Информационно-коммуникационные технологии и безопасность

И.Н. Васильева, НМУ «Национальный институт образования»
О.Г. Сорока, кандидат педагогических наук, доцент БГПУ

В связи с широкомасштабным использованием информационных ресурсов в образовательном процессе на I общего среднего образования особое значение приобретает информационная безопасность детей. Просвещение учащихся в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и в конечном итоге нормальному развитию.

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права. Так в 2009 году было принято Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств N 33-15 «О модельном законе «О защите детей от информации, причиняющей вред их здоровью и развитию». Законодательный акт устанавливает правовые и организационные основы государственной политики и международного сотрудничества государств-участников Содружества Независимых Государств в сфере обеспечения информационной безопасности детей с учетом общепризнанных принципов и норм международного права, в том числе закрепленных в Конвенции ООН о правах ребенка и модельном законе государств-участников СНГ «Об основных гарантиях прав ребенка в государстве» [1].

Международные стандарты в области информационной безопасности детей нашли отражение и в законодательстве Республики Беларусь. Принятый 1 февраля 2010 г. Указ Президента Республики Беларусь № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» [2] устанавливает приоритеты развития национального сегмента глобальной компьютерной сети Интернет, повышения качества и доступности предоставляемой гражданам и юридическим лицам информации о деятельности государственных органов, иных организаций и интернет-услуг.

Постоянное развитие Интернет-технологий и их широкое проникновение в общество ставит перед государством и обществом задачу поддержания эффективного комплекса мер по профилактике, предотвращению и преодолению последствий вредоносных действий в отношении несовершеннолетних, совершаемых с применением Интернета или информационно-коммуникационных технологий. В обеспечении мер по Интернет-безопасности учреждение образования должно играть ключевую роль, так как в современной школе обучение

осуществляется с использованием информационно-коммуникационных технологий.

Именно поэтому школа должна взять на себя главную ответственность за развитие у детей и их родителей медиаграмотности и обучение их навыкам безопасности. Медиаграмотность определяется в международном праве как грамотное использование детьми инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг.

Решение задачи по обеспечению безопасности при использовании компьютера и интернета детьми требует комплексного подхода. Комплексный подход в решении данной проблемы предполагает разработку нормативного правового, технико-технологического, организационно-методического инструментария.

Нормативное правое обеспечение является основой деятельности учреждения образования (УО) по всем направлениям. По нашему мнению в УО должен быть сформирован пакет нормативной правовой документации по вопросам информационной безопасности. К таким документам относятся документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет как педагогических работников, так и школьников, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по Интернет-безопасности, правила безопасного поведения в сети Интернет. В УО приказами должны быть назначены лица, ответственные за контентную фильтрацию, за работу с персональными данными, за организацию работы школьников в сети Интернет и т.д. В организационном плане по обеспечению информационной и медиабезопасности в УО должен выполняться ряд мер технико-технологической направленности:

− установка лицензионного программного обеспечения,

− подключение к системе контентной фильтрации;

− установка и своевременное обновление антивирусных программ,

− установка и настройка программ-фильтров, брандмауэров.

К организационным внутришкольным мероприятиям относятся:

− разработка и реализация правил Интернет-безопасности, с привлечением заинтересованных лиц: директора школы, классных руководителей, преподавателей информатики, учащихся и их родителей, поставщиков услуг интернета, представителей компаний-разработчиков антивирусного программного обеспечения;

− организация работы детей в Интернет по расписанию с ограничением по времени и под наблюдением педагогов,

− регулярная проверка принимаемых мер в области Интернет-безопасности в УО.

Для организации профилактической работы по медиабезопасности с детьми и родителями педагог прежде всего должен сам знать проблемы и опасности,

которые подстерегают пользователя в сети Интернет, и быть готов дать рекомендации по решению данных проблем.

В организационно-методическом аспекте в УО необходимо разработать план мероприятий по профилактике девиантного поведения детей, связанного с использованием компьютера и сети Интернет.

Рекомендуемая тематика для организации профилактической деятельности:

− нежелательная информация в Интернете, как ее избежать,

− проблемы достоверности информации в Интернете, как проверить достоверность информации,

− социальные сети: опасности и правила поведения в социальных сетях,

− кибермошенничества, как их избежать,

− киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации,

− вредоносные программы и методы борьбы с ними,

− полезные ссылки, ресурсы, сервисы в Интернете 1.

