

Министерство образования, науки и молодежной политики
Забайкальского края
ГУ ДПО «Институт развития образования Забайкальского края»

**Иновационные решения
в развитии информационной
образовательной среды:
технологии
информационной
безопасности**

СБОРНИК МАТЕРИАЛОВ

**Министерство образования, науки и молодёжной политики
Забайкальского края
Государственное учреждение
дополнительного профессионального образования
«Институт развития образования Забайкальского края»**

**ИННОВАЦИОННЫЕ РЕШЕНИЯ
В РАЗВИТИИ ИНФОРМАЦИОННОЙ
ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ:
ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

**Материалы
II межрегиональной научно-практической интернет-конференции**

**25 марта 2016 г.
Чита**

ИРО Забайкальского края

2016

УДК 371
ББК 74.202.4.
И 66

И 66 Инновационные решения в развитии информационной образовательной среды: технологии информационной безопасности : материалы научно-практической интернет-конференции. – Чита : ИРО Забайкальского края, 2016. – 26 с.

В сборнике публикуются доклады участников II межрегиональной научно-практической Интернет – конференции «Инновационные решения в развитии информационной образовательной среды: технологии информационной безопасности». В ходе работы конференции обсуждались вопросы развития информационной образовательной среды в Забайкальском крае, психолого-педагогического аспекта обеспечения информационной безопасности детей, правового регулирования информационной безопасности в Российской Федерации, защиты персональных данных несовершеннолетних, как одного из аспектов обеспечения безопасности детей, новых технологий в области защиты детей от информации в сети Интернет и других средств массовых коммуникаций, причиняющей вред их здоровью и развитию.

УДК 371
ББК 74.202.4.

Ответственные за выпуск:

Л.И. Казакова, *директор Центра информационных технологий образования и дистанционного обучения, проректор ГУ ДПО «ИРО Забайкальского края»*

Н.А. Прокофьева, *доцент Центра информационных технологий образования и дистанционного обучения, ГУ ДПО «ИРО Забайкальского края»*

© ИРО Забайкальского края, 2016

Содержание

Томских А.А. О РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ ИНФОРМАТИЗАЦИИ.....	5
Дамбаева Б.Б. РАЗВИТИЕ ИНФОРМАЦИОННОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В ЗАБАЙКАЛЬСКОМ КРАЕ.....	7
Синельников Е.Л. ПРАКТИКА ПРОКУРОРСКОГО НАДЗОРА ЗА ИСПОЛНЕНИЕМ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ДЕТЕЙ ОТ НЕГАТИВНОЙ ИНФОРМАЦИИ.....	10
Истомин А.С. КОРПОРАТИВНАЯ СЕТЬ ПЕРЕДАЧИ ДАННЫХ (КСПД) – КАК ЭФФЕКТИВНЫЙ МЕХАНИЗМ РЕАЛИЗАЦИИ ПРИОРИТЕТНЫХ НАПРАВЛЕНИЙ В ОБЛАСТИ ИНФОРМАТИЗАЦИИ ОБРАЗОВАНИЯ В ЗАБАЙКАЛЬСКОМ КРАЕ.....	12
Игнатенко Н.П., Литавина Ю.А. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ КАК ОДИН ИЗ АСПЕКТОВОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЕТЕЙ.....	15
Черепанова Г.В. РЕГИОНАЛЬНЫЙ КОНКУРС ТВОРЧЕСКИХ РАБОТ УЧАЩИХСЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ».....	17
Полякова В.А. СОВЕРШЕНСТВОВАНИЕ КОМПЕТЕНТНОСТИ ПЕДАГОГОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ.....	21
Беляева Е.А. ПЕДАГОГИЧЕСКИЙ АСПЕКТ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ.....	23
Моргачёв Р.А. БЕЗОПАСНЫЙ ИНТЕРНЕТ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ.....	26

*А.А. Томских,
исполняющий обязанности руководителя
министерства образования, науки и молодежной политики
Забайкальского края*

О реализации государственной политики в сфере информатизации

Стремительное развитие информационных технологий заставило современное поколение детей и подростков столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях информационного общества. Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно-телекоммуникационной сетью "Интернет", которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы. Главным образом это происходит в тех случаях, когда родители (законные представители) в семье отстраняются от своих обязанностей по воспитанию и развитию детей и перекладывают их на внешних игроков.

К рубежу 2010-2011 гг. в России был сформирован некий фундамент для развития единой информационной образовательной среды. Этапы создания развития информационной образовательной среды образования регламентируются следующими нормативно-правовыми актами:

Конвенция о правах ребенка;

Конституция Российской Федерации;

Закон Российской Федерации «Об образовании» от 10 июля 1992 г. № 3266-1;

Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ;

Государственная программа Российской Федерации «Информационное общество (2011-2020 гг.)», утвержденная распоряжением Правительства Российской Федерации от 20.10.2010 г. № 1815-р;

Концепция развития единой информационной образовательной среды в Российской Федерации и сопутствующие ей нормативные акты и федеральные проекты (ИСО, ПНПО, ФЦПРО, МРСО, Нацпроект «Образование»), а также принятие федеральных государственных образовательных стандартов, взрывное и стихийное развитие информационных ресурсов и сервисов в образовании, различные проекты и программы информатизации диктуют условия для развития и становления единого информационного образовательного пространства на уровне региона, которое не должно быть обособленным, и должно быть интегрировано в информационную образовательную среду Российской Федерации, и, вместе с тем, должно обеспечивать неприкосновенность частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасно-

сти информации ограниченного доступа; противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия.

Назревшие проблемы - цифровое неравенство обучающихся, в том числе в сельских школах, недостаточное количество преподавателей для сельских школ, бессистемные закупки в организациях, использование несертифицированных ресурсов, бурное развитие Интернета, соц.сетей и активное бессистемное использование ресурсов в образовательных организациях подтолкнуло к решению проблем через формирование единой информационной образовательной среды как на федеральном, так и на региональном уровнях. Каждый регион решает данные задачи на своем уровне, но в общем виде решение выглядит следующим образом – ИОС решает такие задачи, как развитие электронного обучения и электронно-образовательных ресурсов; наличие сертифицированного электронного контента; организация безопасной информационной среды в школах; перевод отчетности в электронный вид; централизованное на уровне региона хранилище данных.

Несомненны преимущества ЕИОС:

- Единство информационного пространства;
- Безопасность и контролируемость информации;
- Возможность выстраивать индивидуальное обучение;
- Контроль над процессом поступления, обучения, приемом экзаменов;
- Быстрое распространение передовых практик;
- Быстрый доступ к истории обучения и любому контенту;
- Моментальное внесение изменения в контент или его дополнение;
- Возможности стратегического планирования, управления, мониторинга и

контроля и многое другое позволяет говорить о том, что ЕИОС полноценно функциональна и удобна для всех участников образовательного процесса. Процесс развития ИОС может и должен продолжаться как на уровне региона, так и быть успешно интегрированным в общероссийское пространство.

