Приложение 1 к письму ГАУ ДПО ИРО РБ
от 13.08.2018г. № 02-24 / 146

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) О ВОЗМОЖНОСТЯХ ОРГАНИЗАЦИИ РОДИТЕЛЬСКОГО КОНТРОЛЯ ЗА ДОСТУПОМ ДЕТЕЙ В СЕТЬ ИНТЕРНЕТ

Методические рекомендации

Уфа 2018

Методические рекомендации для родителей (законных представителей) о возможностях организации родительского контроля за доступом детей в сеть Интернет:

Методические рекомендации. – Уфа: Издательство ИРО РБ, 2018.

Составители: Шарипова Г.И., Тагиров И.Х.

Введение

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.

Данные методические рекомендации разработаны в соответствии с Федеральным законом от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Цель данных методических рекомендаций - ознакомить родителей (законных представителей) с возможностью и необходимостью организации родительского контроля за доступом детей в сеть Интернет. Методические рекомендации предназначены для родителей (законных представителей), т.к. обеспечение безопасности детей в сети Интернет невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок, находясь в сети Интернет.

С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательной организации, и тем более отдельного педагога. На родительских собраниях, лекториях, встречах со специалистами нужно знакомить их с видами существующих интернет угроз, рекомендациями по обеспечению безопасности ребенка в сети ответственности родителей.

Общий анализ проблемы и необходимость защиты детей в сети Интернет

XXI век стал периодом фундаментального роста и развития различных видов массовой информации, информационных и коммуникационных технологий, глобальной сети Интернет и информационного общества. Все это оказывает самое прямое воздействие на эмоциональное и физическое развитие подрастающего поколения. Сегодня многие ученые обеспокоены негативным влиянием информационного насилия на детскую психику.

Последние годы были ознаменованы большим количеством громких инцидентов, связанных с негативными последствиями нарушений информационной безопасности детей. В России проживает почти 21 миллион детей в возрасте до 14 лет. Из них 10 миллионов активно пользуется Интернетом, что составляет 18% интернет-аудитории нашей страны.

В социальном пространстве информация распространяется быстро, благодаря техническим возможностям. Сама информация часто носит противоречивый, агрессивный и негативный характер и влияет на социально-нравственные ориентиры общественной жизни. В связи с этим, возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Современный школьник, включенный в процесс познания, оказывается незащищенным от потоков информации. Пропаганда жестокости средствами массовой информации, возрастающая роль Интернета, отсутствие цензуры является не только социальной, но и педагогической проблемой.

Современный подросток все меньше общается в реальной жизни со сверстниками, друзьями, одноклассниками. В среднестатистической семье телевизор включен до 7-8 часов в день, а центром внимания детей является компьютер - по статистике, на школьников приходится около 3-4 часа в день, что равнозначно пяти урокам в школе. Современные гаджеты и Интернет заменили детям прогулки на улице, общение со сверстниками и родителями. Сегодня в обществе актуальна следующая проблема – неограниченный доступ ребенка к сети Интернет.

В России 1 сентября 2012 года вступил в силу Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Данный закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ. К информации, запрещенной для оборота среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- 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;

- 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;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Детей и подростков, без всякого сомнения, нужно защищать от разрушающего информационного воздействия на их несформировавшуюся личность. Кроме этого, информационная продукция, запрещенная для детей, не может распространяться в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территории этих организаций.

В Законе определяются виды информации, распространение которой среди детей определенных возрастных категорий ограничено, к ней 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 том числе 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.

Распространение такой информационной продукции допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия, жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом устанавливается классификация информационной продукции по пяти возрастным категориям:

1. информационная продукция для детей, не достигших возраста шести лет;
2. информационная продукция для детей, достигших возраста шести лет;
3. информационная продукция для детей, достигших возраста двенадцати лет;

4. информационная продукция для детей, достигших возраста шестнадцати лет;
5. информационная продукция, запрещенная для детей.

Контентные риски. Что это такое и как их избежать?

Контент – это наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т.д. (например, контент интернет-сайта); мобильный контент – мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.): текст, графика, музыка, видео, игры, дополнительное программное обеспечение.

Информация нежелательного характера, которая несет в себе контентные риски, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относятся:

- пропаганда насилия, жестокости и агрессии;
- разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;
- пропаганда суицида;
- пропаганда азартных игр;
- пропаганда и распространение наркотических и отравляющих веществ;
- пропаганда деятельности различных сект, неформальных молодежных движений;
- эротика и порнография;
- нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Размещение противозаконной информации в сети Интернет преследуется по закону. Это относится в первую очередь к распространению наркотических веществ, порнографических материалов, особенно с участием несовершеннолетних, призывам к разжиганию национальной розни и экстремистским действиям. В российском законодательстве есть возможность в соответствии со статьями уголовного кодекса привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов электронных текстов и видеопродукции.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, порнография, агрессивные онлайн-игры, азартные игры, информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления и др.

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл

происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков – непредсказуемо; под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребенка.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных. Особенно опасными с этой точки зрения является просмотр через сеть Интернет тех или иных видеоматериалов. Очень многие распространители негативного контента преследуют определенную цель – заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия преследуются по закону в соответствии со ст. 272, 273, 274 Уголовного кодекса РФ.

Контентная фильтрация домашнего интернета родителями.

Для ограничения доступа детей к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, сервисы, тарифные опции Интернет-провайдеров, специальные возможности антивирусных программ.

Принцип работы этих систем обычно строится на черных (запрещенных) и белых (разрешенных) списках, либо на основе фильтрации. Наиболее широкое распространение получили три алгоритма фильтрации:

1. фильтрация по ключевым словам (конкретные слова и словосочетания используются для включения блокировки веб-сайта);
2. динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения, загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное);
3. URL-фильтрация (запрашиваемая страница или целый домен, например, dosug.nu, могут быть определены или категорированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Лучшие в мире системы контентной фильтрации используют URL-фильтрацию, основанную на анализе и категоризации Интернет-ресурсов. Такой механизм признан наиболее эффективным методом фильтрации контента.

Для ограничения доступа несовершеннолетних лиц к нежелательному или опасному контенту с настольных компьютеров и мобильных устройств можно использовать **дополнительные опции, предлагаемые большинством Интернет-провайдеров**. Для этого необходимо обратиться в службу технической поддержки провайдера (телефон данной службы обычно указан в договоре) и высказать пожелание подключения данной услуги. Далее необходимо следовать инструкциям оператора.

Можно также использовать **специализированное программное обеспечение и сервисы**. Наиболее популярные, некоммерческие версии: SkyDNS, NetPolice Child, Eyes Relax, Parental Control Bar, Norton Online Family, NetPolice Lite. Помимо этого существует возможность введения ограничения доступа к нежелательным сайтам путем установки дополнений (расширений) в Интернет-браузерах, таких как: Internet Explorer, Mozilla FireFox, Chrome, Opera и других.

Обращаем внимание, что на домашних компьютерах также можно задействовать **антивирусные программы** с функцией «Родительский контроль», которые могут защитить ребенка от нежелательного контента. В основном это коммерческие продукты: Kaspersky Internet Security 2012, Kaspersky Crystal, Kaspersky Internet Security 7.0, KinderGate Родительский контроль, ChildWebGuardian, Spector Pro 6.0, КиберМама, Eset Nod32 и других.

Однако существуют и бесплатные продукты, например, Avira Free Antivirus 2013 с веб-приложением Avira Free SocialShield.

Использование функции родительского контроля подробно описано в инструкциях пользователя для антивируса.

Стоит обратить особое внимание на наличие функции родительского контроля при приобретении антивирусной программы или продлении лицензии на следующий год, сообщить о вашем желании распространителю программного обеспечения. Практически все современные разработчики антивирусных пакетов имеют в своём арсенале продукты для обеспечения безопасности ребенка в сети, блокировки нежелательного и опасного контента.

Возможности родительского контроля.

1. *Фильтры web-сайтов*.

Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается.

Создание белого списка. Более жесткий способ контроля, когда вы самостоятельно составляете белый список сайтов, которые может посещать ребенок.

Создание черного списка. В черном списке указываются сайты, на которые ребенку заходить запрещено. Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Родители могут расширять черный список сайтов на свое усмотрение, при желании, используя автоматизированную информационную систему ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию, утвержденную Постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»» (https://reestr.rublacklist.net).

2. *Ограничение времени, проводимого ребенком за компьютером*. Определяйте расписание пользования компьютером и Интернетом: выбирайте допустимое время суток и продолжительность работы. Так вам не придется прогонять ребенка от компьютера и вступать в конфликт - сеанс закончится сам собой.

