ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ несовершеннолетних в Интернете

Урван Парфентьев,
координатор национального узла Интернет-безопасности в России, ведущий аналитик регионального общественного центра Интернет-технологий

С доступом к Интернету образовательное сообщество получило не только новые возможности, но и угрозы. Объективная реальность современного мира — кибератака и киберунижение, жертвами которых становятся дети. Защита несовершеннолетних от контента, унижающего и оскорбляющего человеческое достоинство, — направление государственной политики, участие в котором не только добровольная обязанность каждого взрослого — родителя, педагога, администратора образовательного учреждения, но и показатель здоровья общества.

• *общество* • *личность* • *компьютерные технологии* • *Интернет-угрозы* • *киберунижение* • *социальные сети* • *Интернет-безопасность*

Сокращение расстояний: версия 4.0

Одно из главных достоинств технического прогресса — сокращение расстояний для информации. Телеграф — пионер мгновенной коммуникации — позволил быстро обмениваться текстовой информацией, пришедший вслед за ним телефон «убрал расстояние» для голосового общения. Третье «теле» — телевидение — донесло до каждого дома изображения, фильмы и визуальную информацию. Следующим этапом должно было стать «разрушение монополии» телестудий на создание и распространение визуальной информации, то есть

возможность создавать и публиковать её любому зрителю — и этим этапом стал компьютер, подключённый к Интернету.

Само собой, стал он им не сразу. На пути эволюции компьютер прошёл стадии научного эксперимента по машинному вычислению и межкомпьютерной коммуникации, «инструмента менеджеров» — средства электронной почты и бухгалтерских таблиц, «электронной газеты», соединившей в себе качества газеты и телеканала. Сейчас, благодаря развитию компьютерных и Интернет-технологий, в особенности программных, компьютер с Интернетом — мощный центр информации, коммуникации и беседы, развлечений, торговли и платежей, деловых процессов. Редкая профессия, требующая специальных знаний, сейчас не требует компьютерных познаний. И это соответствующим образом отражается на Интернет-аудитории. На данный момент в России каждый третий житель выходил в Сеть как минимум раз за шесть месяцев, а каждый день бывает в Интернете столько людей, сколько официально живёт в наших «двух столицах» вместе взятых. К их услугам — миллионы сайтов (только в российском домене, восьмом по размеру среди национальных доменов, зарегистрировано более 2 млн доменных имён), пользовательских сервисов закачки и обмена информацией, доступные цифровые технологии создания и получения контента.

Пожалуй, самая активная категория пользователей Интернета — дети и молодёжь, традиционно осваивающие технические новшества быстрее всех. После подключения всех российских школ к Интернету несовершеннолетняя Интернет-аудитория в среднем оценивается в 10 миллионов пользователей. Тех, кто использует Интернет самостоятельно (а это дети в возрасте 12–18 лет), по данным ФОМ, примерно 7,6 млн человек, из которых 3,1 млн бывает в Сети каждый день. Продолжительность их сеанса «пребывания в виртуальном мире» варьируется от 40–45 минут до шести-семи часов. Это время, а также род занятий в Сети напрямую зависит от места выхода ребёнка в Сеть — это может быть домашний компьютер, Интернет-кафе, мобильный телефон, школа, компьютер у друга или знакомого.

Что делают дети в Интернете? Во-первых, общаются, «на других смотрят, себя показывают». К их услугам — мгновенные коммуникаторы типа пресловутой «аськи», чаты, форумы, дискуссии в блогосфере, а для «себя показать» — персональные странички, собственные блоги и социальные сети. «Себя показывают» они ещё и через создаваемый ими же визуальный контент, который размещают на соответствующих сервисах — например, видеороликам «неплохо живётся» на RuTube. Далее — само собой, развлекаются. Тут тебе и компьютерные игры по Сети (новое поветрие — ролевые онлайн-игры, формирующие ещё и круг общения), и фильмы, и музыка, и забавные ролики. В-третьих — ищут информацию по собственным интересам или для учёбы. Здесь к ним на помощь приходят онлайн-версии СМИ и новостные сервисы, сетевые энциклопедии и миллионы сайтов, посвящённых той или иной тематике. Нередко в виртуальном пространстве складывается «альтернативная жизнь», серьёзно корректирующая повседневную.

Хищник из сети

К сожалению, принцип «если что-то можно использовать на пользу — значит, можно и во вред» характерен и для Интернета. Трансграничность и относительная анонимность Интернета облегчает его использование в антиобщественных, а иногда и противоправных целях. Поскольку у детей психика и мировоззрение находятся в стадии укрепления, вредное воздействие из Интернета оказывает на них гораздо более серьёзное влияние, чем на взрослых.

