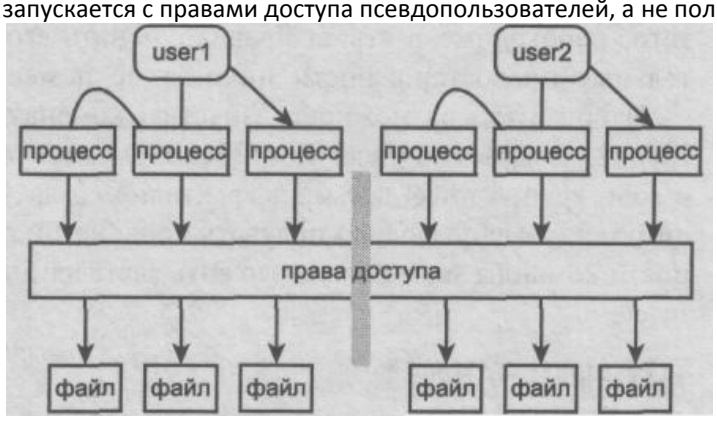
FreeBSD - концепция работы с пользователями. Выполнение команд от имени других пользователей (SU, SUDO).

Модель пользователей и прав доступа, применяемая во FreeBSD (и большинстве систем UNIX), является одноуровневой. Есть только два типа пользователей: обычные и *суперпользователь,* или ***root.*** Права доступа обычных пользователей так или иначе ограничивают их действия в системе. Пользователь **root** — единственный, кто свободен от каких бы то ни было ограничений.
Каждый пользователь FreeBSD имеет ограниченные права доступа и постоянное место для работы в системе — начальный каталог (home directory). Повысить свой статус в системе до уровня **root** дает возможность команда **su.** Она запрашивает пароль **root** — фактически, ключ к царству. Пароль **root** — это самая важная информация в любой UNIX-системе. Получение доступа с правами **root** позволяет создавать, изменять или уничтожать абсолютно все, что содержит система. При регистрации в системе с правами **root** следует проявлять повышенную осторожность и всегда по мнить, что злонамеренный пользователь, дабы получить доступ суперпользователя может прослушивать сеть. Поэтому пароль **root** ни в коем случае нельзя передавать по сети как обычный текст.
Кроме того, необходимо взять за правило менять его хотя бы раз в месяц. Здесь дополнительные предосторожности никогда не помещают. Чтобы иметь возможность запустить команду **su** необходимо принадлежать к элитной группе, называемой **wheel.** Хотя FreeBSD имеет только два типа пользователей — обычные и **root,** группа **wheel** весьма эффективно создает ограниченный круг особо доверенных лиц: тех, кому позволено получать привилегии **root** (с помощью su). Используя возможности команды **su,** можно возложить часть административных задач на других пользователей.
ПРИМЕЧАНИЕ
FreeBSD отличается от многих дистрибутивов Linux и других версий UNIX тем, что при удаленном доступе (посредством Telnet или даже SSH) не позволяет пользователю **root** регистрироваться в системе. Это одна из важных мер безопасности. Для получения доступа в качестве root необходимо зарегистрироваться как обычный пользователь (естественно, принадлежащий к группе **wheel]** и запустить команду **su.** Такой подход затрудняет доступ неавторизованным пользователям, поскольку в этом случае им кроме пароля **root** требуется еще и пароль кого-либо из группы **wheel.**

Пользователей системы можно разделить на реальных людей, подключающихся к системе, и псевдопользователей (таких как bin, **operator, daemon, nobody** и другие). Последние необходимы системе для того, чтобы управлять процессами. Важно понимать, что процессы, как и файлы, принадлежат определенным пользователям и при взаимодействии с другими процессами и файлами подчиняются ограничениям, наложенным на них правами доступа.

Пользователи никогда не работают с файлами непосредственно: выполняемые ими команды запускают процессы (имеющие установленные для пользователя права доступа), а процессы выполняют заданные операции над файлами и взаимодействуют с другими процессами (см. рис. 10.1). Процесс, владельцем которого является первый пользователь (user 1), может работать только с файлами и процессами, принадлежащими ему, но если он попытается изменить что-либо, принадлежащее второму пользователя (user 2), в доступе будет отказано. При простейших системных установках пользо-ватель может вносить изменения лишь в принадлежащие ему файлы и процессы.

Теперь посмотрим, что происходит, если user 1 -- это **root.** В этом случае его процессы имеют "абсолютную власть" над любыми процессами. Если один из процессов пользователя **root** — это программа, изменяющая определенные настройки системы в конфигурационном файле, то система станет уязвимой для атак, поскольку хакеры могут воспользоваться ошибкой в этой программе и, произведя запрос с "неправильными" параметрами, нарушить работу системы или получить контроль над ней. Последствия могут быть совершенно непредсказуемыми. Поэтому большинство системных процессов запускается с правами доступа псевдопользователей, а не пользо-вателя **root.**



Пользователь запускает процессы, которые взаимодействуют с файлами и другими процессами.

su или sudo?
Исторически единственным универсальным способом выполнить команду от имени другого пользователя в Unix была программа su. Запущенная без параметров, она запрашивала пароль суперпользователя и в случае успеха просто подменяла текущее имя пользователя на root, оставляя почти все переменные окружения от старого пользователя (кроме PATH, USER и еще пары-тройки, см. man su от своего дистрибутива). Более корректно было запускать ее как su - — в таком

случае оболочка получала также и правильный environment. При этом доверенным пользователям приходилось помнить пароль root'а и у всех пользователей, перечисленных в группе «wheel» (т.е. в группе, члены которой могли выполнить команду su и стать суперпользователем), был одинаковый неограниченный доступ ко всей системе, что являлось серьёзной проблемой безопасности.

Затем появилась команда sudo, и это был прорыв. Теперь администратор мог указывать список разрешенных команд для каждого пользователя (или группы пользователей), файлы, доступные для редактирования, специальные переменные окружения и многое другое (все это великолепие управляется из /etc/sudoers, см. man sudoers от своего дистрибутива). При запуске sudo спрашивает у пользователя его собственный пароль, а не пароль root.

что хотим сделать?	**правильно**
выполнить команду от имени root	sudo command
отредактировать файл от имени root	sudoedit file
получить оболочку root	sudo -i