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 - 54 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_**А.А. Шумаков**\_\_\_\_**

(Подпись, дата) (И.О. Фамилия)

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

(Подпись, дата) (И.О. Фамилия)

Москва, 2018

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

**Выполнение работы**

**Создание пользователей**

Добавим пользователя «TestUser» и зададим ему пароль «Test»:

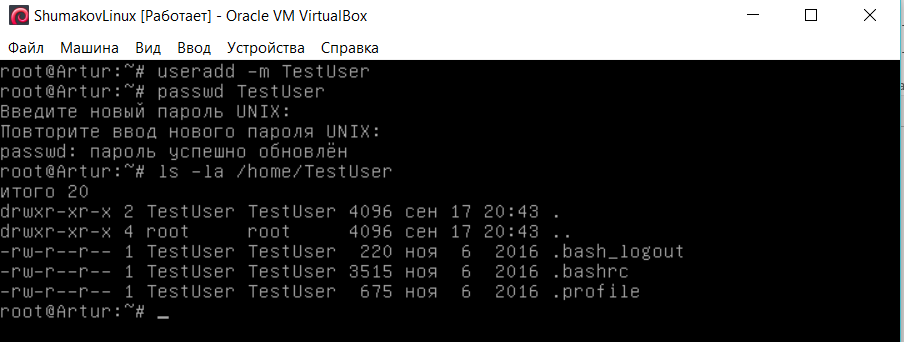
**useradd -m** TestUser

**passwd**

<пароль>

<повтор пароля>

Не забудьте опцию -m. Она создаёт домашний каталог, записывает в него шаблоны сценариев инициализации. По умолчанию, создаётся домашний каталог /home/ИМЯ\_ПОЛЬЗОВАТЕЛЯ. Посмотрим, его содержимое: ls -la /home/user1



Команда автоматически создала следующие сценарии:

~/.bash\_profile — выполняется при входе пользователя в систему;

~/.bashrc — выполняется при каждом запуске дочернего интерпретатора команд;

~/.bash\_logout — выполняется при выходе из системы.

Учётные всех пользователей данные хранятся в файле /etc/passwd



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

login – регистрационное имя пользователя;

password – хэш пароля;

UID – идентификатор пользователя;

GID – идентификатор группы по умолчанию;

GECOS – информация о пользователе (например, полное имя, почта, телефон и т.д., данное поле не имеет чёткого синтаксиса, может использоваться для автоматизации некоторых процессов, например, отправки пользователю почтового сообщения при авторизации его логина в системе);

home – домашняя папка пользователя;

shell – Оболочка - интерпретатор команд. Именно он запускается при входе в Linux и выполняет команды, которые вводите в консоли. Он же вызывается для выполнения командных скриптов.

**Группы пользователей**

Если несколько пользователей должны иметь доступ к файлу или каталогу следует создать группу и предоставить права этой группе.

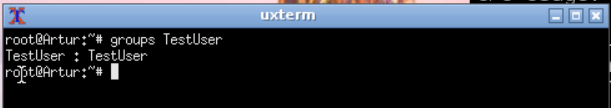
При создании пользователя командой «*useradd -m*» автоматически создаётся так же группа с именем пользователя. Этой группой можно воспользоваться, чтобы дать права на свой файл только одному пользователю.

Команда «***usermod -g*** *ГРУППА ПОЛЬЗОВАТЕЛЬ*» - изменяет первичную группу пользователя.

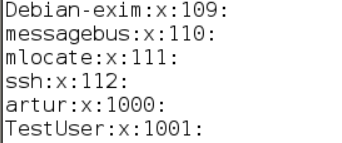
Команда «***usermod -G*** *ГРУППА1,ГРУППА2,... ПОЛЬЗОВАТЕЛЬ*» - задаёт список дополнительных групп пользователя.

Команда «***usermod -a -G*** *ГРУППА ПОЛЬЗОВАТЕЛЬ*» - добавляет к списку групп заданного пользователя заданную дополнительную группу.

