Департамент культуры и туризма администрации Владимирской области

Государственное бюджетное учреждение культуры Владимирской области
«Владимирская областная библиотека для детей и молодежи»

Диалог on-line

Сборник материалов
II Межрегиональной конференции для детей,
молодежи и специалистов, работающих с детьми
и молодежью по Интернет-безопасности
в рамках государственной программы «Обеспечение
информационной безопасности детей, производства
информационной продукции для детей и оборота информационной
продукции во Владимирской области на 2014-2016 годы»

11 февраля 2014 года

Владимир
2014

ББК 78.38
Д 44

Составитель: Прохорова Н. С., заведующий отделом инновационно-мето-дической работы Владимирской областной библиотеки для детей и молодежи;
Пустовойтова Н. В., ведущий методист отдела инновационно-методической работы Владимирской областной библиотеки для детей и молодежи;

Ответственный за выпуск: Сдобникова Т. А., директор Владимирской областной библиотеки для детей и молодежи

Д44 **Диалог on-line:** сборник материалов II Межрегиональной конференции для детей, молодежи и специалистов, работающих с детьми и молодежью по Интернет-безопасности в рамках государственной программы «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2014-2016 годы», 11 февраля 2014 года / Департамент культуры и туризма администрации Владимирской области; Влад. обл. б-ка для детей и молодежи. Отдел иннов.-метод. работы. – Владимир, 2014. – 118 с.

Проблема информационной безопасности подрастающего поколения получила всестороннее рассмотрение в докладах участников конференции: от законодательных мер по защите детей в Интернете, влияния компьютера на здоровье ребенка, до правил поведения в социальных сетях и советов родителям по профилактике Интернет-зависимости у детей.

Материалы сборника публикуются с сохранением авторского стиля. Мнение авторов может не совпадать с позицией библиотеки.

Введение

Сборник составлен по итогам II Межрегиональной конференции для детей, молодежи и специалистов, работающих с детьми и молодежью по Интернет-безопасности «Диалог on-line», состоявшейся в рамках Недели безопасного Рунета 11 февраля 2014 года.

Второй год подряд Владимирская областная библиотека для детей и молодежи проводит это мероприятие при активной поддержке администрации Владимирской области и Владимирского филиала Российской Академии народного хозяйства и государственной службы при Президенте РФ.

В этом году конференция проходила в соответствии с государственной программой «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2014–2016 годы».

Анализируя итоги конференции, специалисты библиотеки отмечают неослабевающий интерес общества к проблемам безопасного использования интернет-контента. Более 190 человек приняли участие в работе конференции (среди них – учащиеся старших классов школ, студенты колледжей и ВУЗов г. Владимира и области).

С приветственным словом к собравшимся обратились представители администрации, Законодательного Собрания, Общественной палаты Владимирской области.

На Пленарном Заседании были заслушаны доклады: председателя комитета Законодательного Собрания по вопросам здравоохранения, демографии, материнства и детства, заслуженного врача РФ И. М. Кирюхиной, председателя Общественной палаты Владимирской области, профессора Н. В. Юдиной; старшего помощника руководителя следственного управления СК РФ по Владимирской области, полковника юстиции И. А. Мининой; аналитика некоммерческого партнерства «Лига безопасного Интернета В. Е. Пономарева (г. Москва); доктора политических наук Р. В. Евстифеева.

В рамках конференции работали 2 секции: «Интернет-контроль» – для специалистов и «Интернет без бед» – для молодежи.

Присутствовавшие на секции «Интернет-контроль» были ознакомлены с деятельностью внештатного сотрудника полиции по выявлению интернет-преступлений против детей и получили комплексный анализ проблемной ситуации; узнали о способах организа-

ции поиска пропавших детей посредством Интернет. Преподаватели ВУЗов, средних общеобразовательных и профессиональных учебных заведений, специалисты библиотек г. Владимира и области, а также Рязани и Нижнего Новгорода поделились с присутствующими опытом по решению проблем Интернет-безопасности, уделив особое внимание вопросам детской и подростковой Интернет-зависимости, отмечая недостаточные усилия общества в деле просвещения родителей. Отдельно был рассмотрен вопрос профилактики зависимости нетрадиционным способом – с помощью театрального искусства.

Интерактивная беседа «Интернет-зависимость: как избавиться от нее и вернуться в реальность» стала особенностью работы молодежной секции. Психологи Владимирской областной библиотеки для детей и молодежи провели дискуссию о причинах формирования Интернет-зависимости, экспресс-тест по ее диагностике и рассказали о способах профилактики. Кроме того, простые упражнения позволили участникам секции задуматься о реальной ценности виртуального и реального миров. Также были озвучены способы защиты личной информации и достижения анонимности при работе или общении в Интернете; присутствующим напомнили об основных видах мошенничества в сети и необходимых мерах безопасности.

Все участники конференции были единодушны во мнении, что необходимо создавать и продвигать позитивный контент в Интернете, повышать квалификацию специалистов, работающих с детьми и их родителями, развивать культуру грамотного использования сети.

Организаторы конференции отмечают: круг вопросов, касающихся проблем Интернет-безопасности, с каждым годом расширяется. Однако взаимодействие неравнодушных специалистов в области науки и образования, культуры и искусства, информационных технологий и здравоохранения способствует формированию в обществе грамотного отношения к Интернет-пространству и его критической оценке. Впереди наиболее сложный и ответственный этап – обучение медиаграмотности каждого человека, независимо от его возраста, финансового и социального положения, так как информационные технологии сейчас участвуют в регулировании всех значимых сфер жизни.

В данном сборнике представлены 23 доклада участников конференции. Порядок размещения – хронологический, в соответствии с выступлениями докладчиков.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

И. М. Кирюхина,
г. Владимир

Влияние компьютера на здоровье детей и подростков, меры профилактики вредного воздействия компьютера на организм

В связи с техническим прогрессом компьютеры прочно вошли в жизнь человека. Не только взрослые, но и подростки, и даже дети не представляют себе жизнь без компьютера и мобильного телефона. Получение информации, образования, досуг обеспечивает компьютер. Компьютеры стали настолько обыденными, что забылись связанные с ними опасности для физического и психического здоровья. При неправильном применении компьютер может явиться источником негативного воздействия на человека и приносить вред здоровью так же, как и другие достижения технического прогресса: будь то самолет, автомобиль, станок или иной механизм. Из помощника и даже друга он может превратиться во врага, наносящего вред здоровью и развитию молодого организма.

Компьютер стал заменять многие активные действия людей: поход в кино, театр, библиотеку, в магазин – все можно получить из Интернета. Многие образовательные программы проходят в форме дистанционного обучения. Погружаясь в виртуальный мир, человек как бы отгораживается от реальности, перестает интересоваться окружающим, забывая простые общечеловеческие ценности, такие как: доброта, мир, любовь, семья, забота о близких, соучастие и сострадание.

Дети, подростки находятся в возрасте формирования личности и получают «компьютерное» воспитание, техногенное, не свойственное человеческой личности, бездуховное. Компьютер заменяет многим детям общение со сверстниками. Нередко в компьютере появляется нежелательная информация, носящая аморальный, агрессивный или циничный характер. Через компьютер может происходить воздействие на ребенка и подростка криминальных личностей, психически больных людей.

Дети меньше гуляют на свежем воздухе, ведут малоподвижный образ жизни. Уединение с компьютером в изолированном помещении приводит к кислородному голоданию, гипоксии, что наносит вред ЦНС, нарушает сон, устойчивость к стрессам. Многие дети нарушают режим дня, теряют ощущение времени, пропускают еду, сон, полезные занятия, уроки. Дети нервничают и расстраиваются, когда у них что-либо не получается. Опасность психических заболеваний грозит каждому, кто проводит за видеоиграми более 2-х часов.

Компьютер может вызвать зависимость, когда подросток без компьютера становится беспомощным, неуверенным в себе, вплоть до панического состояния. Данная зависимость подобна наркотической и относится к психической патологии, требующей лечения.

Лучевая трубка монитора является источником электромагнитного излучения, которое вызывает усталость, снижение работоспособности, ослабляет иммунитет.

Перевод взгляда с экрана на клавиатуру, световая пульсация экрана вызывают напряжение глазных мышц, что неблагоприятно влияет на зрение. Детям и подросткам с патологией зрения занятия на компьютере могут быть противопоказаны.

Страдает опорно-двигательный аппарат: спина, руки в области запястья от однообразных монотонных действий. Ситуацию усугубляет использование неприспособленной мебели, плохая освещенность, влажность и свежесть воздуха.

Даже у взрослых – с медицинской точки зрения – работа на компьютере считается вредной и регламентируется документом СаНПиН 2.2.2/2.4. 1340–03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы». В этом документе регламентированы требования к помещению, микроклимату, содержанию вредных химических веществ в воздухе, уровням шума и вибрации, освещению, уровню электромагнитных полей на рабочих местах, медицинское обслуживание работников, работающих за компьютером. Помещение, где расположен рабочий компьютер, должно проветриваться после каждого часа работы за компьютером, должна проводиться ежедневная влажная уборка. Окна должны иметь жалюзи, должно быть защитное заземление.

Особое требование предъявляется к мебели и – особенно – к стулу. Замена стула табуретками и скамейками – недопустима.

Работа с компьютером требует систематических перерывов, ограничения времени работы. Рекомендуются упражнения для глаз, физкультурные минутки для снятия утомления мышц туловища и конечностей.

Лица, работающие с компьютером более 50% рабочего времени, должны проходить обязательные предварительные медицинские осмотры при поступлении на работу, а работая,– периодические медицинские осмотры.

Беременные женщины переводятся на работу, не связанную с использованием персонального компьютера, или для них ограничивается время работы на компьютере до 3-х часов за рабочую смену.

Студенты, учащиеся, дети дошкольного и школьного возраста должны проходить медицинское освидетельствование на предмет установления противопоказаний к работе на компьютере.

Так, для студентов первокурсников оптимальное время работы на компьютере – 1 час; для студентов старших курсов – 2 часа с перерывом через каждый академический час на 15–20 минут.

Для детей школьного возраста установлено ограничение непрерывной деятельности работы, связанной с фиксацией взора на экране дисплея:

№ п/п	Классы	Время	Число занятий в течение дня
1.	Учащиеся 1–4 классов	15 минут	1
2.	Учащиеся 5–7 классов	20 минут	2
3.	Учащиеся 8 класса	25 минут	2
4.	Учащиеся 9 класса	25 минут	3
5.	Учащиеся 10–11 классов	30 минут	3

Внеучебные занятия на компьютере рекомендуются не чаще 2-х раз в неделю продолжительностью:

– для учащихся 2–5 кл.– не более 60 минут;
– для учащихся 6–11 кл.– не более 90 минут.

Детям дошкольного возраста (5 лет) рекомендуется проводить развивающие игровые занятия не более 10 минут, в возрасте 6 лет –

15 минут. Эти занятия должны проводиться в присутствии родителей, воспитателей или педагога.

Настоящие санитарно-эпидемиологические правила и нормативы разработаны в соответствии с Федеральным законом № 52-ФЗ от 30 марта 1999 г. и называются «О санитарно-эпидемиологическом благополучии населения». Они направлены на предотвращение неблагоприятного влияния на здоровье человека вредных факторов при работе на компьютере.

Родители, отдавая ребенка на «воспитание компьютеру», не проводят контроль над ограничениями, предусмотренными санитарными правилами, не формируют у ребенка бережное отношение к своему здоровью. Взрослые, родители должны установить для детей временные ограничения при работе за компьютером, организовать рабочее место ребенка за компьютером.

Кроме защиты здоровья ребенка от воздействия компьютера, родители должны защитить детей от наносящей вред информации. Родители должны быть в курсе того, чем занимаются их дети в Интернете.

Дети не должны давать информацию о себе, выкладывать фото, свое или семьи. Нельзя открывать файлы, присланные от неизвестных людей – они могут содержать вирусы или фото, видео с нежелательным содержанием. Дети должны знать, что люди в Интернете могут говорить неправду и быть не теми, за кого себя выдают, иногда выбирая образ, противоречащий морали и общечеловеческим ценностям. Дети не должны встречаться с сетевыми друзьями в реальной жизни без взрослых.

В современном мире компьютер прочно вошел в жизнь не только взрослых, но и молодых людей, и даже детей. Умный, нужный, полезный – компьютер при неправильном использовании может стать опасным, вредным, подрывающим здоровье, вызывающим болезни. Именно от взрослых и – прежде всего – от родителей зависит, кем станет компьютер для ребенка.

И. А. Минина,
г. Владимир

Профилактика правонарушений с использованием сети Интернет

Уважаемые участники конференции!

В 2013 году возбуждено 124 уголовных дела о преступлениях, совершенных в отношении детей, из них по фактам убийств – 6; причинению тяжкого вреда здоровью – 8. Почти в 3 раза больше, чем в 2012 году, возбуждено уголовных дел по фактам изнасилования – 60; в связи с совершением развратных и иных действий сексуального насилия – 19. По уголовным делам признаны потерпевшими 138 несовершеннолетних, в том числе в возрасте до 1 года – 9; от 1 года до 14 лет – 90. Более 15 несовершеннолетних пострадали от преступных посягательств со стороны близких, членов семьи, что признается абсолютно парадоксальным явлением.

От преступных посягательств погибло 22 ребенка.

Следственное управление уделяет огромное внимание профилактике преступности против детей, в каждом случае изучаются причины и условия совершенных преступлений.

Отмечаем, что в отличие от предыдущих периодов, сегодня ребенок – вне зависимости от среды проживания – может стать жертвой злоумышленников.

Информационное пространство, призванное иметь позитивное, образовательное, познавательное значение, становится площадкой для недобросовестных людей, имеющих целью завладеть вниманием подростков, вовлечь их в свои пагубные пристрастия или совершить в отношении ребенка преступление.

На основе судебно-следственной практики мы утверждаем: виртуальный мир способен нанести вред ребенку.

На современном этапе произошли серьезные изменения, связанные с неограниченной доступностью детей к СМИ, средствам мобильной связи, сети Интернет, при которой в силу возраста, не обладая способностью фильтровать качество информации, они бесконтрольно посещают небезопасные Интернет-сайты, самостоятельно

выходят посредством системы «Skype» на связь, в том числе – с посторонними лицами.

В качестве свидетельства вывода приведу несколько примеров из следственной практики.

В декабре 2012 года возбуждено уголовное дело по факту совершения насильственных действий сексуального характера в отношении 9-летней жительницы города Коврова. По данным следствия, в ноябре 2012 года, используя сеть Интернет, через программу двусторонней видеосвязи «Skype» взрослый мужчина неоднократно связывался с ребенком и, используя ее беспомощное состояние, обусловленное малолетним возрастом, совершал противоправные действия, выразившиеся в склонении потерпевшей к обнажению и демонстрации частей тела. Мужчина, зарегистрированный в сети Интернет под различными псевдонимами, общался с девочкой в обнаженном виде с закрытым медицинской маской лицом. Проведенными оперативно-розыскными мероприятиями удалось установить личность злоумышленника, это – гражданин одной из бывших союзных республик, и сейчас следствие принимает меры к привлечению иностранного гражданина к уголовной ответственности.

Еще один любитель «острых ощущений» – 56-летний житель Вязниковского района – на протяжении нескольких лет размещал в Интернете объявления, вел активную переписку пикантного содержания с несовершеннолетними девочками, которых призывал стать благородными девицами. Православный поэт – как он себя называет – соблазнял детей деньгами, красивой одеждой, подарками, угощениями, алкоголем под предлогом развития и дополнительного образования в так называемой «школе благородных девиц». Поскольку многим детям из неблагополучных и малообеспеченных семей было недоступно предлагаемое, они подчинялись установленным правилам. В уголовном деле уже 5 потерпевших в возрасте 11,12 и 13 лет, а всего детей, посещавших «поэта» – не менее 20 человек.

Расследование по уголовному делу продолжается, в отношении обвиняемого проводится сексолого-психолого-психиатрическая экспертиза. Однако возникает и параллельный вопрос: откуда приходили ребята в нетрезвом состоянии, с подарками – родителей, в том числе благополучных, видимо, не интересовало?

Приведенные случаи не единичны. Исходя из данных Следственного комитета России, имеют достаточно широкое распространение. В связи с этим мы констатируем появление нового вида преступлений – Интернет-педофилии.

Большое опасение вызывают сайты – продавцы психотропных и наркотических веществ. Распространенность фактов незаконного оборота опасных для жизни и здоровья веществ таким способом может приобрести непредсказуемые масштабы. Молодых людей, вступающих в переписку с продавцами, действующими по принципу бесконтактной схемы, сначала завлекают бесплатной передачей «пробника», а затем вызывают у них привязанность к веществам и потребность постоянного приобретения наркотика за деньги. Следователями расследовано уже 6 уголовных дел данной категории.

Следующая опасная составляющая – вовлечение несовершеннолетних через сеть Интернет в преступную экстремистскую деятельность.

В октябре 2013 года на основе собранных следователем Следственного комитета доказательств судом вынесен приговор 31 летнему жителю города Владимира. Обладая националистическими взглядами, проявляя интерес к идеологии, материалам и субкультуре националистического толка, на своей странице в социальной сети мужчина поместил анкету, привлекая внимание молодых людей с неустойчивым, управляемым сознанием. Таким способом в состав экстремистского сообщества он собрал более 15 несовершеннолетних.

Являясь психологически волевым человеком, используя свое возрастное превосходство, лидер группировки систематически проводил с подростками разъяснительные тактические беседы, снабжал их соответствующей литературой, видео- и аудио материалами, фактически навязывая цель действий – преследование лиц неславянской внешности и происхождения, евреев, активистов оппозиционного движения «Антифа» и совершение преступлений против личности, собственности, общественной безопасности порядка. За время деятельности членами неонацистской группы совершено 14 преступлений экстремистской направленности различной тяжести, в том числе – по умышленному причинению вреда здоровью граждан, грабежам и разбоям. По ряду уголовных дел уже вынесены обвинительные приговоры.

10 февраля 2014 года возбуждено уголовное дело по признакам преступления, предусматривающего ответственность за нарушение неприкосновенности частной жизни. Установлено, что в декабре 2012 года в ходе переписки с молодым человеком в социальной сети «Вконтакте» 10-летняя девочка ответила на его предложение прислать фото в обнаженном виде в обмен на условные «20 голосов». Малолетний ребенок самостоятельно в ванной комнате сфотографировала себя в обнаженном виде и отправила фотографии парню. Впоследствии фото были распространены в социальной сети, в том числе среди учащихся школы, где обучается девочка. В настоящее время проводятся следственные действия и технические мероприятия, направленные на установление лица, совершившего данное преступление, в контакте с которым находится свыше 200 человек.

Как бороться с бесконтрольным использованием несовершеннолетними технических ресурсов?

По мнению следственного управления, необходим постоянный контроль со стороны родителей, усилия образовательных учреждений по обучению детей медиаграмотности.

Действующее российское законодательство определенным образом дисциплинирует СМИ, интернет-производителей. Общеобразовательные учреждения, общественные заведения снабжены системами контентной фильтрации.

Однако на сегодняшний день полным правовым пробелом является ответственность родителей или лиц, их заменяющих, по контролю над использованием несовершеннолетними Интернет-ресурсов, в том числе присутствием в социальных сетях, общением по системе «Skype», в которых обмен информацией происходит в режиме реального времени.

По нашему мнению, исходя из современных реалий, поскольку дети в большей степени используют «домашний» Интернет, в первую очередь родители обязаны прививать ребенку медиаграмотность, навыки взаимодействия в социальных сетях, осведомленность о проблемах виртуального общения, воспитывать в них понимание надлежащего онлайн-поведения и вырабатывать так называемый «информационный иммунитет» для способности противостоять внешним воздействиям.

К сожалению, констатируем, что сами родители нередко проявляют небрежное поведение. Не говоря об известных истинах, приведу один пример.

В июне 2013 года через социальную сеть в сети Интернет жительница Вязниковского района познакомилась с 30-летним мужчиной. Они вели недолгую переписку, а затем, после первой же встречи, договорились о совместной жизни. В доме стало проживать 12 человек, в том числе – 9 малолетних детей в возрасте от 13 лет до 1 года. Мужчина, который ранее находил близкие отношения только с женщинами значительно старше его (последняя дама – 60-летнего возраста), не удовлетворившись новым знакомством, «присмотрел» в новой семье для своих плотских утех 13-летнюю девочку, стал навязывать ей свои взгляды на половую свободу, и уже в сентябре склонил ребенка к сожительству. До конца октября 2013 года мужчина, используя моменты отсутствия в доме взрослых, систематически незаконно вступал с девочкой в половые отношения. Как объяснить поведение мамы? Привести в дом незнакомого мужчину «из Интернета», не зная о его наклонностях, психике, прошлом; уходить на работу, по магазинам, оставляя наедине с чужим человеком своих малолетних детей?..

Полагаем, что невыполнение родительских обязанностей в системе анализируемых правоотношений должно влечь ответственность родителей.

Следственное управление твердо убеждено, что при существующей системе профилактики правонарушений и преступлений с участием несовершеннолетних необходимо повышать роль и значение семьи в воспитании подрастающего поколения и родителей, в чьи обязанности входит главенствующая составляющая процесса формирования личности ребенка.

В связи с этим мы выступили инициаторами разработки изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», Семейный, Уголовный, Административный кодексы Российской Федерации и другие законодательные акты в части расширения и конкретизации обязанностей и ответственности родителей по воспитанию и образованию детей.

В целях повышения статуса института семьи и ответственности родителей за воспитание ребенка, Следственным управлением вы-

сказана инициатива создания в регионе центров семьи, устойчивой службы психологической помощи детям и родителям.

Немаловажным представляется укрепление и активизация общественного контроля в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, при осуществлении которого общественные объединения и иные некоммерческие организации, граждане вправе осуществлять мониторинг оборота информационной продукции и доступа детей к информации, в том числе посредством создания «горячих линий».

