|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«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)**

НАПРАВЛЕНИЕ ПОДГОТОВКИ **09.03.01 Информатика и вычислительная техника**

**Отчет**

|  |  |
| --- | --- |
| **по лабораторной работе № 6** |  |

**Название:**

Исследование методов защиты операционных систем и данных

**Дисциплина:** Операционные системы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Студент | ИУ6-52Б |  |  | С.В. Астахов | |
|  | (Группа) |  | (Подпись, дата) | | (И.О. Фамилия) |
|  |  |  |  | |  |
| Преподаватель |  |  |  | |  |
|  |  |  | (Подпись, дата) | | (И.О. Фамилия) |

Москва, 2021

**Цель работы:** исследование методов защиты информации в Linux.

**Вводная часть.**

**Задание:** Создать нового пользователя и просмотреть содержимое его домашнего каталога.

**Практическая часть:** Для добавления пользователя воспользуемся командой “useradd”, заменим его пароль командой “passwd” и просмотрим содержимое его домашнего каталога командой “ls”.

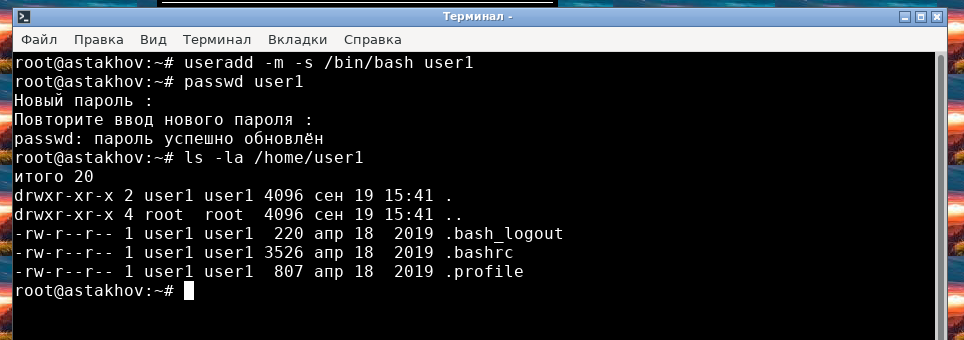


Рисунок 1 - содержимое домашнего каталога пользователя

**Задание:** Задать алиас “ll” для команды “ls -l”. Изменить вид приглашения командной строки.

**Практическая часть:** Изменим алиас команды “ls -l” в файле “.bashrc”. Изменим и раскомментируем строку “PS1=...” в том же файле.

