Дети и Интернет

Интернет занимает все большее место в нашей культуре, особенно у детей и молодежи, для которых выполнение школьных заданий, онлайн-игры и социальные сети становятся одними из самых популярных вариантов времяпрепровождения. Однако вследствие недостаточно согласованных действий при выборе правильного подхода к обучению и защите детей возникают дополнительные проблемы, связанные с использованием Интернета детьми, а также с возможностью их самовыражения. Кроме того, культурные и географические различия в правовых и юридических нормах отражают факт отсутствия единой точки зрения на то, кого следует считать ребенком, а также на то, какие материалы можно считать подходящими для детей, вследствие чего становится трудно определить, какой «контент и типы поведения являются неприемлемыми».

Несмотря на то, что ряд киберпреступлений носит международный характер и требует внимания всех стран, на национальном уровне политические подходы к регулированию контента в основном сводились к использованию различных фильтров, ограничивающих доступ или блокирующих интернет-контент. Кроме того, несмотря на то, что зачастую рекомендуется фильтрация на уровне компьютеров организаций или родительский контроль персональных компьютеров (что является более предпочтительным вариантом фильтрации по сравнению с фильтрацией на уровне сети), ни эти усилия, ни методы фильтрации на местном или национальном уровне не являются на 100% эффективными для регулирования нежелательного контента, поскольку периодически приводят к недостаточной или избыточной блокировке. Фильтрация на уровне сети имеет дополнительные негативные эффекты. Поэтому для родителей, педагогов, опекунов, специалистов и государства в целом крайне важно проводить обучение детей и молодежи, рассказывать им о существующих рисках и ответственности, с которыми они могут сталкиваться при использовании Интернета. Этот подход может помочь молодежи распознавать опасности и избегать их, а также даст им базовые знания о работе в Интернете, позволяющие ответственно использовать преимущества сети.

Введение

Интернет одинаково важен как для детей, так и для взрослых. Сейчас дети и молодежь часто используют Интернет для:

- обучения (получения доступа к информации, знаниям, точкам зрения, средствам обучения и даже преподавателям);
- общения (выражения собственных идей, обмена информацией и опытом);
- общения с друзьями и ровесниками;
- инноваций, творчества и обмена контентом;
- игр и развлечений (игры, фильмы, музыка, книги и т. д.);

Все чаще эти действия происходят вне дома или школы, не за традиционным настольным компьютером, а на портативных устройствах, таких как смартфоны и планшеты.

По сравнению с другими технологиями, предоставляющими информационный контент, такими как радио и телевидение, Интернет предоставляет родителям, опекунам и педагогам уникальные возможности решить, что дети могут делать и видеть. Например, они могут направить ребенка на полезные и познавательные материалы, подходящие для каждого возраста, культуры, интеллектуальных способностей, уровня образования и т.п. Кроме того, они имеют возможность научить детей конструктивно использовать Интернет и избегать онлайн-рисков и неприемлемого контента.

Крайне важно для всех – родителей, опекунов, учителей, образовательных учреждений и правительств – вместе работать над созданием безопасной и доступной среды для детей и молодежи, где бы они ни находились: дома, в школе, в общественных местах, таких как библиотеки или интернет-кафе. Каждый обязан вносить свой вклад в создание подобных сред, чтобы все дети и молодежь могли активно и с удовольствием использовать положительные аспекты Интернета.

При этом, учитывая важность знания возможных рисков, связанных с использованием Интернета детьми, очень важно не переусердствовать в этом. Для начала лучше всего руководствоваться знаниями, полученными в школе, здравым смыслом и придерживаться четких инструкций. Несмотря на большой объем проделанной работы по защите детей Internet Society уверена, что можно сделать еще больше, чтобы защитить детей и молодежь от потенциально опасного интернет-контента и в то же время позволить им в полной мере использовать все возможности и преимущества Интернета.

Кого следует называть «ребенком»?

Один из самых сложных вопросов – определить, кто же такой ребенок, поскольку подходы существенно отличаются в зависимости от социальных и дисциплинарных определений.

