СТАНДАРТЫ ОБРАЗОВАНИЯ

Как защитить ребенка от негативного контента в СМИ и Интернете

ИРО КИРОВСКОЙ ОБЛАСТИ

Кировское областное государственное образовательное автономное
учреждение дополнительного профессионального образования
(повышения квалификации)
«Институт развития образования Кировской области»

Кафедра информационно-технологического
и физико-математического образования

Как защитить ребенка от негативного контента в СМИ и Интернете

Методические рекомендации по проведению общешкольных тематических родительских собраний

Киров

2013

БК

К

Печатается по решению редакционно-издательского совета
ИРО Кировской области

Рецензент:
Г.П. Савиных, к.п.н., проректор по научно-исследовательской работе Института развития образования Кировской области
В.В. Шабардин, Уполномоченный по правам ребенка в Кировской области

Авторы:
Т.С. Пивоварова**,** зав. кафедрой, ***М.В. Кузьмина*****,** преподаватель кафедры информационно-технологического и физико-математического образования ИРО Кировской области

Как защитить ребенка от негативного контента в СМИ и Интернете (методические рекомендации по проведению общешкольных тематических родительских собраний) / Т.С. Пивоварова, М.В. Кузьмина. - Киров: ИРО Кировской области, 2013. - 62 с.

ISBN

Методические рекомендации по проведению общешкольных тематических родительских собраний содержат практические рекомендации для образовательных организаций по вопросам медиабезопасности ребенка в сети интернет и при общении со средствами массовой информации.

Пособие может быть рекомендовано широкому кругу читателей, в числе которых педагоги, учащиеся, родители.

ISBN

Оглавление

Введение

Стремительное развитие информационно-телекоммуникационных технологий, цифровых аудиовизуальных ресурсов, современных средств связи, социальных сервисов и сетей, ставит задачу безопасного использования СМИ и Интернета в самостоятельной образовательной деятельности современных детей и подростков.

Освоение основ компьютерной и информационной безопасности в современном мире входит в базовый уровень личностных и профессиональных компетенций всех участников учебного процесса: от школьника и учителя, до родителей и широкой общественности.

Современные школы находятся в состоянии перехода от привычного стандарта образования к новому, включающему цифровые образовательные аудиовизуальные ресурсы. Именно поэтому, одной из главных задач образовательных организаций является задача сделать этот переход максимально плавным, безболезненным, и в тоже время – продуктивным, чтобы не упустить важные составляющие личностных компетенций, в частности, основ информационной грамотности.

В условиях реализации новых ФГОС, модернизации и совершенствования образовательного процесса для оптимального включения в него разнообразных безопасных информационных ресурсов требуются совместные усилия всего образовательного

сообщества. Важным аспектом данного направления деятельности является работа с родителями по обеспечению личной безопасности детей в информационной образовательной среде.

В соответствии с задачей обеспечении информационной безопасности детства путем реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию, поставленной Национальной стратегией действий в интересах детей на 2013-2017 годы, утвержденной Указом Президента Российской Федерации от 1 июня 2012 года, и решением Общественного совета при Уполномоченном при Президенте Российской Федерации по правам ребенка от 18 сентября 2012 года по инициативе Уполномоченного при Президенте Российской Федерации по правам ребенка с 1 июня 2013 года запланирован запуск Всероссийской информационной кампании против насилия и жестокости в СМИ и других средствах массовой коммуникации.

Кампания направлена против создания и распространения среди детей (в возрасте от 0 до 18 лет) продукции средств массовой информации, печатной продукции, аудиовизуальной продукции на любых видах носителей, программ для ЭВМ и баз данных, а также информации, распространяемой посредством зрелищных мероприятий, размещаемой в информационно-телекоммуникационных сетях (в том числе в сети Интернет), сетях подвижной радиотелефонной связи (СМИ и иные средства массовой

коммуникации), содержащих пропаганду жестокости, насилия, порнографии, педофилии, суицидов и других социальных девиаций, изображение н(или) описание которых способно причинить вред здоровью, физическому, психическому, духовному и нравственному развитию детей.

Кампания включает комплекс информационных, образовательно-просветительских, пропагандистских и организационных мер, направленных на поощрение развития механизмов саморегулирования, родительского и общественного контроля в сфере защиты детей от информации, причиняющей вред их здоровью и развитию, формирование гражданской ответственности всех участников медиасреды и стимулирование добровольного выполнения ими обязанностей по обеспечению информационной безопасности детей, недопущению оборота в доступное для детей время и в доступных для детей общественных местах материалов, содержащих изображения и(или) описания чрезмерного насилия, агрессии и жестокостях, порнографию и другие опасные для детей виды информации, а также созданию, выпуску и обороту информационной продукции, предназначенной для детей, учитывающей их возрастные особенности и потребности в доступе к информации, способствующей их полноценному развинтило и воспитанию.

В связи с этим для реализации Всероссийской информационной кампании против насилия и жестокости в СМП и других средствах

массовой коммуникации в образовательных учреждениях Кировской области планируется проведение цикла родительских собраний.

Данные методические рекомендации отражают вопросы общей безопасности ребенка в информационной образовательной среде, основные характеристики социальных сервисов, источники информационной опасности, способы заражения и проникновения угроз, методики их распознавания, действия по их нейтрализации; меры по ограждению от вредного влияния негативного медийного контента, а также проблемы формирования общей культуры работы детей в информационной образовательной среде и взаимодействия с информационно насыщенном социуме.

Предлагаемые методические рекомендации включают в себя требования к содержанию родительских собраний, вопросы организации, проведения собраний и приложения.

