В специальном выпуске использованы материалы:

1. Жичкина А. Социально-психологические аспекты общения в Интернете. - М.: Дашков и Ко, 2004. - с.27
2. Искусство общения в Интернет, или сказкотерапия в действии // Мир ПК. - 1998. - с.121
3. http://help-antivirus.ru/drweb_classificator.php
4. http://www.stavropol.ru/srv/security.php
5. http://hq-wallpapers.ru/wallpapers/13/hq-wallpapers_ru_animals_61307_1280x1024.jpg
6. http://www.lenagold.ru/fon/clipart/sh/shar/zel.html
7. http://csmres.co.uk/cs.public.upd/article-images/shutterstock_42860701.jpg
8. http://review-tlt.ru/wp-content/uploads/2012/10/toliatti_news_08oct12-500x327.jpg
9. http://img1.liveinternet.ru/images/attach/c/3/77/383/77383227_4278666_89473280.jpg

Автор: Кирисюк Е.В.

Наши координаты:
Адрес: г. Белгород, ул. Щорса, д. 11, МБОУ СОШ № 28
school28@beluo.ru

МБОУ СОШ № 28 г. Белгорода

Специальный выпуск СМИ МБОУ СОШ № 28

Защита от вредоносных программ

Правильное поведение в сети

Фильтры

2013 г.

Опасности в сети Интернет

Основными реальными угрозами при работе в Интернет, в порядке убывания их возможности, являются:

1. Зависание Вашего компьютера при работе в Интернет.
2. Несанкционированный удаленный доступ к информации на Вашем компьютере.
3. Искажение или разрушение данных и программ на Вашем компьютере.

Признаки заражения компьютера:

1. Вывод на экран непредусмотренных сообщений или изображений.
2. Подача непредусмотренных звуковых сигналов.
3. Неожиданное открытие и закрытие лотка CD\DVD дисковода.
4. Произвольный запуск на компьютере каких-либо программ. Частые зависания и сбои в работе компьютера.
5. Медленная работа компьютера при запуске программ.
6. Исчезновение или изменение файлов и папок.
7. Зависание или неожиданное поведение браузера (например, окно программы невозможно закрыть).

1. **Троян** - это программа, которая предоставляет посторонним доступ к компьютеру для совершения каких-либо действий без предупреждения самого владельца компьютера, либо высылает по определенному адресу собранную информацию.
Часто троян называют вирусом. Это не совсем так. В отличие от вирусов, трояны направлены на получение конфиденциальной информации и доступ к определенным ресурсам компьютера.
Возможны различные пути проникновения трояна в вашу систему. Чаще всего это происходит при запуске какой-либо полезной программы, в которую внедрен сервер трояна.
В момент первого запуска сервер копирует себя в какую-нибудь директорию, прописывает себя на запуск в системном реестре, и даже если программа-носитель никогда больше не запустится, система уже заражена трояном. Обычно это происходит, если программы скачиваются не с официальных серверов програам, а с личных страничек.

2. **Вирус** - это программа, которая может проникнуть в компьютер различными путями и вызвать эффекты, начиная от просто раздражающих до очень разрушительных. Вирусы могут проникать в компьютеры через электронную почту, Интернет, с дисков и т.д. Они способны размножаться, заражая другие файлы и программы.
Компьютерные вирусы названы вирусами из-за их сходства с биологическими вирусами.
Также как биологические вирусы проникают в тело и инфицируют клетки, компьютерные вирусы попадают в компьютеры и заражают файлы. Оба типа вирусов могут репродуцировать себя и распространяться путем передачи инфекции от одной зараженной системы к другой. Биологический вирус является микроорганизмом, аналогично и компьютерный вирус является микропрограммой.

3. **Червь** - это программа, очень похожая на вирус. Он способен к самовоспроизведению и может привести к негативным последствиям для Вашей системы. Однако для размножения червям не требуется заражать другие файлы.
Это тип вредоносных или как их еще называют - злоумышленных программ. Компьютерный червь похож на вирус, потому что он попадает в компьютер, прикрепленный к файлу. Но в отличие от вируса, червь имеет свойство воспроизводить себя в вашем компьютере, не требуя каких-либо действий пользователей. Еще одной особенностью компьютерного червя является то, что он распространяется не только по всему вашему компьютеру, но и автоматически рассылает свои копии по электронной почте.
Так же следует понимать, что чем больше червь находится в системе компьютера, тем больше вреда и разрушения он приносит. Черви, в отличие от вирусов, просто копируют себя, повреждая файлы, но репроду-цирование может происходить очень быстро, система перенагружается, что нередко приводит к ее полной неработоспособности.

Хакеры

Хакерами называют тех, кто получает или пытается получить незаконный доступ к данным через компьютерные сети (сейчас обычно через интернет). Нередко они атакуют не защищенные (или слабо защищенные) от вторжения домашние компьютеры, подключенные к интернету. Атака может исходить и изнутри - от программы-шпиона, проникшей на компьютер, например, в качестве вложения в спамерское письмо.

