

Информационная безопасность детей в сети Интернет

В соответствии с Конституцией Российской Федерации человек, его права и свободы имеют приоритетное значение. Права человека могут быть реализованы тогда, когда люди информированы о своих правах и знают, как их использовать. Поэтому образование в области прав человека имеет важнейшее значение для эффективного выполнения установленных стандартов. Осознание молодыми поколениями своих прав и того, как их использовать, зависит, прежде всего, от системы школьного образования. Школы не только должны распространять основные знания о нормах в области прав человека и механизмах для их защиты, но и играть основополагающую роль в укреплении таких ценностей, как уважение к другим людям, отказ от дискриминации, гендерное равенство и демократическое участие. СМИ, информационные и коммуникационные технологии сегодня играют важнейшую роль в жизни детей. Дети каждый день смотрят телевизор часами, но все больше и больше времени они проводят в Интернете, используя навыки, которым они быстро обучаются у своих сверстников. Дети используют интерактивные средства для игры, общения, написания блогов в Интернете, прослушивания музыки, размещения собственных фотографий и поиска других людей для общения в интерактивном режиме. Поскольку существует реальное несоответствие между грамотностью в отношении информационных средств между детьми и взрослыми, большинство взрослых мало знают о том, что делают их дети в Интернете или как они это делают. Виртуальный мир может как предложить детям возможности, так и расставить ловушки. Использование электронных, цифровых и интерактивных информационных средств оказывает значительное положительное воздействие на развитие детей: это увлекательно, это обучает и социализирует. Однако это также несет потенциальную возможность вреда для детей и сообществ, в зависимости от того, как осуществляется использование.

По результатам социологических исследований 88% четырёхлетних 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. Помимо социальных сетей, среди несовершеннолетних популярны следующие виды и формы онлайн-развлечений: сетевые игры; просмотр и скачивание фильмов, клипов, аудиофайлов, программ; обмен файлами.

Классификация Интернет-угроз

Электронная безопасность

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной

информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное программное обеспечение и различные формы вредоносных кодов.

Спам

Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

Кибермошенничество

Кибермошенничество - это один из видов киберпреступлений, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контакт

Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследования

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи.

Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

- Киберзависимости
- Заражению вредоносными программами при скачивании файлов
- Нарушению нормального развития ребенка
- Неправильному формированию нравственных ценностей
- Знакомству с человеком с недобрыми намерениями

Информационная безопасность детей

Согласно российскому законодательству **информационная безопасность детей** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

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. Должны быть законы, которые смогли бы оградить детей от вредной информации в Интернете. Так в России все школы обязали установить программы контентной фильтрации в классах информатики.

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. Конечно же ни кто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Ведь только родители 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.

Медиа-грамотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Медиа-образование выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества.

Защиту детей от информации, причиняющей вред их здоровью и безопасности, прежде всего, семья и школа. Это задача не только семейного, но и школьного воспитания. Проведение уроков медиа-безопасности планируется в образовательных учреждениях на постоянной основе, начиная с первого класса, в рамках школьной программы (в том числе уроков ОБЖ).

Цель проведения уроков медиа-безопасности – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

К информации, запрещенной для распространения среди детей, относится информация:

- 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- 2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- 5) оправдывающая противоправное поведение;
- 6) содержащая нецензурную брань;
- 7) содержащая информацию порнографического характера.

Значимой является совместная работа с родителями по формированию у них базовых знаний, связанных с правилами безопасного пользования Интернет-ресурсами.

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, 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.

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

- Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

Безопасное совершение покупок в Интернет-магазинах

- Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
- Необходимо вместе с ребенком познакомиться с отзывами покупателей;
- Проверьте реквизиты и название юридического лица – владельца магазина;
- Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
- Поинтересуйтесь, выдает ли магазин кассовый чек
- Сравните цены в разных интернет-магазинах
- Позвоните в справочную магазина
- Обратите внимание на правила интернет-магазина
- Выясните, сколько точно вам придется заплатить

Как распознать интернет-и игровую зависимость

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

- навязчивое стремление постоянно проверять электронную почту;
- предвкушение следующего сеанса онлайн;
- увеличение времени, проводимого онлайн;
- увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
- Периодически старайтесь полностью проверять свои домашние компьютеры.
- Делайте резервную копию важных данных.
- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Что делать, если ребенок все же столкнулся с какими-либо рисками

- 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.)

Общие рекомендации по обеспечению безопасности детей и подростков в Интернете

1. **Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной.** Так вам будет проще уследить за тем, что делают дети в Интернете.
2. **Следите, какие сайты посещают ваши дети.** Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.
3. **Расскажите детям о безопасности в Интернете.** Вы не сможете все время следить за тем, что ваши дети делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.
4. **Установите защиту от вирусов.** Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.
5. **Научите детей ответственному поведению в Интернете.** Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в Сети.

6. **Оценивайте интернет-контент критически.** То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.
7. **Если Вы нуждаетесь в консультации специалиста** по вопросам безопасного использования Интернета или если Ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи “**Дети Онлайн**” (www.detionline.com), по телефону: 825 000 15 (звонок по России бесплатный). .

Пять правил безопасного пользования электронной почтой:

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.