Безопасность в сети Интернет

Сегодня огромное количество информации обрабатывают с помощью персональных или рабочих компьютеров, поэтому атаки на компьютерные системы получили большую распространенность. С каждым годом число активных пользователей Интернета растет в геометрической прогрессии, следовательно проблема безопасности при работе в сети все более актуальна. К сожалению, знания пользователей о основах компьютерной безопасности при использовании Интернет отстают от темпов развития сети и лавинообразного роста угроз безопасности. Как программное обеспечение может представлять угрозу информационной безопасности в сети Интернет? К таким угрозам мы можем отнести:

- вредоносное программное обеспечение (вирусы), интернет-мошенничество;
- атаки на отказ в обслуживании;
- кражи денежных средств;
- кражи персональных данных;
- несанкционированный доступ к информационным ресурсам и систем;
- распространение заведомо недостоверной информации.

Кроме того, вам уже известны основные угрозы информационной безопасности пользователя Интернета, которые идут от авторизованных пользователей и электронных методов воздействия.

От авторизованных пользователей:

- Умышленные повреждения или похищения данных хакерами
- Повреждения данных в результате неосторожных действий

Электронные методы воздействия:

- Компьютерные вирусы
- Спам
- Фишинг

Рассмотрим влияние на безопасность со стороны различного вредоносного программного обеспечения, которое распространяется по сети Интернет.

Вредоносное программное обеспечение (англ. Malware, malicious software — вредоносная программа, вредоносное) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или к информационным ресурсам, которые хранятся на нем, предназначенное для несанкционированного владельцем их использования или причинение вреда (нанесение ущерба) владельцу компьютера, информации или компьютерной сети путем копирования, искажения данных, удаление или подмены информации. Термин «вредоносная программа» (malware — это сокращение от «malicious software») с трактовкой корпорации Microsoft обычно используется как общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и тому подобное. Вредоносные программы по виду нанесенного ущерба можно отнести к нескольким категориям.

Вредоносные программы:

- создают помехи в работе системы;
- уменьшают ресурсы компьютера;
- выполняют несанкционированные действия с данными;
- дестабилизируют работу пользователя с компьютером.

Препятствиями в работе зараженного компьютера могут быть различные вредоносные действия: начиная от открытия-закрытия лотка CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения; блокирование антивирусных сайтов, антивирусного программного обеспечения и административных функций операционной системы с целью усложнения их лечения; саботаж производственных процессов, управляемых компьютером (этим занимался известный червь Stuxnet).

Часто зараженный файл выполняет установку другого вредоносного программного обеспечения: загрузка из сети и распаковки другой, еще более вредоносной программы, либо вредоносный код уже содержится внутри файла

(dropper), часто вредоносное программное обеспечение занимает почти все ресурсы компьютера.

К несанкционированным действиям с данными относят: кражу, мошенничество, вымогательство и шпионаж за пользователем. Для кражи может применяться сканирование жесткого диска, регистрация нажатий клавиш (Keylogger) и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы; похищения данных, представляющих ценность или тайну; кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов, платежных систем). Аккаунты при этом применяются для рассылки спама, а через электронную почту можно заполучить пароли от других аккаунтов, в то время как виртуальное игровое имущество можно продать в MMOG (Massively multiplayer online game).

Вредоносное программное обеспечение вызывает блокировку компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств. Зачастую после оплаты компьютер либо не разблокируется, либо вскоре блокируется во второй раз. Вредоносная программа использует телефонный модуль для осуществления дорогостоящих звонков на платные номера, зарегистрированные злоумышленниками, что вызывает значительные суммы в телефонных счетах. Возможно также создание платного программного обеспечения, которое имитирует, например, антивирус, но ничего полезного при этом не делает (fraudware или scareware).