При разумном и эффективном сотрудничестве общественных и государственных институтов информационные и коммуникационные технологии могут быть ключевыми элементами политики, способствующими сохранению культуры России, укреплению нравственных и патриотических принципов в общественном сознании, а также развитию системы культурного и гуманитарного просвещения.

Объединение усилий и отработка механизмов взаимодействия семьи, общества и государства должны быть направлены на построение безопасной, этичной и комфортной среды для информационного обмена, коммуникаций, развития и воспитания молодого поколения. Необходимо, чтобы ребенок с детства привыкал свободно ориентироваться в медиапространстве, умел взаимодействовать с разнообразными источниками информации, не поддавался манипуляциям извне и мог делать самостоятельные выводы о качестве информационных продуктов.

Создание безопасной информационной образовательной среды, продолжение работ по внедрению автоматизированных информационных систем управления, стратегического планирования и контроля, совершенствование механиз-

мов блокировки сайтов в сети "Интернет", содержащих запрещенную информацию, обеспечение системной переподготовки учителей в сфере информационной безопасности должно стать приоритетным направлением информатизации образования Забайкальского края.

Б.Б. Дамбаева,
ректор ГУ ДПО «ИРО Забайкальского края»

Развитие информационной образовательной среды в Забайкальском крае

Модернизация российского образования одним из своих приоритетов выделяет информатизацию образования, главной задачей которой, является создание единой информационно-образовательной среды. Для обеспечения конкурентоспособности российского образования, при федеральной поддержке, на основе общих правил и подходов в России создается ЕИОС – безопасная и удобная, интегрированная, снижающая затраты, использующая современные форматы система, обеспечивающая согласованность и синхронизацию с другими государственными информационными системами и базами данных, адаптирующаяся к потребностям и уровню каждого участника.

Назначение ЕИОС – предоставление современных электронных образовательных ресурсов, информационных сервисов, информационных систем и технологий обучения и воспитания, а также создание условий для обновления форм, средств, технологий и методов реализации образовательных программ и услуг, преподавания дисциплин и распространения знаний, расширения доступа к электронному образованию всех уровней с учетом возможности построения современных механизмов обучения и воспитания.

Комплексная информатизация образования направлена на создание и эффективное функционирование в Забайкальском крае единого образовательного информационного пространства. В структуре ГУ ДПО «Институт развития образования Забайкальского края» находится Центр информационных технологий образования и дистанционного обучения (далее ЦИТОиДО), первоочередной задачей которого являются вопросы методической и информационно-технологической поддержки комплексной информатизации образования в Забайкальском крае.

Системно-структурная организация ИОС проявляется в том, что она представляет собой совокупность взаимодействующих систем (подсистем):

- система дистанционного обучения Забайкалья.

Одним из направлений деятельности ИРО является организация, техническое и методическое сопровождение реализации образовательных программ для общеобразовательных школ края с использованием дистанционных образовательных технологий, электронного обучения. Использование дистанционных образовательных технологий, электронного обучения при реализации программ

начального, основного общего, среднего общего образования обусловлено региональными особенностями Забайкальского края – малая плотность населения (2,4 человека на 1 кв. км) и, как следствие, множеством (более 30 процентов) малокомплектных школ. Большая часть школ, работающих в социально сложных условиях, являются сельскими малокомплектными, малочисленными, труднодоступными, приграничными школами. Введение программ с использованием дистанционных образовательных технологий позволяет осуществить полноценное обучение в вышеуказанных школах. Использование ДОТ позволяет учащимся из малокомплектных школ получить доступ к качественному образованию и выстраиванию индивидуального образовательного маршрута учащегося. Система дистанционного обучения Забайкалья, разработанная сотрудниками Центра, включает образовательный контент учебных предметов базового и профильного уровня. Программы электронного обучения реализуются на уровне дошкольного, начального общего, основного общего, среднего общего, среднего профессионального, постдипломного образования. В настоящее время более 3000 учащихся в 221 школе Забайкальского края проходят обучение с использованием дистанционных образовательных технологий. Дистанционные образовательные технологии используются в практике по обучению детей-инвалидов по индивидуальным образовательным программам, включая реализацию дополнительных образовательных программ. На протяжении нескольких лет дистанционно обучаются педагоги Забайкальского края, которые разрабатывают программы дистанционных курсов по предметам, в том числе элективным; образовательные программы дистанционных курсов составлены с учетом уровня изучения – базового, профильного. В банке данных электронных ресурсов находятся и активно используются в работе разработанные педагогами края ресурсы для интерактивных досок (более 500 единиц), интерактивные ресурсы для систем голосования, прочие ресурсы. В своей работе институт активно использует дистанционные образовательные технологии: вебинары, видеоконференции. Ведётся работа с родителями, более 800 человек из которых, проходят обучение по ЭОР.

Для совершенствования базы образовательного контента Министерство образования Забайкальского края на протяжении 2012-2013 гг. осуществляло закупку интерактивных электронных образовательных ресурсов по основным предметам общеобразовательного курса.

- современные средств коммуникации.

В Забайкальском крае с 2013 г. создана и функционирует единая корпоративная защищенная сеть передачи данных (КСПД), объединяющая между собой все общеобразовательные организации с единым центром обработки данных. Еженедельный мониторинг работы Интернет в образовательных организациях края, эффективная работа службы технической поддержки позволила улучшить качество и уменьшить количество сбоев в работе сети. Централизация доступа к сети Интернет позволила оперативно реагировать и устранять факты отсутствия доступа к сети Интернет, увеличить скорость доступа в половине образовательных организаций в условиях снижения финансирования.

- педагогические технологии.

Повышение качества подготовки специалистов является необходимым условием перехода на инновационный путь развития. Организована масштабная подготовка и профессиональная переподготовка педагогических кадров. Педагоги прошли курсы повышения квалификации: для сетевых преподавателей и разработчиков курсов по программе «Реализация курсов ДО средствами LMS MOODLE»; педагогов-кураторов по программе «Сопровождение образовательного процесса с использованием ДО технологий»; руководителей муниципальных ресурсных центров и специалистов, ответственных за внедрение ДО, по программе «Управление развитием системы ДО на муниципальном уровне». За период с 2011 по 2015 гг. подготовлено 47 руководителей МРЦ, 289 сетевых педагогов и 225 тьюторов.

- мониторинговые исследования.

Проведение большого количества мониторинговых исследований на уровне региона, стало возможным за счёт централизации и объединения всех образовательных организаций в единую сеть. В настоящее время специалистами института проводятся мониторинги готовности к введению ФГОС ДОО, ООО, ОБЗ.

- предоставление первоочередных услуг в области образования.

