Проблемы информационной безопасности подростков

Почему дети и подростки оказываются наиболее уязвимыми пользователями Интернета?

Во-первых, именно дети и подростки, психика которых не до конца сформирована, склонны попадать в интернет - зависимость. Исследования показывают, что среди молодежи интернет-зависимых больше, чем среди людей зрелых.

Во-вторых, когда ребенок проводит в обществе компьютера большую часть жизни, его личность оказывается совершенно неадаптированной к реальности. Маленький человек испытывает трудности в общении со сверстниками, и постепенно уходит из социума, из реальной среды обитания в виртуальную.

Дети и подростки должным образом не владеют собой, не имея волевой регуляции, легко поддаются влиянию им непросто отличать хорошее от плохого, у них не сформированы адекватные схемы поведения и восприятия. Они активно исследуют жизнь, в том числе при помощи Интернета. Все эти особенности – подверженность и чувствительность к внешним стимулам, информации, эффекту новизны – используют веб-дизайнеры сайтов, размещая красочные призывы щелкнуть по той или иной ссылке на странице сайта.

Ожидать того, что в нерегулируемом Интернете ребенок станет скачивать рефераты по истории и при этом совсем не поинтересуется порнографией, наркотиками или рецептами по изготовлению взрывчатки, было бы весьма наивно. Именно негативная, «темная» сторона Всемирной паутины привлекает молодежь. Само по себе это не удивительно: запретный плод сладок. Но именно в Интернете запретный плод еще и доступен. И хотя доступность и дешевизну информации относят к положительным сторонам Интернета, очевидно, что эти особенности Сети имеют негативную сторону.

Под контентными интернет-угрозами понимается информация в Интернете, которая причиняет вред пользователю путем опубликования или пересылки, а также интернет-коммуникация, направленная на причинение вреда собеседнику. Технические и коммуникационные возможности интернет-технологий довольно широки, поэтому список контентных интернет-угроз достаточно разнообразен.

Наиболее типичной и массовой интернет-угрозой для детей и подростков в настоящее время является ***киберунижение и кибертравля*** – именно данная категория лидирует среди обращений на «линию помощи» Центра безопасного Интернета в России.

Иллюзия анонимности и безнаказанности приводит к тому, что некоторые пользователи дают выход агрессии в Интернете, оскорбляя других пользователей или провоцируя их на конфликт. Подобное поведение в Интернете называют «троллингом».

Тро́ллинг (разг. троллить) – вид виртуального общения, в котором один из участников – тролль – нагнетает гнев, конфликт, скрыто или явно задирая, принижая, оскорбляя другого участника или участников. Тролли публикуют провокационные сообщения, чтобы вызвать негативную реакцию пользователей и разжечь спор между участниками коммуникации. Троллинг может быть прямым (оскорбления участников, нарушение правил ресурса, подстрекание, ссоры) и замаскированным (сообщения не по теме, возвращение к другой острой теме, завуалированные сообщения, на первый взгляд позитивные). Тролли хотят получить реакцию в виде прямого конфликта. В перепалке с таким пользователем очень легко потерять над собой контроль и самому стать троллем.

Тролли могут стремиться вызвать раздражение участников коммуникации, но также их целью может быть унижение конкретного человека. В таком случае троллинг может переходить в целенаправленную травлю, или буллинг.

Под ***буллингом*** обычно понимается запугивание, унижение, травля, физический или психологический террор, направленный на то, чтобы вызвать у другого страх, запугать и тем самым подчинить человека себе. Во все времена это была одна из серьезных проблем подростковой среды.