Для просмотра, в какие группы входит пользователь, используется команда «***groups*** *ПОЛЬЗОВАТЕЛЬ*».



Полный список групп с атрибутами содержится в файле */etc/group*.



Файл *group* содержит записи следующего вида:

*group\_name:password:GID:users*

*group\_name* – имя группы;

*password* – пароль (в зашифрованном виде);

*GID* – идентификатор группы;

*users* – список пользователей, входящих в эту группу (через запятую). В этом списке не перечисляются пользователи, для которых эта группа является первичной.

**Управление правами доступа к файлам и каталогам**

В Linux имеется 2 системы управления правами доступа:

•Улучшенная система прав доступа *ACL*.

•Классическая система управления правами доступа.

Пользователь, который создаёт файл или каталог становится его владельцем. И имеет на него все права. Чтобы дать доступ к этому файлу другим пользователям следует:

•Создать группу (*groupadd*)

•Включить в неё этих пользователей. (*usermod*)

•Сменить у файла группу — владельца (*chown*)

•При необходимости, дать права на запись (*chmod*)

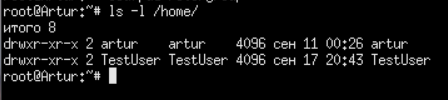
Для каждого файла и каталога linux хранит:

•идентификатор пользователя — владельца,

•идентификатор группы

•16 битовое целое число, где каждый бит определяет права на чтение(r), запись(w), и выполнение(x) для владельца(u), группы(g) и прочих пользователей(o). Тут же хранится бит признака каталога (d) и специальные права suid,sgid(s) и sticky bit(t).

Просмотр прав пользователей на каталоги:



Права на файл и каталог можно изменить командой:

***chmod*** *[****-R****] РЕЖИМ ФАЙЛ*

Если задана опция -R, команда меняет права не только заданного каталога, но и входящих в него файлов и каталогов (рекурсивно).

Режим задаётся в форме [ugoa][+-=][rwxst]

Первая группа символов определяет категорию пользователей: владелец (u), группа (g), прочие пользователи (o), все категории (a). Вторая группа определяет воздействие: разрешить (+), запретить (-) установить (=). Третья группа символов определяет изменяемые права.

**Смена владельца**

Для того, чтобы изменить группу, которой принадлежит файл или каталог следует воспользоваться командой:

***chgrp*** *[****-R****] ГРУППА ФАЙЛ*

При необходимости, пользователя - владельца файла можно сменить командой:

***chown*** *[****-R****] ВЛАДЕЛЕЦ ФАЙЛ*

Если задана опция -R, команда меняет права не только заданного каталога, но и входящих в него файлов и каталогов (рекурсивно).

***chown*** *[****-R****] ВЛАДЕЛЕЦ****:****ГРУППА ФАЙЛ*

Иногда, этой же командой изменяют только группу

***chown*** *[****-R****]* ***:****ГРУППА ФАЙЛ*

**Выполнение команд от имени другого пользователя**

Суперпользователь root имеет права, на абсолютно все операции и работать под этим именем надо как можно меньше. Для того, чтобы выполнить одну команду с правами другого пользователя безопаснее использовать одну из следующих команд:

