Методические рекомендации «Информационная безопасность детей в использовании Интернет-ресурсов», разработанные АОУ ВО ДПО «ВИРО»

Крылова Т.А., кандидат психологических наук, научный сотрудник лаборатории комплексного сопровождения РСО;
Никандрова Н.Н., методист лаборатории воспитания и социализации.

Информационная безопасность детей в использовании Интернет-ресурсов

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 года № 436-ФЗ устанавливает правила медиа-безопасности детей при обороте на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи.

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.

Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов.

Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются с ресурсами, содержащими неэтичный и агрессивный контент. Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки.

Рассмотрим 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 ребенка
- 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 фрм 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.

На сайте «Дети онлайн» родители и педагоги найти рекомендации, которые помогут вам обеспечить медиабезопасность детей в сетях Интернет и мобильной (сотовой) связи.

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

Материалы для педагогов 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.

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 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.

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: 8 800 25 000 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.

В приложении 1 помещены ответы на актуальные вопросы родителей по проблемам безопасного пользования Интернет-ресурсами, которые могут быть рассмотрены в ходе собраний, консультаций, а также размещены на школьных сайтах в рубрике «Для Вас, родители».

В приложении 2 помещены информационные материалы для педагогов к проведению с детьми разных возрастных групп классных часов, бесед по проблемам безопасности в сети Интернет.

Приложение 1

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 без его 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.

Приложение 2

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

Ваш личный Интернет рекомендует:

- 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.

Глоссарий

Антивирусная программа - Программа, предназначенная для предотвращения доступа к персональному компьютеру для вредоносных программ — она обнаруживает инфицированные файлы и удаляет их.

Брандмауэр - Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.

Вирус - Вредоносная программа, которая распространяется, копируя себя в другие программы. Вирус может распространяться через файлы, сообщения электронной почты или веб-страницы. Компьютер может заразиться вирусом во время работы пользователя в Интернете или при открытии вложений электронной почты. Вирусы могут снизить работоспособность компьютера или системы.

Всплывающее окно - Новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит собственного веб-адреса, однако в некоторых случаях может его содержать. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклама.

Дискуссионный форум - Место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация.

В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором, который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

Загрузка - Сохранение файлов из Интернета на собственном компьютере.

Защита данных - Набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.

Информационная безопасность - Политика, реализуемая для обеспечения контроля над рисками информационной безопасности.

Операционная система - Главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся Microsoft® Windows®, Apple® Mac OS и Linux®.

Опасные программы: вирусы, черви и трояны Программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, вирусов, червей или троянов.

Почта; электронная почта; сообщение электронной почты - Электронная передача текста или изображений между адресами компьютерного приложения.

Сервер - Программа, которая распределяет файлы по компьютерам в сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты сети. Сервером часто называют компьютер, на котором установлена серверная программа.

Сетевой дневник - Общественный интерактивный дневник.

Спам - Нежелательная электронная почта, которая, как правило, рассылается в целях прямого почтового маркетинга. Спам почти всегда единовременно рассылается большому кругу получателей.

Хакер, взломщик Человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. Примечание: термин «хакер» имеет два значения — он может также означать опытного компьютерного пользователя. (см. Хакеры и взломщики)

Чат - Дискуссионный форум, работающий в режиме реального времени. В нем пользователи поочередно пишут сообщения, сразу отображающиеся на экране. Сообщения заменяются по мере написания новых, поэтому отображаются только самые последние сообщения.

Червь - Вредоносная программа, которая может независимо распространяться через информационные сети. Черви могут распространяться через электронную почту или бреши в системе защиты информации в обозревателе Интернета или операционной системе. Даже если пользователем не выполняются никакие действия, черви могут получить доступ к незащищенным компьютерам при их подключении к Интернету. Черви затрудняют работу системы или компьютера и могут распространять другие вредоносные программы.

Список основной литературы

1. Горбунова Л.Н., Анеликова Л.А., Семибратов А.М., Смирнов Н.К., Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил.
2. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 года N 436-ФЗ;
3. Федеральный закон Российской Федерации от 21 июля 2011 г. N 252-ФЗ г. Москва «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;
4. «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10.