В регионе функционирует несколько автоматизированных информационных систем, сопровождением, методической и технологической поддержкой которых также занимается ИРО. Региональные информационные системы, позволяют предоставлять такой перечень услуг, как информирование об образовательной организации, очередь в ДООУ и запись в образовательную организацию. Информационная система подключена к единому порталу госуслуг и включена в федеральный сегмент электронной очереди. Кроме того, в крае с 2012 г. населению предоставляется такая услуга, как информирование об успеваемости учащихся (электронный журнал и дневник). Внедрение информационных систем в данной области позволило осуществлять прогнозирование по очередности в ДООУ на территории края, отказаться от предоставления документации на бумажных носителях. На настоящий момент ИРО является техническим оператором информационной системы «Контингент», которая позволит сконцентрировать в единой базе данных сведения обо всех обучающихся края на всех ступенях образования.

- информационная безопасность детей.

Одним из актуальных направлений деятельности в рамках развития информационного образовательного пространства края продолжает оставаться обеспечение информационной безопасности обучающихся. С этой целью институтом обеспечивается комплекс услуг по сопровождению информационных сетей, подготовка и повышение квалификации специалистов, реализующих данную функцию в муниципальных образовательных организациях, организационно-методическое и техническое сопровождение. В результате запуска единого регионального узла контентной фильтрации, разработанной и внедренной информационной системы «ИС Экспертиза-СКФ» организованы работы по формированию базы данных образовательных Интернет-ресурсов, проводятся

блокировки запросов, не соответствующих задачам воспитания и образования. На особом контроле находятся поисковые запросы, связанные с суицидом. Модуль «Информационная безопасность» включен в курсы повышения квалификации работников образования всех категорий. Реализация данного модуля позволяет осуществить информирование педагогов в области информационной безопасности, ознакомить с Федеральным Законодательством в данной области. С целью популяризации вопросы информационной безопасности детей в 2015 г. был проведен ряд мероприятий, таких как конкурс «Информационная безопасность» для детей в возрасте от 8 до 18 лет, краевое родительское собрание на тему «Ребенок в современном информационном обществе: образование, безопасность, развитие».

Е.Л. Синельников,
начальник отдела по надзору за исполнением
законов о несовершеннолетних и молодежи
прокуратуры Забайкальского края, г. Чита

Практика прокурорского надзора за исполнением законодательства о защите детей от негативной информации

Органами прокуратуры Забайкальского края проверки исполнения законодательства, обеспечивающих защиту детей от информации, наносящей вред их здоровью, нравственному и духовному развитию, проводятся прокурорами систематически, при этом особое внимание уделяется вопросам распространения запрещенной информации в сети Интернет и проверкам школ края в части обеспечения защиты детей от негативной информации.

По мерам прокурорского реагирования в 2013 г. приведены в соответствие с федеральным и региональным законодательством нормативные правовые акты органов государственной власти края и местного самоуправления в сфере защиты детей от информации, наносящей вред их здоровью. С целью устранения противоречий по нашей инициативе внесены изменения в 3 региональных закона об административных правонарушениях, о защите нравственности и здоровья детей, о порядке формирования и деятельности экспертной комиссии Забайкальского края, Правительством края утвержден перечень мест, в которых ограничивается или не допускается нахождение детей.

Прокурорские проверки показали, что в муниципальных бюджетных образовательных организациях внедрены программы обучения детей и подростков правилам безопасного поведения в Интернет-пространстве, профилактики Интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, а также системы мониторинговых исследований по вопросам обеспечения безопасности образовательной среды образовательных учреждений. И если ранее в ходе проверок школ выявлялись факты свободного доступа к сайтам, где размещались, например, статьи о способах самоубийств, изготовлении

и употреблении наркотических средств, экстремистская литература, то впоследствии Министерством образования, науки и молодежной политики края приняты меры к закупке, монтажу и эксплуатации соответствующих программно-аппаратных комплексов, позволяющих более качественно и эффективно осуществлять контент-фильтрацию.

Проведенные проверки свидетельствуют о распространенности нарушений требований законодательства о классификации аудио и видеопродукции, реализуемой индивидуальными предпринимателями.

К информации, распространение которой среди несовершеннолетних запрещено, относится также и информация о несовершеннолетнем правонарушителе (в данном случае без согласия самого несовершеннолетнего и его законного представителя), либо потерпевшем от преступления против половой неприкосновенности и половой свободы личности. Вместе с тем, в деятельности средств массовой информации нарушения этого запрета выявляются ежегодно.

Например, публикуются сообщения о совершении несовершеннолетними преступлений с указанием населенного пункта их проживания, года рождения и начальной буквы их фамилии, фотографиями домов или школ, где они обучаются, что в совокупности позволяет сделать вывод о конкретных несовершеннолетних. В 2015 г. по возбужденным прокуратурой края делам привлечены к административной ответственности по статьям 13.14 и 13.15 Кодекса Российской Федерации об административных правонарушениях представители 2 средств массовой информации – электронного периодического издания «Забмедиа», Интернет-телеканала «ЗабТВ» и газеты «Вечорка».

Повсеместно распространены нарушения, связанные с демонстрацией кино и видео продукции и проведением зрелищных мероприятий, что обусловлено отсутствием в крае контролирующего органа. Кроме того, одной из проблем при организации и проведении экспертизы информационной продукции является отсутствие на территории края экспертов, аккредитованных в установленном законом порядке.

Прокурором Черновского района г. Читы вблизи школы № 30 выявлен факт размещения рекламы, содержащей информацию порнографического характера. В отношении рекламодателя ООО «Капитал» возбуждено дело об административном правонарушении по части 1 статьи 14.3 Кодекса Российской Федерации об административных правонарушениях, его генеральный директор привлечен к административной ответственности в виде штрафа в сумме 4 тысяч рублей, незаконная реклама демонтирована.

Прокурорами активно используются полномочия по судебному понуждению Интернет-провайдеров ограничить доступ к сайтам, содержащим информацию, наносящую вред здоровью, нравственному и духовному развитию несовершеннолетних. В 2015г. в суды направлено 248 исковых заявлений о признании информации запрещённой к распространению на территории Российской Федерации, в 2016 г. указанная работа продолжена.

А.С. Истомин, инженер-программист Центра информационных технологий образования и дистанционного обучения ГУ ДПО «ИРО Забайкальского края»

Корпоративная сеть передачи данных (КСПД) – как эффективный механизм реализации приоритетных направлений в области информатизации образования в Забайкальском крае

Заказчиком выступило Министерство образования, науки и молодежной политики Забайкальского края, а также, около 600 образовательных организаций, реализующие программы общего образования. Цели проекта.

Цели и задачи проекта:

- Обеспечить бесперебойный доступ образовательных учреждений края к сети Интернет;
- Обеспечить информационное взаимодействие образовательных организаций для реализации совместных образовательных программ, таких как дистанционное обучение;
- Обеспечить возможность более эффективного управления деятельностью организаций, на основе внедрения современных информационных технологий;
- Увеличить скорости каналов передачи данных;
- Организовать работу службы технической поддержки;
- Организовать работу централизованной системы мониторинга работы Интернет в организациях и службы технической поддержки.

