Памятка родителям

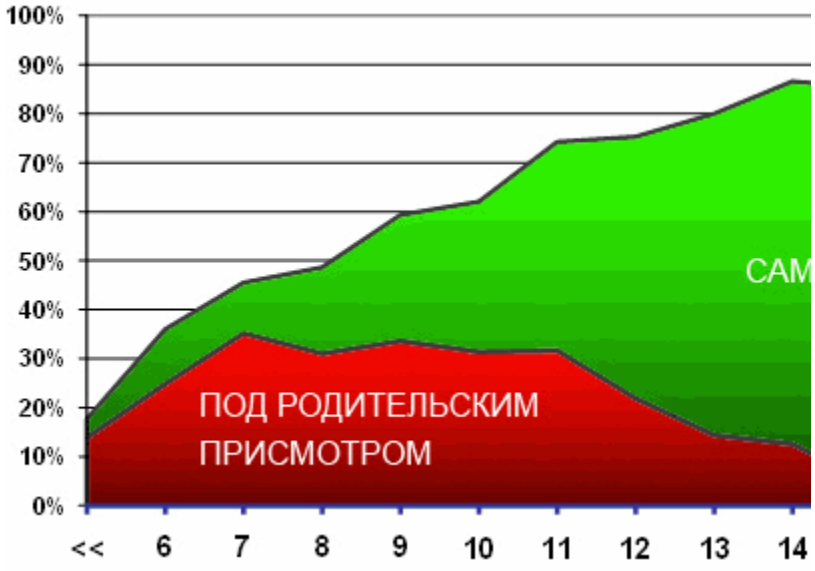
«Безопасность ребенка в интернет: что могут сделать взрослые?»

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома.

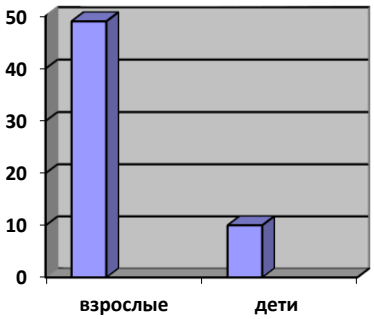
Скорость распространения информационных технологий в наши дни становится все стремительнее. Сегодня говоря о 600 миллионах пользователей персональных компьютеров, и в ближайшей перспективе эта цифра может превысить 1 миллиард. Компьютер широко используется не только на рабочем месте, но и в быту, дома, на отдыхе. Причем для домашнего использования персональные компьютеры приобретаются в гораздо больших объемах, нежели для организаций. Это общемировая тенденция, и наша страна не является здесь исключением. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика.

По данным исследований (ВЦИОМ, ФОМ), проведенных, «взрослая» аудитория Интернета в России составила порядка 40-49 млн. человек, а «детская» аудитория примерно 10 -12 млн. пользователей.

Согласно данным исследования компании RUМетрика, в России, по статистике, около 10 миллионов пользователей Интернета еще не достигли возраста 14 лет. До семи лет большинство детей путешествует по Интернету под руководством старших, затем по разным причинам родительский контроль ослабевает, и юные интернетчики отправляются в свободное плавание по сети. После 11 лет это явление приобретает массовый характер.



Способы использования Интернета детьми от 5 до 14 лет



Что касается серфинга сайтов с нежелательным контентом, то по данным RUМетрики:

48% детской аудитории Рунета не сталкивается с ресурсами нежелательного содержания, в то время как

39% детей просматривали порносайты,

38% наблюдали сцены насилия,

16% интересовались азартными играми,

14% - наркотическими веществами,

16% - экстремизмом или национализмом.

Есть данные о том, что в интернете дольше всего проводят время мальчики, девочки же посещают на 9% больше веб-страниц.

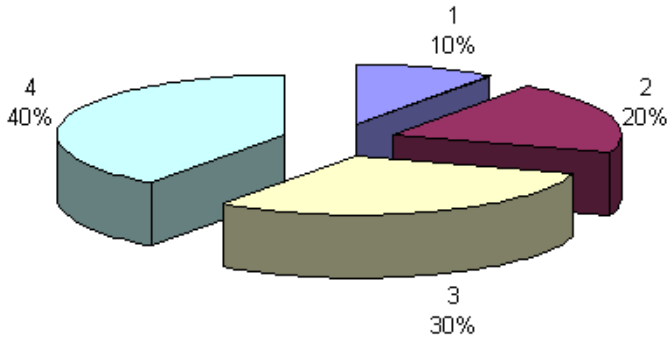
В 2011 году РИА «Новости» со ссылкой на слова Галины Солдатовой, директора Фонда развития интернета обозначило, что около **90% российских** детей пользуются интернетом, при этом родители практически не следят за их активностью в Сети. Средний возраст выхода в онлайн в России - десять лет. При этом доля пользователей интернета среди взрослой аудитории (около 35%) значительно ниже, чем среди подрастающего поколения.

80% российских детей из числа пользователей интернета считают себя завсегдатаями социальных сетей. Правила российских соцсетей, например, «Одноклассников» и «В Контакте», позволяют регистрироваться пользователям старше шести лет. Крупнейшая в мире социальная сеть Facebook принимает в свои ряды только с 13 лет (хотя никто не мешает не достигшим этого возраста детям зарегистрировать аккаунт, он может быть впоследствии заблокирован при появлении подозрений в занижении истинного возраста).

Треть юных пользователей социальных сетей не закрывает свои страницы от посторонних, большинство (60-80%) публикует личную информацию; например, каждый четвертый ребенок выкладывает номер телефона. При этом только 10% родителей знают о том, что дети публикуют контактную информацию в интернете.

Кроме того, российские дети готовы активно общаться с незнакомцами как в интернете, так и за его пределами. По словам Солдатовой, юные пользователи в России в пять раз чаще встречаются с онлайн-незнакомцами, чем их европейские сверстники.

По результатам самого масштабного на данный момент исследования в России «Моя безопасная сеть: Интернет глазами детей и подростков России 2009», проведенного Фондом развития Интернет, только у десятой части опрошенных детей и подростков из 18 регионов страны нет виртуальных друзей (друзей, с которыми пользователи познакомились непосредственно в Интернете). У пятой части (20%) респондентов есть друзья по электронной почтовой переписке. Почти треть школьников общаются с виртуальными друзьями по ICQ и почти половина (40%) - в системе виртуальных дневников (блогов).



