Тамбовское областное государственное
образовательное автономное учреждение
дополнительного профессионального образования
«Институт повышения квалификации работников образования»

Безопасность детей в Интернете

Рекомендации для родителей

Тамбов, 2011 г.

Рецензенты: Мосягина Н.Г., преподаватель технического колледжа ТГТУ, к.т.н.

Рекомендации «Безопасность детей в Интернете». / Автор-сост.: Н.И. Баскакова, / Под общей ред. Н.К. Солоповой, к.п.н., доцента, проректора по учебно-методической работе и информатизации ТОИПКРО. – Тамбов: ТОИПКРО, 2011. – 191 с.

Важной задачей для родителей и педагогов сделать пребывание детей в Интернете более безопасным, научить их ориентироваться в киберпространстве, предупредить об опасностях виртуального мира, дать рекомендации по безопасному поведению в сети Интернет

Рекомендации «Безопасность детей в интернете» адресована руководящим и педагогическим работникам учреждений общего и начального профессионального образования, родителям обучающихся, детям разного возраста.

Введение

Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Одной из важнейших координат их развития становятся информационно-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в интернете более безопасным, научить их ориентироваться в киберпространстве — важная задача для их родителей и педагогов.

В основе предлагаемых рекомендаций лежит разработанная Фондом Развития Интернет классификация Интернет-рисков (опасностей), приведены некоторые результаты исследования «Дети России онлайн», которое было проведено Фондом Развития Интернет по методологии международного исследовательского проекта Еврокомиссии «EU Kids Online II» (2010-11 гг.).

Риски (опасности) по данной классификации разделяются на четыре типа: контентные, коммуникационные, электронные и потребительские. Учитывая их разную природу и механизм действия, в отношении каждого типа рисков даются отдельные рекомендации.

Информация нежелательного характера. Контентные риски Как их избежать.

Для полного понимания этого термина приведем определение понятия контент. 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, рингтоны, 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 относится:

- информация о насилии, жестокости и агрессии,
- информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам,
- пропаганда суицида,
- пропаганда азартных игр,
- пропаганда и распространение наркотических веществ, отравляющих веществ,

- пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи),
- 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, торрентах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Распространение **противозаконной информации** преследуется по закону, например, распространение наркотических веществ через Интернет, порнографических материалов с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям. Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение противозаконной информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких 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, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др.

Неэтичная и **вредоносная** информация может быть направлена на манипулирование сознанием и действиями различных групп людей.

Это могут быть сайты, на которых люди обсуждают способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, и даже сайты, на которых описываются способы самоубийства. Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных, например, просмотр тех или иных видео-материалов через сеть интернет приводит к заражению компьютера вирусами. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия могут преследоваться по закону в соответствии со статьями Уголовного кодекса РФ (ст. 272,273,274).

Что надо знать о проблемах недостоверной информации в Интернете?

В Интернете есть большая доля информации, которую никак нельзя назвать ни полезной, ни надежной, ни достоверной. Пользователи Сети должны мыслить критически, чтобы оценить достоверность, актуальность и полноту информационных материалов; поскольку абсолютно любой может опубликовать информацию в Интернете. В Интернете не существует служб редакторов и корректоров (такие службы функционируют только в электронных средствах массовой информации), никто не проверяет информационные ресурсы на достоверность, корректность и полноту. Поэтому нельзя использовать Интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативно-правовых актов и т.п. .

Рекомендации для родителей по предупреждению контентных рисков «Как избежать материалов с нежелательной информацией»:

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Перечень специальных программных фильтров (интернет-фильтров) приведен в приложении 1. Почти каждый Интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика Интернет-браузеров можно найти подобную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, какое содержимое в Интернете могут просматривать их дети, отсекать «плохие» сайты, содержащие нежелательную информацию, в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался Интернетом, устанавливать ограничения пользования компьютером и Интернетом по времени. Родительский контроль можно устанавливать непосредственно с помощью операционной системы (например,Windows), антивирусных программ (например, антивирус Касперского), специальных программ. Полезные ссылки по настройке родительского контроля приведены в приложении 2.

2. Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

3. Создайте на компьютере несколько учетных записей, когда каждый пользователь сможет входить в компьютер (систему) независимо и иметь собственный уникальный профиль Ребенок сможет входить в систему только под своим логином и паролем, не имея административных прав на контроль системных настроек, установку программ. Учетная запись администратора должна быть у родителя, тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Для работы в Интернете необходимо создавать надежные и защищенные пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

4. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра.

Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред такой информации.

Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с Вами.

5. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информации. Признаки надежного сайта, информации которого можно доверять, включают**:** авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных.

6. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог гораздо конструктивнее, чем

постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Некоторые статистические данные по контентным рискам (всероссийское исследование «Дети России онлайн» на основе методологии проекта EU Kids Online II).

Более 40% детей в России сталкиваются с изображениями сексуального характера в Интернете или других источниках. И каждый шестой из этих детей видит сексуальные изображения ежедневно или почти ежедневно, каждый пятый – систематически: 1-2 раза в неделю. В странах Евросоюза эти цифры в среднем практически в два раза меньше. Данные исследования по России также показали, что младшие дети сталкиваются с сексуальным контентом реже, но при этом испытывают гораздо больший стресс: 40% детей 9-10 лет, имевшие опыт столкновения с изображениями сексуального характера, указали, что были сильно или очень сильно расстроены этим. Данные однозначно показывают, что Интернет в России по сравнению с телевизором, журналами и книгами лидирует в сексуальном просвещении подрастающих поколений. Причем большинство школьников сталкивается с сексуальным контентом случайно – во всплывающих окнах (Рис.1).

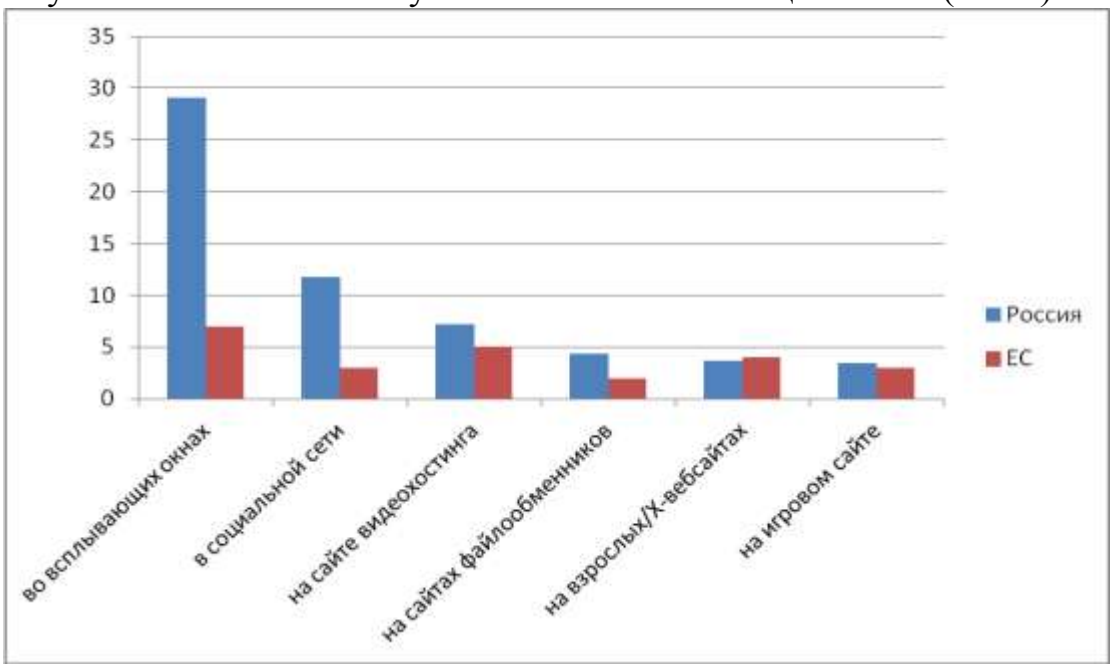

Рис. 1. На каких сайтах школьники сталкивались с сексуальными изображениями.