Реализация:

- Создание единой сетевой инфраструктуры доступа образовательных учреждений к Корпоративной сети передачи данных (КСПД) Министерства образования с центральным узлом в Центре информационных технологий образования и дистанционного обучения (ЦИТО и ДО) ЗабКИПКРО.

Описание проекта

На начало 2010 г. почти все муниципальные общеобразовательные организации Забайкальского края были подключены к сети Интернет в рамках реализации Приоритетного национального проекта «Образование». Каждая организация самостоятельно заключала договор с провайдером на доступ к сети Интернет, и контролировала качество получаемых услуг связи. В результате:

- отсутствие технических специалистов в организациях;
- постоянные перебои связи и низкое качество связи;
- средняя скорость соединений ниже установленного минимального порога (ниже 128 кбит/сек);
- отсутствие возможности контроля и управления качеством услуг связи;
- высокие расходы на эксплуатацию телекоммуникационной инфраструктуры.

Идея создания корпоративной сети передачи данных системы образования Забайкальского края, которая должна была связать все муниципальные общеобразовательные организации в единое информационное пространство, появилась в 2010 г.

В протоколе №4 заседания Межведомственной рабочей группы по вопросам использования информационно-коммуникационных технологий в образовании и науке, а также подготовки квалифицированных кадров в сфере информационно-коммуникационных технологий от 27 декабря 2010 г., определены основные задачи, которые должны решать проектируемые в субъектах РФ виртуальные образовательные сети (ВОС):

- увеличение скорости обмена информацией и сокращение расходов на внутрорегиональный трафик на существующих каналах связи;
- обеспечение дистанционной технической поддержки и администрирования компьютерных систем общеобразовательных учреждений для снятия нагрузки с учителей на местах;
- сокращение расходов на межрегиональный и международный Интернет-трафик за счет организации регионального центра обработки данных;
- повышение информационной безопасности, в т.ч. за счет организации на стыке ВОС и внешних сетей сетевого экрана и регионального сегмента системы исключения доступа к ресурсам, несовместимым с задачами образования и воспитания;
- получение ресурса для организации других видов коммуникаций, например, IP-телефония или телевидение по запросу.

Согласно распоряжению правительства ЗК № 683-р от 14.12.2010 г. «О предоставлении доступа к сети Интернет муниципальным общеобразовательным учреждениям Забайкальского края за счет средств бюджета Забайкальского края» с 1 января 2011 г. единым государственным заказчиком предоставления услуг доступа к сети Интернет является Министерство образования, науки и молодежной политики Забайкальского края.

На первом этапе создания КСПД все договора на оказание услуг связи образовательным учреждениям объединены в централизованные государственные контракты, что позволило оптимизировать расходы, увеличить скорости соединений и подключить к сети Интернет 37 учреждений, не подключенные в рамках проекта «Образование». Территориальная удаленность населенных пунктов и отсутствие качественных наземных коммуникаций привели к большому количеству задействованных операторов услуг связи:

- Сибирьтелеком;
- Читатехэнерго;
- Сибинтертелеком;
- Мегафон;
- РТКом.РУ;
- Вэб Медиа Сервисез;
- АльтегроСкай.

На первом этапе создания КСПД:

- объединены в единую сеть с центральным узлом в ЦОД ЦИТО и ДО образовательные организации, подключенные по наземным линиям связи: Сибирьтелеком и Читатехэнерго (VPN-подключения);
- создан региональный узел контентной фильтрации;

- организована постоянная работа службы технического сопровождения процессов информатизации.

На втором этапе проекта создания Корпоративной сети передачи данных (2013-2014 гг.) решались следующие задачи:

- дальнейшее увеличение ширины VPN-каналов образовательных организаций;

- заведение в ЦОД ЦИТО и ДО трафика учреждений, подключенных по спутниковым соединениям посредством GRE-туннелей с последующим переводом на выделенные линии;

- подключение к КСПД структурных подразделений и удаленно стоящих корпусов образовательных организаций;

- организация автоматизированной системы мониторинга качества работы Интернет.

Результаты.

В процессе реализации данного проекта создана Корпоративная сеть передачи данных системы образования Забайкальского края с центральным узлом в ЦИТО и ДО ЗабКИПКРО:

- централизованные контракты позволили сократить расходы на организацию и эксплуатацию телекоммуникационной инфраструктуры;

- к сети подключены все муниципальные общеобразовательные организации, а также некоторые структурные подразделения и удаленные корпуса учреждений;

- доступ образовательных организаций к информационным системам КСПД осуществляется по защищенным VPN-каналам; значительно увеличены скорости соединений: средняя скорость наземных соединений - 1,14 Мбит/сек, спутниковых соединений - 340 кбит/сек;

- централизация трафика позволила консолидировать вычислительные ресурсы сети в ЦОД, сократить за счет кеширования трафика расходы на внешний канал Интернет;

- объединение организаций в единую сеть обеспечило безопасный и надежный доступ к корпоративным информационным системам и комплексам: корпоративный информационный портал и почта, хостинг сайтов.

Постоянная работы службы технического сопровождения работы КСПД в совокупности с централизованной системой мониторинга работы Интернет в организациях позволили обеспечить высокий уровень бесперебойной работы сети:

- работа дистанционной службы технической поддержки позволила сократить нагрузку на специалистов в образовательных организациях;

- прямое взаимодействие специалистов службы технического сопровождения с операторами связи существенно сократили время устранения проблем;

- разработанная система мониторинга позволяет не только отслеживать наличие связи в образовательных организациях, но и рассчитывает интеграционный показатель качества работы соединения для оперативного выявления и устранения проблем.

Н.П. Игнатенко,

*начальник отдела по защите прав субъекта персональных данных,
надзора в сфере массовых коммуникаций и информационных технологий
Управления Роскомнадзора по Забайкальскому краю*

Ю.А. Литавина,

*ведущий специалист-эксперт отдела контроля и надзора
в сфере массовых коммуникаций и защиты прав
субъектов персональных данных
Управления Роскомнадзора по Забайкальскому краю*

Защита персональных данных несовершеннолетних как один из аспектов обеспечения безопасности детей

Информационная безопасность детей – одна из острых проблем современного мира. Решением этой проблемы заняты самые разные государственные и общественные институты.

Значительная роль в системе обеспечения информационной безопасности несовершеннолетних отведена Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзору.

В полномочия Роскомнадзора входит контроль и надзор в сфере средств массовой информации, информационных технологий и связи, а также контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Именно Роскомнадзор был инициатором разработки Концепции информационной безопасности детей. В 2013-2014 гг. на организованной Роскомнадзором площадке проходило обсуждение этой Концепции. Она была утверждена Распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р. В систему нормативных правовых актов, обеспечивающих информационную безопасность детей, входит Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

В соответствии с требованиями этого закона создана Единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено". Создание единого реестра осуществляет Роскомнадзор.