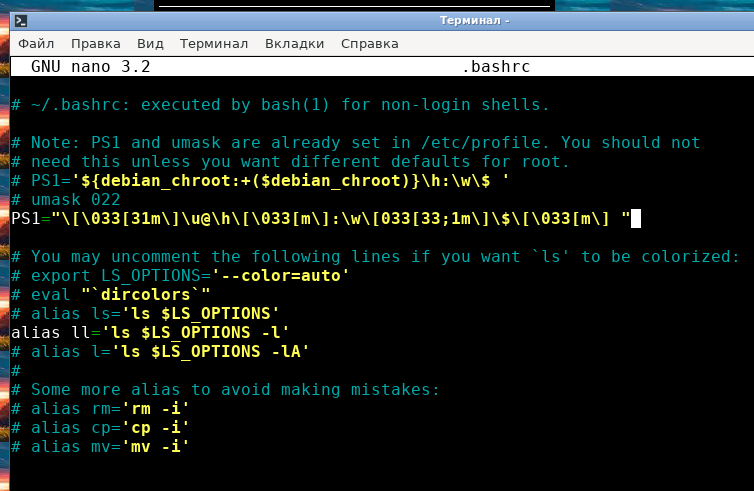


Рисунок 2 - настройка bash пользователя

**Задание:** Просмотреть учетные данные всех пользователей.

**Практическая часть:** Откроем файл “/etc/passwd” в leafpad.

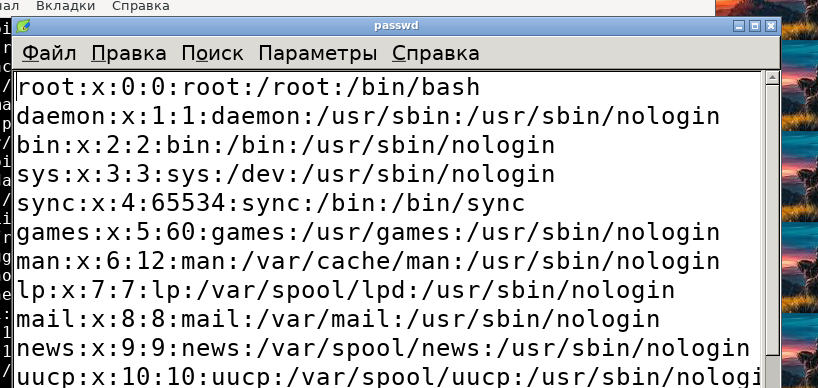


Рисунок 3 - просмотр учетных данных пользователей

**Задание:** Настроить для пользователей группы и просмотреть список групп.

**Практическая часть:** Для настройки групп пользователей воспользуемся командами “groupadd” и “usermod”. Список групп можно получить из файла “/etc/groups”.

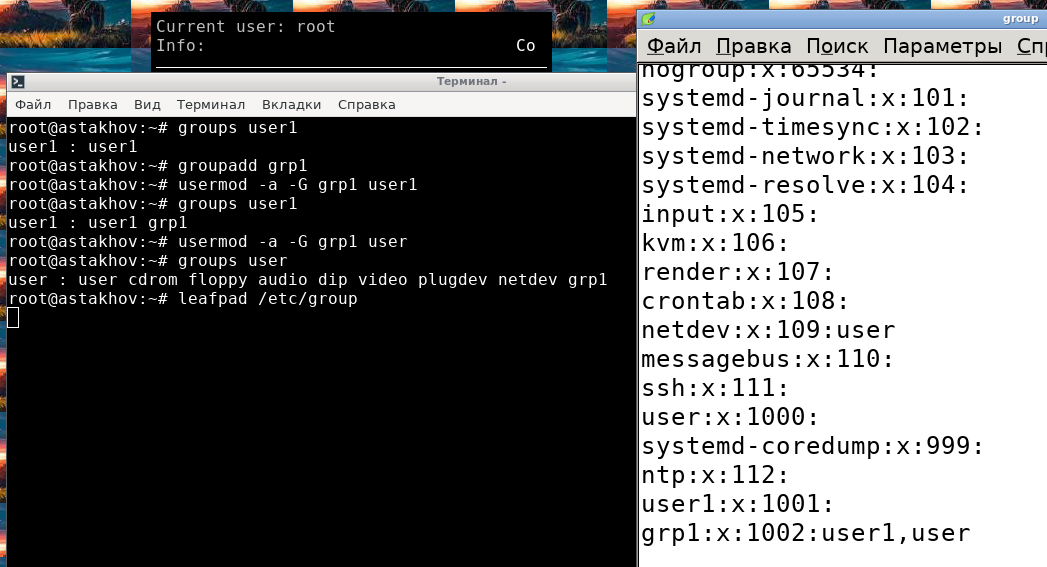


Рисунок 4 - работа с группами пользователей

**Задание:** отнять право “прочих” пользователей редактировать домашний каталог user1.

**Практическая часть:** воспользуемся командой “chmod o-...”.

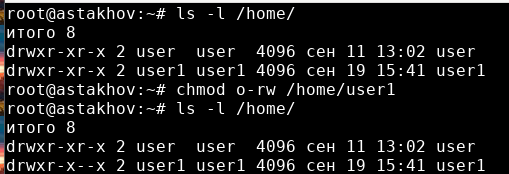


Рисунок 5 - изменение прав доступа к домашнему каталогу

**Задание:** Изменить с помощью ACL права доступа пользователя и группа к файлу и вывести полную информацию о правах доступа к файлу с помощью.

**Практическая часть:** воспользуемся командами “setfacl” и “getfacl”.

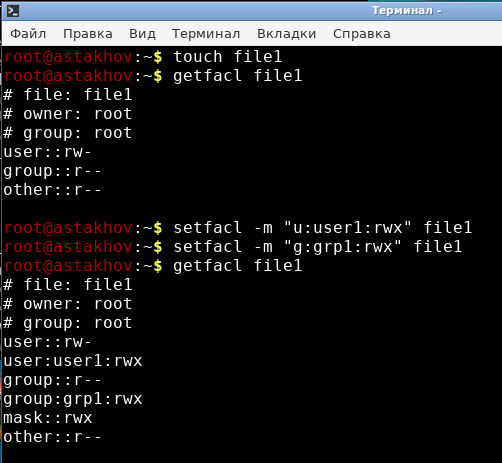


Рисунок 6 - настройка прав доступа с помощью ACL

**Задание:** установить и запустить Selinux.

**Практическая часть:** после установки с помощью apt и активации убедимся в работоспособности selinux с помощью команды “sestatus”.

