# Лабораторная работа 5. Настройка учетных записей пользователей и прав доступа к файлам

**Аннотация:** Цель работы: получить представление об операциях над учетными записями, правах доступа к файлам, изучить команды управления правами доступа к объектам.

**Задание 1**. Создайте новую группу **students**, используя командную строку.

Ход выполнения:

1. Ознакомьтесь с информацией о команде добавления новой группы.

Основа распределения прав доступа в операционной системе Linux лежит на понятии пользователь. Пользователю выдаются определенные полномочия для работы с файлами, а именно на чтение, запись и выполнение.  Пользователи могут объединяться в группы, чтобы уже группам выдавать нужные полномочия на доступ к тем или иным файлам.

Чтобы добавить группу, воспользуйтесь командой *groupadd*:

*groupadd имя\_группы*

Параметры командной строки для утилиты *groupadd* описаны в таблице 1.

Таблица 1. Параметры командной строки *groupadd*

|  |  |
| --- | --- |
| *Параметр* | *Описание* |
| *-g gid* | Код группы (GID), это должно быть уникальное число больше 499 |
| *-r* | Создаёт системную группу с кодом меньше 500 |
| *-f* | Прерывает работу программы, если группа уже существует (При этом группа не изменяется). Если указаны параметры *-g* и *-f*, но группа уже существует, параметр *-g* игнорируется |

2. Создайте группу **students**, применяя команду *groupadd* с ключом прерывания работы программы в случае существования группы.





**Задание 2**. Создайте пользователей **Ann** и **Tom**, используя командную строку.

Ход выполнения:

1. Ознакомьтесь с информацией о команде добавления нового пользователя.

Для создания учетной записи пользователя применяют команду *useradd*.

*useradd имя\_пользователя*

Параметры командной строки для утилиты *useradd* описаны в [таблице](mk:@MSITStore:C:\Users\user\AppData\Local\Temp\Rar$DI00.638\56.Red%20Hat%20Enterprise%20Linux%204%20¦аTГ¦¦¦-¦-¦-¦+TБTВ¦-¦-%20¦¬¦-%20TБ¦¬TБTВ¦¦¦-¦-¦-¦-TГ%20¦-¦+¦-¦¬¦-¦¬TБTВTА¦¬TА¦-¦-¦-¦-¦¬TО.chm::/s1-users-cmd-line.html#TABLE-USERADD-OPTIONS)2.

Таблица 2. Параметры командной строки *useradd*

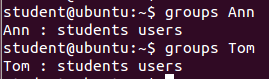
| *Параметр* | *Описание* |
| --- | --- |
| *-cкомментарий* | Комментарий пользователя |
| *-d дом\_каталог* | Домашний каталог, который следует использовать вместо стандартного */home/имя\_пользователя/* |
| *-e дата* | Дата, когда учётная запись должна быть отключена, в формате ГГГГ-ММ-ДД |
| *-f число\_дней* | Число дней после истечения срока действия пароля до отключения учётной записи. (Если указано число 0, учётная запись отключается сразу, как только истекает срок действия пароля. (Если указано число -1, учётная запись не отключается после истечения срока действия пароля. |
| *-g имя\_группы* | Имя или номер группы, которая должна стать основной группой пользователя (здесь должна указываться уже существующая группа.) |
| *-G список\_групп* | Список разделённых запятыми имён или номеров дополнительных групп (помимо основной), членом которых является пользователь. (Здесь должны указываться существующие группы.) |
| *-m* | Создаёт домашний каталог, если он не существует |
| *-M* | Не создаёт домашний каталог |
| *-n* | Не создаёт личную группу для пользователя |
| *-r* | Создаёт системную учётную запись с кодом, меньшим 500, и без домашнего каталога |
| *-p пароль* | Пароль, зашифрованный с помощью *crypt* |
| *-s* | Оболочка входа в систему, по умолчанию */bin/bash* |
| *-u uid* | Код пользователя (UID), это должно быть уникальное число больше 499 |

2. Создайте пользователей **Ann** и **Tom**, которые являются членами групп **users** и **students**, при этом основная группа этих пользователей – students.