Темы родительских собраний:

Тема 1. «Наши друзья - Интернет и СМИ», раскрывает вопросы, связанные с полезным контентом и сервисами информационно-телекоммуникационных сетей (в том числе в сети Интернет), сетей подвижной радиотелефонной связи (СМИ и иных средства массовой коммуникации);

Тема 2. «Опасности и угрозы в Интернете и СМИ» знакомит с видами негативного влияния сети Интернет и СМИ и тем, как избежать их опасного воздействия на ребенка;

Тема 3. «Безопасное использование компьютерных и мобильных устройств», связана с формированием практических навыков безопасного использования медийного и информационного контента, современных гаджетов и девайсов;

Тема 4. «Ответственное поведение учащихся в глобальном информационном пространстве» ориентирован на формирование культуры медиапотребления обучающихся.

I. Тема «Наши друзья - Интернет и СМИ»

Рассматриваемые вопросы:

1. Ребенок и Интернет: аналитическая справка
2. Полезный контент в сети Интернет
3. Полезные ресурсы средства массовой информации

Цель: повышение осведомленности и информированности родителей об образовательных возможностях использования ресурсов Интернет и СМИ.

Содержание темы:

Вопрос 1. Ребенок и Интернет: аналитическая справка

Аналитическое представление ситуации пользования детьми ресурсами сети Интернет на основе результатов социологических исследований, проводимых Институтом общественного проектирования[1], фондом «Общественное мнение», фондом развития Интернет и др.

Вопрос 2. Полезный контент в сети Интернет.

Полезные сервисы информационно-телекоммуникационных сетей, подвижной радиотелефонной связи: виртуальные библиотеки, развивающие игры, дистанционные образовательные проекты, справочные сайты, энциклопедии, создание собственных интернет-ресурсов, виртуальные экскурсии по музеям мира, по объектам культурного наследия разных стран и др.

[1] Журнал «Дети в информационном обществе» №11, 2012 год

Вопрос 3. Полезные ресурсы средств массовой информации. Образовательные детские телепрограммы. Детские фильмы мультфильмы, направленные на воспитание ребенка. Экранизация литературных произведений. Познавательные телеканалы. Семейные телепередачи [3].

Рекомендации по организации и проведению собрания.

Родительское собрание по данной теме проводится в лекционной форме с обязательными примерами и использованием элементов беседы, дискуссии. Возможные вопросы для обсуждения: В чем польза Интернета для ребенка? Какое положительное влияние могут оказывать телевизионные ресурсы на подростка?

В процессе проведения собрания можно предложить просмотр следующих видеоматериалов:

- Виртуальные экскурсии по музеям мира www.googleartproject.com
- Проект Google «Просмотр улиц» http://maps.google.ru/intl/ru/help/maps/streetview
- Виртуальное путешествие Москва-Владивосток http://www.google.ru/intl/ru/landing/transsib/
- Развивавшие игры www.igra-internet.ru – в ходе игры участники узнают о техническом устройстве Сети, ее разнообразных сервисах, а так же об основных угрозах, которые подстерегают пользователей Интернет.

– Детские интернет телеканалы «Улыбка ребенка» http://smiletv.org, «Радость моя» http://www.radostmoya.ru, «PROБумеранг.tv» http://www.probumerang.tv.

II. Тема «Опасности и угрозы в Интернете и СМИ»

Рассматриваемые вопросы:

1. Источники опасности. Виды компьютерных и информационных угроз.
2. Киберзависимость, ее проявления и последствия

Цель: дать представление об источниках информационных и компьютерных угроз, последствиях воздействия на ребенка информации негативного содержания сети Интернет и СМИ, компьютерных угрозах (компьютерное и мобильное мошенничество, манипулятивное воздействие, буллинг, нравственное и моральное развращение). Ввести понятие киберзависимости и ее разновидностей, способствовать формированию представления о негативном воздействии компьютерной зависимости на пользователей Интернета.

Содержание темы:

Вопрос 1. Источники опасности. Виды компьютерных и информационных угроз.

Опасности и угрозы, существующие в Интернете, СМИ и в мобильной среде. Компьютерное и мобильное мошенничество, хакерство, манипулятивное воздействие, кибербуллинг, нравственное и моральное развращение (расизм, терроризм, сексуальные домогательства) и др. Уголовная и административная ответственность за правонарушения.

Подросток в информационном пространстве, как и в реальной жизни, сталкивается с множеством проблем, в силу чего интернет легко становится еще одним значимым источником стрессов в информационном обществе. Результаты исследований Фонда Развития Интернет в 2009–2012 гг., а также содержательный анализ более 5000 обращений за трехлетний период работы горячей линии помощи «Дети онлайн» позволили выявить основные риски онлайн-среды для детей. Разработанная на этой основе классификация включает четыре типа рисков: контентные, коммуникационные, потребительские и технические. (Приложение 2)

В целом, наиболее часто подростки сталкиваются хотя бы с одним из указанных риском контентного (52 %) и технического (48 %) типа. Мальчики немного чаще, чем девочки, сталкивались с пропагандой наркотиков, табакокурения или алкоголя, вредоносными программами и мошенничеством в интернете, а также с тем, что их личная информация в социальных сетях была использована против них. С возрастом дети все чаще сталкиваются с он-лайн рисками. Если каждый третий ребенок 12–13 лет не встречался ни с одним из перечисленных рисков, то в возрастной группе 16–17-летних только каждый десятый подросток смог избежать столкновения с интернет угрозами [2, 4].

Вопрос 2. Киберзависимость, ее проявления и последствия

Понятие киберзависимости и ее влияние на здоровье. Разновидности киберзависимости (игромания, зависимость от социальных сетей, тотализаторы и всякого вида азартные компьютерные игры, интернет-серфинг и шопинг и др.). Симптомы и причины возникновения компьютерной и мобильной зависимости (Приложение 2). Особенности восприятия детьми медиаинформации, влияние компьютерной зависимости на ребенка (уход из социума, агрессия, нарушение здоровья).

Рекомендации по организации и проведению собраний.

