

# **ЛАБОРАТОРНАЯ РАБОТА №8**

## **УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ**

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

Цель работы: Научится администрировать учетные записи пользователей: создавать, удалять, менять политики доступа

Задание:

*Задание (пошагово):*

1. У вас должно быть право на чтение файла `/etc/passwd`. Для ответа на следующие вопросы воспользуйтесь для вывода на экран `/etc/passwd` утилитой `cat` или `less`; Просмотрите в файле `/etc/passwd` поля с информацией о пользователях вашей системы.
  - a) Какой символ используется для разделения полей в `/etc/passwd`?
  - b) Сколько полей используется для описания каждого пользователя?
  - c) Сколько пользователей в вашей системе?
2. Сколько различных входных оболочек используется в вашей системе?

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

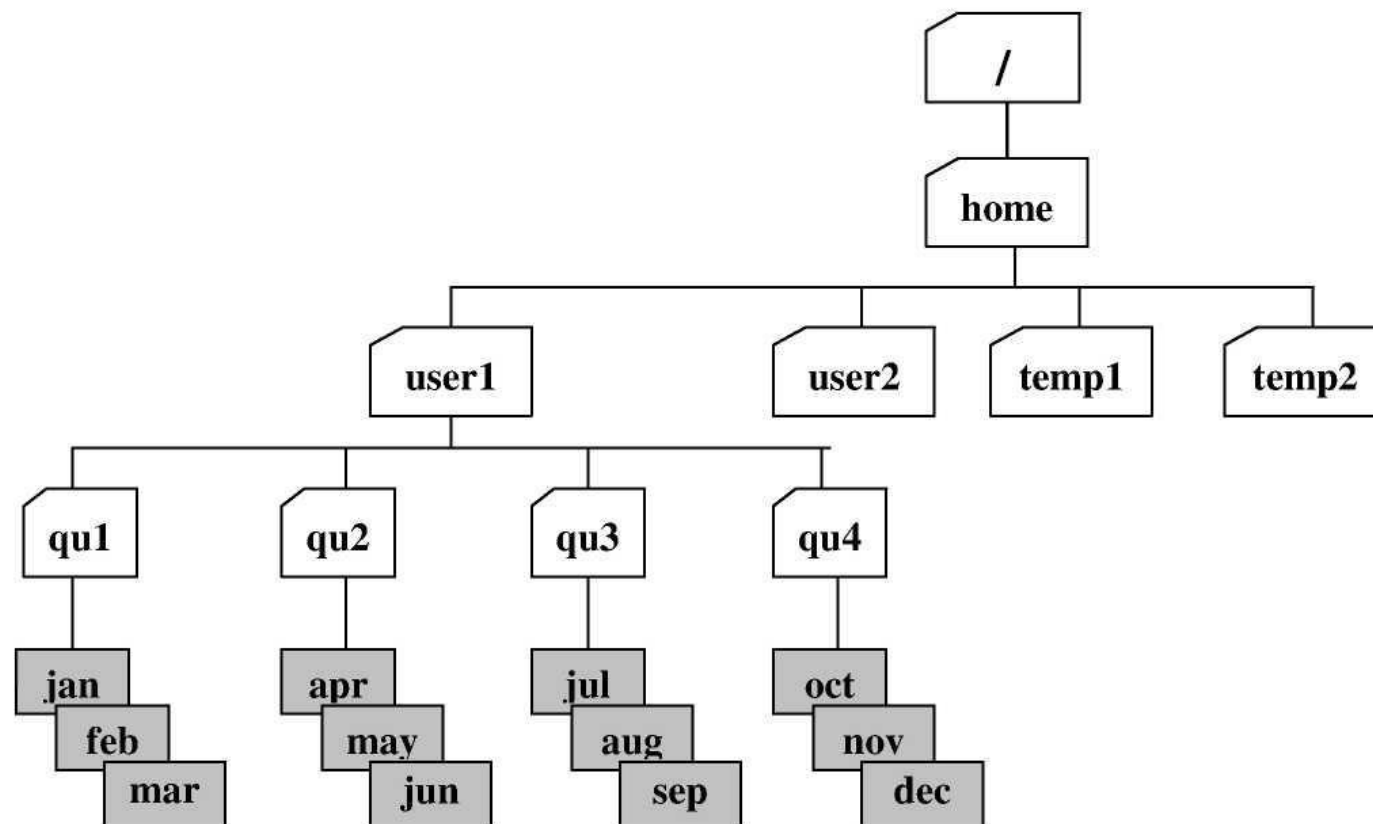
3. Второе поле в `/etc/passwd` хранит пароли пользователей в закодированной форме. Если поле пароля содержит букву `x`, то ваша система использует теневые пароли и хранит закодированные пароли в другом месте. Применяются ли в вашей системе теневые пароли?
4. Добавьте трех новых пользователей с соответствующими домашними директориями: **student7**, **student8**, **student9**. Задайте пароли для каждого из них.
5. Создайте группу **course** и добавьте в нее всех трех пользователей.
6. Для пользователя **student7** выставите ограничение: срок действия пароля 5 месяцев и предупреждение об окончании срока действия пароля 7 дней
7. Заблокируйте пользователя **student8**. Проверьте, что блокировка подействовала.
8. Войдите в систему под пользователем **student9**
9. Создайте два новых файла **file1** и **file2** и две новых директории **dir1** и **dir2**
10. Войдите в систему под пользователем **root**
11. Сделайте **file1** исполняемым. Запускаться файл должен от имени владельца и группы файла