На вопрос, что может расстроить их сверстников в сети, многие дети называли агрессивные видео и фото, сайты, на которых обсуждаются различные способы насилия по отношению к другим и к себе, пропагандируется нездоровый образ жизни, анорексия, наркотики. Каждый четвертый ребенок старше 11 лет (независимо от пола) указал, что сталкивался в Интернете с сайтами, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц.

Около 35% опрошенных детей в возрасте 11-16 лет сталкивались с сайтами, на которых люди обсуждают способы причинения себе боли или

вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, а также сайты, на которых описываются способы самоубийства.

%	Возраст			Общий %
	11-12 лет	13-14 лет	15-16 лет	
Способы причинения себе вреда и боли	9	14	11	12
Способы совершения самоубийства	9	10	11	10
Способы чрезмерного похудения	16	26	30	25
Наркотики, опыт их употребления	4	13	13	11
Сталкивался с чем-либо из перечисленного	26	37	40	35

Рис 2. Частота столкновения российских школьников с сайтами, на которых описываются способы нанесения вреда своему здоровью

По сравнению с Европой, российские дети значительно чаще (36% и 20% соответственно) посещают сайты, где описывается или обсуждается что-либо из вышеперечисленного. Но при этом, как в России, так и в странах ЕС прослеживается одинаковая тенденция: чем старше дети, тем чаще они отвечают, что посещали сайты, связанные с причинением себе физического ущерба и потенциально опасные для здоровья сайты.

В то же время данные исследования показывают, что около половины детей не умеют оценивать сайты с точки зрения достоверности информации, чуть меньше половины не умеют удалять историю своих действий на компьютере и блокировать спам.

Безопасное общение детей в интернете или коммуникационные риски общения в Интернете

Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Интернет - это не только средство массовой информации и всемирный справочник, но и среда для общения. В интернете существует много инструментов, позволяющих организовать места для общения – социальные сети, блоги, чаты, форумы, гостевые книги, списки рассылки и пр.

Примерами коммуникационных рисков могут быть: знакомства в сети и встречи с Интернет-знакомыми, интернет-хулиганство: преследование, запугивание и оскорбления (кибербуллинг), незаконные контакты, и др. С коммуникационными рисками можно столкнуться при общении в мобильных сервисах, чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д.

Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг) – это явления не только виртуальной, но и реальной жизни. Английское слово буллинг (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Буллинг, осуществляемый в виртуальной среде с помощью Интернета и мобильного телефона, называют

кибербуллингом. Кибербуллинг, преследование с использованием цифровых технологий, сильнее всего действует на детей и подростков.

Кибербуллинг не менее опасен, чем реальные издевательства. Если террор может закончиться, когда жертва вернется домой или пожалуется старшим, то кибербуллинг продолжается все время и от него невозможно спрятаться. В отличие от реальной травли, для кибер-буллинга не нужно быть здоровяком, достаточно компьютера, времени и желания кого-то терроризировать. Распространение кибербуллинга, во многом, отражает проблемы морали в обществе, где к человеку не относятся, как к ценности, личности и игнорируют его проблемы и переживания, отвечают цинизмом.

По данным, полученным в исследовании «Дети России онлайн», в среднем по РФ 23% детей, которые пользуются Интернетом, являются жертвой буллинга онлайн или офлайн. Если сравнить виртуальность и реальность, то российские дети подвергаются буллингу в Интернете так же часто, как и в реальной жизни. Оскорбления в чатах, на форумах, в блогах и в комментариях к ним, поддельные страницы или видеоролики, на которых над кем-то издеваются или даже избивают уже давно стали привычной частью Рунета – каждый десятый ребенок 9-16 лет становился жертвой кибербуллинга.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент. Особенно остро переживают кибербуллинг дети 9-10 лет: 52% детей этого возраста, ставшие жертвой подобной ситуации, в первую очередь девочки, указали, что были этим сильно или очень сильно расстроены.

Кроме того, нередко и сами школьники выступают агрессорами. В России 25% детей признались, что за последний год обижали или оскорбляли других людей в реальной жизни или в Интернете. Обращает на себя внимание тот факт, что в России субъектов буллинга в два раза больше, чем в среднем по европейским странам.

Рекомендации для родителей по предотвращению интернет-хулиганства, кибербуллинга

1. Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.

3. Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребёнок подвергается кибербуллингу, различны, но есть несколько общих моментов:

- признаки эмоционального дистресса на протяжении и после использования Интернета,
- прекращение общения с друзьями,
- избегание школы или школьных компаний,
- нестабильные оценки и отыгрывание злости в домашней обстановке,
- перемены в настроении, поведении, сне и аппетите
- не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками,
- склонны к депрессии и чаще своих ровесников думают о самоубийстве.

4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.

5. Объясните детям, что личная информация, которую они выкладывают в Интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.

6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички. Большинство социальных сетей и сервисов электронной почты имеют в настройках опцию "заблокировать пользователя" или "занести в чёрный список".

7. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в Интернете.

8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут попадать под статьи действия уголовного и административного кодексов о правонарушениях.

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

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате Интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.

3. Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.

4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Знакомства в Интернете и встречи с незнакомцами

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам.

Особенно опасным может стать – установление дружеских отношений с ребенком с целью личной встречи **(груминг)**, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Рекомендации по предупреждению встречи с незнакомцами:

1. Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети – с ровесниками или людьми старше себя.

2. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.

3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.

4. Объясните ребенку, что при общении на ресурсах, требующих регистрации (в чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.

5. Объясните ребенку опасность встречи с незнакомыми людьми из Интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с Интернет-другом надо обязательно ходить в сопровождении взрослых.

6. Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в Интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в Интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Некоторые статистические данные по коммуникационным рискам (всероссийское исследование «Дети России онлайн» на основе методологии проекта EU Kids Online II).

Для многих российских школьников не важно, знают ли они своих Интернет-собеседников в реальности. Чем старше ребенок, тем шире у него сеть таких контактов. Если среди российских детей 11-12 лет треть поддерживает в сети контакты с незнакомыми им в реальной жизни людьми, то среди 15-16-летних таких уже больше половины. В Европе большинство школьников общаются в Интернете с теми, с кем они познакомились в реальности, и только четверть из них предпочитают общаться с Интернет-знакомыми. Как в Европе, так и в России в эту группу риска входят больше мальчиков, чем девочек. Чаще всего именно с Интернет-знакомыми, которых они не знают в реальности, российские школьники общаются в социальных сетях, чатах и играя в онлайн-игры. В то время как в Европе даже на этих площадках для общения в числе собеседников лидируют реальные знакомые.

В целом в России за последний год 28% подростков 11-16 лет получали или просматривали сообщения сексуального характера, причем более 10% - раз в месяц и чаще. Эти сообщения могли быть разного характера: подростки могли сами обмениваться неприличными картинками и видео, а некоторые могли подвергаться сексуальному домогательству (грумингу). По сравнению с Европой, в России дети значимо чаще получают сексуальные сообщения (15% в Европе), причем происходит это чаще, чем раз в неделю (12% в России, по сравнению с 3% в Европе). Российские дети и подростки сталкиваются и получают изображение сексуального характера в Интернете чаще, чем в других европейских странах. Дети старшего подросткового возраста (13-14 и 15-16 лет) получают такие сообщения гораздо чаще, чем дети 11-12 лет.

Рис.5 Получение сообщений сексуального характера российскими и европейскими школьниками

Электронные риски

Электронные риски – это вероятность столкнуться с хищением персональной информации и/или подвергнуться атаке вредоносных программ.

Вредоносные программы – различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с Интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из Интернета файлов.

Как узнать, что ваш компьютер заражен?

Учитывая, что вирусы обычно хорошо замаскированы внутри обычных файлов, непрофессионалу трудно их обнаружить. Несмотря на это, даже неопытный пользователь, как правило, замечает, что с компьютером происходит что-то неладное: он тормозит, появляются непонятные сообщения, а иногда он просто зависает и только перезагрузка может вывести его из этого состояния.

Существуют определенные признаки, по которым, с высокой степенью вероятности, можно утверждать, что компьютер заражен вирусами:

- медленная реакция на действия пользователя, особенно при запуске программ,
- искажение содержимого файлов и каталогов или их полное исчезновение,
- частые сбои и зависания компьютера,
- самопроизвольное появление на экране сообщений или изображений,
- несанкционированный запуск программ,
- зависание или странное поведение интернет-браузера,
- невозможность перегрузки компьютера (операционная система не загружается).

