Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт цифрового развития

Кафедра инфокоммуникаций

**«УПРАВЛЕНИЕ ДОСТУПОМ В ФАЙЛОВОЙ СИСТЕМЕ LINUX»**

**ОТЧЕТ**

**по лабораторной работе №11**

**дисциплины**

**«Операционные системы»**

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Выполнил:  Мизин Глеб Егорович  2 курс, группа ПИЖ-б-о-21-1,  09.03.04 «Программная инженерия», направленность (профиль) «Разработка и сопровождение программного обеспечения», очная форма обучения  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | |
|  | | Проверил:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | |
|  | |  | |

Отчет защищен с оценкой \_\_\_\_\_\_\_\_\_\_\_ Дата защиты\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ставрополь, 2022 г.

**Цель работы**: практическое знакомство со средствами обеспечения безопасности в ОС Linux и методами управления доступом к данным в файловой системе ОС Linux ext3fs

**Задание №1**: cоздать группу пользователей с именем g<номер\_бригады>1 и пользователя с именем a в этой группе, используя режим командной строки.

Для добавления группы через терминал была использована команда groupadd



Рисунок 1 – Создание группы



Рисунок 2 – Создание пользователя и помещение его в группу

Что бы добавить пользователя в группу создадим его при помощи команды useradd и добавим с помощью usermod

**Задание №2**: создать группу пользователей с именем g<номер\_бригады>2 и пользователя с именем b в этой группе, используя графический интерфейс пользователя.

Для создания группы через GUI необходимо установить утилиту



Рисунок 3 – Установка утилиты

После установки в поиске можно найти «группы и пользователи» и в специальном окне создать группу или пользователя, а также добавить его в необходимую группу

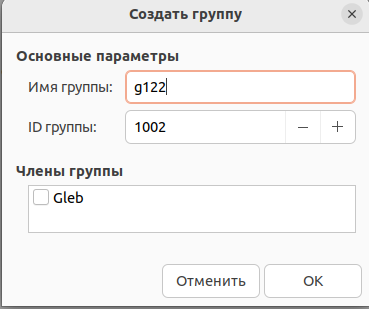


Рисунок 4 – создание группы в GUI

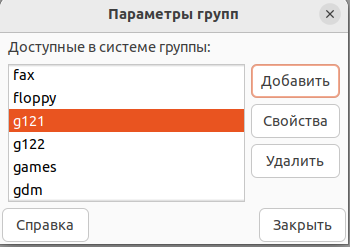


Рисунок 5 – Созданные группы

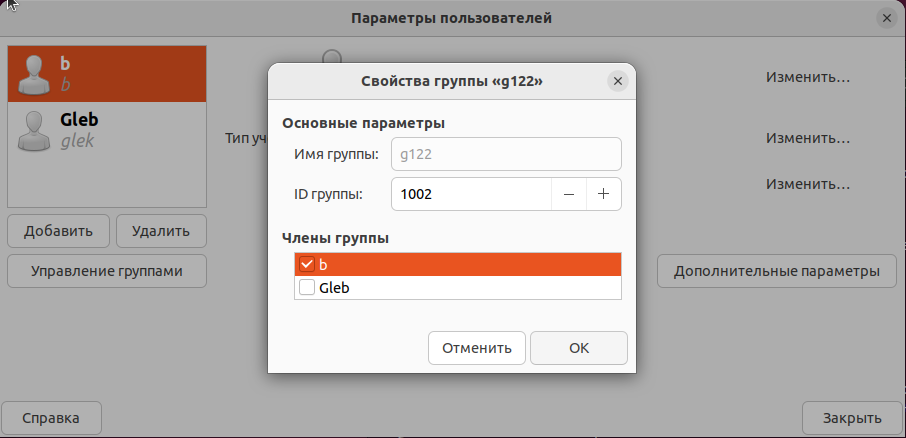


Рисунок 6 – добавление пользователя b в группу g122

**Задание №4**: в домашнем каталоге создать по одному каталогу и файлу на каждого пользователя.

Команда mkdir создаёт каталог, а echo записывает в файл набранный текст



Рисунок 7 – Создание каталогов a и b с файлами

**Задание №5**: разрешить группе чтение, владельцу - чтение и запись файла. Для каталога группе разрешить чтение и выполнение. Для выполнения задания использовать запись прав в 8 сс и маску прав.

