*Федеральное государственное бюджетное образовательное учреждение* *высшего образования*

|  |  |
| --- | --- |
| **Gerb-BMSTU_01** | ***«Московский государственный технический университет  имени Н.Э. Баумана***  ***(национальный исследовательский университет)»***  ***(МГТУ им. Н.Э. Баумана)*** |

ФАКУЛЬТЕТ ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ

КАФЕДРА КОМПЬЮТЕРНЫЕ СИСТЕМЫ И СЕТИ (ИУ6)

**Отчет**

**по лабораторной работе №5**

**Дисциплина:** Операционные системы

**Название лабораторной работы:**

Исследование методов защиты операционных систем и данных

Студент гр. ИУ6-52  **\_\_\_\_\_\_27.09.2018 Бурлаков А.С.**

(Подпись, дата) (И.О. Фамилия)

Преподаватель  **\_\_\_\_\_\_\_\_\_\_\_ Мельников В.Ю.**

(Подпись, дата) (И.О. Фамилия)

Москва, 2018

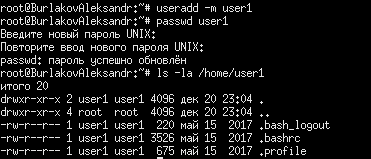
# ВВЕДЕНИЕ

Степень защищенности компьютера во многом зависит от совершенства установленной на нем операционной системы, которая должна обладать развитыми средствами шифрования данных и иметь инструменты настройки безопасности, как для одиночного компьютера, так и компьютера работающего в сети.

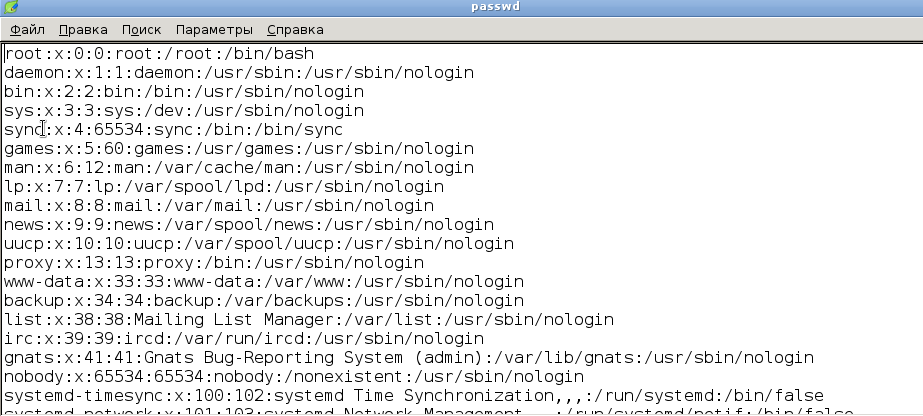
Цель работы - исследование методов защиты операционных систем и информации в операционных системах Linux, Windows и др.

# ОСНОВНАЯ ЧАСТЬ

## Создание пользователей



Пароли всех пользователей в файле /etc/passwd:



Поля файла passwd имеют следующую структуру: login:password:UID:GID:GECOS:home:shell

Команды usermod, userdel, passwd

## Группы пользователей

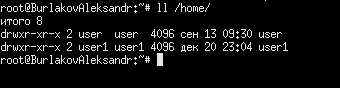
groupadd, groupdel, usermod –g



Файл /etc/group:



## Управление правами доступа к файлам и каталогам

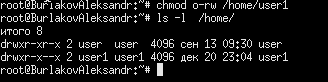


Разберем эти строки:

Для user: Каталог, в него разрешена запись, чтение и запись, для группы-владельца: чтение и запуск, для остальных: чтение и запуск.

Аналогично для user1

Изменим права для user1:



## Смена владельца

## Изменение владельца: chown [-R] Владелец Файл;

## Изменение группы: chgrp [-R] ГРУППА ФАЙЛ.

## 

## Смена пользователя

Команда для смены: su –l ПОЛЬЗОВАТЕЛЬ; для возврата команда exit:



## Выполнение команд от имени другого пользователя

## Выполняется командой sudo –u Пользователь Команда

## Установим sudo следующей командой:

## apt-get install sudo

## Добавим пользователя user в группу sudo:

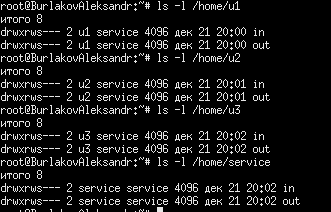
## 

## Выполнение заданий:

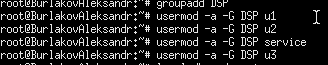
* Создать несколько пользователей, включая пользователя от имени которого работает сервис распознавания.



* Для каждого пользователя создать каталоги:
  + in — для файлов, предназначенных для распознавания
  + out — для распознанных файлов
  + Пользователи не должны иметь доступ к файлам других пользователей. Не забудьте дать права сервису распознавания.



* Создать каталог, в который выкладывают файлы пользователи группы «DSP». Только пользователи этой группы должны иметь к нему доступ.





* Создать файл протокола, в который записывает сообщения сервис распознавания. Все пользователи должны иметь права на чтение этого файла.



# Заключение

1. В ходе данной лабораторной работы были исследованы методы защиты операционных систем и информации в операционных системах Linux