3. Убедитесь, что пользователи входят в указанные группы:

*groups имя\_пользователя*

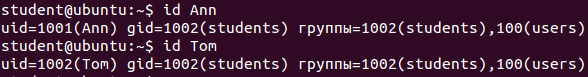
**

Если нужно поменять настройки уже созданного пользователя, то может потребоваться команда *usermod.* У неё тот же набор параметров, что и у команды *useradd*.

*usermod имя\_пользователя*

4. Получите информацию о пользователях **Ann** и **Tom** с помощью команды id:

*id имя\_пользователя*

**

5. Завершите сеанс работы того пользователя, под которым вы зарегистрированы в системе. Попытайтесь зайти в систему под учетными записями пользователей **Ann** и **Tom**.

Для смены пользователя в терминале используется команда *su*:

*su имя\_пользователя*

**

**

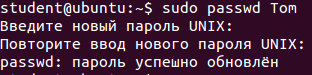
Для подтверждения, что пользователь изменился, используйте команду *whoami*:

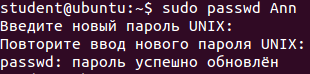
*whoami*

**

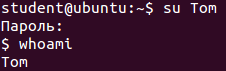
6. Команда *useradd* создает заблокированную учётную запись пользователя. Разблокируйте учётные записи, выполнив команду *passwd*, чтобы назначить пароль:

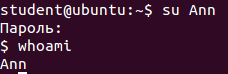
*passwd имя\_пользователя*

**

**

Снова попытайтесь зайти в систему под учетными записями пользователей **Ann** и **Tom**.

****

****

**Задание 3**. Назначьте для пользователя **Ann** срок действия пароля.

Ход выполнения:

1. Ознакомьтесь со способом, позволяющим назначить срок действия пароля учетной записи.

Чтобы настроить устаревание пароля пользователя в приглашении оболочки, воспользуйтесь командой *chage*, передав ей параметр из [таблицы  3](mk:@MSITStore:C:\Users\user\AppData\Local\Temp\Rar$DI00.528\56.Red%20Hat%20Enterprise%20Linux%204%20¦аTГ¦¦¦-¦-¦-¦+TБTВ¦-¦-%20¦¬¦-%20TБ¦¬TБTВ¦¦¦-¦-¦-¦-TГ%20¦-¦+¦-¦¬¦-¦¬TБTВTА¦¬TА¦-¦-¦-¦-¦¬TО.chm::/s1-users-cmd-line.html#TABLE-CHAGE-OPTIONS) и имя пользователя. Чтобы можно было использовать команду *chage*, необходимо включить скрытые пароли.

