



ОПАСНОСТИ ВИРТУАЛЬНОГО МИРА

Памятка для родителей
по безопасному использованию детьми
сети Интернет

Махачкала
2021

Содержание

Введение.....	3
Опасности виртуального мира.....	4
Рекомендации по безопасному использованию детьми сети Интернет.....	5
Возраст 5—8 лет.....	5
Возраст 9—12 лет.....	7
Возраст 13—17 лет.....	8
Что делать, если ребенок все же столкнулся с интернет-угрозами?.....	9
Какие действия необходимо совершить в случае, если ребенок столкнулся с интернет-рисками?.....	10
Словарь интернет-терминов.	11
Список рекомендуемых источников.	14

Введение

«Ребенок дома, за компьютером — значит все в порядке, он в безопасности» — так считают многие родители. И ошибаются. Опасность детей подстерегает не только на улице, но и дома — за монитором компьютера.

Одна из опасностей Интернета — кибербуллинг — запугивание, психологический и физический террор, до чувства страха и подчинения. В Интернете насилие такого рода не редкость, как и различный агрессивный и нежелательный контент, мошенничество, сексуальное домогательство.

Так, посредством интернет-ресурсов «Скайп» и «ВКонтакте» детей затягивают на страницы групп «#Море китов», «#F58», «#F57», «#Киты», «#d28», «#Тихий дом», «#хочувигру», «#рина», «#разбуди меня в 4.20», «#Whales swim up», в которых размещены картинки, цитаты, стихи депрессивного содержания, подводящие подростков к мысли о самоубийстве.

Но киберпространство не только источник угроз, оно открывает и большие возможности для общения и саморазвития. Важно, чтобы мир Интернета не стал единственным увлечением ребенка. Уход ребенка в виртуальный мир может обозначать отсутствие какого-либо хобби, непонимания в отношениях с родителями, занятость родителей на работе и т. д. Но каким бы увлекательным не был виртуальный мир, общение с друзьями, родителями должно оставаться для ребенка важнейшей составляющей в формировании и становлении его как личности.

Чтобы Интернет приносил пользу, а не вред, родителям необходимо научить детей правилам безопасного пользования сетью Интернет так же, как не переходить дорогу на красный свет светофора.

Данная памятка содержит рекомендации по безопасному использованию сети Интернет детьми в соответствии с их возрастными особенностями и интересами. Также в издании приведен словарь наиболее часто встречающихся в Интернете терминов. Издание адресовано родителям для дальнейшего их применения в определении правил использования детьми Интернета.

Опасности виртуального мира

Все большее количество детей получает возможность выхода в Интернет. На сегодняшний день он предоставляет огромное количество неконтролируемой информации. В связи с тем, что возраст детей, с которого они начинают работать в Интернете, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители? Следует понимать, что, подключаясь к сети Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Во Всемирной паутине существует множество интернет-угроз:

- суицид-сайты;
- сайты-форумы потенциальных самоубийц;
- наркосайты (интернет пестрит новостями о «пользе» употребления разного «зелья», рецептами и советами его изготовления);
- сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
- сайты порнографической направленности;
- сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);
- сайты, пропагандирующие экстремизм, насилие и девиантные формы поведения, прямые угрозы жизни и здоровью подростков от незнакомцев, предлагающих личные встречи, различные виды мошенничества;
- секты (виртуальный собеседник может повлиять на мировоззрение подростка).

Чтобы обезопасить юного пользователя от возможных бед в виртуальном пространстве, необходимо совместно с ребенком определить правила посещения Интернета, прийти к соглашению по его использованию!!!

Все сайты доступны для просмотра в Интернете без ограничений. Часто случается, что просмотр этих страниц даже не зависит от ребенка (на многих сайтах отображаются всплывающие окна, содержащие любую информацию). К сожалению, это реалии времени, с которыми необходимо считаться.

Рекомендации по безопасному использованию детьми сети Интернет

Ваши дети растут, а, следовательно, меняются их интересы в связи с этим представляем вам несложные практические советы по безопасному использованию детьми сети Интернет в соответствии с их возрастными особенностями и интересами.

Указанные рекомендации применимы для всех электронных устройств, имеющих выход в Интернет, к которым у ребенка есть доступ.

Возраст 5-8 лет

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями.

В Интернете дети в основном любят играть в сетевые игры и заходить на различные сайты и чаты. Поэтому родителям особенно полезно будет просматривать отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. программы для родительского контроля (например, ChildWebGuardian Pro, Hidetools Parental Control, KinderGate Parental Control, Kids PC Time Administrator, Child Control и др.). В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок.

Несмотря на то, что дети в этом возрасте довольно смысленные, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

1. Желательно, чтобы ребенок играл в Интернете только в присутствии родителей. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

2. Создайте список правил посещения Интернета вместе с ребенком и требуйте их выполнения.

3. Требуйте от ребенка соблюдения временных норм нахождения за компьютером.

4. Покажите ребенку, что вы наблюдаете за ним, не потому что вам этого хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

5. Обязательно объясните ребенку, что общение в Интернете — это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.