Собрание по данной теме проводятся в лекционной форме с обязательными примерами и использованием элементов беседы, дискуссии. Перед собранием рекомендуется провести анонимное анкетирование на выявление степени зависимости детей от Интернета (Приложение 1).

В процессе проведения собрания можно предложить просмотр следующих видеоматериалов и презентаций:

– «Дети в интернете». Видео разработано компанией МТС совместно с факультетом психологии МГУ им. М. В. Ломоносова и Фондом Развития Интернет для проведения урока по теме «Безопасный и полезный интернет» для учащихся 2-4 классов. Материал спроектирован таким образом, чтобы дать школьникам наиболее полное представление о разных сторонах использования сети Интернет — как положительных, так и отрицательных. Детей не

только знакомят с существующими опасностями, но и обучают действовать правильно в случае возникновения неприятных ситуаций. Продолжительность 13 мин. - http://youtube.com/watch?v=p9d0X28iF3g&feature=related.

- «Ах, Интернет, как много в этом слове» - http://slideshare.net/Kaselita/ss-9094435
- «Киберзависимость». Продолжительность 8 минут http://rutube.ru/tracks/2098462.html?v=22ccf08961713ac881565993ec4d3701. При подборке материала к презентации, возможно использование интернет справочника по детской безопасности в Интернете компании Google - http://google.ru/familysafety.

III.Тема «Безопасное использование компьютерных и мобильных устройств»

Рассматриваемые вопросы:

1. Виджеты и гаджеты, обеспечивающие безопасность ребенка в медиапространстве.
2. Рекомендации родителям о том, как обеспечить безопасность ребенка в Интернет и СМИ.

Цель: познакомить родителей с правилами и приемами создания безопасной медиасреды для ребенка.

Содержание темы:

Вопрос 1. Виджеты и гаджеты, обеспечивающие безопасность ребенка в медиапространстве.

Программы родительского контроля, безопасного поиска, возрастного фильтрадля мобильных приложений. Настройка доступа и конфиденциальности. Персональный брандмауэр. Работа с программами по защите ПК (антивирусные программы, почтовые фильтры, антиспам, антибаннер). Создание резервных копий документов, содержащих важную информацию.

Маркировка телевизионных передач. Программируемый телевизионный пульт для детей.

Вопрос 2. Рекомендации родителям о том, как обеспечить безопасность ребенка в Интернет и СМИ.

Практические рекомендации о том, как помочь юным пользователям оставаться в кибер и медиа пространстве и избежать существующих рисков: как защитить ребенка от нежелательного контента в Интернет (Приложение 3); как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете (Приложение 4), как избежать кибербуллинга (Приложение 5); как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников (Приложение 6); как действовать при обнаружении симптомов интернет-зависимости у ребенка (Приложение 7); как научить ребенка не загружать на компьютер вредоносные программы (Приложение 8). Рекомендации к действию, если ребенок все же столкнулся с какими-либо рисками (Приложение 9). Советы родителям от родителей (Приложение 10).

Рекомендации по организации и проведению занятий:

Собрание по данной теме проводится в лекционной форме, с включением элементов обсуждения приводимых примеров и изложением родителей своей позиции по отношению к данному вопросу. Рекомендуется подготовить для родителей памятки.

В процессе проведения собрания можно предложить просмотр видеоматериалов и презентаций из следующего списка:

– «Советы родителей о безопасности детей в Интернете». Григорий Остер, Тутта Ларсен, Светлана Журова, Григорий Гладков и Ева Христенко делятся своим опытом о том, как научить ребенка

правилам безопасности в Интернете и сделать его опыт в Сети полезным и позитивным. Продолжительность 6 мин. - http://youtu.be/jhjnTT5KmEI.

- «Развлечения и безопасность в Интернете». Образовательное видео от YouTube о том, как избежать опасных ситуаций в Интернете. Продолжительность 1 мин. - http://youtu.be/3Ap1rKr0RCE.
- Социальный ролик «Безопасный интернет - детям!». Ролик является победителем конкурса «Безопасный интернет - детям!», проведенного Mail.ru. Продолжительность 1 мин. - http://youtu.be/789j0eDglZQ.
- «Касперский открывает города». Видео IT-экспедиции «Козьмодемьянск - территория безопасности», Республика Марий Эл. 30 июня - 3 июля 2011. Продолжительность 46 мин. - http://youtu.be/p72EnPJ2FHc.
- «Безопасность в Интернете» - http://slideshare.net/Valentina050560/ss-7248641
- «Безопасность детей в интернете» - http://slideshare.net/BoykoEY/ss-6198850
- «Основы безопасности в интернете» - http://slideshare.net/alinakrigr/ss-6795788

IV. Тема «Ответственное поведение учащихся в глобальном информационном пространстве»

Рассматриваемые вопросы:

1. Формирование культуры медиапотребления обучающихся. Сетевая этика участников образовательного пространства.
2. Авторское право, лицензионная политика, персонализация данных

Цель: способствовать воспитанию ответственного поведения учащихся в глобальном информационном пространстве», формированию сетевой культуры и культуры медиапотребления обучающихся, содействовать формированию у учащихся основ гражданско-правовых знаний при работе с Интернет-ресурсами.

Содержание темы:

Вопрос 1. Формирование культуры медиапотребления обучающихся. Сетевая этика участников образовательного сообщества.

Представление о медиакомпетентности взрослых участников образовательного сообщества и о формировании культуры медиапотребления обучающихся. Понятие сетевого этикета, правила общения по сотовой связи, электронной почте, в чате, телеконференции, на форуме. Использование сокращений и смайликов, проверка грамотности, вежливость при написании сообщений, уважение к чужому мнению, сохранение личного

информационного пространства, реакция на угрозы по электронной почте и в мобильной сети.