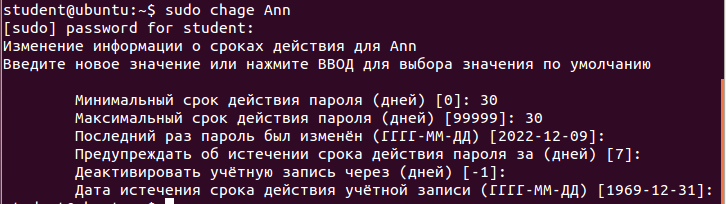
Таблица 3. Параметры команды *chage*

| *Параметр* | *Описание* |
| --- | --- |
| *-m* число\_дней | Определяет минимальный срок (в днях), по истечении которого пользователь должен менять пароль. Если это значение равно 0, срок действия пароля не будет истекать. |
| *-M* число\_дней | Определяет максимальный срок (в днях), в течение которого будет действовать пароль. Если количество дней, заданное этим параметром, и количество дней, заданное параметром *-d*, в сумме определяют день в прошлом, пользователь должен сменить пароль, чтобы использовать эту учётную запись. |
| *-d* число\_дней | Определяет дату смены пароля (число дней, прошедших после 1 января 1970 г.). |
| *-I* число\_дней | Определяет, через сколько дней после истечения срока действия пароля учётная запись будет заблокирована. Если значение равно 0, учётная запись не будет блокироваться. |
| *-E* дата | Определяет дату блокирования учётной записи, в формате ГГГГ-ММ-ДД. Вместо такого формата даты можно также указать число дней, прошедших после 1 января 1970 г. |
| *-W* число\_дней | Определяет, за сколько дней до истечения срока действия пароля будет предупреждаться пользователь. |

Если команде *chage* передаётся только имя пользователя (без параметров), она выводит текущие настройки устаревания пароля и позволяет вам изменить их.

Если системный администратор хочет, чтобы пользователь задал пароль при первом входе в систему, он может назначить пустой или какой-то исходный пароль, который истечёт немедленно, и, таким образом, пользователь должен будет сменить его при первом входе.

2. Ограничьте срок действия пароля пользователя **Ann** 30 днями с предупреждением за 7 дней.



**Задание 4**. Настройте принудительную смену пароля при первом входе пользователя **Tom** на консоли.

Ход выполнения:

1. Заблокируйте пароль пользователя, выполнив команду:

*usermod -L имя\_пользователя*

**

2. Сделайте так, чтобы потребовалась немедленная смена пароля – введите следующую команду:

*chage -d 0 имя\_пользователя*

**

Эта команда задаёт в качестве даты последней смены пароля точку отсчёта эпохи (1 января 1970 г.). При этом значении пароль требуется сменить немедленно, вне зависимости от политики устаревания паролей, если она действует.

3. Разблокируйте учётную запись. Сделать это можно двумя распространёнными способами. Администратор может назначить пустой или какой-то начальный пароль.

Не используйте для назначения пароля команду *passwd*, так как она отменит только что настроенное требование смены пароля.

Назначьте пустой пароль:

*usermod -p "" имя\_пользователя*

**

**

**Задание 5**. Изучите конфигурационные файлы, содержащие информацию о пользователях и группах.

Ход выполнения:

1. Ознакомьтесь с назначением конфигурационных файлов.

В файле */etc/passwd* хранится вся информация о пользователях кроме пароля. Одна строка из этого файла соответствует описанию одного пользователя.



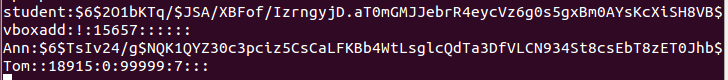
В */etc/group*  хранится информация о группах.





Файл */etc/shadow* хранит в себе пароли, поэтому права, установленные на этот файл, не дают считать его простому пользователю.





2.Найдите информацию о пользователях **Ann** и **Tom** во всех ранее перечисленных файлах. Расшифруйте содержимое найденных записей.

имя**:**хеш пароля**:**id пользователя**:**id группы:полное имя:домашняя директория**:**абсолютный путь к оболочке входа пользователя



имя**:** хеш пароля**:**id группы**:**список пользователей



имя:зашифрованный пароль:последнее изменение пароля:минимальный возраст пароля:максимальный возраст пароля:период предупреждения:период бездействия:срок годности



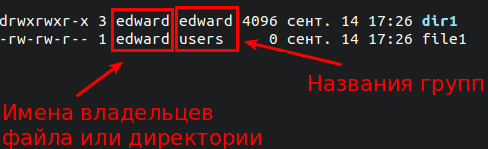
**Задание 6**. Изучите способы изменения прав доступа к объектам файловой системы.

Ход выполнения:

1. Создайте в домашнем каталоге файл **text**.



2. Просмотрите права доступа к файлу **text** с помощью команды *ls –l*.