Хакеры бывают разные. Наиболее многочисленны, но наименее опасны хакеры-любители. На их долю приходится до 80% всех компьютерных атак. Но этих людей интересует не некая цель, а сам процесс атаки. Они испытывают удовольствие от преодоления систем защиты. Чаще всего их действия удается легко пресечь, поскольку хакеры-любители предпочитают не рисковать и не вступать в конфликт с законом.

Более опасны "хакеры-изменники", которые выдают себя за лояльных сотрудников организации. На их долю приходится примерно 3-5% компьютерных атак. "Изменники" обычно идут на совершение подобных преступлений, побуждаемые какой-то обидой или из банального материального расчета. "Изменники" обычно похищают или продают право доступа к ценной информации (номера кредитных карточек, базы данных и т.д.) или ограничиваются актами вандализма.

Примерно 10-15% компьютерных атак совершают члены организованных преступных сообществ - "хакеры - мафиози". Единственная цель этих хакеров - получение прибыли. Поэтому, их мишенью становятся финансовые организации, банки.

Спам

Спам (англ. spam) - массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать.

Виды спама:
- "Письма счастья"
- Распространение политической пропаганды.
- Массовая рассылка для вывода почтовой системы из строя (DoS-атака).
- Массовая рассылка от имени другого лица, для того чтобы вызвать к нему негативное отношение.
- Массовая рассылка писем, содержащих компьютерные вирусы (для их начального распространения).
- Рассылка писем, содержащих душещипательную историю.

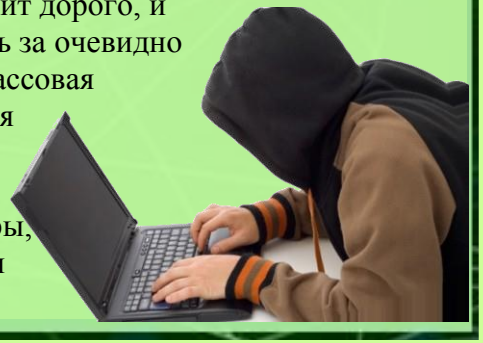
"Письма счастья". Целью такой рассылки является сбор e-mail адресов: после многочисленных пересылок «всем знакомым» в тексте такого письма часто содержатся e-mail адреса всех, кому оно было переслано ранее. А в числе очередных адресатов вполне может оказаться и инициировавший её спамер.

Спамеры собирают e-mail адреса с помощью специального робота или вручную (редко), используя веб-страницы, конференции Usenet, списки рассылки, электронные доски объявлений, гостевые книги, чаты… Некоторые компании занимаются только сбором адресов, а базы потом продают. Некоторые компании продают спамерам e-mail адреса своих клиентов, заказавших у них товары или услуги по электронной почте.

Для рассылки спама используются подключённые к Интернету плохо защищённые или неправильно настроенные компьютеры.

Огромное количество "спамовых" сообщений наносит очевидный вред получателям. В первую очередь речь идёт о времени, потраченном впустую на отсеивание ненужной почты и выискивании среди неё отдельных нужных писем.

Очень часто интернет-трафик стоит дорого, и пользователю приходится платить за очевидно ненужные письма. Кроме того, массовая рассылка спама способна на время полностью блокировать работу не только одного персонального компьютера, но и крупные серверы, обслуживающие абонентов в сети Интернет.



Поведение в сети Интернет

Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования сетью Интернет не установлено. Существуют, однако, общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей.

Законы

В Российской Федерации существует ряд законов в информационной сфере.

1. Закон «О правовой охране программ для ЭВМ и баз данных» регламентирует юридические вопросы, связанные с авторскими правами на программные продукты и базы данных.

2. Закон «Об информации, информатизации и защите информации» позволяет защищать информационные ресурсы (личные и общественные) от искажения, порчи, уничтожения.

3. В Уголовном кодексе РФ имеется раздел «Преступления в сфере компьютерной информации». Он предусматривает наказания за:
   - неправомерный доступ к компьютерной информации;
   - создание, использование и распространение вредоносных программ для ЭВМ;
   - умышленное нарушение правил эксплуатации ЭВМ и их сетей.

Правила поведения в сети Интернет

Пользователям запрещается:

1. Передавать по сети информацию, оскорбляющую честь и достоинство других абонентов сети, содержащую призывы к насилию, свержению существующего строя, разжиганию межнациональной розни а также передавать информацию, которая по закону не подлежит разглашению.

2. Разрабатывать и распространять любые типы вирусов.

3. Вести деятельность, противоречащую национальным интересам России, заниматься в Сети или посредством Сети любой деятельностью, запрещенной законодательством РФ.

4. Производить действия, запрещенные положением статей УК РФ в части преступлений в сфере компьютерной информации, запрещения распространения порнографии, национальной дискриминации и призывов к насилию.

5. Наносить ущерб работоспособности Сети, совершать действия, которые могут повлечь за собой нарушение функционирования Сети, создавать помехи работе других Пользователей, искажать или уничтожать информацию, на компьютерах других пользователей.