В Конвенции Организации Объединенных Наций по правам ребенка в статье 1 указано: “ребенок – это любой человек в возрасте до восемнадцати лет, если по закону, применимому к данному ребенку, он не достигает совершеннолетия ранее”. Несмотря на безобидные цели подобного определения, ограничение по возрасту в 18 лет может быть спорным с различных точек зрения.

Действительно, существуют другие определения ребенка, однако каждое из них определяет этот термин с разных научных точек зрения. Например, в психологии применяются определенные критерии, относящиеся к психологической зрелости и развитию, в то время как в биологии большее предпочтение отдается физическому развитию. С ненаучной точки зрения, при определении того, кто же является ребенком, моралисты придерживаются принципа сознательности и свободы согласования.

Использование Интернета детьми

Похоже, что достижение согласия относительно того, кого же можно называть ребенком, является одним из главных препятствий для обеспечения эффективной защиты детей. Тем не менее, как бы мы ни трактовали этот термин, нам определенно известно, что дети и молодежь постоянно используют Интернет и что он стал неотъемлемой частью современной жизни. Интернет быстро стал доступен для детей, и сейчас большинство молодых людей часто выходят в Интернет.

Дети вовлечены в широкий спектр Интернет-активности, многие области которой сопряжены друг с другом, поскольку платформы Web 2.0 все больше становятся частью культуры современной молодежи. Опрос в 25 странах, проведенный в рамках исследовательского проекта *European Union Kids Online* при финансировании по программе Европейской Комиссии по повышению безопасности Интернета, свидетельствует о том, что чаще всего молодежь использует Интернет для: выполнения школьных заданий (92%), игр (83%), просмотра видеоклипов (75%) и общения в социальных сетях (71%). 59% детей в Европе, которые используют Интернет, имеют свой собственный профиль в социальных сетях. Только 28% детей в возрасте 9-10 лет, но уже 59% детей в возрасте 11-12 лет имеют профиль в социальной сети, что говорит о том, что начало пользования социальными сетями больше связано с переходом в среднюю школу, нежели с достижением минимального возраста, установленного популярными поставщиками.[1] Поэтому определение и регламентирование норм, описывающих общение в Интернете, должно стать неотъемлемой частью детского образования и начинаться уже в начальной школе.

Чтобы обезопасить детей в Интернете, важно помочь им понять, что в сети является безопасным, а что рискованным, чтобы дети могли принимать независимые информированные решения. Обучение безопасности в Интернете является критически важным для защиты молодых людей от угроз в сети: как внешних угроз, таких как «неприемлемый» контент и действия (например, азартные игры) или контакты с «нежелательными» людьми (например, запугивание, выслеживание, мошенничество), так и внутренних угроз, таких как разглашение слишком большого количества персональных данных. Работая вместе с детьми, прислушиваясь к их потребностям и изучая их опыт, мы можем создать такую среду, в которой они смогут использовать максимум возможностей, предлагаемых Интернетом, но при этом действовать ответственно и безопасно. В то же время, подобная среда может помочь детям, которые используют Интернет для совершения «плохих поступков», понять истинные последствия своих действий на более уязвимых субъектах.

Наконец, очень важно помнить, что Интернет не является «вредным» инструментом, подвергающим детей беспрецедентным опасностям. Данная идея согласуется с гибким подходом к образованию, демонстрируя «сохранение адаптивной способности – способности адаптироваться к меняющимся обстоятельствам, сохраняя при этом главную цель, что является крайне важным навыком в эпоху непредсказуемой дестабилизации и непостоянства».[2] Согласно данной теории, в вопросах безопасности детей в Интернете законодательные ограничения и регулирование, в конечном счете, могут оказаться контрпродуктивными. Будет невозможно (и, по сути, бесполезно) пытаться заблокировать каждое действие, которое потенциально может подвергать детей опасности в Интернете; более здоровый и гибкий подход предполагает, что именно обучение и подготовка станут теми инструментами, которые помогут родителям, педагогам или государству решать проблемы, связанные с безопасностью детей в Интернете. Мы должны стремиться к тому, чтобы дети осваивали Интернет постепенно, и использовать гибкие стратегии, объясняя им, как вести себя в интерактивной среде и избегать существующих в ней опасностей. Поэтому наша главная цель состоит в том, чтобы дети поняли важность «сетевого этикета», внушить им руководящий принцип «прежде чем щелкнуть мышью, подумай».