3. *Установка запретов на использование детьми отдельных программ.*

Во избежание различных недоразумений родители могут ограничить список используемых ребенком программных продуктов. Большинство современных

операционных систем имеют в своем составе инструмент доступа пользователей к программным продуктам, что дает возможность ограничения доступа ребенка к нежелательным программным продуктам.

4. *Управление доступом к игровым приложениям*.

Возможности родительского контроля позволяют помочь детям играть в безопасные, дружелюбные, занимательные и обучающие игры, соответствующие их возрасту. В частности, родители могут блокировать как все игры, так и только некоторые из них. Дополнительно родители могут устанавливать разрешение или запрет на доступ к отдельным играм, исходя из допустимой возрастной оценки и выбора типа содержимого.

5. *Журнал отчетов о работе ребенка за компьютером*.

С целью анализа того, чем занимался ребенок за компьютером в отсутствие взрослых, какие программы запускал, какие сайты просматривал в Интернете, с кем общался и т.д., родительский контроль ведет аудит всех действий подрастающего пользователя. В журнал записываются адреса посещенных детьми страниц Интернета. В некоторых программах журнал с отчетом можно получать по электронной почте, что очень удобно, если родитель находится вне дома, и хочет просмотреть, какие сайты посещал ребенок.

Как помочь ребенку, если он уже столкнулся с Интернет-угрозой.

- 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 Ваши или свои 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, Сестры и др.)

Сервисы, позволяющие родителям контролировать использование Интернета детьми

КиберМама™ http://www.cybermama.ru - программа для ограничения времени работы на компьютере детей и подростков. Позволяет создавать расписание работы ребенка за компьютером и автоматически контролировать нежелательных игр и программ, блокировать доступ в Интернет. Программа проста и понятна в использовании и не требует от родителей специальных компьютерных навыков и знаний.

NetKids - сервис, который позволяет родителям контролировать использование интернета детьми. NetKids это: Блокировка доступа к опасным сайтам; Отчеты о посещенных сайтах; Мониторинг общения в социальных сетях; Контроль загрузки фотографий и личной информации; Отчеты о поисковых запросах; Мониторинг

почтовых сообщений и записей в блогах. Вся работа осуществляется через удобный и понятный web-интерфейс.

KinderGate Родительский Контроль 1.0. Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого, доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru.

Интернет Цензор – интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте. Программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. «Интернет Цензор» может использоваться как в домашних условиях, так и в образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

Полезные сайты для родителей

http://www.nachalka.com/bezopasnost – Безопасность детей в Интернете

http://detionline.com/ – Дети России Онлайн. Сделаем Интернет безопаснее вместе

http://www.ifap.ru/library/book099.pdf – Безопасность детей в Интернете

http://www.microsoft.com/ru-ru/security/default.aspx – Центр безопасности Microsoft

http://stopfraud.megafon.ru/parents/ – Безопасный Интернет от Мегафон

http://www.fid.su/projects/journal/ – Фонд развития Интернет. Журнал «Дети в информационном обществе»

http://www.mts.ru/help/useful_data/safety/ – Безопасный Интернет от МТС

http://safe.beeline.ru/index.wbp – Безопасный Интернет от Билайн

http://www.saferunet.ru/ – Центр безопасного Интернета в России

http://www.friendlyrunet.ru/safety/74/index.phtml – Фонд «Дружественный Рунет»

http://netpolice.ru/filters/ – Фильтры NetPolice

http://www.socobraz.ru/index.php/Сообщество_родителей – Сообщество родителей СОЦОБРАЗ

http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx – Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?

http://windows.microsoft.com/ru-RU/windows7/products/features/parental-controls – Родительский контроль в Windows 7

http://play.mirchar.ru/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detey.html – Консультации для родителей по обеспечению безопасности детей в Интернет

http://www.internet-kontrol.ru/ –Защита детей от вредной информации в сети Интернет

http://www.oszone.net/6213/ – Обеспечение безопасности детей при работе в Интернет

http://wiki.saripkro.ru/index.php/Интернет-безопасность_для_родителей – Интернет-безопасность для родителей

http://www.sch169.ru/doc/pam.pdf – Как защититься от интернет-угроз

Информационная безопасность

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (далее - методические рекомендации). В данных методических рекомендациях содержится памятка для родителей об информационной безопасности детей и памятка для обучающихся об информационной безопасности:

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:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

3. К информации, запрещенной для распространения среди детей, относится:

4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

5. 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;

6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

8. оправдывающая противоправное поведение;

9. содержащая нецензурную брань;

10. содержащая информацию порнографического характера.

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

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. 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;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4. 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

1. 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.

2. 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.

3. 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)

4. 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).

5. 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

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.

2. 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.

3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".

14. 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

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.

9. 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.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. 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.

13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. 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

1. 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).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. 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.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. 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.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. 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.

10. 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.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. 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.

Памятка для обучающихся об информационной безопасности

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);

2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;

3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;

4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;

5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;

2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;

3. Незаконное копирование файлов в Интернете - воровство;

4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;

5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;

2. Пользуешься Интернет-источником - делай ссылку на него;

3. Открывай только те ссылки, в которых уверен;

4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;

5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;

2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против

преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им

мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то

злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового пространства.

Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Список использованной литературы:

1. О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 N 436-ФЗ [Электронный ресурс] // СПС Консультант Плюс (дата обращения: 13.07.2018).
2. Гендина Н. И. Основы информационной культуры школьника: учебно-методический комплекс для учащихся 5-7-х классов общеобразовательных организаций / Н. И. Гендина, Е. В. Косолапова. – М.: РШБА, 2017. – 432 с.
3. Безопасный интернет – детям! Полезные советы для тебя и твоих друзей [Электронный ресурс]: сайт // Министерство внутренних дел Российской Федерации.
4. Линия помощи «Дети онлайн» [Электронный ресурс]: сайт. – Режим доступа: http://detionline.com/.
5. Методические рекомендации по контролю за использованием несовершеннолетними сети Интернет во внеучебное время.Методические рекомендации / Сост. О.В. Пикулик, С.В. Синаторов. – Саратов: ГАОУ ДПО «СарИПКиПРО». – 2012. – 39 с.
6. Правила поведения учащихся в современной информационной среде [Электронный ресурс]: сайт. – Режим доступа: http://5319sc5.edusite.ru/DswMedia/ravila_povedenija_v_inv_srede.pdf
7. Сайт «Безопасность детей» Онлайн Энциклопедия
8. Журнал «Дети в информационном обществе» - Режим доступа: http://detionline.com/journal/numbers/28

Приложение 1 к письму ГАУ ДПО ИРО РБ
от 13.08.2018г. № 02-24 / 146

ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ РЕСПУБЛИКИ БАШКОРТОСТАН

Методические рекомендации по вопросам информационной безопасности детей в сети Интернет

Методические рекомендации

Уфа 2018

Методические рекомендации по вопросам информационной безопасности детей в сети Интернет:

Методические рекомендации. – Уфа: Издательство ИРО РБ, 2018.

Составители: Шарипова Г.И., Тагиров И.Х.

Введение

Проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с постоянным ростом несовершеннолетних пользователей. Число пользователей Интернета в России стремительно растет и молодеет, доля детской аудитории среди них очень велика. Для многих российских школьников Интернет становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которые являются запрещенными для детей, так как могут нанести вред их физическому и психическому здоровью.

Интернет стал неотъемлемой частью нашей жизни. С помощью всемирной паутины мы находим нужную информацию, общаемся с друзьями, узнаем последние новости, совершаем покупки. Но, как известно, в Интернете есть не только полезное. Интернет для детей таит в себе множество опасностей. Существует множество сайтов пропагандирующих порнографию, проституцию, насилие, войны, межнациональную и религиозную рознь, употребление наркотиков и алкоголя. Такого рода информация может травмировать психику ребенка, вызвать страх, панику и внушить им ужас. Большинство взрослых, которые знакомы с Интернетом, понимают и осознают эту проблему. Но лишь немногие из них знают, как правильно защитить детей от такого рода информации.

Цель методических рекомендаций - помочь учителям, родителям и учащимся усвоить правила пользования Интернетом, знать источники опасности, которые таит в себе всемирная паутина, и первоочередные шаги для обеспечения безопасности.

Виды on-line угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

1. При общении в сети Интернет у каждого обязательно появляются виртуальные знакомые и друзья. Подобные отношения многим кажутся безобидными, поскольку Интернет-друг является как бы «ненастоящим» и не может принести реального вреда. Однако это не так. Кроме своих сверстников и интересных личностей, общение с которыми пойдет на пользу, ребенок может завязать знакомство не только с педофилом и извращенцем, но и с мошенником и хулиганом. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и киберунижением, доставляя объекту травли множество страданий. Для ребенка такие переживания могут оказаться критичными, поскольку он более раним, чем взрослые люди.