Развитие инфокоммуникационных технологий привело к распространению ***кибербуллинга*** – агрессивного, умышленного действия, совершаемого группой лиц или одним лицом с использованием электронных форм контакта, повторяющегося неоднократно и продолжительное время в отношении жертвы, которой трудно защитить себя. Виртуальная среда, в которой происходит кибербуллинг, позволяет агрессорам чувствовать себя менее уязвимыми и менее ответственными за свои действия. Анонимность –основной фактор, отличающий кибербуллинг от обычного буллинга, осуществляемого в непосредственном контакте. Другие отличия проявляются в том, что кибербуллинг продолжается и вне организации, посещаемой ребёнком, более агрессивно и скрытно, что зачастую не позволяет родителям и педагогам своевременно видеть эмоциональные реакции жертвы.

Троллинг и кибербуллинг преимущественно встречаются в социальных сетях, на форумах и в чатах. Для кибертравли используются также электронная почта и онлайн-мессенджеры (например, ICQ, Wiper). Опасность распространения унижающей ребенка информации заключается в том, что в отличие от «обычного» унижения, сцены, изображающие сам процесс унижения, распространяются на неограниченный круг лиц. Такие видео или фото могут быть доступны будущим друзьям и знакомым даже в случае переезда ребенка в другой город.

Еще одна опасность заключается в том, что на данный момент удалить все экземпляры унижающих текстов или изображений из Интернета почти невозможно – ничто не мешает кому-то сохранить их на своем компьютере и опубликовать в Сети повторно даже через несколько лет.

Второй по массовости интернет-угрозой является вовлечение ребенка

в сексуальные действия через Интернет.

Секстинг и груминг распространены в России более широко, чем съемки детской порнографии.

Секстинг (от англ. sex и texting) означает общение на тему секса посредством мобильного телефона или через Интернет.

Груминг – установление в Интернете дружеских отношений с ребенком с целью сексуальной эксплуатации.

Суть угрозы заключается в том, что с ребенком в Интернете выходит на контакт некий человек (нередко представляющийся сверстником), входит в доверие к ребенку, в ряде случаев при этом готовя его к сексуальным действиям путем соответствующих бесед или пересылки сексуально ориентированных материалов. Цель – реальная встреча для совершения сексуальных действий или через Интернет посредством веб-камеры, либо обменом откровенных фотографий. Наиболее популярным местом для «охоты» за детьми являются социальные сети; дальнейшие контакты могут осуществляться через онлайн-мессенджеры, электронную почту, приватный чат, а также по мобильному телефону.

Беседы о сексе с малознакомыми «френдами» из социальных сетей могут таить в себе немалую опасность.

Не менее актуальной угрозой, исходящей из Интернета, является вовлечение несовершеннолетних в преступные ***экстремистские и радикальные группировки***.

Экстремизм (от лат. extremus – крайний) – приверженность к крайним мерам и действиям в политике, совокупность идей, намерений, оправдывающих при принятии решений крайние меры.

Девизы экстремистов: «Кто не с нами – тот против нас», «Гильотина –лучшее лекарство от перхоти» – предполагают отказ от таких инструментов общения, как диалог, переговоры, компромиссы, которые называются «пустой болтовней». «Нормальным» считается конфликтное, агрессивное навязывание собственной точки зрения.

Онлайн-рекрутинг начинается с безобидного действа: сторонники или противники – не важно, втягиваются в дискуссию. Это дает экстремистам возможность обозначить свою позицию и тактику и заинтересовать аудиторию. После многоэтапных вербовочных бесед потенциальному рекруту делается предложение об участии. Если рекрут не уверен в своем желании вступить в группу, его направляют в чаты для «дозревания» или отсева.

Рекрутам предоставляются специальные игры, где они привыкают к насилию, как единственному способу решения жизненных проблем.

Главная идея «Большой игры» – проведение диверсий против власти в России. Это целая интернет-индустрия.

ПОДРОСТКОВЫЙ ВОЗРАСТ В ПЛАНАХ ТЕРРОРИСТОВ

Террористические организации очень заинтересованы в постоянном пополнении своих рядов. Чтобы привлечь новых членов в свои банды, террористы используют специальные приемы вербовки, опираются на ряд психологических особенностей людей. Большой интерес для террористов представляет подростковый и юношеский возраст. Людей более старшего возраста привлечь к участию в террористической деятельности сложнее: их труднее обмануть, они склонны тщательно продумывать свои действия, у них сформировано чувство ответственности за своих близких и свой народ.