---

1 Дополнительные статистические данные можно найти по адресу http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20 reports.aspx

2 Andrew Zolli & Ann Marie Healy (2012) " *Resilience: Why Thins Bounce Back*" (Гибкость: почему все возвращается), Free Press,

С учетом этого в следующих разделах будет показан ряд опасностей, с которыми дети сталкиваются в Интернете.

Проблемы, связанные с определением жестокого обращения с детьми и порнографией

Первая попытка на международном уровне дать определение «детской порнографии», как формы жестокого обращения с детьми была сделана в Дополнительном протоколе к Конвенции по правам ребенка[3] по торговле детьми, детской проституции и детской порнографии. Однако более позднее определение, которое было дано в Конвенции Совета Европы по защите детей от сексуальной эксплуатации и сексуального насилия[4], вынесенное на подписание в октябре 2007 г., является более четким. В статье 20 детская порнография определяется как «любой материал, в котором изображен ребенок, реально участвующий или симулирующий поведение, возбуждающее половую страсть, или любое изображение детских половых органов, прежде всего, для сексуальных целей».

Поскольку подобное поведение обычно бывает скрытым, а также в связи с отсутствием универсального определения, что можно классифицировать как материал с половыми извращениями с детьми, непонятно, насколько широко распространены подобные материалы. Эта сложность дополнительно усугубляется недостатком данных из многих регионов мира о производстве и распространении материалов с половыми извращениями с детьми; а также изменением глобальной структуры производства и потребления подобных материалов. Быстрое развитие сегмента цифровых камер и компьютерных технологий, в результате которого они стали более широкодоступными и позволили создавать снятые или измененные в цифровом формате изображения, привело к тому, что становится еще сложнее собрать достоверную статистическую информацию о масштабах проблемы.

Кроме того, отсутствие универсальной законодательной базы на национальном уровне или глобальных директив, явно запрещающих материалы с половыми извращениями с детьми, делает защиту детей в Интернете очень сложной задачей. Только в некоторых странах и регионах были приняты законы, которые вносят материалы с половыми извращениями с детьми в разряд противозаконных. Несмотря на то, что во многих странах уже начался процесс правовой реформы, в большинстве стран по-прежнему руководствуются устаревшим законодательством относительно неприемлемого поведения, которое неадекватно трактует сексуальные преступления или совращения, совершаемые через Интернет.

Простое отсутствие четкого соглашения на правительственном уровне относительно размеров проблемы и соответствующего законодательного урегулирования только подчеркивает важность соответствующего обучения и инструктажа детей родителями и в школе. Очень важно, чтобы они знали, как реагировать на материалы, содержащие половые извращения с детьми, при использовании Интернета или при столкновении с преступниками, которые могут попытаться заманить их в опасные ситуации.

[3] http://www.unicef.org/crc/index_protocols.html

[4] http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

Другие потенциальные угрозы

Дети и молодежь сталкиваются с самыми различными рисками во время использования компьютера. Некоторые из них связаны с угрозами для их безопасности и конфиденциальности. Другие могут быть связаны с умышленным или неумышленным нарушением законов, например авторских прав или клеветой. Они также могут иметь серьезные последствия.[5]

Какие же существуют риски для детей и молодежи?

- Случайный или умышленный просмотр недопустимых изображений или материалов.
- Домогательства сексуальных преступников в чатах, других формах социальных сетей или по электронной почте.
- Запугивание или домогательства по сети.
- Разглашение скрытой персональной информации и кража данных (вследствие публикации в общедоступных ресурсах избыточного количества информации или иным образом).
- Вирусы, шпионские и вредоносные программы.
- Фишинговые сообщения
- Излишний меркантилизм: реклама и веб-сайты, посвященные продуктам.
- Последствия соблазна принять участие в пиратстве, связанном с программным обеспечением, музыкой и видео.[4]

По численности молодежь является самой быстрорастущей возрастной группой, использующей Интернет; в то же время в тех случаях, когда они недостаточно информированы и имеют ограниченную возможность оценить риск и принять решение, они становятся уязвимыми. Сотрудничество нескольких заинтересованных сторон на местном, национальном и международном уровнях является эффективным способом информирования о важности проблем защиты детей в некоторых регионах мира. Более того, для пресечения правонарушений требуется сотрудничество множества агентств на местном и национальном уровнях, сотрудничество и обмен информацией являются крайне важными для обеспечения защиты детей.