Наверное, практически каждый наслышан о «ренессансе» порнобизнеса, наступившем «благодаря» Интернет-технологиям — буквально тонны порнографического

контента хлынули в Интернет как к тем, кто любит «клубничку», так и к тем, кто этого не хочет или к этому не готов. Особняком здесь стоит тема детской порнографии — вовлечения детей в создание сексуального контента и его публичная демонстрация, в том числе опять же детям. Анонимность Интернета позволяет преступнику выдать себя за кого-то другого (за родственника или за сверстника) и заманить ребёнка к себе с преступными целями (скажем, для похищения или вовлечения в съёмки детской порнографии) либо получить обманом какие-то данные, которые помогут совершить преступление — скажем, обокрасть дом, «увести» деньги или что-то ещё.

Но иногда и сами дети могут использовать «высокие технологии» во вред — чаще всего своим же сверстникам. Детские шутки, иногда невинные, иногда опасные, с появлением доступных цифровых технологий перешли все границы фантазии — и главная опасность их заключается в том, что о событии становится известно не только его участникам, но всем пользователям Интернета. Записочки с оскорблениями сменились «атаками» с нецензурными словами по СМС и электронной почте, сцены унижения и насилия над сверстниками снимаются на видео или мобильный телефон и затем выкладываются в Сеть, создаются страницы, порочащие достоинство конкретного ребёнка — и хорошо, если не с компьютерным монтажом, изображающим в чём-то откровенно неприличном. Дошло до того, что хулиганы унижают сверстника специально для того, чтобы снять сцену на мобильный и показать всем, желательно через Сеть. Это явление получило название «кибер унижение» — или, точнее, «кибертравля» — и очень распространено в странах с высоким проникновением мобильных и Интернет-технологий. В том числе и в России. В результате, если с негативной обстановкой в школе ребёнок ещё как-то может мириться, то подобное «вынесение сора из избы» его просто надламывает. Причём до степени суицида. В США уже стало нарицательным имя Меган Майер — девочки, доведённой до самоубийства оскорблениями относительно её внешности через Интернет.

Да, проблема не новая — дети, как давно известно, очень жестоки. Но Интернет-технологии делают эти детские «забавы» исключительно опасными. В России ситуация усугубляется тем, что дети оказались совершенно беззащитными перед киберпреследователями. До 1991 года немалую роль в борьбе со школьными хулиганами играла пионерская организация, цементировавшая детский коллектив и имевшая рычаги воздействия, дополнявшие воспитательную работу педагогов. Сейчас же заполнить этот вакуум некому — тем более что и самих педагогов многочисленные скандалы подталкивают к самоустранению от функций воспитания питомцев.

Ещё один ключевой блок проблем, порождаемых Интернетом — это доступность для ребёнка информации и пропаганды, искажающей социальное становление будущей личности. Антиобщественный, а иногда преступный образ жизни нередко пропагандируется специально среди несовершеннолетних — в расчёте на пополнение преступных рядов. Романтизация преступного мира, с которой российское общество столкнулось в последние двадцать лет — это лишь одна из граней этой проблемы. Через сайты, форумы, блоги и социальные сети детей вовлекают в преступные и экстремистские сообщества (при этом не следует путать внесистемную политическую оппозицию или молодёжные субкультуры с настоящими экстремистами), а также в тоталитарные секты. Воздействие такой «промывки мозгов» блестяще описано в «Золотом телёнке» на примере пана Козлевича — только вот ставить заслон ей в Интернете зачастую некому, и некому подготовить ребёнка к критическому восприятию информации. Именно поэтому высока доля молодёжи

www.saferunet.ru

Национальный узел Интернет-безопасности в России содержит общую информацию об Интернет-угрозах, действиях против безопасности общества и личности в Интернете, похищении и сексуальной эксплуатации детей, программно-технических и экономических угрозах, культуре и этике в World Wide Web, новости и анонсы по теме сайта.

в преступных группировках — но разочарование из-за свернувшего под откос жизненного пути (недостатка образования, низкого социального статуса и т.п.) наступает тогда, когда ситуацию исправить уже сложно.