Различия киберпреступлений от традиционных реальных преступных посягательств обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время.

В последние годы получили распространение такие общественно опасные посягательства на личность несовершеннолетнего в сети, как кибербуллинг (cyberbullying) – подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придираться, провоцировать, донимать, терроризировать, травить. В молодежном сленге является глагол аналогичного происхождения — быковать.

Кибербуллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе).

Наиболее опасными видами кибербуллинга считаются киберпреследование — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также хеппислепинг (Happy Slapping — счастливое хлопанье, радостное избиение) — видеоролики с записями реальных сцен насилия. Эти ролики размещают в интернете, где их могут просматривать тысячи людей, без согласия жертвы. Начинаясь как шутка, хеппислепинг может закончиться трагически. Название «хеппислепинг» происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона.

Взрослые пока мало задумываются об опасностях обширной кибер-практики своих детей, хотя о последствиях буллинга реального приходится слышать часто: сообщения о травмах, нанесенных сверстниками, попытки суицидов и трагические смерти. Кибербуллинг остается невидимым, а нанесенный им ущерб — нераспознанным. Но вполне реальным, несмотря на виртуальность этой проблемы.

Встречается в виртуальной среде и так называемый буллицид – доведение ребенка до самоубийства путем психологического насилия.

2. Опасная для детей информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться на электронных ресурсах, содержащих материалы экстремистского и террористического характера.

Для сведения. Запрещается использование сетей связи общего пользования для осуществления экстремистской деятельности, на территории Российской Федерации запрещаются распространение экстремистских материалов, а также их производство или хранение в целях распространения. В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность (ст. 12, 13 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»).

Законом запрещены также возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения (ст. 1 Федерального закона «О противодействии экстремистской деятельности»).

3. Особую опасность представляют для незрелой психики несовершеннолетних электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.

Определить, особенно ребенку, сектантский ли сайт, который встретился ему в сети, очень трудно – иногда для того, чтобы понять, что этот сайт принадлежит секте, приходится проводить целые расследования. Как правило, это касается сайтов для родителей и их детей, сайтов про административные технологии в бизнесе, сайты по психологической консультации и проч. Подавляющее большинство лидеров сект любыми путями стремятся присутствовать в Интернете и рекламировать свою деятельность, предоставляя ложную информацию о себе. Главная проблема деструктивных сект в сети – это предоставление ложной информации. Попасть под негативное влияние секты через сайт очень легко – если ребенок читает в сети соответствующий материал, смотрит видео и фото-информацию, то он уже вступает во взаимодействие с вербовщиком секты, невольно участвует в психологической игре организаторов секты, нередко попадая от них в зависимость. Сектанты всегда вербуют новых адептов через интерес, так что если сайт интересен, кажется важным для несовершеннолетнего пользователя и весьма актуальным в его жизненных обстоятельствах – не исключено, что этот сайт может быть сектантским. Всегда надо проверять и перепроверять полученную информацию.

Для сведения. Вовлечение малолетних в религиозные объединения, а также обучение малолетних религии вопреки их воле и без согласия их родителей или лиц, их заменяющих, запрещены (ст. 3 Федерального закона от 26.09.1997 № 125-ФЗ «О свободе совести и о религиозных объединениях»). Запрещается также создание и деятельность религиозных объединений, цели и действия которых противоречат закону (ст. 6 указанного Федерального закона).

4. Доверчивость и наивность детей нередко используют в своих целях компьютерные мошенники, спамеры, фишеры. Несовершеннолетние нередко переходят по присланным им злоумышленниками ссылкам без подозрений, скачивают неизвестные файлы, которые могут оказаться вирусами или содержать незаконную информацию.

Недостаточно информированный об опасностях в сети ребенок может сообщить злоумышленнику номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и многое другое.

Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть в совершение антиобщественных, противоправных, в том числе уголовно-наказуемых деяний. При этом следует иметь в виду, что привлечение к уголовной ответственности взрослого лица за вовлечение несовершеннолетнего в совершение преступления не исключает уголовной ответственности и самого подростка в случаях, когда он достиг установленного уголовным законом возраста.

По мнению психологов, анонимность и отсутствие запретов освобождают скрытые комплексы (в первую очередь, связанные с тягой к насилию и сексуальностью), стимулируют людей переходить некоторые нравственные границы. Есть немало примеров, когда подростки используют сетевые возможности, чтобы досаждать людям, с которыми в реальной жизни их связывают неприязненные отношения. Злоумышленник в таком случае преследует жертву, направляя ей угрозы с помощью сетевых средств. Подобные факты зафиксированы и в отечественной правоохранительной практике. Сетевая среда способна оказывать определенное влияние и на психическое здоровье личности.

Известны случаи вовлечения подростков через Интернет:

– в действия, носящие оскорбительный (статья 130 УК РФ «Оскорбление») и клеветнический характер (статья 129 УК РФ «Клевета»);

– в экстремистскую деятельность (статья 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»; статья 282.1 «Организация экстремистского сообщества»; статья 282.2 «Организация деятельности экстремистской организации»; статья 239 «Организация объединения, посягающего на личность и права граждан»);

– в преступную деятельность по изготовлению и сбыту наркотических средств и психотропных веществ и склонению к их потреблению несовершеннолетних (статьи 228, 228.1, 230 УК РФ), незаконному обороту оружия, взрывных устройств и взрывчатых веществ (статья 222 «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств», статья 223 «Незаконное изготовление оружия»), сильнодействующих или ядовитых веществ в целях сбыта (ст. 234 УК РФ);

– в секс- и порнобизнес, включая незаконное распространение порнографических материалов и предметов (статья 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (статья 242.1), вербовку несовершеннолетних сверстников (сверстниц) в занятие проституцией (статья 240 «Вовлечение в занятие проституцией»; статья 241 УК РФ «Организация занятия проституцией») и другие виды преступлений.

Ребенку следует объяснить, что указанные общественно опасные деяния, независимо от того, совершаются ли они с применением традиционных способов и средств или с использованием информационно-телекоммуникационных сетей, уголовно наказуемы, в том числе для подростков, достигших установленного законом возраста уголовной ответственности (16 лет, а за отдельные виды преступлений – с 14 лет в соответствии со статьей 20 УК РФ).

Для сведения. Действия совершеннолетнего лица (достигшего 18-летнего возраста), вовлекшего, в том числе с использованием интернета или мобильной связи, несовершеннолетнего в совершение преступления или антиобщественного действия (в систематическое употребление спиртных напитков, одурманивающих веществ, в занятие бродяжничеством или попрошайничеством), склонившего ребенка или подростка к потреблению наркотических средств или психотропных веществ, уголовно наказуемы (статьи 150, 151, 230 УК РФ).

5. Пропаганда наркотиков, насилия и жестокости, суицидального поведения, абортов, самоповреждений может быть весьма опасной для неокрепшей детской психики. Ребенок на веру принимает многие сомнительные идеи, особенно если они грамотно изложены. Например, о том, как лучше покончить с собой или от приема каких таблеток «станет веселее», как без обращения к врачу избавиться от нежеланной беременности и т.д. Этим пользуется немало людей, использующих детей в корыстных и иных личных целях. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как криминальная, в том числе коммерческая эксплуатация ребенка.

Для сведения. Пропаганда насилия и жестокости, порнографии, в том числе в средствах массовой информации и рекламе, запрещена российским законодательством (ст. 4 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации", ст. 31, "Основы законодательства Российской Федерации о культуре" (утв. ВС РФ 09.10.1992 № 3612-1), ст. 5 Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе»).

В Российской Федерации запрещены также:

– распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров;

– пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также распространение иной информации, распространение которой запрещено федеральными законами (ст. 4 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации");

– производство и распространение книжной продукции, продукции средств массовой информации, распространение указанных сведений посредством использования информационно-телекоммуникационных сетей или совершение иных действий в этих целях (статья 46 Федерального закона от 08.01.1998 № 3-ФЗ (ред. от 06.04.2011) "О наркотических средствах и психотропных веществах").

За совершение указанных деяний установлена административная ответственность (ст. 6.13 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ).

Для сведения. В случаях, когда такая пропаганда носит признаки склонения несовершеннолетнего к потреблению наркотических средств и психотропных веществ, виновный, достигший шестнадцатилетнего возраста, привлекается к уголовной ответственности по статье 230 УК РФ, предусматривающей за такие действия наказание на срок от шести до двенадцати лет.