Вопросы информационной безопасности в Интернете могут обсуждаться на классных часах, факультативных занятиях, во время уроков информатики, ОБЖ. Это могут быть библиотечные уроки информационной культуры, выставки, викторины, проводимые педагогами-библиотекарями и др.

В учреждениях образования рекомендуется:

создание на сайте учреждения информационного листка или отдельной страницы, посвященной вопросам безопасного Интернета. Например, «Дети в Интернете» или «Безопасность», «Безопасный Интернет»;

создание информационного стенда «Неделя безопасного Интернета»;

выпуск школьной газеты/информационного листка; тема выпуска: «Интернет. Территория безопасности», для всех классов

создание памяток и буклетов для учителей, детей и их родителей;

ежегодное проведение дня (недели) медиабезопасности, уроков по Интернет-безопасности, внеклассных мероприятий и т.п.

Во время мероприятий по медиабезопасности следует ознакомить обучающихся:

− с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;

− с информацией о необходимости критического отношения к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, признаках отличия достоверных сведений от недостоверных, способах нейтрализации вредной и опасной для детей информации, распознавания признаков злоупотребления доверчивостью;

− с правилами общения в социальных сетях (сетевой этикет);

− ознакомить обучающихся с адресами помощи в случае интернет-угрозы.

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

---

[1] На сайте нашего журнала смотрите Web-mix (коллекцию ссылок на информационные ресурсы) на тему «Безопасность детей в сети Интернет»

− противозаконная, неэтичная и вредоносная информация в Интернете: как ее избежать,

− достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту,

− этика сетевого общения,

− личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.

− социальные сети: как общаться в сети и не попасть в сети мошенников и злоумышленников,

− что такое хакерство: этика и основы,

− интернет-зависимость: угрозы, реальность, проблемы, решения,

− Web -серфинг: как не потерять себя и свое время в Интернете,

− как распознать кибермошенничество и не стать жертвой,

− «нигерийские письма»: предложения в письмах и как не попасться на удочку мошенников,

− что такое киберхулиганство: как не стать жертвой и киберхулиганом;

− как защитить свою почту от спама и не стать спамером,

− компьютерные вирусы и методы борьбы с ними,

− киберпреступления в законодательстве Республики Беларусь,

− безопасность в Интернет-магазинах,

− компьютерные игры, как не стать игроманом,

− мобильные угрозы в современном мире,

− как правильно вести себя с киберхулиганами и защититься от нежелательного общения.

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

Предлагаем использовать следующие формы:

Ступень обучения		Форма проведения
I	1-4 классы	урок-путешествие, урок-викторина, урок-соревнование, урок-игра, беседа, флешмоб, Web-квест, конкурс рисунков «Мой безопасный Интернет» и т.д.
II	5-9 классы	урок - пресс-конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча со специалистами медиа-сферы, системными администраторами, разработчиками ПО и т.д.
III	10-11 классы	деловая игра, урок-презентация проектов,

		день медиабезопасности, дискуссия, дебаты, урок-встреча со специалистами медиа-сферы, системными администраторами, разработчиками ПО, организация волонтерского движения в учреждениях образования по вопросам безопасности ребенка в Интернет, театрализованное представление для юных пользователей компьютера и сети Интернет на тему «Компьютер и вирус» и т.д.

На факультативных занятиях по информатике для младших школьников можно использовать онлайн-игры, которые содержат основные понятия об устройстве Интернета, правилах работы в нем, в том числе — о сетевом этикете. Так, например, игра «WildWebWood» (http://www.wildwebwoods.org/) создана на основе справочника Совета Европы «Интернет-грамотность», переведена на русский язык и будет интересна детям младшего и среднего школьного возраста. В нашей стране он-лайн игру о безопасном поведении в сети Интернет предлагает Национальный правовой портал http://mir.pravo.by.