Ситуация осложняется серьёзным разрывом между государством и обществом в российской социальной культуре, в результате которого сложно выстроить цельный механизм государственной защиты пользователей. Массовые нарушения законности в отношении граждан сотрудниками правоохранительных органов вызвали столь же массовое недоверие к ним общества (в соцопросах фигурируют цифры от 55 до 69% недоверия), в результате чего коммуницировать с правоохранителями в деле защиты Интернета обычные пользователи не хотят. Судя по многочисленным блогам, низок уровень доверия Интернет-среды и к органам государственной власти, в том числе из-за возникновения целого ряда неприемлемых в этой среде законодательных инициатив. В этих условиях очень легко подменять идеи сетевого саморегулирования полным отрицанием необходимости каких-либо сдерживающих факторов в виртуальной среде, что успешно и делают виртуальные хулиганы и матёрые преступники.

От страуса к учёному коту

Попытки защиты детей от противоправного воздействия через Интернет в России до недавнего времени носили хаотичный характер — но даже они считались большим достижением, так как зачастую отрицалась сама взаимосвязь между Интернет-действиями ребёнка и отклонениями в его здоровье и социальном развитии. Ситуация начала меняться с резким ростом детской Интернет-аудитории, в том числе с подключением всех российских школ к Интернету.

Решение проблемы Интернет-безопасности детей лежит в комбинации двух средств: соответствующего образования и воспитания несовершеннолетних и разумного противодействия доставлению опасного контента до ребёнка. Каждое из этих средств в отдельности, как показала практика, даёт лишь частичный эффект.

Глубокое проникновение Интернета в повседневную жизнь требует и соответствующей подготовки ребёнка к жизни в «виртуальном мире». Однако российское пространство довольно долго испытывало недостаток профессиональной и компетентной информации по вопросу. Ситуацию усугубляет то, что в школе проблемы компьютерной грамотности до сих пор рассматриваются с программно-технической точки зрения, при этом практически исключается «пользовательская» составляющая и тем более этика компьютерного мира. В связи с этим, а также ограниченностью использования Интернета в школах, основная нагрузка по воспитанию юных «граждан виртуального мира» ложится на родителей — которые так же, как работники сферы образования, просто не готовы к грамотному решению возникшей перед ними задачи.

Осведомлённость родителей об Интернет-угрозах в России довольно невысока из-за слабой «интернетизированности» родителей, не работающих с компьютером, и недостатке профессиональной информации, доведённой до родителей понятным им языком. Как правило, родитель не воспринимает Интернет как источник угроз для ребёнка, а если и желает принять меры предосторожности, то не знает, где получить квалифицированную и в то же время понятную информацию, которой он смог бы воспользоваться. Для большинства родителей единственным источником сведений по вопросу стали СМИ — которые вообще-то выполняют совершенно другие задачи.

Из журналистских публикаций люди усвоили, что есть такой страшный зверь — вирус, и ещё один страшный зверь — троян, от которых можно защититься антивирусом. До места, где говорится о том, что антивирус надо обновлять, дочитало гораздо меньшее количество сограждан, поэтому ещё довольно часты изумления

в стиле «я поставил антивирус, а меня всё равно заразили». Ещё в народе знают, что при платежах в Интернете деньги магическим образом могут исчезать в неизвестном направлении, в результате чего некоторые стали бояться даже банкоматов — не говоря уже об Интернет-магазинах. Ибо, исходя из прочитанных ими журналистских материалов, в Интернете водятся страшные жулики, которые в данный конкретный момент охотятся именно за их деньгами. Как можно видеть, вместо одной крайности получилась другая — вместо недооценки Интернета получилась его демонизация, с примерно аналогичным эффектом.

В сложившихся условиях функцию просвещения на себя взяли коммерческие компании и общественные организации, работающие в сфере безопасности Интернета. Производители ПО стали активнее рассказывать о встроенных в их программные продукты механизмах защиты детей от вредных проявлений в Интернете, стали разрабатываться информационно-просветительские курсы для детей и взрослых, а также появились специальные ресурсы для детей — обучающего и развлекательного характера. Софтверный гигант Microsoft русифицировал типовые курсы по безопасности в Интернете для младшего и старшего школьного возраста, родителей и педагогов. Ответом «мира свободного ПО» стало целое пространство для безопасного времяпровождения в Сети — проект «Тырнет», где ребёнок одновременно и учится и играет. Аналогичным путём пошли создатели Детского портала Москвы — создав, по сути, три сайта для детей, молодёжи и родителей. Обучающе-развлекательное пространство также сформировали ВГТРК (проект «Бибигоша») и Студия «Жужа» (одноимённое имя проекта).