Отсутствие универсальных подходов к защите детей

Существуют культурные и географические различия, связанные как с концепцией детства, так и с пониманием того, что является уместным и приемлемым. Что касается контента, и «неприемлемого контента» в частности, состав детей не является однородным. Все дети отличаются – по возрасту, образованию, языку, культуре, религии, степени зрелости, опыту, интересам и т.п. Некоторые дети быстро меняются по мере взросления и развития. Ответственность за определение того, какой контент является приемлемым для отдельного ребенка, лучше оставить родителями, опекунами и педагогами, которые знают ребенка.

Распространение новых технологий, неизбежное отставание в разработке политик, связанных с ними, а также разнообразие культур и уровней развития дополнительно усложняют поиск решений. С другой стороны, не менее важно разрабатывать и публиковать материалы, соответствующие культурным, возрастным и языковым критериям, делая их привлекательными и легкодоступными.

[5] Угрозы такого типа являются важными, но выходят за рамки настоящего документа.

Подходы к контролю доступа к нежелательному контенту

Многие страны мира решили разрабатывать свои национальные подходы, регулирующие использование Интернета. Подобные попытки имели разную степень успеха, а иногда и неожиданные последствия. Это можно наблюдать в растущем числе стран, в которых в последние годы было принято решение просто ограничить доступ к Интернет-контенту. Кроме того, все большее число стран пытается применять фильтры в Интернете – технический подход к контролю доступа к контенту. Как правило, используется три способа блокировки доступа к веб-сайтам: блокировка по IP-адресам, фильтрация DNS и блокировка URL-адресов с помощью прокси-сервера. Блокировка по ключевым словам, при которой блокируется доступ к веб-сайтам на основе ключевых слов, найденных на запрошенных URL-адресах, или блокировка поиска на основе «черного» списка терминов является более совершенным способом, который применяется во все большем числе стран. Указанные методы можно применять в разных точках, например: у поставщика услуг Интернета, на уровне организации или отдельного устройства, подключенного к Интернету.

Существует множество разных способов фильтрации, все они направлены на ограничение доступа к определенным веб-сайтам. Ряд из них основан на списке «плохих сайтов», который создают поставщики услуг Интернета или органы власти и внедряют на уровне сети, однако родители, опекуны, преподаватели или другие полномочные органы также имеют доступ к программам и инструментам, способным осуществлять мониторинг, отслеживать и блокировать доступ к определенным действиям в Интернете на устройствах, используемых их детьми; например:

- прокси-серверы и программы, разрешающие или блокирующие доступ к определенным сайтам и протоколам (включая защиту от вирусов, фильтры нежелательной электронной почты, блокировка всплывающих окон, антишпионские программы, программы для удаления файлов «cookie» и т. д.)
- Программы для фильтрации контента, которые находят и блокируют определенный контент или веб-сайты
- Параметры конфигурации, которые задают уровень конфиденциальности и мониторинга сайтов (например, фильтр Google SafeSearch, Privolock)

Однако фильтрация не может быть эффективной на 100%. Технологии фильтрации часто склонны к двум характерным недостаткам: недостаточная и избыточная блокировка. Под недостаточной блокировкой понимается неспособность заблокировать доступ ко всему целевому контенту. С другой стороны технологии фильтрации часто блокируют контент, который они не должны блокировать, что называется избыточным блокированием. Оба указанных недостатка появляются вследствие создания множества «черных» списков с использованием сочетания ручных настроек и автоматизированных поисковых систем, которые часто содержат веб-сайты, классифицированные неправильно. Дополнительные проблемы возникают, когда контент размещается под тем же IP-адресом или в том же домене. Более того, методы фильтрации не удаляют незаконное содержимое из Интернета,[6] и их зачастую можно обойти. Они также могут случайным образом ограничить свободное и открытое общение и тем самым ограничить права отдельных людей или групп меньшинств.