В ближайшее время в рамках взаимодействия с областной комиссией по делам несовершеннолетних и защите их прав начнется процесс формирования рекомендаций для родителей по использованию возможностей сети Интернет, исключающих доступ несовершеннолетних к ресурсам, способным нанести вред их психическому и нравственному развитию. А также о способах контроля над поведением несовершеннолетних, имеющих доступ к сети Интернет, созданию условий информационной безопасности детей. Созданный документ планируется к распространению во всех образовательных учреждениях области.

Я призываю всех, неравнодушных к анализируемой проблеме, принять участие в разработке документа, высказывая конструктивные предложения.

7 мая 2013 года Российская Федерация ратифицировала Конвенцию Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений, устанавливающую международные стандарты в данной сфере. При этом процесс расширения использования – как детьми, так и правонарушителями – информационных и коммуникационных технологий выделен в самостоятельную причину происходящего.

В качестве мер влияния и изменения ситуации предложено сотрудничество по принятию необходимых законодательных и иных мер, направленных на:

– повышение уровня информированности в области защиты и обеспечения прав детей от лиц, регулярно вступающих в контакт с детьми в сфере образования, здравоохранения, социальной защиты, правосудия и правоохранительной деятельности, а также в областях, связанных со спортом, культурой и досугом;

– на обеспечение включения в программы начального и среднего школьного образования информации для детей об опасностях, связанных с сексуальной эксплуатацией и сексуальным насилием, а также информации о способах защиты себя, адаптированной к их развивающимся способностям. Такая информация должна даваться в более широком контексте полового воспитания, и в ней особое внимание уделяется ситуациям повышенной опасности, в особенности связанным с использованием новых информационных и коммуникационных технологий; и другие меры. Крайне полезные обязательства, к которым необходимо относиться неформально.

Аспектов темы информационной безопасности детей – множество. К примеру, продажа и бесплатное распространение через торговую сеть и Интернет книжной продукции, пропагандирующей прямо или косвенно гомосексуализм, педофилию. Такая «литература» формирует у детей отношение к этим отклонениям как к норме. Но сегодня открыто противником ситуации выступает, пожалуй, только Уполномоченный по правам ребенка во Владимирской области.

Конечно, следует констатировать позитивные перемены, происходящие в молодежной среде. Внимание несовершеннолетних стали привлекать анти-кафе – заведения для занятий по интересам для людей без вредных привычек. Активизировался спрос на занятия спортом и т. д.

Наша задача – отвлекать детей от зомбированного пользования техническими ресурсами. Пора возвращать прежние ориентиры и воспитывать в детях дух созидания, патриотизма, жизнелюбия.

Следственное управление открыто для диалога, и готово принять конструктивные предложения по улучшению качества жизни детей региона, для их реализации через коллегиальные органы, членом которых является наше ведомство.

В. Е. Пономарев,
г. Москва

Формирование безопасной интернет-среды. Опыт Лиги безопасного интернета

Коллеги!

Лига безопасного интернета была создана 3 года назад. Членами Лиги стали ведущие операторы связи и участники интернет-индустрии. Все это время мы следовали своей главной цели: искоренение опасного контента путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей.

Исходя из этой задачи определились основные направления нашей деятельности:

- борьба с опасным контентом
- поддержка позитивного контента
- международная деятельность
- повышение активности общества

К сожалению, вопрос борьбы с противоправным контентом своей актуальности не теряет несмотря на то, что работа по очищению Рунета ведется и приносит результаты. Примечательно, что формируется именно система самоорганизации, которая включает взаимодействие и интернет-компаний, и государственных органов (Роскомнадзор, Роспотребнадзор, ФСКН, другие правоохранительные органы) и рядовых пользователей.

Приведу несколько цифр.

Так, по данным международной ассоциации горячих линий INHOPE в феврале 2011 года доля Российской Федерации как хостера детской порнографии составляла 29%, и Россия делила это печальное первенство с США и Таиландом. Однако за 2 года этот показатель снизился до 13%, и теперь Россия занимает в этом списке третье место. Наибольшее число ресурсов с детской порнографией сейчас зарегистрировано в Нидерландах и США.

В 2013 г. Управлением «К» МВД РФ в России было заведено 1506 уголовных дел по ст. 242 (1) УК РФ «Распространение детской

порнографии», в 953 делах использованы материалы, собранные с участием кибердружинников Лиги.

В 2013 Экспертным центром Лиги проведено 313 исследований материалов с порнографическими изображениями несовершеннолетних, на основании которых Роскомнадзором вынесено 1456 решений о включении сайтов в Единый реестр запрещенных сайтов.

Одновременно растет ответственность владельцев сайтов за размещаемый контент. Так, в 2013 году по обращениям аналитиков горячих линий Лиги безопасного интернета противоправный контент был удален в добровольном порядке:

- детская порнография – с 14 754 серверов,
- реклама наркотиков – с 359 серверов,
- призывы к суициду – со 105 серверов.

С теми, кто по разным причинам не удалял противоправный контент добровольно, работа продолжается. Мы передаем информацию на горячую линию Роскомнадзора и в правоохранительные органы.

Таким образом, стратегия разработки удобных и понятных пользователю инструментов создания безопасной интернет-среды подтвердила свою правильность. Доступ ко всем инструментам организован через кнопки, размещенные на сайте Лиги.

Деятельность Лиги нашла поддержку в регионах России. В настоящее время заключены соглашения о сотрудничестве с Костромской, Ульяновской, Омской, Томской областями, Пермским краем.

Сегодня Лига предлагает не только кнопку «Сообщить об опасном контенте», но и другие инструменты. К ним относятся:

- средства контентной фильтрации
- материалы для повышения грамотности в сфере безопасного использования интернета.

Остановимся на этих инструментах подробнее.

Средства контентной фильтрации.

Для удобства я буду называть его «Веб-фильтр». Контентный фильтр Лиги выполняет задачу анализа контента «на лету», в момент открытия страницы пользователем. Если фильтр обнаруживает на странице противоправный контент, пользователь видит страницу блокировки.

Анализ страниц именно «на лету» позволяет избежать ситуаций, в которых злоумышленник может внедрить на страницу нежелатель-

ный контент, и это останется незамеченным администрацией сайта. Наш веб-фильтр не пропустит такой контент незамеченным, ведь проверка осуществляется непосредственно перед показом страницы в браузере конечного пользователя.

Главной особенностью фильтра является то, что он работает на любых сайтах, в т. ч. в социальных сетях.

Сегодня мы предлагаем три варианта решений для разных условий:

• Решение для оператора связи.

• Решение для образовательных учреждений с единой точкой подключения.

• Решение для пользователей и отдельных компьютеров.

Предлагаемые решения прошли пилотное тестирование и успешно применяются на практике.

В Костромской области оператор КГТС предлагает своим пользователям «родительский контроль» на основе решения для операторов связи. Сегодня несколько тысяч семей используют «родительский контроль» на постоянной основе. Есть факты отказа от этой услуги, но их сравнительно немного – большинство людей работают в безопасной интернет-среде.

В Омской области реализована схема, в которой все учебные заведения выходят в интернет через единый электронный центр, который и решает задачу фильтрации всего контента, который передается в школы и ВУЗы. Сегодня 788 школ и образовательных учреждений Омской области используют безопасную интернет-среду, которая обеспечивается программно-аппаратным комплексом Лиги.

«Веб-фильтр» – сервис, доступный любому пользователю. Достаточно зарегистрироваться на сайте Лиги на странице сервиса и настроить компьютер для использования «Веб-фильтра». В настоящее время более 1000 семей из разных регионов России постоянно используют сервис «Веб-фильтр» на домашних компьютерах.

Система фильтрации постоянно совершенствуется. Сейчас наши специалисты внимательно изучают критерии определения опасной для детей информации, которая недавно была разработана по заданию Роскомнадзора специалистами МГУ.

Важным направлением сегодня становится работа по повышению уровня грамотности, в первую очередь – в области безопасности

в интернете. Сегодня многие компании и общественные объединения проводят уроки безопасного интернета для детей.

Мы предлагаем нашу версию таких уроков. Нам удалось найти заинтересованных преподавателей и – самое главное – детей, с которыми мы обсуждали не только вопросы непосредственной безопасности, но как лучше эту информацию представить. Сами школьники дали много подсказок, как сделать урок интересным, как расставить акценты и какими примерами сопровождать материалы.

Сегодняшняя концепция образования предлагает учителю максимум свободы в выборе тематики и методов проведения урока. Мы предлагаем материалы, которые могут быть использованы как в готовой форме, так и в качестве основы для подготовки авторских уроков и методик.

Материалы к урокам безопасного интернета представлены в трех вариантах: для начальной, средней школы и старшеклассников. Дополнительно для удобства преподавателей мы предлагаем примерные планы уроков.

Дополнительные материалы по безопасности в интернете мы представляем на сайте Лиги в разделе «Энциклопедия безопасности». Здесь можно найти обзоры, рекомендации, интересные статьи и инфографику из разных источников.

В целом можно констатировать, что обучению детей методам безопасного использования интернета в обществе уделяется достаточное внимание. При этом много говорится, что современные дети уже становятся «цифровым поколением», они растут в окружении современной компьютерной техники и достаточно легко осваивают новые технологии. На этом фоне возник феномен так называемого «цифрового разрыва» между родителями и детьми.

Мы используем слово «родители», т.к., во-первых, большинство взрослых являются родителями и, во-вторых, задачи, которые решают родители, практически совпадают с решениями, которые находят школьные учителя и другие специалисты, работающие с детьми.

Любопытные факты были получены в результате исследования «Юный интернет-пользователь в 2013 году». Исследование было проведено по заказу ОАО «Мобильные ТелеСистемы», компании «Лаборатория Касперского» и НП «Лига безопасного интернета» с целью

выработки рекомендаций по развитию подходов в области просвещения и защиты несовершеннолетних пользователей интернета и мобильной связи. В исследовании приняли участие 8 888 детей из всех ФО РФ. Средний возраст – 13, 8 лет.

Выяснилось, что абсолютное большинство детей (8 из 10) (82,5%) выходят в интернет из дома. При этом больше половины детей (58,3%) свободно посещают любые сайты. Только 2 из 10 родителей (21,5%) объяснили детям, на какие сайты ходить можно, 9% детей пользуются интернетом в присутствии родителей и только каждому 30-му ребенку родители вообще запрещают интернет.

При этом абсолютное большинство детей встречались с противоправным контентом или попадали в неприятную ситуацию в интернете. Около четверти опрошенных (28,3%) предпочитают найти выход из такой ситуации самостоятельно, каждый десятый (11,2%) посоветуется с друзьями, а 15% (15, 4%) просто отключат компьютер.

Мы оцениваем положительно тот факт, что 4 из 10 детей (39,1%) при возникновении неприятной ситуации в интернете обратятся за советом и помощью к родителям.

Таким образом, можно констатировать, что влияние родителей на использование детьми интернета является значительным.

Последние исследования, например, факультета психологии МГУ, показывают, что величина «цифрового разрыва» между юными интернет– пользователями и старшим поколением сильно преувеличена, в обществе есть потребность в обучении безопасному использованию интернета и родителей. Во многом это объясняется повышенной ответственностью родителей. Им приходится находить решения и для себя, и для детей, часто – для детей разного возраста.

В ответ на эту потребность Лига безопасного интернета запустила проект «Интернет-канал для родителей». Интернет-канал «Лига-ТВ» – информационный интернет-ресурс, направленный на информирование взрослой аудитории, прежде всего родителей, об особенностях использования интернета, в первую очередь, детьми.

Цель канала: создать единую интернет-площадку, где заинтересованные родители могут найти наиболее точную информацию по обеспечению безопасности детей в сети интернет.

На портале размещаются краткие тематические видеоролики и другие материалы, описывающие основные угрозы, с которыми можно столкнуться в сети и рекомендации, как этим угрозам противостоять.

Канал публикует как собственные материалы редакции, так и лучшие материалы из сети интернет, что позволяет сформировать единую картину сложившейся ситуации. В перспективе большая часть материалов будет готовиться «по заявкам зрителей», отвечая наиболее актуальным запросам аудитории.

Девиз канала «Для родителей, которым не все равно» определяет состав авторов: к участию в работе канала приглашаются эксперты и все заинтересованные лица и организации, а также интернет-ресурсы.

Завершая выступление, хочу отметить, что в соответствии в основной своей целью – «самоорганизация интернет-сообщества» Лига безопасного интернета предлагает комплекс инструментов, использование которых позволяет осознанно создать безопасную интернет-среду, в первую очередь, для детей и семьи. Ко всем инструментам обеспечен удобный доступ с сайта Лиги. Мы приглашаем всех внести свой собственный вклад в формирование такой безопасной интернет-среды.

Опыт трех лет подтвердил правильность выбранной стратегии, и мы будем двигаться в этом направлении, ибо «дорогу осилит идущий».

Р. В. Евстифеев,
г. Владимир

Социальные сети и молодежь: интересно, полезно, опасно?

Явление, называемое социальными сетями, или социальными медиа (Social Media), в совокупности с новыми информационными технологиями – сетью Интернет и возможностями коммуникации – серьезно изменили и продолжают изменять жизнь современного человека.

Одним из таких изменений стало неимоверно расширившееся коммуникационное пространство человека, позволяющее ему общаться, обмениваться эмоциями и информацией с другими людьми, с которыми (по разным причинам) непосредственный контакт невозможен или затруднен. И если до информационной эпохи круг общения человека ограничивался его родственниками, друзьями, соседями, находящимися в непосредственной пространственной близости, то с развитием средств коммуникации, таких как: почтовая связь, телефония, а теперь и Интернет – этот круг стал практически безграничным.

Такая ситуация создает как позитивные, так и негативные последствия. Дело в том, что любому человеку свойственно стремиться к общению с себе подобными. Именно в процессе общения мы становимся самими собой. Обмениваясь эмоциями и знаниями друг с другом, мы становимся людьми: развиваемся, социализируемся, проверяем себя, пробуем социальную реальность, исследуем ее. Доступный, интуитивно понятный интерфейс социальных медиа, простота пользования, получения и отправления собственной информации не предъявляют серьезных требований к пользователю и делают этот вид коммуникаций особенно популярным среди молодежи.

Однако здесь таятся и проблемы. Встреча с другими людьми, столкновение с их интересами, желаниями и волей не всегда носит характер добровольного равноправного обмена, а, чаще всего, происходит в виде весьма жесткой конкуренции, создающей ситуацию навязывания и властного подчинения.

Современные социальные медиа являются крайне притягательным пространством для организации общения человека. Такие популярные социальные сети, как: Facebook (более миллиарда пользователей по всему миру), ВКонтакте (более 200 миллионов пользователей, в основном – в России), Twitter (более 200 миллионов пользователей в мире) и другие – не только привлекают молодежь, жаждущую общения, но и становятся серьезными средствами коммуникации для бизнеса, науки, систем управления. Социальные медиа все больше и больше конкурируют с традиционными средствами массовой информации и даже заменяют их.

Одно из самых интересных и влиятельных исследований о современных информационных сетях – книга Мануэля Кастельса «Власть как коммуникация». В этой книге обращается внимание на то, что тот, кто управляет коммуникацией, тот обладает властью над нами. В процессе общения происходят изменения в нашем разуме. Появляются новые мысли, рождаются новые эмоции. Все это определяет наши действия, влияет на них, видоизменяет их. Получается, что тот, кто способен управлять коммуникацией в нужном для себя направлении, будет способен влиять и на наше поведение и тоже в нужном для себя направлении.

Сетевое общество, сложившееся – в целом – к началу двадцать первого столетия, построено вокруг цифровых сетей коммуникации (хотя полностью и не определяемое ими). В настоящее время, по мнению Кастельса, процесс осуществления властных отношений окончательно преобразовался в новый организационный и технологический порядок, вырастающий из быстрого развития глобальных цифровых сетей коммуникации как фундаментальной системы обработки символов в настоящее время. Кастельс пишет о «фундаментальной битве по поводу определения общественных норм и применения этих норм в повседневной жизни», именно эта битва формирует человеческий разум, а коммуникация находится в центре этого сражения.

Это – нелегкое сражение хотя бы потому, что оно проходит почти незаметно для нас, и мы очень поздно можем обнаружить, что мы уже побеждены. Этому способствует ряд характеристик социальных медиа, таких как: интерактивность, взаимодействие, виртуальность, анонимность и ряд других. При этом в медиасферу активно и созна-

тельно вторгаются различные социальные, экономические и политические силы, продвигая свои интересы через такие механизмы, как: формирование повестки дня, фрейминг (англ.– «framing», «установление рамок»), продвижение новостей и т. д.

Шансов остаться самим собой у человека, вступившего в это сражение, совсем немного. Однако, они есть. Один из таких шансов – понимание того, что происходит при коммуникации в социальных сетях, овладение современными методиками критической оценки информации и критическим мышлением в целом. Это, конечно, требует специальных занятий, времени и усилий, то есть вырабатывания особой привычки мыслить критически. Однако только так можно получить максимум пользы от такого сложного и многомерного явления, каким являются сегодня социальные медиа.

Таким образом, критическое мышление, навыки поиска информации, ее распознавания и понимания, овладение способами защиты от ненужной и даже вредной информации – вот примерный арсенал средств, необходимых для современного молодого человека, выходящего в конкурентную и жесткую среду сетевой коммуникации и желающего не только оставаться самим собой, но и быть успешным.

Помочь молодому человеку стать обладателем такого арсенала – одна из важнейших задач современного образования и общества в целом.

Т. В. Пантюхова,
г. Нижний Новгород

Взрослые и дети гуляют в Интернете: опыт работы Нижегородской государственной областной детской библиотеки

Сегодня уже очевидно, что Интернет стал частью нашей реальной жизни. Наши дети родились и живут в цифровой среде и покоряют виртуальное пространство.

Взрослые (библиотекари, педагоги, родители) тоже стараются приспособиться к нетрадиционной (для себя) среде: освоить, понять, принять ее и создать модели общения, коммуникаций. Также определить эффективные пути сотрудничества поколений: младшего и старшего.

Взрослые и дети одновременно получают практики виртуального общения. Но реагирование на ситуацию и достойный выход из нее у взрослых и детей происходит по-разному. И определяется это жизненным опытом, скоростью реакции, здравым смыслом.

Большая часть виртуальных прогулок происходит за пределами детской библиотеки. Но, тем не менее, в детской библиотеке происходит встреча сообществ: взрослого, ребенка и «интернет-жителей». Встречи предусматривают открытость, осторожность и ответственность. Библиотекарь становится модератором, управленцем, менеджером, навигатором встреч. Несомненно, чтобы успешно управлять, библиотекарям необходимо владеть базовыми компетенциями, в их числе – информационно-коммуникационная. Отработка и приобретение компетенций происходит во время повышения квалификации. Например:

– создание и проведение курса «Использование информационно-коммуникационных технологий и социальных серверов» в рамках повышения квалификации сотрудников библиотек;

– обсуждение на площадке блога библиотеки темы: «Плюсы и минусы социальных серверов и электронных»;

– организация и участие во всероссийских и дистанционных семинарах «По-новому думать и творить»;

– изучение и обсуждение федеральных законов, направленных на информационную безопасность детей.

Надо отметить, что детская библиотека по умолчанию – территория безопасности. Это значит:

1. Виртуальное путешествие юных читателей проходит в сопровождении библиотекаря. Прежде всего, это выражается в контроле за посещением сайтов и онлайн – и офлайн играми. Безопасное путешествие по Интернет-ресурсам обеспечивают традиционные и электронные выставки, стенды с информацией, издательская продукция, посвященная правилам посещения и безопасного поведения в Интернете.

2. Рекомендуемые сайты, полезные ссылки (в печатных и электронных изданиях, сайте, блоге библиотеки) прошли отбор и цензуру.

3. Использование дидактики в индивидуальном, групповом, массовом общении с пользователями. Библиотекарь готов научить, предостеречь, помочь.

Последний пункт рассмотрим более подробно. В индивидуальном общении с пользователями библиотекарь руководствуется правилом: «не запрещай, а объясняй».

При проведении массовых занятий преобладают диалоговые формы. Так на встречах «Интернет: мир без границ?», «Интернет – возможно все?» в ходе обсуждения и обмена мнениями выявляется отношение подростков к Интернету, качеству и достоверности информации, способах ее получения.

Все активности библиотекарей можно свести к одной цели – формирование информационной культуры у читателей в содружестве с библиотекарями, педагогами и родителями. На достижение данной цели, объединение поколений, совмещение формального и неформального общения, сопровождение программ нового образовательного стандарта и внедрение инноваций в библиотеке направлена проектная деятельность. Акцент необходимо сделать на следующие виды проектов: культурно-образовательные, социальные, исследовательские.

Создание и реализация проектов способствуют не только формированию информационной культуры, но и развитию личности участников проекта, а также приобретение навыков и приемов работы в команде, использованию информационно-коммуникационных

технологий. Примеры проектов: «Лети с приветом, вернись с ответом», «Что читать сегодня детям», «Вдохновись Геометрией», «Мы – многоугольники». Вы спросите, как эти проекты связаны с Интернет безопасностью? В эти проекты включены задания по поиску и оцениванию информации, представленной на сайтах. Например, введите в любую поисковую систему слово «многоугольники». Проанализируйте первую десятку сайтов (индикаторы для анализа представлены в таблице, которая выдается ребятам).

В 2013 году создана программа по формированию информационной культуры «Взрослые и дети гуляют в интернете». Программа предусматривает систематическое проведение интерактивных занятий для разных возрастов. Так, дошкольники знакомятся с темой «Что такое интернет», ребята младшего школьного возраста на занятии «Тук, тук – стучится в дверь друг или враг?» учатся правильно вести себя при регистрации на социальных серверах и выборе виртуальных друзей. Подростки обсуждают взаимоотношения со сверстниками на встрече «Против кого дружить будем?», старшие подростки в командах создают правила безопасной интернет-жизни.

В заключение хочется поделиться проблемами, наблюдениями, выводами.

1. Цифровое поколение вступает в период активной профессиональной и родительской деятельности. Цифровые дети воспитывают цифровых детей. Цифровые дети занимают рабочие места. Для библиотекарей – это вызов, который заключается в смене картины мира, мышления и сознания.