6. Помимо указанной выше информации в Сети есть немало сомнительных развлечений, таких как онлайн-игры, пропагандирующие секс, жестокость и насилие, требующие немалых финансовых вложений. Дети бывают вовлечены в азартные игры в сети.

Онлайн-игры играют значительную роль в жизни современных детей и подростков. Для многих они становятся важной составляющей повседневности, определяют стиль, круг общения, влияют на жизненные ценности (и сами становятся ценностью, а нередко и сверхценностью). В результате увлечения играми ребенок может сильно снизить успеваемость в школе, прекратить заниматься социально полезными видами деятельности, сократить до минимума время, проводимое с родными и реальными друзьями, полностью переключиться на виртуальные формы общения и досуга, то есть приобрести Интернет-зависимость, которую многие психологи склонны считать болезнью.

Особого внимания требует предупреждение влияния на установки личности ребенка распространенных в глобальных сетях игр с элементами насилия. Исследования показали, что жестокие игровые эпизоды нередко приводят к нарастанию агрессивности поведения несовершеннолетних. Очевидно, с развитием технологий указанная проблема будет только усложняться, поскольку компании–разработчики игр постоянно повышают качество соответствия игрового пространства реальности, а это ведет к возрастанию степени погружения личности в виртуальную среду.

В соответствии с п. 3 ст. 14 Закона об основных гарантиях прав ребенка в целях обеспечения безопасности жизни, охраны здоровья, нравственности ребенка, защиты его от негативных воздействий предусмотрено проведение экспертизы (социальной, психологической, педагогической, санитарной) предназначенных для детей: настольных, компьютерных и иных игр, игрушек и игровых сооружений. С учетом сложившейся в экспертной практике и закрепленных в законодательстве субъектов РФ критериев их безопасности для нравственного, психического здоровья и нормального развития детей среди несовершеннолетних не допускается распространение игр, в том числе компьютерных и электронных, и игрушек: 1) провоцирующих ребенка на агрессивные действия; 2) вызывающих у него проявление жестокости по отношению к персонажам игры, в роли которых выступают играющие партнеры (сверстники, взрослые) или сама сюжетная игрушка; 3) провоцирующих игровые сюжеты, связанные с безнравственностью и насилием; 4) вызывающих преждевременный и нездоровый интерес к сексуальным проблемам, не соответствующий возрастным потребностям ребенка; 5) провоцирующих ребенка на пренебрежительное или негативное отношение к расовым особенностям и физическим недостаткам других людей. Любого из указанных критериев в отдельности достаточно, чтобы признать игру (игрушку) вредной для здоровья и развития детей и подростков.

7. Психологами отмечается распространенность в среде пользователей, в том числе несовершеннолетних, случаев болезненного пристрастия к участию в сетевых

процессах, так называемой "Интернет-зависимости", проявляющегося в навязчивом желании неограниченно долго продолжать сетевое общение. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире.

Нередко несовершеннолетние настолько привязываются к виртуальному миру и своему вымышленному персонажу, что забывают обо всем остальном. Для подростков Интернет, как виртуальная среда иногда кажется даже более адекватной, чем реальный мир. Возможность перевоплотиться в некую бестелесную "идеальную личность" открывает для них новые ощущения, которые им хочется испытывать постоянно или все более часто.

Зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определённой деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр и интернет-зависимости. Специалисты отмечают, что в некоторой степени указанная зависимость близка к патологической увлеченности азартными играми, а ее деструктивные эффекты схожи с возникающими при алкоголизме и наркомании, однако, в отличие от последних, имеют нехимическое происхождение.

Таким образом, Интернет-зависимость (как вид нехимической зависимости) – это навязчивая потребность в использовании Интернета, сопровождающаяся социальной дезадаптацией и выраженными психологическими симптомами. Патология проявляется в разрушении обычного образа жизни, смене жизненных ориентиров, появлении депрессии, нарастании социальной изоляции. Происходит социальная дезадаптация, нарушаются значимые общественные связи.

Выделяется 6 основных типов интернет-зависимости с учетом того, к чему сформировалось пристрастие у конкретной личности: "киберсексу", виртуальным знакомствам, сетевым азартным играм, компьютерным играм или навязчивому перемещению по Web-узлам:

1) Навязчивый веб-серфинг — бесконечные путешествия по Всемирной паутине, поиск информации.

2) Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.

3) Игровая зависимость — навязчивое увлечение компьютерными играми по сети.

4) Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.

5) Пристрастие к просмотру фильмов через интернет, когда больной может провести перед экраном весь день не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.

6) Киберсексуальная зависимость — навязчивое влечение к посещению порносайтов и занятию киберсексом.

О клиническом феномене зависимости от игр и ПК (лудомания, игромания, гэмблинг) говорят с конца 1980-х годов, сначала за рубежом, теперь, по мере продвижения информационных технологий, и в России.

Основные признаки Интернет-зависимости: 1) чрезмерное, немотивированное злоупотребление длительностью работы в сети, не обусловленное профессиональной, учебной или иной созидательной деятельностью; 2) использование Интернета как преобладающего средства коммуникации; 3) создание и эксплуатация виртуальных образов, крайне далеких от реальных; 4) влечение к Интернет-играм и (или) созданию вредоносных программ (без какой-либо цели); 5) субъективно воспринимаемая невозможность обходиться без работы в сети

При появлении указанных выше признаков следует обратиться за медицинской (психологической и (или) психиатрической помощью), так как в запущенном состоянии Интернет-зависимость и игромания значительно хуже поддаются коррекции.

8. Опасность для детей представляют также социальные сети и блоги, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него деструктивной психологической и нравственно-духовной обработке.

Социальные сети стали пользоваться популярностью несколько лет назад, так как, во-первых, удовлетворяют потребность интернет-пользователей в коммуникациях и социализации, а, во-вторых, – открывают простор для творчества и самовыражения (функционал позволяет создавать и публиковать контент самостоятельно и без премодерации).

Пользователи социальных сетей (как всемирных, так и русскоязычных) могут общаться друг с другом в киберпространстве, выкладывать фотографии и видео, делиться со своими друзьями ссылками на интересный по той или иной причине контент, обмениваться виртуальными подарками и так далее. В Рунете наблюдался колоссальный рост активности пользователей благодаря социальным сетям Odnoklassniki.ru и Vkontakte.ru. В целом, с ростом популярности блогосферы и социальных сервисов Интернет вошел в новую, Web 2.0-эпоху, когда пользователи являются не столько потребителями информации, сколько её создателями, причем активными.

Массовость и бурный рост социальных сетей повлекли за собой и целый ряд негативных последствий, среди которых – появление новых форм киберпреступлений: от мошеннических махинаций и нарушений авторских прав до распространения детской порнографии, пропаганды педофилии, торговли детьми.

Злоумышленникам особенно легко искать своих несовершеннолетних жертв с помощью таких сайтов как «Вконтакте», «Одноклассники» и «Мой мир». Совершенно не стесняясь, педофилы создают свои группы и сообщества прямо в социальных сетях, выкладывают в открытый доступ фото и видео-материалы порнографического содержания.

На созданные несовершеннолетними пользователями в социальных сетях странички уже в течение 2-3 дней могут поступить как прямые непристойные предложения, так и сообщения от педофилов, входящих в доверие к детям и подросткам под видом сверстников и даже заводящих с ними дружеские отношения.

Безопасный поиск в сети Интернет

Поисковые системы, такие как http://www.yandex.ru/ и http://www.google.com, имеют механизмы, которые ограничивают попадание потенциально опасных веб-сайтов и сайтов с непристойным содержимым в результаты поиска.

Безопасный поиск в Google

Работая с поисковой системой Google, есть возможность включить функцию фильтрации результатов поиска. Для этого нужно перейти по ссылке http://www.google.com/preferences. На открывшейся странице установить флаг - Не показывать непристойные результаты.

В поисковой системе Google также можно включить защиту настроек безопасного поиска. Она позволяет защитить эти настройки паролем. Для того чтобы парольная защита работала, необходимо иметь учетную запись Google.

Безопасный поиск и дополнительные возможности Yandex.

Для включения фильтрации результатов поиска в системе Yandex необходимо в ссылке Настройки установить параметр Фильтрация страниц в значение Семейный поиск.

Компания Яндекс предлагает сервис Яндекс.DNS (http://dns.yandex.ru/). Это - служба, которая позволяет блокировать мошеннические сайты, сайты, распространяющие вредоносные программы, и ресурсы, не предназначенные для детей.