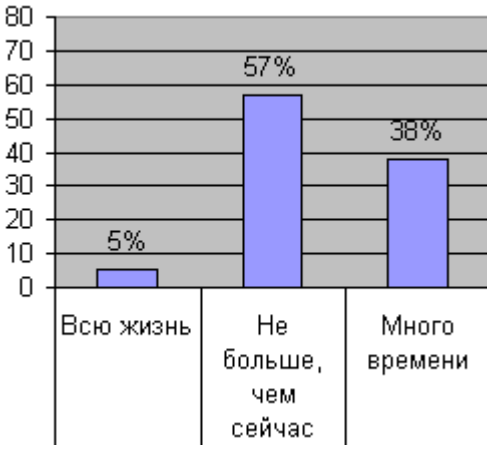
Есть ли у тебя виртуальные друзья?

1. Виртуальных друзей нет
2. Есть друзья по электронной почтовой переписке
3. Есть друзья в ICQ
4. Есть друзья в системе виртуальных дневников

Интересно отметить, что виртуальные друзья есть и у большинства старшеклассников, и у большинства учеников младших классов (60 % учащихся младших классов и 62 % учащихся старших классов).

Свое поведение в сети дети оценивают как «такое же, как и в жизни». Причем, в ответах младших школьников и старшеклассников различий нет.

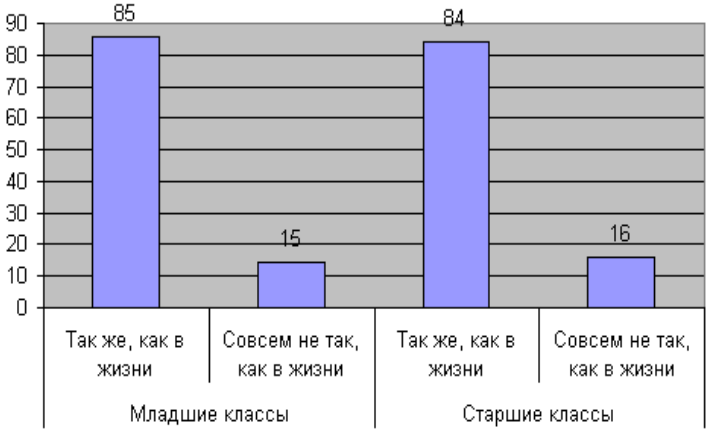
«Как ты ведешь себя в сети Интернет?»



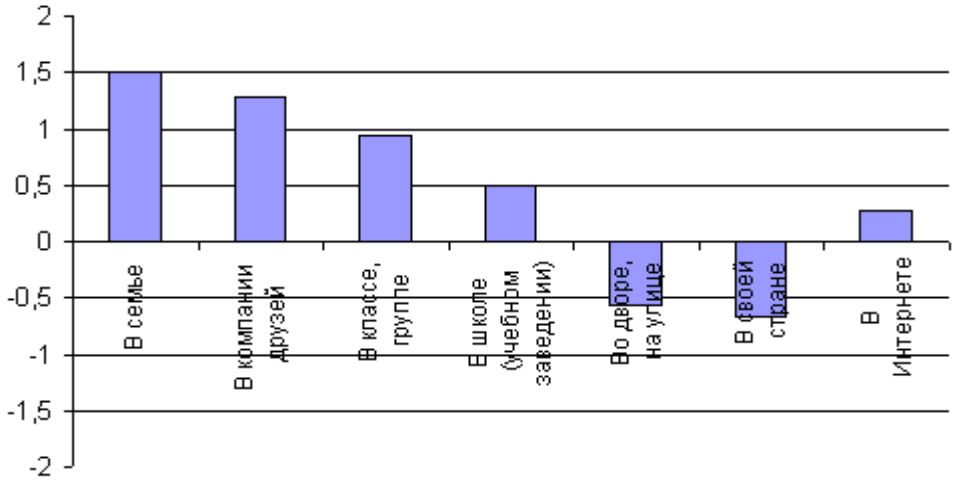
Дети проводили бы в сети не больше времени, если бы получили неограниченный доступ. Однако почти треть опрошенных отмечают, что проводили бы в Интернете больше времени, так как он «затягивает». И лишь 4% школьников заявили, что проводили бы в Сети всю свою жизнь.

Ответы на вопрос: «Как скажется на учебе неограниченный доступ к Интернету?» разделились: 58 % детей считают, что интернет поможет им в учебе, остальные предполагают, что скорее всего неограниченный доступ отвлечет от учебы, так как в Интернете очень много чего интересного, не связанного с учебой.

«Сколько времени ты проводил бы в Интернете, если бы получил неограниченный доступ?»



И еще одна интересная цифра – субъективное ощущение безопасности ребенка в ситуациях общения, в социуме. Наиболее безопасно дети чувствуют себя в семье, компании друзей, в классе и, менее, в школе. Безопасно, хотя и в меньшей степени – в интернете. Нет ощущения безопасности во дворе, на улице и в стране.