2. Говорить с детьми о безопасности в Интернете должен не только подготовленный специалист, а и продвинутый пользователь Сети. Готовы ли реальные библиотекари к такому общению?

3. Эффективность усвоения правил безопасного поведения в Сети возможна только в объединении усилий, условий и возможностей библиотеки, школы, семьи.

4. Программная и системная работа с темой, а не активизация во время Недели, месячника, конкурса.

5. Библиотеки готовы стать культурно-образовательными площадками по формированию информационной культуры, организационно-методическими и консалтинговыми центрами по проблеме.

В библиотеках наработан опыт, апробированы программы и проекты по проблеме. Библиотека умеет создавать и хранить цифровые коллекции, интегрировать деятельность с социокультурными учреждениями и продвигать интеллектуальные и информационные ресурсы, то есть библиотека умеет быть полезной, и на сегодняшней день знает, как стать полезной.

6. Грантовые проекты по формированию безопасного поведения в сети имеет смысл реализовывать на базе детских библиотек.

7. Информационная безопасность, прежде всего, уровень информационной культуры пользователя, а вернее каждого человека, не только пользователя разнообразных гаджетов. Основной вклад детской библиотеки, ее сотрудников – это формирование у юных читателей и у их близкого взрослого окружения информационной культуры, а также развитие личности в условиях информационного общества. Личности, которая проживает в мире выбора, рисков, разнообразия и несет ответственность за свои поступки, активности, инициативы.

О. Н. Лебедева,
г. Рязань

Дети. Интернет. Библиотека: взгляд из Рязанской областной детской библиотеки

Современные дети много общаются с телевидением, видео и компьютером. Если предыдущее поколение было поколением книг, то современное получает массу информации из других источников, основным из которых, конечно же, является Интернет. Изначально Интернет развивался вне какого-либо контроля, и сейчас он представляет собой огромное количество информации, причем далеко не всегда безопасной. С каждым годом поколение, активно пользующееся Сетью, становится все моложе, поэтому проблема обеспечения безопасности детей в Интернете особенно актуальна.

А кто им может в этом помочь, если не их родители и взрослые?

По инициативе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в декабре 2013 г. была подготовлена «Концепция информационной безопасности детей». На сайте Роскомнадзора представлена новая версия концепции с обновленными файлами, документ призван «сформулировать законодательные предложения в сфере защиты детей от вредоносной информации и конкретизировать сложные правовые понятия». Все заинтересованные лица могут принять участие в обсуждении концепции.

Раздел 20, подпункт 20.5 включает в себя часть: «Вклад библиотек в развитие информационного и медиаобразования», где написано «…Наиболее подготовленными к продвижению идей медиа – и информационной грамотности в России являются две профессиональные группы: учителя и библиотекари».

Наша библиотека на протяжении многих лет взволнована проблемой безопасности детей в Интернете и для ее решения использует разнообразные интересные формы работы, доказывая, что библиотекари – проводники в мире информации. За активную работу в проекте «Безопасный Интернет» Российская государственная детская библиотека наградила нас Почетной грамотой.

В отделе автоматизации происходит обучение и приобщение детей к безопасному, грамотному использованию компьютера и сети Интернет. Для этого мы проводим индивидуальные и групповые обучающие занятия, для которых разрабатываются специальные образовательные программы.

С целью повышения информированности и грамотности детей и взрослых выпускается полиграфическая продукция, в которой доступным языком излагается важная информация о правилах безопасного пользования Сетью.

Библиотека широко использует Интернет как инструмент социальной активности, установление партнерских связей с библиотеками России и мира.

Это – мероприятия краеведческого характера. Большой популярностью, к примеру, пользуются скайп-игры «Мы знаем ваш город!», в которых принимают участие читатели нашей библиотеки и дети из других городов. В процессе игры демонстрируются возможности и польза новых технологий.

Правила игры просты, а эффективность этих мероприятий очень велика. После приветствия команд, участники задают друг другу по 10 вопросов о своем городе. Если во время игры при ответе на вопрос возникают затруднения с ответом, каждая команда может воспользоваться тремя подсказками: книгой, Интернетом, помощью старшего товарища. После завершения игры команды награждаются призами и дипломами библиотек-участниц.

Как вы понимаете, подготовка к игре сопряжена с интересным и увлекательным процессом поиска и получения различной информации о том городе, с которым предстоит очередная скайп-игра, а также отбором информации для составления вопросов о собственном городе.

География скайп-игры расширяется. Рязань встречалась по разные стороны экрана с Нижним Новгородом, Орлом, Тольятти, Ярославлем, Белгородом, Липецком, Пензой и г. Уральск (Казахстан), что дает нам основания считать, что такие мероприятия нужны и интересны современным школьникам.

Библиотека активно поддержала инициативу РГДБ по созданию каталога лучших веб-ресурсов для детей, который называется «Вебландия». Специалисты нашей библиотеки отбирают и оценивают

для каталога те сайты, на которых юные пользователи найдут только познавательную, развивающую и обучающую информацию. Мы знакомим наших читателей с этим ресурсом, советуем обращаться к нему при самостоятельной работе.

Но Интернет может быть не только другом и помощником. Его часто используют не только в благих целях… Неприятности, приходящие из компьютера, примерно те же, что и в обычной жизни: вирусы, кражи и грабежи, оскорбительные выражения и преследование, вымогательства и угрозы, неэтичная и навязчивая реклама, терроризм и экстремизм. Поэтому необходимо научить школьников защищаться от всего вредного в Сети, привлечь внимание юных пользователей к осмысленному освоению Интернет-пространства.

Мы проводим информационные часы, посвященные актуальной теме: «Пароль – иллюзия или защита», где дети узнают, какие опасности могут подстерегать их на безграничных просторах Интернета; в чем может быть угроза при размещении личных данных на страницах социальных сетей; какие правила должны соблюдаться при выборе пароля.

Очень популярна компьютерная викторина «С библиотекой на орбите Интернета», где в знаниях и умениях пользоваться глобальной сетью соревнуются не только дети, но и отдельным блоком проводится акция «Дети против родителей».

В компьютерном секторе библиотеки проводятся информационные лектории, на которых активно используется проект «Разбираем Интернет» http://www.razbiraeminternet.ru/. Это совместный продукт Google, Фонда Развития Интернет, факультета психологии МГУ им. М. В. Ломоносова и Федерального Института Развития Образования. В проекте «Разбираем Интернет» дети узнают об устройстве «электронного мозга» сетевого пространства; о том, как получить доступ к полезной информации и знаниям в Интернете; как быстро находить ответы на самые необычные вопросы; как критически оценивать онлайн-контент, т. е., – как общаться, соблюдая простые правила безопасности.

С целью привлечения внимания к проблемам безопасного использования сети Интернет библиотекой проводятся конкурсы:

• компьютерного рисунка «Киндернетик» (2010 г.),

• «М☺я сеть» (2012 г.) На этот конкурс принимались рисунки (возможно, с использованием компьютерных технологий), презентации, видеофильмы, стихи, рассказы…

• «И опасный, и полезный – Интернет нам всем известный» (2014 г.) – областной конкурс творческих работ /комиксов/, к участию в нем принимались рисованные истории, иллюстрирующие положительные и отрицательные стороны использования Интернет, а также важность навыков безопасной работы в Сети.

Конкурсы популярны не только среди учащихся школ г. Рязани, но и широко известны в области.

В 2004 году решением Еврокомиссии принят особый день для глобального веб-пространства, названый «Днем безопасного Интернета». Он ежегодно отмечается в первый вторник февраля как символ общественного порицания опасного и «грязного» контента на веб-страницах.

Ежегодно в этот день (начиная с 2010 года) Рязанская областная детская библиотека проводит круглые столы «Безопасный Интернет для всех». В их работе ежегодно принимают участие: представители министерства культуры и туризма Рязанской области, министерства образования Рязанской области, Уполномоченного по правам ребёнка в Рязанской области, отдела «К» по борьбе с компьютерными преступлениями в сети Интернет УМВД России по Рязанской области, Рязанского государственного университета, заведующая детским психиатрическим отделением Рязанской областной клинической психиатрической больницы, провайдеры, учителя, библиотекари, родители.

Целью этих мероприятий являются:

– популяризация культуры безопасного использования Интернета,

– повышение технической грамотности педагогов, библиотекарей и родителей,

– привлечение внимания к проблеме безопасности детей в сети Интернет.

Выступления участников на них посвящены актуальным проблемам обеспечения безопасности детей в сети, культуре поведения и нравственности в виртуальном пространстве, компьютерной зависимости и методам ее профилактики. Специалистами разных областей даются советы о том, как помочь в обеспечении безопасности детей в Сети.

На круглых столах «Безопасный Интернет для всех» у нас есть опыт использования скайп-включения других регионов с целью обмена опытом в этом направлении.

Совместно с заведующей детским психиатрическим отделением Рязанской областной клинической психиатрической больницы, которая является постоянным участником работы круглого стола, сотрудниками отдела автоматизации разрабатывается анкета с целью выявления интернет-зависимости детей и информировании об этом родителей.

Проблемы безопасности в Сети волнуют не только взрослую аудиторию: дети так же активно делятся своими мыслями друг с другом. На недавней online-дискуссии ученики старших классов Рязанского и Липецкого регионов обсудили следующие проблемы:

• Нежелательное содержание веб-сайтов – как избежать?

• Мошенники, хакеры – как не стать их жертвой?

• Некорректное общение (грубость, хамство, киберунижения) – где найти защиту?

• Интернет-зависимость – как справиться с ней?

Обе стороны узнали много нового и полезного в этом направлении.

По итогам одного из круглых столов «Безопасный Интернет для всех» библиотекой была достигнута договоренность с ОАО «Мобильные ТелеСистемы» об организации в стенах библиотеки образовательно-выставочного проекта «Дети в Интернете». Проект представляет собой комплекс образовательных мероприятий, объединяет проведение интерактивной выставки и серии обучающих занятий, рассказывающих о потенциальных рисках при использовании Интернета.

В октябре 2012 года Рязанская областная детская библиотека организовала межрегиональную конференцию «Безопасность детей – забота общая». В конференции приняли участие библиотекари, преподаватели, социальные работники, представители общественных организаций, работающих с детьми, представители правоохранительных органов, родители. Особое внимание на ней было уделено осмыслению интернет-угроз для детей и подростков.

Мы не будем останавливаться на достигнутом, продолжим активно заниматься проблемой безопасности детей в Интернете, привлекать общественное внимание к этой проблеме. Нужно помнить, что безопасность наших детей в Интернете во многом зависит от нас!

А. С. Симкин,
г. Владимир

Онлайн-безопасность детей: помощь технологиями и экспертизой

Интернет – это интересный и яркий мир.

В сети можно:

• общаться (посредством электронной почты, социальных сетей, чатов, форумов, блогов (наибольшую популярность в России получили такие сервисы, как: вКонтакте, Одноклассники, Livejournal, Facebook, Twitter и др.), месседж-клиентов (ICQ, QIP, Mirnada, Skype, Trillian) и т.д.;

• искать любую информацию и обмениваться ей;

• работать;

• развлекаться;

• совершать покупки и многое другое…

Но, как и в реальности, в интернете часто встречаются опасности. Как правило, они хорошо замаскированы.

Общероссийское исследование «Билайн» показывает:

– 83% респондентов сталкивались в Интернете с нежелательной информацией и с заражением компьютеров вирусами;

– 55% опрошенных считают, что обеспечивать безопасность в Интернете самостоятельно – сложно;

– 88% понимают под «Безопасным Интернетом» защиту от вирусов и вредоносных программ;

– 45% понимают «Безопасный Интернет» как защиту детей от нежелательной информации.

К 2016 г. пользователей мобильного Интернета ожидается уже 120 млн. человек. 93% детей в возрасте от 12 до 17 лет являются активными пользователями Интернета. Причем 81% детей используют Интернет без присмотра взрослых.

46% школьников посещали сайты, содержащие неправомерный и опасный контент.

74% пользователей Интернета хотели бы, чтобы вопрос защиты безопасности детей в Интернете взял на себя оператор.

В настоящее время очень важно не столько ограждать детей, сколько предоставлять им позитивную инициативу, фокусировать их внимание на образовательной сути Интернета.

Эффективная защита детей от негативного контента в Сети должна не просто ограничивать доступ к определенным сайтам и порталам. Нужно предложить взамен позитивную альтернативу: увлекательные, интересные и безопасные ресурсы для развития, общения и обучения.

В настоящее время создается большое количество новых ресурсов для детей, но часто они либо исчезают, либо «портятся». Помимо этого, многие сайты не соответствуют возрастным категориям детей, а мнение детской аудитории относительно контента не учитывается. Также встает вопрос о том, кто выступает экспертом с точки зрения отбора и наполнения ресурса познавательной и интересной информацией. Экспертов по детскому контенту крайне мало, а качество экспертизы основано на размытых критериях.

Учитывая сложившуюся ситуацию, Российская государственная детская библиотека и компания «Вымпелком» (бренд «Билайн») запустили в прошлом году рекомендательный портал детских интернет-сайтов «Вебландия» (находится по адресу www.web-landia.ru). Портал «Вебландия» позволит родителям и детям избегать негативного контента, находя познавательную и позитивную информацию в Сети.

Основные цели проекта:

1. Создание и постоянное поддержание списка безопасных и полезных ресурсов для детей в сети Интернет;

2. Рекомендательная сеть формата «дети – детям»;

3. Создание коммуникационной среды для безопасного и плодотворного общения детей между собой, а также детей и экспертов (библиотекарей и педагогов);

4. Позитивная альтернатива запретительным мерам, принимаемым по защите детей от информации, причиняющей вред их здоровью и развитию.

Список проверенных и полезных сайтов для детей «Вебландии» постоянно пополняется и контролируется экспертным советом, в который входят педагоги, детские библиотекари, психологи, а также члены Центра интернета и его региональных представительств.

В настоящее время уже отобрано свыше 1700 проверенных ресурсов, которые разбиты на 14 тематических разделов (игры, подготовка к школе, развитие и т. д.). Имея понятный и простой интерфейс, «Вебландия» предоставляет подросткам и детям возможность вместе обсуждать понравившийся ресурс, узнавать мнение экспертов и рекомендовать его своим друзьям.

СЕКЦИЯ ДЛЯ СПЕЦИАЛИСТОВ «ИНТЕРНЕТ-КОНТРОЛЬ»

Т. А. Мачинскене,
г. Владимир

Формирование навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде

Научить, нельзя запретить

Современные дети начинают пользоваться компьютером и интернетом буквально с пеленок, поэтому приучать их к безопасному пользованию сетью надо очень рано. Вот только как это сделать так, чтобы Интернет стал для ребенка океаном возможностей, а не рисков? Безусловно, проблему детской безопасности в Интернете невозможно решить исключительно при помощи государственного регулирования. Но ответственность за легитимное Интернет-пространство нельзя и перекладывать только на государственные органы. Безопасный интернет должны формировать участие государства, саморегулирование среды с точки зрения правил и норм поведения непосредственно участников рынка и обучение населения цифровой грамотности.

Законодательно контролировать недобросовестных участников Интернет-индустрии начали в ноябре 2012 года. Роскомнадзор (на него была возложена роль технического исполнителя в этом процессе) начал вести реестр вредных для детей адресов в Интернете.

Первыми итогами работы программы, ограничивающей доступ к сайтам в сети, информация на которых запрещена в нашей стране, стали 4173 обращения только в первый день открытия так называемого «черного списка».

Но эти показатели вам покажутся незначительными на фоне цифр, представленных представителями Google: каждый месяц пользователи по всему миру задают Google более 100 млрд. поисковых запросов. На крупнейший видеохостинг YouTube ежеминутно загружается 72 часа уникального видео, что в разы превышает объем киноконтента, показываемого крупнейшими голливудскими киностудиями в год.

С помощью панорамных снимков на картах Google (Street View) можно совершить путешествие по 200 городам России и другим странам, а благодаря виртуальным коллекциям Арт-проекта – пройтись по 180 музеям по всему миру.

Сегодня Интернет открывает уникальные возможности для образования и доступа к знаниям, которые еще недавно было трудно себе представить.

Мы понимаем, что в Сети можно не только найти полезный контент, но и столкнуться с определенными рисками. В первую очередь, это опасность для самых юных пользователей Интернета – детей и подростков, которые не хуже взрослых умеют пользоваться новыми технологиями, но не всегда понимают, как защититься от интернет-угроз.

В марте 2013 года я принимала участие в Международной конференции «Детская безопасность и цифровая грамотность в Интернете» в г. Москва.

Мероприятие было организовано Министерством связи и массовых коммуникаций Российской Федерации совместно с Российской ассоциацией электронных коммуникаций (РАЭК) при поддержке Google Россия. В конференции приняли участие педагоги, представители российских и международных ассоциаций и организаций, представляющих интересы Интернет-отрасли.

Я бы хотела кратко обрисовать решения проблемы, которые были предложены на конференции. Но прежде чем приступить к основной части своего выступления, я более подробно остановлюсь на двух терминах, которые очень активно использовались всеми участниками конференции.

«Цифровое поколение», «поколение Y» – поколение подростков (до 2000 г.р.), растущее в новой социальной ситуации развития. Дети информационной социализации. Интернет как глобальная реальность (особенность Интернета – генеративность, создание новой реальности), в которой в той или иной степени находятся все пользователи Сети, выступает для этого поколения Y макрофактором социализации.

Более того, мыслительные процессы детей поколения Y отличны от мышления их предшественников, представителей поколения X, к которому относятся практически все сидящие в этом зале. Главное отличие – в способе обработки информации, способности справиться

с огромными пластами информации, обработать ее, вычленить необходимую и абстрагироваться от лишнего, «спама».

То есть, для этих детей, проводящих достаточно много времени за компьютером (а по результатам исследований, на которых я остановлюсь позже, около 4 часов в день в среднем подростки проводят в Интернете, в том числе в социальных сетях), реальность становится похожа на компьютерную программу, когда можно – совершив ошибку – нажать кнопку отмены Ввода, и все проблемы будут решены.

И второй термин – «цифровая компетентность». Это – способность использовать информационные и коммуникационные технологии для доступа к информации, для ее поиска, организации, обработки, оценки, а также для продуцирования и передачи, которая достаточна для того, чтобы успешно жить и трудиться в условиях информационного общества.

На конференции также были обнародованы результаты исследования «Цифровая компетентность». Исследование проведено Аналитическим Центром Юрия Левады при поддержке компании Google в январе 2013 года. В нем приняли участие 1203 подростка 12–17 лет и 1209 родителей детей этого возраста из 58 городов России. Подобного рода масштабные исследования проводились в России уже второй раз, и результаты, полученные в 2013 году, по словам представителей Фонда, свидетельствуют о значительном увеличении (на порядок) количества пользователей Сети.

Проведенное исследование позволило сделать ряд выводов о цифровой компетентности российских подростков и их родителей, а также путях их повышения.

1. Интернет-активность детей (как ежедневная, так и почасовая), а также разнообразие использования детьми различных устройств значительно превышает использование Интернета родителями. Это означает, что использование Интернета становится неотъемлемой частью образа жизни цифрового поколения. И этот образ жизни в большинстве случаев расходится с образом жизни их родителей. В условиях возрастающей мобильности и персональности Интернета родителям и педагогам важно становиться его компетентными пользователями, быть «на одной волне» с детьми, обсуждать с ними эту значимую часть их жизни, изучать вместе новинки, возможности и риски. А также выстраивать

вместе баланс между реальностью и виртуальностью, стремясь к умеренному и целесообразному использованию Интернета.

2. Большинство подростков (80%) и половина родителей (50%) демонстрируют высокую уверенность в использовании Интернета, что создает иллюзию достаточной или даже высокой компетентности российских Интернет-пользователей. Однако полученные данные об уровне цифровой компетентности разрушают миф о том, что цифровое поколение все знает и все умеет в Интернете. Цифровая компетентность и российских детей, и их родителей невелика: она составляет примерно треть от максимально возможного.

3. 75% родителей и 68% детей учились использованию Интернета самостоятельно, бессистемно и неорганизованно, не имея возможности регулярно и систематически обсуждать опыт пользования Интернетом. Такая ситуация показывает высокую необходимость подготовки специальных методических пособий и обучающих программ по повышению цифровой компетентности педагогов и школьников.

4. Немаловажно, что – по сравнению с родителями – подростки готовы активно учиться, но у них также чаще встречается «почивание на лаврах», когда иллюзия цифровой компетентности приводит к недостатку мотивации: «мне уже не надо учиться»,– как бы говорит подросток. Поэтому особую важность приобретают программы, в которые включено «мотивирующее» звено, работающее на осознание необходимости повышения цифровой компетентности.

5. Высокая интенсивность использования Интернета подростками показывает, что значимость Интернета для цифрового поколения продолжает расти: он не только является основным источником информации и инструментом коммуникации, но и превращается в важнейший фактор социализации подростков. Такое положение дел требует специального внимания к формированию ответственных и сознательных «цифровых граждан».

6. И дети, и родители осознают высокий образовательный потенциал Интернета и его роль в развитии коммуникационных навыков и в процессе обучения. В связи с этим большинство родителей отмечают необходимость обеспечения доступа детей к Интернету при условии использования инструментов безопасного поиска и безопасного доступа в Интернет.

Все это подтвердило необходимость повышения цифровой грамотности детей, педагогов и родителей.

Я бы хотела рассказать о работе, которая проводится в этом направлении во Владимирском социально-реабилитационном центре.

Важно отметить, что с 2013 года наше учреждение принимает участие в реализации долгосрочной целевой программы Владимирской области на 2013–2015 годы «Детство без насилия», утвержденной Постановлением Губернатора Владимирской области от 28 июня 2013 г. N 759. Цель программы – профилактика жестокого обращения в отношении детей; обеспечение реабилитации детей и семей, ставших жертвами насилия, жестокого обращения и преступных посягательств; повышение информированности детей о возможных рисках и опасностях; повышение ответственности родителей за действия, направленные против детей; формирование в обществе нетерпимого отношения к различным проявлениям насилия по отношению к детям. Одним из направлений работы в рамках данной программы стало обучение детей, родителей, педагогов правилам ответственного и безопасного поведения в современной информационной среде, способам защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи.