Однако нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае Вы и Ваши дети должны быть крайне внимательны, когда получаете сообщения по электронной почте от неизвестного адресата с вложением, когда скачиваете файлы из Интернета, пользуетесь чужими носителями информации или открываете файлы, скопированные с чужого компьютера.

Рекомендации по снижению рисков заражения компьютера вирусами и хищению персональной информации:

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
5. Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п).

7. Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.

8. Расскажите ребенку, что если он пользуется Интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о вашем ребенке.

Потребительские риски

Потребительские риски - злоупотребление в Интернете правами потребителя, включают в себя:

- хищение персональной информации с целью кибермошенничества,
- потеря денежных средств без приобретения товара или услуги,
- риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию,
- азартные игры на деньги.

Хищение личной информации

Кража личных данных или кибермошенничество – любой вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в Интернете. Хищение личных данных через Интернет иногда называется *фишингом*.

Многие интернет-аферы – это варианты мошеннических схем, существовавших еще до появления Сети, число которых увеличилось вместе с популярностью онлайн-шоппинга и других типов электронной коммерции. Для обмана пользователей интернет-мошенники используют электронную почту, чаты, форумы и фальшивые веб-сайты.

Виды кибермошенничества: вишинг, фишинг, фарминг, нигерийские письма и т.п (см. словарь терминов).

Вы можете самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками.

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытия ваших банковских счетов;
- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;
- сведения о сделках, которые слишком хороши, для того, чтобы быть правдой;
- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
- грамматические и орфографические ошибки.

Рекомендации по предупреждению кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете.
2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.
3. Не отправляйте о себе слишком много информации при совершении Интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.
4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
5. Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:
   - Ознакомьтесь с отзывами покупателей.
   - Избегайте предоплаты.
   - Проверьте реквизиты и название юридического лица – владельца магазина.
   - Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
   - Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
   - Сравните цены в различных Интернет-магазинах.
   - Обратите внимание на правила Интернет-магазина.
   - Выясните, сколько точно вам придется заплатить.
6. Посещая веб-сайты, нужно самостоятельно набирать в браузере адрес веб-сайта или пользоваться ссылкой из «Избранного» (Favorites); никогда не нужно щелкать на ссылку, содержащуюся в подозрительном электронном письме.
7. Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.
8. Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Азартные игры на деньги. Как уберечь детей от азартных игр.

Множество детей обожают искать развлечения (например, игры) в Интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако, им нельзя играть в азартные игры на деньги.

В чем состоит отличие между игровыми сайтами и сайтами с азартными играми.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Кроме этого, существует такие понятия как клиентские и браузерные игры, то есть игры через Интернет. Клиентские и браузерные игры бывают платные, бесплатные и условно-бесплатные. Условно-бесплатные - это такие игры, где можно играть бесплатно, но есть возможность что-либо улучшать (например, улучшить ваш персонаж или получить какие-либо игровые привилегии) за счет внесения реальных денег.

Как предостеречь детей от игр на деньги?

1. Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному).

2. Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей.

3. Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

4. Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги.

5. Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца.

6. Контролируйте поведение своих детей в Интернете. Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

Интернет-зависимость

То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление

Сети, полагая, что она – безграничный источник новых знаний. Вскоре выяснилось, что подростки не столько пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в он-лайновые игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей; Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени, появляется интернет-зависимость.

Обратите внимание на психологические особенности вашего ребенка. Социально дезадаптированные дети имеют повышенную вероятность к приобретению Интернет-зависимости. Причина в том, что Интернет позволяет оставаться анонимным, не бояться осуждения (если что-то сделал неправильно, всегда можно поменять имя и начать все заново), предоставляет гораздо более широкий выбор возможностей к общению, чем реальный мир.

В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет комфортным. Поэтому, если у ребенка что-то не получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

Интернет-зависимость – навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам Интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в Интернет.

В случае Интернет-зависимости выделяют следующие типы онлайн-активности:

- навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации,
- пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети),

- игровая зависимость – навязчивое увлечение компьютерными играми по сети,
- навязчивое желание потратить деньги – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянное участие в интернет-аукционах,
- пристрастие к просмотру фильмов через Интернет.