При помощи команды chmod можно менять права r(read) w(write) x(execute) для групп и пользователей как для директорий, так и для файлов

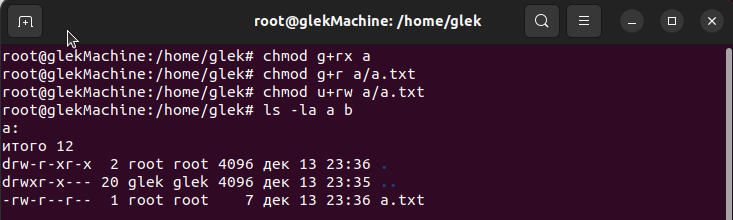


Рисунок 8 – Смена прав

**Задание №6**: на один из созданных каталогов установить sticky-бит.

Sticky бит нужен для того что бы обезопасить файлы в каталогах одних групп от других, а именно этот бит не позволяет удалять файл любому пользователю кроме его создателя. Происходит добавление при помощи того же chmod, но с ключом t

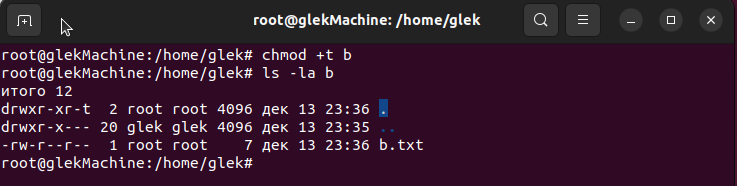


Рисунок 9 – Добавление sticky бита

**Задание №7**: записать в каталог со sticky-битом по копии файла от каждого пользователя бригады, выполнить удаление записанных файлов (проверка действия sticky-бита).

При помощи команды chown передадим права владения для папки b пользователю b.

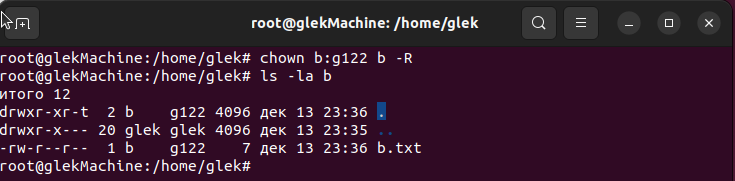


Рисунок 10 – Передача прав

Теперь командой su b создадим файл через команду touch, после чего переключимся на пользователя a и попытаемся удалить файл. После использования команды ls можно заметить, что файл не удалён.

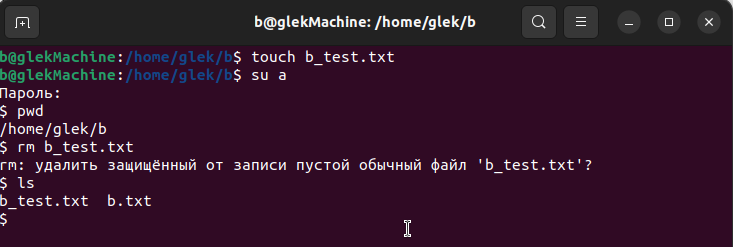


Рисунок 11 – Проверка Sticky бита

**Задание №8**: cкопировать один из выполняемых файлов, созданных в работе 5 в один из созданных каталогов и установить ему бит SGID. С помощью команды ls –l получить результаты установки.

Бит SGID разрешает пользователям запускать исполняемые файлы с правами владельца или группы исполняемого файла. Создаётся этот бит командой chmod с ключом s