Существует два основных способа использования этой службы.

Первый из них применим в том случае, если для выхода в Интернет используется Wi-Fi-маршрутизатор. Настроив его в соответствии с инструкциями, размещенными на сайте, вы защитите от перехода на нежелательные сайты все домашние устройства. Это - настольные компьютеры, ноутбуки, мобильные телефоны, планшеты.

Второй способ заключается в настройке отдельных компьютеров и мобильных устройств. Соответствующие инструкции также приведены на сайте.

Еще одна возможность по повышению безопасности работы детей в Интернете заключается в использовании приложения Яндекс.Браузер. Это - веб-браузер от компании Яндекс, в функции которого входит оповещение о посещении опасных сайтов. Например, сайтов SMS-мошенников или ресурсов, распространяющих компьютерные вирусы. Кроме того, браузер поддерживает проверку загружаемых файлов средствами "Лаборатории Касперского", что является дополнительным фактором защиты.

Скачать установочный файл приложения можно, перейдя по адресу http://browser.yandex.ru/.

В нижней части окна настроек есть ссылка Показать дополнительные настройки. Она открывает список параметров, среди которых стоит обратить внимание на кнопку Настройки содержимого в разделе Защита личных данных. Щелчок по этой кнопке открывает окно, в котором можно заблокировать прием cookie-файлов. Такие файлы часто используются веб-сайтами для отслеживания предпочтений пользователя, и например, для показа контекстной рекламы, соответствующей этим предпочтениям.

Помимо вышеописанных средств настройки поисковых систем общего назначения, использования службы Яндекс.DNS и безопасного браузера

Яндекс.Браузер, безопасность детей в Интернете можно значительно повысить, если предложить им специальные детские поисковые службы.

Детские поисковые системы и каталоги

Основная ценность детских поисковых систем заключается в том, что в результатах поиска будут появляться только сайты, которые безопасны для детей. То есть использование таких поисковых систем решает проблему безопасного поиска. Обычно они не обладают столь же большим охватом материалов, который характерен для обычных поисковых систем. Но их ценность не в объеме материалов в поисковой выдаче, а в том, что поиск осуществляется по безопасным детским ресурсам.

1. Поисковая система http://kids.quintura.ru/ предназначена специально для детей. Главная особенность этой поисковой системы заключается в предложении слов, связанных с поисковым запросом. Эти наборы слов называют картами ассоциаций. Начать поиск можно как традиционным способом - введя поисковый запрос в строку поиска и нажав кнопку Найти, так и щелкнув по одному из подходящих слов.
2. Поисковая система http://agakids.ru представляет собой инструмент поиска по детским сайтам и подборку полезных ресурсов. Для начала поиска нужно ввести поисковый запрос в соответствующее поле. На странице результатов поиска можно, установив соответствующий переключатель под полем ввода запроса, изменить способ поиска. Кнопки Текст и Картинки позволяют, соответственно, искать текстовые материалы и изображения
3. Портал http://www.kinder.ru/ представляет собой каталог детских сайтов, составленный вручную. Для поиска по каталогу можно воспользоваться строкой, которая расположена в верхней части страницы. Искать можно и другим способом: переходя в разделы, соответствующие интересующим ребенка категориям.

Безопасность ребенка в социальных сетях

В социальных сетях присутствуют не только порядочные пользователи, но и люди, которые способны принести ребенку вред. Как повысить безопасность ребенка, который пользуется социальными сетями?

Радикальное решение проблемы заключается в том, чтобы запретить ребенку пользоваться этими службами. Но, учитывая распространенность и популярность социальных сетей, учитывая желание ребенка общаться со сверстниками, такое решение трудноосуществимо на практике. Столкнувшись с полным запретом социальных сетей на домашнем компьютере, ребенок, вероятнее всего, обойдет этот запрет - например, пользуясь социальной сетью с компьютера кого-нибудь из сверстников. И пользуясь, естественно, совершенно бесконтрольно.

Гораздо лучше, во-первых, ознакомить ребенка с основными правилами безопасного поведения в социальных сетях, разъяснить ему возможный риск. Во-вторых - настроить вместе с ним параметры безопасности и конфиденциальности его учетной записи. И, в-третьих - контролировать его работу в социальных сетях с помощью специального программного обеспечения.

Как результат, ребенок, овладевший приемами безопасной работы, понимающий возможные риски и, кроме того, пользующийся социальной сетью под

вашим присмотром, будет защищен от возможных опасностей гораздо лучше, чем тот ребенок, которому запрещают работать в социальных сетях. Рано или поздно он все равно с ними столкнется, и лучше будет, если его знакомство с социальными сетями произойдет правильно и с вашим участием.

Общие правила безопасности

Залог безопасности ребенка в социальных сетях - доверительные отношения с родителями и исполнение некоторых правил. Эти правила нужно разобрать вместе с ребенком.

1. **К выбору социальной сети нужно подходить ответственно**. Не следует регистрироваться во всех найденных социальных сетях. Перед регистрацией нужно собрать сведения о социальной сети, прочесть правила. Отзывы желательно искать на независимых интернет-ресурсах. Например, популярные социальные сети **Facebook**, **ВКонтакте**, **Одноклассники** способны быть достаточно безопасными для ребенка при выполнении правил.

2. **При регистрации в социальной сети нужно использовать сложный пароль**. Это - залог того, что учетную запись не взломают. В данном случае взлом учетной записи опасен, во-первых, тем, что злоумышленник может узнать конфиденциальные данные ребенка. Это могут быть сведения о городе проживания, фотоальбомы, скрытые от общего просмотра. Во-вторых, контроль над учетной записью перейдет злоумышленнику, и он сможет от имени ребенка совершать какие-либо действия. Если при регистрации в социальной сети используется система восстановления пароля с указанием секретного вопроса и ответа, убедитесь, что ответ на вопрос сложно узнать или подобрать. Иначе взлом учетной записи может быть осуществлен через подбор ответа.

3. **Не рекомендуется использовать при регистрации в социальной сети возможность указания данных почтового ящика ребенка**. Это может привести к неконтролируемому оповещению о его учетной записи тех, с кем когда-либо велась переписка. Как результат, будет сложнее управлять списком друзей ребенка.

4. **Нельзя никому сообщать данные для входа в учетную запись в социальной сети**. В частности, пароль нужно держать в секрете от всех. Мошенники иногда рассылают пользователям социальных сетей электронные письма, в которых под разными предлогами просят сообщить пароль. Например, письмо может выглядеть так, как будто оно отправлено от имени администрации сайта или от имени интернет-провайдера. Ни администрация социальной сети, ни провайдер никогда не попросят о подобном. Такие сообщения следует игнорировать.

5. **После завершения работы в социальной сети нужно выполнять процедуру выхода**. Для этого служит команда **Выход** или другая подобная. Она обычно расположена в правой верхней области окна. Если не выйти из учетной записи, а, например, просто закрыть окно браузера, доступ к учетной записи могут получить посторонние. Особенно это справедливо при работе с учетной записью социальной сети на чужом компьютере.

6. **Очень внимательно подходите к выбору друзей в социальных сетях.** Рассматривайте каждую кандидатуру вместе с ребенком. Для наибольшего уровня безопасности следует добавлять в друзья только тех пользователей, которых вы знаете в реальной жизни. Учителя, одноклассники, родственники - вот те люди, с которыми можно установить дружеские отношения в социальных сетях. С ними

можно безопасно общаться. К любым другим пользователям, особенно к тем, которые сами предлагают добавиться в друзья, следует относиться с большой осторожностью. Не зная человека лично, вы не можете быть уверены в том, что он - тот, за кого себя выдает.

7. **Воспользовавшись настройками учетной записи, ограничьте возможность связи с ребенком посторонних**. Это позволит ребенку получать сообщения только от тех людей, которые, с вашим участием, добавлены в список его друзей. От посторонних ребенок может получить сообщение любого содержания, с любыми изображениями или видеоклипами. Если подобные настройки не предусмотрены, предложите ребенку не открывать сообщения от незнакомцев без вашего участия.

8. **Расскажите ребенку о том, что переходить по ссылкам, которые кто-либо отправил ему в сообщении, опасно**. Эти ссылки могут вести на сайты, распространяющие вредоносные программы. Если ссылку отправил, например, одноклассник в ходе беседы - по такой ссылке можно перейти. Если же сообщение со ссылкой пришло неожиданно, прежде чем переходить по ней, следует уточнить у автора сообщения, куда она ведет. Если ответа получить не удается, возможно, учетная запись автора сообщения взломана и сообщение отправил мошенник. Опасно скачивать и открывать файлы, приходящие в сообщениях.