Компания МТС предлагает on-line урок по теме «Полезный и безопасный Интернет» (http://www.detionline.com/mts/about). Всем взрослым (педагогам и родителям) рекомендуем к прочтению информационно-аналитический журнал «Дети в информационном обществе», который был учрежден в рамках Года безопасного интернета в России при поддержке Министерства связи и массовых коммуникаций РФ. Журнал выпускает с 2009 года. На сегодняшний день выпущено 16 номеров журнала, все они находятся в свободном доступе в сети по адресу: http://detionline.com/journal/. Приведем тематику лишь некоторых номеров: «Сетевая агрессия» (№16), «Что они пишут и читают?» (№8), «Один в онлайне» (№7), «С кем они общаются?» (№6), «Во что играем?» (№2), «Дети в информационном обществе» (№1) и др.

Риски сети Интернет

Трехлетний малыш, слушающий сказку в наушниках из плейера, четырехлетний малыш, рисующий не в альбоме, а на планшете, шестилетний ребенок, играющий «в гонки» на компьютере, двенадцатилетний подросток, приглашающий в гости очередного виртуального друга в социальной сети, пятнадцатилетняя девушка, проводящая все свободное время в чатах и интернет-сообществах… Эти картины нынче не удивляют, не так ли? Не удивляют, но вызывают серьезную тревогу и опасения. Предоставляя множество новых возможностей, компьютер и интернет несут в себе и новые риски.

Традиционно риски разделяются на четыре типа: контентные, коммуникационные, электронные и потребительские. Для удобства представим их в виде схемы.

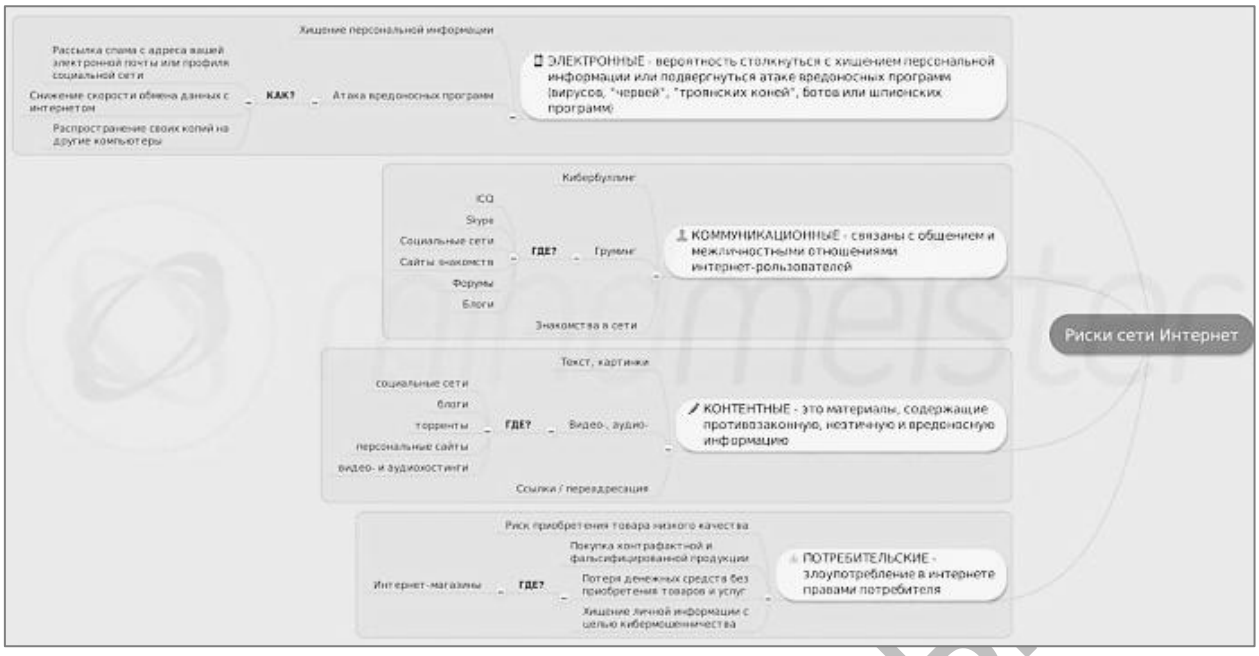

Схема 1. Риски сети Интернет

Подробные рекомендации по предупреждению рисков сети Интернет Вы найдете на страницах пособия «Глобальная сеть: правила пользования / Рекомендации для родителей», подготовленного при поддержке МТС и Фонда развития Интернет [3].

