Оглавление

Введение

Актуальность исследования обусловлена радикальными переменами в социальной, политической и экономической жизни общества под влиянием информатизации. В настоящее время наблюдается процесс перехода общества к качественно новому состоянию, названными учёными информационным обществом.

Информация и информационная деятельность призваны играть ключевую роль в данном обществе. Переход к информационному обществу чаще всего идентифицируют по смене доминирующих технологий. Однако сами технологии не всегда оказывают непосредственное воздействие на социальную сферу, включая образование. Более важными оказываются изменения, инициируемые ими в обществе и влияющие на сферу образования.

Образование в Информационном обществе перестаёт быть способом усвоения готовых и общепринятых знаний, оно становится способом информационного обмена человека, а в нашем случае и ребёнка, с окружающими людьми, который предполагает также генерирование информации в обмен на полученную.

Различие между знанием и информацией, относительность знаний вследствие их быстрого устаревания, превращение образования в непрерывное – все эти процессы ведут к вытеснению знаний информацией в качестве основного элемента образовательного процесса, превращению знания в информацию о мире. В связи с этим, одной из основных задач образования становится обучение работе с информацией.

На этапах компьютеризации школы возможное влияние компьютера на систему образования были раскрыты в работах А.Г. Гейна, А.П. Ершова, В.Н. Каптелина, А.А. Кузнецова, А.Л. Семёнова и др. В последние годы потенциал самого компьютера оказывает на систему образования намного меньшее влияние, чем, например, «примитивные модели поведения»,

которые насаждаются в компьютерных играх и выхолощенный рекламный стиль сообщений «экранной культуры» сети Интернет. Интернетизация массированно воздействует на психику, модификацию поведения. С другой стороны, Интернет имеет возможность занять определённое место в системе образования, выступая фактором повышения её эффективности и модернизации.

Актуальность безопасности школьника в информационной сфере определяется, с одной стороны, действием объективно возникающих в современном обществе и образовании ситуаций цивилизованных изменений, влияющих на становление и развитие личности подрастающего человека как субъекта социального поведения.

С другой стороны, наличием проблемной ситуации в связи с необходимостью изменения приоритетов в науке, образовании, общественном сознании и социальной практике и перехода от традиции значимости безопасности общества к значимости безопасности человека. В частности, в системе образования данная проблема определяется противоречием между существующей необходимостью обеспечения информационной безопасности учащихся, использующих Интернет в образовательном процессе, и отсутствием механизма ее реализации в образовательном пространстве школы. Проблемность ситуации состоит в отсутствии единой научно разработанной теории информационной безопасности, несоответствии потенциальных возможностей информатизации образования и получаемыми в настоящее время результатами. Отсутствие законодательных и нормативно-правовых документов, определяющих уровень нравственности данных, циркулирующих в информационных электронных сетях, обостряет проблему воспитания подрастающего поколения, использующего ресурсы Глобальной Сети.

В частности, в системе образования данная проблема определяется противоречием между существующей необходимостью обеспечения. Закон

Российской Федерации «О безопасности» (1992 г.), Конституция Российской Федерации (1993 г.) (ст. 2 и 7), Закон Российской Федерации «Об информации, информатизации и защите информации» (1995 г.), Концепция национальной безопасности Российской Федерации (2000 г.), Доктрина информационной безопасности Российской Федерации (2000 г.) создают правовую основу безопасности человека.

Базовым концептуальным документом, определяющим политику государства в этой области, является Доктрина информационной безопасности Российской Федерации, в которой обозначены интересы личности и общества в целом. В качестве интересов личности, определяющих состояние ее безопасности, выделены реализация конституционных прав и свобод, обеспечение личной безопасности, повышение качества и уровня жизни, духовное, интеллектуальное и свободное развитие человека и гражданина.

Уголовный кодекс Российской Федерации (1996 г.) не предусматривает меры борьбы с сайтами, регистрирующими и опрашивающими несовершеннолетних без согласия их родителей, а также содержащими информацию, которая может отрицательно влиять на психику, поведение и духовное здоровье подрастающего поколения. В связи с этим, существует необходимость совершенствования законодательства в области информации для обеспечения защиты несовершеннолетних от компьютерных преступлений, от нежелательной по содержанию информации, а также ограничения самими Интернет - ресурсами доступа к такого рода информации детей.

В настоящее время общество находится на пороге смены образовательной парадигмы - переход от образования в условиях ограниченного доступа к информации к образованию в условиях неограниченного доступа к информации. Необходимость ее смены означает осознание несоответствия ранее сложившихся и ставших традиционными представлений нынешней педагогической практике (по Г. Л. Ильину). В

связи с переходом к Информационному обществу и внедрением Инновационных компьютерных технологий в образовательный процесс, с изменением целей обучения, его направленностью на развитие творческой активности школьников возрастает роль самостоятельной деятельности учащихся с использованием ресурсов Интернета. Современное состояние информационного пространства Сети можно определить как источник трансформации воздействия информационной среды в угрозы информационной безопасности школьников. Данный фактор не позволяет однозначно рассматривать Интернет как благоприятную образовательную среду. К факторам информационной среды, которые могут стать опасностями информационной безопасности школьников, следует отнести следующие:

1. Доступность, неподконтрольность, неограниченный объем поступления циркулирующей информации к школьникам.

2. Наличие в информационной среде модифицированных физических носителей информации, воздействующих на физиологические системы ребёнка.