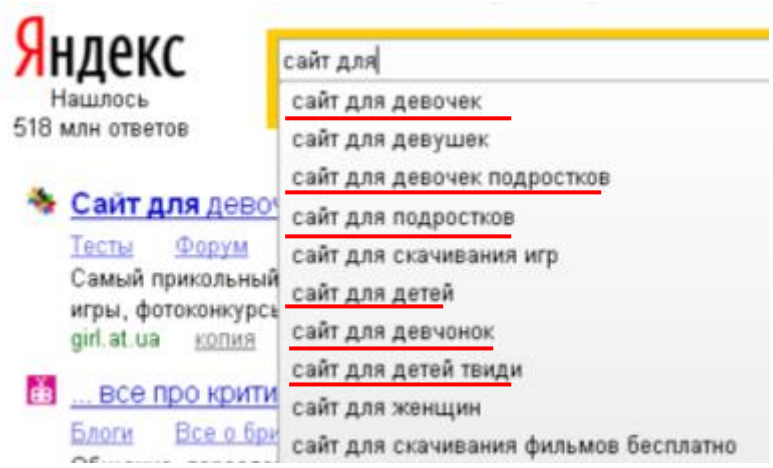


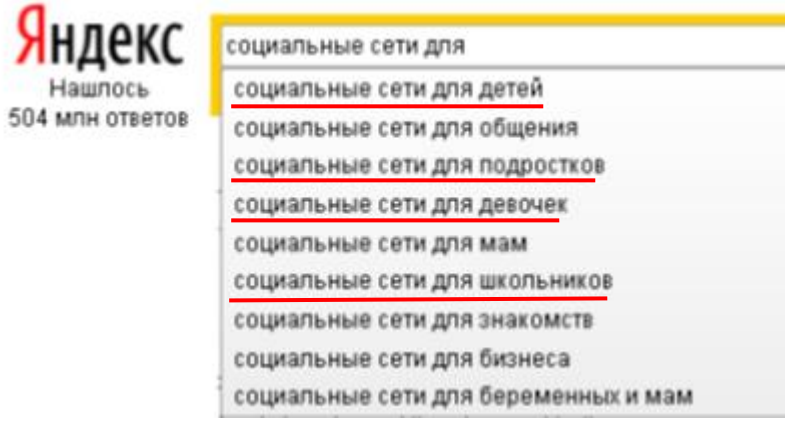
Итак, дети чувствуют себя безопасно в сети интернет.

Так нужно ли разрешать детям пользоваться всемирной паутиной?

Большинство исследователей, специалистов, да и просто рядовых пользователей с уверенностью отвечают на этот вопрос утвердительно. Говорят, что интернет позволяет детям обучаться, развиваться, учиться виртуальному общению, которое наряду с общением реальным стало неотъемлемой частью нашей жизни. Этим обосновывается создание «безопасного» детского интернета — зоны, схожей по своему назначению с детскими площадками в реальном мире. Здесь дети могут общаться со своими сверстниками, играть с ними в разные игры, есть сайты, похожие на детские книжки. Сказки, стихи, обучающая литература для малышей и даже книжки-раскраски — все это можно найти на виртуальных полках детского интернета. Специально для самых маленьких пользователей создаются даже целые поисковые системы, индексирующие только детские странички.

Детский интернет — это не только широчайшее предложение. Это еще и огромный спрос, как со стороны детей, так и со стороны родителей. Чтобы убедиться в этом, достаточно забить в поисковую систему слова «сайты для» или «соцсети для» и получить список наиболее частых поисковых запросов, начинающихся с этих слов.





Как видите, при любом из вышеприведенных запросов, Яндекс моментально выдает «сайты для детей».

Но есть и другая статистика!

Количество негативных интернет-ресурсов растёт. По данным Генпрокуратуры РФ, в настоящее время насчитывается более 7 тысяч террористических сайтов, где в подробностях учат, как сделать взрывчатку или совершить терракт. По данным американского исследовательского центра TopTenReviews, 12% всех сайтов (24,8 млн) содержат материалы для взрослых. В связи с этим можно утверждать, что дети впервые сталкиваются с порно, как только начинают пользоваться Интернетом.

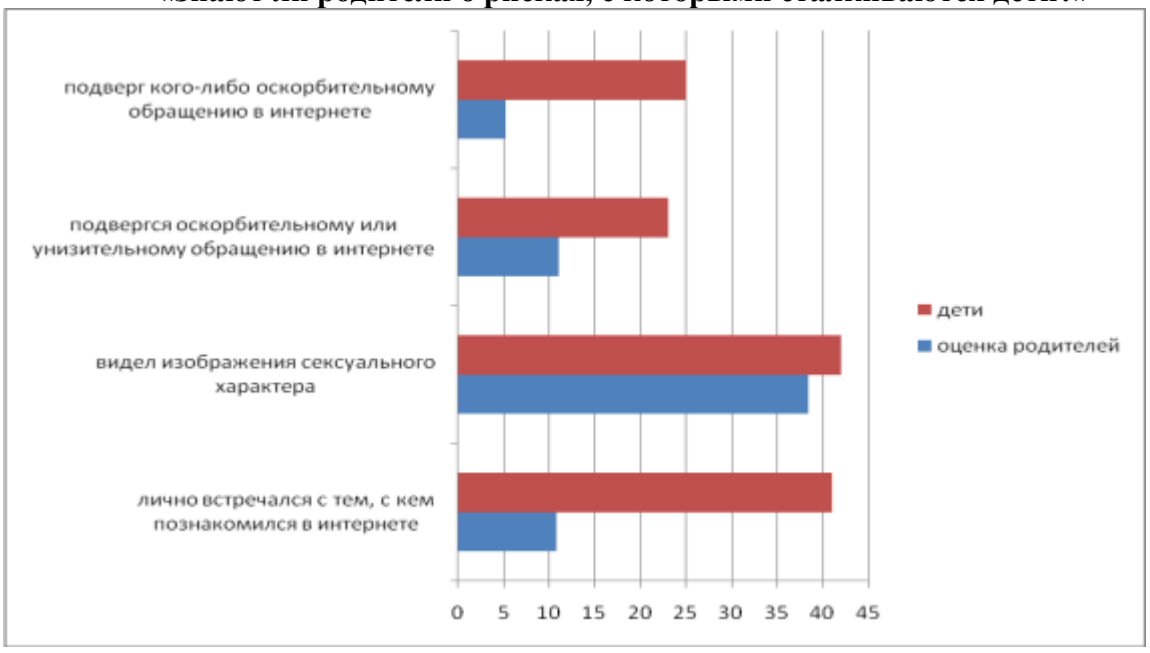
Не заставляют ждать своего появления и новые интернет-угрозы. Дети, часто не задумываясь, рассказывают своим онлайн-друзьям, где они живут или по какому графику работают их родители, отправляют дорогостоящие SMS мошенникам и часами сидят в социальных сетях, что не может не сказаться на их психическом и физическом здоровье. Кроме того, в последнее время участились случаи преследования и запугивания детей через различные интернет-сервисы. По данным нескольких опросов, в среднем, каждый второй подросток сталкивался с унижениями и оскорблениями в Сети.