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

12. Установите в качестве владельца файла **file1** пользователя **student7** и группу **course**
13. Войдите в систему под пользователем **student7**. Попробуйте перейти в директорию пользователя **student9** и сделать запись в файле **file1**.
14. Войдите в систему под пользователем **root**. Разблокируйте пользователя **student8**. Проверьте, что блокировка снята
15. Перейдем к управлению учетными записями пользователей. Создайте в ОС Linux двух пользователей (**user1** и **user2**) и задайте их пароли. Зарегистрируйтесь в первой консоли как **user1**.
16. С помощью **Ctrl+Alt+F2 (Alt+F2)** откройте второй текстовый терминал и зарегистрируйтесь как **user2**.
17. Аналогично откройте третий текстовый терминал и зарегистрируйтесь в нем с правами суперпользователя.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

18. Нажатием **Ctrl+Alt-F1(Alt-F1)** вернитесь в первую консоль. Теперь, переключая консоль, вы можете работать с объектами операционной системы от имени двух разных пользователей и администратора системы. Основная часть задания выполняется с правами обычного пользователя. Переходите в третью консоль и используйте права **root** только при выполнении соответствующих пунктов задания.





# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

19. С правами `user1` попробуйте войти в каталог `/root`. Объясните результат. С помощью команды `ls-la/` просмотрите список основных каталогов и укажите, каких прав доступа вам недостает для входа в каждый из каталогов
20. Переключитесь в консоль администратора и создайте два новых временных каталога `mkdir-m777 /home/temp1` и `mkdir-m777 /home/temp2`. Проверьте права доступа к каталогам `/home/user1` и `/home/user2`: они должны быть установлены в 755. Вернитесь в консоль `user1`.
21. Пользуясь командой `mkdir`, создайте в домашнем каталоге пользователя `/home/user1` четыре каталога с именами: `qu1`, `qu2`, `qu3`, `qu4`. При создании каталогов объявите следующие права доступа к ним: (`qu1`-777, `qu2` -404, `qu3` -1333, `qu4` -505. Пример: `cd; mkdir-m777 qu1`). С помощью команды `ls/home/user1` убедитесь в том, что каталоги созданы. Какие из предоставленных прав кажутся Вам лишними смысла? Почему?

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

22. Задайте права доступа к файлам "по умолчанию". Для этого установите `umask022`. Поясните, какие права к вновь создаваемым файлам и каталогам будут предоставляться пользователю, членам его группы и остальным.
23. В каждом из каталогов создайте по три текстовых файла с именами (**jan, feb, mar**), (**apr, may, jun**), (**jul, aug, sep**), (**oct, nov, dec**). В каждый файл запишите календарь на определенный месяц текущего года. Например, команда `cal 1 2010 > jan` создает в текущем каталоге файл `jan` и записывает в него календарь на январь 2010 года. Не забывайте, что использование относительного (короткого) имени файла требует, чтобы Вы находились в нужном каталоге. В противном случае следует указывать полный путь к создаваемому файлу. Для навигации по каталогам используйте команды `cd` и `pwd`. В каком случае создание файлов не удалось? Почему?
24. С помощью команды `chmod` измените нужные права доступа в "недоступные" каталоги `qu2`, `qu4` и создайте там указанные файлы. После этого верните каталогам прежние права доступа.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