Рекомендации по предупреждению Интернет-зависимости

В первую очередь необходимо обратить внимание на возможные признаки Интернет-зависимости у вашего ребенка.

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.
2. Поговорите с ребенком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.
3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.
4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в Интернет с помощью телефона или иных мобильных устройств во время урока.

Если вы обнаружили возможные симптомы Интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
2. Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения

домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.

3. Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.

4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий – например, от бездумного обновления странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями – при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.

6. Дети с Интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время «выпадет» из жизни Интернет-сообщества.

7. В случае серьезных проблем обратитесь за помощью к специалисту.

Правила безопасности при работе в социальных сетях

Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют.

Одна из ключевых проблем социальных сетей - открытось большинства учетных записей. В частности, по различным оценкам, порядка 500 миллионов пользователей социальных сетей по всему миру держат свою частную информацию в открытом доступе, а эта информация может собираться с помощью автоматизированных решений. К примеру, подобный функционал может быть встроен во всевозможные приложения, которыми славится один из самых популярных подобных сервисов Facebook. Кроме того, пользователи социальных сетей регулярно становятся жертвами спама - на данный момент порядка 57% учетных записей в рамках подобных сервисов получают спам, а это 76-процентный рост по сравнению с показателем 2009 года. Ни для кого не секрет, что **в социальных сетях** хранится много нежелательной информации: экстремистской информации, призывы к разжиганию национальной ненависти, порнография и т.п.. Существует еще одна опасность - социальные сети становятся неизлечимой зависимостью. Люди перестают общаться в реальной жизни, превращаясь в зомби.

Рекомендации при работе в социальных сетях.

Проявляйте осторожность при переходе по ссылкам, которые **вы получаете в сообщениях от других пользователей или друзей.** Не следует бездумно открывать все ссылки подряд - сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.

- **Контролируйте информацию о себе, которую вы размещаете.** Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля, система может предлагать ответить на секретный вопрос. Это может быть дата вашего рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или старайтесь не использовать личные сведения, которые легко найти в сети.
- **Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.** Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет

лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно также необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.

- **Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.** При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны указывать то, что эти адреса электронной почты будут использованы для этой данной, но зачастую не делают этого.
- **Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.** Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.
- **Не добавляйте в друзья в социальных сетях всех подряд.** Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.
- **Не регистрируйтесь во всех социальных сетях без разбора.** Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которой требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.
- **Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.** На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, не смотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.
- **Проявляйте осторожность при установке приложений или дополнений для социальных сетей.** Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться также серьёзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.
- **Старайтесь не посещать социальные сети с рабочего места.** Любая социальная сеть может стать средой для распространения вирусов и других

вредоносных или шпионских программ, что может привести не только к заражению вашего компьютера и всей корпоративной сети, но и к потере данных, составляющих коммерческую тайну вашей компании .

- **Расскажите вашим детям об опасностях, которые могут подстерегать их в социальных сетях.** Если ваши дети посещают социальные сети, расскажите им о правилах безопасного пользования этими ресурсами.

Куда обращаться, чтобы защитить ребенка

Фонд поддержки детей, находящихся в трудной жизненной ситуации - общероссийский проект "телефон доверия". По телефону **8-800-2000-122** предоставляются психологические консультации по проблемам насилия и принуждения к сексуальной эксплуатации, оказывается помощь жертвам подобных преступлений, а также консультации по всем психологическим проблемам детей и подростков. Все консультации, а также звонок на телефонный номер Линии помощи, бесплатны; консультации предоставляются круглосуточно.

На сайте Фонда **http://www.fond-detyam.ru** можно получить консультации, вступив в переписку со специалистами Фонда

На сайте **http://www.ya-roditel.ru** есть полезные материалы, адресованные родителям, обеспокоенным интернет-угрозами детям.

Центр безопасного интернета в России

1. На сайте **www.saferunet.ru** необходимо кликнуть на красный баннер "горячая линия" и сообщить о противоправном контенте.

2. Там же: линия помощи - консультации по вопросам Интернет-угроз.