Вредоносные программы также выполняют другую незаконную деятельность: получение несанкционированного доступа к ресурсам самого компьютера или третьих ресурсов, доступных через него, в т.ч. прямое управление компьютером (так называемый backdoor), осуществляют организацию на компьютере открытых vpn-туннелей и общедоступных прокси-серверов. Зараженный компьютер (в составе ботнета) может быть использован для проведения DDoS-атак, сбор адресов электронной почты и распространение спама, в т.ч. в составе ботнета. К такой деятельности относится также накручивания электронных голосований, кликов по рекламным баннерам; генерирования монет платежной системы Bitcoin, и даже использование эффекта 25-го кадра для зомбирования человека.

- **Rootkit** (руткит, от англ. Root kit, то есть «набор root’а») программа или набор программ, предназначенный для скрытия следов присутствия злоумышленника или вредоносного программного обеспечения от посторонних глаз.
- **Ransomware** (от англ. Ransom — выкуп и software — программное обеспечение) — это вредоносное программное обеспечение, которое работает как вымогатель.
- **Ботнет** (англ. Botnet от robot и network) — это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, которая скрыто устанавливается на

компьютере жертвы и позволяет злоумышленнику выполнять определенные действия с использованием ресурсов зараженного компьютера.

Нежелательное программное обеспечение может записывать файлы, которые не являются истинно вредными, но в основном нежелательными: шутливое программное обеспечение, то есть которое делает какие-либо вещи, которые беспокоят пользователя. Например, программа Adware показывает рекламу, а программа Spyware посылает через сеть Интернет информацию, несанкционированную пользователем. Создается так называемое «отравления» документов, дестабилизирующее программное обеспечение, которое открывает их (например, архив размером менее мегабайта может содержать многие гигабайты данных, а при его распаковке может надолго «зависнуть» архиватор, или даже переполниться жесткий диск). Программы удаленного администрирования могут применяться как для того, чтобы дистанционно решать проблемы с компьютером, так и для вредоносных целей.

Иногда вредоносное программное обеспечение для собственного «жизнеобеспечения» устанавливает дополнительные утилиты: IRC-клиенты, программные маршрутизаторы, открытые библиотеки перехвата клавиатуры. Такое программное обеспечение не является вредным, но вместе с ним устанавливается более вредоносная программа, которая определяется антивирусами. Бывает даже, что вредоносен только скрипт из одной строки, а остальная часть программы вполне легитимна.

Классификация вредоносных программ по методу размножения:

- **эксплойт** — теоретически безвредный набор данных (например, графический файл или сетевой пакет), который некорректно воспринимается программой, которая работает с такими данными. Здесь вред наносит не один файл, а неадекватное поведение программного обеспечения с ошибкой. Также эксплойтами называют программы для генерирования так называемых «отравленных» данных;
- **логическая бомба** в программе срабатывает при определенном условии, является неотъемлемой от полезной программы-носителя;
- **троянская программа** не имеет собственного механизма размножения;
- **компьютерный вирус** размножается в пределах компьютера и через сменные диски. Размножение через локальную сеть возможно, если пользователь сам выложит зараженный файл в сеть. Вирусы одновременно делятся по типу файлов, которые заражаются (файловые, скриптовые, загрузочные), по способу прикрепления к файлам (паразитные, сопутствующие и перезаписывающие исходный файл) и т.д.;
- **сетевой червь** способен самостоятельно размножаться с сети. Делятся на IRC, почтовые, такие, которые размножаются с помощью эксплойтов и т.д.

Вредоносное программное обеспечение может образовывать цепочки: например, с помощью эксплойта на компьютере жертвы разворачивается загрузчик, который устанавливает из сети Интернет основное тело (программный код) червя.

Подробнее о программах, заражающих компьютер можно прочитать в статье

https://www.polnaja-jenciklopedija.ru/nauka-i-tehnika/kompyuternye-virusy.html

Угрозы здоровью пользователя Интернет

Чрезмерное, неконтролируемое и необдуманное использование Интернета может вызвать угрозы психическому здоровью пользователей.

Угрозы психическому здоровью пользователя интернета:

- информационная перегрузка от распространения информации с воздействием на психику;
- отчуждение от реальности.