По данным Евросоюза основные угрозы, с которыми сталкиваются сегодня дети в Сети:

- Незаконный контент
- Педофилы, груминг, незнакомцы
- Чрезмерное или сексуальное насилие
- Иной вредоносный контент
- Материалы, возбуждающие ненависть
- Реклама / коммерческое убеждение
- Предвзятость / ложное информирование
- Использование личной информации
- Кибербуллинг, скрытое преследование, домогательство
- Гэмблинг, финансовое мошенничество
- Причинение вреда самому себе (суицид, анорексия и др.)
- Вторжение, нарушение частной жизни
- Незаконная деятельность (хакерство, скачивание данных

И снова цифры! Данные, озвученные на конференции, посвященной безопасности детей в интернет.

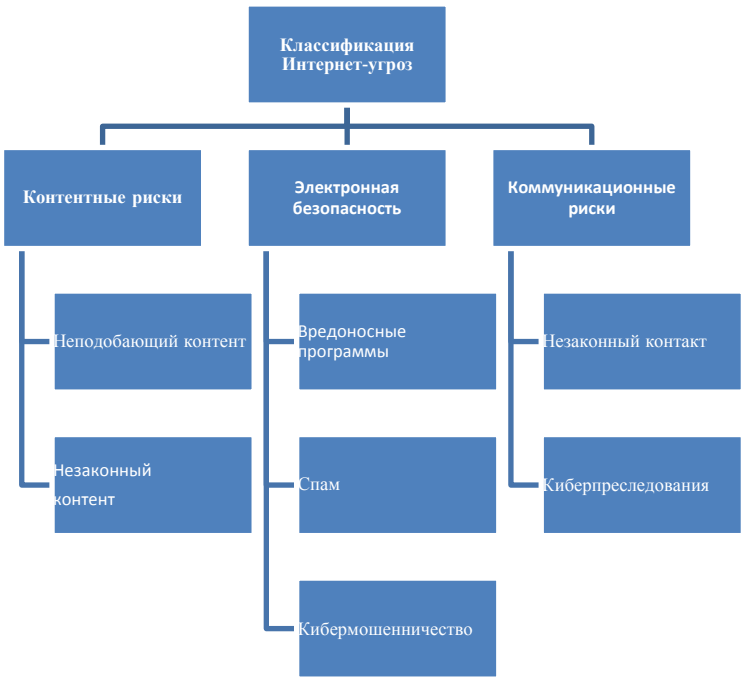
«Знают ли родители о рисках, с которыми сталкиваются дети?»



За три года работы Единой системы контентной фильтрации (в эту систему включены более 50 тысяч российских школ) заблокировано более миллиарда «плохих» запросов. Т.е. запросов к ресурсам, содержащим агрессивный контент или противоправную информацию. Такие данные привел генеральный директор Центра анализа Интернет-ресурсов (ЦАИР) Игорь Поляков. По его словам, когда российские школы оснащались контент-фильтрами, ЦАИР предполагал, что база «нехороших» сайтов будет пополняться 1000 ресурсов ежедневно. Сегодня ежесуточно в базу добавляется 70 000 ресурсов. А из всего объема запросов школьников 1,5-2% приходятся на «плохие» сайты. «Школьная» статистика обращения детей к такого рода сайтам - лишь одна сторона медали. В школе, на уроках дети находятся под постоянным присмотром педагогов. А вот обеспечение безопасности работы детей в интернете на домашнем компьютере зависит только от родителей, иначе дети предоставлены сами себе. До 80% «нехороших» сайтов дети находят благодаря поисковым системам.

Сегодня в мире уже возникло устойчивое понимание того, что проблема детской безопасности в Интернете – это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального до регионального и международного. В решении этой проблемы необходимо действовать системно и использовать не только правовые регуляторы, но и нормы обычаев и морали, а также технические и технологические возможности. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности – родителей и детей, а также профессиональной информационной культуры журналистов и учителей.

Итак, с какими же угрозами может встретиться ребенок в Интернет?



1. **Контентные риски**
   Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.
   - **Неподобающий контент**
     В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся

неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

- **Незаконный контент**
  В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

2. **Электронная безопасность**
   Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.
   - **Вредоносные программы**
     Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.
   - **Спам**
     Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.
   - **Кибермошенничество**
     Кибермошенничество - это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.
3. **Коммуникационные риски**
   Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.
   - **Незаконный контакт**
     Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.
   - **Киберпреследования**
     Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

1. ***Информирование о путях обеспечения безопасности ребенка в сети Интернет***

29.12.2010 принят федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», где под информационной безопасностью понимается состояние защищенности детей, при котором отсутствует риск, связанный с

причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В соответствии с законом в субъектах РФ разрабатываются региональные программы, позволяющие обеспечить информационную безопасность. Однако, обеспечение безопасности со стороны остальных видов угроз ребенку, находящемуся в сети интернет, остается делом педагогов и родителей.

Как обеспечить ребенку безопасность?

Можно говорить о нескольких стратегиях обеспечения родителями безопасности детей:

- **запрет –** отсутствие выхода в сеть в доме;
- **ограничение доступа к сети**, связанного с ограничением либо по времени, либо к определенным сайтам, ресурсам, т.е. фильтрация;
- **переключить внимание** на сайты, специализирующиеся на контенте для детской аудитории;
- **научить способам безопасной работы** в Интернет.