Основные законодательные акты, связанные с уголовной и административной ответственностью за Интернет и мобильное хулиганство, хакерство.

Вопрос 2. Авторское право, лицензионная политика, персонализация данных.

Авторское и смежное право. Основные объекты авторского и смежного прав. Имущественные и неимущественные права. Основные законодательные акты, связанные с уголовной и административной ответственностью за нарушение авторских и смежных прав.

Типология компьютерных программных продуктов (свободное, условно-свободное, лицензионное, пиратское и др.); Сравнение качества и возможностей лицензионных и «пиратских» продуктов: компьютерных программ, музыки, фильмов, рисунков (полнота и качество звука, грамотный перевод и звуковой дубляж, полнота цвета). Ответственность за нарушение авторских и смежных прав. Ознакомление с понятием о персональных данных, о личной и публичной информации, о размещении информации в открытом доступе. Организация личного информационного пространства в сети Интернет, с учетом правил информационной безопасности, Грамотное использование чужой и сохранение личного медийного сетевого контента.

Рекомендации по организации и проведению занятий:

При изучение данной темы рекомендуется рассмотреть вопросы о лицензионных и пиратских продуктах, ввести понятия об авторских и смежных правах, сообщить об ответственности за их нарушения, привести соответствующие примеры. Рекомендуется обратить внимание родителей на правила сетевого этикета, познакомить их с ситуациями интернет и мобильного хулиганства, хакерства, а также с уголовной и административной ответственностью за указанные деяния.

При ознакомлении со вторым вопросом можно ввести понятия о персональных данных, личной и публичной информации, о том, какую информацию о себе, своей семье и других людях можно, а какую нежелательно (и почему) размещать в открытом доступе.

Приложение 1

Тест для определения степени зависимости личности от Интернета

1. Чувствуете ли Вы себя озабоченным Интернетом (думаете ли Вы о предыдущих он-лайн сеансах и предвкушаете ли последующие)?
2. Ощущаете ли Вы потребность в увеличении времени, проведенного в Сети?
3. Были ли у Вас безуспешные попытки контролировать, ограничить или прекратить использование Интернета?
4. Чувствуете ли Вы себя усталым, угнетенным или раздраженным при попытках ограничить или прекратить пользование Интернетом?
5. Находитесь ли Вы в он-лайн больше, чем предполагали?
6. Были ли у Вас случаи, когда Вы рисковали получить проблемы в учебе или в личной жизни из-за Интернета?
7. Случалось ли Вам лгать членам семьи, врачам или другим людям, чтобы скрыть время пребывания в Сети?
8. Используете ли Вы Интернет для того, чтобы уйти от проблем или от дурного настроения (например, от чувства беспомощности, виновности, раздраженности или депрессии)?

Респондент считается интернет-зависимым в случае пяти или более положительных ответов на эти вопросы.

Приложение 2

Риски пользователей в Интернете

Контентные риски в Интернете

Контентные риски возникают в процессе использования находящихся в Сети материалов (текстов, картинок, аудио- и видеофайлов, ссылок на различные ресурсы), содержащих противозаконную, неэтичную и вредоносную информацию (насилие, агрессию, эротику или порнографию, ненавистнический контент, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.). Столкнуться с ними можно практически везде: в социальных сетях, блогах, на торрент-сайтах, персональных сайтах, видеохостингах.

Коммуникационные риски в Интернете

Коммуникационные риски возникают в процессе общения и межличностного взаимодействия пользователей в Сети. Например, незаконные контакты (груминг, сексуальные домогательства), знакомства в Сети и последующие встречи с интернет-знакомыми в реальной жизни; наиболее распространен кибербуллинг; каждый четвертый подросток отмечает, что за последний год сталкивался с оскорблениями, унижениями или преследованием в Сети, но в курсе оказывается только один родитель из десяти. С коммуникационными рисками можно столкнуться при общении в чатах, онлайн-

мессенджерах (ICQ, Google talk, Skype), социальных сетях, сайтах знакомств, форумах, блогах.

Потребительские риски в Интернете

Потребительские риски возникают в результате злоупотребления в интернете правами потребителя. Они включают в себя: риск приобретения товара низкого качества, различных подделок, контрафактной и фальсифицированной продукции; потерю денежных средств без приобретения товара или услуги; хищение персональной информации с целью кибермошенничества.

Технические риски в Интернете

Технические риски определяются возможностями реализации угроз повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушения ее конфиденциальности или хищения персональной информации посредством вредоносных программ (вирусы, «черви», «троянские кони», шпионские программы, боты и др.).

Киберзависимость

Важно понимать, что зависимость – это болезнь, при которой человек уже не принадлежит себе полностью. Понимание, поддержка и эмоциональный контакт с зависимым человеком необходимы для того, чтобы помочь ему избавиться от зависимости. Важный принцип профилактики - осознание опасности возникновения зависимости. Основа преодоления зависимости – замещение, выстраивании новой

системы самосознания человека, в которой он учится заново взаимодействовать с окружающим его миром при поддержке и помощи близких людей.

Интернет-зависимость

Термин «зависимость» заимствован из психиатрии для облегчения идентификации проблемы Интернета путем ассоциации ее с характерными социальными и психологическими проблемами. Понятие Интернет зависимости было впервые введено в начале 1990-х для описания патологической, непреодолимой тяги к использованию Интернета. Собственно зависимость - это стремление постоянно переживать некое состояние, за которое человек готов платить как деньгами, так и негативными последствиями.

Наблюдается от 1 до 10 симптомов зависимости, в которые входят чрезмерное время, проводимое в сети, увеличивающееся беспокойство при нахождении в реальном мире, ложь или скрывание количества времени, проведенного в киберпространстве, вялое функционирование в реальном мире. Злоупотребление Интернетом ведет к социальной изоляции, увеличивающейся депрессии, неприятностей в семье, неудачам в учебе и другим проблемам.