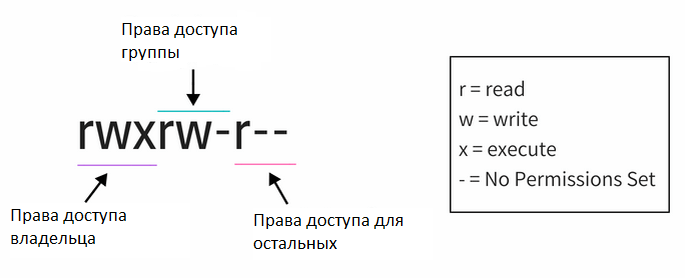
В первом столбце указаны права доступа к файлам, в третьем – владелец файла, в четвертом – группа. Первый символ первого столбца «-» означает тип файла – обычный. Остальные 9 символов характеризует набор прав доступа к файлу.

* **Первая группа из трех символов обозначает** права доступа владельца файла или директории (u - user).
* **Вторая группа из трех символов обозначает** права доступа на файл или директорию для системной группы (g - group).
* **Третья группа из трех символов обозначает** права доступа на файл или директорию для всех остальных (o - other).

У этих трёх групп **одинаковая комбинация символов**, то есть:

|  |  |
| --- | --- |
| **r** | read, то есть, право доступа на чтение файла или директории. |
| **w** | write, то есть, право на изменение и удаление файла или директории. |
| **x** | eXecute, то есть, право на запуск файла как программы или вход в директорию. |

Если вместо какого-то символа идёт тире (минус), то это значит, что отсутствуют права на изменение и удаление файла или директории.



В примере на рисунке владелец получает полный доступ к файлу, группа – право на чтение и изменение, все остальные – только на чтение.

Для изменения владельца файла используется команда *chown*. Если нужно изменить группу файл, то примените команду *сhgrp*. А для изменения прав доступа к файлу – команду *chmod*.

3. Измените права доступа к файлу символьным способом. Опции, применяемые в символьном способе, перечислены в таблице 4.

Таблица 4.Опции символьного способа изменения прав доступа к объектам файловой системы.

|  |  |
| --- | --- |
| *Опция* | *Описание* |
| *+* | Устанавливает право доступа |
| *-* | Отменяет право доступа |
| *=* | Присваивает набор прав доступа |
| *u* | Устанавливает право доступа для пользователя, который создал файл и является его владельцем |
| *g* | Устанавливает право доступа для группы |
| *o* | Устанавливает право доступа для прочих пользователей |
| *а* | Устанавливает право доступа для владельца, группы и прочих пользователей |

Следующая команда предоставит право на запись файла **text** для всех пользователей:

*chmod a+w text*

**

Чтобы добавить для группы право на выполнение файла **text** и снять право на запись, воспользуйтесь командой

*chmod g+x-w text*

**

4. Измените права доступа к файлу абсолютным способом (метод двоичных масок).

В случае применения этого способа девять символов прав доступа кодируются одним числом. Пример расшифровки цифрового кода приведен в таблице 5. Набор символов *rwxr-xr-* соответствует числу 754.

Таблица 5. Пример расшифровки цифрового кода.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 цифра | | | 2 цифра | | | 3 цифра | | |
| 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |
| r | w | x | r | - | x | r | - | - |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 4+2+1 | | | 4+0+1 | | | 4+0+0 | | |
| 7 | | | 5 | | | 4 | | |

5. Измените права доступа к файлу **text** следующим образом:

*chmod 765 text*

**

Как после применения этой команды изменились права доступа к файлу **text**?

**rwx rw- r-x**

**Задание 7**. Выполните самостоятельно следующие задания.

Ход выполнения:

1. Изучите команды *chown*, *chgrp* и особенности их использования с различными ключами.

**$ chown пользователь опции /путь/к/файлу**

Также можно указать через двоеточие группу, например, **пользователь:группа**. Тогда изменится не только пользователь, но и группа.