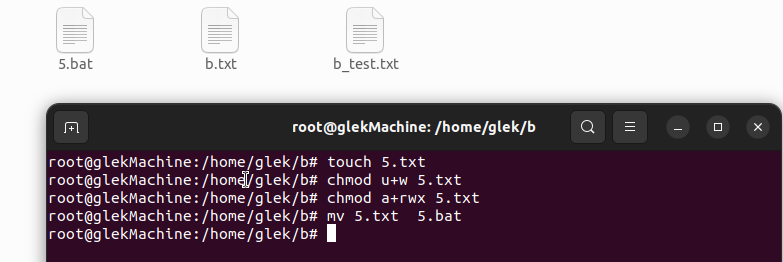


Рисунок 12 – Копирование файла 5.bat

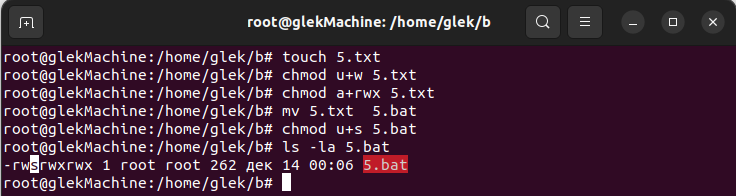


Рисунок 13 – добавление SGID бита

**Задание №9**: проверить, установлена ли поддержка ACL-списков компьютере, на котором выполняется лабораторная работа. На компьютере с поддержкой ACL-списков установить для одного из созданных каталогов правила по умолчанию и получить результаты установки с помощью утилиты getfacl.

Проверим работает ли поддержка ACL списков при помощи команды getfacl. С помощью команды setfacl установим правила по умолчанию для каталога b.

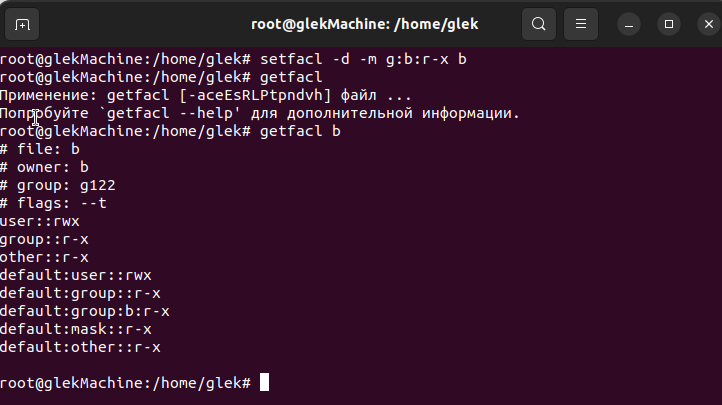


Рисунок 14 – Установка правил по умолчанию для каталога b

**Вывод**: ознакомились со средствами обеспечения безопасности в ОС Linux и методами управления доступом к данным в файловой системе ОС Linux ext3fs

**Контрольные вопросы**:

1. Группы пользователей, назначение, создание и использование.

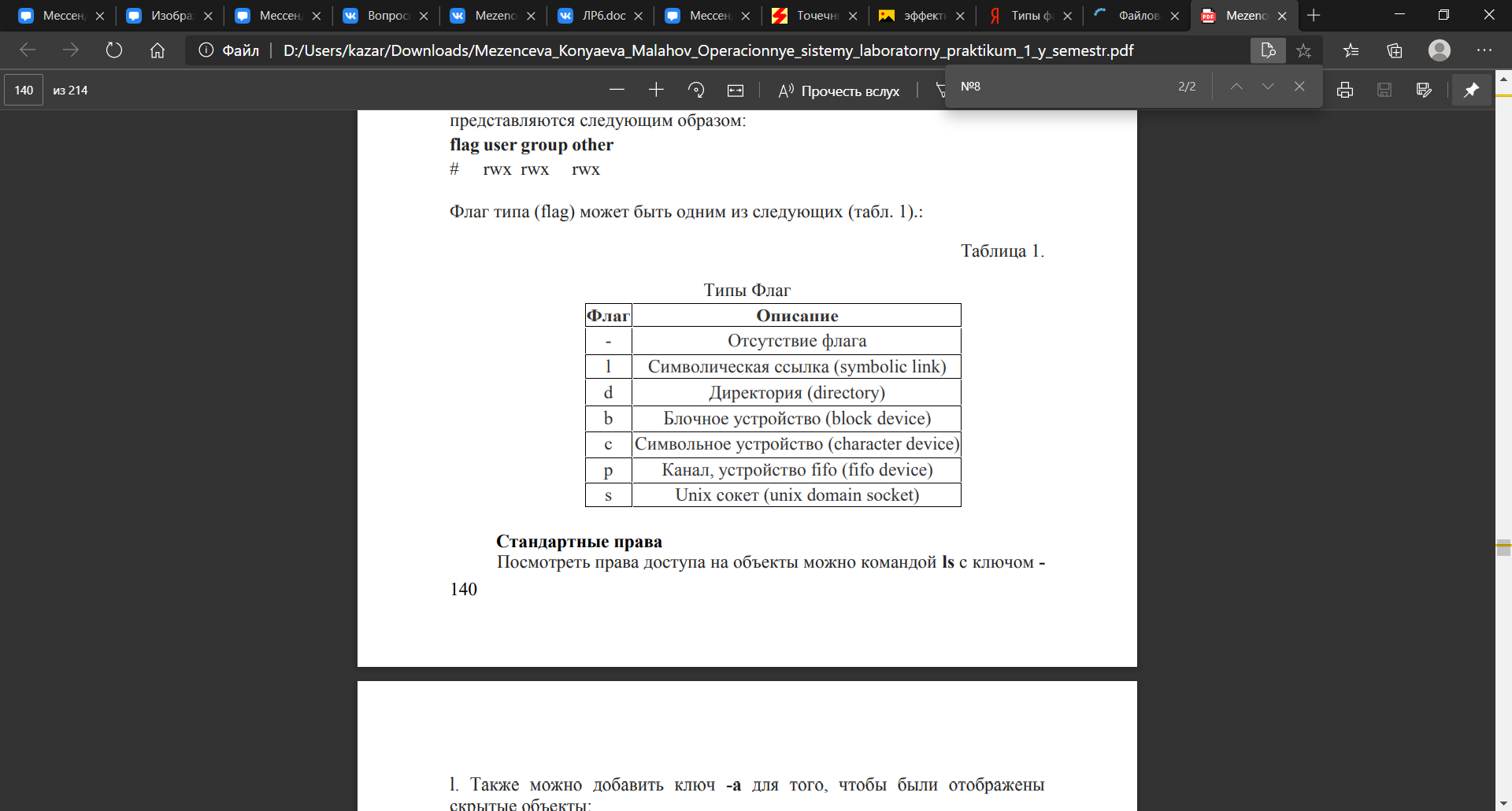
В многопользовательской ОС Linux с целью защиты информации