По мнению специалистов Центра когнитивной терапии, в последние годы, наряду с зависимостью от алкоголя, сигарет, еды и наркотиков исследователи наблюдают примеры зависимости от видов

деятельности - азартных игр, импульсивной сексуальной активности, клептомании (краж из магазинов), потребности тратить деньги и др.

В августе 1997 список видов «нематериальной» зависимости пополнился: патологическое использование Интернета. Pathological Internet Use, (сокращенно PIU) стало обозначением официально признанного психического расстройства. Многие психотерапевты говорят, что Интернет-зависимость не есть самостоятельное заболевание. Как правило, этот диагноз свидетельствует о других, серьезных проблемах ребенка - депрессия, коммуникационные проблемы и др. Все они, так или иначе являются признаками неспособности справиться со стрессом и формами той или иной дезадаптации в реальной жизни. Генетически заложенный, но нерастраченный запас энергии, человек стремится разделить с анонимным и виртуальным другим.

Проблема патологической зависимости начинается тогда, когда стремление ухода от реальности, связанное с изменением психического состояния, начинает доминировать в сознании, становясь центральной идеей, вторгающейся в жизнь, приводя к отрыву от реальности. Происходит процесс, во время которого человек не только не решает важных для себя проблем (например, бытовых, социальных), но и останавливается в своем личностном развитии. Этому процессу могут способствовать биологические (например, индивидуальный способ реагирования на алкоголь, как на

вещество, резко изменяющее психическое состояние), психологические (личностные особенности, психотравмы), социальные (семейные и внесемейные взаимодействия) факторы. Патологическая зависимость включает в себя не только патологическое действие, но и мысли о состоянии ухода от реальности, о возможности и способе его достижения [1].

«Интернет-зависимость» - это термин, обозначающий большое количество проблем поведения и контроля над влечениями. Основные пять типов зависимости, которые были выделены в процессе исследования, характеризуются следующим образом:

1. Пристрастие к виртуальным знакомствам - избыточность знакомых и друзей в Сети.

2. Навязчивая потребность в Сети - игра в онлайновые азартные игры, постоянные покупки или участия в аукционах.

3. Информационная перегрузка (навязчивый web-серфинг) - бесконечные путешествия по Сети, поиск информации по базам данных и поисковым сайтам.

4. Компьютерная зависимость - навязчивая игра в компьютерные игры (стрелялки – Doom, Quake, Unreal и др., стратегии типа Star Craft, квесты)

5. Влечение к посещению порносайтов.

Важным фактором, благодаря которому эти явления получили широкое распространение, является анонимность личности в Сети, что связано с четырьмя главными расстройствами:

1. Усиление различных отклонений от нормы, ложь, совершение противоправных действий (просмотр и скачивание непристойной или запрещенной информации). Подобное поведение часто начинается как любопытство, а заканчивается как влечение.

2. Виртуальный мир, в котором человек чувствует себя намного комфортней, чем в реальной жизни, что создает угрозу для успешности реальной жизни. В подобных случаях используется персональная психотерапия, цель которой - уменьшение желания «сбежать» из реального мира.

3. Интерактивные компоненты сети облегчают создание киберзависимости, которая негативно влияет на внутрисемейные отношения и стабильность семьи и в первую очередь ведет к отдалению людей в реальной жизни. В этом случае применяется индивидуальная и семейная терапия, в процессе которой все члены семьи совместно работают над примирением в семьи.

4. Возможность создания альтернативных он-лайн персонажей, в зависимости от настроения и желания самого пользователя, что создает возможность уйти от реального мира с его эмоциональными проблемами (например, стресс, депрессия, беспокойство), или же от простых жизненных сложностей (проблемы в учебе, расстройства в

семье). Мгновенное бегство в фантастический мир Интернет служит поддержкой для привыкания, за которым следует ухудшение настроения и психологические разногласия, которые лечатся психотерапией и, в случае необходимости, фармакологическим вмешательством [5].

Влечение к Интернету развивается благодаря трем главным факторам:

- Персональный контроль и анонимность передаваемой информации.
- Внутренние чувства, которые на подсознательном уровне устанавливают больший уровень доверия к общению в он-лайн.
- Доступность непристойной и интерактивной информации.

Что делает Интернет притягательным в качестве средства «ухода» от реальности?

- возможность анонимных социальных действий (особое значение имеет чувство безопасности при осуществлении интеракций, включая использование электронной почты, чатов, ICQ и т.п.)
- возможность реализации представлений с обратной связью (в том числе возможность создавать новые образы «Я»; вербализация представлений и/или фантазий, не возможных для реализации в обычном мире, например, персонажи в играх, ролевые игры в чатах и т.д.)

- широкая возможность поиска нового собеседника, удовлетворяющего практически любым критериям (важно отметить, что нет необходимости удерживать внимание одного собеседника – т.к. в любой момент можно найти нового)
- неограниченный доступ к информации (информационный вампиризм) (опасность стать зависимым от Всемирной Паутины для тех, для кого компьютерные сети оказываются, чуть ли не, а иногда и единственным средством общения)

Психологические симптомы:

- Хорошее самочувствие или эйфория за компьютером.
- Невозможность остановиться.
- Увеличение количества времени, проводимого за компьютером.
- Пренебрежение семьей и друзьями.
- Ощущения пустоты, депрессии, раздражения не за компьютером.
- Ложь учителям или членам семьи о своей деятельности.
- Проблемы с учебой [6].

Физические симптомы:

- Синдром карпального канала (туннельное поражение нервных стволов руки, связанное с длительным перенапряжением мышц).
- Сухость в глазах.
- Головные боли по типу мигрени.
- Боли в спине.

- Нерегулярное питание, пропуск приемов пищи.
- Пренебрежение личной гигиеной.
- Расстройства сна, изменение режима сна.