Основной проблемой обеспечения психологической безопасности, в первую очередь психологического здоровья пользователей компьютерных и сетевых технологий, стала проблема информационной (когнитивной) перегрузки. Специфика гипертекстового формата представления информации привела к возникновению у пользователя Интернета особого психологического феномена, получившего название «проблема потери ориентации в гиперпространстве» (англ. Lost in hyperspace problem). Этот психологический феномен проявляется в том, что пользователь не может локализовать свое местонахождение в информационном пространстве веб-сайта, он постоянно возвращается к одним и тем же материалам, не понимает, куда ему надо обращаться за нужной информацией (даже если подозревает, что она существует где-то в исследуемом гипертекстовом пространстве), не знает, как вернуться к ранее просмотренным темам, забывает начальные мотивы своего поиска и содержание просмотренных веб-страниц и т.п. Потеря ориентации в гиперпространстве часто ведет к потере смысловых связей между просмотренными материалами, и почти всегда вызывает крайне поверхностное восприятие их содержания.

Второй, не менее существенной проблемой является бесконтрольное распространение в сети информации, которая может нанести психологическую травму или спровоцировать пользователя на совершение любых противоправных действий. Для решения этих проблем достаточно успешно ведутся работы по совершенствованию различных видов пользовательского интерфейса, а также по созданию приложений, способных фильтровать информационный поток по заданным наборам параметров.

У отдельных пользователей Интернета, которые тратят сеть много времени, наблюдается эффект отчуждения от социального окружения. Известны случаи, когда интенсивное применение Интернета приводит к сужению социальных

связей вплоть до одиночества, сокращение семейного общения и даже к развитию депрессивных состояний. Существуют и другие данные, свидетельствующие о негативном влиянии Интернета на индивидуальную и групповую психическую деятельность. Например, было доказано, что использование Интернета может способствовать аутизации детей и подростков, вести к нарушениям в процессах их социальной адаптации и тому подобное.

Специалисты-психологи отмечают сложные взаимоотношения человеческой психики с феноменом виртуальной реальности (англ. MUD — Multi-User Dimensions), о возможной связи виртуального мира с проблематикой измененных состояний сознания, неконтролируемой психологической зависимости от Интернета, которая приобретает болезненные формы. Психологическую опасность представляет захват ролевыми играми в Интернете, их возможной связи с асоциальным поведением, психологическая мотивация использования аватара как попытку изменить свою идентичность или создавать множественную сетевую идентичность и тому подобное.

Опасностей психологического влияния Интернета на человека можно избежать через самоконтроль времени работы в Интернете, развитие умения ставить цели, задачи и осуществлять предметный поиск сведений в Интернете. А проблемы, которые уже возникли из-за необдуманного использования Интернета, важно обсуждать с родителями и психологами.

Каких правил следует придерживаться при пользовании Интернетом?

Вам уже известны общие правила безопасного использования Интернета:

- перед подключением к Интернету необходимо проверить, включена ли антивирусная защита на компьютере пользователя, и обновить (если необходимо) версию защитного программного обеспечения;
- не рекомендуется активизировать гиперссылки, которые могут привести к загрузке на компьютер пользователя любых файлов;
- не рекомендуется устанавливать на компьютер пользователя программное обеспечение из неизвестным веб-сайтов;
- не следует активизировать баннеры (рекламного или развлекательного характера), которые размещены на незнакомых пользователю веб-сайтах;
- запрещается открывать файлы, приложенные к электронным почтовым отправлениям, адресант которых пользователю неизвестен;
- не рекомендуется делиться в Интернете любой личной информации;
- запрещается проводить любые финансовые операции через небезопасные веб-сайты (веб-сайты, которые не могут предъявить сертификаты установленного образца, обеспечивающих безопасность транзакций)
- используйте защищенные сайты, которые обычно требуют ввода имени пользователя и пароля. Пароль должен состоять не менее чем из восьми

символов, учитывая буквы и числа. И главное, паролем не должно быть что-то очевидное, какие-то простые слова или даты;

- не соглашаться на встречу с человеком, с которым познакомились через Интернет, не присылать свое фото интернет-знакомым, не давать незнакомым людям такую информацию, как полное имя, адрес, номер школы, расписание занятий или сведения о семье.