25. С помощью команд `cd` и `ls` войдите в каждый из созданных каталогов и просмотрите список созданных файлов. Для просмотра каталога необходимо последовательно ввести две команды: `cd` и `ls`. При просмотре используйте два режима: `ls` без аргументов и `ls -l`. В каких случаях не удалось войти в каталог? В каких случаях не удалось посмотреть список файлов? Почему?
26. Прочитайте содержимое одного из файлов в "темном" каталоге (например, `cd/home/user1/qu3`; `cataug`). Сделайте выводы.
27. Перейдите во 2-ю консоль и с правами пользователя `user2` войдите в каталог `/home/user1/qu1`. Создайте в каталоге `/home/user2` новый файл `quart1` путем конкатенации нескольких имеющихся (catjanfebmar>`/home/user2/quart1`). С помощью команды `file` определите тип созданного файла. Попробуйте вывести его на экран командой `cat`. Что представляет собой данный файл?
28. С помощью команды `chmod` установите права доступа `077` на созданный файл `quart1`. Вновь попробуйте прочесть его. Ответьте, почему владельцу файла запрещается доступ, если файл доступен для всех? Что необходимо сделать, чтобы вернуть владельцу права на доступ?



# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

29. Установите для файла `quatr` права на доступ 4700. Кому и какие права вы при этом предоставили? Как воспользоваться этими правами? Какие из предоставленных прав не имеют смысла?
30. Перейдите в консоль администратора и передайте право владения на файлы `may` и `aug` пользователю `user2` (команда `chown`). Поочередно из консолей `user1` и `user2` проверьте, как изменились права владения файлами после его передачи. Может ли пользователь `user2` воспользоваться предоставленными правами?
31. С правами пользователя `user1` из каталогов `/home/temp1` и `/home/temp2` с помощью команды `ln` создайте две "жесткие" ссылки на файл `dec` с именами `dec_h1` и `dec_h2` (пример: `ln/home/user1/qu4/dec/home/temp1/dec_h1`). Чем созданные ссылки отличаются от исходного файла? На сколько байт уменьшилось дисковое пространство после создания этих ссылок?

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

32. С помощью команды `ln-s` создайте из каталогов `/home/temp1` и `/home/temp2` две символические ссылки на файл `dec` именами `dec_sl1` и `dec_sl2`. Чем отличаются созданные ссылки от исходного файла? Попробуйте прочитать содержимое файлов символических ссылок. Что они собой представляют?
33. С правами пользователя `user2` с помощью команды `cp` создайте в каталогах `/home/temp1` и `/home/temp2` по одной копии файла `dec` другим именем (`dec_copy1`). Чем отличаются исходный файл и его копия (обратите внимание на то, кто является владельцем исходного файла и его копии)? Чем отличаются права доступа на эти файлы? Вернитесь в консоль `user1`.
34. С помощью команды `rm` удалите файл `dec`. Что произошло с "жесткими" и символическими ссылками на данный файл? Что произошло с его копиями? Что нужно сделать для того, чтобы файл перестал существовать (на логическом уровне)?
35. С правами `user1` удалите файлы из каталогов `/home/temp1` и `/home/temp2`. Какие файлы не удалось удалить? Почему? Попробуйте удалить оставшиеся файлы правами пользователя `user2`. Объясните результат.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

36. Попробуйте удалить любой из каталогов **qu1**, **qu2**, **qu3**, **qu4** с помощью команды **rmdir** (не удаляя предварительно из них файлов). Объясните результат.
37. Войдите в консоль администратора и с правами **root**, пользуясь командой **chattr**, заблокируйте файл **febot** любых изменений. Установите параметр запрета любых операций, кроме добавления данных для файла **mar**. Вернитесь в консоль **user1**. С помощью команды **lsattr-1** проверьте наличие дополнительных атрибутов у файлов.
38. С правами пользователя **user1** добавьте одну строку **finish** в конец файлов **feb** и **mar** (воспользуйтесь для этого командой **echofinish>> file\_name**). Убедитесь в успешном завершении операции, объясните результат.
39. С правами пользователя **user1c** помощью команды **rm-rf** последовательно удалите ранее созданные каталоги **qu2**, **qu3**, **qu4** вместе с файлами. Объясните результат.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

40. С помощью команды `md5sum` вычислите и запишите контрольную сумму для одного из файлов в каталоге `/home/user1/qul`. Добавьте один символ в этот файл с помощью команды `echo` (например, `echo a>>/home/user1/qul/jan`). Вновь вычислите контрольную сумму файла и сравните два результата.
41. С помощью команды `cat/dev/fd0` попробуйте прочесть специальный файл устройства. Объясните результат? Для чего служат специальные файлы?
42. С помощью команды `find` правами администратора найдите в корневом каталоге файлы:
- имеющие атрибуты `SUID` (`find / -type f -perm -4000`);
  - файлы, которым разрешено модифицировать всем (`find / -type f -perm -2`);
  - файлы, не имеющие владельца (`find / -nouser`);
  - объясните, какой интерес могут представлять для администратора указанные категории файлов?

