Методические рекомендации «Интернет – территория безопасности»

Важная задача для педагогов - научить детей ориентироваться в киберпространстве, найти эффективные пути их полноценного развития в современных условиях неограниченного доступа к информации (телевидение, интернет и т.д.) и – одновременно – формирования информационного иммунитета, который проявляется в невосприимчивости личности к негативным воздействиям, в умении выявить, идентифицировать угрозы, содержащиеся в информации и защититься от них.

Педагогическое воздействие необходимо направлять не только на формирование умения работать с информацией, но и на формирование умения защищаться от негативного ее воздействия с раннего школьного возраста.

Рекомендации «Интернет – территория безопасности» адресованы руководящим и педагогическим работникам образовательных организаций, родителям обучающихся, детям разного возраста.

г.Зима – 2013г.

Оглавление

Введение

Серьезной и глобально значимой проблемой стало злоупотребление плодами информационно-коммуникационных технологий и их использование для совершения преступлений против детей.

Дети особенно уязвимы в условиях интенсивного развития новых информационных технологий (интернета, мобильной и иных видов электронной связи, цифрового вещания), доступности СМИ, распространения информационно-телекоммуникационных сетей общественного пользования, интенсивного оборота рекламной продукции, электронных и компьютерных игр, кино-, видео-, иных аудиовизуальных сообщений и материалов. Их бесконтрольное использование нередко оказывает на детей психотравмирующее и растлевающее влияние, побуждает их к рискованному, агрессивному, жестокому, антиобщественному поведению, облегчает их вовлечение в криминальную деятельность, развратные действия, азартные игры, тоталитарные секты и иные деструктивные организации.

Сегодня возникло устойчивое понимание того, что проблема детской безопасности в современном информационном пространстве – это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального, до регионального, государственного и международного.

Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

Медиаобразование выполняет важную функцию защиты от противоправного и манипуляционного воздействия средств массовой коммуникации, а также способствует предупреждению криминальных посягательств на детей с использованием информационно-телекоммуникационных сетей.

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права. Международные стандарты в области информационной безопасности детей нашли отражение и в российском законодательстве.

Принятый 29 декабря 2010 года Федеральный закон Российской Федерации № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила медиа-безопасности детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях подвижной радиотелефонной связи. Закон определяет информационную безопасность детей как состояние защищенности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному нравственному развитию. Кроме того, принят Федеральный закон Российской Федерации от 21 июля 2011 г. № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию", направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребенке порочные наклонности, сформировать у ребенка искаженную картину мира и неправильные жизненные установки. Закон устанавливает порядок прекращения распространения продукции средств массовой информации, осуществляемого с нарушением законодательно установленных требований.

Каждый выпуск периодического печатного издания, каждая копия аудио-, видео- или кинохроникальной программы должны содержать знак информационной продукции, а при демонстрации кинохроникальных программ и при каждом выходе в эфир радиопрограмм, телепрограмм они должны сопровождаться сообщением об ограничении их распространения.

Закон запрещает размещение рекламы в учебниках, учебных пособиях, другой учебной литературе, предназначенных для обучения детей, а также распространение рекламы, содержащей информацию, запрещенную для распространения среди детей, в детских образовательных организациях.

Учитывая следующие обстоятельства такие как:

· большое количество детей, находящихся в социально неблагополучных условиях,

· их высокую уязвимость для лиц, совершающих противоправные действия с применением высоких технологий,

· массовое проникновение Интернет-технологий в России,

· быстроту распространения информации в сети Интернет,

одной из важных и первостепенных проблем является необходимость защиты несовершеннолетних от противоправных действий с использованием сети Интернет.

Постоянное развитие Интернет-технологий и их широкое проникновение в общество ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий. Эффективное функционирование такого комплекса представляется возможным в условиях широкого вовлечения пользователей Интернета по принципу социально-ответственного «электронного гражданина» на основе общественно-государственного партнерства. Для реализации такого комплекса мер был создан центр безопасного интернета России при финансовой поддержке Федерального агентства по печати и массовым коммуникациям (http://www.saferunet.ru).