Согласно исследованиям Кимберли Янг опасными сигналами (предвестниками) являются:

- Навязчивое стремление постоянно проверять электронную почту
- Предвкушение следующего сеанса он-лайн.
- Увеличение времени, проводимого он-лайн.
- Увеличение количества денег, расходуемых он-лайн [6].

Приложение 3

Как защитить ребенка от нежелательного контента в Интернете

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Как помочь ребенку избежать столкновения с нежелательным контентом:

Рекомендации Фонда Развития Интернет

1. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода.
2. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены.
3. Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.
4. Включите программы родительского контроля и безопасного поиска, которые помогут оградить ребенка от нежелательного контента.
5. Постоянно объясняйте ребенку правила безопасности в Сети.

6. Тем не менее помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Рекомендации Центра безопасного Интернета в России

1. Используйте специальные настройки безопасности (инструменты родительского контроля, настройки безопасного поиска и другое).
2. Выработайте «семейные правила» использования Интернета. Ориентируясь на них, ребенок будет знать, как поступать при столкновении с негативным контентом.
3. Будьте в курсе того, что ваш ребенок делает в Интернете. Чаще беседуйте с ребенком о том, что он делает в Сети.

Приложение 4

Как научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете

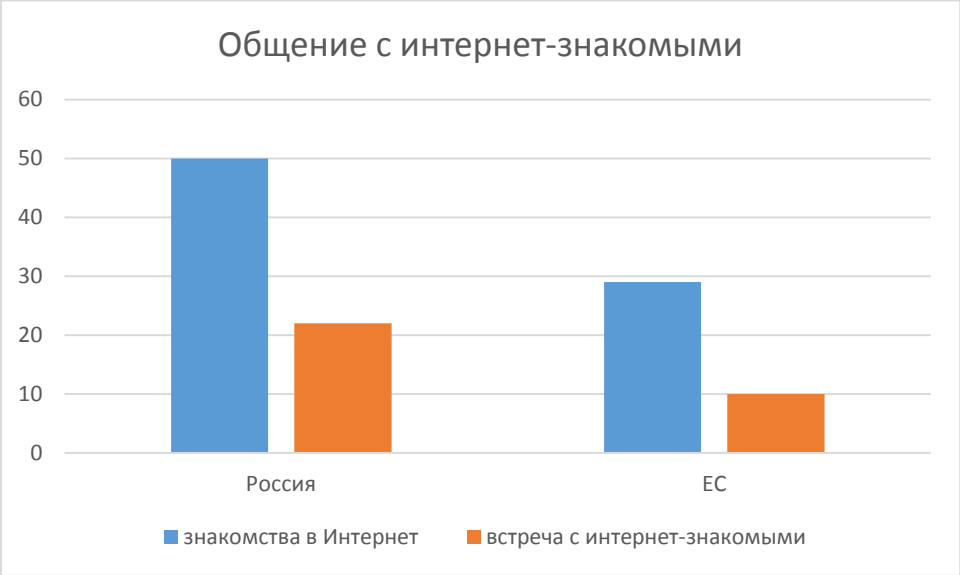
Рекомендации Фонда Развития Интернет

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

По европейским данным, значимость проблемы «встречи с онлайн-незнакомцами» во многих странах Европы существенно снизилась. В России этот вопрос остается одним из самых важных среди коммуникационных Интернет-рисков. Половина российских детей

постоянно знакомятся в Интернете с новыми людьми, а 22% детей признаются, что встречались с интернет-знакомыми в реальной жизни. В Европе знакомятся в Интернете 29% детей, но встречаются с онлайн-знакомыми в реальности меньше – около 10%.



Предупреждение груминга:

1. Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются.
2. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии.
3. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.

4. Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;
5. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Рекомендации Центра безопасного Интернета в России

Объясните ребенку основные правила поведения в Сети:

1. Нельзя делиться с виртуальными знакомыми персональной информацией, а встречаться с ними в реальной жизни следует только под наблюдением родителей.
2. Если интернет-общение становится негативным – такое общение следует прервать и не возобновлять.

Приложение 5

Как избежать кибербуллинга

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

Основной площадкой для кибербуллинга в последнее время являются социальные сети. Особенно остро переживают кибербуллинг дети 9-10 лет.

Рекомендации Фонда Развития Интернет по предупреждению кибербуллинга:

1. Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости так же неприятно, как и слышать.
2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Возможно, стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем.
3. Если ребенок стал жертвой буллинга, помогите ему найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.

4. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз.
5. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Рекомендации Центра безопасного Интернета в России по защитите от кибербуллинга:

1. Не провоцировать. Общаться в Интернете следует этично и корректно. Если кто-то начинает оскорблять ребенка в Интернете – необходимо порекомендовать уйти с такого ресурса и поискать более удобную площадку.
2. Если по электронной почте или другим онлайн-каналам кто-то направляет ребенку угрозы и оскорбления – лучше всего сменить электронные контакты (завести новый email, Skype, ICQ, новый номер мобильного телефона).
3. Если кто-то выложил в Интернете сцену киберунижения ребенка, необходимо сообщить об этом администрации ресурса. Можно также обратиться на горячую линию. Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и тем более не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

1. **Беспокойное поведение.** Даже самый замкнутый школьник будет

переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2. **Неприязнь к Интернету.** Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
3. **Нервозность при получении новых сообщений.** Негативная реакция ребенка на звук письма на электронную почту или на телефон должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Приложение 6

Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников

Кибермошенничество – один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое)

Рекомендации Фонда Развития Интернет по предупреждению кибермошенничества:

1. Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.
2. Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.
3. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые **правила безопасности**:
   - ознакомьтесь с отзывами покупателей*;*
   - проверьте реквизиты и название юридического лица –

владельца магазина*;*

- уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs);
- поинтересуйтесь, выдает ли магазин кассовый чек;
- сравните цены в разных интернет-магазинах;
- позвоните в справочную магазина;
- обратите внимание на правила интернет-магазина;
- выясните, сколько точно вам придется заплатить.