9. **Объясните ребенку, что он не должен никому сообщать каких-либо личных сведений о себе**. К таким сведениям относятся номер телефона, домашний адрес, время начала занятий в школе и другие подобные. Эти данные могут быть использованы злоумышленниками. Такие сведения не следует публиковать даже в том случае, если опубликованная запись предназначена только для друзей. Злоумышленник, взломавший учетную запись одного из друзей, может получить к ним доступ.

10. **Попросите ребенка с осторожностью относиться к приложениям, которые можно устанавливать в социальных сетях**. Обычно это игры или другие развлекательные приложения. Они могут собирать данные о пользователях, либо, если они созданы злоумышленниками, использоваться для взлома учетных записей. Заранее сказать, окажется ли опасным приложение, нельзя. Надежнее всего не пользоваться ими.

11. **Расскажите ребенку о том, что если он заметил что-то странное в своей учетной записи, то пароль к ней нужно немедленно сменить**. На взлом учетной записи могут указывать следующие признаки: исчезли какие-нибудь фотоснимки, или, наоборот, появились новые, которых никто не выкладывал, на стене появились неожиданные записи.

Пользуясь этими рекомендациями и ознакомив с ними ребенка, вы значительно повысите уровень его безопасности в социальных сетях. Но главное в безопасности ребенка, который работает в Интернете - доверительные отношения с родителями.

«Группы смерти» в социальных сетях: как родителям распознать опасное увлечение ребенка

Уже не первый год в социальных сетях детей вовлекают в «суицидальный квест» - виртуальную игру, финалом которой становится самоубийство. Тысячи страниц в интернете наполнены фотографиями, видео- и аудио-контентом, убеждающим, что жизнь – бессмысленна, любовь – безответна, предательство – обратная сторона дружбы, и только смерть имеет значение.

Сотни людей, скрытых под фальшивыми именами, выдают нашим детям задание за заданием, внушая им уверенность в том, что по-настоящему счастливое существование откроется только в «тихом доме» – месте, куда эти наставники «пропишут» их после суицида.

Инструкция для родителей по обнаружению опасных сигналов на страницах социальных сетей

Для начала, необходимо обнаружить все возможные страницы, которые завел ваш ребенок в социальных сетях (это может быть одна страница, а может быть и больше). Если вам неизвестно, в каких именно социальных сетях присутствует ваш ребенок, попробуйте ввести его имя, фамилию и город, в котором вы проживаете, в поисковой строке Яндекса https://www.yandex.ru/ или Google https://www.google.ru/.

Если поиск через поисковые системы не дал результатов, то изучите те устройства, с которых возможен выход в интернет для вашего ребенка.

Ребенок может посещать социальные сети с компьютера или любого устройства, которым пользуются все члены вашей семьи, с личного мобильного телефона либо планшета.

Если у вас есть доступ к устройствам, которыми пользуется ребенок, вы можете просмотреть посещенные им страницы, зайдя во вкладку «История» в интернет-браузере (Firefox, Opera, Explorer , Яндекс.Браузер, Google Chrome и т.п.). Однако, если ребенок знает об этой возможности и не хочет, чтобы вы видели страницы, которые он посещал, история, скорее всего, будет очищена, либо ребенок будет пользоваться браузером в режиме «инкогнито». Но это также может послужить и сигналом внимательнее присмотреться к тому, что делает ваш ребенок в интернете.

Ребенок может общаться со злоумышленниками с помощью таких ресурсов как «ask.fm» http://ask.fm/ , инстаграм https://www.instagram.com/ , а также мессенджеров Viber http://www.viber.com/ru/ , whatsapp https://www.whatsapp.com/ или по Scype https://www.skype.com/ru/ . Вызывающие тревогу признаки можно, в принципе, обнаружить в любой социальной сети, в которой имеет страницу ваш ребенок: от Моймир@mail.ru https://my.mail.ru/my/welcome до «Одноклассников» https://ok.ru/.

Необходимо понимать, что основной площадкой для вовлечения в «игру», доводящую до самоубийства, является социальная сеть «ВКонтакте», однако этот «квест» распространяется и в других социальных сетях. Так, в 2017 году для вовлечения в «игру» стал активно использоваться инстаграм, поэтому на активность ребенка именно в этих социальных сетях следует обратить особое внимание.

Страница пользователя «ВКонтакте» состоит из нескольких **разделов (вкладок)**, в каждом из которых могут быть обнаружены признаки вовлеченности в

субкультуру, пропагандирующую суицид, или воздействия конкретных пользователей, склоняющих к самоубийству.

Раздел «Стена»

«Стена» страницы – это то, что вы можете видеть, прокручивая вниз ленту страницы ребенка.

Стена может быть ***открытой*** (в настройках пользователь указал, что основную информацию с его страницы видят все пользователи) и тогда вы сможете увидеть то, что ребенок пишет на своей странице от своего имени или какими записями со страниц других пользователей или сообществ в социальной сети он посчитал важным поделиться на своей странице (то есть сделал *репост*).

Помимо записей на «стене», обратите внимание:

- ✓ ***на «статус»*** (слова, которые находятся сразу под ником (именем) пользователя). Вы не увидите реальный «статус» ребенка, если в этот момент он слушает музыку, транслируя ее на свою страницу. Обратите внимание на «статус» позже, когда название композиции исчезнет. Тревожный знак, если в статусе присутствуют:
  - номера (ребенку может быть присвоен номер в списке тех, кто совершит суицид);
  - даты (особенно, если на протяжении нескольких дней вы видите «обратный отсчет»)
  - определенные слова, которые сопровождаются значком решетка # (так называемые «хештеги», например, #f57 #f58 #d28 #морекитов #четыредвадцать #тихийдом);
  - символы, изображающие могильные кресты;
  - символы китов или слова «грустный кит», «киты плывут вверх» и т.д.
- ✓ ***на дату рождения*** (пользователь может либо прибавить себе лет, чтобы спокойно заходить на страницы, отмеченные знаком 18+, либо не указывать год своего рождения или по каким-либо причинам указать, что он младше своего возраста);

- ✓ на указанное ребенком ***«место работы»*** (заполняется во вкладке «карьера». Как правило, подростки указывают в качестве «места работы» какой-либо паблик, то есть сообщество, где они могу быть, например, администраторами (привлекаться для размещения определенного контента /картинок, аудио- и видеозаписей, текстов и т.п./) либо просто ассоциируют себя с данным пабликом или страницей). Перейдите по ссылке, указанной как «место работы» и внимательно изучите содержание открывшейся страницы;
- ✓ на ***«контактную информацию»*** (здесь может быть указан домашний либо какой-либо иной адрес, мобильный телефон, дополнительный телефон, веб-страница в качестве «личного сайта», скайп, а также ссылка на страницы ребенка в других сервисах: инстаграме / instagram.com /, фейсбуке /facebook.com/ или твиттере / twitter.com /. Если номер телефона высвечивается как ссылка, кликните на нее, возможно, так вы обнаружите еще одну страницу ребенка.

Раздел «Фотографии»

Под основной информацией вы можете видеть *горизонтальную ленту*, где слева направо указывается количество друзей, подписчиков, фотографий, отметок или видеозаписей.

Раздел «Фотографии» заслуживает особого внимания. В ленте под основной информацией может быть указано незначительное количество фотографий – в эту статистику идут только те фото, которые пользователь выставлял на своей странице как свой аватар или выкладывал у себя на стене. Они останутся в альбомах «Фотографии со страницы» и «Фотографии на стене», если в дальнейшем пользователь поменял фото аватара или удалил со стены, но не удалил из этих альбомов. Однако, на самом деле, на странице пользователя бывает значительно больше фото в виртуальных альбомах, и значительное их число может быть скрыто в альбоме «Сохраненные фотографии», который нужно еще поискать.

Для того чтобы ознакомиться со всеми фотографиями ребенка, кликните на горизонтальной ленте под основной информацией на цифру с фотографиями и вы перейдете на вкладку *«Альбомы»*. Также вы можете попасть на эту вкладку, если кликните на фотографию аватара и далее слева внизу перейдете по ссылке «Фотографии со страницы…», а затем зайдете в раздел «Все фотографии …».

Уделите внимание всем фотографиям в альбомах, **особенно – в альбоме «Сохраненные фотографии», если он открыт, так как с 2017 года сайт «ВКонтакте» по умолчанию скрыл этот альбом, если иное не отмечено пользователем в настройках приватности.** Ребенок, который много времени проводит в пабликах, пропагандирующих суицид, либо является администратором этих сообществ, обычно сохраняет в этом альбоме много фотографий с суицидальным содержанием *(контентом)*. Даже если вам кажется, что в этом альбоме, на первый взгляд, нет ничего подобного, досмотрите все сохраненные фотографии до конца (их бывает много, от 5 до 10 тысяч (иногда и больше), и очень часто фото с порезами, виселицами, лезвиями и таблетками перемежается вполне нейтральными картинками).