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

- 43. Зарегистрируйтесь в системе в консольном режиме с правами root.
- 44. Используя команду `cat` правами **root**, просмотрите содержимое файла `/etc/passwd`.
- 45. Аналогично изучите содержимое файла `/etc/shadow`.

Вам необходимо создать учетные записи и определить права доступа для десяти (10) сотрудников: `w_gromov`, `n_kalinina`, `e_ivanova`, `r_klinova`, `b_rebrov`, `k_beglov`, `i_frolov`, `d_lavrov`, `m_kruglov`, `t_uporov`, работающих в одном подразделении и занятых созданием и редактированием текстовых документов различного уровня конфиденциальности.

Разграничение доступа к информации должно быть произведено на основании следующих требований:

о допуск к секретным сведениям имеют четыре пользователя: `w_gromov`, `n_kalinina`, `b_rebrov`, `k_beglov`;

о три пользователя: `n_kalinina`, `b_rebrov`, `k_beglov` работают над созданием секретных документов, каждый по своему профилю. Их домашние каталоги и файлы должны быть полностью недоступными как друг для друга, так и для всех остальных, исключая `w_gromov`;



# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

- о три пользователя: `i_frolov`, `d_lavrov`, `e_ivanova` имеют допуск к конфиденциальной информации и работают над документами с соответствующим грифом. Они имеют право читать файлы с конфиденциальной информацией, созданные своими коллегами, без права их модификации;
- о все секретноносители имеют право знакомиться с конфиденциальными файлами;
- о три пользователя: `r_klinova`, `m_kruglov`, `t_uporov` могут работать только с открытой информацией. Их файлы должны быть доступны для чтения каждому сотруднику подразделения (без права модификации);
- о `w_gromov` является редактором подразделения и имеет право читать и модифицировать файлы всех сотрудников и всех уровней конфиденциальности. Завершенные документы копируются пользователем `w_gromov` в его домашний каталог, который должен быть недоступен для всех остальных сотрудников подразделения.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

46. Укажите в отчете, какие коллизии вы усматриваете в сформулированных требованиях? Как реализовать указанные требования таким образом, чтобы пользователи не могли по своему усмотрению изменять установленный порядок?
47. С помощью команды **groupadd** создайте четыре пользовательских группы: **alfa**, **beta**, **nabla**, **sigma**. Формат команды **groupadd-gGIDgroup\_name**. Идентификатор группы **GID** можно назначать произвольно, начиная с номера 100 (например, **groupadd-g101 alfa**).
48. Создайте учетные записи для вышеуказанных десяти новых пользователей. Регистрационные данные (кроме паролей и групп) сведены в таблицу. Пароли назначайте произвольно, длиной не менее 8 символов, не забывая фиксировать их в черновике отчета. Для пользователей **e\_ivanova**, **r\_klinova** задайте одинаковые пароли. Распределите сотрудников по группам таким образом, чтобы удовлетворить вышеперечисленным требованиям. Изобразите в отчете схему, поясняющую разграничение доступа сотрудников подразделения к компьютерной информации.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

49. Пять первых пользователей (w\_gromov, n\_kalinina, e\_ivanova, r\_klinova, b\_rebrov) зарегистрируйте с помощью команды `useradd`. Синтаксис команды: `useradd -u UID -g group_name -d dir_home -m -p password -e date_del_user user_name`. Например, `useradd -u 501 -g sigma -d /home/n_kalinina -p v5g7K2S4 -e 2011-01-07 n_kalinina`. Параметр `-m` обеспечивает создание домашнего каталога пользователя, если он еще не существует. Прочие параметры команды можно не указывать. *Помните, имя пользователя не должно начинаться с цифры и содержать заглавных и русских букв, символов типа \*#%л.... Идентификаторы пользователей **UID** назначаются, начиная с 500. Дата удаления учетной записи пользователя вводится в формате ГГГГ-ММ-ДД.*
50. Пять последних пользователей зарегистрируйте с помощью командного файла `adduser`, которая запрашивает значения в интерактивном режиме. При вводе данных ориентируйтесь на подсказки системы [в квадратных скобках]. Все параметры, кроме имени

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

пользователя, его идентификатора, имени группы, пароля и домашнего каталога можно игнорировать. Для ввода параметра по умолчанию вводить **Enter**.