Список дополнительной литературы

1. Барбара Гутман, Роберт Бэгвилл. Политика безопасности при работе в Интернете — техническое руководство. CITForum 2009 [Электронный ресурс]. — URL: http://www.citforum.ru/internet/security_guide/index.shtml
2. Безопасность детей в Интернете. Nachalka.com 2008 [Электронный ресурс]. — URL: http://www.nachalka.com/bezopasnost
3. Безопасность дома [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/default.mspx
4. Беки Уорли. Интернет: реальные и мнимые угрозы/ Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2004. — 320 с.
5. Будунов Г.М. Компьютерные технологии в образовательной сфере: «за» и «против». — М.: АРКТИ, 2006. — 192 с.
6. Галатенко В.А. Основы информационной безопасности. [Текст] 4-е изд. учеб.пособие, ВУЗ // — М: Издательство Бином. Лаборатория знаний, Интуит, 2008—205 с.
7. Евтеев Л. Безопасность ребенка в Интернете. Инновационная образовательная сеть «Эврика» — Пермь, 2009. [Электронный ресурс]. — URL: http://www.diaghilev.perm.ru/class/sobr4—2.htm
8. Интернет-СМИ «Ваш личный Интернет» [Электронный ресурс]. — URL: http://contentfiltering.ru/
9. Ленков С.В., Перегудов Д.А, Хорошко В.А. Методы и средства защиты информации. В 2 томах. Том 1. Несанкционированное получение информации [Текст] // — М: Издательство: Арий, 2008 г. 464 с.
10. Прохода А. Н. Обеспечение Интернет-безопасности. Практикум: Учебное пособие для вузов. [Текст] // — М.: Горячая линия — Телеком, 2007. — 180 с: ил.
11. Основы безопасности детей и молодежи в Интернете — интерактивный курс по Интернет-безопасности. Владельцами авторских прав на сайт являются проект Финский день информационной безопасности и

WSOYpro [Электронный ресурс]. — URL: http://laste.arvutikaitse.ee/rus/html/copyright.htm
12. Кимберли Янг. Тест на Интернет-зависимость / Перевод теста, выполненный и адаптированный В.А.Буровой/ Клиника СПО Центр — М: 2009 [Электронный ресурс]. — URL: http://www.psyhelp.ru/texts/iad_test.htm

Сайты

WWW.MICROSOFT.COM/RUS/CHILDSAFET

WWW.CONTENT-FILTERING.RU

- **Center for Safe and Responsible Internet Use**
  http://responsiblenetizen.org
  Целью Центра Безопасного и Ответственного Использования Интернета является информирование родителей, учителей, библиотекарей о том, как эффективнее помочь ребенку приобрести необходимые знания, умения и навыки для безопасного Интернет-серфинга.
- **ChatDanger**
  http://www.chatdanger.com/
  Сайт информирует пользователей Интернета о потенциальных угрозах и принципах онлайн безопасности в чатах, программах мгновенных сообщений, онлайн играх и при использовании электронной почты.
- **MaMaMedia**
  http://www.mamamedia.com/
  Детский портал, работающий в сотрудничестве с ведущими Интернет-провайдерами и компаниями по производству программного обеспечения. Помогает детям посредством онлайн игр и конкурсов приобретать опыт по безопасному использованию Интернета.
- **MissDorothy**
  http://www.missdorothy.com/
  Сайт США создан в 2000 г. с целью обсуждения различных тем и с помощью обучающей программе, ознакомляя детей всего мира и их родителей.
- **ChildWise**
  http://www.childwise.net
  ChildWise - некоммерческая организация, целью работы которой, является предотвращение, защита и сокращение эксплуатации и половой агрессии в отношение детей в Австралии и за границей. ChildWise предоставляет помощь и поддержку людям и организациям, разрабатывает и поставляет инновационные программы защиты детей, работает в сотрудничестве с правительством и общественностью для определения стратегии борьбы с эксплуатацией и половой агрессией в отношение детей и защищает их права.
- **Nobody'sChildrenFoundation**

http://www.fdn.pl

Фонд Одиноких детей - некоммерческая неправительственная организация, которая обеспечивает широкие возможности помощи оскорбленным детям, их родителям, и опекунам. Деятельность фонда направлена на детей, подвергнутых жестокому физическому, психологическому и сексуальному обращению, их родителей и опекунов, а так же на профессионалов, занимающихся делами жестокого обращения с детьми.

- **ChildnetInternational**

http://www.childnet-int.org

Некоммерческая организация ставит перед собой цель сделать Интернет безопасным для детей, подчеркивает его позитивные аспекты и предлагает советы для детей и родителей, как избежать потенциальных опасностей, с которыми ребенок может столкнуться.

- **Pedowatch**

http://www.pedowatch.com/

Ресурс с 1996 года поддерживает ДжулиПози (JuliePosey), которая в сотрудничестве с правоохранительными органами США, активно борется с сексуальными приставаниями к детям в Интернете и распространением незаконной детской порнографии в Сети.