* **-c, --changes** - подробный вывод всех выполняемых изменений;
* **-f, --silent, --quiet** - минимум информации, скрыть сообщения об ошибках;
* **--dereference** - изменять права для файла к которому ведет символическая ссылка вместо самой ссылки (поведение по умолчанию);
* **-h, --no-dereference** - изменять права символических ссылок и не трогать файлы, к которым они ведут;
* **--from** - изменять пользователя только для тех файлов, владельцем которых является указанный пользователь и группа;
* **-R, --recursive** - рекурсивная обработка всех подкаталогов;
* **-H** - если передана символическая ссылка на директорию - перейти по ней;
* **-L** - переходить по всем символическим ссылкам на директории;
* **-P**- не переходить по символическим ссылкам на директории (по умолчанию).



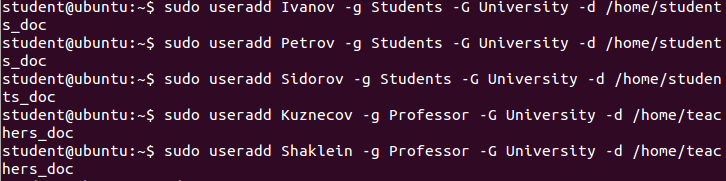


2. Создайте две группы: Преподаватели и Студенты.

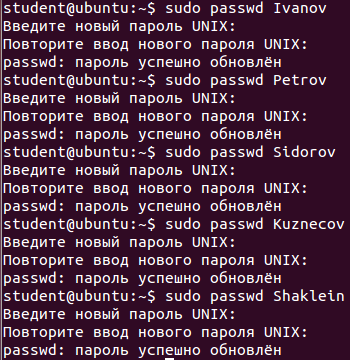




3. Создайте три учетные записи студентов: Иванов, Петров, Сидоров с домашней директорией /home/students\_doc и две учетные записи преподавателей: Кузнецов и Шаклеин с домашней директорией /home/teachers\_doc.



4. Включите созданные учетные записи студентов в группу Студенты, а учетные записи преподавателей в группу Преподаватели. Пароли задавайте произвольно.



5. Для экспериментов создайте папку «Эксперимент» в каталоге /home. Установите полный доступ к папке для Преподавателей и Студентов (больше никаких прав ни у кого не должно быть).





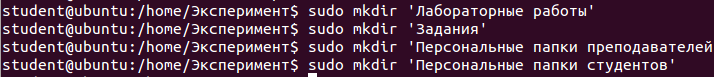








6. Создайте в папке «Эксперимент» четыре папки: «Лабораторные работы», «Задания», «Персональные папки преподавателей», «Персональные папки студентов».



«Лабораторные работы» – здесь студенты будут создавать свои файлы. Эти файлы будут изменять преподаватели (при необходимости). Реализуйте необходимые права на эту папку.









«Задания» – здесь преподаватели будут помещать задания для лабораторных работ. Студенты должны иметь доступ только для чтения. Реализуйте необходимые права на эту папку.





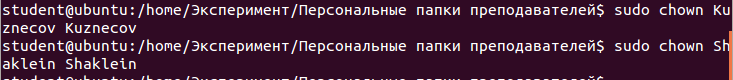




«Персональные папки преподавателей» – здесь создайте две папки по фамилиям преподавателей и выставите права единоличного доступа преподавателя на эту папку.