В конце 2010 года в нашем Центре был оборудован компьютерный класс. Все компьютеры подключены к сети Интернет. На компьютерах в компьютерном классе установлены программы ограничения доступа несовершеннолетних к нежелательным ресурсам в сети Интернет: Child Protect (ограничение доступа к таким социальным сетям, как: Одноклассники, Мой мир, facebook, vkontakte.ru); Blok Program (ограничение доступа к сайтам, содержащим ненормативную лексику, ссылки на азартные игры и др.).

Безусловно, компьютерный класс открыл пред нами новые возможности: за это время около 200 воспитанников стационарного отделения школьного возраста были включены в работу по программе обучения компьютерной грамотности «КОМП». Ребята приобретали навыки работы с текстовыми и графическими редакторами, создавали презентации при подготовке к мероприятиям, пробовали свои силы в создании мультфильмов. Для ребят регулярно организуются телемосты, онлайн-игры с воспитанниками социально– реабилитацион-

ных центров Владимирской области. Эта интересная форма работы дает детям возможность познакомиться со сверстниками из других городов, научиться преодолевать коммуникативные барьеры. Дети очень ответственно готовятся к каждой встрече, и после онлайн-общения с удовольствием рефлектируют: анализируют поведение (свое и своих собеседников), учатся быть более раскованными, открытыми и просто грамотно излагать свои мысли.

Опираясь на опыт, представленный на конференции в Москве, для воспитанников стационарного отделения, родителей и педагогов Центра нами была составлена и сейчас уже успешно апробирована подпрограмма по основам информационной безопасности «Интернешк@».

Цель подпрограммы: формирование у детей навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи:

– формирование информационной, коммуникативной, потребительской и технологической компетентности;

– информирование детей о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

– формирование навыков правильного реагирования на опасности сети Интернет;

– профилактика формирования у несовершеннолетних интернет – зависимости и игровой зависимости;

– предупреждение совершения несовершеннолетними правонарушений с использованием информационно-телекоммуникационных технологий;

– формирование у детей практических навыков защиты своего информационного пространства.

Целевая группа: данная подпрограмма ориентирована на детей в возрасте от 7 до 18 лет, оказавшихся в трудной жизненной ситуации, проходящих социальную реабилитацию в Центре, а также членов их семей и специалистов учреждения.

Подпрограмма охватывает четыре основных модуля:

1) Контент и необходимость критически оценивать информацию в Сети: информационная компетентность, контентные (содержательные) риски, которые возникают в процессе использования находящихся в Сети материалов, содержащих неэтичную, противозаконную, вредоносную информацию. Практикум учит распознавать ложь в Интернете.

2) Онлайн-коммуникация и противодействие агрессии в Интернете (кибербуллингу) – коммуникативная компетентность: Интернет как инструмент коммуникации, коммуникативная компетентность, самопрезентация и Я-концепция, сетевые возможности для обучения, безопасность общения в Интернете. В этом разделе также отрабатываются коммуникационные риски: кибербуллинг, груминг.

3) Потребление услуг (электронные покупки, платежи) – потребительская компетентность и потребительские риски, (например, «нигерийские письма»).

4) Использование технических инструментов безопасности (антивирусное программное обеспечение, родительский контроль и пр.) – технологическая компетентность.

Каждый раздел построен по следующей схеме:

Лекция

Практикум: Разминка – мотивационный разогрев;

Упражнение – актуализация опыта;

Дискуссия – рефлексия опыта;

Рекомендации – обобщение опыта:

– оценочные и рефлексивные материалы;
– интерактивная игра;
– рекомендуемая литература.

Занятия с детьми в условиях компьютерного класса проводятся 1 раз в неделю, повторяются ежеквартально, что связано с особенностью работы учреждения и средним сроком проживания воспитанников в стационарном отделении.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается ребенок, находящийся в сети Интернет. С родителями мы стараемся вести разъяснительную работу,

используя разнообразные формы: выступления на родительских собраниях, индивидуальные беседы, информация на сайте Центра, встречи со специалистами, распространение информационных материалов, буклетов для родителей по обеспечению информационной безопасности в сети Интернет.

Обучение педагогических работников проводится в форме семинаров, мастер-классов, круглых столов, вебинаров. На них рассматриваются проблемы информационной безопасности детей в сети Интернет, меры борьбы с нежелательным контентом, виды и формы информационно – психологического воздействия и методы защиты от него, правила и нормы сетевого этикета, причины возникновения девиантной формы поведения детей и методы работы по их профилактике и устранению.

Мы уверены, что комплексное решение поставленной задачи позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет.

Интернетом нужно научиться пользоваться так, как учат детей пользоваться спичками: держать их дома никто не запрещает, но нужно не забывать, что «спички – детям не игрушки». Информационные технологии становятся неотъемлемой частью жизни современного человека. Владение информационными технологиями, цифровая компетентность ставятся в один ряд с такими качествами, как умение читать и писать. Наша с вами задача – быть компетентными самим, уметь сопровождать детей по пространству Интернета, действуя по принципу «Учить, нельзя запретить», а не наоборот.

С. Е. Савосько,
г. Владимир

Реализация социокультурного проекта в рамках долгосрочной целевой программы «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2013–2015 годы» (психолого-педагогические аспекты), из опыта работы ГБОУ СПО «Владимирский областной колледж культуры и искусства»

Владимирский областной колледж культуры и искусства готовит специалистов в области культуры, сегодня ВОККИ – единственное учебное заведение, осуществляющее подготовку студентов по специальностям: «Библиотековедение», «Театральное – декорационное искусство», «Актерское искусство», «Социально-культурная деятельность», «Народное художественное творчество», «Театральная и аудиовизуальная техника».

С 2009 года студенты и преподаватели колледжа участвуют в реализации социокультурных проектов в рамках различных целевых программ: «Долгосрочная целевая программа Владимирской области «Комплексные меры противодействия злоупотреблению наркотиками и их незаконному обороту на 2010–2014 годы», долгосрочная целевая программа Владимирской области «Комплексные меры профилактики правонарушений во Владимирской области на 2013–2015 годы», долгосрочная целевая программа «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2013–2015 годы».

В рамках реализации целевых программ накоплен большой опыт и подготовлены проекты:

– 2009 г.– спектакль «Звезда над крышей», режиссер – постановщик – заслуженный работник культуры РФ Т. Джулай, художник – постановщик – заслуженный работник культуры РФ Рыжова Е. А.

– 2010 г.– хореографический спектакль «Мы против наркотиков!», режиссер – постановщик Ю. Зимокос (спектакль награжден дипломом за 3-е место в РФ на Всероссийской олимпиаде научных и студенческих работ в сфере профилактики наркомании и наркопреступности в номинации «Организация профилактики наркомании и наркопреступности в сфере досуга молодежи»).

– 2011 г.– реалити-проект «Легко ли быть молодым?», режиссер– постановщик – заслуженный работник культуры РФ Т. Джулай;

– 2012 г.– «Морфий. Дневник доктора Полякова», режиссер А. Кузнецов;

– 2013 г.– медиа-спектакль «Серебряный котел дури», постановщики – Р.Г Захаров, к.п.н., Н. Н. Зуева, Д. В. Абашкин, художник-постановщик – заслуженный работник культуры РФ Рыжова Е. А.

В последние десятилетия социокультурное проектирование как инновационная деятельность приобретает популярность. Изучением этого вопроса занимались: Маркова А. П., Бирженюк Г. М., Дридзе Т. М., Альтшуллер Г. С. и другие. Это специфическая технология, представляющая собой конструктивную творческую деятельность, суть которой заключается в анализе проблем и выявлении причин их возникновения, выработке целей и задач, разработке путей и средств достижения поставленной цели.

Чаще всего сферами социокультурного проектирования становятся актуальные проблемы современной молодежи. Развитие личности подростка в значительной степени обусловлено влиянием социокультурной среды. В периодизации детского развития одним из самых критических периодов, в результате которого происходит перестройка сознания, является подростковый возраст. Подросток особенно подвержен влиянию, поскольку у него нет устоявшихся взглядов, твердой жизненной позиции – эти личностные образования находятся в стадии формирования. Поэтому, включая студентов колледжа в активную деятельность по реализации социокультурных проектов, решается ряд психолого – педагогических задач:

– оптимизация условий саморазвития и самореализации личности путем включения в различные виды социокультурной деятельности;

– создание духовно насыщенного культурного пространства;

– устранение или минимизация факторов, вызывающих отклоняющиеся формы поведения и т. д.

В 2013 году на основании приказа департамента культуры и туризма администрации Владимирской области ГБОУ СПО «Владимирский колледж культуры и искусства» в рамках реализации долгосрочной целевой программы «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2013–2015 годы» подготовил спектакль рок-фантазию «Точка невозврата», режиссер-постановщик Прозоровская Е. Ю., художник-постановщик – заслуженный работник культуры РФ Рыжова Е. А.

Цель этой программы – создание безопасной информационной образовательной среды для обеспечения, сохранения и укрепления нравственного, физического, психологического и социального здоровья детей и молодежи, профилактика у детей и подростков интернет – зависимости.

15 ноября 2013 г. на сцене колледжа прошла премьера рок-фантазии «Точка невозврата». После премьеры состоялось обсуждение спектакля, в котором принимали участие: постановочная группа, администрация ГБОУ СПО ВОККИ, представители департамента культуры и туризма администрации Владимирской области, представители Управления образования г. Владимира,

Комиссии по делам несовершеннолетних и защите их прав, МУ «Молодежный центр».

В течение декабря 2013 года зрителями рок-фантазии стали учащиеся общеобразовательных школ и студенты средних специальных учебных заведений Киржачского, Кольчугинского, Судогодского, Ковровского районов.

После спектакля каждый зритель получал опрос-анкету и решал для себя сам: зависим он или нет. Показ спектакля рок – фантазия «Точка невозврата» планируется в марте 2014 г. в рамках Областной театральной недели «Театр, где играют дети».

Е. Ю. Прозоровская,
г. Владимир

Технология создания социокультурного проекта: реализация замысла рок-фантазии «Точка невозврата»

В современном обществе проблема Интернет-зависимости становится все более актуальной и серьезной: миллионы людей проводят в Интернете много часов, общаясь в чатах, на форумах, ICQ, по электронной почте, в социальных сетях, посещая различные сайты или играя во всевозможные виртуальные игры. Уже в 90-х годах прошлого столетия в мире начали активно исследовать проблему, связанную с навязчивым желание человека войти в Интернет, находясь в offline, и его неспособность выйти из Всемирной паутины, будучи online. В России феномен интернет-аддикции или интернет-поведенческой зависимости стал предметом изучения только в последнее десятилетие.

Как показывают исследования, наиболее подвержена Интернет-зависимости молодежь, особенно школьники, в силу своего возраста и отсутствия четко сформированной картины жизни. Доказано, что зависимость от Интернета, как и любая другая, подрывает здоровье – психическое, духовное, физическое. Это не может не волновать тех, кому небезразлична судьба подрастающего поколения.

Администрацией Владимирской области была принята долгосрочная целевая программа «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции на 2013–2015 годы». В рамках этой программы во Владимирском областном колледже культуры и искусства 15 ноября 2013 г. состоялась премьера рок-фантазии «Точка невозврата», воплощенная силами студентов театрального отделения. Как отмечает «Зебра ТВ», студенты «попытались предостеречь своих ровесников от интернет-зависимости, становящейся, по мнению старшего поколения, одной из самых страшных напастей XXI века».

На этапе подготовки проекта мы столкнулись с целым рядом трудностей: произведений, которые могли бы стать литературной ос-

новой постановки, оказалось крайне мало, а аналогичных творческих проектов на эту тему мы не нашли вообще. В результате, наш выбор пал на актуальный роман современного российского писателя Станислава Миронова «Virtuality», где автор в очень жесткой форме говорит о причинах и последствиях замещения подростками реальной жизни виртуальной.

Значительно переработав текст, мы оставили ту сюжетную линию, где раскрывается судьба главной героини романа – Виктории Потаповой, пытавшейся уйти от реальных проблем в Сеть. А проблем в ее жизни было немало: издевательства одноклассников, побои матери-алкоголички, предательство любимого человека. Как тут не сбежать в виртуальный мир, где, кажется, тебя ценят и понимают. Но в лабиринтах Интернета очень легко заблудиться и потерять себя. У Виктории началось раздвоение личности, а затем и амнезия. Девушка подошла к точке невозврата, после прохождения которой пути назад нет. Вслед за автором романа мы решили говорить о проблеме жестко, так, чтобы зритель получил «эмоциональный ожог» и задумался о последствиях неразумного использования Интернета.

Жанр театрализованного представления, который был выбран для постановки, позволил соединить художественный вымысел и реальные факты из жизни. А яркие средства выразительности усилили эмоциональное восприятие этой драмы и помогли создать зрелищный образ представления.

Черно-белое декорационное решение постановки отличалось простотой и лаконичностью форм: 5 треугольных конструкций создавали образ лабиринта Интернета, а, перемещаясь, становились экраном, на котором видеокадры демонстрировались, визуализируя жизнь в Сети.

Видеоматериал подбирался и монтировался с особой тщательностью, чтобы точно «бить в цель», выражая авторский взгляд на тот или иной аспект проблемы. Песни в стиле рок из репертуара групп «Трактор Боулинг», «Люмен», «Ария», исполняемые «живьем», позволяли говорить с молодежью «на их языке», языке протеста – жёстко, с вызовом, ярко и эмоционально.

В пластических композициях преобладала резкость изломанных линий, что давало возможность зрителю почувствовать хаос, происходящий в голове главной героини, когда она вспоминала о превращении

девушки с ником «Добро» в злобного тролля, играющего на чужих слабостях. Картины реальной жизни, всплывающие в воспоминаниях главной героини, были сняты как черно-белый фильм, а с помощью приёма теневого театра и интересных световых эффектов мы попытались создать иллюзию виртуального пространства.

Постановка получилась довольно жесткой, но, думается, иначе достучаться до подростков вряд ли получилось бы. «Не хотелось агитировать или «промывать зрителю мозги», хотелось, чтобы каждый «примерил на себя» судьбу главной героини и задумался: а может, и он не застрахован от этой опасности?» – размышляла студентка 2 курса и наша вокалистка Светлана Хамидова.

Работая над театрализованным представлением, студенты глубоко погрузились в проблему и многие пересмотрели свое отношение к интернету. «Интернет затягивает, знаю по себе. Проект стал для меня поводом задуматься. Стал больше читать, а в Сеть захожу только, чтобы уладить дела»,– сказал после премьеры исполнитель роли Альтер-эго Семен Дегилев.

В заключительных словах «Точки невозврата» прозвучала главная мысль автора романа, которую мы хотели донести до зрителя: иногда, чтобы понять, что ты живешь неправильно, нужно оказаться на самом краю. «Интернет, без сомнения, очень нужная и полезная вещь. Это – венец прогресса мира технологий и развлечение нашего дня. В мире десятки миллионов интернет-зависимых людей. Может, даже сотни. Но остальная часть населения от этого свободна. Среди какого числа быть вам? Решайте сами».

Выходя из зала, одни зрители говорили: «Сильно встряхнуло», другие доказывали: «Это не про нас», но равнодушных не было. Свою порцию «эмоционального шока» получили и взрослые. Многие предлагали устроить семейный просмотр, ведь, по их мнению, не только дети, но и родители часто даже и не подозревают, какие опасности таит в себе Интернет.

Думается, нашим студентам удалось «достучаться» до ровесников, сидящих в зрительном зале. Рок-фантазия «Точка невозврата» была с успехом сыграна как на сцене колледжа культуры и искусства, так и во многих городах Владимирской области. Зрители благодарили творческую группу «за интересную трактовку произведения, ори-

гинальную задумку и очень качественную постановку спектакля» (Саша Гаврилов, г. Ковров). «Здорово, технологично и по-молодежному» (Юра Антонов, г. Лакинск). На портале активной молодежи города Коврова шло обсуждение проекта: «подобных премьер уже давно не было в нашем городе, а ведь сила искусства и так называемая «наглядная» профилактика во много раз действеннее, чем просто профилактические, зачастую скучные, лекционные занятия».

Призывая молодежь не заменять реальный мир виртуальным, мы сознаём, что воздействие искусством имеет отсроченный результат. Но если молодой зритель почувствовал сопричастность проблеме, получил сильное эмоциональное впечатление, заставляющее включить механизм самосохранения, мы считаем, что цель создания проекта достигнута.

Е. А. Беляева,
г. Владимир

Подготовка участников образовательного процессак безопасному использованию сети Интернет

Сегодня Интернет – это часть ежедневной жизни каждого человека, в том числе и педагогов, детей, родителей. Интернет стал таким популярным, потому что обладает рядом уникальных возможностей: быстрый поиск информации, общение, получение дополнительного образования, расширение территориальных границ, обеспечение досуга, формирование информационной компетентности. Но в то же время взаимодействие участников образовательного процесса и «Всемирной паутины» – одна из самых актуальных проблем. Человек, захваченный безграничными возможностями Интернета, зачастую не может разглядеть рисков и угроз сети. Наиболее уязвимыми пользователями сети оказываются дети, и задача взрослых – защитить их от сетевых угроз.

Владимирский институт повышения квалификации работников образования уделяет первостепенное внимание проблемам обеспечения информационной безопасности детей. Главным направлением нашей работы является оказание методической поддержки педагогам в вопросах безопасного использования сети Интернет. В связи с этим сотрудниками кафедры информатизации образования института была разработана инвариантная лекция «Обеспечение информационной безопасности» и проведены проекты: «Безопасный мир – детям!» и «Создаем курс для родителей по информационной безопасности детей».

Цель проекта «Безопасный мир – детям!» – методическая поддержка педагогов, специалистов, руководителей общеобразовательных учреждений (ОУ), дошкольных образовательные учреждений (ДОУ) в сфере обеспечения информационной безопасности детей. В ходе проекта рассматривались следующие вопросы:

- Что такое «информационная безопасность детей»?
- Как педагогу стать «с веком наравне» в этом вопросе?
- Как подготовить детей к жизни в информационном обществе?

• Как сделать родителей союзниками в борьбе за информационную безопасность ребенка?

В другом проекте – «Создаем курс для родителей по информационной безопасности детей» – основной целью явилось оказание методической помощи родителям по вопросам информационной безопасности школьников.

«Возможен ли мир в цифровом мире?» – основополагающий вопрос проекта. Кроме этого, рассматривались проблемные и учебные вопросы, такие как:

• Интернет приносит больше пользы или вреда?

• Медиаобразование в России: решение проблем или путь в никуда?

• «Сеть», сплетенная – кем?

• Как подготовить детей к жизни в информационном обществе?

• С какими опасностями можно столкнуться в Интернете?

• Что такое «информационная безопасность детей»?

• Какие документы помогут родителям в обеспечении безопасности детей в Интернете?

• Какие ресурсы для самообразования родители могут порекомендовать своим детям?

• Какую политику по обеспечению информационной безопасности проводит наше государство?

• Как организовать безопасное общение детей в сети Интернет?

• Какое существует законодательство в области информационной безопасности?

Противоречивая информация, размещенная на разных Интернет-ресурсах; наркотики; случайные знакомства в социальных сетях; нецензурная лексика; азартные игры – все это пагубно влияет на детскую психику и влечет к необратимым последствиям среди учащихся. Сталкиваясь с опасностью при использовании Интернета, они часто не знают, как поступить и к кому обратиться в такой ситуации, и вынуждены действовать методом проб и ошибок. При таких обстоятельствах надо защищать детей от информации, способной нанести им вред, надо обеспечить их безопасность, поскольку ребенок иногда не способен правильно оценить степень угрозы информации, которую он получает или передает. Надо отметить, что темпы информатизации оказались столь быстрыми, что и семья, и школа оказались не гото-

выми к угрозам нового типа, методы борьбы с которыми еще только разрабатываются.

Без сомнения, можно и нужно контролировать доступ ребенка в сеть (ставить пароли, фильтры, вводить ограничение времени и пр.), но вряд ли только такие меры дадут желанный эффект: запретный плод – сладок. Наша задача – научить детей правильно и безопасно использовать Интернет, и поэтому мы активно вовлекаем в проекты и детей.

Так, например, 1 февраля 2014 года стартовал проект «В мире кодов», целями которого являются: активизация творческой деятельности учащихся; развитие ключевых компетенций обучающихся через самостоятельную познавательную и исследовательскую деятельность; знакомство учащихся с многообразием окружающих человека кодов; ролью кодирования информации в жизни человека; развитие коммуникативных умений и навыков учащихся при работе в группах и др. Таким образом, можно обеспечить информационную безопасность не запретами использования сети Интернет, а предоставлением альтернативы.

Несомненно, играют огромную роль и несут ответственность в отношении информационной безопасности детей их родители. Для родителей группой педагогов был разработан информационный курс «Интернет и безопасность». Данный курс открыт для всех, бесплатен и имеет массу преимуществ:

• удобная навигация, дружелюбный интерфейс;

• актуальная и достоверная информация, представленная в разных видах;

• занимательные задания и упражнения;

• полезные советы и многое другое.

Курс имеет много возможностей для своего использования:

• информирование родителей (самостоятельное изучение ими материалов или организация работы с курсом);

• ресурс для родительского лектория (проведение родительских собраний);

• источник для работы с обучающимися (проведение классных часов, проектов, внеклассных мероприятий);

• организация самообразования педагогов в сфере информационной безопасности детей и др.

Здесь каждый может найти информацию о различных типах угроз, рисков, способы защиты от них и полезные советы, представленные в виде правил для родителей.

Таким образом, обеспечение информационной безопасности и воспитание информационной культуры детей должно стать приоритетным направлением работы каждого образовательного учреждения, однако преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников.