Тревожными сигналами являются:

- ✓ картинки с мемами (короткие высказывания или картинки, которые мгновенно становятся популярными). На картинках – слова «одиночество», «прыгай», «боль», «смерть», «тоска», «вешайся», «достали», фоном для которых служат могилы, виселицы, ножи, лезвия, таблетки либо многоэтажные дома, мосты, рельсы, поезда, безрадостные пейзажи, серое небо, открытые окна многоэтажек и т.д.
- ✓ -подписи к фотографиям, дискредитирующие общечеловеческие ценности, например:

«Я перестал верить в любовь»
«Влюбленных много, счастливых мало»
«Счастливые люди не курят»
«Скажи, как мне быть жизнерадостным?»
«Пора завязывать с дерьмом. Я про людей»
«Жизнь разносилась как туфля, из потолка растет петля»
«Недосып как стиль жизни»
«Тебя предадут те, кому ты больше всего веришь»
«Нас только трое: я, мое одиночество и бухло»
«Ничего не радует»

«Коллективный суицид. С собой покончили: Вера, Надежда, Любовь».

«Каждый был хоть однажды настолько одинок или расстроен, что думал о суициде...»

«Любовь - медленный суицид»

- ✓ изображения атрибутов БДСМ (психосексуальная субкультура, включающая ролевые игры в господство и подчинение): плети, наручники, люди в соответствующей одежде;
- ✓ изображения китов;
- ✓ изображения оккультных символов: пентаграмм, числа 666 и т.п.;
- ✓ изображение знака со словами «ОНО» и «АД» (этот знак был разработан как символика «суицидального квеста»);
- ✓ изображение часов, показывающих время 4:20;
- ✓ изображения пачек с сигаретами с акцентом на надписи «курение убивает» (часто сопровождаются четным числом роз);
- ✓ избражения подростков-самоубийц Рины Паленковой, псковских «Бони и Клайд»;
- ✓ изобржения порезанных рук, вскрытых вен, ссадин, гематом, проколотых булавками губ и т.д.

Раздел «Друзья» и «Подписчики»

Обратите внимание на аватары (фотографии) «друзей», особенно на те, где вместо фотографии изображен символ либо герой аниме. Организаторы и участники суицидальных пабликов часто берут себе такие имена и фамилии как: Августина, Октябрина, Милена, Мирон, Фридрих, Ада, Рина, Сетх, Рейх, Лис, Кот, Кит, Тян, Енот, Шрам, Штерн, Холод, Камболина и т.д.

Просмотрите тех, кто *подписан* на страницу вашего ребенка (по каким-то причинам ваш ребенок предпочел не добавлять этих пользователей в «друзья» и они остались в «подписчиках»). Нередко число друзей может быть в пределах 20, но число подписчиков превышает сотню, что (в совокупности с анализом их аваторов и содержания страниц) может свидетельствовать о том, что ребенок «раскручивается» как потенциальный «суицидник».

Если вы заметили перечисляемые здесь тревожные признаки на страницах известных вам друзей или одноклассников вашего ребенка, постарайтесь сообщить об этом его родителям.

Раздел «Интересные страницы»

В этой вкладке вы увидите список групп (сообществ, пабликов), на которые подписан ваш ребенок в социальной сети. Здесь же находятся страницы людей, на которых ребенок подписался сам, но они не добавили его «в друзья». Имеет значение порядок расположения «интересных страниц» в расположенной слева вкладке: страницы, которые ребенок посещает чаще всего, попадают в верхнюю часть списка.

Обратите внимание на страницы:

- ✓ со словами из списка с хештегами, приведенного выше (тихий дом, мертвые души, f57, f58, море китов и т.д.)

- ✓ с изображением сатанистских символов и знаков (кресты, «звезды», а также знак с использованием слов «ОНО» и «АД»);
- ✓ с названиями, включающими слово «Suicide», в том числе, написанным с ошибками («suecid», «suicid» и т.д.), а также с названиями с использованием иероглифов, иврита, арабской вязи, санскрита, экзотических шрифтов (примеры: אבימאתך אנו , νεκρές ψυχές, ƎRRØR, のサンドイッチ サーモン) и т.п.;
- ✓ с цифрами вместо названия;
- ✓ со словами «смерть», «мертвый», «суицид», «подростки», «грусть», «выход», «ад», «кит», «кот», «лис», «4:20», «разбуди», «шрамы», «порезы», «вены», «кровь» и т.д.;
- ✓ -посвященные книгам «50 дней до моего самоубийства», «Сказка о самоубийстве» либо фильмам (например, «Зал самоубийц»);
- ✓ посвященные подросткам-самоубийцам.

Группы могут быть ***открытые*** (вступить в них может любой желающий), ***закрытые*** (для вступления в группу необходимо подать заявку) или ***частные*** (в такие группы «вход» возможен только по приглашению администратора). **На закрытые и частные группы следует обратить особое внимание – именно в таких группах, как правило, начинает вестись планомерная обработка по алгоритмам «суицидального квеста».**

Кроме того, тревогу должны вызывать (в совокупности с другими признаками) группы, в которых есть ссылки на дополнительные страницы под названиями *«убежище», «бункер бана» или «бункер бункера».* Это означает, что создатели отдают себе отчет, что их деятельность противоречит законодательству и сообщество может быть заблокировано, для чего сразу же создается пустая страница, в которую «перетекут» подписчики из основной группы.

Немаловажно, что суицидальный контент может скрываться под внешне нейтральными, безобидными названиями типа «радость моя», поэтому перейдите к содержанию и просмотрите его.

Чтобы увидеть новости, которые получает ваш ребенок «его глазами», нажмите на плашку «Новости» справа от надписи «Друзья» на одноименной вкладке.

Что нужно делать родителям при обнаружении на страницах детей «групп смерти»

Подозревая, что ребенок заинтересовался нежелательным контентом, проверяйте историю посещения ресурсов через браузер, но только когда ребенок этого не видит. Между прочим спрашивайте, на каких соцсетях он любит больше «тусоваться» и где бывают его сверстники. Так вы узнаете, чем ваш ребенок дышит, и проявите заинтересованность жизнью подростка, что для его эмоционального равновесия на данный момент важно.

Если ребенок истерит, скажите спокойно: «Почему ты так со мной поступаешь, я же себя с тобой так не веду». Ребенок нуждается в доверительных отношениях, ведь он в таком возрасте чувствует себя одиноким в этом «враждебном» мире.

Потому добавьте: «Я тебе доверяю, не обижай меня». Не задавайте вопросов — после искренности и любви, сквозящих в ваших словах, ребенок начнет открываться сам, пусть и не с первого раза.

Вместо дежурного «Как дела в школе?» спросите: «Тебе нравится твой класс? Твой учитель? Почему?» Вместо «Что ты сегодня ел?» — «Тебе понравился школьный обед? Чем именно?» Призыв к чувствам ребенка заставляет его давать развернутые ответы, а не «Все ок», «Да» или «Нет» — так вы узнаете о его эмоциональном состоянии, плюс ребенок, поняв (после нескольких дней), что вам важны его чувства, будет готов к вашим вопросам о любовных и дружественных отношениях, страхах и разочарованиях в жизни.

Что не нужно делать родителям при обнаружении на страницах у детей «групп смерти»

Требовать от ребенка пароль от соцсетей или просить показать его сообщения — это вызовет обиду и гнев подростка за то, что родители нарушают его личное пространство, которое в этом возрасте — главная психологическая потребность.

Употреблять фразы (даже в ссоре): «Из-за тебя у меня болит голова», «Своим поведением ты доведешь меня до больницы», «Как тебе не стыдно, ты мать довел до слез!» и т. п. Они вызывают злость у ребенка на самого себя, ведь на самом деле он любит своих родителей. В результате возникает аутоагрессия, которая подталкивает ребенка на нанесение физического вреда себе.

Лезть в душу, задавая вопросы, которые в вашей семье раньше не практиковались: «Как дела на личном фронте?», «У тебя уже был секс с этой девочкой?» и т. п. Во-первых, ребенок постесняется откровенничать и закроется. Во-вторых, если раньше подобные темы не поднимались в семье, подросток начнет подозревать, что за ним началась слежка. Поэтому станет еще больше «шифроваться» — закрывать свои странички от других пользователей, уходить как можно на более продолжительный период из дома, и вам будет труднее понять причину изменений в его поведении.

