

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.

Основные риски действия 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.

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.

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

Материалы для подготовки и проведения родительских собраний по проблемам информационной безопасности детей

Выделим ключевые рекомендации, которые могут помочь родителям в решении проблемы безопасного пользования Интернет-ресурсами.

Защита 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.

Порядок опознавания интернет и игровую зависимость

В России все более актуальны проблемы так называемой «интернет-зависимости» и зависимости от компьютерных игр. 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.

Порядок действий, если Ваш 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.)

Рекомендации для детей по информационной безопасности в Интернете Для учащихся начальных классов

- Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
- Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
- Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься, и номер твоего телефона должны знать только родители и друзья.

- **Никогда не отправляй свои фотографии людям, которых не знаешь лично.** Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.

- **Не встречайся с людьми, с которыми познакомился в Интернете, без родителей.** Многие люди выдают себя не за тех, кем являются на самом деле.

- **Общаясь в Интернете, будь дружелюбен с другими.** Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.

- **Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.**

Для учащихся 5-9 классов

- **Регистрируясь на сайтах, не указывайте личную информацию, которую могут все увидеть.** Не нужно, чтобы незнакомые люди знали, как вы выглядите и где учитесь.

- **Не рассказывайте незнакомым как где вы живете, можете сказать название города, но не адрес, по которому Вас могут найти.**

- **Общайтесь по веб-камере только с друзьями.** Следите, чтобы ваш разговор видели только вы, потому что чужие люди могут записать видео, которое видно через веб-камеру и использовать его в своих целях.

- **Нежелательные письма от незнакомых людей называются «Спам», на них нельзя отвечать, а лучше вообще не открывать** потому, что в них могут быть вирусы.

- **Если вы ответите, то люди отправившие письмо, будут знать, что ваш почтовый ящик работает и дальше посылать вам спам.**

- **Не забудьте сохранить все неприятные сообщения, которые вы получили, чтобы потом показать их взрослым.** Взрослые помогут вам и скажут, как правильно поступить. Не расстраивайтесь, если Вы получили плохое сообщение.

- **Если вас кто-то расстроил или обидел, расскажите все взрослому.**

Для учащихся 10-11 классов

- **Не публикуйте свои личные данные и личные данные своих друзей.**

- **К личным данным относятся номера мобильного и домашнего телефонов, адрес электронной почты и любые фотографии, на которых изображены ты, твоя семья или друзья.**

- **Если Вы публикуете фото- или видеоматериалы в Интернете – любой желающий может скопировать их и потом воспользоваться в своих целях.**

- **Не верьте спаму (нежелательной электронной рассылке) и не отвечай на него.**

- **Не открывайте файлы, полученные от людей, которых Вы не знаете.** Неизвестно, что они могут содержать: это может быть как вирус, так и незаконный материал.

- **Следите за тем, что пишете.** Не пишите людям то, что никогда бы не сказали им в лицо.

- **Не забывайте, что люди в Интернете могут говорить неправду.**

- **Лучше не встречайтесь со своими виртуальными друзьями в реальной жизни без присутствия взрослых, которым Вы доверяете.**

- **Никогда не поздно рассказать родителям, если что-то смущает или настораживает.**