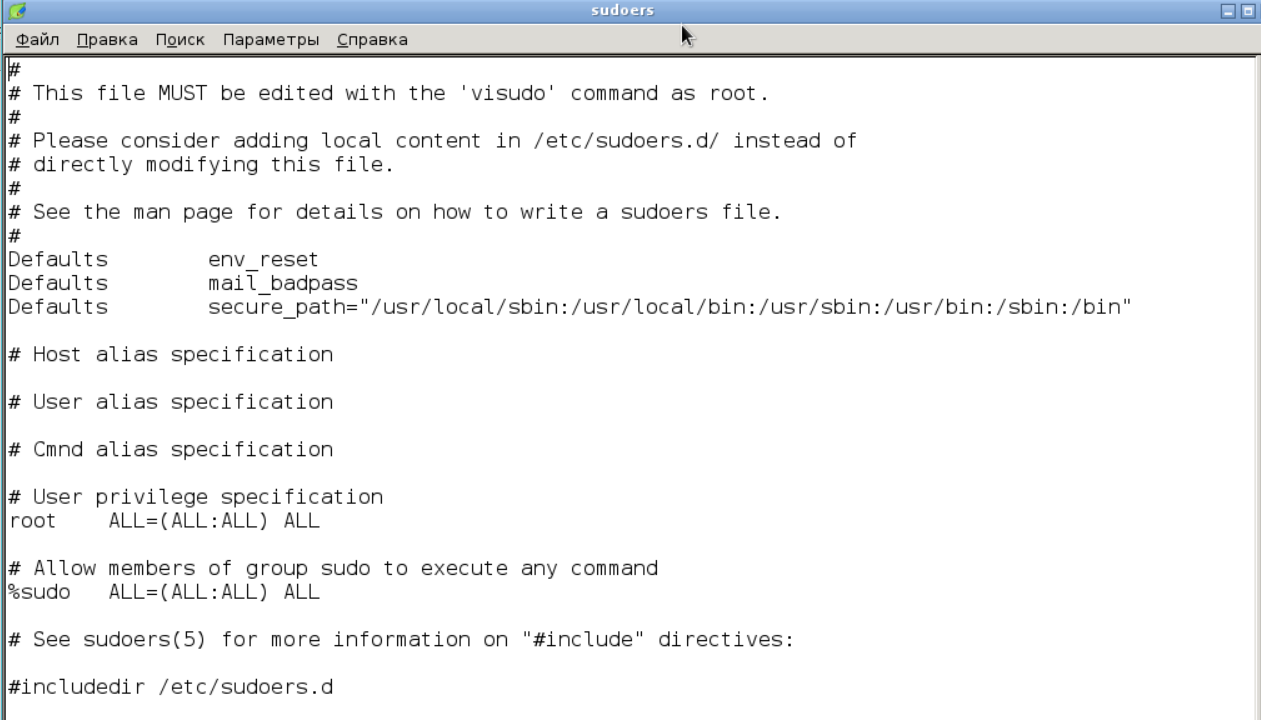
***sudo -u*** *ПОЛЬЗОВАТЕЛЬ КОММАНДА*

**sudo** КОММАНДА (для выполнения команды от имени root)

sudo (обычно расшифровывается как «superuser do») – запуск команд от имени суперпользователя. Во многих дистрибутивах эта утилита является предустановленной, но в используемых в ЛР облегчённых дистрибутивах её нет. Установить её можно следующей командой:

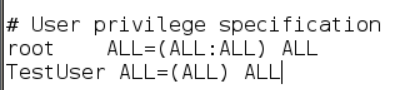
*apt-get install sudo*

После установки требуется добавить пользователя в группу sudo. Для этого необходимо отредактировать файл /etc/sudoers.



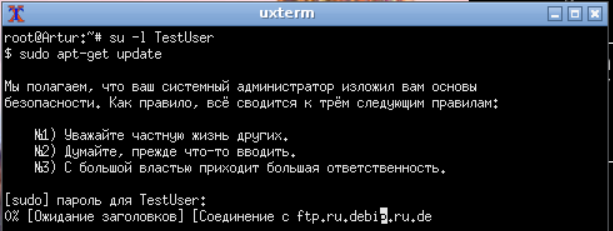
Найдите строку с привилегиями пользователей (*user privilege specification*) и добавьте после строки пользователя root следующую запись:

*TestUser ALL=(ALL) ALL*



Убедитесь, что теперь можно устанавливать недостающие пакеты без смены пользователя:

*sudo apt-get update*

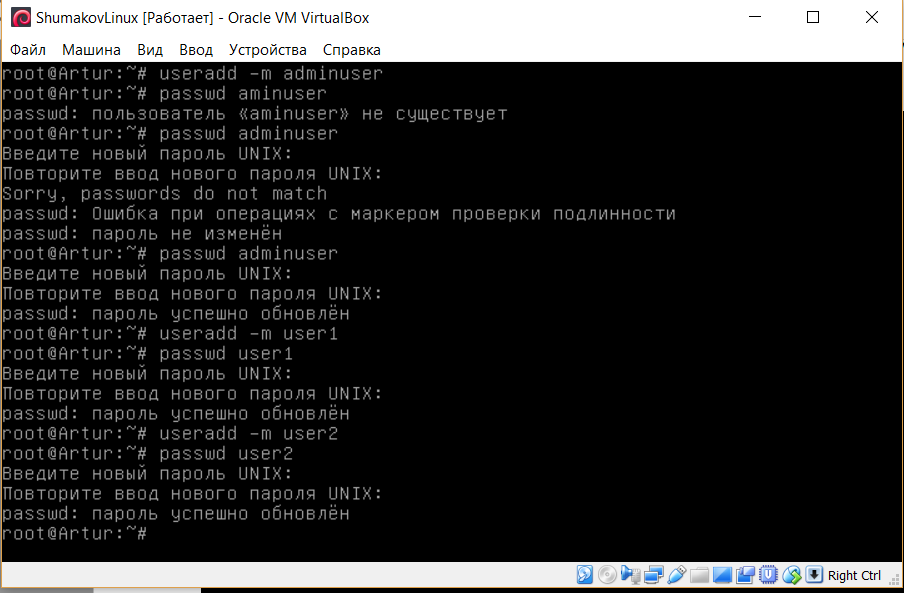


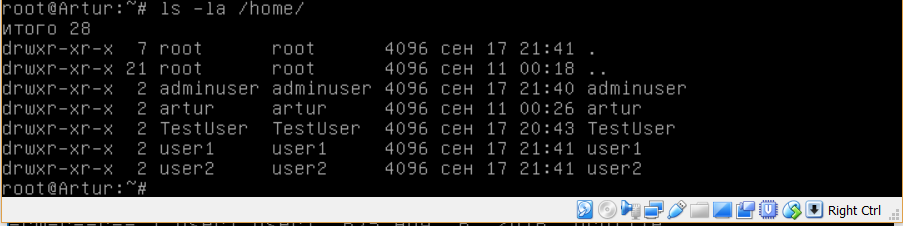
**Выполнение заданий лабораторной работы**

Предположим, в вашей организации в нескольких подразделениях стоят сканеры, пользователи сканируют на них документы и записывают на сервер. На сервере работает программа, которая распознаёт файлы из одного каталога и записывает файлы с распознанным текстом в другой каталог.

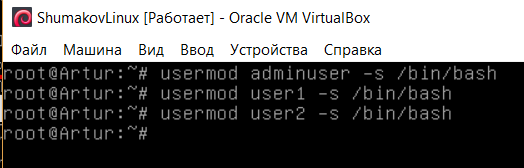
Пользователи загружают распознанные тексты документов в систему документооборота, кроме документов «для служебного пользования», которые записывают в специальный каталог. К этому каталогу имеют доступ только определённая группа пользователей.

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





Укажем для пользователей запуск bash при авторизации



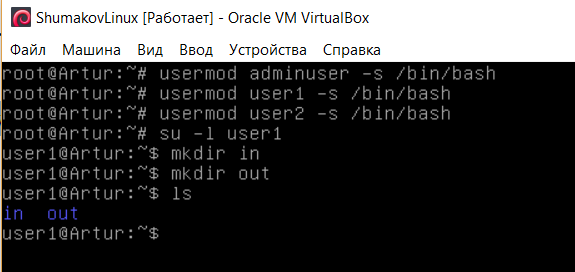
1. Для каждого пользователя создать каталоги:

• in — для файлов, предназначенных для распознавания

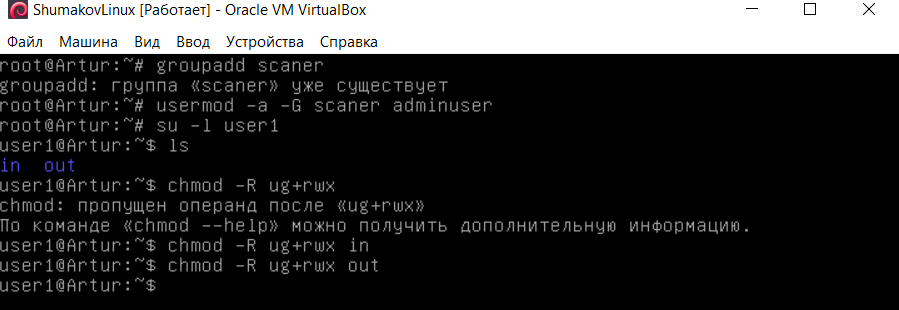
• out — для распознанных файлов

Пользователи не должны иметь доступ к файлам других пользователей. Не забудьте дать права сервису распознавания.

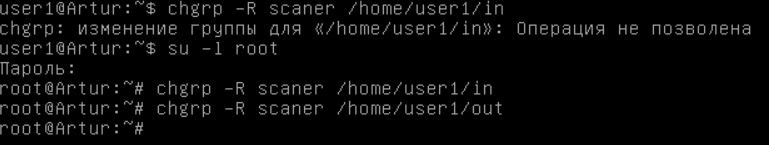
Создадим указанные каталоги для первого пользователя user1



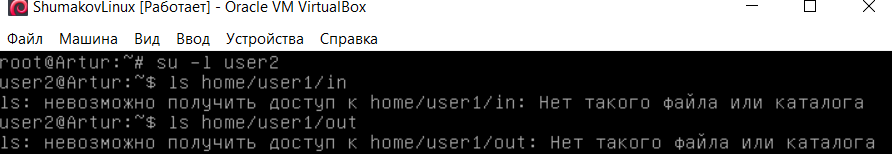
Создадим группу scaner для пользователя adminuser и дадим доступ до директории для её группы.