Набирающей масштабы интернет-угрозой является использование интернет-технологий для пропаганды и популяризации потребления ***наркотиков среди молодежи***. На соответствующих интернет-ресурсах (сайты бесплатного хостинга, профильные форумы, реже – сообщества в социальных сетях) подросткам предлагаются рецепты изготовления одурманивающих веществ и смесей из подручных материалов, а также предоставляется возможность приобретения подобных средств. Опасность заключается в использовании Интернета для наркотизации подрастающего поколения (средним возрастом начала потребления наркотиков в России считается 13 лет).

Здесь уместно напомнить родителям и педагогам о проявлении такого понятия, как бдительность. ***Бдительность*** *– это внимательное отношение человека к окружающей действительности. Наблюдение за подростками может рассказать о многом.*

Особую опасность для детей и подростков представляют ролевые компьютерные игры, которые приводят к психологической зависимости от компьютера и Интернета.

Ролевые компьютерные игры – это игры, в которых ребенок принимает на себя роль компьютерного персонажа. Игра разработана таким образом, что обязывает ребенка выступать в роли конкретного или воображаемого компьютерного героя. Обычно игрок добивается победы, выполняя задания (квесты), и растет в способностях и статусе. Когда «герой» набирает определенное количество очков, он получает очередной уровень.

Сетевые игры – это игры, в которых присутствует многопользовательский режим, позволяющий играть по сети с другими пользователями со всего мира. Как правило, это командные игры, которые могут продолжаться по нескольку суток.

Именно при игре в ролевые и сетевые компьютерные игры происходит очень глубокий и тотальный процесс вхождения ребенка в игру. Можно наблюдать буквально психологическое слияние ребенка с компьютером.

В крайне тяжелых случаях можно даже наблюдать, как ребенок теряет свою индивидуальность и отождествляет себя с компьютерным персонажем.

Игровая зависимость – форма психологической зависимости, проявляющаяся в навязчивом увлечении видеоиграми и компьютерными играми.

Игроманы отказываются от друзей, переходят на нездоровую пищу, забрасывают учебу, у них повышается агрессивность, склонность к насилию и ряд других факторов. Считается, что зависимые геймеры (игроки) нуждаются в психологической помощи, их проблемы не сложившаяся личная жизнь, неудовлетворенность собой, потеря смысла жизни и обычных человеческих ценностей. Появляются и другие трудности – подавленное настроение, плохое самочувствие, низкая активность; повышенный уровень тревожности и социальная дезадаптация.

Шутер – жанр видеоигр и по совместительству разговорное название игр-стрелялок. А само название появилось от англ. Shooter, что в переводе на русский означает «стрелялка или просто игра, где можно пострелять из чего-либо».

Широкое распространение в последнее время получили способы интернет-мошенничества. Каждый пользователь Интернета сталкивался с предложениями отправить СМС на определенный номер, чтобы получить причитающийся выигрыш. Сформировалось целая отрасль способов интернет-мошенничества, получившая название фишинг.

Фи́шинг (англ. phishing, от fishing – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на фейковый сайт, внешне очень похожий на настоящий.

Фейками (Фейк–от англ. fake, которое переводится как подделка, фальсификация, подлог, обман.) называют поддельные страницы или сайты, которые имитируют страницы других реальных пользователей или компаний, например, банков.

Основная задача такой страницы – убедить другого пользователя в том, что он попал на реальную страницу сайта.

После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг основан на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее.

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытия

ваших банковских счетов;

- обещания большой денежной выгоды с минимальными усилиями

или вовсе без них;

- сведения о сделках, которые слишком хороши для того, чтобы быть

правдой;

- запросы о пожертвованиях от лица благотворительных организаций

после сообщений в новостях о стихийных бедствиях;

- грамматические и орфографические ошибки.