Но создать «Интернет-манежик» для ребёнка мало. Ибо всем понятно, что он рано или поздно выберется из «лягушатника» специального пространства и войдёт в «обычный» Интернет, к которому его следует подготовить. Одна из точек зрения заключалась в создании так называемого «белого списка» проверенных и отобранных сайтов, которые могут быть разрешены ребёнку. По сути, это означало тот же «лягушатник», только немного большего объёма. Другая — теория «чёрного списка» — предполагала доступ ребёнка ко всем ресурсам, за исключением тех, которые представляют угрозу для здоровья и мировоззрения ребёнка. Она гарантировала свободу оборота информации, но не решала на сто процентов задачи ограждения ребёнка от опасного контента — ибо для включения сайта в «чёрный список» его создатель должен знать о наличии такого сайта, а сайты в Интернете множатся каждую секунду.

На теориях «белого» и «чёрного» списков построены различные программно-технические решения фильтрационного типа — программы «родительского контроля», в том числе встроенные в операционные системы, непосредственно программы-фильтры, специализированные поисковики или адаптированные для детей версии обычных поисковиков. В частности, при оснащении всех российских школ Интернетом была предпринята попытка решить проблему доступа к нежелательному контенту чисто фильтрационными методами — поставив систему соответствующего характера. Однако последующие проверки показали, что, несмотря на рассылку фильтрационного программного обеспечения по школам, практика доступа оттуда к, примеру, сетевой порнографии сохраняется. К тому же фильтры не решают проблемы Интернет-образования пользователей и не объясняют, почему они вообще нужны — из-за чего они воспринимаются как элемент цензуры.

www.mosparents.ru

Портал для родителей г. Москвы, содержит информацию о различных аспектах воспитания и образования детей, консультации специалистов по вопросам педагогики и психологии.

Защита ребёнка от Интернет-угроз

В европейских странах повышением осведомлённости пользователей об Интернет-угрозах занялись специальные независимые проекты, посвящённые непосредственно Интернет-безопасности

пользователей. Работая в тесном контакте с образователями и производителями, эти проекты не представляли интересов никого из них и потому, в отличие от инициатив бизнес-игроков, не могли быть заподозрены в «задней мысли». В рамках таких проектов, получивших название «национальные узлы безопасности в Интернете», готовилась и распространялась информация о проблемах использования Интернета, конкретных видах интернет-угроз, их опасном воздействии, а также давались конкретные советы по защите детей и взрослых от вредоносного вторжения из Сети в компьютер и мозг.

Для тех, кто не смог найти в материалах узла решение персональной проблемы, заработали «линии помощи» — телефонные и Интернет-каналы консультаций по вопросам безопасного использования Интернета. Эти линии поддерживались как центрами по повышению осведомлённости пользователей, так и теми организациями, которые «осведомлённостью» не занимались. Однако ввиду очевидности, что одна работа вытекает из другой, «линии помощи» стали активно интегрироваться с центрами осведомлённости, и в данный момент большинство «линий помощи» работает вместе с центрами осведомлённости как единые национальные узлы безопасности в Интернете. Помимо адресных советов, несколько таких консультационных линий оказывают также психологическую помощь жертвам Интернет-преступлений — детям и родителям.

Практическая деятельность Интернет-пользователей в защите (в первую очередь детей) от Интернет-угроз выразилась в формировании общественных механизмов выявления противоправного контента и оперативного принятия мер по пресечению его оборота в Интернете. В первую очередь стали формироваться общественные «горячие линии», на которые пользователь, наткнувшийся на противоправный контент, может сообщить координаты этого контента. «Горячая линия», проверив сообщения пользователя, задействует общественные и — при необходимости — правоохранительные рычаги для того, чтобы доступ к такому контенту был прекращён. Если с правоохранительными рычагами всё понятно, то в общественные механизмы включаются хостинг- и контент-провайдеры, экспертные организации, а с недавних пор ещё и регистраторы доменов. Такое саморегулирование оказалось эффективнее и быстрее, чем правоохранительные рычаги — и это достоинство «горячих линий» было использовано для преодоления проблемы трансграничности Интернета, причём самими же правоохранителями. Если сайт выявлен в одной стране, а расположен в другой, то полиции необходимо задействовать Интерпол — а сигналы по его линии могут идти до полугода, в то время как из одной «горячей линии» в другую информация попадёт в течение суток. Объединённые в сеть INHOPE, «горячие линии» уже «накрыли» основные интернетизированные страны и расширяют сеть трансграничного взаимодействия.