Поскольку сетевые фильтры часто представляют собой результаты собственной разработки и/или используют секретные «черные списки», зачастую отсутствует

[6] В считаные минуты можно определить другое доменное имя, ссылающееся на тот же адрес в Интернете.

прозрачная возможность маркировки и ограничения доступа к сайтам. Подобная недостаточная прозрачность особенно беспокоит, когда корпорации, создающие технологии фильтрации содержимого, работают вместе с недемократическими режимами, чтобы установить общенациональные схемы фильтрации контента. В большинстве стран, где применяется фильтрация и блокировка контента, списки блокировки, генерируемые в коммерческих продуктах, дополняют собственными списками, ориентированными на темы и организации для конкретной страны или языка.

Несмотря на то, что использование Интернета в школе осуществляется под контролем с применением фильтров, многие дети осуществляют доступ к Интернету из других мест и на других устройствах, на которых фильтры могут отсутствовать, и с минимальным контролем. Дети и молодежь все чаще подключаются Интернету с использованием других устройств, поддерживающих подобное подключение, например, с помощью смартфонов, планшетных компьютеров и игровых приставок. Это означает, что даже если на домашнем или школьном компьютере установлены фильтры, дети и молодежь все равно смогут получить доступ к Интернету без фильтров с использованием других средств или, возможно, даже в обход фильтров, установленных на компьютере. Поэтому очень важно научить детей правильно вести себя в Интернете, а также обсудить с ними проблемы, с которыми они могут столкнуться.

Могут высказываться мнения, что фильтрация на уровне сети, например фильтрация DNS, также приводит к нестабильности сети, способствует разобщенности и подрывает основы Интернета.[7] Другие подходы к контролю контента, такие как наложение ареста на имя домена, предназначенные не только для защиты молодежи, подвержены большинству тех же проблем, что и при использовании фильтрации DNS, включая простой обход, неспособность решить проблему, которая лежит в основе, а также подталкивание к созданию теневой сети, которая будет недоступной для правоохранительных органов.

Несмотря на то, что программы могут блокировать доступ к высокопрофильным веб-сайтам, в настоящее время не существует решения, которое будет неизменно надежным и абсолютно эффективным. Технологии позволяют точно идентифицировать и выделить определенные категории контента, находящегося на миллионах веб-сайтов и в других интернет-приложениях, таких как группы новостей, списки электронной почты, чаты, мгновенные сообщения и социальные сети. Фильтрация не может заменить советы и надлежащее участие родителей. В любом случае эти методы не позволяют удалить предосудительный или незаконный контент из Интернета; они только затрудняют к нему доступ.

Наконец, Internet Society обеспокоена тем, что защита детей в Интернете может стать явным или скрытым поводом для введения дальнейших ограничений на правительственном уровне. Она считает, что с помощью блокировки интернет-контента невозможно обеспечить 100% безопасность детей и молодежи. Тем не менее, мы можем повысить безопасность детей и молодежи, рассказав детям, родителям, опекунам, педагогам и коллегам, как отличать и как поступать с опасным контентом на компьютерах, в Интернете, на мобильных телефонах, и как обеспечить ответственный и безопасный подход к использованию технологий, а также предоставить простые в использовании настраиваемые средства для управления доступом и контентом.

[7] Дополнительные сведения о блокировке DNS можно найти на сайте http://www.internetsociety.org/what-we-do/issues/dns/finding-solutions-illegal-line-activities

Недавние политические директивы

В 2011 г. ОЭСР опубликовала отчет под названием *Защита детей в Интернете: риски, с которыми сталкиваются дети в Интернете, и политика их защиты*[8], а в 2012 г. ОЭСР приняла *Рекомендацию Совета по защите детей в Интернете*[9], определяющую три основных принципа:

- расширение возможностей;
- пропорциональность и фундаментальные ценности;
- гибкость.