Т. А. Горланова,
г. Владимир

Интернет, которому можно доверить ребенка

Согласно российскому законодательству, информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией (в том числе, распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

Все начинается с детства. Формируется характер, выбираются друзья, складываются взаимоотношения с близкими людьми, вырабатываются нормы поведения, а главное – закладываются традиции семейного воспитания в будущей семье. В связи с этим и с тем, что возраст людей, которые начинают работать в Интернете, становится все моложе, возникает проблема обеспечения безопасности детей. А кто им может в этом помочь, если не их родители и взрослые?

Проведенные специалистами Детского оздоровительно-образовательного центра г. Владимира исследования показали, что родителям надо помочь преодолеть трудности и приобрести опыт в воспитании собственного ребенка.

Поэтому мы выбрали главным направлением нашего сотрудничества просветительскую деятельность по волнующим родителей вопросам воспитания через «Родительский клуб». Каждое занятие происходит в интерактивной форме на позитивной ноте. Психолог клуба создает обстановку доверия и свободного общения. Педагоги-психологи акцентируют внимание участников на проблеме вопроса и вырабатывают практические рекомендации для принятия решения в условиях жизненной ситуации, которые получает в руки каждый слушатель нашего клуба.

Обсуждаемая сегодня тема информационной безопасности детей востребована слушателями клуба, т.к. о вреде электронных носителей говорят много и на всех уровнях. Выстраивая занятие, опираюсь на факт, что современные дети уже с малых лет учатся обращаться

с компьютером. Их окружают телевизоры, они постоянно общаются по телефону. Родители понимают, что без всех этих средств существовать в нашем мире невозможно, и нужно научить ребенка со всем разумно обращаться.

• В каком возрасте наиболее часто возникает интернет-зависимость? Как считают психологи, для детей 7–8 летнего возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате (находясь в Интернете) ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. До 7 лет у детского сознания нет защитного барьера от виртуальной агрессии, только после 12 лет дети учатся разделять виртуальное и реальное.

Как показали различные исследования, первые симптомы интернет– зависимого поведения возникают в 9–11 классе средней школы. Однако «разгар болезни» наступает на первом – втором курсе ВУЗа, в период возрастающей ответственности за свою жизнь, а также решения сложной задачи по выстраиванию отношений с окружающим миром.

• Следует знать, что интернет зависимое поведение – это проявление нарушенных отношений подростков с окружающим миром, неспособность (невозможность) приспособиться к нему или следствие болезни (в частности, депрессии).

Чего делать нельзя: наказывать, отключать Интернет, лишать других удовольствий. Все эти действия не только бесполезны, но и вредны, так как подталкивают ребенка к бегству из дома.

Что надо делать: поддерживать подростка в преодолении возникающих жизненных трудностей, обучать новым способам преодоления кризисных ситуаций, обучать умению регулировать свои эмоции, строить отношения со сверстниками, управлять своим временем. Родители, не забывайте спрашивать ребенка об увиденном в Интернете. Например, начните с расспросов, для чего служит тот или иной сайт.

На занятии специалисты Центра предлагают конкретные полезные действия с целью сохранения здоровья детей при использовании носителей:

• рекомендации родителям по преодолению компьютерной зависимости;

• шесть способов избежать компьютерной зависимости;

• советы тем, кто хочет освободиться от игровой зависимости или помочь в этом друзьям и близким;

• простые правила общения по мобильному телефону;

• что и когда смотреть;

• рекомендации детских невропатологов и психологов родителям по сохранению психосоматического здоровья детей.

Родители должны понять, что выход из этой ситуации только один: культуру обращения с умной техникой нужно воспитывать с детства, т. к. телевизор с компьютером заменили и бабушкины сказки, и мамины колыбельные. Лучше всего, если дети будут смотреть какую-либо передачу вместе с родителями, чтобы потом обсудить увиденное. Задача родителя – научить ребенка думать при восприятии информации, а не принимать ее слепо как руководство к действию. Лучше выбрать конкретную передачу и посвятить просмотру определенное время, а не бесцельно блуждать по каналам.

Интересен факт, что среди детей, страдающих от компьютерной зависимости, очень мало девочек. Что это: случайность или закономерность? Что в девочке есть такое, что охраняет ее от компьютерной зависимости? Чем объясняется предрасположенность мальчиков к данной зависимости?

Психологи объясняют это тем, что девочки более вовлечены в деятельность и в домашний труд, их интересы и увлечения шире, их психическое развитие опережает психологическую зрелость мальчиков, они – в отличие от мальчиков – менее болезненно переживают кризисные возрастные периоды.

Мальчики в определенном возрасте менее успешны, не всегда и не все умеют выразить то, что чувствуют, им не хватает эмоциональной поддержки со стороны взрослых. Это рождает чувство неуверенности, снижает самооценку, падает уровень общительности. И тогда потребность в личной успешности начинает удовлетворяться игрой.

На занятии специалисты обращают внимание родителей и на санитарные нормы пользования Интернетом, так как подвергается нагрузке не только психическое здоровье ребенка, но и физическое. Существуют Санитарные правила и нормы (СанПиН 2.2.2.542–96),

которые необходимо соблюдать не только при работе на уроке, но и дома:

– проведение упражнений для глаз через каждые 20–25 минут работы за ВДТ и ПЭВМ;

– проведение упражнений (физкультминутки) в течение 1–2 минут для снятия локального утомления, которые должны выполняться индивидуально при появлении начальных признаков усталости;

– запрет на компьютерные игры перед сном.

Специалисты нашего Центра используют и другие формы работы.

Тема компьютерной безопасности прошла через родительские собрания, наш клуб за это время посетили более 500 родителей. Разработаны памятки и рекомендации для родителей по преодолению компьютерной зависимости, по сохранению психосоматического здоровья детей. В работе с родителями и педагогами используются презентации: «Влияние компьютера и интернета на подростка», «Проблемы безопасного интернета для молодого поколения». На индивидуальных консультациях педагогами-психологами используется «Тест для определения степени компьютерной зависимости». Защитит детей тот родитель, кто всегда будет интересоваться жизнью своего ребенка. Пусть он чувствует вашу любовь и заботу. Тогда проблем с воспитанием будет меньше.

И. Ю. Осипова,
г. Владимир

Безопасность детей в Интернете и организация родительского контроля

Для актуализации проблемы безопасного использования Интернета подростками в колледже ведется работа не только с детьми, но и с родителями.

Знание сущности информационной безопасности и оказываемого вреда – в случае пренебрежения ею – помогает уменьшить ее воздействие.

Оптимальная форма проведения – практикум.

Интернет – глобальная сеть, объединяющая огромное количество персональных компьютеров по всему миру. Ежедневно более миллиарда людей по всему миру используют Интернет для работы, покупок, поиска информации и развлечений, а также для общения с друзьями и коллегами.

Интернет – хранилище огромного количества информации, изображений и идей.

Там вы можете посещать лучшие музеи мира, получать образование, управлять личными финансами и планировать отдых, а также играть в игры, загружать музыку и фильмы, покупать товары и услуги и заводить друзей.

Интернет изменил нашу жизнь, предоставил новые способы общения. Интернет сделал дальнюю связь доступнее, а исследования – эффективнее. То, как мы учимся, следим за новостями, делимся впечатлениями и развлекаемся, все больше зависит от того, подключены ли к Интернету наши компьютеры, сотовые телефоны и другие устройства.

Интернет дает новые мощные возможности для связи и общения. Однако вместе с ним в наши дома проникает и внешний мир. Это требует изменить представление о защите и безопасности в Интернете.

Обычно покидая безопасную атмосферу дома и выходя в окружающий мир, мы инстинктивно усиливаем защиту, становясь более подготовленными к возможным опасностям. Вернувшись домой, мы снова снижаем защиту и расслабляемся. Эти действия мы соверша-

ем автоматически, не задумываясь. Однако безопасность в Интернете требует повышения уровня защиты даже в собственном доме или там, где мы обычно чувствуем себя в безопасности.

Поскольку Интернет превращает компьютер в окно между внешним миром и домом, Интернет-безопасность диктует необходимость использовать средства, контролирующие, кто (или что) входит в наш дом, и развивающие бдительность: кому стоит доверять, кому нет.

При любом выходе в Интернет существует угроза внешней безопасности. Эти опасности могут угрожать вашей семье, вашей конфиденциальности, вашему авторитету и вашему компьютеру.

Вот почему важно знать, как защитить себя в Интернете. Особенно актуальна тема безопасности детей в Интернете.

В подростковом возрасте Интернет становится частью социальной жизни детей: в Интернете они знакомятся и проводят время, ищут информацию, связанную с учебой или увлечениями. При более высоком уровне грамотности использование Интернета открывает множество возможностей. Родителям может быть очень сложно узнать о том, чем их ребенок занимается в Интернете. В этом возрасте дети также склонны к риску и выходу за пределы дозволенного.

Современные подростки все чаще лгут своим родителям о том, чем они занимаются в Интернете. Об этом говорится в новом отчете разработчика антивирусных продуктов McAfee. Исследование основано на опросе детей в возрасте от 13 до 17 лет.

«Около половины родителей опрошенных подростков считают, что их дети сообщают им все о своей деятельности в Интернете, а сами родители полностью контролируют активность своих отпрысков в Сети. Однако наше исследование показывает, что обманы детьми своих родителей по поводу привычек использования Интернета становятся все более частыми»,– говорится в исследовании McAfee.

Так, оказалось, что подростки, несмотря на хорошую осведомленность обо всех опасностях Интернета, очень часто подвергают себя риску, например, публикуя в Сети персональную информацию или личные фотографии и скрывая это от родителей. Многие дети признались в том, что в Интернете они получают доступ к «нежелательному контенту», тогда как 73,5% их родителей не знают об этом, не имея никаких подозрений по этому поводу.

В частности, 43% подростков признались в том, что в Интернете они получали доступ к различным сценам насилия, 36% просматривали контент эротического содержания, а 32% – просматривали в Сети порнографический контент. Более 70% подростков находят различные способы, чтобы обойти ограничения на использование Сети, выданные родителями. В 2010 г., когда проводилось аналогичное исследование, таких было только 45%.

Технические ограничения и запреты могут оказаться неэффективным способом повышения уровня безопасности в Интернете.

Дети 14–17 лет могут захотеть сохранить свои действия в тайне, особенно если родители раньше не интересовались и не узнавали о способах использования Интернета ребенком. Важным моментом для семьи становится участие в открытых дискуссиях, а для родителей – заинтересованность в том, что ребенок делает и с кем общается в Интернете.

Основными моментами, на которые необходимо обратить свое внимание, становятся:

– знакомство родителей с возможными интернет-рисками и обозначение путей защиты от них;

– оказание информационной помощи родителям в организации контроля за безопасностью детей;

– актуализирование понятия «киберпреступность»;

– наметить пути преодоления проблем, связанных с медиабезопасностью;

– дать возможность поделиться опытом.

Таким образом, можно обозначить следующие «правила», соблюдение которых может сделать посещение Интернета менее опасным для детей:

– посещать Интернет вместе с детьми, поощрять детей делиться с родителями их успехами и неудачами в деле освоения Интернет;

– объяснять детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с близкими своим беспокойством;

– объяснить ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании он-лайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя;

– помочь ребенку выбрать регистрационное имя, не содержащее никакой личной информации. Объяснить ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д. Объяснить, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками;

– научить детей уважать собеседников в Интернет. Убедить их в том, чтобы они понимали, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни;

– объяснить детям, что никогда не стоит встречаться с друзьями из Интернет. Люди могут оказаться совсем не теми, за кого себя выдают;

– приучить детей спрашивать о том, в чем они не уверены, так как не все, что дети могут прочесть или увидеть в Интернете – правда;

– установить контроль над посещением детей Интернет с помощью специального программного обеспечения. Это поможет отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает;

– установить правила использования домашнего компьютера и постараться найти разумный баланс между нахождением в Интернет и физической нагрузкой ребенка. Кроме того, необходимо, чтобы компьютер стоял не в детской комнате, а в комнате взрослых;

– выработать семейное соглашение о работе детей в Интернет.

Если дети хотят посещать Интернет, следует выработать вместе с ними соглашение по использованию Интернет. В нем необходимо однозначно описать права и обязанности детей, четко сформулировать ответы на следующие вопросы:

– какие сайты могут посещать дети и что они могут там делать;

– сколько времени дети могут проводить в Интернет;

– что делать, если детей что-то беспокоит при посещении Интернет;

– как защитить личные данные;

– как следить за безопасностью;

– как вести себя вежливо;

– как пользоваться чатами, группами новостей и службами мгновенных сообщений.

Информационные источники, полезные ссылки:

(http://www.oszone.net/6213/) Обеспечение безопасности детей при работе в Интернет статья, ссылки, материалы.

(http://www.securitylab.ru/software/1423/) Каталог программ Защита детей от интернет угроз на SecurityLab.ru. Описание, сравнение, оценки (http://laste.arvutikaitse.ee/rus/html/etusivu.htm) интерактивный курс по Интернет-безопасности.

Е. Ю. Миронова,
г. Гусь-Хрустальный

Веб-квест как средство формирования компетентности родителей в сфере информационной безопасности детей

В России около 10 миллионов пользователей глобальной сети Интернет – это дети. Они могут играть, знакомиться, познавать мир… Но, в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность – защитить их от негативного контента. В Федеральном законе от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» под информационной безопасностью понимается состояние защищенности детей, при котором отсутствует риск, связанный с причинением вреда информацией, распространяемой в том числе в сети Интернет,– вреда их здоровью, физическому, психическому, духовному и нравственному развитию. Указом Президента РФ от 1 июня 2012 г. N 761 «О Национальной стратегии действий в интересах детей на 2012–2017 годы» определены задачи и меры государства, направленные на обеспечение информационной безопасности детства.

В школе безопасный доступ детей в Интернет обеспечивается контентной фильтрацией от нежелательной информации. Школа также должна информировать родителей о правильном использовании интернет-технологий, быть активным участником на «рынке свободного времени» ребенка, обучать детей информационной безопасности и обеспечивать ее в образовательном процессе. Педагоги должны быть компетентны в вопросах информационной безопасности.

Обеспечение безопасности семьи, а в особенности – детей имеет очень большое значение. Именно через ежедневное общение со своим ребенком родители узнают о вопросах и проблемах, которые его волнуют. Помогая ребенку решить эти проблемы, родители учат его правильно вести себя в той или иной ситуации. Задача родителей – обеспечить информационную безопасность ребенка дома, тем самым активно сотрудничать в этом вопросе со школой.

Очень часто родители не понимают и недооценивают угрозы, которым подвергается школьник, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях. Родители, с ранних лет обучая ребенка основам безопасности дома и на улице, между тем «выпускают» его в Интернет и не знают, что точно также нужно обучать его основам безопасности в сети. Ребенок абсолютно беззащитен перед потоком информации, обрушивающейся на него из сети. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно решить ее силами только образовательного учреждения.

На региональной площадке Вики-Владимир сотрудниками кафедры информатизации ВИПКРО был проведен межрегиональный телекоммуникационный проект для педагогов, специалистов и руководителей всех видов ОУ «Создаем курс для родителей по информационной безопасности детей», основной целью которого явилось оказание методической помощи родителям по вопросам информационной безопасности школьников.

По результатам проекта мною разработан веб-квест «Как родители «код безопасности» искали… или Посторонним вход запрещен!». Целью веб-квеста явилось обучение родителей в сфере информационной безопасности детей. Участие в веб-квесте предполагается командное – семейное. Родителям важно не только общаться с ребенком на тему безопасности в режиме онлайн, но и сделать его активным участником процесса обеспечения безопасности. Каждое задание квеста моделирует ситуацию в семье, связанную с рисками во Всемирной паутине, как для ребенка, так и для взрослого.

В форме увлекательной интернет-игры вместе с виртуальной семьей Ивановых участники должны:

– «собрать «угрозы», которым может быть подвергнут ребенок в Интернете;

– узнать, как защититься от кражи персональных данных;

– узнать, как делать покупки через Интернет;

– собрать признаки Интернет-зависимости, риски потери здоровья;

– создать символ семейной онлайн – безопасности;

– создать семейные правила пользования Интернетом.

Переходя со странички на страничку, знакомясь со ссылками, команды предлагают свое решение, свои правила.

Создавая веб-квест, мы, по сути, создаем микромир, в котором участники квеста передвигаются с помощью гиперссылок, моделируя физическое пространство. Ведь часть ее, представленная на сайте для работы, находится на самом деле на различных веб-сайтах. А благодаря действующим гиперссылкам участники этого не ощущают, а работают в едином информационном пространстве, осваивают новые сервисы, выполняют задания, что способствует сплочению семьи.

Совместная деятельность требует общения и, следовательно, является целью общения. На данном ресурсе предусмотрено общение между всеми участниками веб-квеста. В комментариях они высказывают свое мнение, спрашивают, делятся своими удачами, впечатлениями. Каждый может посмотреть и оценить работы других участников.

На специальной странице команды знакомятся с критериями оценки выполненных заданий. Все участники квеста, успешно выдержавшие испытания, получают Сертификаты интернет-защитника.

Таким образом, веб-квест, используя информационные ресурсы, помогает эффективно решать целый ряд практических задач, так как в процессе работы над веб-квестом развивается ряд компетенций:

– использование информационных технологий для решения профессиональных задач;

– самообучение и самоорганизация;

– работа в команде;

– умение находить разные способы решения проблемной ситуации.

И самым лучшим из них является собственный пример. Если мы будем всегда внимательны к своей собственной безопасности, то и ребенок будет повторять эти же действия. Любой киберпреступник внимательно наблюдает за нашими действиями в сети и безошибочно выбирает себе жертву, и если мы приучим ребенка к интернет-безопасности, то шанс стать жертвой сетевого мошенничества, вымогательства, преследования – значительно снизится.

Список источников

1. Быховский, Я. С. Образовательные веб-квесты // Материалы международной конференции «Информационные технологии в образовании. ИТО-99».– http://ito.su/1999/

2. Вылегжанина, И. В. Безопасность ребенка в информационном обществе. Методические рекомендации для образовательных учреждений по проведению родительского всеобуча на тему детской безопасности в Интернете, Киров, 2011 – http://ozyorsk-shkola.ru/wp-content/uploads/2012/05/bezopasnost_rebjonka_v_informacionnom_obshhestve_copy.pdf

3. Веб-квест как способ активизации учебной деятельности учащихся – http://metodist.edu54.ru/node/40675

Н. В. Костина,
А. А. Медведникова,
Ю. М. Монахов,
И. И. Семенова,
г. Владимир

Особенности процесса пропаганды в социальных сетях

В настоящее время социальные сети прочно вошли в жизнь огромного количества людей в разных странах мира. Одной из возможных психологических атак в социальных сетях является пропаганда. Социальная сеть не только предоставляет информацию пользователям с целью информировать, но и формирует у читателей определённое мировоззрение или конкретную точку зрения на какое-то событие, интерпретируя информацию определённым образом, и, тем самым, влияя на общественное сознание.

В настоящее время мы имеем дело с пропагандой в Интернете, в частности, в социальных сетях. Процесс пропаганды стал намного проще благодаря возможностям техники: теперь вместо длительных процессов печати и раздачи листовок можно одним щелчком мыши разослать всем нарисованную листовку или отсканированный плакат.

Кроме того, пропагандистскими методами стали теперь не только призывные лозунги, сформулированные в повелительном наклонении, но так называемая скрытая пропаганда (комментарии к записям и фотографиям пользователей, распространение аудио – и видеофайлов, которые несут в себе определённую идею и др.) Все это активно используется для незаметного воздействия на общественное мнение.

Проблема безопасности в Интернете не отрицается и активно обсуждается различными организациями, но пока нет сколько-нибудь эффективных методов ее решения. Одним из направлений научной деятельности кафедры информатики и защиты информации является исследование процессов пропаганды в социальных сетях, в частности – разработка методики оценки восприимчивости пользователей к предоставляемой информации (в том числе к пропаганде).

Цель этой работы заключается в комплексном исследовании механизмов и факторов, объективно влияющих на распространение пропагандистских материалов в социальных сетях, а также в разработке методики оценки эмоциональной составляющей текстовых сообщений. Объектом исследования являются микроблоги узла социальной сети.

Методика расчета численных выражений эмоциональности текстов выглядит следующим образом. Основная формула расчета имеет вид:

$$PMI_{(слово,шкала)} = \log_2\left(\frac{f(слово,шкала)}{f(слово)\cdot f(шкала)}\right), \qquad (1)$$

где f (слово) – количество результатов запроса для каждого слова из текста;

f (шкала) – количество результатов поискового запроса всех слов из шкалы в блогах и новостях;

f (слово, шкала) – количество результатов запроса употребления каждого слова из текста с любым из слов из шкал.

Ранее авторами было получено восемь шкал (радость, вдохновение, неясность, недовольство, страх, злость, расстройство, равнодушие) для оценки текста. Каждая шкала состоит из семантических дифференциалов, ассоциирующихся с ней и наиболее полно ее описывающих.

Анализируемый текст фильтруется от стоп-слов и знаков препинания. Вычисляется значение параметров из формулы посредством поисковых запросов с помощью «Яндекс API». Затем рассчитывается PMI–IR для всего текста.

Далее вычисляется нормированное значение PMI для конкретного слова по формуле:

$$PMI_{норм}(слово,шкала) = \frac{pmi(слово,шкала)}{\log_2(f(слово,шкала))}, \qquad (2)$$

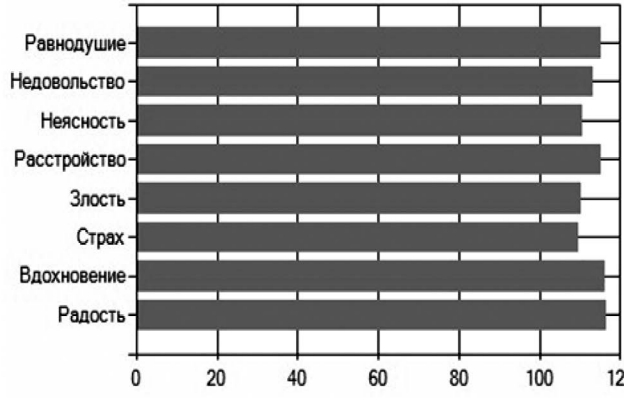
Значения PMIнорм складываются отдельно для каждой шкалы, и получается значение PMI (шкала). Затем сравнивают восемь полученных значений и выявляют принадлежность текста к определенной шкале.