- **CyberAngels**

http://www.cyberangels.org/

"Кибер Ангелы" - первая европейская организация по защите детей в сети Интернет, основанная в 1995 году.

- **i-SAFE America**

http://www.isafe.org/

Фонд i-SAFE AmericaInc., основанный в 1998 году является лидером в области безопасности интернет-образования. I-SAFE - некоммерческий фонд, миссия которого состоит в том, чтобы обучить ответственности и обеспечить безопасность молодёжи при пользование Интернетом. Целью фонда является обучение студентов распозновать и избегать опасных, пагубных или незаконных действий, а так правильно реагировать на них.

- **PedofiliaNo**

http://www.pedofilia-no.org/

Единственная независимая испанская организация по борьбе с детской порнографией в международной сети Интернет. Включает статьи и новости на эту тему.

- **Le Portal Societe de L'infarmation**

http://www.internet.gouv.fr/

Официальный сайт французского правительства о мероприятиях в области регулирования Интернет.

- **NetAlert**

http://www.netalert.net/

Организация, созданная в 1999 году при поддержке государства с целью вести просветительскую деятельность и давать независимые консультации по

вопросам организации доступа к сетевому контенту. Организацяи является консультационным органом при правительстве Австралии по вопросам Интернет-безопасности. В сферу деятельности NetAlert входит распространение положительного опыта безопасного использования Интернета, особенно среди несовершеннолетних и их семей.

- **WiredSafety**
  http://www.wiredsafety.org/
  «Безопасность Сети» - это самая крупная онлайн-добровольческая организация, занимающаяся помощью жертвам кибер-преступлений и сексуальных домогательств, образованием и предоставлением информации о всех аспектах онлайн-безовасности.
- **Global Internet Liberty Campaign (GILC)**
  http://www.gilc.org/
  «Глобальная кампания за свободы в Интернет» - это международное движение, объединяющее ряд организаций, в основном некоммерческих и правозащитных. Задачи, которые ставят перед собой члены GILC, - борьба с нарушением прав человека в Интернет, в первую очередь свободы слова и неприкосновенности частной жизни. Ограничения доступа к Интернет, криптография, государственный контроль за коммуникациями - эти темы также входят в область интересов GILC.
- **Messeging Anti-Spam Work Group (MAAWG)**
  http://www.maawg.org/
  Анти-спамовская Рабочая Группа представляет собой коалицию компаний, объединивших свои усилия в борьбе со спамом, вирусами и защите от различных интернет-атак Совместная работа компаний в MAAWG помогает находить новые решения для предотвращения и избежания онлайновых угроз, а также способствует совершенствованию систем безопасности.
- **Europe'sInformationSociety**
  http://europa.eu.int/information_society/index_en.htm
  Сайт посвящён развитию информационного общества в Европе.
- **Internet Corporation for Assigned Names and Numbers (ICANN)**
  http://www.icann.org/
  Международная организация по присвоению доменных имен и номеров)является некоммерческой организацией по назначению адресов и имен в Интернете, управлению системами доменных имен и утверждению параметров протоколов.
- **Internet Hotline Providers in Europe Association (Inhope)**
  http://www.inhope.org/
  Ассоциация Inhope способствует сотрудничеству между интернет-провайдерами "горячих линий". Её миссия состоит в устранение детской порнографии из Интернета и защите молодых людей от вредного и незаконного использования Интернета. Главными целями Inhope является создание и снабжение эффективных национальных "горячих линий",

обучение и поддержка новых "горячих линий", способствование распространению понимания безопасности Интернета.

- **Insafe**
  http://www.saferinternet.org
  Организация предоставляет информацию о безопасном использовании Интернета и коммуникационных технологиях, работает в сотрудничестве правительственными организациями, представителями Интернет-индустрии, средствами массовой информации и родителями. Организация поддерживает работу «горячей линии», по которой принимаются сообщения о размещении незаконного онлайн контента от Интернет-пользователей по всему миру.
- **InternetWatchFoundation**
  http://www.iwf.org.uk/
  InternetWatchFoundation (Фонд Интернет Наблюдения) поддерживает работу «горячей линии», которая позволяет Интернет-пользователям, столкнувшимся с детской онлайн порнографией в любой стране мира, с незаконным взрослым контентом или пропагандой расовой нетерпимости на сайтах хостинг-провайдеров Великобритании, сообщить об этом в организацию InternetWatchFoundation.
- **InternetContentRatingAssociation**
  http://www.icra.org/
  Некоммерческая Международная Организация, сотрудничающая с мировыми лидерами в сфере защиты детей от нежелательной информации в Интернете. Организация предоставляет родителям необходимую информацию для контроля за онлайн путешествиями детей.