В обеспечении мер по Интернет-безопасности образовательное учреждение должно играть ключевую роль, так как в современной школе обучение проводится с использованием технологий, отвечающих своему времени, имеются в виду информационно-коммуникационные технологии. Поэтому школа должна взять на себя главную ответственность за развитие у детей и их родителей цифровой грамотности и обучение их навыкам безопасности.

Решение задачи по обеспечению безопасности при использовании компьютера и интернета детьми требует комплексного подхода, решения множества психолого-педагогических вопросов. Эти направления должны стать основой для решения проблем медиабезопасности в образовательных учреждениях. Стимулируя детей к более широкому разнообразию онлайн-деятельности и одновременно с этим обучая их критически оценивать ресурсы, развивая навыки безопасного поведения в сети, педагоги приумножают те преимущества, которые дает обучение в онлайне, усиливает защиту наших детей и повышают компетентность всех участников образовательного процесса. Особые усилия необходимы в отношении наименее привилегированных и самых младших детей. Нормативно-правое обеспечение является основой деятельности образовательного учреждения по всем направлениям. В образовательном учреждении должен быть сформирован пакет нормативно-правовой документации федерального, регионального и муниципального и учрежденческого уровней по вопросам информационной безопасности. К таким документам относятся документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет как педагогических работников, так и школьников, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет-безопасности, правила

безопасного поведения в сети Интернет. В образовательном учреждении приказами должны быть назначены лица, ответственные за контентную фильтрацию, за работу с персональными данными, за организацией работы школьников в сети Интернет и т.д. В организационном плане по обеспечению информационной и медиабезопасности в образовательном учреждении должен выполняться ряд мер технико-технологической направленности:

- установка только лицензионного программного обеспечения,
- подключение к системе контентной фильтрации;
- установка антивирусных программ,
-установка и настройка программ-фильтров, брандмауэров.

К организационным внутришкольным мероприятиям относятся:

- разработка и реализация правил Интернет-безопасности, с привлечением заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщиков услуг интернета,
- организация работы детей в Интернет по расписанию с ограничением по времени под наблюдением педагогических работников,
- регулярная проверка принимаемых мер в области Интернет безопасности в образовательном учреждении.

Для организации профилактической работы по медиабезопасности с детьми и родителями педагогический работник должен знать проблемы и опасности, которые подстерегают пользователя в сети Интернет, и быть готов дать рекомендации по решению данных проблем.

Для организации профилактических мер в образовательном учреждении необходимо периодически проводить мониторинг, диагностику проблем по Интернет-безопасности среди детей и родителей. Данный мониторинг и разъяснительную работу можно проводить в Интернет-проекте «Дневник.ру». В этом проекте реализованы функции школьного модератора, в обязанности которого входит модерация нежелательного содержания в сети проекта и есть возможность применять действенные санкции к нарушителям правил пользования интернетом. В Интернет-проекте «Дневник.ру» можно организовать виртуальные мероприятия с родителями по вопросам Интернет-безопасности, разместить рекомендации в электронном виде.

В аспекте программно-методического обеспечения в образовательном учреждении должна быть разработана программа (раздел, модуль комплексной программы по профилактике девиантного поведения детей), в которую должны быть включены темы по медиабезопасности, о безопасном поведении в сети Интернет. Такие же темы и проблемы должны включаться в программы воспитательной деятельности. Рекомендуемая тематика для организации профилактической деятельности:

- нежелательная информация в Интернете, как ее избежать (журнал «Дети в информационном пространстве» №1, статья - Опасный контент в Рунете по данным Национального Узла Интернет-безопасности в России).
- проблемы достоверности информации в Интернете, как проверить достоверность информации (журнал «Дети в информационном пространстве» №3 – Год безопасного интернета, раздел практикум, статья - Сайт сайту рознь).
- социальные сети: опасности и правила поведения в социальных сетях,
- кибермошенничества, как избежать кибермошенников,
- киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации (журнал «Дети в информационном пространстве» №2, статья Кибер-агрессоры).
- вредоносные программы, методы борьбы с ними
- полезные ссылки, ресурсы, сервисы в Интернете.

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, обществознания, ОБЖ, классных часов. В образовательном учреждении

рекомендуется проводить день медиабезопасности, уроки по Интернет-безопасности, внеклассные мероприятия и т.п.