Для проверки этой методики был проведён эксперимент. Были выбраны 2 текста одного и того же события, но из разных источников. Первый текст считаем нейтральным, второй – эмоционально окрашенным (Рисунок 1).

Нейтральный текст:	Эмоционально окрашенный текст:
В парке Славы Тернополя 9 мая 2013 проходило празднование Дня Победы в Великой Отечественной войне. Во время празднования народные депутаты Украины и другие присутствующие на мероприятии лица препятствовали гражданам и представителям отдельных политических партий пройти к Вечному огню. На Украине возбуждено уголовное дело по факту драки. Беспорядки устроили депутаты от националистической партии «Свобода». 9 мая они пытались помешать сторонникам левых сил возложить цветы к Вечному огню. Среди участников церемонии было много ветеранов. В конфликт вмешались бойцы спецподразделения «Беркут». Они оттеснили националистов и задержали наиболее активных участников столкновений. В прокуратуре отметили, что санкция статьи, по которой открыто производство, предусматривает ограничение свободы на срок до пяти лет или лишение свободы на срок до четырех лет.	С дымовыми шашками, беспорядками, драками и задержаниями – так неспокойно прошел День Победы в Тернополе. Столкновений избежать не удалось. Народные депутаты, презрев всяческие права демонстрантов на воспоминания и заслуженные почести, весьма агрессивно пытались помешать самым простым и традиционным мероприятиям для Дня Победы. Элементарно ветераны не могли спокойно возложить цветы к монументу в честь павших в войне, не могли просто пройти по улице, не боясь за собственную жизнь! А когда же служители правопорядка силой пробили путь демонстрантам к мемориалу, защищая ветеранов от летящей в них пиротехники, власти вдруг самих сотрудников милиции объявили некомпетентными и нарушающими закон. Беспредел! Разве это есть демократическое государство? По факту расколотое на два беспрестанно противоборствующих лагеря, под перекрёстный огонь которых попадает всё мирное население вплоть до ветеранов.

Рисунок 1. Нейтральный и эмоционально окрашенный тексты для сравнения

На рисунке 2 представлены гистограммы полученных результатов анализа текстов и вычисления параметров PMI по шкалам.



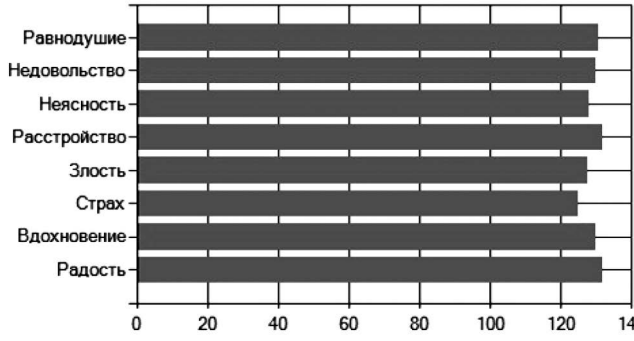


Рисунок 2. Результаты анализа нейтрального (вверху) и эмоционально окрашенного (внизу) текстов

Анализ показал, что значения PMI эмоционально окрашенного текста действительно выше. Авторы считают, что данный параметр можно специально менять для корреляции с интересами пользователя социальной сети путем добавления или удаления уникальных слов сообщения из различных шкал. Таким образом, зная все PMI сообщений профиля узла, появляется возможность ориентироваться на пользователя, тем самым помогая ему лучше усваивать информацию.

Что же касается исследования процессов распространения пропаганды в социальных сетях, здесь авторы основываются на результатах, полученных эмпирическим путём. В рамках работы необходимо было определить критерий эффективности рассылки пропагандистских сообщений и выделить факторы, влияющие на эффективность. В качестве критерия оценки был выбран параметр, равный отношению количества вступивших в группу новых пользователей к количеству отправленных пользователям сообщений с приглашением.

Эффективность рассылки зависит от восприятия информации получателем сообщения. Основываясь на проведенных экспериментах и полученных результатах, был предложен перечень факторов, влияющих на развитие и продвижение сообщений пропаганды.

1. Дружеские связи с источником – сообщение, отправленное другом, вызывает больше доверия. Повышает эффективность на 10–15%.

2. Интерес к группе – рассылка с использованием таргетинга (целевой аудитории по интересам, ВУЗу и т.д.) повышает эффективность на 15–30%.

3. Наполнение и привлекательность профиля источника и группы – чем больше информации, тем больше доверия. Повышает эффективность на 10–15%.

4. Информационный повод – актуальность сообщения в выгодный для получателя временной интервал повышает эффективность рассылки на 40–50%.

5. Возраст и пол источника – к примеру, сообщения, рассылаемые девушками в возрасте от 18 до 24 лет, более эффективны на 30–40%.

6. Активность в группе – группа не должна быть «мертвой»: чем актуальней в ней информация, тем рассылка эффективней на 15–18%.

В настоящее время работа в области пропаганды в социальных сетях ведется в обоих направлениях. В ближайшее время планируется разработать усовершенствованную методику оценки эмоционального окраса текста для более объективного распознавания характера сообщений, а также продолжить изучение процессов распространения информации в социальных сетях с целью выявления дополнительных параметров влияния на восприятие информации и дальнейшей разработки методов защиты от распространяемой пропаганды.

С. А. Сомова,
г. Владимир

Участие в сетевом семейном квесте – один из видов эффективного обучения родителей Интернет-безопасности

Здравствуйте! Вас приветствует Сомова Светлана Алексеевна, учитель русского языка и литературы МБОУ «Энтузиастская Основная Общеобразовательная Школа» Юрьев-Польского района, Владимирской области.

Тема моего доклада: «Участие в сетевом семейном квесте „Как родители «код безопасности» искали… или Посторонним вход воспрещен!“ – один из видов эффективного обучения родителей Интернет безопасности».

Дети и подростки – активные пользователи Интернета. С каждым годом сообщество интернет-пользователей молодеет. Одной из важнейших координат их развития становятся инфо-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 родителей.

Этот вопрос затронула Сетевая научно-практическая конференция «Аспекты информатизации образования: информационная безопасность (опыт, проблемы, перспективы)», где была организована работа секций. Я приняла участие в секции № 3: «Работа с родителями по информационной безопасности детей». Здесь были затронуты вопросы: «Что такое контентные риски? Какие они бывают?» (незаконные, неэтичные, вредоносные). «Что может расстроить подростков в сети?»

Для обучения по данным темам была предложена полезная информация на нескольких сайтах:

http://learningapps.org/display?v=pms38oqgc

негативный контент

https://docs.google.com/file/d/0B5JUeIwxuLHwbjQ4RHVUeXVBdUU/edit

риски и минусы негативных контентов
https://docs.google.com/file/d/0B5JUeIwxuLHwUzB3ZGpCNXNMZWc/edit

презентация «Рекомендации родителям по минимизации риска в социальных сетях»
https://docs.google.com/presentation/d/10khN_-iVNfOxK-DP5DrLaWE90kulvpmoiYBYM3xGPRg/edit#slide=id.p

безопасный интернет для детей
https://docs.google.com/file/d/0B5JUeIwxuLHwb0ZaczRIUDcxN3c/edit

классификация интернет-угроз
https://sites.google.com/site/roditelidetibezogfsnost/kontentnye-riski/negativnyj-kontent

родителям об информационной безопасности детей

После этого предлагалось выполнить некоторые задания для закрепления материала: решить кроссворд, «записать» правильно текст, основываясь на полученных знаниях. Для любого родителя необходим стимул конечного результата. Таковым стал сертификат участника конференции, который нацеливает на умение четко преподнести готовую информацию ребенку или найти верное решение сообща. В любом случае – это диалог двух поколений: родителей и детей.

Продолжалась работа в Интернете по данной теме в сетевом семейном квесте: «Как родители „код безопасности“ искали… или Посторонним вход воспрещен!», где главной целью было то, чтобы родители получили один из видов эффективного обучения Интернет безопасности.
https://docs.google.com/forms/d/1NYwYya5lUVxFhi0YzzeX2fjeQjaZK9yTHOV3X9u9itM/viewform

Здесь после регистрации по ссылке надо было выполнить 6 заданий. Первое – работа с информационными материалами, которые дают ответ на вопросы:

– Каким угрозам может быть подвержен ребенок?

– Какие симптомы компьютерной зависимости вы знаете? Как их определить?

В статье были также даны информационные правила для родителей.

• Уважаемые родители! Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой.

• Уважаемые родители! Знайте, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые легко можно настроить самостоятельно.

• Уважаемые родители! Создайте на компьютере несколько учетных записей, чтобы каждый пользователь мог входить в компьютер (систему) независимо и иметь собственный уникальный профиль.

• Уважаемые родители! Поддерживайте доверительные отношения с ребенком, чтобы всегда быть в курсе, с какой информацией он сталкивается в сети.

• Уважаемые родители! Объясните детям, что далеко не всё, что они могут прочесть или увидеть в Сети,– правда. Необходимо проверять информацию, увиденную в Интернете.

• Уважаемые родители! 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 контента.

Следующее задание направлено на защиту от кражи персональных данных. Для этого надо было освоить новый сервис loonapix. Мы – семья Сомовых (папа, мама, дочка) – с удовольствием сделали это. В комментариях шел обмен мнениями по поводу персональных данных. Еще родители поделились опытом, как надо правильно делать покупки через Интернет, чтобы не навредить себе, родным, окружающим. Здесь не затрагивался вопрос о переводе платежей или об оплате по карте другими системами. В задании дана была четкая лекция по поводу заказов через Интернет.

Самой «нужной» для семейного квеста стала страничка, где родители с интересом познакомились с информацией о рисках потери здоровья и зависимости от Интернета:

Психологические симптомы:

1. Хорошее самочувствие или эйфория за компьютером.

2. Невозможность остановиться.

3. Увеличение количества времени, проводимого за компьютером.

4. Пренебрежение семьей и друзьями.

5. Ощущения пустоты, депрессии, раздражения не за компьютером.

6. Ложь работодателям или членам семьи о своей деятельности.

7. Проблемы с работой или учебой.

Физические симптомы:

1. Синдром карпального канала (туннельное поражение нервных стволов руки, связанное с длительным перенапряжением мышц).

2. Сухость в глазах.

3. Головные боли по типу мигрени.

4. Боли в спине.

5. Нерегулярное питание, пропуск приемов пищи.

6. Пренебрежение личной гигиеной.

7. Расстройства сна, изменение режима сна.

https://sites.google.com/site/roditelidetibezogfsnost/risk-poteri-zdorova/psihologiceskie-problemy

Ведь дети поколения «игрек» и «зет» – совершенно разные по умению использовать полученную информацию, а также добывать ее определенными способами.

Для создания символа семейной онлайн-безопасности – это следующее задание – надо было освоить сервис imagechef или graphing. У нас, семьи Сомовых, это получилось. Сервис интересный, простой, но требующий усидчивости и творчества.

http://graphing.ru/data/jpeg/ulv69785856.jpeg

Последним, 6-м заданием квеста стала презентация, созданная на тему: «Интернет. Правила для родителей», где выработали совместные семейные правила пользования Интернетом.

http://www.docme.ru/doc/205848/internet.– pravila-dlya-roditelej.– somovy-

Итогом этой работы стал Семейный Сертификат Интернет-защитника.

Помогали осваивать новые серверы, учили правильной работе в Интернете, задавали наводящие вопросы, давали исчерпывающие ответы модераторы квеста: Полякова Виктория Александровна, проректор по информатизации ВИПКРО, кандидат педагогических наук и Джакония Елена Сергеевна, методист кафедры информатизации ВИПКРО. Они научили родителей, а те, в свою очередь, будут работать со своими детьми по Интернет-безопасности.

Спасибо за внимание! Удачи в освоении Интернета!

А. В. Кручинин,
г. Владимир

Комплексная защита персональных данных

В современном мире к защите конфиденциальных сведений предъявляют все большие требования. Поскольку персональные данные (ПД) касаются каждого человека, к обеспечению гарантий по их сохранности и неразглашению надо относиться очень серьезно. Поэтому их защита является очень важной задачей.

Мероприятия по защите ПД включают в себя несколько этапов.

Первый – проведение аудита. На данном этапе необходимо определить, какие именно ПД обрабатываются в организации, цели и способ их обработки, а также список лиц, которые работают с ПД. При проведении аудита следует учитывать как автоматизированную обработку с использованием персональных компьютеров, так и обработку ПД на бумажных носителях.

Следующим этапом является разработка частной модели актуальных угроз и вероятного нарушителя. Данный документ разрабатывается на основании экспертных оценок. Модель угроз позволяет определить актуальные угрозы, класс информационной системы персональных данных, уровень защищенности и список мер по обеспечению безопасности.

Третий этап включает внедрение организационных мер и разработку комплекта организационно-распорядительных документов. Последний в зависимости от типа организации может содержать до 40 документов (приказы, акты, журналы и т. д.). По завершении разработки документации необходимо провести инструктаж персонала, который непосредственно имеет доступ к ПД.

Четвертый этап – проектирование системы защиты. Важно, чтобы система защиты перекрывала все актуальные угрозы, которые были определены в модели угроз. Как правило, система защиты состоит из компонентов:

– антивирусная система;

– система защиты от несанкционированного доступа;

– система межсетевого экранирования.

Если в вашей организации используется передача ПД по открытым каналам связи, таким как Интернет, то в дополнение к вышеописанным системам необходимо применять средства шифрования.

После выбора проектного решения можно приступать к установке и настройке средств защиты на персональные компьютеры и серверы, на которых идет обработка, хранение или передача ПД. При выборе средств защиты нужно учитывать наличие сертификатов ФСТЭК или ФСБ России.

Завершающим этапом защиты ПД является аттестация. Это – комплекс организационно-технических мероприятий, в результате которых подтверждается соответствие объекта требованиям безопасности информации, установленным нормативными актами.

В заключение следует отметить, что при проведении мероприятий по защите ПД нужно придерживаться комплексного подхода, в результате которого ваша система будет надежно защищена от различных типов угроз.

СЕКЦИЯ ДЛЯ МОЛОДЕЖИ «ИНТЕРНЕТ БЕЗ БЕД»

О. А. Сморжанюк,
г. Владимир

Фишинговые атаки: способы реализации и методы защиты

Современное общество уже немыслимо представить без социальных сетей, информационных интернет-ресурсов и электронных платежных систем. Идентификация на этих ресурсах уже давно дефакто приравнивается к идентификации личности, а значит, аккаунты в социальных сетях и интернет – порталах представляют собой отличную цель для злоумышленников.

Данная статья посвящена фишингу (от английского слова «fishing» – рыбалка) – способу интернет-мошенничества, с помощью которого злоумышленник может завладеть персональными данными жертвы, ее паролями и идентификационными данными в различных информационных системах.

Рассмотрим самые популярные виды фишинга:

1. Использование поддельных сайтов. Например, кто-то присылает вам ссылку на запись в популярной социальной сети и обещает, что по данной ссылке вы найдете свои провокационные фотографии, о которых говорит весь Интернет. Вы, не задумываясь, переходите по данной ссылке, вводите свои логин и пароль и… лишаетесь своего аккаунта в социальной сети. Оказывается, что жертва данного вида мошенничества не увидела опечатку в адресе сайта, а значит, перешла на сайт-ловушку, а не на сайт социальной сети.

Такие сайты-ловушки выглядят так же, как и их оригиналы, элементы дизайна полностью идентичны. Отличается только адрес сайта и функции, которые он выполняет, а именно – крадет пароли жертвы и/или заражает машину жертвы вирусами или троянскими программами.

Далее могут разворачиваться различные сценарии: аккаунт жертвы в социальной сети будет рассылать всем друзьям ссылки на зараженный ресурс; аккаунт будет рассылать рекламу или размещать за-

ведомо ложные новости; компьютер жертвы может стать частью глобальной бот-сети, которая будет использоваться злоумышленниками в целях атаки на различные интернет-ресурсы без ведома хозяина.

Защита от данного вида мошенничества проста – внимательность при переходе по ссылкам, своевременное обновление антивирусных программ и внесение потенциально опасных адресов сайтов в «черный» список браузеров.

2. Поддельные антивирусы и программы. В целом, такие программы по своей сути очень похожи на поддельные сайты. На некоторых сайтах вы можете получить уведомление, что ваш антивирус устарел, и мигающий яркий баннер (рекламное объявление) любезно предложит установить новейшую версию программы. Но после того как произойдет установка, ваш компьютер окажется зараженным, и дальнейшие события будут развиваться по сценариям, изложенным выше.

Также после установки поддельных программ компьютер может оказаться заблокированным программой-вымогателем. Такие программы внедряются в операционную систему, блокируют все попытки закрыть ее и обещают удалиться после того, как на указанный номер мобильного телефона будет перечислена определенная сумма.

Методы борьбы с этим способом фишинга могут быть следующие: устанавливайте программы только с официальных сайтов разработчиков, своевременно обновляйте антивирусные программы. Если заражение смс-блокером все-таки произошло – ни в коем случае не отправляйте злоумышленникам деньги, а постарайтесь найти противодействие на сайтах разработчиков антивирусов или обратитесь к специалистам.

3. СМС-рассылки. Этот вид фишинговых атак направлен на получение денег с мобильного счета жертвы. Например, жертва получает сообщение, что ее банковская карта заблокирована и нужно перезвонить по определенному номеру для получения деталей. Это – обман. У всех крупных банков заключены партнерские соглашения с операторами мобильной связи о СМС-рассылках. Получая официальные смс о списании или поступлении средств на ваш счет, вы будете видеть, что смс пришел от пользователя MINBANK или SBERBANK

или другое. Но банки никогда не рассылают смс с обычных мобильных номеров. Это – первый признак мошенничества.

Содержание сообщений, которые рассылаются с помощью такой атаки, может быть разным, каждый месяц появляются новые смс, например: «ваш сын попал в аварию, позвоните по следующему номеру», или «я поцарапала вашу машину, перезвоните» и т. д.

Защита в этом случае может быть только одна – здравый смысл. Если вы получили сообщение якобы от банка с обычного мобильного номера, но все равно переживаете за сохранность своих средств – позвоните по горячей линии вашего банка и уточните, могла ли прийти данная смс действительно из банка. Если вы получили сообщение о неприятностях с вашими родственниками – перезвоните родственникам, а не по номеру, который указан в сообщении.

4. Мошенничество в интернет-магазинах. В последнее время все большую популярность приобретает интернет-торговля. С помощью Интернета теперь можно купить все – от буханки хлеба до квартиры. Но стоит понимать, что интернет-торговля – это также хорошее поле для деятельности мошенников. Прежде чем покупать товар в интернет-магазине, убедитесь, что он действительно существует. Обычно сертифицированные магазины размещают на сайте все юридические и банковские реквизиты, адреса офисов и пунктов выдачи. Пользуйтесь услугами магазинов, которые имеют хорошие отзывы среди пользователей. Например, сервис Яндекс.маркет предоставляет отзывы и рейтинги практически обо всех интернет-магазинах на территории стран СНГ.

Если вы покупаете товар на международных торговых интернет-площадках, таких как ebay или avito – предварительно напишите продавцу с вопросами о товаре, просмотрите рейтинг и отзывы о продавце на сайте (сервис ebay имеет такую возможность). Перед тем как перечислить деньги за товар – выпустите виртуальную электронную карту, на которую зачислите необходимую для покупки сумму. Тем самым вы избежите компрометации данных своей банковской карты. Если вы не получили в течение определенного продавцом времени свой товар – пожалуйтесь администрации торговой площадки и потребуйте компенсацию. Если вы столкнулись с мошенничеством в интернет-магазине, который действует на тер-

ритории РФ, то обязательно напишите заявление в полицию о мошенничестве.

В данной статье рассмотрены далеко не все способы интернет-мошенничества, а лишь самые актуальные на данный момент. Хочется отметить, что чем опытнее и осведомленнее пользователи Интернета, тем сложнее злоумышленникам придумать преступную схему, которая позволит извлечь им большую прибыль.

П. В. Синев,
И. Р. Дубов,
г. Владимир

Методы достижения анонимности в сети Интернет

В то время как большая часть компьютеров всего мира интегрирована в сеть, а большая часть населения не может обходиться без взаимодействия посредством Интернета, все сложнее скрыть свою личность в Глобальной сети от других ее пользователей. С ростом количества пользователей и растущей доступностью высокоскоростных каналов передачи данных Интернет давно перестал быть «игрушкой» IT-специалистов и в полной мере охватывает все слои современного общества. В настоящее время новостные ленты популярных социальных сетей охватывают аудиторию, которая не уступает аудитории любого федерального телеканала.

Очевидно, что такой огромный информационный потенциал не может остаться без внимания государства. Одни государства вводят цензуру в своем национальном сегменте Сети, другие находят способы по ограничению свободы слова, третьи организуют сбор и контроль информации, передаваемой пользователями в сети. Нашумевшие скандалы вокруг таких людей, как Джулиан Ассанж и Эдвард Сноуден – подтверждение тому, насколько серьезна может быть проблема.

В России в последние годы также наблюдается тенденция к регулированию нашего сегмента Сети, однако законодательство в этой области еще нуждается в доработке, и ряд спорных законов об Интернет-СМИ уже вызвал массу негодования как у рядовых пользователей, так и у владельцев крупных порталов.

В настоящей статье не ставится задачи рассуждать о правильности и правомерности принятия тех или иных решений по контролю над деятельностью в Интернете, здесь будут рассмотрены методы, позволяющие оставаться «инкогнито», общаясь в сети.

Чтобы было проще, разделим анонимность в Интернете на два направления:

1. «Социальная анонимность» – это то, что человек сам (осознанно или неосознанно) рассказывает о себе.

2. «Техническая анонимность» – когда утечка деанонимизирующих данных связана с техническими средствами.

