Памятка для родителей об информационной безопасности детей

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

информация, запрещенная для распространения среди детей;
информация, распространение которой ограничено среди детей определенных возрастных категорий.
К информации, запрещенной для распространения среди детей, относится:
информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
способность 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;
обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
оправдывающая противоправное поведение;
содержащая нецензурную брань;
содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

ОБЩИЕ ПРАВИЛА ДЛЯ РОДИТЕЛЕЙ

Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

ВОЗРАСТ ОТ 7 ДО 8 ЛЕТ

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7 - 8 лет

Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
Используйте специальные детские поисковые машины.
Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
Научите детей не загружать файлы, программы или музыку без вашего согласия.
Не разрешайте детям использовать службы мгновенного обмена сообщениями.
В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

ВОЗРАСТ ДЕТЕЙ ОТ 9 ДО 12 ЛЕТ

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
Расскажите детям о порнографии в Интернете.
Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

ВОЗРАСТ ДЕТЕЙ ОТ 13 ДО 17 ЛЕТ

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
Компьютер с подключением к сети Интернет должен находиться в общей комнате.
Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
Приучите себя знакомиться с сайтами, которые посещают подростки.
Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.
Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Основные риски действия Интернет-угроз. 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.
Неправильному формированию нравственных ценностей.

Знакомству с человеком с недобрыми намерениями.

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.

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.

Выделим ключевые рекомендации, которые могут помочь родителям в решении проблемы 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 уверен.

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 отсутствии 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.

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 Whols)

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, виртуальнаяаддикция) 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 вИнтернете;

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). На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет.

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.

Актуальные вопросы родителей

Сколько времени ребенок может проводить за компьютером?

Все родители, наверняка, часто говорят о том, что их дети много времени проводят за домашними заданиями или что их дети мало гуляют и, в основном, сидят дома. Поэтому родители вряд ли удивятся результатам исследований, показывающим, что дети проводят за компьютером слишком много времени. Этому вопросу родителям надо уделить особое внимание.

Сегодняшним детям компьютер заменил множество разнообразных действий. Эта машина помогает им в выполнении домашних заданий, а при необходимости предоставляет услуги телефонной связи, «игровой площадки», музыкального и видео сервиса и других развлечений. Ваше беспокойство должно зависеть от того, каким образом ваш ребенок использует отведенное ему для компьютера время и много ли времени ему остается для других занятий и развлечений. Если ребенок, просыпаясь утром или вбегая домой после школы, в первую очередь включает компьютер и сидит за ним до тех пор, пока не ляжет спать, у вас, скорее всего, будут проблемы. Совсем маленьким детям до пяти лет не следует проводить много времени за компьютером. Жизненно важным для них является развитие познавательных способностей и изучение других видов деятельности. Дети 10-летнего возраста должны совмещать компьютер с другими занятиями. В отношении раннего школьного возраста трудно сказать, сколько точно времени отвести ребенку на компьютер, т.к. в этом возрасте дети очень различаются по развитию. Некоторые дети пытаются в любую свободную минуту выйти в чат (наподобие тех из нас, взрослых, которые любят болтать по телефону). Других притягивает сам компьютер: учебные программы, создание веб-страниц, устройство компьютера. Наш совет – внимательно следите за поведением ребенка. Какие-либо изменения в его поведении станут лучшим индикатором негативных явлений, которые должны насторожить Вас. Например, если ребенок перестал общаться с друзьями, заниматься спортом или просто выходить на улицу, или же у него резко упала успеваемость в школе – все это вы должны проанализировать. Если ваш ребенок замкнут или необщителен, то вы должны со всей серьезностью отнестись к увлечению Вашего ребенка компьютером. Поэтому, решение вопроса лимита времени, проводимого Вашим ребенком за компьютером, зависит, прежде всего, от Вас самих, с учетом того, что Вы будете внимательно следить за поведением ребенка и хорошо представлять себе, для чего именно ребенок использует компьютер.При этом некоторые медики предлагают четкие возрастные схемы максимально допустимого времени пользования компьютером.

С какого возраста можно разрешать ребенку пользоваться своей собственной электронной почтой?

Не существует жесткого возрастного ограничения. Самый простой ответ: вы можете допустить ребенка к e-mail в том случае, если он выражает желание пообщаться с кем-нибудь модным образом. Прежде чем зарегистрировать почтовый ящик, предложите ему для начала использовать ваш и под присмотром написать, например, брату или лучшему другу. Электронная почта – это здорово, потому что она преодолевает все географические и возрастные барьеры. Как правило, дети становятся готовыми к использованию e-mail с 7-8 летнего возраста.

Следует ли использовать программу контроля за поведением ребенка в Интернете?

Родители, в целом, еще не пришли к единому мнению по этому вопросу и, как правило, делятся на два лагеря. Одна сторона считает, что контроль за поведением дает детям гарантию безопасности, другие категорически возражают им тем, что это равносильно организации слежки за детьми. Программы контроля предназначены для того, чтобы точно знать, что ваш ребенок делает в Интернете. Они позволяют Вам вести запись адресов, которые ваш ребенок посещает в Интернете. Известны даже случаи, когда ведение подобных записей помогало представителям правоохранительных органов. Видимо, вывод может быть следующий. Если вы решились поставить компьютерную деятельность Вашего ребенка под контроль, вам следует поставить его в известность. Если же вы контролируете своего ребенка безего ведома, вы, действительно, шпионите за ним. Скорее всего, если вы расскажете ребенку, что установили программу контроля в целях его собственной безопасности, он поймет вас. И, наконец, помните, что вашей основной целью является воспитание молодого человека, который сможет правильно пользоваться Интернетом, даже если никто не будет его контролировать.

Ребенок скачивает много музыки из Интернета. Законно ли это?

Ответ зависит от того, где ваш ребенок берет эту музыку. В настоящий момент общая ситуация с музыкой в Интернете достаточно сложная и запутанная. Есть сайты, которые требуют помесячной оплаты за скачивание определенного количества песен. Есть сайты, которые совершенно бесплатно предлагают музыку для скачивания на законных основаниях, т.к. музыканты дали свое разрешение пользоваться образцами их музыки или же они каким-то другим образом получают свои авторские гонорары. Существуют сайты, на которых необходимо платить за каждую скачанную песню, т. е. своего рода «слушаешь, пока платишь». А еще есть сайты, с которых можно скачать любую музыку совершенно свободно, но это, по всей вероятности, будет нарушением авторских прав. Дети особенно любят такие сайты, поскольку у них обычно нет денег для скачивания музыки. На сайтах, где предлагается обмен музыкальными записями, пользователи могут обмениваться музыкальными файлами друг с другом. Это своего рода громадный клуб по обмену музыкой. Главная проблема в том, что музыканты, создающие музыку, не получают своих авторских гонораров. Кроме того, подобные сайты не дают гарантии качества. Наконец, очень легко подцепить какой-нибудь вирус, пользуясь услугами таких бесплатных сайтов.

Ребенок часто, отходя от компьютера, посылает своим друзьям подробные сообщения о том, где он находится в это время. Хорошо это или плохо?

Многие программы мгновенных сообщений предлагают вам размещать сообщения, извещающие желающих связаться с вами людей о том, что вас нет у компьютера. Дети могут детально и подробно информировать о том, куда они собрались идти и долго ли они будут отсутствовать. Некоторым родителям такие сообщения очень нравятся, поскольку они точно знают, где находится в настоящее время их ребенок. Однако все-таки следует объяснить ребенку, что не следует быть слишком откровенным в Сети.