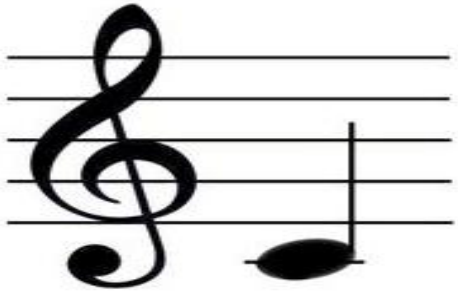
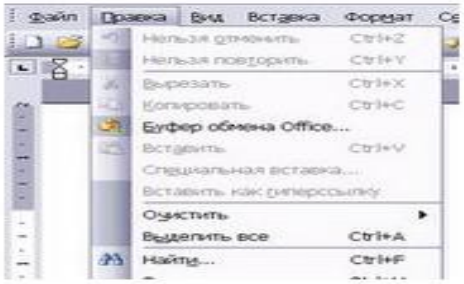
Р,  ,#

 ,  ,Пы





 4 = ы

Рабочие группы и домены

Рабочая группа — это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети.

Принципиально важно, что каждый компьютер в рабочей группе равноправен (т. е. сеть получается одноранговой) и поддерживает собственную локальную базу данных учетных записей пользователей (Security Accounts Manager, SAM).

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях.

Действительно, вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер Comp1 под локальной учетной записью User1, будет отказано в доступе к принтеру, установленному на компьютере Comp2, поскольку в его локальной базе нет пользователя с именем Userl (рис).

- Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах, где работают пользователи и расположены ресурсы.

В ОС Windows XP Professional для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию).

В этом случае подключение к любому сетевому компьютеру осуществляется от имени его локальной гостевой учетной записи, которая включается с помощью Мастера настройки сети (по умолчанию она отключена) и для которой настраивается нужный уровень доступа.

Для ОС Windows XP Home Edition этот способ сетевого взаимодействия является основным и отключить его нельзя (поэтому компьютеры с данной ОС невозможно сделать участниками домена).

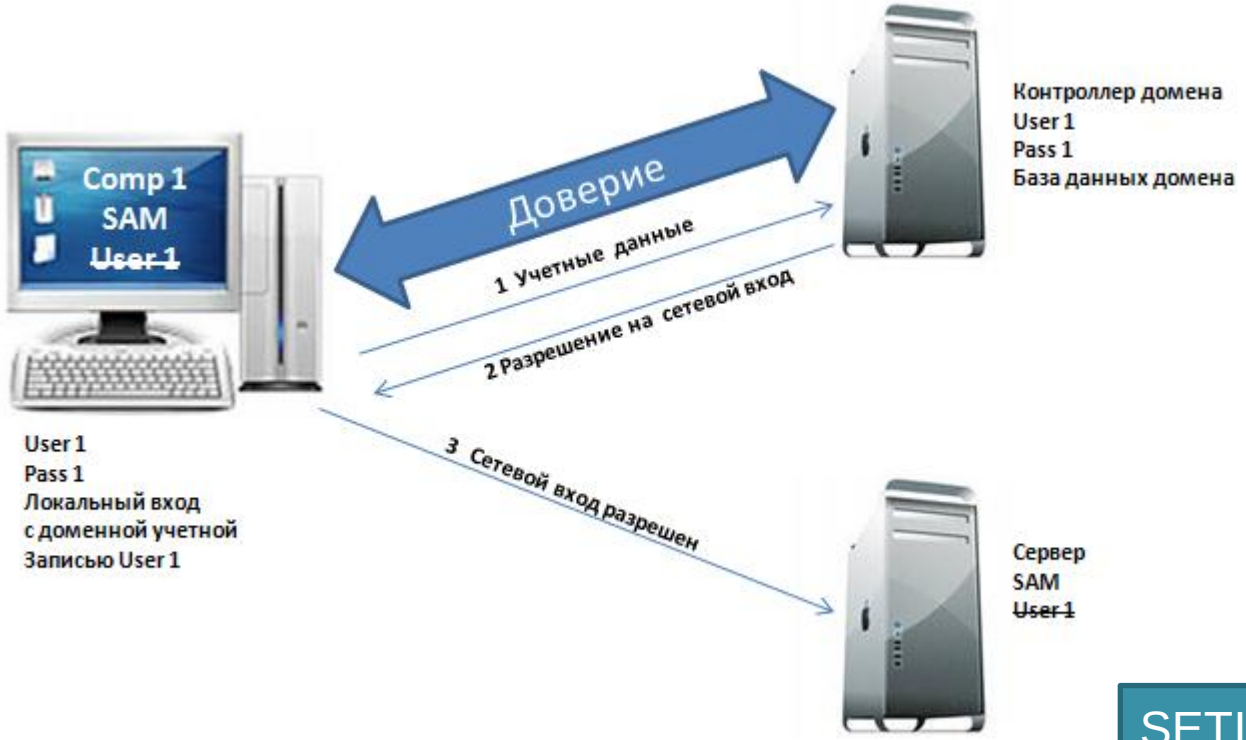
Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей. В крупных сетях следует применять **домены**.

Домен — это логическая группировка компьютеров, объединенных общей базой данных пользователей и компьютеров, политикой безопасности и управления.

Домены создаются на основе сетевых ОС Windows, а база данных, поддерживается контроллерами домена.

Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам/

Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем уже без проверки предоставлять ему доступ к ресурсам всех компьютеров домена.



Основные угрозы при работе в сети

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много.

- «взлом» компьютера обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;
- повреждение системы чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании — «Denial of Service») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда — даже всей сетевой инфраструктуры организации;

Основные меры безопасности при работе в сети

Их можно сформулировать в виде следующего набора правил:

- отключайте компьютер, когда вы им не пользуетесь. Как любят говорить эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;
- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые «уязвимости», снижающие защищенность вашего компьютера. Наличие уязвимостей нужно внимательно отслеживать (в том числе читая «компьютерную» прессу или информацию в Интернете), чтобы вовремя предпринимать меры для их устранения.

- кража данных из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет получить доступ к защищаемой, часто — конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;
- уничтожение данных имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из не¬проверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;
- без необходимости не предоставляйте ресурсы своего компьютера в общий доступ. Если же это все-таки потребовалось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;
- установите (или включите) на компьютере персональный межсетевой экран (брандмауэр). Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;

- даже если вы единственный владелец компьютера, для обычной работы применяйте пользовательскую учетную запись: в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

- Сложным считается пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например **jxglrg$N**. Разумеется, пароль не должен совпадать с именем вашей учетной записи. В операционных системах Windows сложный пароль можно сгенерировать автоматически, используя команду NET USER с ключом /RANDOM, например:

NET USER Имя_Пользователя /RANDOM

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем от-кройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку HTML;

- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа WebMoney, Яндекс-Деньги и т. д.

- Для организации работы в сетях Microsoft применяются две модели: рабочие группы, используемые при небольшом числе компьютеров, и домены, позволяющие легко объединять большое число пользователей, рабочих станций и серверов.
- Все сетевые ОС и хранящиеся на компьютерах данные должны быть надежно защищены, причем желательно, чтобы применяемая система безопасности была многоуровневой.