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

- с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
- с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;
- с правилами общения в социальных сетях (сетевой этикет);
- ознакомить обучающихся с адресами помощи в случае интернет-угрозы, номером всероссийского детского телефона доверия (8-800-2500015), контактной информацией об аппарате Уполномоченного при Губернаторе Иркутской области по правам ребенка. *(Семенова Светлана Николаевна, тел:(3952) 34-19-17, сайт: http://irkutsk.rfdeti.ru, e-mail: irkutsk@rfdeti.ru Адрес: 664011, г. Иркутск, ул. Горького, д. 31, каб. 105)*

Тематика проведения различных школьных мероприятий по медиабезопасности может быть самой разнообразной, например:

- противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать,
- достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту,
- этика сетевого общения,
- личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.
- социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников,
- что такое хакерство: этика и основы,
- интернет- зависимость: угрозы, реальность, проблемы, решения (журнал «Дети в информационном пространстве» №4, статья - Опасная грань).
- Web-серфинг: как не потерять себя и свое время в Интернете,
- как распознать кибермошенничество и не стать жертвой,
- нигерийские письма: предложения в письмах и как не попасться на удочку мошенников,
- что такое киберхулиганство: как не стать жертвой и киберхулиганом;
- как защитить свою почту от спама и не стать спамером,
- компьютерные вирусы и методы борьбы с ними,
- киберпреступления в законодательстве России,
- безопасность в коммерческих Интернет-сервисах: Интернет-магазины, услуги различных фирм и др.,
- компьютерные игры, как не стать игроманом,
- азартные игры в Интернете – поле чудес для….?
- мобильные угрозы в современном мире,
- как правильно вести себя с киберхулиганами и защититься от нежелательного общения,
- твоя жизнь не игрушка.

Большое значение для эффективности мероприятий по медиа-безопасности имеет не только содержание, но и форма его проведения.

Целесообразно использовать следующие формы:

1-4 классов – урок-путешествие, урок-викторину, урок-соревнование, урок-игру, беседу;

5-8 классов – урок - пресс-конференцию, урок-викторину, урок-соревнование, урок-презентацию проектов, урок-практикум, урок-встречу со специалистами медиа-сферы, системными администраторами и т.д.;

9-11 классов – деловую игру, урок-презентацию проектов, день медиа-безопасности, мозговой штурм, дискуссию, дебаты, встречу со специалистами медиа-сферы, системными администраторами и т.д.

На уроках информатики для младших школьников рекомендуем использовать онлайн игры, содержащие основные понятия об устройстве Интернета, правилах работы в нем, в том числе — о сетевом этикете. Например, игра «Прогулка через дикий Интернет лес (Wild Web Wood)» (http://www.wildwebwoods.org), создана на основе справочника Совета Европы «Интернет-грамотность», переведена на русский язык и будет интересна детям младшего и среднего школьного возраста.

Компания МТС предлагает он-лайн урок по теме: «Полезный и безопасный Интернет» (http://www.detionline.com/mts/about).

Компания «Билайн» предлагает прослушать 9 уроков по безопасному использованию мобильной связи «Уроки мобильной грамотности».

Для проведения мероприятий по медиабезопасности рекомендуем использовать ссылки на информационные ресурсы, приведенные ниже в перечне информационных ресурсов.

1. Что надо знать педагогу об опасностях Интернета

Для обеспечения безопасности детей в сети Интернет и собственной безопасности необходимо знать виды Интернет-угроз, уметь их распознать и предотвратить. Для этого необходимо рассказать детям о виртуальном мире как можно больше, о его возможностях и опасностях. Необходимо проанализировать и затем вместе с детьми изучить интересные и полезные Интернет-ресурсы по безопасному поведению в сети Интернет. Необходимо научить детей и родителей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на нежелательный и агрессивный контент в Интернете, рассказать куда в подобном случае они могут обратится.

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.