Кроме того, данные рекомендации[10] призывают правительства:

- демонстрировать свои стремления и лидерские качества через собственную политику;
- поддерживать координированную реакцию всех заинтересованных сторон; поощрять согласованность и последовательность внутренних инициатив по защите детей в Интернете среди общественных и частных заинтересованных сторон;
- поощрять углубленное информирование и обучение в качестве основных средств поддержки детей и родителей;
- поддерживать реально обоснованную политику защиты детей в Интернете;
- стимулировать разработки и использование технологий для защиты детей в Интернете с учетом принципов уважения прав детей и свободы других пользователей Интернета;
- укреплять международные сети национальных организаций, занимающихся защитой детей в Интернете;
- обмениваться информацией о подходах национальной политики к защите детей в Интернете и в частности к развитию эмпирических основ для сравнительного количественного и качественного анализа международных политик;
- поддерживать региональные и международные усилия по созданию ресурсов для улучшения политических и рабочих показателей уровня защиты детей в Интернете;
- повышать координацию работы с различными международными и региональными организациями и органами, которые осуществляют поддержку усилий правительства в данном регионе и привлекают заинтересованные стороны, не входящие в правительство, если применимо.

Информирование и подготовка детей: конструктивная роль родителей, опекунов и педагогов

Наверное, самый эффективный способ решения проблем, возникающих при использовании Интернета, – информировать и подготовить детей и молодежь, чтобы они знали, как защитить себя и своих друзей. Методики подготовки включают рассказ о правовых границах на языке, понятном в данном возрасте, а также открытое обсуждение культурных, моральных и этических норм и ожиданий внутри общества. Именно родители, педагоги, частный сектор, правительство и др. должны помочь молодежи научиться понимать и уважать эти границы и нормы. Информирование и подготовка детей и молодежи также позволяет им избежать других угроз, включая мошенничество, шпионские и вредоносные программы.

---

[8] http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en

[9] http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False

[10] http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False

Несмотря на то, что появляются эффективные стратегии, которые родители могут применять для управления использованием Интернета их детьми, существует также много приемов, позволяющих детям уклоняться или противостоять подобному контролю со стороны родителей. Часто это дополнительно осложняется тем фактом, что дети обладают большими знаниями и опытом в области использования новых средств, чем их родители. Тем не менее, дети и молодежь обычно устанавливают доверительные отношения со взрослыми и ровесниками, советы и мнения которых для них важны (надежные авторитеты). Важно, чтобы такие надежные авторитеты сами знали о возможных рисках и способах решения, умели эффективно делиться информацией с теми, кому она необходима, и выступали в качестве примеров для подражания или источников надежной информации и советов. Кроме того, важно понимать, что эти надежные авторитеты со временем меняются. К тому моменту, когда ребенок достигнет «подросткового возраста», на него все большее влияние будут оказывать ровесники.

Кроме того, родители, опекуны, воспитатели и надежные авторитеты должны играть активную роль в обучении детей и молодежи, рассказывать им о рисках, с которыми они могут сталкиваться при просмотре сексуально откровенных материалов, а также при общении с интернет-преступниками и мошенниками и способах избежать этих рисков. Не менее важно, чтобы дети также знали, как выстраивать личное общение со знакомыми и друзьями, и внимательно относились к разглашению своих персональных данных в Интернете. Безусловно, чтобы обучение проходило эффективно, важно чтобы родители, опекуны и педагоги обладали достаточной компьютерной грамотностью.

Способность родителей контролировать доступ и использование Интернета детьми осложняется, как минимум, двумя факторами. Первый состоит в том, что, несмотря на то, что родители отвечают за безопасность своих детей, они также должны уважать растущую независимость детей и их права на конфиденциальность.

