## Тема. 5.3 Безопасность работы в локальной сети.

Рассмотрим безопасность в локальной сети исходя из требований Национального стандарта согласно ГОСТу Р ИСО/МЭК 17799-2005. Для этого вводятся такие понятия как управление сетевыми ресурсами, средства контроля сетевых ресурсов, контроль сетевого доступа, политика в отношении использования сетевых служб.

**Управление сетевыми ресурсами**

Цель: обеспечение безопасности информации в сетях и защиты поддерживающей инфраструктуры.

**Средства контроля сетевых ресурсов**

Для обеспечения требуемого уровня безопасности компьютерных сетей и его поддержки требуется комплекс средств контроля. Руководители, отвечающие за поддержку сетевых ресурсов, должны обеспечивать внедрение средств контроля безопасности данных в сетях и защиту подключенных сервисов от неавторизованного доступа, В частности, необходимо рассматривать следующие меры и средства управления информационной безопасностью:

- следует распределять ответственность за поддержание сетевых ресурсов и компьютерных операций
- следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установленное у конечных пользователей;
- если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям, а также для защиты подключенных систем.

**Контроль сетевого доступа**

Цель: защита сетевых сервисов.

Доступ как к внутренним, так и к внешним сетевым сервисам должен быть контролируемым. Это необходимо для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, обеспечивая:

- соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;
- соответствующие механизмы аутентификации в отношении пользователей и оборудования;
- контроль доступа пользователей к информационным сервисам.

**Политика в отношении использования сетевых служб**

Несанкционированные подключения к сетевым службам могут нарушать информационную безопасность целой организации. Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы. Контроль доступа, в частности, является

необходимым для сетевых подключений к важным или критичным приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации вне сферы непосредственного управления и контроля безопасности со стороны организации.

Следует предусматривать меры безопасности в отношении использования сетей и сетевых сервисов.

При этом должны быть определены:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

Необходимо, чтобы эти меры согласовывались с требованиями в отношении контроля доступа.

Рассматривая работу в локальных сетях, необходимую для обеспечения безопасности в школе и дома, остановимся на вопросах основ безопасности при работе в сетях, принципах построения защищенных операционных систем (ОС), основных угрозах при работе в сети, основных мерах безопасности при работе в сети.

**Основы безопасности при работе в сетях.**

В современном информационном мире, когда все компьютеры объединенные в локальную сеть имеют доступ в Интернет, актуальным становятся вопросы защиты от взлома злоумышленниками.

Рассмотрим основные принципы построения защищенных операционных систем:

- все современные ОС являются *многопользовательскими* — они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;
- чтобы отличить одного пользователя от другого, применяются *учетные записи* (accounts) с уникальными *именами* и *паролями;*
- учетные записи различаются *уровнем полномочий (привилегий, прав)* — набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные,* обладающие максимальными привилегиями, и *пользовательские,* набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например форматировать разделы жесткого диска или менять настройки сети.

В различных версиях ОС Windows дополнительно существуют учетные записи с уровнем прав, средним между административным и

пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»).

Кроме того, существует два типа учетных записей — *локальные* из базы данных конкретного компьютера с ОС Windows, и *глобальные учетные записи в домене,* которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

- для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает не только непосредственный доступ, но и другие возможности работы с компьютером, например *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

В операционных системах Windows допускается также сетевой вход без указания имени и пароля *(анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях Microsoft;

- после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений,* т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой — только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

**Основные угрозы при работе в сети.**

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Мы приведем только основные из них:

- *«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;
- *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 по следствиями;
- *уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы — все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

**Основные меры безопасности при работе в сети.**

Меры безопасности при работе в сети довольно просты. 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.

***Рекомендации по защите компьютеров***

Для ОС Windows корпорацией Microsoft создан специальный веб-узел Windows Update, обратившись к которому (например, с помощью программы WUPDMGR.EXE или команды **Windows Update** или **Центр обновлений** в меню **Пуск),** нетрудно просмотреть и скачать список обновлений, рекомендуемых для вашего компьютера:

- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из непроверенных 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;
- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю (лучше — ежедневно или даже несколько раз в день);
- 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.

Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику — пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «Gfhjkm». Однако этот способ следует применять с осторожностью — взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования вашего компьютера и для входа, например, на игровой веб-сайт;

- 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 откройте. 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.;
- при проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии Secure Sockets Layer (SSL) — в этом случае адресная строка обязательно должна начинаться с «https://»;
- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать резервные копии системы и данных на съемном жестком диске или на DVD-RW — это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;
- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях — как в домашних, так и в корпоративных, — ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

Защита локальной сети и данных актуальна на всех уровнях

корпоративной инфраструктуры, т.к. затрагивает безопасность серверов и рабочих станций. Microsoft предлагает целостное решение по построению информационной системы, основанной на серверной платформе Windows Server 2008 R2 и рабочих станциях Windows Vista и Windows 7.

В систему защиты сети и данных от несанкционированного доступа входяты следующие технологии:

- Система управления доступом
- Система аудита
- Система аутентификации пользователей
- Аутентификация с использованием смарт-карт
- Политика на ограничение использования программ
- Служба управления правами
- Центр сертификации
- Встроенные средства шифрования
- Шифрующая файловая система EFS
- Поддержка протокола IPSec
- Безопасность беспроводных соединений
- Организация виртуальных частных сетей (VPN)

Для защиты компьютеров дома или в сети можно использовать брандмауэр.

*Брандмауэр* — это программное или аппаратное обеспечение, которое блокирует атаки хакеров и не позволяет вирусам и вирусам-червям попасть на компьютер через Интернет.

Если компьютер используется дома, включение брандмауэра — эффективный и важный этап его защиты. Если сеть развернута дома, необходимо защитить каждый входящий в нее компьютер. Для защиты сети служит аппаратный брандмауэр, например маршрутизатор. Кроме того, на каждом компьютере следует установить программный брандмауэр для блокировки распространения вируса в случае, если один из компьютеров все же будет заражен.

Если компьютер используется в сети школы или другой организации, то соблюдается политику, заданную администратором сети. Администраторы могут настраивать все компьютеры в сети так, что включить брандмауэр нельзя, пока они подключены к сети. В этом случае о необходимости включения брандмауэра на конкретном компьютере можно узнать у администратора сети.

Брандмауэр входит в состав большинства операционных систем Windows, начиная с Windows XP.