В настоящей статье пойдет речь о технической анонимности. Помимо базовых правил «этикета» безопасной работы в Интернете таких, как: выбор устойчивых паролей, очистка кеша браузера, использование защищенного соединения, ограничение Java-script на подозрительных сайтах – к наиболее распространенным средствам технической анонимности и защиты данных чаще всего относят следующие средства:

– Прокси-серверы (Proxy-server);
– Виртуальные частные сети VPN);
– Система Tor;
– Сеть I2P.

Рассмотрим каждый из них подробно.

Прокси-сервер.

Когда говорят прокси-сервер, то имеют в виду что-то, выступающее посредником между клиентом и адресатом. В разрезе же обеспечения анонимности прокси-серверы бывают:

– HTTP-(веб)-прокси-серверы. Такие серверы пропускают через себя только HTTP-трафик, по умолчанию добавляя в передаваемый трафик данные о применении прокси;

– SOCKS-прокси-серверы. В отличие от HTTP-прокси-серверов, SOCKS передаёт всю информацию, ничего не добавляя от себя. Протокол SOCKS находится на сеансовом уровне модели OSI, этим достигается независимость от высокоуровневых протоколов: HTTP, FTP, POP3 и др., что и позволяет SOCKS пропускать через себя весь трафик, а не только HTTP;

– CGI-прокси или «анонимайзеры», которые, по сути, представляют собой web-сервер с формой, где клиент вводит адрес нужного сайта. После чего открывается страница запрошенного ресурса, но в адресной строке браузера виден адрес CGI-прокси. CGI-прокси, как и любой web-сервер, может использовать https для защиты канала связи между собой и клиентом.

В общем виде схема соединения через прокси-сервер выглядит, как показано на рисунке 1. [7]

Рисунок 1. Схема соединения через прокси-сервер

Среди плюсов такого подхода можно отметить дешевизну, в Интернете можно без труда найти публичные серверы. Среди минусов – необходимость доверия к серверу и отсутствие шифрования на канале между вами.

VPN / SSH

Говоря «VPN-туннель» в данном разделе, подразумевают также и SSH-туннели. Так как (несмотря на некоторые различия) основной принцип у них одинаков. Общая схема такого соединения представлена на рисунке 2. [7]

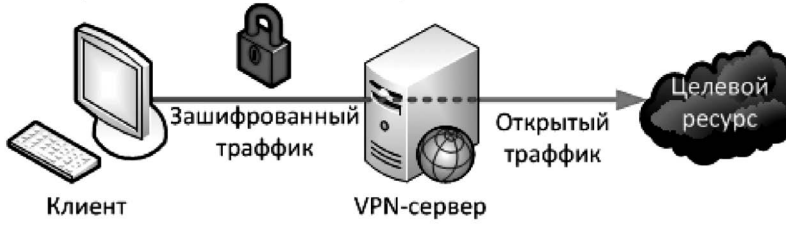


Рисунок 2. Схема соединения через VPN/SSH-туннель

VPN (англ. Virtual Private Network – виртуальная частная сеть) – обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений) [5].

В настоящее время провайдерами предлагаются следующие протоколы VPN:

– PPTP – используется наиболее широко; быстрый, легко настраивается, однако считается «наименее защищенным» по сравнению с остальными.

– L2TP + IPSec. L2TP обеспечивает транспорт, а IPSec отвечает за шифрование. Данная связка имеет более сильное шифрование.

– OpenVPN – безопасный, открытый, а следовательно, распространенный; позволяет обходить многие блокировки, но требует отдельного программного клиента.

– SSTP – такой же безопасный, как и OpenVPN, отдельного клиента не требует, однако сильно ограничен в платформах: Vista SP1, Win7, Win8.

SSH (англ. Secure Shell – «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений. [6]

SSH-туннель – это туннель, создаваемый посредством SSH-соединения и используемый для шифрования туннелированных данных. Используется для того, чтобы обезопасить передачу данных. При пересылке через SSH-туннель незашифрованный трафик любого протокола шифруется на одном конце SSH-соединения и расшифровывается на другом. В настоящее время под термином «SSH» обычно подразумевается именно SSH-2, т.к. первая версия протокола ввиду существенных недостатков сейчас практически не применяется. Протокол SSH устойчив к атакам путем присоединения посредине (англ.– session hijacking) и прослушке трафика. Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA. Для аутентификации клиента также может использоваться ЭЦП RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с Telnet) и даже ip-адреса хоста (режим обратной совместимости с rlogin). Аутентификация по паролю наиболее распространена; она безопасна, так как пароль передается по зашифрованному виртуальному каналу. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают. Для

создания общего секрета (сеансового ключа) используется алгоритм Диффи-Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью CRC32 в SSH1 или HMAC-SHA1/HMAC–MD5 в SSH2.

К плюсам такого подхода относят высокую криптографическую стойкость применяемых алгоритмов шифрования и устойчивость к большинству атак. К минусам – необходимость доверия к стороне сервера и стоимость услуг компании, его предоставляющей.

I2P – «Проект Невидимый Интернет».

I2P (сокр. от англ. «Invisible Internet Project», рус.– «Проект Невидимый Интернет») – это анонимная сеть, работающая поверх Интернета. В ней есть свои сайты, форумы и другие сервисы. По своей архитектуре она полностью децентрализована, также в I2P нигде не используются ip-адреса.

Проект I2P был начат в 2003 году для поддержки всех, кто участвует в создании более свободного общества и заинтересован в новом нецензурируемом, анонимном и безопасном средстве общения и распространения информации. [2]

Внешне сеть I2P похожа на Интернет и отличается невозможностью цензуры благодаря использованию механизмов шифрования, P2P-архитектуре и переменным посредникам (хопам). Использование таких механизмов позволяет весьма увеличить сложность деанонимизации, MITM-атак и сделать полностью невозможной прозрачную для пользователя подмену пакетов.

В настоящий момент единственным централизованным элементом сети является своеобразная реализация обычных DNS-серверов. От привычных DNS он отличается в следующих вещах [5]:

– Для определения дестхеша (адреса) используется локальная база адресов.

– База адресов периодически обновляется с серверов имен, тогда как в традиционных DNS адрес определяется по запросу к нему (однако в некоторых ОС и браузерах осуществлено кэширование).

– Поддомены не привязаны к домену-родителю, однако поставщик адресных подписок волен ограничить регистрацию субдоменов по разрешению домена-родителя.

– Возможно использование нескольких серверов имен. В официальной реализации роутера конфликты решаются по схеме «первый пришел – первый обслужил» [5], но стоит заметить, что дестхеши, явно указанные пользователем в адресных базах «privatehosts» и «userhosts», идут первыми, то есть имеют большее влияние, чем подписки.

– Поскольку сеть одноранговая – адреса являются хешами, которые хопы адресующего (посредники) используют для адресации посредникам адресата [6].

– Сервера имен находятся внутри одноранговой сети, хотя технически возможно обновлять базу извне.

– Большинство серверов имен, в противоположность регистраторам внешних имен, на настоящий момент не требуют платы за регистрацию доменов в своей базе. Основной критерий – доступность сервера по адресу-дестхэшу. Поскольку сеть является одноранговой и децентрализованной, скорость и надежность сети напрямую зависит от участия людей в передаче чужого трафика. Официальный роутер по умолчанию сконфигурирован на его раздачу.

Для доступа в I2P необходимо установить на своем компьютере программу-маршрутизатор, которая (де) шифрует, (раз) сжимает трафик и направляет его пирам в I2P. Для работы с внутрисетевыми сайтами необходимо настроить браузер для направления HTTP-пакетов роутеру, слушающему определенный порт. Для обращения к внешнему интернету через I2P необходимо использовать прокси-серверы изнутри I2P (outproxy), которых на настоящее время мало. Также внутренние сайты в сети I2P доступны из внешнего интернета через прокси.

Весь трафик в сети шифруется от отправителя до получателя. В сумме при пересылке сообщения используется четыре уровня шифрования (сквозное, чесночное, туннельное, а также шифрование транспортного уровня), перед шифрованием в каждый сетевой пакет автоматически добавляется небольшое случайное количество случайных байт, чтобы ещё больше обезличить передаваемую информацию и затруднить попытки анализа содержимого и блокировки передаваемых сетевых пакетов. В качестве адресов сети используются криптографические идентификаторы, представляющие собой открытые

криптографические ключи, которые не имеют никакой логической связи с реальным компьютером.

IP адреса в сети I2P не используются нигде и никогда, поэтому определить истинный адрес какого-либо узла в сети не представляется возможным. Все передаваемые сетевые пакеты имеют свойство расходиться по нескольким разным туннелям, что делает бессмысленным попытки прослушать и проанализировать с помощью сниффера проходящий поток данных. Также происходит периодическая смена (примерно, каждые 10 минут) уже созданных туннелей на новые, с новыми цифровыми подписями и ключами шифрования (цифровые подписи и ключи шифрования, разумеется, у каждого туннеля свои).

По этим причинам нет необходимости беспокоиться о том, чтобы прикладные программы обеспечивали шифрование своего трафика. В любом случае сеть I2P произведет четырехуровневое шифрование всех пакетов и обезопасит передачу/приём всех данных. [2]

К недостаткам данной технологии относится ее пока малое развитие, и проект развивается исключительно за счет энтузиазма его участников. Все это сказывается на скорости передачи данных и количестве ресурсов, которые доступны в сети.

Все эти средства не гарантируют стопроцентной анонимности, и каждое из них имеет свои достоинства и недостатки, однако оставляет потенциал для энтузиастов всего мира разрабатывать новые способы обходить препятствия цензуры свободного общения и распространения информации. Интернет уже сейчас стал во многом проекцией нашей реальной жизни на виртуальную реальность. То, каким образом будет он развиваться, и определит вектор направления движения всего человечества. Выбор за нами.

Список источников

[1] Комаров, А. За гранью невидимости: новые методы сохранить инкогнито в инете. // Хакер.– 2008.– № 12.

[2] Защита конфиденциальных данных и анонимность в Интернете [HTML] (https://ru.wikibooks.org/wiki/Защита конфиденциальных данных и анонимность в Интернете)

[3] Олифер, В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов.– СПб.: Питер, 2001.– 672 с.

[4] Сетевая анонимность: общие вопросы [HTML] (https://www.pgpru.com/faq/anonimnostjobschievoprosy)
[5] Анонимность в сети Интернет. Компьютер-Пресс.– 2010.– № 9
[6] Материалы интернет-ресурса «Википедия»: https://ru.wikipedia.org/
[7] Материалы интернет-ресурса: http://habrahabr.ru/

И. Н. Андреев,
г. Владимир

Цензура в Рунете

Цензура – контроль власти за содержанием и распространением информации с целью ограничения либо недопущения распространения идей и сведений, признаваемых этой властью нежелательными.

До 2012 года к сайтам применялись блокировки операторами связи, хостинг-провайдерами или регистраторами доменов только по решению суда на региональном и федеральном уровне. С 2004 года ведется федеральный список экстремистских материалов, который по состоянию на 31 января 2014 года содержит 2201 запись (закон № 114-ФЗ).

Законы, принятые в 2012–2013 годах:

• Внедрение реестра запрещенных сайтов, доступ к которым операторы связи обязаны блокировать без решения суда с предварительным уведомлением сайтов перед внесением в реестр (Закон о внесении изменений в Федеральный закон «О защите детей от информации, причиняющий вред их здоровью и развитию» № 139-ФЗ от 28 июля 2012 года, касающийся трех категорий информации: детской порнографии, пропаганды употребления наркотиков и суицида).

• Использование реестра правообладателями для досудебной блокировки – Закон от 2 июля 2013 года № 187-ФЗ.

• Закон № 398-ФЗ от 28 декабря 2013, добавляющий следующие категории запрещенной информации: призывы к массовым беспорядкам, осуществление экстремистской деятельности, участие в массовых публичных мероприятиях. Закон позволяет использовать реестр запрещенных сайтов для блокировки без решения суда с последующим уведомлением сайтов.

В качестве инструмента для блокировки применяется «единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов» eais.rkn.gov.ru. Операторы связи обязаны блокировать страницы и домены сайтов из реестра при наличии специального оборудования для глубокого анализа трафика (DPI), либо блокировать их ip-адреса – что и делается в большинстве случаев.

Роскомнадзор сообщает, что по состоянию на 13 декабря 2013 года в реестре содержится 3361 запись, в том числе в 894 случаях внесен IP-адрес сетевого ресурса. Согласно данным проекта «РосКомСвобода», блокирование этих 894 сетевых адресов приводит к тому, что абонентам российских операторов связи оказываются недоступны 35 498 сайтов.

Технические способы обхода блокировок используют возможность доступа к заблокированным сайтам через другие доступные ресурсы. К таким способам относятся: кэш поисковых систем, онлайн-переводчики, rss-агрегаторы, прокси-серверы, веб-анонимайзеры (сайты, работающие как прокси-серверы), виртуальные частные сети (VPN), анонимные сети.

Технические методы обхода приводят к увеличению времени отклика, снижению скорости, большим объемам трафика, ограничению функциональности заблокированных сайтов.

Кроме того, для обхода цензуры в интернете известны следующие явления:

• эффект Стрейзанд – попытка удаления информации приводит к ее более широкому распространению путем дублирования на других серверах;

• эзопов язык – иносказание, намеренно маскирующее мысль автора.

Множество вариантов обхода блокировок сайтов делает их бессмысленными для тех, кто ищет запрещенную информацию, при этом используемые способы блокировки отрицательно сказываются на развитии русскоязычного сегмента интернета, целостности и связности глобальной сети, увеличивая размеры «закрытого Интернета».

М. В. Пивоварова,
г. Владимир

Опыт работы МБОУ СОШ № 44 по интернет-безопасности

Скорость распространения информационных технологий в наши дни становится все стремительнее. Сегодня мы говорим уже о почти стопроцентном доступе к компьютеру и Интернету.

В современной школе информация, информационные возможности являются важным компонентом учебного процесса. Учебные классы оснащаются компьютерной техникой, и ее качественное бесперебойное функционирование существенно определяет качество полученных знаний, способствует формированию компетентности учащихся.

Безусловно, обеспечение информационной безопасности учебного процесса, в том числе непрерывного функционирования компьютерных и информационных ресурсов, является весьма важным качеством. Приняты соответствующие меры по созданию безопасной информационной системы в школе, которая опирается на нормативно-правовую базу, определяющую порядок защиты информации.

Конечно, родительское воспитание и контроль являются важным фактором обеспечения информационной безопасности учебного процесса. Родительский контроль может не только блокировать доступ к нежелательным для детей сайтам, но ограничивать использование Интернет по времени суток, дням недели или длительности сеанса. Существует множество программ и фильтров, которые помогут вам контролировать открытие нежелательной информации и время, которое можно проводить в Интернете. Для защиты детей в онлайн-среде не существует единого верного решения.

Анализ медиапотребления детей и подростков, проведенный институтом социологии образования РАО, НИУ «Высшая школа экономики» и социологическим центром ВЦОМ к 2013 году показал волнующие данные. Вот некоторые из них:

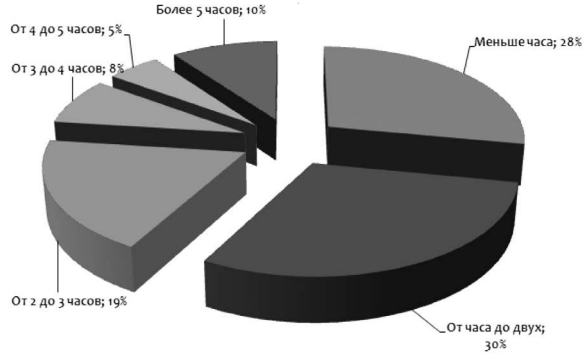
– на сегодняшний день в России насчитывается 20% пользователей Интернета. Это – дети в возрасте до 14лет;

– 25% пятилетних детей используют Интернет;

– у детей есть возможность выхода в Интернет из школы, но большинство выходят из дома, и самостоятельно, родительский контроль над использованием ребенком Интернета сохраняется до 11 лет;

– в среднем, по 2, 5 часа в день ребенок проводит в Интернет-пространстве.

Сколько времени в день школьники проводят в Интернете?



Больше всего времени дети проводят в соцсетях, общаются по скайпу, играют в онлайн-игры.

Рейтинг наиболее популярных видов деятельности в Интернет

Более 300 000 сайтов – содержат негативную информацию.

«Каждый второй ребенок 11–16 лет сталкивался в интернете с угрозами физическому здоровью, пропагандой насилия и расовой ненависти».

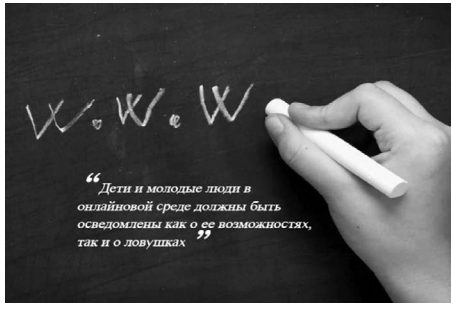
«Более трети детей 9–16 лет сталкивались в сети с материалами сексуального характера».

Каждый десятый ребенок подвержен кибербуллингу (виртуальной травле, опасной агрессии киберсреды).

В России происходит процесс вестернизации медиапотребления среди детей и подростков из-за недостатка качественного отечественного контента.

В число Интернет – угроз, подстерегающих юных пользователей, входят:

– доступ к нежелательному содержимому;
– сообщение конфиденциальной информации в сети;
– контакты с незнакомыми людьми;
– назначение личных встреч (по имеющимся данным 15% назначали встречу с незнакомцами через Интернет и 10% ходили на встречу в одиночку);



– угроза заражения компьютера вредоносными программами;
– финансовые потери.

В 2013 году мы впервые приняли участие в конференции «Диалог – онлайн», заинтересовались этой острой проблемой, получили полезную для нас информацию и с учениками старших классов решили взять в качестве проекта тему: «Информационная безопасность в нашей школе», а фраза: «Дети и молодые люди в онлайновой среде должны быть осведомлены как о ее возможностях, так и о ловушках» – стала нашим девизом.

Разработали план мероприятий и акций, которые провели в прошедшем году.

Воспитательной компонентой в младших классах является карта, по которой путешествуют дети, переходя от одного этапа к другому. Так, на равнине Безопасности для работы была выбрана тема Инфор-

мационной безопасности. Во все классы начальной школы приходили гости: Информатик и Антивирус. Они проводили уроки информационной безопасности для детей, показывали видеоролики и проводили интерактивную программу. Также дети от каждого класса подготовили тематические стенгазеты, которые размещены для всех учеников школы.

В школе оформлены информационные стенды, проведены школьные конкурсы и викторины, классные часы.

В декабре была организована конференция, участниками которой были ученики 5-х, 6-х и 7-х классов. Наша встреча посвящена важной теме настоящего времени: «Право ребенка в современном информационном пространстве». Мы говорили о праве ребенка на информацию в целом и акцентировали внимание на следующих вопросах: «Основные угрозы личной безопасности в Интернете», «Дети и социальные сети», «Влияние компьютерного языка на речь современной молодежи».

Выступление нашего гостя – главного библиотекаря отдела продвижения чтения и внешних связей Владимирской областной библиотеки для детей и молодежи Краюхиной Александры Геннадьевны «О методах обеспечения безопасного информационного пространства для детей, опыт Владимирской областной библиотеки для детей и молодежи».

В дальнейшем зам. директора МБОУ СОШ № 44 Г. П. Беркунов провел «Беседу с начинающими интернет-пользователями».

В старших классах также проводились открытые уроки с приглашением системного администратора для консультации по информационной безопасности.

Данная тема всегда находится в центре внимания учителей, на протяжении учебного процесса ей отводится важная роль в воспитании детей. Таким образом, в выступлении приводятся примеры работы последних нескольких месяцев как показатель заинтересованности детей в этой важной и актуальной проблеме.

Список источников

Анализ содержания и структуры информационного потребления современных российских детей и подростков по возрастным категориям 0–6 лет, 6–12 лет, 12–16 лет и 16–18 лет. [Электронный ресурс] Режим доступа: chttp://yandex.ru/yandsearch?text=вестернизации%20медиапотребления%20&lr=192

М. В. Маркова,
г. Владимир

Безопасный Интернет

Как и в реальности, в интернете часто встречаются опасности. Как правило, они хорошо замаскированы. Для того чтобы работа в интернете была безопасной, необходимо соблюдать несколько основных правил:

1. Никому и никогда не разглашайте свои пароли.

В качестве пароля лучше не использовать осмысленные слова, желательно использовать строчные и заглавные буквы, а также цифры. Не рекомендуется записывать пароли на бумажках и хранить их в открытом доступе, отправлять свои пароли по электронной почте или в социальных сетях.

2. Подумайте и посоветуйтесь с родителями, прежде чем добавить незнакомого человека к себе в список «друзей».

3. Старайтесь не встречаться с теми, с кем вы знакомитесь в Интернете. Если тебе все-таки предлагают встречу, то обязательно расскажи о своих планах родителям.

Имейте в виду, что опубликовать информацию в Интернете может любой человек. Практически каждый может создать свой сайт, при этом никто не контролирует, насколько правдива данная информация.

4. Уважайте собеседников в Интернете. Помните, что даже в Интернете существует «сетевой этикет». Если Вы пишете сообщение заглавными буквами, то собеседник может подумать, что Вы кричите на него.

5. Используйте правило: чем меньше Вашей личной информации в интернете, тем лучше: ведь просмотреть ее может каждый.

6. Не скачивайте самостоятельно информацию (музыку, фильмы), если от Вас требуется сначала оплатить услугу.

Очень часто для того чтобы скачать в Интернете фильм, музыку, книгу, Вас просят либо отправить SMS с кодом активации, либо ввести номер Вашего телефона. Казалось бы, это просто и так удобно! Но время идет, а доступ не активируется, кроме этого с баланса мобильного телефона начинают списываться деньги.

Рекомендация: перед тем, как отправить SMS, внимательно прочитайте условия предоставления этой услуги, обращая особое внимание на условия оплаты!