Линия помощи работает в Интернет-варианте:

- по всем вопросам, связанным с безопасным использованием Интернета - посредством тематических веб-форм обращений на сайте, или через электронную почту **helpline@saferunet.ru** ;

- по общим вопросам, в том числе по вопросам, связанным с безопасным использованием Интернета – посредством тематических веб-форм на специальном сайте **www.psyhelpline.ru**

Линия помощи "Дети - онлайн"

Линия помощи "Дети - онлайн" — служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками интернета и мобильной связи.

Обратиться на линию помощи можно:
- телефон **8-800-250-00-15** (звонить с 9.00 до 18.00 по рабочим дням, время московское, звонки по России бесплатные)
- по электронной почте **helpline@detionline.com**
- на сайте **www.detionline.com**

Информационные ресурсы

1. http://www.nachalka.com/bezopasnost
2. http://detionline.com/helpline/rules/parents Дети России онлайн
3. http://www.ifap.ru/library/book099.pdf
4. http://www.fid.su/projects/journal/ - фонд развития Интернет
5. http://stopfraud.megafon.ru/parents/ - безопасный интернет от Мегафона
6. http://www.mts.ru/help/useful_data/safety/ -безопасный Интернет от МТС
7. http://safe.beeline.ru/index.wbp - безопасный Интернет от Билайн
8. http://www.saferunet.ru/ - горячая линия по безопасному Интернету
9. http://www.microsoft.com/ru-ru/security/default.aspx

Список терминов

Блог (англ. **blog**, от web log — интернет-журнал событий, интернет-дневник, онлайн-дневник) — веб-сайт, основное содержимое которого — регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа.

Веб-обозрева́тель, бра́узер (от англ. *Web browser)* - программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой.

Видеохо́стинг — сайт, позволяющий загружать и просматривать **видео** в браузере, например через специальный проигрыватель.

Вишинг - разновидность фишинга - распространенным сетевым мошенничеством, когда клиенты какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п.

При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в Интернете достаточно сложно.

Интернет-мошенничество или кибермошенничество – это один из видов киберпреступления, целью которого является обман пользователей.

Кибербуллинг (cyber-bullying) - это виртуальный террор, чаще всего подростковый.

Контент - (от английского content - содержание) – это абсолютно любое информационно значимое, содержательное наполнение информационного ресурса или веб-сайта. Контентом называются тексты, мультимедиа, графика.

Социальная сеть (от англ. **social** networking service) — платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации **социальных** взаимоотношений.

Фарминг (англ. *pharming*) — это процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура (файл hosts, система доменных имен (DNS)).

Фишинг (от англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) – это вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным - логинам и паролям.

Фишинг-атаки проводятся через электронную почту, всплывающие сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера.

Нигери́йские пи́сьма — распространённый вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама).

Приложение 1

Рекомендуемые Интернет –фильтры

Интернет–фильтры позволяют ограничить доступ в Интернет. Такие программы умеют блокировать доступ к определенным сайтам, например порноресурсам, сайтам с информацией об оружии и наркотиках, а также для контроля времени нахождения в сети.

1. **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% защиту от опасных и нежелательных материалов. 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 организациях – образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

Фильтр «Интернет Цензор» можете скачать бесплатно на официальном сайте http://www.icensor.ru/

2. **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, и тем, что содержат вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, пиринговых сетей и сайтов знакомств. Что и говорить, сурово, но порой лучше перебдеть. Впрочем, можно изменить уровень фильтрации в разделе «Правила > Запрет категорий». Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания (загрузки) видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. Причем, данное приложение понимает любые сетевые протоколы, используемые для загрузки файлов. 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.