4. Объясните ребенку, что нельзя отправлять слишком много информации о себе при совершении интернет-покупок: данные счетов, пароли, домашние адреса и номера телефонов. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

Приложение 7

Алгоритм действий при обнаружении симптомов интернет-зависимости у ребенка

Рекомендации Фонда Развития Интернет

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

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и так далее.
2. Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и прочее). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в Сети.
3. Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате, – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает ребенок.
4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий, например от бездумного обновления

странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями, при этом общаясь друг с другом вживую. Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.
6. Дети с интернет-зависимостью субъективно ощущают невозможность обходиться без Сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время выпадет из жизни интернет-сообщества.
7. В случае серьезных проблем обратитесь за помощью к специалисту.

Приложение 8

Как научить ребенка не загружать на компьютер вредоносные программы

Рекомендации Фонда Развития Интернет

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

1. Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
3. Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
4. Периодически старайтесь полностью проверять свои домашние

компьютеры.

5. Делайте резервную копию важных данных.
6. Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Приложение 9

Что делать, если ребенок все же столкнулся с какими-либо рисками

Рекомендации Фонда Развития Интернет

1. Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать.
2. Постарайтесь внимательно выслушать рассказ о том, что произошло, понять, насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка.
3. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил ваши или свои деньги в результате интернет-мошенничества и прочее) – постарайтесь его успокоить и вместе с ним разберитесь в ситуации: что привело к данному результату, какие неверные действия совершил сам ребенок, а где вы не рассказали ему о правилах безопасности в Интернете.
4. Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной

жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и тому подобное), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

5. Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств: зайдите на страницы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться (например, для обращения в правоохранительные органы);
6. Если вы не уверены в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете, как поступить в той или иной ситуации – обратитесь к специалисту (телефон доверия, горячая линия и другое), где вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и другие).

Если вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи “Дети

Онлайн” по телефону: 8 800 25 000 15 (звонок по России бесплатный). На линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В. Ломоносова и Фонда Развития Интернет.

Приложение 10

Советы родителям от родителей

1. Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что делают дети в Интернете.
2. Обращайте внимание на то, какие сайты посещает ребенок. Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.
3. Расскажите детям о безопасности в Интернете. Вы не сможете все время следить за тем, что они делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.
4. Используйте настройки конфиденциальности и управления доступом к вашему местоположению. На YouTube, Blogger, в социальных сетях и на многих других сайтах пользователи могут размещать собственный контент. Обычно автору предоставляется возможность ограничить доступ к личному блогу, фотографиям, видео и информации в профиле. Особенно важно ограничивать

доступ к таким данным, как имя, адрес или номер телефона, которые ребенок размещает на общедоступных сайтах.

5. Храните пароли в тайне. Напоминайте детям, что пароли нельзя никому сообщать. Также необходимо, чтобы для детей стало привычкой снимать флажок "Запомнить меня" при входе в свой аккаунт с компьютеров, установленных, например, в школе, интернет-кафе или библиотеке.
6. Не доверяйте незнакомцам. Объясните детям, что не следует назначать личные встречи с людьми, с которыми они познакомились в Интернете, и сообщать им личную информацию, потому что незнакомцы могут выдавать себя за кого-то, кем они на самом деле не являются.
7. Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное программное обеспечение.
8. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.
9. Научите детей ответственному поведению в Интернете. Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по SMS, электронной почте, в чате или размещать в комментариях на его странице в Сети.
10. Оценивайте интернет-контент критически. То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать

надежные источники информации от ненадежных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

Глоссарий

Веб-серфинг

С чего обычно начинается веб-серфинг? Как правило, первое, куда заходит пользователь, это главная страница Яндекс, Mail, Google или других поисковых систем. К сожалению, в результате поиска любой информации ребенок рискует получить совсем не то, что искал, и неизвестно, как это может отразиться на его психике и мировосприятии.

Даже на обычные запросы поисковая система может выдавать совершенно неожиданные результаты. Простой пример. Ребенок хочет найти какие-то игры и вводит в строку поиска запрос «Игровые порталы». Поисковая система выдает ссылки на различные игровые порталы. На первый взгляд, ничего страшного, ответ вполне ожидаемый. Но если перейти по ссылкам, то на каждом втором портале помимо деления на игры «для мальчиков» и «для девочек» есть еще и раздел «для взрослых». Дети любознательны, поэтому вероятность того, что ребенок заинтересуется «взрослыми» играми и зайдет в такой раздел, достаточно велика.

Кроме таких очевидных запросов, дети обязательно будут искать в интернете информацию о том, о чем наверняка много говорят сверстники в школе. А именно — об отличиях девочек и мальчиков, мужского и женского организмов. Нет ничего страшного в желании изучить анатомию и физиологию человека, например, в

энциклопедиях — ребенку свойственно познавать мир. Однако даже в википедии есть статьи, которые не очень подходят для детей. Можно также предположить, что среди ссылок, которые ребенок получит по соответствующему запросу, окажутся и ссылки на порносайты.

Кроме того, злоумышленники с помощью методов «черной» поисковой оптимизации могут специально продвигать опасные ссылки в топ поисковой выдачи. Зачастую такие ссылки не только ведут на сайты сомнительного содержания (как правило, это мошеннические страницы или порноресурсы), но и являются вредоносными. Причем, многие любознательные подростки и сами проявляют интерес к сомнительным сайтам. По статистике, некоторые из них настойчиво пытаются попасть на порносайты и сайты экстремистского содержания.

