Тема 5.2 Установка паролей на ПК и папки. Меры безопасности при работе с электронной почтой.

Для разграничения доступа на одном компьютере современные операционные системы позволяют разграничивать доступ к информации и другим частям операционной системы (сервисы, программы и т.д.) с помощью учетных записей с задаваемыми правами доступа. На ОС по умолчанию представлены две учетные записи: администратор (полный доступ), гость (минимальный доступ). Также существует такое понятие как группы пользователей – это некий набор предустановленных прав, которые можно назначать пользователям. Для того чтобы однозначно авторизовать того или иного пользователя применяются пароли. Это может быть применимо для ограничения и контроля деятельности работы детей на домашнем компьютере.

С помощью этого же механизма также регламентируется доступ к файловой системе, в частности к папкам. Необходимым условием работы любого компьютера в сети является установка на нем персонального межсетевого экрана с функцией анализа активности программного обеспечения. По тому же принципу, но более сложными механизмами связанными с централизованным администрированием, реализуется разграничение прав доступа в доменной структуре учреждения, например школы.

Самым распространенным путем утечки информации является электронная почта. В настоящее время злоумышленники активно развивают методы социального инжиниринга, которые позволяют проникнуть даже на самый защищенный пользовательский компьютер.

Социальная инженерия – технология использования человеческого фактора для взлома информационной безопасности. Именно человек является наиболее слабым звеном в системах защиты. Один из приемов использования социальной инженерии – методика введения пользователя в заблуждение путем сообщения ему важных для него данных, оказывающихся на самом деле ложными.

Пример подобной методики - фишинг. Фишинг – вид онлайнового мошенничества, целью которого является получение идентификационных данных пользователей. Для этого рассылаются электронные письма от имени популярных брендов и вставляются в них ссылки на фальшивые сайты. Оказавшись на таком сайте, пользователи рискуют сообщить информацию конфенденциального характера.

Злоумышленники рассылают письма с троянскими программами, которые были спрятаны под фотографиями. Для заманивания пользователей на сайты-ловушки текст письма составляется так, чтобы у читающего не возникло сомнения в правдивости написанного.

Основой защиты от таких атак является, как ни странно, «обучение» пользователей. Необходимо информировать пользователей об этом виде угроз.

Для борьбы с фишинг-атаками используются средства контентной фильтрации, такие как системы контроля электронной почты, фильтры,

обеспечивающие фильтрацию сообщений Интернет-пейджеров. Антивирусная фильтрация и проверка на наличие шпионских программ позволяют значительно снизить уровень воздействия фишинг-атак на сеть. Целью многих подобных атак является установка на компьютере пользователя троянцев или программ-шпионов, дающая возможность злоумышленникам получить доступ к персональным данным пользователя.

Большинство клиентских почтовых программ использует протоколы POP3 и IMAP4 для подключения к пользовательскому почтовому ящику и считывания почты, и протокол SMTP — для отправки писем. Веб-доступ к почтовым ящикам осуществляется по протоколу HTTP.

Для обеспечения защиты при приеме и передаче почтовых сообщений рекомендуется использовать *протокол SSL (Secure Sockets Layer)*.

Программа Microsoft Outlook, например, для работы с почтовым сервером Exchange использует *протокол RPC,* включающий в себя встроенные механизмы обеспечения безопасности канала.

При работе с электронной почтой следует обязательно пользоваться современными антивирусными программами и, желательно, средствами защиты от нежелательной почты — *спама.*