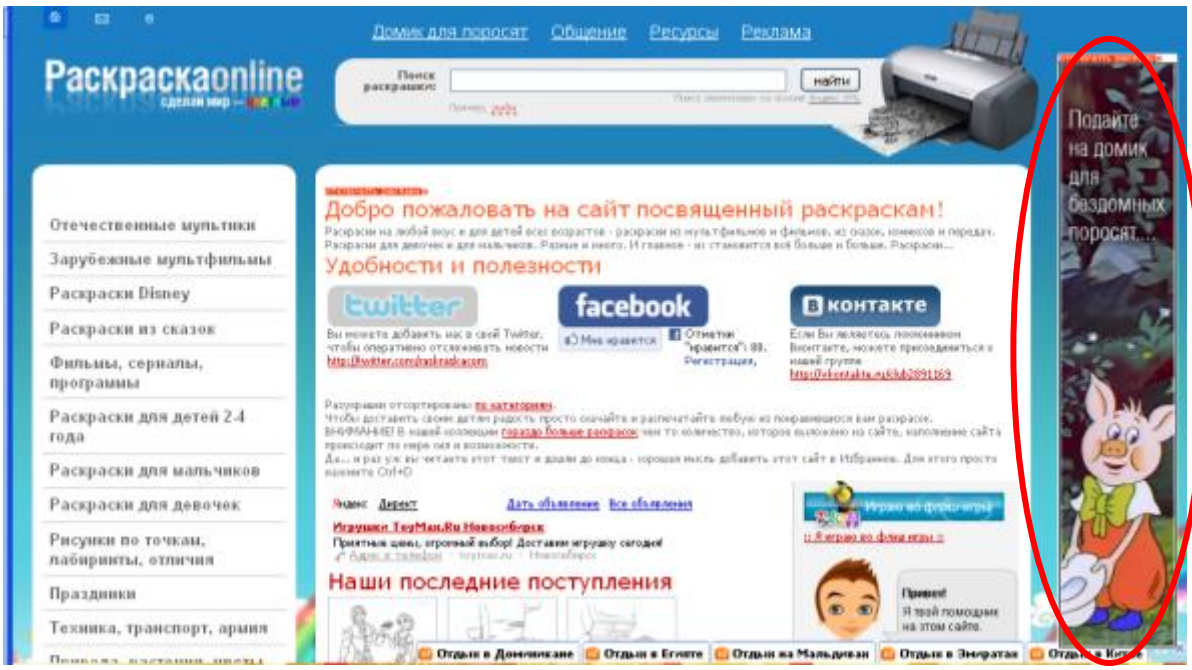
Здесь нет однозначно «хороших» и «плохих» способов.

Так, запрет – это возможность кардинально решить проблему: нет доступа – нет опасности. Однако в окружающем ребенка пространстве такая возможность остается. В силу любознательности, стремления не отстать от друзей, ребенок найдет способ ею воспользоваться, причем бесконтрольно.

Ограничение доступа к сети по времени позволяет учесть возрастные особенности детей и обеспечить безопасную для здоровья работу на компьютере.

Ограничение доступа к определенным сайтам может быть обеспечено с помощью настроек системы безопасности в Windows XP, ряда компьютерных программ, услуги родительского контроля, предоставляемой провайдером. Однако каждый день появляется огромное количество новых вирусных вредоносных программ, вирусов, сайтов с незаконным контентом, что сохраняет вероятность угрозы для ребенка.

На данный момент существует целый ряд сайтов, не декларирующих открыто систему безопасности детей в сети, но уделяющих достаточно внимания и своему содержанию, и отслеживанию обсуждений, их модерации. В их число входят порталы для самых маленьких (Жужа.ру, Смешарики), повествующие о жизни мультперсонажей, сетевые версии любимых журналов («Мурзилка», «Ералаш», «Юный натуралист»), интернет-радио для юных слушателей (Deti.FM, ТЫРНЕТ-Радио), библиотеки сказок и рассказов для детей, совместные ресурсы для родителей и малышей («Солнышко», 7я.ру, Мама.ру). На детских игровых ресурсах (RU-Kids, Игры для девочек) также предусмотрена модерация сообщений, система фильтров и внимательнейший отбор предлагаемых игр. Однако и на данных сайтах можно встретить рекламные баннеры сомнительного содержания. Например, на сайте «Раскраскаonline» (http://www.raskraska.com/) ребенку предлагается пожертвовать деньги на домик для бездомных поросят с помощью sms, а на следующей странице – реклама электронных сигарет и чудо-методики для похудания.



Научить способам безопасной работы есть не что иное, как формирование интернет-культуры, осуществляющееся в соответствии с возрастными особенностями ребенка, его потребностями. Однако и в данном случае сохраняется опасность столкновения ребенка с Интернет-угрозами.

Что делает ребенок младшего школьного возраста в сети Интернет?

В 7 – 8 лет происходит повышение интереса к Интернет. Для детей этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Находясь в интернете, ребенок может попытаться посетить сайты или пообщаться в чатах, разрешения на которые он не получил бы от родителей. Семи- и восьмилетние дети обладают сильным чувством семьи. Они только начинают развивать чувство своей моральной и половой индивидуальности и обычно интересуются жизнью старших детей. Дети 7—8 лет доверчивы и не сомневаются в авторитетах.

Дети этого возраста любят путешествовать по интернету и играть в сетевые игры. Возможно, они используют электронную почту и могут также заходить на сайты и чаты, посещать которые родители не разрешали.

Дети этого возраста начинают активно самостоятельно осваивать виртуальное пространство, любят путешествовать по Интернету, играть в сетевые игры, они начинают общаться в детских чатах, стремятся использовать электронную почту для переписки с друзьями. Однако нужно иметь в виду, что они могут заходить на сайты и чаты, посещать которые родители им не разрешали.

К концу периода любопытство и стремление найти ответы на свои вопросы начинает толкать их к поискам проблем и попыткам сломать существующие границы. У детей этой возрастной группы уже есть понимание того, с чем можно ознакомиться в интернете. Соблазн искать и найти что-то необыкновенное – очень велик. На протяжении всего детства ребенок должен проверять барьеры на прочность и развиваться в ходе такого обучения. Младшие школьники уже в состоянии понять важность безопасности в сети, однако не все из них способны постоянно помнить об этом. Злоумышленнику легко увлечь и обмануть такого ребёнка. Однако с детьми этого возраста уже не пройдёт номер с ограниченным списком сайтов - они остро почувствуют попытки контролировать их, и попробуют либо отключить ограничивающую программу, либо найти другой компьютер для выхода в сеть - у друзей или знакомых, что может быть ещё более опасно.

Родительский контроль в данном случае должен быть более незаметным и ненавязчивым. Хорошую помощь могут оказать фильтры, отсекающие контент по определённым ключевым словам и блокирующие доступ к сайтам из чёрного списка. Таким образом ребёнок получает достаточно свободы, и при этом ограждён от нежелательного контента.

Мальчики и девочки стремятся оставаться в безопасности, находясь в онлайновой среде. Информация по вопросам безопасности в интернете должна быть своевременной, соответствующей возрасту, должна учитывать культурные особенности страны, а также соответствовать ценностям и законам общества, в котором живет ребенок или молодой

Ключевые проблемы безопасности

Исследования проблем безопасности детей в Интернете показывают, что существует несколько ключевых проблем, из-за которых использование ребёнком сети может стать для него опасным.