Сегодняшние школьники легко осваивают любые устройства и технологии, предназначенные для общения и передачи информации. Однако насколько они готовы к тому, чтобы правильно ориентироваться в пространстве интернета, насколько способны противостоять тем рискам и угрозам, с которыми неизбежно сталкивается практически любой пользователь сети? И что необходимо делать государству, обществу, системе образования, родителям для того, чтобы защитить юных пользователей и помочь им освоиться в интернете? В рамках исследовательского проекта Еврокомиссии EU Kids Online II, посвященного изучению вопросов безопасности интернета для детей и подростков, были получены ответы на эти вопросы и подготовлены соответствующие рекомендации. Всего в исследовании приняли участие 25 стран Евросоюза, а также Россия и Австралия. Результаты исследования доступны на сайте http://detionline.com

Ситуация с мобильным интернетом стала весьма актуальна в России в течение последних полутора лет. По данным социологов, сегодня почти пользуется интернетом,

при этом каждый третий из них (18%) использует для выхода в интернет мобильный телефон или мобильное устройство. По данным нашего исследования, в России мобильным интернетом пользуется треть школьников 9-10 лет и 60% подростков 15-16 лет. В России каждый второй ребенок 9-10 лет пользуется интернетом ежедневно и почти треть - один-два раза в неделю. Частота пользования растет с возрастом: среди школьников старше 13 лет уже более 75% бывают онлайн ежедневно.

Самая популярная сеть среди российских детей ВКонтакте, которую ежедневно посещают более 20 млн пользователей (по данным Livelnternet), 89% опрошенных нами детей имеют там профиль. На втором месте Одноклассники — ее назвали 16% детей. Еще 4% школьников пользуются Facebook, 2% — MySpace и 5% — другими социальными сетями, среди которых на первом месте Мой Мир.

Учителей и родителей может порадовать полученный в исследовании обнадеживающий результат: 80% российских детей объявили, что пользуются интернетом в учебных целях. Возможно, это итог программы модернизации образования: дети могут узнавать домашние задания, следить за успеваемостью, отслеживать события и получать нужную информацию через школьные интернет-порталы.

В сентябре 2013г. ТРЦ было организовано он-лайн анкетирование школьников города Зимы на предмет навыков безопасного поведения в сети Интернет. Всего опрошено 965 обучающихся 5-11(12)-х классов. С полными результатами опроса можно ознакомиться на сайте ТРЦ www.ztrc.ru в разделе «Безопасный интернет».

2. Какие опасности поджидают пользователя в сети Интернет. Классификация рисков в сети Интернет.

2.1. 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. В данных рекомендациях дается информация о возможных рисках и опасностях в сети Интернет. Рекомендации для родителей по преодолению этих рисков приводятся в буклете «Интернет – территория безопасности Вашего ребенка», который можно найти на сайте ТРЦ www.ztrc.ru раздел «Безопасный интернет».

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 (журнал «Дети в информационном пространстве» №2, статья «Нужны ли мы себе?»).
- 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 иинтернет приводит к заражению компьютера вирусами. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь и возможность манипулировать данными и действиями зараженного и 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. Коммуникационные риски или риски общения в сети Интернет.

2.2. Коммуникационные риски. Знакомства в Интернете и встречи с Интернет-незнакомцами.

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.

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. Анонимность и приватность в сети - давно иллюзия. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против человека. "То, что попало в интернет, останется там навсегда, - напоминает Касперский (один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского»). -Завтра наши дети могут сильно пожалеть о своем поведении и оставленных следах в соцсетях. Это может негативно отразиться на их карьере, социальном статусе и вообще представляет собой благодатную почву для шантажа в будущем. Не говоря о том, что опубликованная информация может задеть и нас, родителей". 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.

2.3. 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.

2.4 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.

«Нигериийские письма» — распространённый вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причём ещё до распространения Интернета, когда такие письма распространялись по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине 1980-х гг. В 2005-м году нигерийским спамерам была присуждена антинобелевская (шнобелевская) премия по литературе.

Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п..

Наиболее часто письма отправляются от имени бывшего короля, президента, высокопоставленного чиновника или миллионера с просьбой о помощи в банковских операциях, связанных с переводом денег из Нигерии или другой страны за границу,

получением наследства и т. п., якобы облагаемых большим налогом или затруднённых по причине преследований в родной стране.