6. Добавьте детские сайты в раздел «Избранное». Создайте там папку для сайтов, которые часто посещает ваш ребенок.

7. Используйте специальные детские поисковые системы, например MSN Kids Search.

8. Установите на компьютер средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

9. Научите ребенка не выдавать в Интернете информацию о себе и своей семье.

10. Создайте семейный электронный ящик, чтобы контролировать переписку детей.

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

12. Приучайте ребенка советоваться с вами перед опубликованием какой-либо информации в Интернете (в чатах, регистрационных формах и профилях).

13. Научите ребенка не загружать файлы, программы или музыку без вашего согласия.

14. Не разрешайте использовать службы мгновенного обмена сообщениями.

15. Создайте «белый» список сайтов и вносите в него только сайты с хорошей репутацией.

16. Не забывайте беседовать с ребенком о его друзьях в Интернете.

17. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните ребенку, что он в безопасности, если сам рассказал вам об угрозах или своих тревогах. Похвалите его и посоветуйте обратиться к вам еще раз в подобных случаях.

Возраст 9—12 лет

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

1. Создайте вместе с ребенком список правил и временных норм посещения Интернета и требуйте их выполнения.

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате под присмотром родителей. 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. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.

4. Не забывайте беседовать с ребенком о его друзьях в Интернете.

5. Настаивайте, чтобы ребенок никогда не соглашался на личные встречи с друзьями по Интернету.

6. Позволяйте ребенку заходить только на сайты из «белого» списка, который создан вместе с ним.

7. Приучите ребенка не выдавать личную информацию посредством электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и т. д.

8. Приучите ребенка не устанавливать программы на компьютер без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Создайте ребенку ограниченную учетную запись для работы на компьютере.

10. Настаивайте на том, чтобы ребенок предоставлял вам доступ к своей электронной почте, чтобы вы убедились, что он не общается с незнакомцами.

11. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните ребенку, что он в безопасности, если сам рассказал вам об угрозах или своих тревогах. Похвалите его и посоветуйте обратиться к вам еще раз в подобных случаях.

Возраст 13—17 лет

В этом возрасте подростки активно используют поисковые системы (например, Google, Яндекс, Yahoo!, Mail.ru, Рамблер и др.), 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. В данном возрасте зачастую родителям уже весьма сложно контролировать своих детей, так как об Интернете они знают значительно больше своих родителей. Тем не менее, необходимо строго соблюдать правила интернет-безопасности, чаще просматривать отчеты программ родительского контроля, чтобы контролировать деятельность подростков в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на их надежность.

1. Создайте список домашних правил посещения Интернета вместе с ребенком и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Не забывайте беседовать с ребенком о его друзьях в Интернет. Спрашивайте о людях, с которыми ребенок общается посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди ему знакомы.

3. Необходимо знать, какими чатами пользуется ребенок. Поощряйте использование модерлируемых чатов и настаивайте, чтобы ребенок не общался в приватном режиме.

4. Настаивайте на том, чтобы ребенок никогда не встречался лично с друзьями по Интернету.

5. Приучите ребенка не выдавать личную информацию посредством электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и т. д.

6. Помогите ребенку защититься от спама. Научите подростка не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

7. Приучите ребенка не устанавливать программы на компьютер без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение.

8. Обсудите с ребенком проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

9. Приучите ребенка сообщать вам о любых угрозах или своих тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните ребенку, что он в безопасности, если сам рассказал вам об угрозах или своих тревогах. Похвалите его и посоветуйте обратиться к вам еще раз в подобных случаях.

10. Обязательно сами просматривайте сайты, которые посещает ваш ребенок.

Что делать, если ребенок все же столкнулся с интернет-угрозами?

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить угрозу для ребенка.

Родителям следует обратить внимание на поведение ребенка, которое может свидетельствовать о том, что ребенок стал жертвой **кибербуллинга**:

Беспокойное поведение

Даже самый замкнутый подросток будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу — самые явные признаки того, что ребенок подвергается агрессии.

Неприязнь к Интернету

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Интернете. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

Нервозность при получении новых сообщений

Негативная реакция ребенка на звук уведомления при получении письма на электронную почту или сообщения в социальной сети.

Какие действия необходимо предприниматься в случае, если ребенок столкнулся с интернет-рисками?

1. Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать.

2. Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.

3. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию — 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.

4. 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.), категорично настаивайте на избегании встреч с незнакомцами, проверьте все новые контакты ребенка за последнее время.

5. 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).

6. 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 ситу-

ации обратитесь к специалисту (телефон доверия 8-800-2000-122), который даст вам рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций.

Словарь интернет-терминов

Аккаунт (от англ. — account) — учетная запись, регистрационная запись.

Антивирус пакет компьютерных программ, останавливающий проникновение вирусов на компьютер, осматривающий содержимое компьютера на предмет наличия вирусов.

Администраторы, модераторы сайта специальные сотрудники сайта, которые следят за исполнением установленных на сайте правил.

Браузер — программа, позволяющая просматривать страницы в сети Интернет. Самые популярные Opera, Mozilla Firefox, Google Chrome, Internet Explorer.

