Информационная безопасность. Интернет как средство коммуникации. Кибербуллинг.

01

Что такое интернет?

Интернет – это мировая компьютерная сеть, объединяющая сотни тысяч локальных государственных, корпоративных, общественных, образовательных и домашних сетей на основе стандартных соглашений о способах обмена информацией и единой единой системы адресации.

Интернет используется как:

- Среда для реализации бизнес-технологий.
- Среда для образования.
- Среда для работы СМИ.
- Среда для обработки и хранения информации.
- Среда для образования.

Интернет как коммуникативное пространство.

Создание интернета повлияло на коммуникацию. Общение в виртуальной среде происходит с помощью своеобразного дискурса, сформировавшегося в компьютерных сетях.

Интернет-коммуникации – это такие методы общения, при которых передача информации происходит по каналам Интернета с использованием стандартных протоколов обмена и представления информации в различной форме: голос, видео, документы, мгновенные сообщения, файлы.

Типы коммуникационных ресурсов интернета:

- Электронная почта
- Дискуссионные группы или форумы
- Веб-конференции
- Чаты
- Блоги
- Социальные сети

Виды онлайн-агрессии:

- Кибербуллинг
- Троллинг - Форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.
- Хейтинг - Негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.
- Флэйминг - это бесцельная дискуссия в чате, личной переписке или комментариях, сопровождающаяся негативными эмоциями. Как и любой конфликт, флейминг порой приводит стороны к использованию недопустимых техник словесной атаки, в первую очередь грубых: оскорбления и угрозы. К одной или обеим из сторон конфликта может спонтанно подключаться большое количество людей.
- Кибersталкинг - Использование Интернета для преследования или домогательств человека, группы людей или организации.
- Грифинг - акт нанесения морального или материального ущерба людям в компьютерных играх.
- Сэкстинг - Пересылка личных фотографий, сообщений интимного содержания посредством современных средств связи

02
Что такое кибербуллинг?

Кибербуллинг – это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала.

Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия.

Для того чтобы скомпрометировать человека могут создаваться страницы, копирующие его личную информацию, для дальнейшего оскорбления якобы от его лица. С этой же целью может подбираться пароль к реальной странице человека. При неблагоприятном завершении отношений в качестве мести другим партнером могут быть опубликованы в сети интимные фотографии, банковские счета или разглашение любой другой личной информации.

Жертвы кибербуллинга обычно более уязвимы, чем те, кто подвергается непосредственным нападкам. Нет защиты в виде прекращения учебного дня – в личную жизнь могут вмешиваться постоянно, в любое время суток и по всевозможным источникам. Спрятаться дома не получится, точно так же, как и попросить защиты у старших или руководящих – регламент общения онлайн не подразумевает вмешательства других людей.

Еще одна особенность, делающая кибербуллинг более мощным оружием, чем нападки в реальной жизни – это скорость распространения информации. В интернете информация распространяется в секунды, и компрометирующее видео может быть просмотрено всеми общими знакомыми и сотней посторонних людей в течение десяти минут после съемки. Кроме того ширина задействованной аудитории при использовании не личных сообщений достигает колоссальных размеров. Все файлы хранятся в сети и могут быть вновь подняты даже после того, как первая волна улеглась.

Кибербуллинг в социальных сетях не заметен для взрослых, а сами дети не спешат сознаваться в подобном и просить помощи. Понять, что происходит можно по косвенным признакам, таким как закрытость, уход человека в мирфантазийили компьютерных игр. В процессе постоянно действующих стрессовых факторов нарушается сон, снижается настроение, могут появляться различные боли, ухудшиться общее состояние здоровья. Поскольку в школьном возрасте кибербуллинг часто производится одноклассниками, то это может отражаться на посещаемости школы, а также успеваемости, могут пропадать личные вещи. Кроме этого, интернет-травля может сочетаться с непосредственным буллингом, тогда возможны ссадины и синяки от побоев.

