Безопасность в интернете

Защита информации - это меры, направленные на то, чтобы не потерять информацию, не допустить ее искажения, а также не допустить, чтобы к ней получили доступ люди, не имеющие на это права.

В результате нужно обеспечить **доступность информации** - возможность получения информации за приемлемое время;

целостность (отсутствие искажений)информации;

конфиденциальность информации (недоступность для посторонних).

Средства защиты информации

Зависимость современных организаций от компьютерных технологий стала настолько сильной, что вывод из строя компьютерной сети или программного обеспечения может остановить работу предприятия. Чтобы этого не произошло, нужно соблюдать правила *информационной безопасности.*

Технические средства защиты информации	***Программные средства защиты информации***	***Организационные средства защиты информации***
Замки, решетки на окнах, системы сигнализации и видеонаблюдения, другие устройства, которые блокируют возможные каналы утечки информации или позволяют их обнаружить.	Обеспечивают доступ к данным по паролю, шифрование информации, удаление временных файлов, защиту от вредоносных программ и др.	Распределение помещений и прокладку линий связи таким образом, чтобы злоумышленнику было сложно до них добраться; политику безопасности организации.

Человек - слабое звено

Самое слабое звено любой системы защиты - это человек.

Некоторые пользователи могут записывать пароли на видном месте (чтобы не забыть) и передавать их другим, при этом возможность незаконного доступа к информации значительно возрастает.

Поэтому очень важно обучить пользователей основам информационной безопасности.

Опасность «инсайдеров»

Большинство утечек информации связано с «инсайдерами» (англ. inside - внутри) - недобросовестными сотрудниками, работающими в фирме.

Известны случаи утечки закрытой информации не через ответственных сотрудников, а через секретарей, уборщиц и другого вспомогательного персонала. Поэтому ни один человек не должен иметь возможности причинить непоправимый вред (в одиночку уничтожить, украсть или изменить данные, вывести из строя оборудование).

Цели злоумышленников

Если компьютер подключен к Интернету, появляются дополнительные угрозы безопасности. Атаку через сеть могут проводить злоумышленники и боты (программы-роботы), находящиеся в других городах и странах. Можно выделить три основные цели злоумышленников:

- *использование вашего компьютера* для взлома других компьютеров, атак на сайты, рассыл-ки спама, подбора паролей и т.п.;
- *кража секретной информации* - данных о банковских картах, имен и паролей для входа на почтовые сервера, в социальные сети, платежные системы;
- *мошенничество* - хищение чужого имущества путем обмана.

Вирусы и мошенничество

Первые две угрозы связаны, главным образом, с вредоносными программами: вирусами, червями и «троянцами», которые позволяют злоумышленнику управлять компьютером через сеть и получать с него данные.

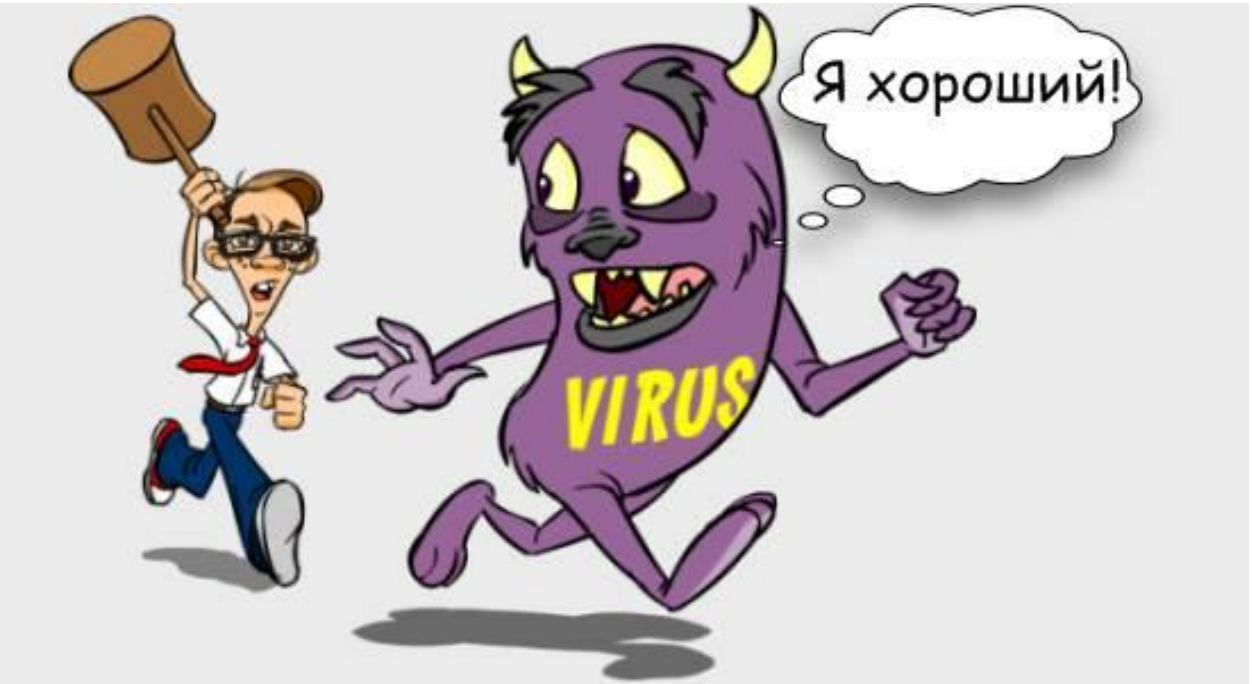
Мошенничество процветает потому, что многие пользователи Интернета очень доверчивы и неосторожны. Классический пример мошенничества - так называемые «нигерийские письма», приходящие по электронной почте. Пользователя от имени какого-то бывшего высокопоставленного лица просят принять участие в переводе крупных денежных сумм за границу, обещая выплачивать большие проценты. Если получатель соглашается, мошенники постепенно выманивают у него деньги.