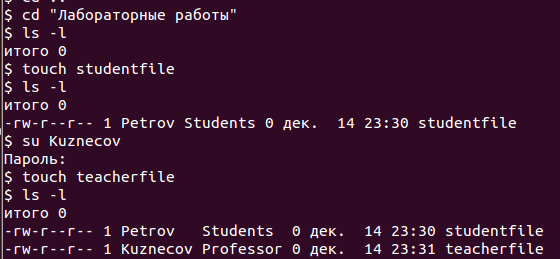








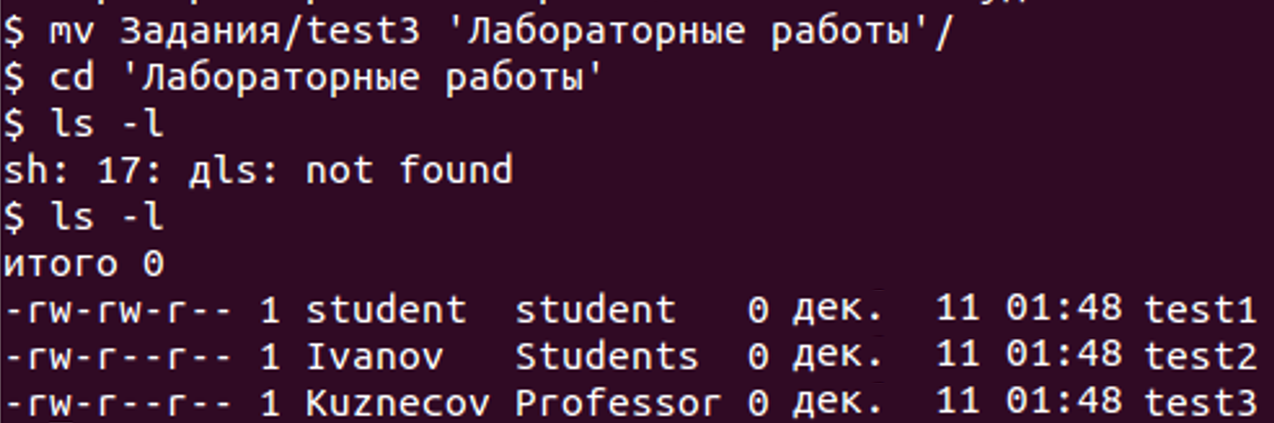
7. Посмотрите на права файлов в папках «Задания» и «Лабораторные работы». Чем отличаются права на эти файлы и от чего они зависят?





Права на файлы не наследуются от прав каталога, по умолчанию они имеют права 644, а каталоги 755.

8. Создайте еще один файл в папке «Задания». Переместите его в папку «Лабораторные работы». Какие права получил файл? Чем отличается наследование/передача прав при перемещении и при копировании? Сделайте выводы.

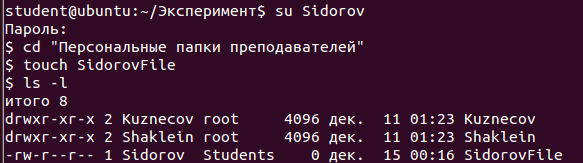


При копировании создается новый файл, при перемещении просто меняется расположение.  
При копировании права устанавливаются в соответствии с тем, кто копирует.

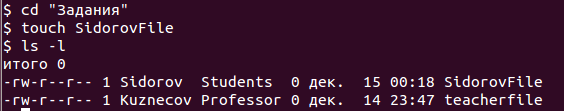
9. Предположим, студент Сидоров стал лаборантом – добавьте его в группу преподавателей. Сейчас он принадлежит двум группам. Экспериментально проверьте, какие права получит Сидоров – максимально запрещающие или максимально разрешающие?











Смог зайти в папку для преподавателей и создать файл

Максимально разрешающие

**Задание 8.** Ответьте на следующие вопросы**:**

1. Как определить имя рабочего терминала пользователей, работающих в системе? Who



2. Как определить, когда последний раз была загружена система?

who –b

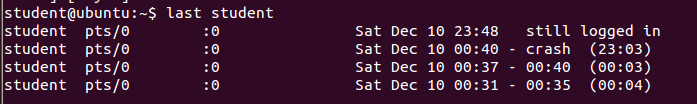


3. Как установить оболочку, используемую по умолчанию, при создании пользователя?

useradd -s

4. Как узнать время входа в сеанс конкретного пользователя?

last username



5. В каком файле содержится информация о последних сеансах?

/var/log/lastlog

/var/log/wtmp