пользователей и обеспечения безопасности самой ОС используются

группы пользователей со следующими свойствами:

* каждый пользователь входит в минимум одну группу. Группа, присваиваемая пользователю при его создании, называется основной. Все остальные группы в которые будет включен пользователь, будут являться дополнительными.
* группа пользователей может содержать некоторое количество
* пользователей, но не может содержать или включаться в другие группы.
* группа может быть пустой, т.е. не содержать в себе ни одного пользователя.

2. Типы файлов файловой системы ext3fs.



3. Управление доступом к файлам и каталогам в ОС Linux.

Существует три способа управления доступом к файлу или каталогу. Было определено, что каждый файл должен иметь владельца (owner), группового владельца (group owner), а также может потребоваться доступ для всех остальных пользователей (everyone). Эти названия обычно приводятся как пользователь/группа/остальные (user/group/others) или коротко ugo. Реализация управления доступом к файлам и каталогам в ОС Linux разрешает или запрещает доступ с помощью трех бит: бита чтения (Read), бита записи (Write), бита выполнения (eXecute). Они представляются следующим образом: flag user group other # rwx rwx rwx.

4. Команда просмотра прав доступа на объекты.

Посмотреть права доступа на объекты можно командой ls c ключом -l

5. Стандартные права доступа к объектам файловой системы ОС Linux и формы их записи.

Для назначения обычных прав используются три восьмеричных цифры (9 битов). Первая цифра определяет права для владельца файла, вторая – права для основной группы пользователя, третья - для всех остальных пользователей. Так, например, чтобы задать права на файл всем, нужно установить права 777 (rwxrwxrwx).

6. Установка прав доступа с помощью команды chmod.

Права устанавливаются командой chmod. По умолчанию использовать ее может только root. Команда chmod поддерживает установку прав как в восьмеричном представлении, так и в символьном (маска режима доступа).

Синтаксис команды:

chmod <опции> <права> <объект или регулярное выражение>

Опции: Из самых полезных и часто используемых опций можно выделить одну: -R - рекурсивное назначение прав. Т.е. назначить права всем объектам, руководствуясь регулярным выражением.

7. Назначение битов SUID, SGID.