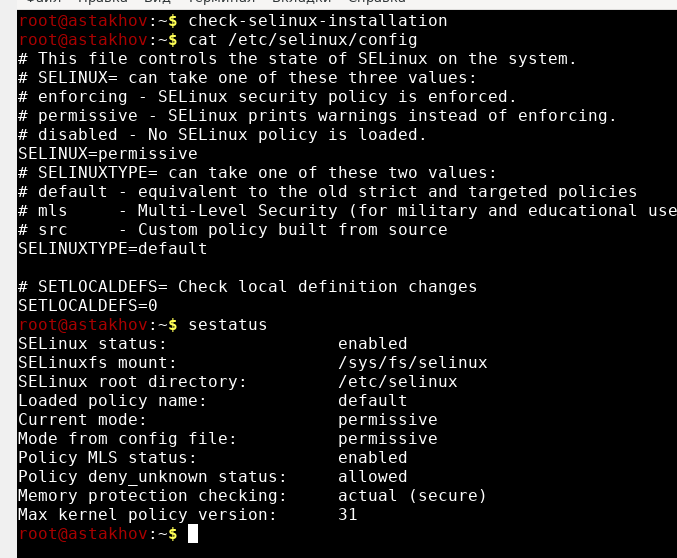


Рисунок 7 - статус selinux

**Задание:** Просмотреть контекст безопасности для пользователя и процессов.

**Практическая часть:** При работе selinux контекст безопасности отображается при вызове команды “id” и “ps”.

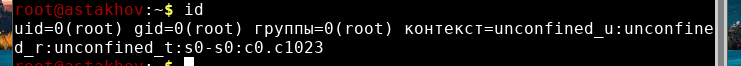


Рисунок 8 - контекст безопасности пользователя

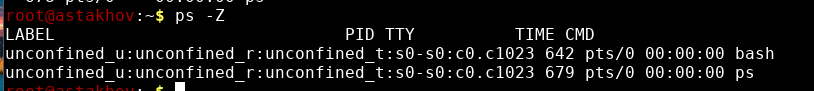


Рисунок 9 - контекст безопасности процессов

**Задание:** Установить сервер Apache и настроить его для работы с selinux.

**Практическая часть:** Изначально после запуска selinux сервер не будет работать из-за блокировки 81 порта от веб-сервисов. После настройки 81 порта так же надо разрешить доступ веб-сервисов к файлам с разметкой веб-страниц.