Пользователи	UID	Пароль	Группа	Домашний каталог	Дата удаления учетной записи
i_frolov	501			/home/i_frolov	T+ 10 дней
m_kruglov	502			/home/m_kruglov	T+ 30 дней
b_rebrov	503			/home/b_rebrov	T+ 12 дней
d_lavrov	504			/home/d_lavrov	T+ 60 дней
e_ivanova	505			/home/e_ivanova	T+ 30 дней
t_uporov	506			/home/t_uporov	T+ 15 дней
k_beglov	507			/home/k_beglov	T+ 45 дней
n_kalinina	508			/home/n_kalinina	T+ 30 дней
r_klinova	509			/home/r_klinova	T+ 90 дней
w_gromov	510			/home/w_gromov	не удалять

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

51. Переключаясь во вторую консоль, отслеживайте изменения, происходящие в файле `/etc/passwd` по мере ввода новых учетных записей.
52. Попробуйте с правами пользователя посмотреть файл `/etc/shadow`. Повторите попытку просмотра с консоли супер пользователя. Почему поля, отведенные для хэшированных паролей у пользователей `e_ivanov` и `r_klinov` различаются?
53. Из первой консоли с помощью команды `su` измените права администратора на права пользователя `w_gromov`. Почему система не запрашивает пароль? С помощью команды `exit` верните себе права администратора. Был ли запрошен пароль? (В различных дистрибутивах Linux возврат полномочий администратора организован различным образом).
54. Запустите оболочку `MidnightCommander` в режиме редактирования (F4) файла паролей `/etc/passwd` и удалите в учетной записи пользователя `n_kalinin` символ признака пароля (между первым и вторым двоеточием), включая пробел. Сохраните изменения в файле, завершите сеанс в `MidnightCommander`, с помощью `Ctrl+Alt+F2` (`Alt+F2`) откройте второй текстовый терминал и зарегистрируйтесь пользователем `n_kalinina`, но теперь с «пустым»



# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

паролем. Сделайте вывод относительно опасности предоставления прав на запись в этот файл. Завершите сеанс для пользователя `n_kalinin` с помощью команды `exit`.

55. Пользователь `d_lavrov` уволен за дисциплинарный проступок. С помощью команды `userdel -user_name` удалите его учетную запись вместе с домашним каталогом. В реальных условиях необходимо вначале скопировать в другую директорию файлы пользователя, представляющие ценность для организации.

56. Зарегистрируйте вместо уволенного пользователя нового сотрудника `f_mironov` с предоставлением ему аналогичных прав (пароль должен быть новым!).

57. Пользователь `r_klinova` уехала в командировку сроком на две недели. Заблокируйте ее учетную запись, для чего с правами администратора войдите в режим редактирования файла паролей и вставьте во второе поле (между первым и вторым двоеточием) любой символ, который не разрешено использовать для пароля. Попробуйте зарегистрироваться во второй консоли с правами `r_klinova` и убедитесь в том, что для этого пользователя система не доступна.

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

58. Зарегистрируйтесь во второй консоли с правами пользователя **k\_beglov**, вызовите команду **passwd** и измените свой пароль. В качестве нового пароля введите **qwerty**.
59. Перейдите в консоль администратора и назначьте пользователю **k\_beglov** новый пароль **zxcvbnm**. Затем с помощью команды **chage** (**changeaging**-изменить информацию об устаревании) установите для этого пользователя минимальное время действия паролей, равное 5 дням. С какой целью устанавливается минимальный срок действия пароля?
60. Просмотрите электронную справку по файлу **/etc/sudoers**. Отредактируйте его таким образом, чтобы предоставить следующим пользователям дополнительные права за счет использования команды **sudo**:
- о пользователю **e\_ivanova**-право монтировать файловые системы,
  - о пользователю **b\_rebrov**-право изменения владельца файлов.
- Ответьте, чем отличается предоставление прав пользователям с помощью **sudo** от использования эффективных идентификаторов **SUID**?

# УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

61. Из второй консоли с правами пользователя `f_mironov` создайте файл `cal2010` > `/home/f_mironov/cal2010`. С помощью команды `su` переключите консоль на пользователя `b_rebrov` и с помощью временно предоставленных ему привилегий передайте права на созданный `f_mironov` файл другому владельцу `n_kalinina`. Каким еще путем можно предоставить подобные права пользователям, не передавая им "опасных" полномочий администратора?
62. Просмотрите с правами администратора системные журналы в каталоге `/var/log` и убедитесь, что система зафиксировала факты присвоения полномочий администратора