Риски для безопасности и здоровья детей

В аналитическом обзоре «Возможности информационных и коммуникационных технологий в дошкольном образовании», проведенном под эгидой ЮНЕСКО и опубликованном в 2010 году, риски для безопасности и здоровья детей классифицированы так, как показано на рисунке 1 [4].

Рисунок 1. Риски для безопасности и здоровья детей

Для преодоления обозначенных рисков необходимо:

а) организовывать занятия с соблюдением СанПиН норм [5];

б) не рассматривать ИКТ как способ или средство подавления или вытеснения других видов деятельности, а умело интегрировать их в существующую систему учебных занятий;

в) информировать учащихся и их родителей о возможных рисках, связанных с использованием компьютера и сети Интернет;

г) выявлять и использовать наиболее адекватные инструменты ИКТ (оборудования или программного обеспечения);

д) постоянно повышать уровень компьютерной грамотности педагога (в том числе в части современных ИКТ и методики их использования в образовательном процессе).

Родители как партнеры

Учитывая цифровой разрыв между поколениями[2], некоторые родители совершенно оправданно опасаются того, что не смогут помочь своим детям в освоении средств ИКТ, защитить их от потенциальных угроз. Поэтому очень важно вовлечь родителей в обучение их детей средствами ИКТ и снять у них тревожность.

Вовлекать родителей в обучение их детей средствами ИКТ можно следующим образом:

− проводить на регулярной основе семинары для небольших групп родителей, где они могут обсудить то, как их дети работают с ИКТ;

− организовать открытые уроки, чтобы родители «увидели все своими глазами» и понаблюдали за действиями детей;

− организовывать выставки детских работ, выполненных с использованием ИКТ, для того, чтобы продемонстрировать успехи детей и пробудить общий интерес к ИКТ;

− вовлекать родителей в работу с детьми в группе при осуществлении проектной и исследовательской деятельности средствами ИКТ;

− разрешать детям брать персональные устройства домой (в случае организации обучения по модели «1 ученик – 1 компьютер»);

− проводить консультации для родителей относительно цифровых образовательных ресурсов, которые можно использовать (приобрести) специально для пользования дома;

− предложить родителям список рекомендованных ресурсов сети Интернет для использования дома;

− совместно (с детьми и родителями) вырабатывать правила поведения в сети Интернет, создавать памятки и газеты и пр.

Страничка родителя

В каком возрасте следует разрешить детям посещение Интернета?

Возраст аудитории сети Интернет молодеет с каждым годом и это непреложная истина.

---

[2] В **предыдущих статьях мы раскрывали значение терминов «цифровые аборигены» и «цифровые мигранты».**

Дети уже в возрасте семи лет могут пользоваться Интернетом в школе, поэтому, скорее всего, захотят иметь в доступ в Сеть и дома. Однако у тех, кто еще не достиг десятилетнего возраста, обычно нет навыков критического мышления, столь необходимого для самостоятельного посещения Интернета. Поэтому всякий раз, когда дети выходят в Сеть, садитесь рядом и следите за тем, чтобы они посещали только те сайты, которые выбрали вы. Внушите им, что никогда нельзя сообщать в Интернете личные сведения.

Следует ли разрешать детям иметь собственные учетные записи электронной почты?

Предпочтительнее, чтобы дети пользовались общим семейным адресом, а не собственным ящиком. Когда они станут старше и будут настаивать на своей независимости, тогда можно будет завести для них отдельный адрес.

Справочно:

В модели «1 ученик – 1 компьютер» учащиеся начальных классов имели собственный почтовый адрес. Информация обо всех учетных записях и паролях в обязательном порядке хранится у учителя. Без ведома педагога ученик не может поменять пароль от своего почтового ящика.

Родители же в свою очередь могут синхронизировать свой почтовый ящик с ящиком ребенка, чтобы держать под контролем все сообщения, адресованные ребенку.

Какими внутрисемейными правилами следует руководствоваться при использовании Интернета?

Выработайте вместе с детьми соглашение по использованию Интернета. В нем должны быть описаны права и обязанности для каждого члена семьи. А также — четко сформулированы следующие пункты:

Какие сайты можно посещать и что разрешается там делать.

Сколько времени можно проводить в Интернете.

Что делать, если что-нибудь вызывает у ребенка ощущение дискомфорта.