Ещё одно важное достоинство «горячих линий» — функция посредника между гражданином и государством, исключающая их взаимный контакт. В ряде стран, включая Россию, многие люди, наткнувшись на опасный контент, воздержатся от заявления о нём в полицию. А вот общественным посредникам они пишут, особенно если учесть, что последние принимают информацию и анонимно. При этом «горячие линии» не подменяют полицию, а выступают своеобразным «фильтром» отсева негодных сообщений, что повышает эффективность работы полиции и процент раскрываемости.

В России такой Национальный Узел возник в августе 2008 года, изначально включая в себя все три «положенных» составляющие — ресурс информационно-просветительской работы, «Горячую линию» по противоправному контенту и «Линию помощи» для Интернет-пользователей. Помимо традиционных памяток по безопасности в Сети, российскому пользователю стали доступны отечественные материалы по конкретным видам Интернет-угроз и характеру их влияния, сравнительные исследования «у них» и «у нас» — к тому же рассчитанные на восприятие человеком, далёким

от программистских таинств. Причём материалы как текстовые, так и в форме видеороликов. Часть материалов посвящена такой актуальной проблеме, как защита ученика от Интернет-угроз в школе — вопросам обучения детей Интернету, практике работы учащегося в компьютерном классе, основным мерам предосторожности, их достоинствам и недостаткам, а также действиям администрации школы и учителя по защите детей от негативного контента.

Одно из таких действий — возможность поучаствовать в закрытии сайта с противоправным контентом, «выскочившим» на монитор во время урока. Для этого достаточно сообщить об этом сайте на «Горячую линию». В отличие от большинства зарубежных аналогов, российская «Горячая линия» Национального Узла работает по двенадцати видам противоправного контента, так что без внимания не останется практически ни один вид «нехорошего действия» в Сети. А в отличие от дежурной части милиции, «Горячая линия» принимает сообщения анонимно. Все полученные сообщения исследуются аналитиками Линии, которые в соответствии с установленными регламентами определяют, есть ли в ссылке «нехороший» контент или нет. При необходимости Линия имеет возможность провести экспертизу силами ведущих исследователей в необходимой области — особенно если надо проанализировать тексты. Далее информация направляется в пользовательский сервис, хостинг- или контент-провайдеру, а с недавних пор — регистратору домена, который обеспечивает недоступность сообщённого контента. В качестве «последнего защитника» задействуются правоохранительные органы. Если же сайт расположен не в России, то к закрытию противоправного контента подключается такой же Узел в стране его местонахождения — через сеть «горячих линий» INHOPE, в которую Россия вступила в мае 2009 года.

Проблема киберунижений — Интернет-хамства, кибертравли и распространения порочащей информации — резко повысила роль «Линий помощи». Перед ними встала задача оказания психологической помощи тем, кто пострадал от подобных действий в Интернете. В России эта задача решается привлечением к работе «Линии помощи» профессиональных психологов, уже оказывающих консультационные услуги по телефону — к примеру, Правозащитного движения «Сопротивление», Коалиции «Ангел».

Все эти инициативы готовы прийти на помощь учителю, родителю и самому учащемуся. Используя материалы специализированных информационно-аналитических ресурсов, можно получить необходимые данные для подготовки соответствующего урока или обеспечения защиты детей при самостоятельной работе в Интернете. При обнаружении противоправного контента на мониторах детей можно не только сказать «нельзя», но и в течение нескольких секунд сообщить тем, в чьи задачи входит прекращение доступности такого контента. И содержащиеся на специализированных ресурсах сведения помогут оперативно диагностировать поражение ребёнка Интернет-угрозами и, если недостаточно собственных усилий, направить его туда, где ему помогут и вернут в «полноценную жизнь». Часть специализированных веб-ресурсов в России уже получила одобрение образовательной среды — к примеру, Microsoft разрабатывал веб-курс для преподавателей совместно с АПК и ППРО, а Национальный Узел Интернет-безопасности в России работает при поддержке Минобрнауки и Федерального агентства по образованию.

http://www.microsoft.com/rus/protect/default.mspx

Страница компании Майкрософт содержит разделы по информационной безопасности, защите пользователей от нежелательного содержания и контактов, компьютеров от наиболее распространённых технических угроз.

О перспективах в плане Интернет-безопасности говорить всегда сложно, ибо Интернет — среда быстроразвивающаяся. Несомненно то, что сейчас в России на кибербезопасность детей обращено самое серьёзное внимание. Подготовлены или уже принимаются законодательные инициативы, усиливающие защиту детей от доступа к контенту, не соответствующему задачам образования и воспитания; ужесточается уголовная ответственность за Интернет-преступления. **НО**