



Беседа

Информационная безопасность в сети Интернет

Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам. Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов.

Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются с ресурсами, содержащими неэтичный и агрессивный контент. Все чаще дети становятся жертвами и заложниками интернета и людей, использующих их в своих целях.

По результатам социологических исследований 88% четырехлетних детей выходят в сеть вместе с родителями. В 8-9-летнем возрасте дети всё чаще выходят в сеть самостоятельно. К 14 годам совместное, семейное пользование сетью сохраняется лишь для 7% подростков. Больше половины пользователей сети в возрасте до 14 лет просматривают сайты с нежелательным содержанием. 39% детей посещают порносайты, 19% наблюдают сцены насилия, 16% увлекаются азартными играми. Наркотическими веществами и алкоголем интересуются 14% детей, а экстремистские и националистические ресурсы посещают 11% несовершеннолетних пользователей. Исследования показали, что 90% детей сталкивались в сети с порнографией, а 65% искали ее целенаправленно. При этом 44% несовершеннолетних пользователей Интернета хотя бы раз подвергались в сети сексуальным домогательствам.

Поэтому появилась новая задача – обеспечить безопасность детей в сети Интернет. Это достаточно сложно, так как Всемирная паутина изначально развивается полностью бесконтрольно. В ней есть очень много информации, доступа к которой у детей быть не должно.

Кто в ответе за наших детей в интернете?

Безопасность детей одна из главных задач цивилизованного общества,

поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу:

1. Правительство. С 1 сентября 2012 года начал действовать Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее — Закон). Он направлен на защиту детей от травмирующего воздействия на их неокрепшую психику негативной и, способной развить в ребенке порочные наклонности информации.

Актуальность этой проблемы очень высока. В силу отсутствия жизненного опыта, неокрепшей психики, ребенок более других подвержен воздействию через компьютерные игры, мобильную связь, рекламу, и особенно, через всемирную паутину сети «Интернет». Законом вводится само понятие информации, причиняющей вред здоровью и развитию детей.

Делится она на два основных вида:

1) Запрещенная к размещению. Это информация, вызывающая у детей страх, панику, а также оправдывающая насилие и противоправное поведение, в том числе информация, побуждающая к действиям, представляющим угрозу их жизни и здоровью, провоцирующая детей на суицид.

2) Информация, распространение которой ограничено возрастной категорией ее потребителей, которые сформированы по четырем возрастным категориям: не достигшие 6 лет, достигшие 6 лет, достигшие 12 лет, достигшие 16 лет.

Например, для детей, достигших 6 летнего возраста: допускается к обороту продукция, содержащая ненатуралистическое изображение или описание несчастного случая, аварии, ненасильственной смерти, но без демонстрации их последствий, которые могут вызвать у детей ужас, страх.

К обороту продукции, допускаемой для детей, достигших 16 лет, может быть отнесена информация о наркотиках, с указанием последствий их употребления, но без демонстрации применения, и при условии, что выражается отрицательное или осуждающее отношение к их потреблению.

Федеральным законом № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон „О защите детей от информации, причиняющей вред их здоровью и развитию“ и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет». были добавлены исключения для «информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети „Интернет“, кроме сетевых изданий», и для комментариев и сообщений, размещаемых на сайте сетевого издания его читателями.

2. Поисковики. Многие поисковые сервисы такие как Yandex, Ramler имеют в своем арсенале большое количество настроек, помогающих родителям оградить детей от нежелательного контента в Интернете. А так же есть поисковые системы, предназначенные специально для детей.

3. Семья. В первую очередь за безопасность детей в Интернете отвечают родители. Ведь только они могут полностью контролировать своих детей.

4. Образовательные учреждения.

Защита детей от информационных угроз и рисков Интернет-ресурсов связана с формированием медиа-грамотности. В образовательных учреждениях данная

задача может решаться педагогами с использованием различных форм медиа-образования. В Российской Федерации все школы обязаны устанавливать программы контентной фильтрации в классах информатики.

Как защитить ребенка от нежелательного контента в Интернете

- приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;
- объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены;
- старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

- будьте в курсе того, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;
- объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;
- если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;
- не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствие взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
- интересуйтесь тем, куда и с кем ходит ваш ребенок.

Как избежать кибербуллинга

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью

различных интернет-сервисов.

Предупреждение кибербуллинга:

- объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать;
- научите детей правильно реагировать на обидные слова или действия других пользователей;
- объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;
- старайтесь следить за тем, что Ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Родителям следует обратить внимание на ряд признаков в поведении ребенка, которые могут свидетельствовать о том, что **ребенок стал жертвой кибербуллинга:**

- **Беспокойное поведение**

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

- **Неприязнь к Интернету**

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

- **Нервозность при получении новых сообщений**

Негативная реакция ребенка на звук письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Что делать, если ребенок все же столкнулся с какими-либо рисками и обратился к вам за помощью

- установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать;
- постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;
- если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.) —

постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете;

- если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;
- соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы);
- если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС и др.)