На данный момент в большинстве популярных поисковых систем есть опция так называемого «Безопасного поиска». Это первый ключевой момент, на который родителям стоит обратить внимание. Включенная опция «Безопасный поиск» или «Семейный фильтр» (у разных поисковых систем эта функция называется по-разному) предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. Многие известные поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. Более подробно о данной опции можно прочитать на порталах самих поисковых систем mail.ru, Bing и Yahoo.

Социальные сети

Дети, как правило, любят социальные сети — там можно общаться, назначать встречи, играть и просматривать видео и фото. Именно их популярность и привлекательна для злоумышленников. Например, могут предложить участвовать в уникальном конкурсе, где можно выиграть путевку в Швейцарию. В данном случае перед нами классический пример мошенничества. Как показывает практика, даже взрослые, получив подобные сообщения, попадаются на удочку. В другом сообщении предлагают познакомиться, а ссылка якобы на личные фото отправителя на самом деле вела на порнографический сайт. Вряд ли кто-либо из родителей порадуется, если их ребенок откликнется на призыв незнакомца встретиться или пройдет по ссылке, чтобы посмотреть его «личные фотографии».

Но проблема заключается и в том, что опасные ссылки могут приходить и от знакомых и друзей. Злоумышленники прилагают немало усилий для того, чтобы заполучить доступ к чужим учетным записям. Логины и пароли воруются на поддельных сайтах, копирующих страницы известных ресурсов. Заманив на такую страницу свою потенциальную жертву (например, с помощью ссылки вроде «интересно — посмотри!»), пользователя под разными предлогами просят ввести свои логин и пароль к социальной сети. Введенные данные попадают к злоумышленникам. В результате они получают доступ к персональной информации пользователя и

используют украденную учетную запись в своих целях — для рассылки вредоносных ссылок, спама и мошеннических сообщений.

Пользоваться социальными сетями сегодня — огромный риск для детей, которые еще не слишком хорошо ориентируются в жизни. И родителям ни в коем случае нельзя забывать об этом.

IM — переписка

У детей и подростков переписка в чат-клиентах по популярности занимает второе место после социальных сетей. Какие в данном случае могут возникать проблемы? Сейчас много так называемого чат-спама, он представляет собой предложение сомнительных услуг и товаров.

Чтобы оградить пользователей от такой рекламы, во многих приложениях и онлайн-чатах существуют специальные функции. В некоторых приложениях есть встроенные инструменты или специальные дополнения и плагины, которые могут блокировать спам в IM-клиентах.

Например, плагин Bot Sentry в pidgin не дает спам-ботам внести адрес пользователя в свои базы. Этот плагин позволяет пользователю задать любой вопрос желающему добавить его в списки контактов. Тот, кто не смог ответить на вопрос, не имеет возможности добавить ваши данные в свой список контактов, а спам-боты обычно на явно «человеческие» вопросы ответить не могут. Аналогичные дополнения есть и для Miranda-IM, и для других клиентов.

Электронная почта

Электронная почта для современных детей — не самый популярный способ общения. Но поскольку почта нужна для регистрации на различных форумах, в социальных сетях, мессенджерах, онлайн-играх и на многих других ресурсах, она используется повсеместно. Для неопытного пользователя почта таит несколько неприятных сюрпризов.

Во-первых, если злоумышленники получат доступ к почтовому ящику, им станут доступны аккаунты пользователя на всех ресурсах, где при регистрации использовался адрес взломанной электронной почты. Еще одна неприятная составляющая современной электронной почты — спам. Ребенок имеет возможность получать весьма небезопасные сообщения.

Переход по ссылкам на сайты «недетского» содержания в спам-сообщениях может не только навредить психике ребенка, но и подвергнуть компьютер риску заражения вредоносными программами. В почте могут встречаться и разнообразные мошеннические письма.

Сегодня многие почтовые сервисы работают над фильтрацией спама и над созданием инструментов для тонкой настройки фильтрации. Например, если ребенок постоянно получает письма от одного адресата и обычный спам-фильтр пропускает их, то можно настроить фильтр таким образом, чтобы он блокировал все сообщения

с определенными параметрами (адрес отправителя, домен, с которого приходит письмо, ключевые слова в теме и в тексте сообщения).

Контентные риски – это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Интернет-Груминг – это тактический подход взрослого человека к несовершеннолетнему, как правило, с сексуальными целями.

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

Кибермошенничество – один из видов киберпреступления, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и другое).

Брандмауэр – это специальная программа или устройство, которое позволяет блокировать попытки хакеров, вирусов и червей получить доступ к вашему компьютеру через Интернет.

Литература:

1. Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. / Цифровая компетентность подростков и родителей. Результаты всероссийского исследования — М.: Фонд Развития Интернет, 2013. — 144 с.
2. Цымбаленко С., Шариков А., Майорова-Щеглова С., Макеев П. / Влияние интернета на российских подростков и юношество в контексте развития российского информационного пространства. Результаты социологического исследования – М.: Общероссийская общественная детская организация «Лига юных журналистов», 2012 г. – 99 с.
3. Цымбаленко С.Б. Акмеологические основания развития подрастающего поколения в системе информационно-коммуникативных взаимодействий. – М.: Международная академия акмеологических наук, 2011. – 204 с.
4. Цымбаленко С.Б. Подросток в информационном мире: практика социального проектирования. – М.: НИИ школьных технологий, 2010. – 256 с.
5. Короленко Ц.П., Дмитриева Н.В. «Социодинамическая психиатрия»
6. Бурова В.А., психотерапевт, по материалам: www.psyline.ru/inzav.htm Egger, Prof. Dr. M. Rauterberg «Internet Behavior and Addiction», 1996
7. Ivan Goldberg, MD Web Publishing 1996-1999
8. Kimberly Young Web Publishing 1996-1999
9. Maressa Hecht Orzack, Ph.D. Web Publishing 1996-1999