Неосведомлённость детей

Это, несомненно, самый важный аспект обеспечения безопасности. Правильно проинструктированный ребёнок, знающий все возможные риски и способы их избежать, ведёт себя в Интернете более ответственно. Родители могут во многом положиться на разумное отношение своего ребёнка к сети, если они уверены в том, что он знает, что делает. Однако это относится лишь к детям с определённого возраста, и опять-таки не означает, что родители, учителя или опекуны могут полностью самоустраниться от вопроса безопасности ребёнка.

Неосведомлённость взрослых

К сожалению, даже многие родители, опекуны не имеют полного представления о том, каким рискам подвергается их ребёнок в сети. Неосведомлённость варьируется от недооценивания рисков, до чрезмерной опеки и паники, спровоцированной тревожными сообщениями в СМИ. Обе крайности пагубны, взрослые могут эффективно защищать ребёнка лишь в том случае, если имеют полное и верное представление об онлайновых рисках для их детей.

Недостаточная техническая грамотность взрослых и детей

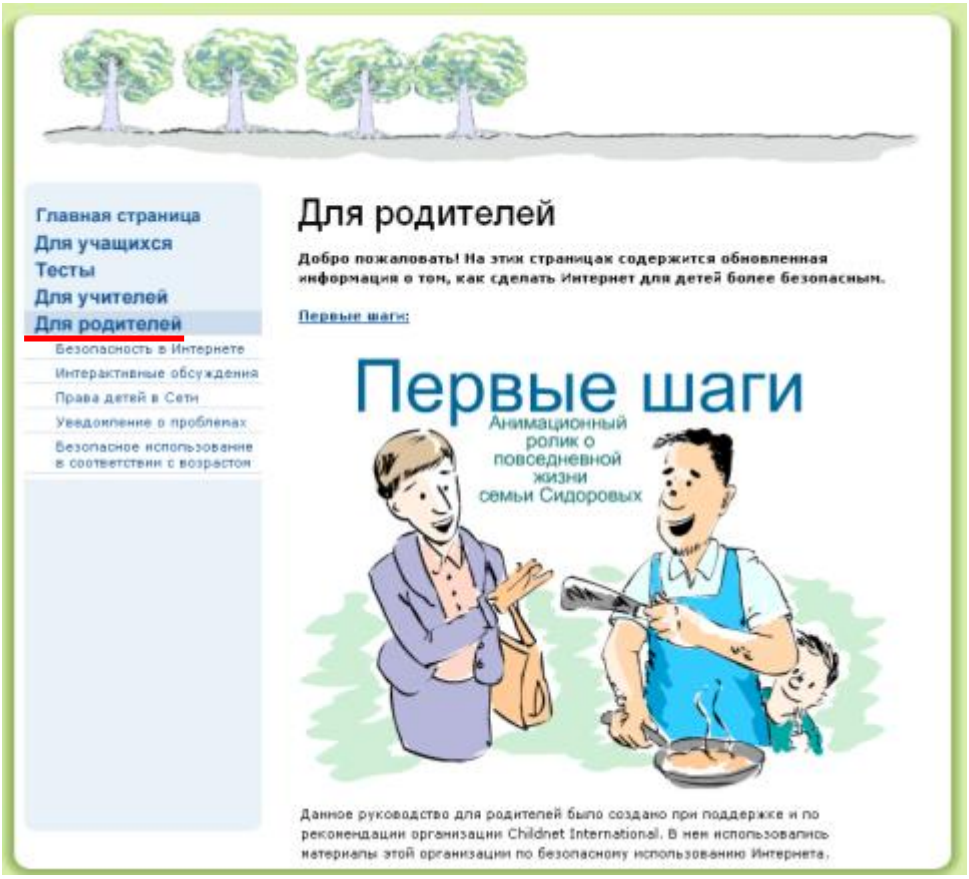
Несмотря на то, что многие дети быстро осваивают новые технологии и программы, немногие из них озабочены собственной безопасностью. Ребёнок может отключить антивирус, файерволл или программу родительского контроля, если ему покажется, что они ограничивают его возможности в онлайне, и если взрослый не позаботится о том, чтобы запретит ему такие действия. Таким образом, с технической точки зрения взрослым следует изучить все возможности обеспечения безопасности ребёнка с помощью компьютерных программ (семейных фильтров, блокираторов рекламы, антивирусов и файерволлов), установить и должным образом настроить все необходимые программы. Детям же необходимо разъяснить необходимость и важность таких программ.

Проблемы доверия

Это также крайне важный аспект безопасности. Ребёнок должен знать, что он может доверять вам, что вы поможете ему при возникновении трудной ситуации, и главное, не будете обвинять его. Большинство детей не склонны рассказывать родителям о неприятных происшествиях в сети, опасаясь, что те сочтут, что дети сами спровоцировали такую ситуацию, и накажут их, либо ограничат доступ в сеть. Кроме того, если ребёнок чувствует, что ему некому доверять в реальной жизни, он будет более склонен делиться своими проблемами с незнакомцами в онлайне, искать их дружбы и поддержки.

- Посмотрите **анимационный ролик «Первые шаги» о повседневной жизни семьи** Сидоровых, разработанный корпорацией Microsoft .

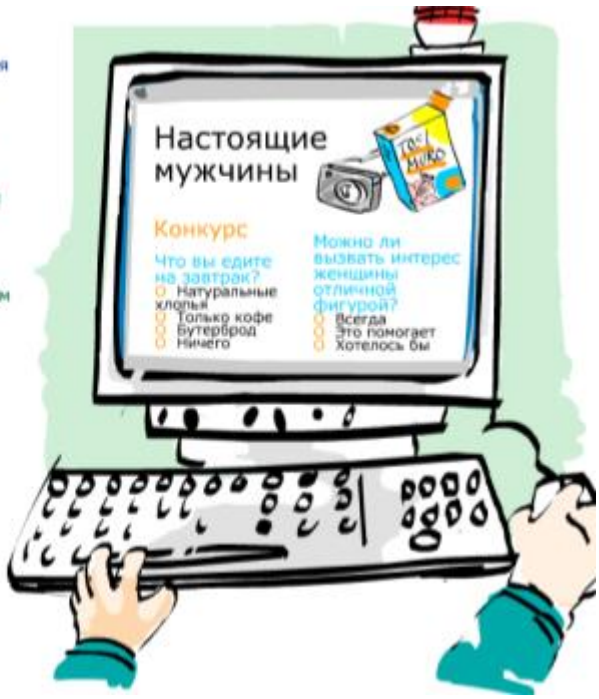
(Для этого распакуйте файл ChildSafetyCourse.msi, установите программу. Откройте вкладку «Для родителей»)



Обсудите с родителями представленные ситуации с точки зрения возможных способов поведения. Нажимая каждый из вариантов, просмотрите ответы, предлагаемые создателями ролика.