Ещё одним важным нормативным актом в рассматриваемой сфере является Федеральный закон от 29.12.2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Роскомнадзор в рамках своих полномочий осуществляет контроль за соблюдением требований законодательства Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, к

производству и выпуску средств массовой информации, вещанию телеканалов, радиоканалов, телепрограмм и радиопрограмм, а также к распространению информации посредством информационно-телекоммуникационных сетей (в том числе информационно-телекоммуникационной сети "Интернет").

Один из аспектов информационной безопасности детей – это защита их персональных данных.

Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

Федеральная служба не только ведет реестр операторов, осуществляющих обработку персональных данных, проводит контрольно-надзорные мероприятия в отношении операторов, осуществляющих обработку персональных данных, но и организует просветительскую работу в области защиты персональных данных.

В целях повышения уровня правовой грамотности подростков, их родителей, педагогов в области защиты персональных данных Роскомнадзор открыл информационно-развлекательный портал <http://персональныеданные.дети/>.

Одна из ключевых идей этого ресурса заключается в том, что защита личной информации может приравниваться к защите реальной личности.

По словам руководителя Роскомнадзора А.А. Жарова, цель создателей проекта – предоставить молодым людям «инструменты и информацию, необходимые для принятия решений в вопросах виртуальной жизни».

На сайте <http://персональныеданные.дети/> можно найти информационные тексты, презентации, а также тесты и интерактивные игры, целью которых является закрепление прочитанного материала.

Знакомясь с персонажами сайта Галей и Васей, Хакером и Агентом, подростки узнают, что такое персональные данные, какие персональные данные относятся к категории специальных и биометрических, как защитить личные данные в Интернете, каковы правила безопасного общения в Сети, как защитить гаджеты от вредоносных программ.

Информационные материалы, размещенные на сайте, могут быть использованы как в рамках школьных уроков по теме персональных данных, так и во внеурочной деятельности.

Только объединив усилия органов государственной власти и школы, родителей и педагогов, мы сможем обеспечить безопасность наших детей как в виртуальном пространстве, так и в реальной жизни.

Г.В. Черепанова,
и.о. заведующей кафедрой методики
преподавания информатики и ИКТ
ЦИТОиДО ГУ ДПО «ИРО Забайкальского края»

Региональный конкурс творческих работ учащихся «Информационная безопасность»

Сегодня часто реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация неизбежно оказывает воздействие на человека, и соответственно она обязательно должна фильтроваться. Если взрослый человек справляется с этой задачей (и то не всегда и не каждый), то ребенок этого делать еще не умеет. А значит, он нуждается в защите своего информационного окружения со стороны взрослых людей. Прежде всего, конечно, со стороны родителей.

Последние 10–15 лет информационное окружение, перетерпело гигантские изменения. Произошло это преимущественно благодаря техническому прогрессу, который зачастую несет с собой не только новые огромные позитивные возможности, но и не менее огромные опасности. А значит, мы обязаны научиться охранять его, справляться с ним эффективно.

Сейчас, когда почти в каждый дом пришли компьютер и безлимитный Интернет, которые принесли огромные возможности их пользователям. Но вместе с возможностями пришли радикальные перемены в информационное окружение ребенка. Ребенок, еще не умея фильтровать поступающую информацию, не имея еще устойчивых социальных моделей, получил доступ к социальным сетям, форумам, чатам, сайтам знакомств, онлайн-играм, информационным сайтам и блогам самого разного качества и содержания. На него буквально хлынул огромный, мощный поток самой разной информации. Он стал с ней взаимодействовать, зачастую один на один. Ситуация значительно ухудшается тем, что очень многие родители с компьютером «на вы» и по умению пользоваться персональным компьютером ребенок зачастую очень быстро обходит своих родителей. Ситуация особенно обострилась в последние годы - с распространением индивидуальных переносных вычислительных устройств, таких как планшетные компьютеры и смартфоны. Таким образом, доступ в Интернет становится переносным и фактически неконтролируемым.

Поэтому проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем».

Между тем существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников. В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию.

Уполномоченным по правам ребенка в Российской Федерации П.А. Астаховым в статье «Информационная безопасность несовершеннолетних: диалог и ответственность государства и гражданского общества» озвучено: «Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать».

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").

Насыщенность современной информационно-образовательной среды деструктивной, вредной для развития детей информацией приобретает катастрофические масштабы. Дети и подростки, в силу возраста не обладают способностью фильтровать качество информации. У них не сформированы критерии различия, они не видят опасностей и не осознают рисков, принимают всю информацию, не понимая, что она может быть противозаконной, неэтичной, недостоверной, вредоносной. Информационное воздействие становится главным рычагом управления людьми. Современные информационно-коммуникативные технологии (ИКТ) меняют не только структуру отношений, но и образ жизни людей, мышление, механизмы функционирования семьи, общественных институтов, органов власти.

Исходя из понимания информационной безопасности детей как защиты ребенка от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия. С целью

повышения компетенции учащихся по вопросам информационной безопасности в Российской Федерации проводится ряд мероприятий: федеральный проект «Единый урок по информационной безопасности», квест по цифровой и медиаграмотности для детей и подростков «Сетевичок», Неделя безопасного Рунета, конкурсы творческих работ детей «Информационная безопасность» и др.

Ежегодно в Забайкальском крае проводится конкурс творческих работ учащихся «Информационная безопасность». Детям предлагается различными способами выразить свое понимание информационной безопасности, понимание рисков и угроз, которые могут встретиться в сети Интернет, безопасности в мобильных, социальных сетях.

Свое представление данной проблемы учащиеся реализуют в различных формах – номинациях конкурса: «Рисунок», «Социальный плакат», «Стихотворение», «Рассказ», «Видеоролик», «Веб-ресурс». Конкурс проводится для учащихся 3-х возрастных категорий (1-5класс, 6-8 класс, 9-11 класс).

Работы в номинациях «Рисунок» и «Социальный плакат» в 2015 году были выполнены в различных техниках изобразительного искусства, отсканированы и представлены на конкурс.

Анализируя работы конкурса 2015 года мы увидели, что в номинации «Рисунок» конкурсанты – учащиеся 1-5 классов, постарались раскрыть свое понимание информационной безопасности, через изображение различных интернет-угроз. Основной идеей представленных на конкурс рисунков стала защита информации от вирусов.

Работы участников номинации «Социальный плакат» показали более широкое понимание проблемы информационной безопасности. Ребята отразили такие проблемы как защита персональных данных, защита от спама, родительский контроль, кибер-буллинг¹.

Номинации «Стихотворение» и «Рассказ» ребята представили свои стихотворения и рассказы. Поразили интересными работами, показывающими как положительные, так и отрицательные стороны сети Интернет, интернет, понимание детей об интернет-зависимости. Основной идеей представленных на конкурс рассказов стала экранная зависимость людей, где компьютер заменил реальную жизнь. Ребята показывают, насколько это не правильно, и дают своим героям шанс изменить свою жизнь.