Фишинг

Фишинг (англ. phishing, искажение слова fishing - рыбная ловля) - это выманивание паролей. Для этого чаще всего используются сообщения электронной почты, рассылаемые якобы от имени администраторов банков, платежных систем, почтовых служб, социальных сетей. В сообщении говорится, что ваш счёт (или учетная запись) заблокирован, и дается ссылка на сайт, который внешне выглядит как настоящий, но расположен по другому адресу (это можно проверить в адресной строке браузера). Неосторожный пользователь вводит своё кодовое имя и пароль, с по-мощью которых мошенник получает доступ к данным или банковскому счету.

Антивирусы и последние версии браузеров содержат специальные модули для обнаружения подозрительных сайтов («антифишинг») и предупреждают о заходе на такой сайт. Кроме того, нужно помнить, что администраторы сервисов никогда не просят пользователя сообщить свой пароль по электронной почте.

Вредоносные программы



Вредоносные программы, распространяющиеся через Интернет, представляю серьезную угрозу безопасности данных. Они мешают нормальной работе компьютера, перезаписывают, повреждают или удаляют данные,замедляют работу компьютера и вызывают другие неполадки.

Подобно действию вирусов, поражающих человека (от обычного гриппа до вируса Эбола), воздействие компьютерных вирусов также может быть различным: от раздражающего до разрушительного.

Правила безопасной работы в интернете

Нужно помнить, что многих проблем можно избежать, если

- работать в Интернете только из-под ограниченной учетной записи (без прав администратора).
- своевременно обновлять программное обеспечение;
- вовремя устанавливать «заплатки», связанные с безопасностью.
- чтобы ваши пароли не украли, лучше не запоминать их в браузере (иногда они хранятся в открытом виде и могут быть украдены троянской программой).
- заходя под своим именем в закрытую зону сайта с другого компьютера, нужно отмечать флажок «Чужой компьютер», иначе следующий человек, открывший эту страницу, сможет получить доступ к вашим данным.

Публичность информации

Нужно понимать, что размещая какую-то информацию в Интернете, вы делаете ее доступной для широкого круга лиц, включая работодателей, милицию, официальные органы и даже преступников. Возможны ситуации, когда эта информация (личные данные, фотографии, высказывания на форумах и в блогах) может быть использована против вас, даже если она находится в закрытом разделе сайта.

Шифрование информации

Для передачи информации, которую необходимо сохранить в тайне, лучше применять шифрование (например, упаковать данные в архив с паролем).

Наибольший уровень безопасности обеспечивается при денежных расчетах через Интернет: вместо протокола HTTP используют защищенный протокол **HTTPS** (англ. Hypertext Transfer Protocol Secure - безопасный HTTP), который предусматривает шифрование данных (например, с помощью алгоритма RSA). Поэтому нужно проверять, чтобы адрес на странице ввода пароля в таких системах начинался с «https : //», а не с «http: //».

Безопасность > неудобства

Забота о безопасности часто доставляет неудобства. Система с полностью отключенной безопасностью и антивирусом не досаждает пользователю ограничениями, вопросами и подтверждениями. Но за это неизбежно приходится расплачиваться сбоями, простоями и потерей данных в самый неподходящий для этого момент.

Время, потраченное на соблюдение простых правил безопасности, окупается всегда!