В арсенале фишинга создание подставных страниц, кража личной информации, размещенной в социальных сетях (имя, фотография, адрес, телефон, список контактов) и использование ее для создания страниц-клонов.

Надо помнить, что в Интернете обитают не только добропорядочные пользователи, но и мошенники, которые только и мечтают о том, как бы обокрасть доверчивых пользователей или добыть у них ценную информацию.

Нигерейские письма.

Реклама и интернет-шопинг.

Баннер – графическое изображение, содержащее информацию рекламного характера.

Интернет-баннер (от англ. banner – знамя, флаг) – небольшая картинка или анимация, играющая роль гиперссылки на рекламируемый ресурс рекламодателя. *Задача баннера* – привлечь внимание пользователя, чтобы перенаправить его на другую страницу. Есть целый класс баннеров, получивших ***название вымогателей***. К ним относятся баннеры - блокировщики.

Понятие «информационная безопасность» сегодня трактуется как в широком, так и в узком смысле. В широком смысле – это информационная безопасность человека, общества и государства. В узком смысле – это безопасность самой информации и каналов ее приема (передачи), а также организация защиты от применения противником информационного оружия в ходе боевых действий.

Мы больше будем ориентированы на рассмотрение вопросов, связанных с обеспечением информационной безопасности личности, и в связи с этим стоит дать определение понятию «личность».

Личность – понятие, выработанное для отображения социальной природы человека, рассмотрения его как субъекта социокультурной жизни, определения его как носителя индивидуального начала (интересы, способности, устремления, самосознание и т.д.), самораскрывающегося в контекстах социальных отношений, общения и предметной деятельности и общении. Личность, как ключевой элемент социума наиболее подвержена различным социальным опасностям, поэтому понимание безопасности в контексте соотношения интересов личности, общества и государства предполагает рассмотрение информационно-психологической безопасности как аспекта общей проблемы.

Для сведения информационных угроз к минимуму – нужно снизить уровень риска, но для начала необходимо выделить: характер воздействия; объект воздействия, а так же условия осуществления данных воздействия, и в связи с этим выработать возможные меры защиты.

Объектом воздействия является молодежь в возрасте от 12 до 18 лет. Данная группа лиц наиболее подвержена воздействию той или иной информационной опасности ввиду того что личность еще не совсем сформировалась, а процесс социализации еще только происходит.

Так же необходимо выяснить почему современный школьник предпочитает проводить свое свободное время именно так и рассматривать проблемы, связанные с воспитанием нового поколения.

Интернет – это распределенная всемирная база знаний, включающая в себя множество различных информационных массивов (информационных ресурсов, баз данных или знаний), состоящих из документов, данных, текстов, объединенных между собой трансграничной телекоммуникационной информационной паутиной или сетью. Но не вся информация может положительно повлиять на подростка. В виду своего возраста и низкому

уровню развития защитных реакций от нежелательной информации ребенку, можно без труда навязать практически любую точку зрения и идеологию, что впоследствии негативно скажется как на личности школьника, так и на отношениях с родителями, сверстниками и учителями, а это так же негативно влияет на развитие личности. Особую угрозу таит в себе чрезмерная демонстрация насилия, цинизма, жестокости, что коренным образом противоречит любым нравственным барьерам. И несмотря на то, что сеть интернет – кладезь полезной и интересной информации, выбирать нужное и полезное умеет не каждый.

Информация, сегодня, имеет куда больший вес, чем в прежние времена, и от того какую информацию мы выбираем для себя истинной напрямую зависит уровень информационной безопасности и безопасности личности в целом. Подростки менее защищены в данном плане, именно поэтому тема обеспечения информационной личности подростка востребована реальностью. Только грамотная и слаженная работа всех социальных институтов способна воспитать личность безопасного типа. При этом педагог и родители играют большую роль в воспитании ребенка.