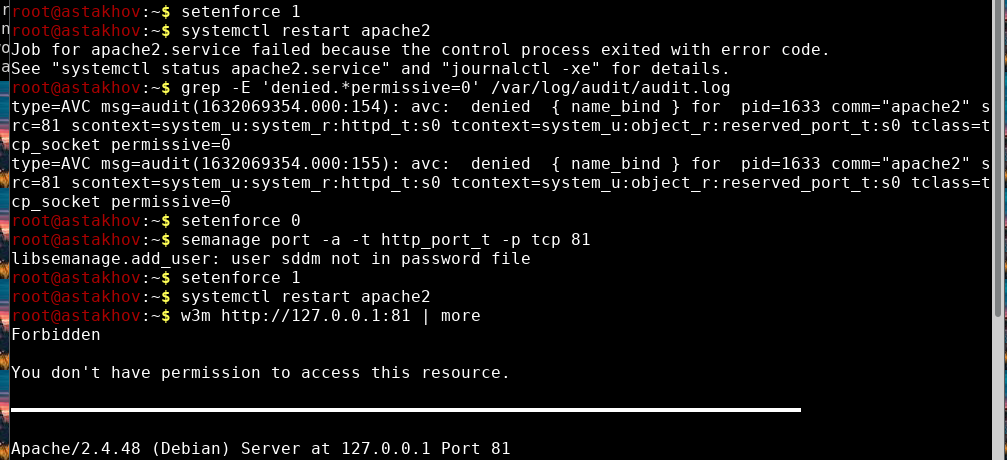


Рисунок 10 - настройка доступа к 81 порту

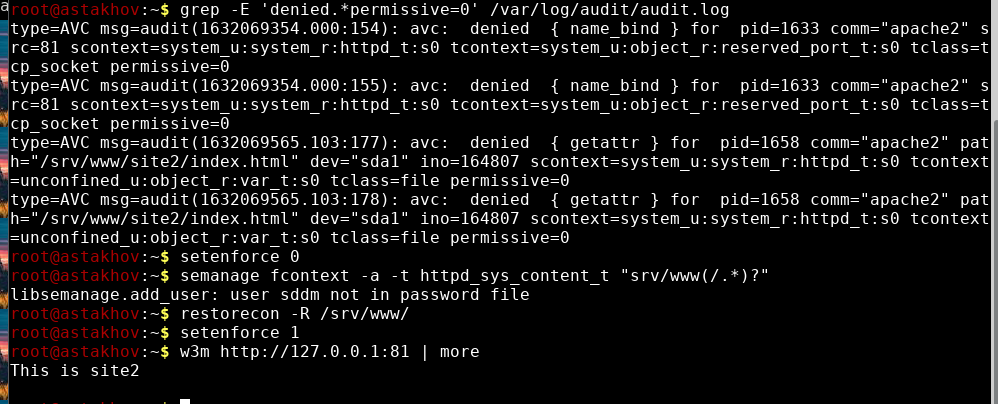


Рисунок 11 - настройка доступа к файлам с разметкой

**Задание к ЛР**

**Задание:** 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.

**Практическая часть:** создадим пользователей командами

“useradd -m user1”,

“useradd -m user2” ,

“useradd -m user3” ,

“useradd -m scanner”

и описанный в задании каталоги и файлы для каждого пользователя командами ниже, запустив их в домашнем каталоге каждого пользователя (кроме scanner)

“mkdir docs”,

“mkdir docs/in”,

“mkdir docs/out”

Для scanner создадим папку “DSP” и файл лога командой “touch scan.log”.

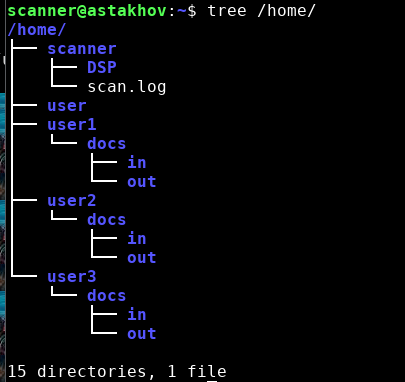


Рисунок 12 - структура каталогов

Создадим группу “DspGroup”(команда “groupadd DspGroup”) и добавим в группу “DspGroup” пользователей 2, 3 и сканер.

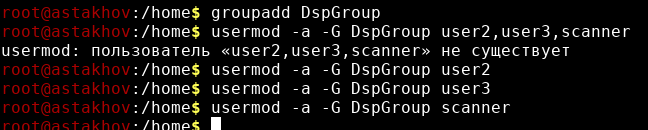


Рисунок 13 - настройка группы “DspGroup”

Сканер добавим в группы всех пользователей, чтобы он имел доступ к их файлам.



Рисунок 14 - настройка групп пользователей

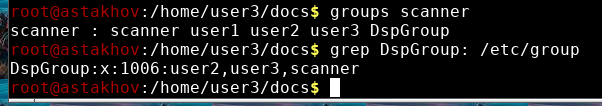


Рисунок 14 - группа “DspGroup”

Для директории “DSP” и директорий “docs”, “in”, “out” пользователей группе-хозяину все права командой “chmod g+rwx .”, а для остальных - отключим их командой “chmod o-rwx .”, находясь в соответствующих каталогах. Для лога сканера для группы-хозяина и “остальных” оставим разрешения только на чтение командами “chmod g-wx scan.log” и “chmod o-wx scan.log”.

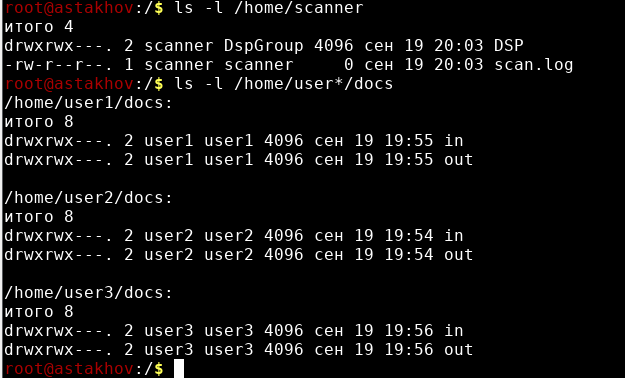


Рисунок 14 - разрешения для файлов

**Вывод:** в ходе лабораторной работы были изучены модели управления доступом в ОС семейства Linux.