Какие данные нельзя сообщать в сети

Как защитить личные данные.

Как следить за безопасностью.

Как вести себя вежливо и корректно.

Как пользоваться службами чатов, группами новостей и мгновенными сообщениями.

Для эффективности такого соглашения крайне важно участие детей в его составлении. Распечатайте его и держите рядом с компьютером для напоминания всем членам семьи, регулярно просматривайте и вносите изменения по мере того, как дети взрослеют.

Очевидно, что сейчас невозможно гарантировать стопроцентную защиту детей от нежелательного контента. Никакие фильтры никогда такой гарантии не

дадут. Но мы, взрослые, можем и должны формировать у ребят навык «безопасного» поведения в Интернете.

Методы решения этой проблемы представлены на страницах сайта http://www.nachalka.com/ [6]:

1. Родители должны знать, чем заняты их дети. Самое простое – разговаривать с ребенком: чем живет, чем интересуется, какие сайты любит посещать и почему, с кем дружит, в том числе, и в Интернете.

Кроме того необходимо установить на домашнем компьютере «родительский контроль», антивирусные программы, бесплатное программное обеспечение «Интернет Цензор» (www.icensor.ru), NetPolice, KidGid семейный фильтр на поисковой машине.

2. Дети должны владеть основами ОБЖ. Мы учим их не разговаривать с незнакомцами? Мы объясняем, что нельзя называть незнакомцам свой домашний адрес? В сети все то же самое!

3. Учитель должен понимать, зачем он отправляет детей в Интернет. Если учитель сформулировал конкретные задачи урока, реализуемые с помощью Интернет-ресурсов, то варианты обеспечения безопасности могут быть следующими:

закрытые среды обучения, например, учебные блоги/сайты, где могут оставлять комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог/сайт;

постановка конкретной учебной задачи: что надо найти? где? как использовать?

формирование навыков критического мышления;

список проверенных учителем ресурсов, с которых предлагается использовать информацию;

все те же фильтры и контроль системного администратора, если таковой в школе имеется.

Самое главное – приучать детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями сети.

Безусловно, вопросы обеспечения Интернет-безопасности учащихся не исчерпаны материалом данной статьи.

Читайте материалы по данной теме на сайте нашего журнала.

Кроме того, в сентябре 2014 года в Национальном институте образования состоится очно-дистанционный мастер-класс «Безопасность детей в сети Интернет».

Информация о проведении мероприятия будет размещена на сайте http://adu.by

Присоединяйтесь!

Словарик

Кибербуллинг (от английского слова bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или

психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. В сети Интернет – это преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети.

Литература

1. Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств № 33-15 «О модельном законе «О защите детей от информации, причиняющей вред их здоровью и развитию». − [Электронный ресурс]. − Режим доступа: http://www.levonevski.net/pravo/norm2013/num16/d16565.html − Дата доступа: 01.03.2014.

2. Указ Президента Республики Беларусь № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет». [Электронный ресурс]. − Режим доступа: http://www.pravo.by/main.aspx?guid=3871&p2=1/11368. − Дата доступа: 01.03.2014.

3. Глобальная сеть: правила пользования (Как защитить ребенка от столкновения с вредоносной информацией в сети? Как научить его справляться с последствиями таких встреч?) / Рекомендации для родителей [Электронный ресурс]. − Режим доступа: http://goo.gl/UmyiOo − Дата доступа: 05.03.2014.

4. Калаш, И. Возможности информационных и коммуникационных технологий в дошкольном образовании: аналитический обзор [Электронный ресурс]. − Режим доступа: http://ru.iite.unesco.org/news/639068/. − Дата доступа: 05.03.2014.

5. Требования при работе с видеодисплейными терминалами и электронно-вычислительными машинами: СанПиН (утвержден постановлением Министерства здравоохранения Республики Беларусь 28.06.2013 № 59)

6. Безопасность детей в Интернете / М.А. Смирнова. − [Электронный ресурс]. − Режим доступа: http://www.nachalka.com/bezopasnost − Дата доступа: 15.08.2012.

7. Джентельменское соглашение родителей и детей / М.А. Смирнова. − [Электронный ресурс]. − Режим доступа: http://www.nachalka.com/bezopasnost_2. − Дата доступа: 15.08.2012.