i>

## **Вывод**

*Получили практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе CentOS*