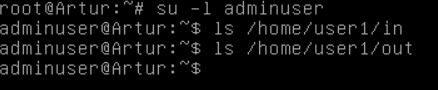


Изменим группу директории на scaner

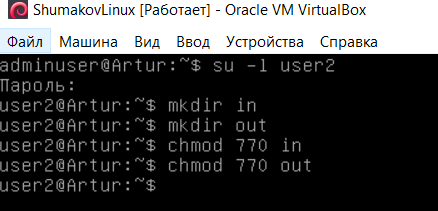


Проверим доступ до файла для пользователей user2 и adminuser

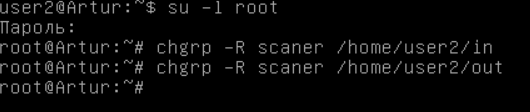




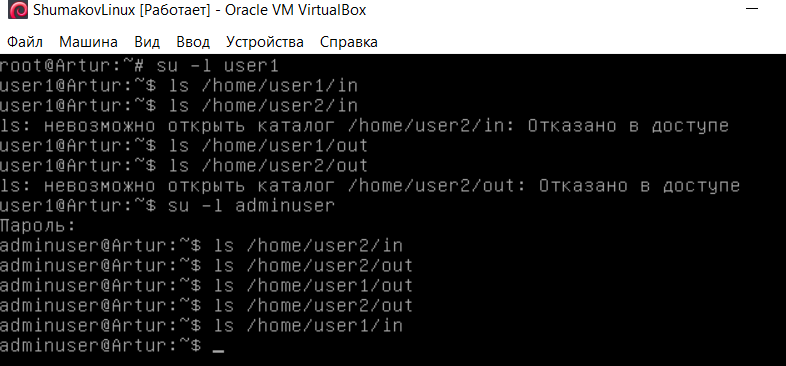
Создадим директрии in и out для user2



Изменим их группу



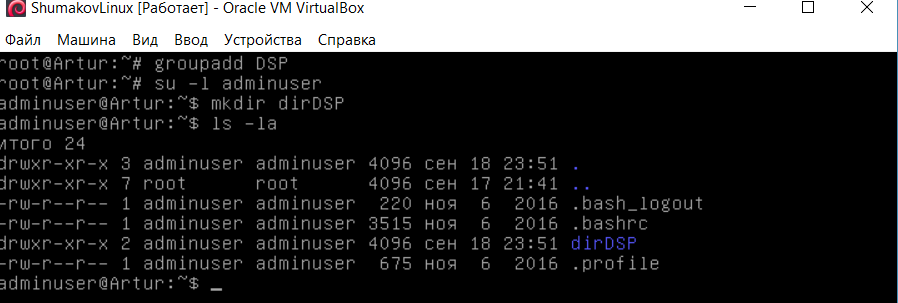
Проверим доступ



3. Создать каталог, в который выкладывают файлы пользователи группы

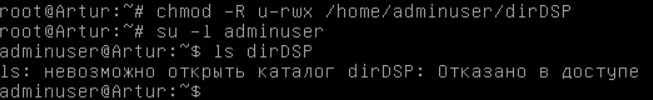
«DSP». Только пользователи этой группы должны иметь к нему доступ.

Создадим группу DSP и каталог dirDSP



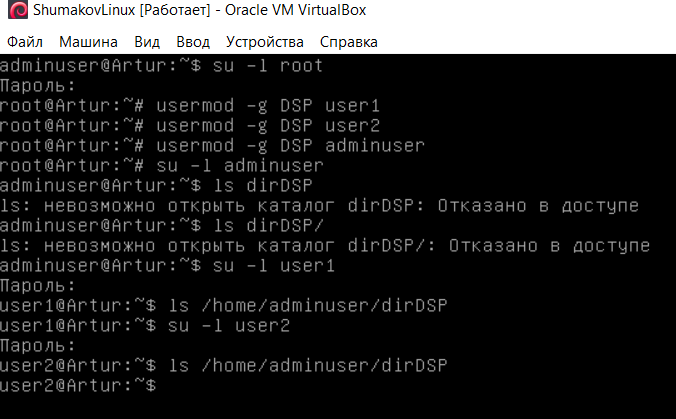
Изменим группу файла на DSP и проверим доступ до неё для adminuser





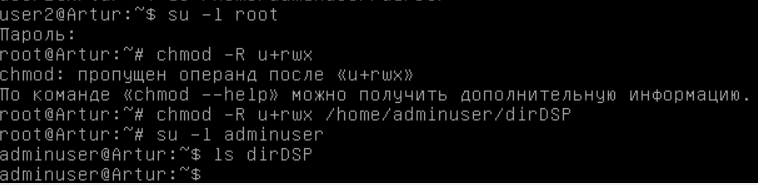
Укажем для всех пользователей основную группу DSP и проверим доступ до

Файла



Поскольку adminuser — создатель каталога, он всё ещё не имеет доступа к

директории.