Второй представляет собой тот факт, что очень немногие родители полностью понимают интернет-культуру своих детей.[11] Часто родители не могут понять, почему дети и молодежь пользуются социальными сетями. Кроме того, существует огромный разрыв поколений в отношении к конфиденциальности и правам человека и в отношении к данным, которыми они обладают и которые разглашают. Проблемы безопасности, конфиденциальности, интернет-преступлений и киберпреследования являются сложными, как с технической, так и психологической точек зрения, и родителям может быть очень непросто с ними справиться. Эти факторы указывают на острую необходимость поощрять родителей общаться со своими детьми, обсуждать их действия в Интернете и уровень их опыта. Подобное участие позволит родителям, опекунам, педагогам и другим надежным авторитетам оградить детей и молодых людей от возможных бед.

Не менее важно подготовить детей, привив им навыки работы в Интернете. Сюда относится обучение и поощрение использования имеющихся информационных технологий, обучение принятию правильных решений (в одиночку или в группах), чтобы по мере взросления дети сами стали новым поколением надежных авторитетов.

[11] Способы использования детьми Интернета и мобильного телефона для работы, игр и общения

Вывод

Помимо работы напрямую с детьми в их семьях, в школах и других заведениях, где возможны личное общение и консультации, существуют другие меры, доступные правительствам, некоммерческим и общественным организациям, позволяющие повысить информированность и сделать так, чтобы дети и молодежь могли использовать преимущества Интернета, оставаясь в безопасной среде. Далее приведены примеры некоторых возможных инициатив:

- Участие всех заинтересованных лиц в мероприятиях по информированию сообщества: правительственные агентства, частный интернет-сектор, неправительственные организации, группы сообществ и широкая общественность в целом.[12]
- Создание горячих линий в Интернете, по которым можно сообщить о нарушениях в сети, а также для получения советов и консультаций.
- Стимулирование образовательных программ с участием поставщиков услуг Интернета, а также правоохранительных органов для разработки оптимальных методик по борьбе с незаконным контентом и действиями.
- Создание интернет-сайтов или платформ, которые будут выступать в качестве образовательной основы для детей, подростков, родителей и учителей. Эти сайты должны содержать актуальную и регулярно обновляемую информацию по вопросам безопасности в Интернете, а также видеосюжеты для самостоятельного изучения на различных языках.

Интернет меняется настолько быстро, что технические меры защиты вряд ли смогут решить проблему. Более надежными и эффективными являются те меры, которые предусматривают подготовку с участием семьи, сообщества, обучение и подготовку, чтобы дети и молодежь имели все возможности и преимущества при использовании Интернета.

[12] Чтобы ознакомиться с примерами правил безопасности при использовании Интернета, посетите веб-сайт www.kidsap.org и прочитайте международное руководство по безопасности в Интернете ECPAT

Приложение

«Вопросы и ответы» для родителей, детей и педагогов

Далее приведен ряд советов в отношении использования Интернета, о которых должны знать родители, учителя (и дети).

- Компьютер должен находиться дома на видном месте, чтобы взрослые могли контролировать, для каких целей он используется.
- Обучение тому, что представляют собой компьютеры, должно проводиться на всех уровнях – дети, родители и учителя.
- Родители и учителя должны вместе с детьми использовать Интернет.
- Родители должны (согласовав это со своими детьми) установить разумные рамки и временные ограничения использования Интернета.
- Родители и педагоги должны ознакомиться и внимательно изучить опасности, связанные с Интернетом.
- Родители и педагоги должны подчеркнуть, что принцип «Не говорить с незнакомцами» также относится и к общению в сети.
- Родители и педагоги должны запрещать своим детям загружать и/или передавать фотографии без надлежащего контроля.
- Должен применяться весь арсенал средств фильтрации и родительского контроля как дома, так и в школе.
- Родители и педагоги обязаны внушить детям необходимость соблюдения конфиденциальности в раннем возрасте, пояснив, почему это важно для детей уважать и использовать право на «уединенность».

Internet Society
Galerie Jean-Malbuisson 15
CH-1204 Geneva, Switzerland
(Женева, Швейцария)
Тел.: +41 22 807 1444
Факс: +41 22 807 1445
http://www.internetsociety.org

1775 Wiehle Ave. Suite 201
Reston, VA 20190, USA (США)
Тел.: +1 703 439 2120
Факс: +1 703 326 9881
Электронный адрес:
info@isoc.org