Кибербуллинг в социальных сетях не заметен для взрослых, а сами дети не спешат сознаваться в подобном и просить помощи. Понять, что происходит можно по косвенным признакам, таким как закрытость, уход человека в мирфантазийили компьютерных игр. В процессе постоянно действующих стрессовых факторов нарушается сон, снижается настроение, могут появляться различные боли, ухудшиться общее состояние здоровья. Поскольку в школьном возрасте кибербуллинг часто производится одноклассниками, то это может отражаться на посещаемости школы, а также успеваемости, могут пропадать личные вещи. Кроме этого, интернет-травля может сочетаться с непосредственным буллингом, тогда возможны ссадины и синяки от побоев.

Вычислить обидчика также трудно, ведь он может не обладать физической силой или авторитетом среди остальных сверстников, чтобы испортить кому-то жизнь, особенно если действия совершаются анонимно.

Как бороться с кибербуллингом?

- Важно помнить о том, что кибербуллинг, как и прямое психологическое насилие являются уголовно наказуемыми, и, несмотря на анонимность, трафики, история браузера и подобные вещи, предоставляемые интернет-компанией, при нанесении реального ущерба, довольно легко помогут установить реальную личность агрессора.
- При фактах угроз, преследований, шантажа и прочих вариантах необходимо сохранять страницу с данными сообщениями или материалами, чтобы остались доказательства. Единичные негативные акты, особенно от незнакомых, оптимально игнорировать – буллер не станет ввязываться в дальнейшее общение.
- Никогда не стоит следовать требованиям агрессора, вступать в переговоры или пытаться откупиться.
- Когда атаки продолжаются, несмотря на блокировку (агрессор может писать с других страниц и адресов) или имеют прямые угрозы, то необходимо обращаться в правоохранительные органы, с фактами, подтверждающими факт угроз. Обращения в милицию заслуживают и случаи порнографического и интимного террора.
- Родителям стоит уделять больше внимания качеству отношений с ребенком, чтобы тот мог в любой момент посоветоваться относительно того, что отвечать обидчику. За то время, пока берется пауза на ответ можно и самому успокоиться и вместе с взрослым придумать такой вариант, который не только не удовлетворит агрессора, но и выставит его в смешном ракурсе.

03

Информационная безопасность.

Информационная безопасность – меры по защите информационной среды общества и человека.

Цели информационной безопасности:

- защита национальных интересов;
- обеспечение человека и общества достоверной и полной информацией
- правовая защита человека и общества при получении, распространении и использовании информации.

Объекты обеспечения информационной безопасности:

- информационные ресурсы;
- система создания, распространения и использования информационных ресурсов;
- информационная инфраструктура общества (информационные коммуникации, сети связи, центры анализа и обработки данных, системы и средства защиты информации);
- средства массовой информации;
- права человека и государства на получение, распространение и использование информации
- защита интеллектуальной собственности и конфиденциальной информации.

Источники информационных угроз.

Внешние:
- Политика стран
- Информационная война
- Преступная деятельность
- Прочие источники

Внутренние:
- Отставание по уровню информатизации
- Отставание по технологиям
- Недостаточный уровень образования
- Прочие источники

Виды информационных угроз.

Преднамеренные:

- Хищение информации
- Компьютерные вирусы
- Физическое воздействие на аппаратуру

Случайные:

- Ошибки пользователей
- Ошибки профессионалов
- Отказы и сбои аппаратуры
- Форс-мажорные обстоятельства

Компьютерный вирус – это программа, написанная программистом, способная к саморазмножению и выполнению разных вредоносных действий.

Вирусы по величине вредного воздействия

- Неопасные
- Опасные
- Очень опасные

Вирусы по среде обитания:

- Файловые
- Макровирусы
- Сетевые
- Загрузочные

Антивирусная программа (антивирус) — любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Методы защиты информации. При разработке методов защиты информации в информационной среде следует учесть следующие важные факторы и условия:

- расширение областей использования компьютеров и увеличение темпа роста компьютерного парка
- высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования
- расширение доступа пользователя к мировым информационным ресурсам
- усложнение программного обеспечения вычислительного процесса на компьютере.
- ограничение доступа к информации
- шифрование информации
- контроль доступа к аппаратуре
- законодательные меры.

Спасибо за внимание!