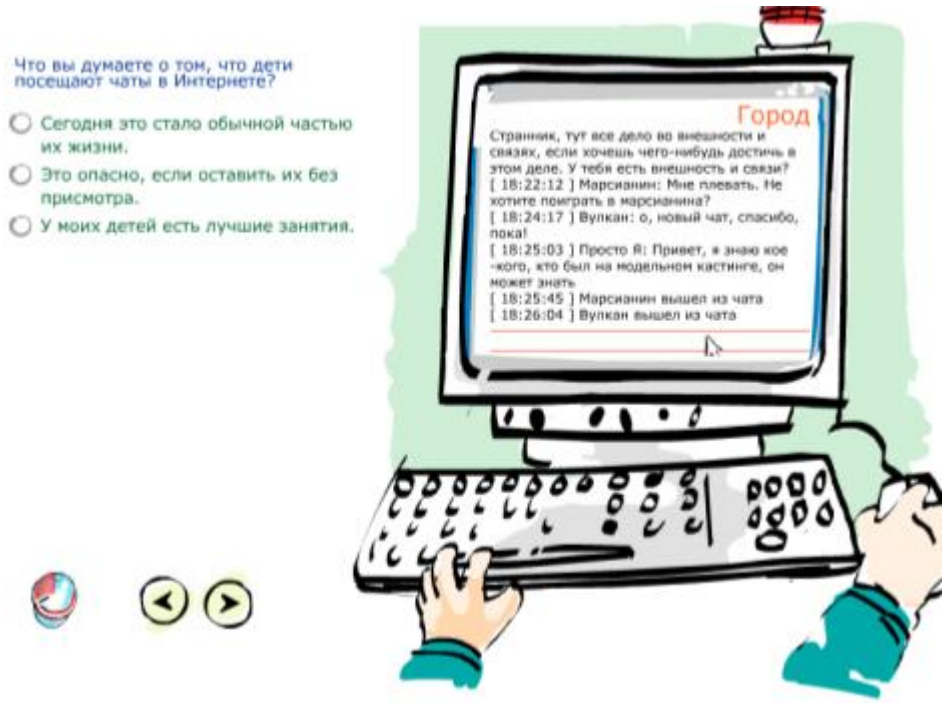
Как вы думаете, почему эта компания проводит конкурсы для детей?

- С помощью Интернета можно напрямую обратиться к целевой аудитории.
- Это недорогой способ проведения маркетинговых исследований.
- Таким образом они собирают адреса электронной почты респондентов и продают их другим организациям.



Что вы думаете о том, что дети ищут ответы на интересующие их вопросы в интерактивных форумах?

- Это ужасно!
- Хорошо, что в этом возрасте они учатся искать информацию.
- Я думаю, что мой ребенок способен оценить достоверность полученной информации.



- **Способы родительского контроля**

  Есть два основных пути обеспечения родительского контроля: данная услуга может быть обеспечена антивирусными программами, либо специально созданными под эту задачу утилитами (программами).

  Среди антивирусных программ:

  Kaspersky Internet Security 2012 и Kaspersky CRYSTAL,
  Panda Internet Security
  Avira Premium Security Suite
  Dr.Web Security Space
  Microsoft Windows Live Family Safety

  И другие.

  С исследованием эффективности фильтров родительского контроля, обеспечиваемых антивирусными программами, можно познакомиться здесь.

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра web-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

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. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

Довольно часто применяется более жесткий способ контроля – создание белого списка. Ребенок может посещать только те web-сайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребенок даже не в курсе, о чем вообще сверстники ведут разговор, интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается. Родителям, возможно, придется отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к web-сайтам. Есть еще одна, если так можно выразиться, группа риска – это программы обмена мгновенными сообщениями. Ребенок наивен, он можно нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. Напрашивается и вторая опасность – собеседники ребенка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьезных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.

Приведем пример нескольких утилит и программ, выполняющих функции родительского контроля:

Crawler Parental Control 1.1
KidsControl 2.02
ParentalControl Bar 5.22
Spector Pro 6.0
КиберМама
KinderGate
ОдинДома

На сайтах разработчиков содержатся и руководства по настройке данных продуктов. С видеоруководствами по настройке родительского контроля можно ознакомиться также на http://www.youtube.com/

KinderGate - обзор интернет фильтра для детей
Mipko Time Sheriff
ChildWebGuardian - обзор интернет фильтра для детей
Контент-фильтр NetPolice в действии
Kidgid - обзор интернет фильтра для детей
Dr.Web Бастион Pro
InternetCensor
Родительский контроль в Panda Internet Security 2010
Родительский контроль в Windows Vista
Родительский контроль в Windows 7

СОВЕТЫ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ДЕТЕЙ 7 – 10 ЛЕТ ПРИ ПОЛЬЗОВАНИИ ИНТЕРНЕТОМ.

- Старайтесь держать компьютеры с подключением к Интернету в общих комнатах, в которых можно легко осуществлять визуальный контроль над тем, что делает ваш ребенок в Интернете. Преступнику гораздо труднее завязать отношения, если экран компьютера хорошо вами просматривается.
- Создайте при участии детей свод домашних правил пользования Интернетом и требуйте его неукоснительного соблюдения.
- Приучите детей посещать только те сайты, которые вы разрешили.
- Используйте средства блокирования нежелательного материала (например, MSN Premium’s Parental Controls) как дополнение, но не замену к родительскому контролю. Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.
- Создайте семейный электронный ящик, на который будет приходить вся ваша электронная почта, вместо того чтобы позволять детям иметь собственные адреса.
- Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
- Маленькие детям не следует пользоваться чатами — слишком велика опасность. Только когда ваш ребенок подрастет, можно разрешить общаться там, где есть контроль над сообщениями (или, говоря компьютерным языком, «модерация»). Вообще имеет смысл, чтобы дети общались только в таких чатах.
- Если ваши дети пользуются чатами, вам следует знать, какими именно, и с кем они там беседуют. Лично посетите чат, чтобы проверить, на какие темы ведутся дискуссии.
- Внушите детям, что никогда нельзя покидать общий чат. Многие сайты имеют «приватные комнаты», где пользователи могут вести беседы наедине — у администраторов нет возможности читать эти беседы. Такие «комнаты» часто называют «приватом».
- Научите детей не загружать программы, музыку или файлы без вашего разрешения.
- Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.
- Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