Веб-сайт (от англ. website: web — паутина и site место) в компьютерной сети. Когда говорят «своя страничка в Интернете», то подразумевается целый веб-сайт или личная страница в составе чужого сайта. Кроме веб-сайтов в сети Интернет так же доступны WAP-сайты для мобильных телефонов.

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

Всемирная паутина — это все веб-сайты Интернета.

Груминг — установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Интернет — всемирная система объединенных компьютерных сетей для хранения и передачи информации.

Игнор — игнорирование, нанесение в черный список.

Логин (от англ. log in — входить в) — это имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого

Онлайн-игры — игровой процесс основан на взаимодействии с другими игроками и игровым миром, требующий постоянного подключения к Интернету.

Интернет-магазин — это интерактивный сайт, в котором: рекламируются товары и услуги, принимаются заказы на товары и услуги, посетителю предлагаются различные варианты оплаты заказанных товаров и услуг, возможна их мгновенная оплата через Интернет.

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

Киберпространство (от англ. cyberspace) — метафорическая абстракция, используемая в философии и в компьютерных технологиях, является (виртуальной) реальностью, которая представляет Ноосферу. Второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

Ронтент — это информация, расположенная на страницах сайта. Информация может быть как текстовая, так и графическая, мультимедийная и т. д. Другими словами контентом называют все то, что можно найти при помощи поисковиков.

Пароль — набор символов, известный только одному пользователю, необходимый для авторизации (для «входа») на сайте.

Поисковая машина (поисковый движок) комплекс программ, предназначенный для поиска информации. Обычно является частью поисковой системы. Поисковые машины или поисковики Yandex, Rambler, Google и прочие. Они помогают пользователю быстро найти необходимую информацию.

Почтовый ящик — дисковое пространство на почтовом сервере, выделенное для хранения, отправки писем пользователя и т. д. (приходящих на его адрес и подлежащих отправке).

Родительский контроль — это программы и службы, которые позволяют взрослым отслеживать, как ребенок использует компьютер: от филь-

трации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств — обеспечить безопасность ребенка в Интернете, эти инструменты иногда называют семейными настройками и настройками семейной безопасности. Windows 7, Windows Vista, Xbox 360, Xbox Live, Bing и другие продукты Microsoft включают встроенные настройки семейной безопасности.

Сайт (от англ. site — место, буквально «место, сегмент, часть в сети») — совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединенных под одним адресом.

Система мгновенного обмена сообщениями (от англ. instant messaging, IM) — службы мгновенных сообщений для обмена сообщениями в реальном времени через Интернет. Могут передаваться текстовые сообщения, звуковые сигналы, изображения, видео. Широкому кругу пользователей известно некоторое количество популярных сетей (и клиентов) обмена сообщениями, таких как Skype, ooVoo, Mail.Ru Agent client, Yahoo! Для мобильной связи — Viber, WhatsApp и т. д.

Спам (англ. spam) рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выразившим желания их получать. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.

Социальные сети — сайты в Интернете, на которых рядовые пользователи заводят свои странички для общения с друзьями. Одна из обычных черт социальных сетей — система «друзей» и «групп». Самые популярные русскоязычные: ВКонтакте, Одноклассники.ги, Мой Мир, Мой Круг и др.

Тролли, троллинг (от англ. trolling — ловля на блесну) — размещение в Интернете провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления и т. п.

Файлы, скачивание. Вся информация в компьютере сохраняется в виде файлов. Это могут быть текстовые файлы, музыкальные, видео-, графические, мультимедийные материалы и пр. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, то есть сохранять на компьютер.

Чат, чаттер (от англ. chatter — болтать) — средство обмена сообщениями по компьютерной сети в режиме реального времени. Характерной особенностью является коммуникация именно в реальном времени, что

отличает чат от форума. На форуме можно написать вопрос и ждать, пока кто-нибудь посчитает нужным на него ответить, а в чате общение происходит мгновенно, но только с теми, кто присутствует в нем в настоящий момент.

«Черный список» сайтов (black list), или как еще его называют «скам лист», представляет собой список сайтов, проектов или людей, которые проводят мошеннические операции в сети или не выполняют взятые на себя обязательства. В такие «черные списки» (black list) никогда не помещают заглянуть, прежде чем начать с кем-то сотрудничать или пользоваться каким-либо сервисом.

Хештег, хэштег (метка) или **хэш-тег** (от англ. hashtag: hash — знак решетка + tag — метка) — тип пометки или тега, используемый в микроблогах и социальных сетях, облегчающий поиск сообщений по теме или содержанию. Представляет собой слово или объединение слов, которому предшествует символ #, например: #искусство, #техника, #видео.

Электронная почта (англ. email, e-mail, от англ. electronic mail) технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределенной (в том числе глобальной) компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, вложение, ящик, доставка и другие), так и характерные особенности — простоту использования, задержки передачи сообщений, достаточную надежность и в то же время отсутствие гарантии доставки.



ПОМНИТЕ! Влияние Интернета на ребенка может быть как положительным, так и отрицательным. И каким будет это влияние во многом зависит от правил работы в сети Интернет, которые должны быть четко установлены в вашей семье.