В номинации «Видеоролик» учащиеся, используя различные подходы, представили работы по тематике конкурса.

Одна из работ конкурса представляла собой учебно-познавательную программу «Учись вместе с нами» где авторы задавали вопросы об интернете, информационной безопасности учащимся своей школы, а также рассказали правила работы в сети Интернет.

В другой работе данной номинации учащиеся показывают положительные и отрицательные стороны сети Интернет, выделяют популярные Интернет-

¹ Киберпреследование (или кибер-буллинг) — это преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов

опасности, наводит на размышление о том, что Интернет это то, что мы выберем для себя - добро или зло.

В работах всех номинаций учащихся прозвучал призыв взрослым защитить детей от ненужной и негативной информации в сети Интернет.

Подготовка конкурсных работ способствует формированию у учащихся умения ориентироваться в современной информационной среде, воспитанию у детей навыков самостоятельного и критического мышления, поддержке творческой деятельности детей в целях их самореализации в информационной среде.

В 2016 году в условия конкурса внесены некоторые изменения: в номинации «Социальный плакат» учащимся предлагается изобразить свое представление информационной безопасности с помощью графического редактора, что способствует повышению медиаграмотности учащихся.

По результатам проведения конкурса в 2015 году можно сделать выводы, что представление учащихся об информационной безопасности не достаточно полно. Не получили отражение в работах конкурса такие вопросы информационной безопасности как: защита личных данных, кибермошенничество, кибербуллинг, интернет- и игровая зависимость, вредоносные программы.

В своих работах участники старались выразить свое понимание проблемы информационной безопасности детей в Интернете. Ребята показали умение осознанного отбора информации, умение ориентироваться в современной информационной среде, умение работать с информационными технологиями. Представленные работы показали насколько разное понятие информационной безопасности учащимися. Мы считаем, что в современное время данный конкурс актуален тем, что через поддержку творческой деятельности учащихся мы формируем у детей не только умение работать с техникой, но и умение ориентироваться в современной информационной среде, воспитываем навыки самостоятельного и критического мышления.

С полным спектром работ конкурса можно познакомиться на сайте <http://blog.zabedu.ru/infbez>

Мы считаем, что в современном информационном обществе необходимо научить ребенка правильно управлять хаотическим потоком информации, критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации; отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной; избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации; распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность; распознавать манипулятивные техники, используемые при подаче рекламной и иной информации; критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях; анализировать степень достоверности информации и подлинность ее источников; применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

В.А. Полякова,
проректор по информатизации
ГАОУ ДПО ВО «Владимирский институт
развития образования имени Л.И. Новиковой»

Совершенствование компетентности педагогов в сфере обеспечения информационной безопасности детей

Обеспечение информационной безопасности детей в обществе глобальной сетевой коммуникации – задача, которой уделяется приоритетное внимание государства и общества. Немаловажная роль в выполнении этой задачи отводится системе образования и ключевой её фигуре – учителю. Педагог может предупредить об опасности в сети, научить средствам защиты детей и их родителей, причем сделать это в увлекательной и доступной форме, уместно и ненавязчиво.

Влияние авторитетного и знающего педагога на ученическую и родительскую аудитории трудно переоценить, однако можем ли мы сказать, что каждый учитель способен сегодня подготовить ребенка к жизни в небезопасном для него информационном мире? Вероятно, не всегда. Опыт общения с педагогами свидетельствует о том, что в силу разных причин (невысокого уровня компьютерной грамотности, отсутствия постоянного доступа к сети Интернет, нехватки времени или желания и пр.) не все педагоги оказываются готовыми к подобной деятельности. Следовательно, педагогов, которые родились и выросли в нецифровом мире, надо готовить к новому и непривычному для них роду деятельности. Оставим за рамками статьи о рассмотрении материально-технических условий подготовки педагога к обеспечению информационной безопасности детей, остановимся на её содержании и формах.

Система развития компетентности педагогов в сфере обеспечения информационной безопасности детей, которая сложилась в региональной системе повышения квалификации педагогических кадров во Владимирской области, включает два основных компонента: **формальный и неформальный**[2]. Причем следует заметить, что удельный вес неформального сектора с развитием непрерывного образования заметно возрастает и, вероятно, будет увеличиваться и в дальнейшем.

Формальный компонент образует обучение педагогов вопросам обеспечения информационной безопасности детей на курсах повышения квалификации. В соответствии с постановлением Губернатора области от 09.12.2013 г. №1372 «Об утверждении государственной программы Владимирской области «Обеспечение информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции во Владимирской области на 2014-2016 гг.»» в образовательные программы повышения квалификации всех категорий педагогов Владимирского института развития образования имени Л.И.Новиковой включены обязательные занятия, на кото-

рых слушатели получают представление об основных информационных угрозах, способах защиты от них, а также методические рекомендации по организации работы с детьми и родителями, перечень дидактических материалов, информационных ресурсов по теме и др.

Разумеется, этого недостаточно в быстро меняющемся информационном мире, и региональная информационно-образовательная среда предлагает педагогам межкурсовые мероприятия, которые образуют **неформальный компонент** системы. Так, в 2013 г. педагоги региона принимали участие в сетевом телекоммуникационном проекте по разработке дистанционного курса для родителей «Родителям об информационной безопасности детей» (<https://sites.google.com/site/roditelidetibezogfsnost/>), который собрал не только достоверную информацию по теме, но и задания, тесты, викторины, которые будут интересны взрослым и детям. 22 доклада педагогов региона и 292 комментария к ним стали итогом сетевой научно-практической Интернет-конференции «Аспекты информатизации образования: информационная безопасность (опыт, проблемы, перспективы)» в 2014-2015 учебном году и по настоящее время находятся в открытом доступе на сайте (<https://sites.google.com/site/saitkonferencii/>). Опыт педагогов в формировании у детей и родителей навыков безопасного использования ИКТ составил основу методических рекомендаций, опубликованных в региональном методическом издании [1].

Методические разработки 22-х учителей Владимирской области к Единому уроку безопасности в сети Интернет, который прошел 30 октября 2014 г., размещены на региональном сайте проектной деятельности «WikiВладимир» с целью распространения успешного опыта обеспечения информационной безопасности детей.

Важнейшей составляющей неформального компонента системы является самообразовательная деятельность педагога. В сети Интернет немало достойных ресурсов, посвященных проблеме защиты детей от негативного информационного воздействия, например, Центр безопасности компании Google или компании Microsoft. В региональном информационном пространстве методическую поддержку самообразования педагогов оказывает интерактивная страница сайта проектной деятельности «WikiВладимир» «Информационная безопасность образовательного учреждения» (<http://wiki.vladimir.i-edu.ru/>), на которой модераторы сайта и активные пользователи делятся актуальной информацией.