Безопасность Вашей электронной почты.

Основная задача мошенников – рассылка спама и вредоносных программ!

Рекомендации:

1. Обратите внимание на адрес, с которого Вы получаете письмо!

Адрес, в котором используются случайные последовательности символов, скорее всего, создан не человеком, а некой программой для рассылки распространения вирусов или спама.

2. Если к письму прикреплен файл, не спешите его открывать. Обратите внимание на расширение файла. Чаще всего, файлы вредоносных программ имеют «исполняемое» расширение:.exe, .com, .bin,. vbs, .pif.

1. Злоумышленники научились встраивать вредоносный код в документы Microsoft Office, в файлы картинок (.jpg, .wmf), в flash-анимацию (.swf) и в музыкальные файлы (.mp3). Необходимо осторожно относиться к вложенным файлам такого типа.

2. Все файлы, пришедшие с электронной почтой, необходимо проверять антивирусной программой.

3. Если на Вашем компьютере уже установлен антивирус, следите за тем, чтобы он был всегда включен, периодически обновляйте базы данных своего антивируса.

Мошенничество в социальных сетях:

Основная цель мошенников – распространение спама и вредоносных программ.

Спам от «друзей» или незнакомых пользователей.

Пользователи социальных сетей часто сталкиваются со спамом, который приходит к ним в «личные сообщения» от имени «друзей» или незнакомых пользователей. Это означает, что аккаунты этих людей взломаны. Как правило, чужие учетные записи взламываются с помощью специальных вирусов, которые собирают на зараженных компьютерах всю вводимую информацию.

С помощью чужих страниц мошенники отправляют всем пользователям из списка контактов жертвы ссылки на порнографические,

вредоносные или мошеннические ресурсы и приложения. Как правило, такие ссылки сопровождаются завлекающим текстом.

Пример 1: «Вот, наконец, вышла программа для просмотра гостей, которые заходят на твою страницу…»

Пример 2: «Видела твои фото, я такого не ожидала, посмотри сам!..»

Пример 3: «В этой базе данных есть вся информация на любого человека».

Отправлять спам-ссылки мошенники могут не только через сервис «сообщения», но и через публикацию соответствующих «статусов». Статусы отображаются в ленте новостей у «друзей» жертвы. Статусы могут быть не только текстовыми, но и в виде информационного сообщения самой соцсети о том, что «такому-то пользователю нравится видео XXX». Если вы нажмете на это окно видео-плеера, ваш браузер может быть перенаправлен на совершенно другой ресурс.

Также помните о том, что если мошенники взломали именно вашу учетную запись, они получат полный доступ к вашим личным данным: фотографиям, записям, комментариям, видео, личной переписке и т.д.

Совет:

– Никогда не переходите по подозрительным ссылкам;

– Не публикуйте нигде в интернете свой логин и пароль для входа в социальную сеть. Лучше использовать разные пароли для разных социальных сетей и других интернет-сервисов;

– Не поддавайтесь на призыв кого-то из «администрации сайта» сообщить ваш логин и пароль под каким-либо предлогом. Помните, что никто из администрации сайта не будет спрашивать у вас пароль;

– Регулярно меняйте пароль от социальной сети (хотя бы раз в месяц);

– Остерегайтесь «фишинговых» сайтов.

Фишинговый сайт – мошеннический сайт, сходный по написанию с названием известных сайтов, основная цель которого – получить Ваш пароль и использовать Ваши учетные данные для рассылки спама и вредоносных программ. Например, vkontahte.ru, vk0ntalkte.ru и т.д.

Скачать файл.

Мошенники в соцсетях предлагают своим «жертвам» не только «заманчивые» интернет-сайты, но и зараженные файлы. Например, в социальной сети от пользователя из списка «друзей» вы получаете архивный файл и сообщение:

«В этом архиве неизвестные фото с нашего выпускного».

Фотографий с Вашего выпускного там не будет, однако будет вредоносная программа, которая незаметно начнет работать в системе.

Совет:

Не принимайте и не открывайте файлы от незнакомых пользователей. Осторожно принимайте файлы, которые отправляют вам «друзья». Прежде, чем принять и открыть файл, задайте несколько уточняющих вопросов относительно содержания файла.

Сокращение ссылок.

Для того, чтобы сокращать длинные адреса конкретных страниц, существуют специальные сервисы. Они шифруют громоздкие строчки в ссылки такого вида: http://bit.ly/***.

С помощью короткой ссылки можно скрыть любую вредоносную информацию, и при этом пользователь ничего не заподозрит, пока не перейдет по ней.

Чаще всего мошенники используют сервисы 2sms.ru и bit.ly

Совет:

Будьте осторожны, переходя по любым коротким ссылкам. Не переходите по сокращенным ссылкам, если вы не знаете автора или нашли эту ссылку на подозрительном ресурсе.

При получении ссылок типа 2sms.ru/jkvkj даже через SMS – будьте внимательнее! При открытии с мобильного телефона или компьютера запустится вредоносная программа.

Просьбы о помощи.

В социальных сетях почти ежедневно появляются просьбы о помощи для тяжело больных людей и животных. Подавляющее большинство таких объявлений настоящие, но есть мошенники, которые используют подобные информационные поводы для получения прибыли.

Пример: «Ребенку нужна 4-я отрицательная группа крови. Телефон для связи 8908*******». Такие номера могут быть привязаны к коротким premium-номерам. Если вы позвоните на такой номер, с вашего счета спишется определенная сумма.

Совет:

В любом сообщении с просьбой о помощи должны быть указаны дополнительные контакты для связи помимо мобильного телефона. Если указан только номер телефона, нужно быть осторожным и не спешить звонить на указанный номер!

Помоги мне зарегистрироваться.

Вам может позвонить незнакомец, который скажет, что при регистрации в социальной сети он случайно ошибся номером и на ваш телефон пришло SMS с кодом подтверждения его регистрации. Собеседник извиняется и просит подтвердить регистрацию, отправив ответное SMS.

Знайте, что звонящий – это мошенник. Если вы «подтвердите регистрацию», отправив ответное SMS, ваш номер может быть подписан на платную услугу.

Совет:

Когда вам звонит незнакомый человек и просит отправить SMS, задайте ему вопрос, почему он не может повторно зарегистрировать аккаунт?

Зачем ему нужен аккаунт, которым он не сможет в дальнейшем управлять?

Если все же вы стали жертвой мошенничества, то сообщите нам об этом в колл-центр своего оператора.

Звонок на незнакомый номер.

В социальных сетях и на сайтах знакомств мошенники создают страницы, где указываются данные и размещаются фотографии вымышленных людей. С помощью этих страниц они знакомятся с другими пользователями сайта.

Со временем мошенники входят в доверие и предлагают перейти собеседнику на более «близкое» общение и оставляют свой номер телефона. Номера мошенников имеют необычный трехзначный код, который используется для предоставления платных услуг.

При звонке на телефон с данным кодом взимается дополнительная плата. В результате общение по телефону оборачивается большим счетом за мобильные услуги, который присылают позднее. В данном случае абоненту трудно что-то доказать, так как мошенник часто меняет телефоны и создает новые страницы. Вычислить его практически невозможно.

Совет:

Будьте внимательнее при знакомствах в интернете. Не раскрывайте незнакомому человеку свои личные данные, которыми могли бы воспользоваться злоумышленники.

«Билайн» рекомендует несколько раз подумать, если при знакомстве в интернете вам предлагают отправить SMS на короткий номер или совершить звонок на любой подозрительный номер (сообщите этот номер своему оператору, чтобы он смог его своевременно заблокировать). Будьте бдительны!

Фальшивые антивирусы.

В интернете мошенники активно распространяют поддельные антивирусы, которые никак не защищают компьютер, но выдают ложную информацию о заражениях. Причем такие программы настойчиво требуют заплатить за активацию. Данные о том, что ваш компьютер якобы заражен, выдают и некоторые сайты (мошеннические или взломанные). При заходе в определенный раздел в окне браузера появляется сообщение:

«Сообщение Центра безопасности Windows: Ваш компьютер и личная информация подвергаются опасности, требуется немедленная очистка от вирусов и троянских программ!»

Ниже имеется кнопка «лечить все» – после нажатия загружается поддельный антивирус, а вы перенаправляетесь на другой мошеннический сайт.

Совет:

Покупайте только лицензионное программное обеспечение известных производителей на официальных сайтах поставщиков. Там же вы можете загрузить тестовую версию, чтобы оценить работу выбранного продукта.

И. А. Скурлова,
Е. К. Булгакова,
г. Владимир

Интернет-зависимость: как избавиться от нее и вернуться в реальность

Данное выступление было представлено на конференции в сопровождении практической части, которая включала в себя дискуссию, игры и опрос. Несмотря на практический характер выступления, вся информация носит просветительский характер и содержит лишь общие рекомендации, т.к. для разрешения проблем с искоренением Интернет-зависимости необходим индивидуальный подход.

Речь пойдет об Интернет-зависимости, о причинах ее формирования, способах ее диагностики и профилактики.

Каждый человек на Земле абсолютно уникален, и в то же самое время между всеми людьми много общего.

Игра «Покажи, кто ты»

Цель: снятие напряжения, эмоциональная разгрузка.

Ход игры: ведущий просит выполнить предлагаемые действия только тем присутствующим, к которым это относится. Например: Поднимите руки те, кто учится в старших классах школы; Помашите правой рукой те, у кого в имени есть буква «А», и т.д.

Психологи бьют тревогу: проблема Интернет-зависимости приобретает характер эпидемии. Миллионы людей проводят все больше своего времени в сети, забывая о реальной жизни. Прежние увлечения позабыты, общение с друзьями становится виртуальным. Странички в социальных сетях, форумы, чаты и онлайновые игры поглощают все свободное время современной молодежи. Возраст Интернет-зависимых людей снижается с каждым годом. Замечено: часы, проведенные в Интернете, пролетают незаметно. Часы складываются в дни, недели, месяцы и даже годы. Реальная жизнь превращается в виртуальную.

Молодые люди тратят на Интернет свое жизненное время, которое они могли потратить на общение с друзьями, построение личных отношений с противоположным полом, занятия спортом и достижение новых побед, поиск интересных занятий, работы, зарабатывание

денег, путешествия и открытие новых граней окружающего мира. Вместо того чтобы жить полной и интересной жизнью, современная молодежь «просиживает» ее у компьютера!

Почему же возникает зависимость от Интернета? Интернет-среда привлекает своей доступностью и анонимностью. Можно виртуально общаться, оставаясь невидимкой. Можно свободно выражать свои мысли и отстаивать свою точку зрения, не опасаясь общественного мнения. Наконец, можно создавать любые виртуальные образы своего «Я», воплощая тем самым свои фантазии и желания, удовлетворяя потребности.

Что скрывается за пагубным пристрастием к Интернету?

Дискуссия с участниками на тему:
«Причины возникновения Интернет-зависимости»

Цель: создание возможности обратной связи с присутствующими.

Каждый желающий может в свободной форме выразить свое мнение о причинах возникновения Интернет-зависимости.

Причины Интернет-зависимости

1. Особенности характера.

Психологи отмечают, что большинство людей, подверженных Интернет-зависимости, отличается неуверенностью в себе, проблемами в общении, неудовлетворенностью своей жизнью, низкой самооценкой и комплексами. Таким образом, уходом в виртуальный мир пользователи пытаются компенсировать эти недостатки, зачастую создавая себе противоположные образы.

Игра «Встаньте с мест»

Цель: выявление особенностей характера участников.

Ход игры: ведущий попеременно показывает участникам игры разное количество пальцев на руках и каждый раз просит, чтобы встало с места определенное количество людей.

При анализе итогов игры ведущий обращает внимание на различное поведение участников в ходе игры. Кто-то пытался каждый раз попасть в нужное количество людей, кто-то побоялся оказаться лишним, а кто-то решил, что лучше не участвовать в игре и остаться лишь наблюдателем.

2. Реализация своих желаний и потребностей – осознанных и подсознательных. Ресурсы Интернета способны удовлетворить любые потребности – правда, только на виртуальном уровне.

3. Самореализация, стремление к самовыражению: ведение блогов, публикация своих творений, комментарии к чужим проблемам на форумах и т.д. Среди зависимых от Интернета много тех, кто по каким-то причинам не смог реализовать себя в реальной жизни и ушел в жизнь виртуальную. Важно понимать, что успехи в Интернете никак не могут влиять на то, что происходит в реальной жизни: настоящая жизнь неумолимо проходит мимо.

4. Нехватка общения и поиск общественной поддержки в сетях. К примеру, возможность анонимно высказать свое мнение и получить одобрение. Или попросить совета, как решить ту или иную проблему, в которой сложно признаться друзьям и близким.

Упражнение «Сколько у меня друзей»

Цель: показать участвующим в работе секции различия между реальным и виртуальным миром.

Ход упражнения: ведущий предлагает участникам вспомнить количество «друзей» в социальных сетях и поразмыслить, со сколькими из них они знакомы в реальности, что их связывает с ними и представить: на чью помощь они могут реально рассчитывать при возникновении сложной жизненной ситуации.

В чем опасность Интернет-зависимости? На первый взгляд, Интернет-зависимость кажется достаточно безобидной. Но эта видимость обманчива, последствия ее – самые серьезные:

• упущенное время и бесцельно потраченные годы жизни,

• пассивное отношение к жизни, безвольность (нежелание действовать, избегание ответственности и ситуаций, когда нужно делать выбор),

• социальная дезорганизация (страх перед реальными отношениями, неумение общаться, что ведет к проблемам в личной жизни и невозможности создать семью, эффективно трудиться и т.д.),

• социальная изоляция (социофобия, одиночество, депрессии).

Подростковая Интернет-зависимость – бегство от реальности. Подросток ищет в виртуальном мире то, чего ему остро не хвата-

ет в обычной жизни: общения, понимания, поддержки. Как правило, такие дети отличаются обидчивостью, повышенной ранимостью и тревожностью. Они испытывают сложности в выражении эмоций, неспособны делиться своими переживаниями, замкнуты, с трудом адаптируются в коллективе и не умеют строить отношения со сверстниками.

Если ребенок проводит все свое время в социальных сетях, предпочитая общаться с виртуальными друзьями, он нуждается в помощи.

Интернет-зависимость у подростка сигнализирует о серьезных психологических проблемах, которые необходимо решать вместе с психологом.

К тому же, зависимость от Интернета делает ребенка апатичным, подавляет волю. В будущем это ведет к тому, что ему сложно будет адаптироваться к нормальной жизни, ставить перед собой цели, добиваться желаемого, развиваться, работать, строить отношения с другими людьми.

Проведение теста на определение Интернет-зависимости

Цель: выявление склонности к развитию Интернет-зависимости.

Всем участникам раздаются бланки опросников. Анонимно каждый участник секции в своем листе должен отметить только те утверждения, которые имеют прямое отношение к нему. После заполнения бланков под руководством ведущего происходит самостоятельная обработка результатов.

Как избавиться от Интернет-зависимости? Многие, страдающие Интернет-зависимостью понимают все это, но не пытаются хоть както изменить свою жизнь. Интернет-зависимость – это зависимость психологическая. Для избавления от нее нужна не только сила воли, но и помощь профессионала для выяснения причин этой зависимости. Ведь зачастую причиной является затянувшаяся депрессия: человек пытается скрыться от проблем в сетях Интернета, его посещают суицидальные мысли.

Важно понять, что уход в виртуальное пространство не решит реальных проблем. Необходимо помнить, что каждый человек сам ответственен за свою жизнь и тот выбор, который он делает.

Вот несколько советов, которые могут помочь избавиться от Интернет-зависимости:

1. Занятия спортом, увлечение (хобби), общение с людьми, разделяющими ваши увлечения.

2. Пополнение запаса знаний не из Интернета, а из печатных изданий.

3. Творческий подход к повседневным домашним делам: приготовление нового блюда для семейного обеда, оформление книжного уголка и т.д.

4. Прогулки с друзьями, совместный поход в кафе, парк или кинотеатр.

5. Организация тематического семейного вечера, совместное разгадывание кроссвордов, игра в настольные игры.

6. Определение лимита времени пользования компьютером и Интернетом.

7. Реальное общение с друзьями, связь по телефону вместо переписки в социальных сетях.

8. Использование таймера в работе за компьютером позволит лучше контролировать свое время.

9. Запрет на принятие пищи за компьютером.

10. Составление списка причин, по которым необходимо отказаться от чрезмерно частого использования Интернета.

11. Избегание сайтов, вызывающих привыкание.

12. Не стоит включать компьютер без необходимости.

13. Отключить малозначимые, не имеющие важности уведомления, поступающие на электронную почту.

14. Каждый раз, заходя в Интернет, нужно планировать, какие сайты необходимо посетить и сколько времени на это потребуется. С каждым разом стоит уменьшать количество времени пользования Интернетом, пока оно не будет сведено к минимуму.

15. Необходимо регулировать график своего сна. Многие люди, находящиеся в Интернет-зависимости, имеют серьезные проблемы со сном из-за того, что целыми ночами не смыкают глаз перед монитором.

16. Сидя перед компьютером, нужно делать перерывы каждые пятнадцать минут – глаза и мышцы должны отдыхать.

Очень важно признать все возможные опасности для себя. Только тогда можно стать независимым и уверенным в себе человеком, построить отношения с окружающими, наладить личную жизнь, научиться оптимально распределять свое время, действовать, ставить цели и добиваться их, самостоятельно решать проблемы и успешно преодолевать любые жизненные трудности, увидеть возможности для самореализации и узнать, какими практическими способами можно реализовать себя.

Сведения об авторах

Андреев И. Н. – директор студии Интернет-дизайна «Реарт», г. Владимир;

Беляева Е. А. – старший преподаватель кафедры информационного образования государственного автономного образовательного учреждения дополнительного профессионального образования (повышения квалификации) Владимирской области «Владимирский институт повышения квалификации работников образования им. Л. И. Новиковой» (ВИПКРО), г. Владимир;

Булгакова Е. К. – психолог государственного бюджетного учреждения культуры Владимирской области «Владимирская областная библиотека для детей и молодежи», г. Владимир;

Дубов И. Р. – доктор технических наук, профессор кафедры вычислительной техники факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;

Евстифеев Р. В. – доктор политических наук, заведующий кафедрой политологии Владимирского филиала федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Владимир;

Кирюхина И. М. – депутат Законодательного Собрания Владимирской области, председатель комитета Законодательного Собрания по вопросам здравоохранения, демографии, материнства и детства, заслуженный врач РФ, г. Владимир;

Костина Н. В. – магистрант кафедры информатики и защиты информации факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;

Кручинин А. В. – руководитель отдела по защите конфиденциальной информации ООО «ИнфоЦентр», г. Владимир;
Лебедева О. Н. – заместитель директора по автоматизации Государственного бюджетного учреждения культуры Рязанской области «Рязанская областная детская библиотека», г. Рязань;
Маркова М. В. – специалист по маркетингу ОАО «Вымпелком», г. Владимир;
Мачинскене Т. А. – заместитель директора ГКУСО ВО «Владимирский социально-реабилитационный центр для несовершеннолетних», г. Владимир;
Медведникова М. А. – магистрант кафедры информатики и защиты информации факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;
Минина И. А. – старший помощник руководителя следственного управления Следственного комитета Российской Федерации по Владимирской области, полковник юстиции, г. Владимир;
Миронова Е. Ю. – заместитель директора по учебной работе МБОУ «ООШ № 16», г. Гусь-Хрустальный;
Монахов Ю. М. – кандидат технических наук, доцент кафедры информатики и защиты информации факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;
Осипова Н. Ю. – преподаватель ГБОУ СПО ВО «Владимирский политехнический колледж», г. Владимир;
Пантюхова Т. В. – заместитель директора по научно-методической и инновационной деятельности государственного бюджетного учреждения культуры Нижегородской области «Нижегородская государственная областная детская библиотека», г. Нижний Новгород;
Пивоварова М. В. – педагог-организатор «МБОУ СОШ № 44», г. Владимир;

Пономарев В. Е. – аналитик некоммерческого партнерства «Лига безопасного Интернета», г. Москва;
Прозоровская Е. Ю. – преподаватель театральных дисциплин ГБОУ СПО «Владимирский областной колледж культуры и искусства», г. Владимир;
Савосько С. Е. – преподаватель психологии ГБОУ СПО «Владимирский областной колледж культуры и искусства», г. Владимир;
Семенова И. И. – кандидат технических наук, доцент кафедры информатики и защиты информации факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;
Симкин А. С. – технический директор Владимирского филиала ОАО «ВымпелКом», г. Владимир;
Синев П. В. – магистрант кафедры вычислительной техники кафедры вычислительной техники факультета информационных технологий института инновационных технологий государственного бюджетного образовательного учреждения высшего профессионального образования «Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир;
Скурлова И. А. – психолог государственного бюджетного учреждения культуры Владимирской области «Владимирская областная библиотека для детей и молодежи», г. Владимир;
Сморжанюк О. А. – ведущий инженер отдела информационного обеспечения Владимирского филиала федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», г. Владимир;
Сомова С. А. – учитель русского языка и литературы МБОУ «Энтузиастская ООШ», с. Энтузиаст Юрьев-Польского района Владимирской области.

Содержание

Департамент культуры и туризма администрации Владимирской области

Государственное бюджетное учреждение культуры Владимирской области

«Владимирская областная библиотека для детей и молодежи»

ДИАЛОГ ON-LINE

Сборник материалов
II Межрегиональной конференции для детей,
молодежи и специалистов, работающих с детьми
и молодежью по Интернет-безопасности
в рамках государственной программы «Обеспечение
информационной безопасности детей, производства
информационной продукции для детей и оборота информационной
продукции во Владимирской области на 2014-2016 годы»

11 февраля 2014 года

Компьютерная вёрстка И. Гришановой

Подписано в печать 00.00.2014 г.
Формат 60x84/16. Бумага офсетная. Печатных листов 7,25
Тираж 100 экз. Заказ №741.

Отпечатано в типографии «Транзит-ИКС»
г. Владимир, ул. Электрозаводская, 2.