Существуют два специальных бита: SUID (Set User ID - бит смены идентификатора пользователя) и SGID (Set Group ID - бит смены идентификатора группы). Когда пользователь или процесс запускает исполняемый файл с установленным одним из этих битов, файлу временно назначаются права его (файла) владельца или группы (в зависимости от того, какой бит задан). Таким образом, пользователь может даже запускать файлы от имени суперпользователя. Восьмеричные значения для SUID и SGID равны 4000 и 2000, символьные: u+s и g+s. Установка битов SUID или SGID

позволит пользователям запускать исполняемые файлы от имени владельца (или группы) запускаемого файла.

8. Назначение бита Sticky.

Еще одно важное усовершенствование касается использования sticky-бита в каталогах. В отличии от установки sticky на каталог, на файл такой бит устанавливать не имеет смысла. Каталог с установленным sticky-битом означает, что удалить файл из этого каталога может только владелец файла или суперпользователь.

9. Способы установки битов SUID, SGID, Sticky.

Установить SUID и SGID можно командой chmod:

chmod 4755 doc.pl - устанавливает на файл doc.pl бит SUID и заменяет обычные права на 755 (rwxr-xr-x).

Установить sticky-бит на каталог можно используя команду chmod:

chmod +t alex - добавление к текущим правам.

10. Необходимость использования ACL-списков.

Возможностей стандартных прав ОС Linux недостаточно для реализации сложных схем доступа. Списки управления доступом (ACL – Access Control List списки) предоставляют более тонкую организацию управлению доступом пользователей к указанным каталогам и файлам по сравнению с традиционными правами доступа ОС Linux

11. Недостатки ACL-списков.

Недостаток ACL-списков в снижении производительности системы, поэтому их использование не следует разрешать на файловых системах, хранящих системные файлы, где вполне достаточно традиционных прав доступа Linux

12. Виды ACL-списков. Содержимое ACL-списков.

ACL-список включает в себя набор правил. Правило определяет, как указанный пользователь или группа может получить доступ к файлу, с которым связан ACL-список. Есть два вида правил: правила доступа (access ACLs) и правила по умолчанию (default ACLs). Правило доступа определяет информацию о доступе для отдельного файла или каталога. ACL-список по умолчанию принадлежит исключительно каталогу, он определяет информацию доступа по умолчанию (ACL-список) для любого имеющегося в каталоге файла, которому не предоставлен явно заданный ACL-список.

13. Подключение ACL-списков.

Перед тем как получить возможность использования ACL-списков, нужно установить программный пакет acl. Linux поддерживает ACLсписки на файловых системах ext2, ext3 и ext4.

14. Назначение утилит getfacl и setfacl.

Утилита getfacl отображает ACL-список указанного файла. При использовании утилиты getfacl для получения информации о файле.

Утилита setfacl с ключом –m позволяет добавить или изменить одно или несколько правил в ACL-списке файла.

15. Проверка наличия ACL-списка у файла или каталога.

Чтобы посмотреть, установлены ли ACL-списки на объектах, достаточно воспользоваться командой ls -l: Символ "+" в конце списка стандартных прав сообщает о наличии установленных прав ACL

16. Маска эффективных прав – назначение и использование.

Строка, начинающаяся со слова mask, указывает на маску эффективных прав. Эта маска ограничивает эффективные права, выделенные с помощью ACL-списков группам и пользователям. Она не затрагивает права владельца файла или группы, с которой связан файл. Но, поскольку утилита setfacl всегда устанавливает маску эффективных прав на минимальные ограничительные права доступа к файлу, устанавливаемые в ACL-списке, эта маска не оказывает никакого влияния до тех пор, пока она не будет установлена явным образом после установки для файла ACL-списка. Маску можно установить, указав mask вместо ugo и не указывая имя в команде setfacl

17. Установка правил по умолчанию для каталога.

Если не задано иное, то все объекты, создаваемые в каталоге, у которого есть ACL-списки, не наследуют права ACL каталога, в котором они создаются. Но иногда возникают ситуации, когда необходимо, чтобы все объекты, создаваемые внутри каталога, наследовали его ACL права. Эта возможность называются ACL по умолчанию. Для добавления правил по умолчанию для каталога в команде setfacl используется ключ –d (default).

18. Копирование ACL- списков.

Принцип копирования:

· Снять ACL c одного объекта

· Записать их на другой

19. Создание нового пользователя в режиме командной строки.

useradd - создать пользователя.

20. Создание нового пользователя в графическом режиме. Управление пользователями.

**Gnome-system-tools**