- Если, несмотря на все меры предосторожности, ваши дети познакомились в интернете со злоумышленником, не вините их. Вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

2. По вопросам информационной безопасности и безопасного использования сети Интернет вами и вашим ребенком можно обратиться на следующие сайты:

- Вопросы безопасности ребенка в сети, защита NetPolice http://content-filtering.ru/Eduandinet/
- Вопросы обеспечения информационной безопасности от компании Microsoft http://www.microsoft.com/rus/protect/default.mspx#.
- Вопросы безопасности - сайт от компании Semantec http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids.
- **Лига безопасного Интернета** http://www.ligainternet.ru/roditelskii-kontrol-tekhnicheskie-resheniya
- **Один дома.** Четкий и надежный детский интернет-фильтр. Детский портал с включенным каталогом рекомендованных детских Интернет-ресурсов. Специальный портал для родителей. Консультации психологов. http://odindoma.org/
- **Ребенок в сети**. Сайт от компании Panda http://www.detionline.ru/.
- Специальный портал, созданный по вопросам безопасного использования сети Интернет. Безопасный Интернет http://www.saferinternet.ru/. Документы, материалы и мн. другое.
- **«Антивирусная школа»** http://av-school.ru. Данный портал создан с целью информирования интересующихся пользователей о возможностях использования персонального компьютера в повседневных делах и учебном процессе, формирования понимания роли информационных технологий, получения новых знаний и навыков для работы с компьютером, общения и обмена опытом между участниками. Этот портал создан специалистами «Лаборатории Касперского».
- **Форум «VirusInfo»** http://virusinfo.info/forum.php?referrerid=775 здесь также можно получит ответы и помощь в решении проблем информационной безопасности.
- **Сайт «Безопасность в Интернет»** который создан специально для детей, родителей и учителей, на котором можно найти много интересной информации и советов http://www.e-teaching.ru/SiteCollectionDocuments/pil/inet_safety/html/etusivu.htm
- http://www.nachalka.com - сайт для людей от 6-и лет и старше, имеющих отношение к начальной школе. Для детей это безопасная площадка, где можно узнавать что-то интересное, создавать что-то новое, играть в умные игры, общаться со сверстниками, участвовать в проектах и конкурсах. *"Пока мы спорим "пущать" или "не пущать" учеников начальной школы в Интернет - они уже здесь. Мы снова опоздали. Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контакта. Никакие фильтры никогда такой гарантии не дадут. Но мы можем формировать у ребят навык "безопасного" поведения в Интернете. Как?"* Этому и не только посвящен раздел сайта "Безопасность детей в Интернет" http://www.nachalka.com/bezopasnost.
- Международный онлайн - конкурс по безопасному использованию http://interneshka.net/parents/index.phtml
- Азбука безопасности для детей и подростков http://azbez.com/safety/internet

- От компании Microsoft: книга "Безопасность детей в Интернет" http://www.ifap.ru/library/book099.pdf .
- Всероссийский Интернет-урок информатики «Безопасность детей в Интернете». Это проект Компании Microsoft совместно с АПКиППРО http://www.e-teaching.ru/history/Pages/i-yrok.aspx.
- Эксперты предлагают родителям рекомендации для обеспечения безопасности детей http://school-sector.relarn.ru/wps/?p=1758
- Интерактивная игра «Джунгли Интернета» http://school-sector.relarn.ru/wps/?p=1706 Игра предназначена для детей в возрасте от 7 до 10 лет и по заказу совета Европы «Строим Европу для детей и вместе с детьми». http://www.wildwebwoods.org/popup.php?lang=ru .
- Детский сайт ТВИДИ. Правила безопасности в сети Интернет. Безопасный поиск, общение http://www.tvidi.ru/ch/main/safe.aspx
- Детский поисковик AGAKIDS http://www.agakids.ru/#section_main Визуальная поисковая система детских сайтов "AGAKIDS" создана в помощь детям для поиска детских ресурсов на просторах Интернета.
- http://www.gogul.tv/ Детский браузер.
- http://www.moskids.ru/ Детский портал для детей города Москвы. Очень яркий и интересный для детей, родителей и учителей портал

Внутрисемейные правила использования интернета

Перед тем как дети начнут осваивать интернет, неплохо убедиться, что все понимают, что следует и что не следует делать в Сети. Можно написать кодекс поведения, которому все согласны следовать. Кроме того, можно составить правила пользования для каждого ребенка в семье; в зависимости от возраста. Каждый подписывает свое соглашение, чтобы показать, что понимает правила и соглашается следовать им в интернете.

Ниже приведен образец. Его можно скопировать, пересмотреть для нужд именно вашей семьи и напечатать для личного использования. Семейные правила пользования Сетью можно прикрепить около каждого компьютера. Для напоминания.

Соглашение о кодексе поведения в интернете

Я обязуюсь:

1. Обращаться к моим родителям, чтобы узнать правила пользования интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в интернете (___ минут или ___ часов).
2. Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.
3. Всегда немедленно сообщать родителям, если я увижу или получу в интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в интернете.
4. Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в интернете, без разрешения родителей
5. Никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через интернет или обычной почтой.
6. Никогда никому, кроме своих родителей, не выдавать пароли интернета (даже лучшим друзьям).
7. Вести себя в интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречит закону.
8. Никогда не загружать, не устанавливать и не копировать ничего с дисков или из интернета без должного разрешения.
9. Никогда не делать без разрешения родителей в интернете ничего, требующего платы.
10. Сообщить моим родителям мое регистрационное имя в интернете и имена в чате, перечисленные ниже:

    _____
    _____
    _____
    _____

Имя (ребенок) _____ Дата _____
Родитель или опекун _____ Дата _____