6. Заниматься хакерством, т.е. получать (или пытаться получить) несанкционированный доступ к чужой информации и любым ресурсам Сети.

Безопасность работы в сети Интернет

Особенности общения в сети Интернет

Все формы Интернет-общения, в связи с его опосредованностью компьютером, обладают некоторыми особенностями.

1. Анонимность. Несмотря на то, что иногда есть возможность получить некоторые сведения анкетного характера и даже фотографию виртуального собеседника, этого недостаточно для реального и более-менее адекватного восприятия личности. Кроме того, при виртуальном общении наблюдается скрывание или презентация ложных сведений о себе. Вследствие подобной анонимности и безнаказанности в Сети проявляется и другая особенность, связанная со снижением психологического и социального риска в процессе общения - аффективная раскрепощенность, ненормативность и некоторая безответственность участников общения. Человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до оскорблений, нецензурных выражений, сексуальных домогательств), так как риск разоблачения и личной отрицательной оценки окружающими минимален.

2. Добровольность и желательность контактов - пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент.

3. Затрудненность эмоционального общения и, в то же время, стойкое стремление к эмоциональному наполнению текста, которое выражается в создании специальных значков для обозначения эмоций (смайлов).

4. Стремление к нетипичному, ненормативному поведению. Зачастую пользователи Интернета представляют себя с иной стороны, чем в условиях реальной жизни, проигрывают нереализуемые ими в реальности роли и сценарии поведения.

Другое важное следствие интернет-общения - это возможность создавать о себе любое впечатление по своему выбору. В сети Интернет люди часто создают себе «виртуальные личности». Виртуальная личность наделяется именем, часто псевдонимом (который еще называют - «ник»). Конструирование виртуальных личностей в Интернете нередко связано с недостатками или невозможностью реализации человеком себя в реальной жизни.

Интернет-зависимость

Виртуальное общение может иметь замещающий характер, это происходит в случае формирования Интернет-зависимости. Такая зависимость проявляется в том, что люди настолько предпочитают жизнь в Интернете, что фактически начинают отказываться от своей реальной жизни, проводя до 18 часов в день в виртуальной реальности. Интернет-зависимые получают в Интернете различные формы социального признания. Их зависимость может говорить о том, что в реальной жизни социального признания они не получают, а также о том, что в реальной жизни у этой группы людей могут существовать определенные трудности в общении, которые снижают их удовлетворенность реальным общением.

В целом можно сказать, что основными причинами обращения к Интернету, как инструменту общения может быть:

- достаточное насыщение общением в реальных контактах, в подобных случаях пользователи быстро теряют интерес к Интернет-общению, если появляются новые возможности для удовлетворения соответствующих потребностей в реальной жизни;
- возможность реализации качеств личности, проигрывания ролей, переживания эмоций, по тем или иным причинам недоступным им в реальной жизни, что иногда приводит человека к подмене своей реальной личности выдуманным "Я", становится настолько привычным и необходимым, что вызывает стойкую интернет-зависимость.

Последнее - наиболее опасная особенность общения в Интернете, способная перерасти в психические отклонения и, таким образом, нанести серьезный вред здоровью человека.

Советы по безопасному поведению в сети

1. Не запускайте у себя на компьютере программы из ненадежных источников и не открывайте приложения к письмам. Сначала сохраните это приложение в файл и проверьте его антивирусной программой.

2. Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. Чтобы не получать письма от этого адресата впредь, нужно написать жалобу администратору сети, откуда прислано это письмо.

3. Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам - назойливые рекламные письма - и письмо попало в Ваш ящик не по ошибке, а специально.

4. Обязательно установите на ВСЕ компьютеры антивирусную программу для защиты от троянов и вирусов в режиме резидентного монитора (тогда она будет проверять все запускаемые программы и открываемые документы автоматически).

5. Ограничьте доступ к Вашему компьютеру с помощью программ управления доступом (их можно посмотреть на сайте www.listsoft.ru) и введите установки безопасности (запрос пароля BIOSом при включении компьютера).

6. Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте (не на жестком диске Вашего компьютера).

7. Для повышения безопасности следует установить на компьютере персональный пакетный фильтр - программу, которая поможет защитить Ваш компьютер от несанкционированного доступа злоумышленников к нему через Интернет путем блокирования некоторых принимаемых и передаваемых пакетов.

8. Не думайте, что вирусы и трояны могут находиться только в программах, загруженных из Интернета - как показывает печальный опыт покупателей пиратских CD, на них все чаще появляются программы, также зараженные вирусами или троянскими конями.

9. Надеемся, что, воспользовавшись этими советами, Вы сможете эффективно противостоять «атакам» на Ваш компьютер и впредь строить свои отношения с интернетом только в рамках дружественного общения с приятным виртуальным собеседником.

10. Чтобы нежелательные посетители не могли проникнуть в Ваш компьютер через Интернет, установите брандмауэр это средство защиты, которое отслеживает и ограничивает обмен данными между компьютером и сетью или Интернетом.