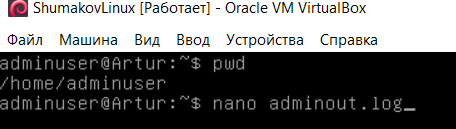


4. Создать файл протокола, в который записывает сообщения сервис

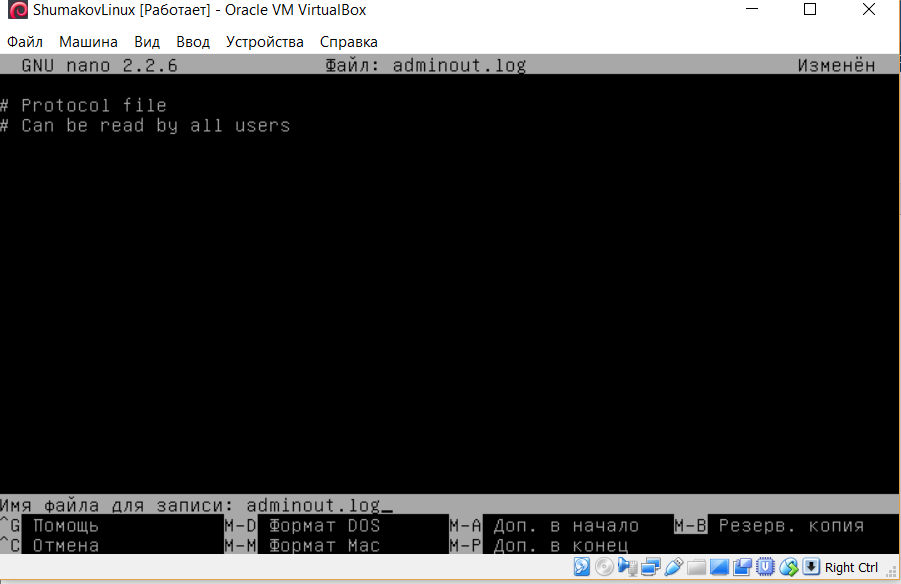
распознавания. Все пользователи должны иметь права на чтение этого

файла.

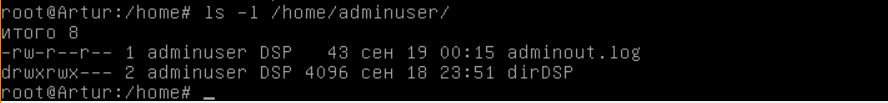
Создадим файл в nano



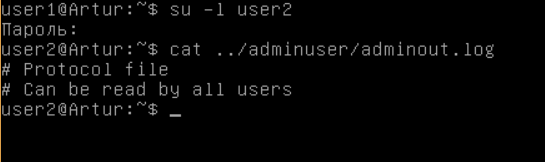
Укажем в нём строки



Проверим доступ до файла на чтение для всех пользователей

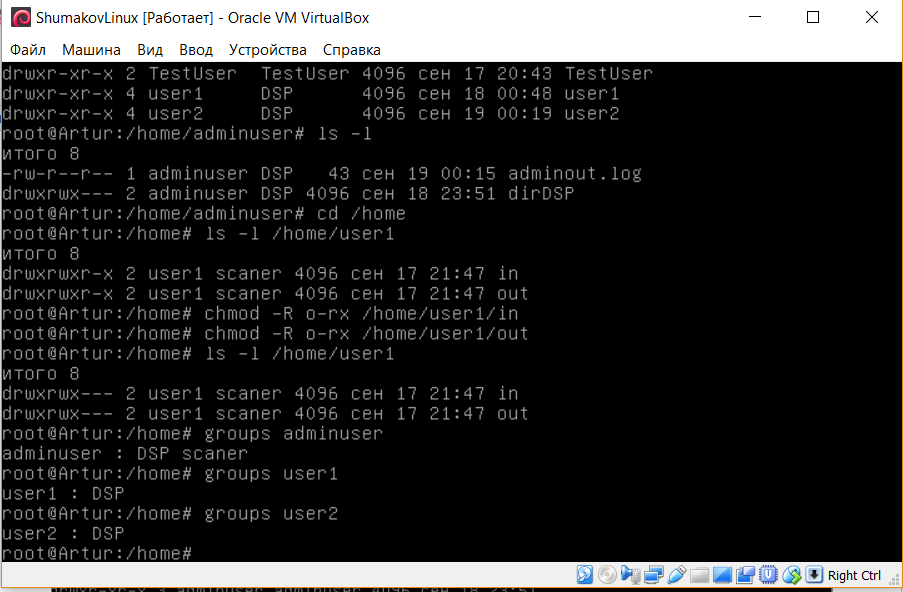


Файл adminout.log уже имеет права доступа для чтения для всех пользователей.



Отменены права доступа к папкам dirDSP, in и out для прочих пользователей.







AppArmor



**Вывод:** В ходе работы были изучены метод защиты операционных систем и

информации в операционных системах Linux, Windows.