Наконец, педагоги могут вовлечь своих детей в совместную деятельность по освоению опыта безопасного общения, обучения и сотрудничества в сети Интернет. Ежегодно с 2013 г. на сайте «WikiВладимир» для школьных команд проводится телекоммуникационный проект «Дети в Интернете», который помогает детям и взрослым сообща решать важные задачи:

- узнать основные виды опасностей, подстерегающих в сети Интернет;
- научиться правильно реагировать на опасности сети Интернет;
- повысить культуру поведения в сети;
- стать активным в решении проблем безопасного использования Интернета;

– пропагандировать безопасное поведение в сети Интернет среди детей и взрослых и др.

Участие в проектах, несомненно, способствует повышению культуры безопасного и ответственного использования сети Интернет детей и взрослых нашего региона.

Таким образом, исходя из своих потребностей и возможностей, педагог может выстроить индивидуальную траекторию развития своей компетентности в сфере обеспечения информационной безопасности детей, выбирая из предлагаемых в рамках формального и неформального компонентов системы повышения квалификации наиболее эффективные и значимые для себя формы.

Литература:

1. Информационная безопасность детей: методические рекомендации для педагогов / под ред. В.А. Поляковой // Научно-методический журнал "Наша новая школа". – Владимир: ГАОУ ДПО ВО ВИРО, 2015. – 76 с. - № 3 (23).

2. Полякова, В.А. Проблемы подготовки педагогов в области применения ИКТ в профессиональной деятельности / В.А. Полякова // Научное обеспечение системы повышения квалификации кадров . – 2015. – № 1 (22). – С. 47-58.

Е.А. Беляева,

старший преподаватель, методист

кафедры информатизации образования

ГАОУ ДПО ВО «Владимирский институт

развития образования имени Л.И. Новиковой»

Педагогический аспект проблемы обеспечения информационной безопасности детей

Аннотация: статья посвящена вопросу информационной безопасности детей. Особое внимание обращается на виды зависимостей и угроз сети Интернет, а также альтернативе противоправному использованию Интернета.

Ключевые понятия и слова: информационная безопасность детей, угрозы сети Интернет, дополненная реальность.

В связи с нарастающим глобальным процессом активного формирования и широкомасштабного использования информационных ресурсов особое значение приобретает информационная безопасность детей. Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

В литературе можно найти множество определений понятия информационной безопасности детей. В федеральном законе "О защите детей от информации, причиняющей вред их здоровью и развитию" информационная безопасность детей трактуется как состояние защищенности детей, при котором отсут-

ствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

С какими же опасностями могут столкнуться дети в Интернете?

Самая распространенная угроза для детей – это откровенные материалы сексуального характера. Многочисленные видеоролики и снимки, которые содержат «жесткую эротику», могут дезориентировать ребенка, ранить его психику. Ребенок может стать жертвой педофилов и порнографов.

Чрезвычайно опасны также электронные ресурсы, содержащие материалы экстремистского и террористического характера, электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами. Лидеры сект стремятся присутствовать в Интернете и рекламировать свою деятельность, предоставляя ложную информацию о себе. Попасть под негативное влияние секты через сайт очень легко: если ребенок читает соответствующий материал, смотрит фото- и видеoinформацию, то он уже вступает во взаимодействие с вербовщиками секты, нередко попадая от них в зависимость.

Представляют несомненную опасность для детей и взрослых компьютерные мошенники, спамеры, фишеры. Дети нередко переходят по ссылкам, которые им присылают злоумышленники, скачивают файлы, содержащие вирусы или незаконную информацию. Недостаточно информированный об опасностях Сети ребенок может сообщить злоумышленнику номер кредитной карты родителей, пароль от электронного кошелька, настоящий адрес и т.п.

Пропаганда наркотиков, насилия и жестокости, суицидального поведения, аборт, самоповреждений может быть весьма опасной для неокрепшей детской психики. Ребенок на веру принимает многие сомнительные идеи, особенно, если они грамотно и привлекательно изложены.

Отношения, которые возникают с виртуальными знакомыми и друзьями, могут казаться безобидными, поскольку Интернет-друг кажется «ненастоящим» и не может, по мнению ребенка, принести ему реального вреда. Однако это далеко не так. Ребенок может завязать знакомство с мошенниками и хулиганами, может столкнуться с виртуальным хамством и розыгрышами, которые часто заканчиваются такими негативными последствиями как:

- кибербуллинг (подростковый виртуальный террор)– нападения с целью нанесения вреда, которые осуществляются через электронную почту, в чатах, социальных сетях. Наиболее опасным видом кибербуллинга является киберпреследование– скрытое выслеживание жертвы с целью организации нападения, избиения;

- хеппислепинг – видеоролики с записями реальных сцен насилия;

- буллицид – доведение ребенка до самоубийства путем психологического насилия.

Другой опасностью, которая подстерегает детей, имеющих доступ к компьютеру и Сети, может стать Интернет-зависимость. К основным типам Интернет-зависимости относятся:

- навязчивый веб-серфинг – бесконечные путешествия по сети Интернет;

- пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, форумах, избыточность знакомых и друзей в Сети;
- кибераддикция – зависимость от компьютерных игр;
- навязчивая финансовая потребность – игра в Сети в азартные игры, ненужные покупки в интернет-магазинах и постоянное участие в Интернет-аукционах;
- пристрастие к просмотру фильмов через Интернет;
- киберсексуальная зависимость – влечение к посещению порносайтов и др.

Как мы видим, рисков и угроз для детей в Сети огромное количество, поэтому необходимо контролировать их действия в Сети. Но как? Ведь пик пользования Интернетом среди детей приходится на то время, когда родители отсутствуют дома и, соответственно, не могут контролировать, какие сайты посещают дети, с какой информацией они знакомятся.

В этом случае возможно использование различных программ родительского контроля, таких, как KinderGate- родительский контроль, Интернет Цензор, КиберМама, NetKids, KidsControl, Один дома, NetPoliceChild, детский браузер Гоголь и др.

Очевидно, что необходимо как можно раньше знакомить детей с правилами безопасного поведения в Интернете, напоминать им, чтобы они не выкладывали личную информацию о себе и близких в Сети, не делились своими планами с виртуальными друзьями. Наша задача – не запретить детям пользоваться Интернетом, а научить их использовать его грамотно и безопасно.

Альтернативой противоправному использованию Интернета может стать использование средств ИКТ в образовательных и культурно-познавательных целях, например:

- виртуальные экскурсии и 3d путешествия;
- дополненная реальность;
- участие в сетевых проектах и конкурсах и др.

Виртуальная экскурсия открывает множество возможностей для получения образования. Учащиеся могут побывать в самых отдаленных уголках планеты, отправиться в виртуальный тур по любому знаменитому музею. Пусть виртуальный тур и отличается от обычного, но в любом случае он намного «реальнее», чем скучные тексты и картинки.