3. Kaspersky Internet Security 2011 (www.kaspersky.ru, 105 Мбайт) – антивирусная программ, которая защищает ваш компьютер от вирусов и в состав которого входит модуль родительского контроля. Приложение способно не только ограничивать время, проводимое за компьютером, но и контролировать общение детей при использовании различных Интернет-пейджеров, например, ICQ (поддерживаются клиентские приложения для

сетей MSN, Jabber, IRC, Mail.ru и Yahoo).Действия подрастающего поколения в социальных сетях (FaceBook, MySpace, Twitter) тоже не останутся без внимания модуля родительского контроля, причем, в определенных случаях, можно не только создать «черный список» для контактов, но и произвести запись сообщений. Для ограничения доступа к веб-ресурсам предусмотрено 14 категорий – родителям достаточно включить нужные. Если ресурс, к которому ребенок стремится получить доступ, не найден в базе данных, будет произведен эвристический анализ веб-страницы. Другой интересный момент касается запрета передачи конфиденциальных данных, например, реквизитов банковской карты или домашнего адреса (на тот случай, если чадо вознамерится оплатить какие-либо услуги). Модуль родительского контроля позволит запретить загрузку следующих типов файлов: «Музыка», «Видео», «Программы» и «Архивы». Однако данный запрет действует лишь при использовании протокола HTTP, и если ваш ребенок знаком с премудростями FTP или использует локальный прокси с нестандартным портом, то без труда обойдет такое ограничение. К сожалению, модуль родительского контроля KIS 2011 не поддерживает фильтрацию по протоколам.

4. Интернет-фильтр «Кибер Папа» бесплатная программа, которая ограничивает возможности ребенка выйти за пределы детского Интернета при использовании любого браузера.
Программа работает по принципу «белого списка» и чрезвычайно проста в использовании. После инсталляции программы и включения фильтра, ребенок может переходить только по страницам проверенных детских сайтов (блокируются также все статические и динамические объекты веб-страниц, не принадлежащие к списку проверенных детских ресурсов).
Отключить фильтр могут только родители, используя известный им пароль от программы.
Скачать можно программу на официальном сайте http://cyberpapa.ru/

5. KidsControl - программа предназначена для ограничения доступа детей к нежелательным Интернет ресурсам, а также для контроля времени нахождения в сети. С помощью программы вы можете установить ограничение доступа к нежелательным ресурсам по различным категориям – сайтам, с содержанием информации для взрослых, online-играм и казино, форумам, указав галочкой на определенную категорию, и установить ограничение самостоятельно с помощью черного списка. Скачать можно программу на официальном сайте http://www.kidscontrol.ru/

Приложение 2

Настройка родительского контроля в операционной системе

Функции "родительского контроля" есть даже в популярной сегодня операционной системе Windows 7, которая устанавливается на большинство новых компьютеров и ноутбуков. В частности, Windows 7 дает возможность ограничивать время, которое ребенок проводит за компьютером: вы можете, скажем, разрешить ему играть в игры или пользоваться социальными сетями 2-3 часа в день. Остальное время молодой человек пусть проведет на улице или в каком-нибудь развивающем кружке, которых, к счастью, сейчас предостаточно не только в Москве и других крупных городах. Еще операционная система от Windows позволяет устанавливать запрет на доступ детей к тем или иным играм или программам. Например, если вы не хотите, чтобы ребенок смотрел мультфильмы или фильмы, хранящиеся на жестком диске, можно запретить запуск мультимедийного плеера.

О том, как включить "родительский контроль" в Windows 7 и других операционных системах этого семейства, можно узнать на сайте windows.microsoft.com/ru-RU. Если подвести курсор мыши к меню "Помощь", вы увидите выпадающее меню. Выберите в нем вашу систему - Windows 7, Vista и так далее. После этого в открывшемся разделе найдите пункт "Безопасность" и перейдите в него. В нижней части правого меню вы увидите раздел "Родительский контроль", где находятся подробные сведения о возможностях этой функции и даются советы по настройке.

Настройка безопасности в поисковых системах

Родителям следует знать, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые с легкостью можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска», которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

В Google фильтрация результатов поиска включается в разделе "Настройки поиска", который появляется при клике мыши на значок шестеренки в правом верхнем углу заглавной страницы www.google.ru. В меню "Безопасный поиск" установите режим "Строгая фильтрация", который предусматривает отсеивание непристойных картинок и текста. Не забудьте нажать кнопку "Сохранить настройки".

Применять фильтр к результатам поиска позволяет и Яндекс. В разделе "Настройки - Остальное" есть пункт "Настройка результатов поиска", а в нем - меню "Фильтрация страниц".