Другой распространённый вариант — письма, якобы, от работника банка или от чиновника, узнавшего о недавней смерти очень богатого человека «с такой же фамилией», как у получателя письма, с предложением оказать помощь в получении денег с банковского счёта этого человека.

В условиях современной жизни, многие люди находят весьма удобным для себя не тратить время на походы по магазинам. Ведь при помощи Интернета можно заказать все необходимое с доставкой на дом за несколько минут. Пара щелчков мышкой, быстрое оформление заказа и вскоре товар уже в ваших руках. К сожалению, не все так легко и просто, как представляется на первый взгляд. Мошенники не дремлют даже в Интернете и доверчивый пользователь вполне может оказаться ни с чем, заплатив при этом немало денег. Потребительский риск заключается в потере денежных средств без приобретения товара или услуги, или приобретения товара низкого качества, контрафактной и фальсифицированной продукцию.

3. Игровая и интернет зависимость.

Существует еще одна опасность – зависимость от компьютерных игр. Это – проблема, которой было уделено довольно много внимания в прессе и различных научных работах. К примеру, ученые выяснили, что 30% игроков проводят за компьютером слишком много времени, а 10% находятся в сильной психологической зависимости от своей любимой игры. Заодно посмотрели, чем эта зависимость иногда кончается – а кончается она плохо, и потому нуждается как минимум в научном присмотре. Что же такое эта «компьютерная игровая зависимость» и в чем она проявляется? Игровая зависимость являет собой форму сильной психологической привязанности к игре – в компьютерном варианте вплоть до желания жить в виртуальном мире. Возвращение в реальный мир связано исключительно с удовлетворением естественных потребностей, общение с живыми людьми сведено к минимуму. Особенно тяжелые формы игровой зависимости предполагают также крупные денежные траты на игру, злоупотребление кофе и энергетическими напитками, злость и раздражение при отрывании от игры, пренебрежение питанием и сном. Зависимость от игр сравнима с наркотиками и алкоголем, человек не может контролировать себя в плане времяпровождения за игрой, живет в своем собственном мире и не желает общаться с родными и друзьями – ибо они пока еще не «виртуальны». Любое время, проведенное вне игры, является для такого человека мучением.

Сегодня Всемирная паутина настолько тесно вплетена в нашу жизнь, что становится все трудней сказать, где заканчивается реальный мир и начинается виртуальный. С помощью Интернета можно делать все больше и больше. Но чрезмерное увлечение интернетом может привести к формированию болезненного пристрастия – зависимости. Как следствие – серьезные проблемы с учебой, работой, в отношениях с близкими людьми, вплоть до разрушения связей с родными и окружающим миром. Особую тревогу вызывает тот факт, что зависимости чаще всего подвергаются дети в подростковом возрасте. 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 онлайновые 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.

При необходимости у родителей должна быть возможность для обращения к школьному психологу. Школьный психолог должен быть знаком с проблемами Интернет-зависимости и может дать необходимые рекомендации родителям.

4. Социальные сети: некоторые аспекты безопасности.

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 и 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.

Анонимность и приватность в сети - давно иллюзия. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против человека. "То, что попало в интернет, останется там навсегда, - напоминает Касперский (один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского»). - Завтра наши дети могут сильно пожалеть о своем поведении и оставленных следах в соцсетях. Это может негативно отразиться на их карьере, социальном статусе и вообще представляет собой благодатную почву для шантажа в будущем. Не говоря о том, что опубликованная информация может задеть и нас, родителей". 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.

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 - «Безопасность детей в интернете», брошюра от microsoft
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 - Центр безопасного Интернета в России, горячая линия по безопасному Интернету.
9. http://www.microsoft.com/ru-ru/security/default.aspx - безопасный интернет от microsoft
10. http://www.mvd.ru/userfiles/broshyura_k_01_02_2012.pdf - брошюра МВД России «Безопасный интернет»

Глоссарий

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

Сетевой дневник
Общественный интерактивный дневник.

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

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

Дискуссионный форум
Место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация. В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором, который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

Загрузка
Сохранение файлов из Интернета на собственном компьютере.

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

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

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

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

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

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

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

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

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

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

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