Дополненной реальностью (AR – augmentedreality) называют симбиоз реального мира и виртуальной, компьютерной реальности. Чаще всего дополненная реальность – это визуальное дополнение реального мира путем проецирования и наведения каких-либо виртуальных, мнимых объектов на настоящее пространство (на экране компьютера, телефона и подобных устройств).

Суть дополненной реальности в том, что она стирает границу между материальными предметами и компьютерной информацией. Любой материальный предмет в ней можно сделать гиперссылкой, а сам мир в этом случае превращается в гигантский пользовательский интерфейс. Применение данной технологии зависит от задач, которые ставит группа разработчиков. Приложения, отоб-

ражающие в дополненной реальности слой информации, привязанной к географическим координатам, называют AR-браузерами.

Накопленный с 2009 г. кафедрой информатизации образования Владимирского института развития образования имени Л.И. Новиковой опыт проведения межрегиональных сетевых конкурсов и проектов для всех участников образовательного процесса показывает эффективность методической поддержки педагогам, специалистам, руководителям ОО, ДОО и родителям в сфере обеспечения информационной безопасности детей в неформальном образовательном пространстве регионального сайта проектной деятельности «WikiВладимир». В процессе проектной деятельности на учебно-практических занятиях в системе повышения квалификации осуществляется обсуждение актуальных изменений и последних тенденций в нормативном и правовом регулировании информационной безопасности в Российской Федерации, ознакомление с новейшими методами, технологиями и разработками в области защиты информации школьного сектора.

Литература:

1. Анализ содержания и структуры информационного потребления современных российских детей и подростков по возрастным категориям 0–6 лет, 6–12 лет, 12–16 лет, 16–18 лет // Концепция информационной безопасности детей. – Режим доступа: http://rkn.gov.ru/docs/Razdel_1.pdf (дата обращения: 20.01.2016 г.)
2. Гафнер, В.В. Информационная безопасность: учебное пособие / В.В. Гафнер // ГОУ ВПО «Уральский государственный педагогический университет». – Екатеринбург, 2009. – Ч. 1, 2.
3. Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации». – Режим доступа: <http://base.garant.ru/70207766/> (дата обращения: 28.01.2016 г.)
4. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008. – 544с.
5. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

Р.А. Моргачёв,

заместитель директора по ИКТ

МОУ СОШ № 240, г. Борзя

Безопасный интернет в образовательном учреждении

Информационное наполнение любого сайта может быть представлено в абсолютно разных формах: текст, мультимедийные файлы, флэш анимации и т.д.

В настоящее время для создания сайта не требуется большого количества времени. А размещаемая информация на сайте может относиться к опасному контенту.

От информации, которую школьник может увидеть, прочитать, или прослушать в глобальной сети Интернет, будет зависеть, поможет ли она ребенку в

процессе обучения, или напротив, повлияет отрицательно. В лучшем случае, ребенок просто не воспримет возникшую перед глазами негативную информацию. Чаще всего опасный контент влияет на душевное состояние ребенка, наносит психологическую травму, влияет на восприятие окружающего мира, пробуждает в ребенке агрессию и злость.

Опасный контент может включать в себя:

1. элементы порнографии;
2. сцены насилия и жестокости;
3. информацию о религиозных сектах и оккультизме;
4. информацию о наркотиках и алкоголе;
5. экстремистские материалы;
6. вредоносные программы.

В наше время информационные технологии активно используются в образовательных учреждениях для проведения уроков, онлайн-мероприятий.

Таким образом, повышается риск просмотра и использования опасного контента. Что можно использовать для предотвращения просмотра и использования опасного контента в образовательном учреждении?

Основные решения, направленные на закрытие просмотра и использования опасного контента:

1. Использование программного обеспечения для контентной фильтрации.

Существует платное и бесплатное программное обеспечение для контентной фильтрации. Недостатки использования данного программного обеспечения заключается в сбоях.

2. Настройка сетевого оборудования с заменой DNS-серверов.

В отличие от программного обеспечения замена DNS-серверов позволяет устранить недостаток сбоя программного обеспечения, снизить время на установку и настройку. Стандартно компьютер получает адреса DNS-серверов провайдера, общедоступные, которые подлежат частичной фильтрации или фильтрация отсутствует полностью.

Несколько компаний открыли публичный бесплатный доступ к своим DNS-серверам, в которых используются "детские" фильтры.

Яндекс предоставляет DNS – сервера 3-х режимов: базовый, безопасный, семейный.

Базовый 77.88.8.8 / 77.88.8.1

Безопасный 77.88.8.88 / 77.88.8.2

Семейный 77.88.8.7 / 77.88.8.3

SkyDNS- один из первых отечественных сервисов. Есть платные и бесплатные тарифы. Имеется возможность ручного составления черных и белых списков, блокировка сайтов по категориям, блокировка рекламы, статистика. На бесплатном тарифе урезаны возможности ручной блокировки, статистика только за месяц и т.д. Без регистрации сервис фильтрует только фишинговые и вредоносные сайты. Есть возможности родительского контроля путем фильтрации опасных сайтов и замены поисковых систем на безопасный поиск от SkyDNS. Управление аккаунтом на сайте осуществляется через приложение, устанавливаемое на компьютер под управлением Windows.

Адрес DNS SkyDNS: 193.58.251.251

Так же есть безопасные DNS-сервера Google, Norton, COMODO, Лига Безопасного Интернета.

Многие изготовители сетевого оборудования (например, Zyxel) в настройках добавляют опции родительского контроля для выбора фильтрации, а также использование безопасных DNS-серверов.

3. Установка родительского контроля и настройка файервола в антивирусной программе.

Большинство антивирусных программ платного и бесплатного распространения имеют встроенные функции файервола и родительского контроля.

4. Настройка браузера.

Существует большое количество бесплатных расширений и дополнений, которые направлены на расширение функционала браузеров для удобной работы в Интернете (например, для GoogleChrom – AdultBlocker).

Большое количество таких расширений предоставляется бесплатно.

У каждого перечисленного решения есть свои плюсы и свои недостатки. Наиболее эффективное решение, направленное на закрытие просмотра и использования опасного контента, это использование комбинированного метода из предоставленных решений.

Заключение.

Благодаря правильной организации контентной фильтрации в школе учащиеся будут защищены от опасного контента. Но не стоит забывать, что сейчас практически в каждом доме имеется компьютер, и порой самый безобидный поиск в Интернете может хранить в себе опасность.

Литература:

1. Официальный сайт SkyDNS. – Режим доступа: <http://www.skydns.ru>
2. Яндекс. DNS. – Режим доступа: <https://dns.yandex.ru>
3. Лига Безопасного Интернета. - Режим доступа: <http://www.ligainternet.ru>
4. Антивирусная защита. - Режим доступа: <http://www.comss.ru>