Первоочередные меры для повышения безопасности при использовании сети Интернет

- Регулярно скачивайте обновления для программного обеспечения.
- Установите антивирусное и антишпионское программное обеспечение.
- Установите фильтр (например, Интернет-Цензор).
- Установите спам-фильтр.
- Не открывайте писем от пользователей, которых вы не знаете.
- Лучший способ защиты детей - правильное воспитание.

Все то, чему вы учите своего ребенка, вы должны подкреплять собственным примером, иначе от обучения будет мало пользы.

Помните, что правильное воспитание - залог хорошего будущего ребенка. Для лучшего взаимопонимания и устранения возможных недоразумений, лучше сразу расставить все точки над «и», установить некоторые ограничения для самостоятельного выхода в Интернет. Обсудите это с детьми, чтобы они понимали необходимость подобных запретов, тогда вместе вы обязательно

можете сделать прогулки ребенка в сети наиболее безопасными. Составьте список правил работы детей в Интернете и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без ограничений.

Рекомендательный список Web-сайтов и порталов для ознакомления родителями и детьми

Центр безопасного Интернета в России (режим доступа: http://www.saferunet.ru/) – Сайт содержит рекомендации о поведении детей различных возрастов в сети Интернет. Эти рекомендации будут полезны родителям, которые хотели бы оградить своих детей от преждевременного знакомства с некоторыми особенностями современной сети Интернет.

Защита детей от вредной информации в сети Интернет (режим доступа: http://www.internet-kontrol.ru/) - Детские поисковики / Настройка системы контекстной фильтрации "Родительский контроль" в различных версиях Windows / Статьи о детях, компьютерах и Интернете / Новости мира Интернета / Что необходимо знать родителям, оставляя детей наедине с мировой паутиной / Способы борьбы с вредной информацией в разных странах.

Безопасность детей в Интернете - Российский офис Microsoft в рамках глобальных инициатив Microsoft (режим доступа: http://www.ifap.ru/library/book099.pdf) - Информация для родителей и детей: памятки, советы, рекомендации для различных возрастных особенностей детей.

Nachalka.com - Сайт предназначен для учителей, родителей, детей, имеющих отношение к начальной школе (режим доступа: http://www.nachalka.com/bezopasnost)

Дети России он-лайн / (режим доступа: http://detionline.com/) - Ресурсы для детей и родителей: исследования, образовательные проекты, журналы о безопасном поведении детей в сети Интернет.

Дети он-лайн /Линия помощи (режим доступа: http://detionline.com/helpline/about) -Бесплатная всероссийская служба телефонного и он-лайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи.

Фонд развития Интернет (режим доступа: http://www.fid.su/) - Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности сети Интернет.

Лига безопасного Интернета (режим доступа: http://www.ligainternet.ru/inform-about-illegal-content) - Горячая линия по приёму сообщений о противоправном контенте в сети Интернет. Также на сайте имеется возможность оставить на портале свое сообщение о противоправном интернет-контенте анонимно.

Дети в Интернете (режим доступа: http://detionline.com/mts/about) - Комплекс образовательных мероприятий, объединяющий в себе интерактивные выставки и серию обучающих уроков для младших школьников. Брошюры по безопасному поведению в интернете.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

О РАЗМЕЩЕНИИ НА ИНФОРМАЦИОННЫХ СТЕНДАХ, ОФИЦИАЛЬНЫХ ИНТЕРНЕТ-САЙТАХ И ДРУГИХ ИНФОРМАЦИОННЫХ РЕСУРСАХ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ И ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ УПРАВЛЕНИЕ В СФЕРЕ ОБРАЗОВАНИЯ, ИНФОРМАЦИИ О БЕЗОПАСНОМ ПОВЕДЕНИИ И ИСПОЛЬЗОВАНИИ СЕТИ "ИНТЕРНЕТ"

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (далее - методические рекомендации).

Методические рекомендации направлены на качественное повышение уровня информационной деятельности общеобразовательных организаций и органов, осуществляющих управление в сфере образования, в части информирования учащихся, их родителей (законных представителей) и педагогических работников об основных аспектах информационной безопасности.

Методические рекомендации позволят общеобразовательным организациям и органам, осуществляющим управление в сфере образования, актуализировать уже используемые и размещенные информационные материалы, так и подготовить их в случае их отсутствия с учетом лучших практик и рекомендаций.

В рамках методических рекомендаций рассматриваются следующие инструменты:

1. информационные стенды;

2. официальные интернет-ресурсы;

3. средства массовой информации (школьные газеты, педагогические издания и другие).

Информационные стенды

На информационных стендах в общеобразовательных организациях, расположенных в фойе учреждений и в кабинетах, оснащенных персональными устройствами для выхода в сеть "Интернет", рекомендуется разместить информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.

В приложении N 1 к методическим рекомендациям представлен образец памятки для размещения на информационных стендах.

Средства массовой информации

В средствах массовой информации, ориентированных на обучающихся, рекомендуется в течение учебного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности, а также различные памятки общего характера.

В средствах массовой информации, ориентированных на педагогическую

общественность, рекомендуется в течение календарного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности как несовершеннолетних, так и общеобразовательных организаций, а также различные памятки, обзоры нормативно-правового регулирования данной сферы и информацию о актуальных мероприятиях и событиях в данной сфере.

В ходе проведения Единого урока по безопасности в сети "Интернет" рекомендуется обеспечить выпуск тематического выпуска средства массовой информации либо серии публикаций, среди которых рассмотреть организованные мероприятия для обучающихся, их родителей (законных представителей) и педагогической общественности.

Официальные Интернет-ресурсы

Общеобразовательным организациям рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

N	Раздел/подраздел	Формат представления материалов	Содержание материалов
1.	Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся	Копии документов в формате *PDF	Размещаются копии документов, т.е. сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие.
2.	Нормативное регулирование	Копии документов в формате *PDF	Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на

			соответствующие документы на сайтах органов государственной власти.
3.	Педагогическим работникам	Текст на странице сайта Копии документов в формате *PDF	Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников.
4.	Обучающимся	Текст на странице сайта	Размещается информационная памятка (приложение N 2) и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся.
5.	Родителям (законным представителям) обучающихся	Текст на странице сайта	Размещается информационная памятка (приложение N 3).
6.	Детские безопасные сайты	Текст на странице сайта	Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов.

Органам, осуществляющим управление в сфере образования, рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

Приложение N 1

ПАМЯТКА
ДЛЯ ОБУЧАЮЩИХСЯ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;
2. Пользуешься Интернет-источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;
5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

Приложение N 2

ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ДЛЯ РАЗМЕЩЕНИЯ НА ОФИЦИАЛЬНЫХ ИНТЕРНЕТ-РЕСУРСАХ

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;

2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;

4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать

вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то

злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего

труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!

Приложение N 3

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:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

3. К информации, запрещенной для распространения среди детей, относится:

4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

5. 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;

6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

8. оправдывающая противоправное поведение;

9. содержащая нецензурную брань;

10. содержащая информацию порнографического характера.

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

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. 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;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4. 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

1. 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.

2. 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.

3. 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)

4. 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).

5. 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

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. 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.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. 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

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.

9. 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.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. 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.

13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. 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

1. 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).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. 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.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. 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.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. 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.

10. 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.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. 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.

Список использованных источников

1. Агитова С. Защита детей от ситуаций, угрожающих их жизни, здоровью и развитию / С. Агитова // Народное образование. – 2015. – № 5. – С. 57 – 67

2. Ковалева И. Защитить глаза от компьютера / И. Ковалева // Здоровье школьника. – 2015. – № 9. – С. 50 – 51.

3. Помощь рядом [Электронный ресурс]: сайт. – Режим доступа:https://pomoschryadom.ru/

4. Порваткина И. Социализация личности ребёнка / И. Порваткина // Современная библиотека. – 2015. – № 4. – С. 36 – 44.

5. Постановление Главного государственного санитарного врача РФ от 3 июня 2003 г. N 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» [Электронный ресурс]: сайт // Система ГАРАНТ. – Режим доступа: http://base.garant.ru/4179328/

6. Разбираем Интернет [Электронный ресурс]: сайт. – Режим доступа: http://www.razbiraeminternet.ru/.

7. Силаев, А. А. Гигиенические требования к организации работы детей и подростков с компьютером / А. А. Силаев, Л. Ю. Кузнецова, Н. Д. Бобрищева-Пушкина, О. Л. Попова // Практика педиатра. Гигиена. – 2009. – октябрь. – С. 27-30.