3. Наличие в информационных потоках специфических элементов, целенаправленно изменяющих психофизиологическое состояние детей и подростков;

4. Наличие в информационной среде информации манипулятивного характера, дезориентирующих школьников, ограничивающих их возможности в условиях слабой правовой образованности и в силу возрастных особенностей несовершеннолетних.

Таким образом, актуализация качественно новых угроз безопасности учащихся, затрагивающих сущность информационной связи общества и человека, а также отсутствие педагогических условий обеспечения информационной безопасности школьника в системе образования свидетельствует об актуальности данной работы.

Цель исследования: разработка механизма обеспечения информационной безопасности учащихся, использующих Интернет в образовании.

Объект исследования: информационная безопасность школьников как целостное социально-педагогическое явление.

Предмет исследования: педагогические условия обеспечения информационной безопасности школьника в образовательном учреждении, создание условий и мотивации для противостояния спам – Интернету.

Гипотеза исследования: состоит в том, что информационная безопасность школьника в образовательном учреждении может быть достигнута при успешной реализации педагогических условий, обусловленных с целеполаганием и ценностями информационно-образовательной среды; реализацией воспитательной функции образования на основе приобщения учащихся к информации культурного, этического, гуманистического характера; обеспечением мотивированного включения подростков в разнообразные виды деятельности в информационной сфере; реализацией практической направленности отбора содержания образовательных ресурсов Интернета и применения интерактивной технологии фильтрации поступающей информации.

Цель и гипотеза определили постановку **задач** работы:

- проведение теоретического анализа, педагогической, социологической, методической литературы по проблемам развития личности и ее социализации в эпоху Интернета;

- изучение отечественного и зарубежного опыта обеспечения информационной безопасности школьника и выявление сходства и отличия;

- изучение готовности современного учителя к использованию образовательных ресурсов Интернета;

- - анализ и обобщение полученных результатов экспериментальной работы, определение педагогических условий обеспечения информационной безопасности учащихся, использующих Интернет в образовании.

Для осуществления поставленной цели используются следующие **методы исследования:**

теоретические – изучение научной литературы по вопросу информационной безопасности школьников, анализ специальной литературы;

эмпирические – анализ процесса обеспечения информационной безопасности школьника, изложенная в работах современных педагогов и ученых.

Теоретическая база исследования – работы следующих ученых в области информационной безопасности школьников Л.П. Владимировой, Т.А. Малых, Е.С. Полат, Н.И. Саттаровой и др.

Теоретическая значимость в обобщении материала по вопросам информационной безопасности школьников.

Практическая значимость заключается в разработке конкретных рекомендаций по обеспечению информационной безопасности школьника в учебном процессе и дома.

Структура выпускной квалификационной работы - введение, три главы, заключение и список литературы.

Глава 1. Теоретические основы информационной безопасности школьника в учебном процессе

1.1 Основные аспекты информационной безопасности в школе

Информационная безопасность в школе – составное понятие, включающее технические, этические и правовые аспекты. Сейчас учителя-предметники встают на один уровень с учителем информатики. Информатика становится интегрированной в другие предметы, развивается метод учебных проектов. Многие истины школьники узнают не через теоретические статьи учебника, а на практике, оформляя свои исследования, осуществляя поиск и структурирование информации[6].

Воплощение в жизнь национального проекта по подключению всех общеобразовательных учреждений Российской Федерации к сети Интернет позволило учителям и школьникам получить огромные возможности приобретения новых, актуальных знаний, доступа к разнообразным медиахранилищам, библиотекам, виртуальным галереям и многому другому, необходимому для дальнейшего полноценного существования в информационном обществе. Уже сейчас на просторах мировой сети создается множество электронных образовательных ресурсов по различным областям знаний, специализированных порталов, где можно получить консультацию по любому интересующему вопросу [1].

Школы оснащаются компьютерной техникой, информационно-коммуникационные технологии (ИКТ) широко применяются в сферах образовательной деятельности, Наряду с очевидными положительными тенденциями по реализации национального проекта «Образование» возникает ряд и негативных аспектов . Современный этап жизни российского общества, связанный с Глобализацией информационного пространства, создает новые проблемы для развития личности.

В социальном пространстве информация распространяется быстро, благодаря техническим возможностям. Сама информация часто носит противоречивый, агрессивный и негативный характер и влияет на социально - нравственные ориентиры общественной жизни. Деформация и деструктивные изменения духовной сферы общества в форме искаженных нравственных норм и критериев, неадекватных социальных стереотипов и установок, ложных ориентаций и ценностей, влияют на состояние и процессы во всех основных сферах общественной жизни. В связи с этим, возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Современный школьник, включенный в процесс познания, оказывается незащищенным от потоков информации[4].

Пропаганда жестокости средствами СМИ, возрастающая роль Интернета, отсутствие цензуры является не только социальной, но и педагогической проблемой, т.к. напрямую зависит от уровня и качества образованности подрастающего поколения, степени зрелости личности и готовности ее к самореализации в обществе. Поэтому возникает острая необходимость расширения содержания общего среднего образования, введения в него новых компонентов, связанных с обучением школьников информационной безопасности. Сегодня проблема обучения информационной безопасности школьников в Информационно-компьютерно технологичной–насыщенной среде становится все более актуальной.

Особая роль в решении данной задачи отводится учителям, преподавателям информатики, специалистам в области компьютерных технологий. На сегодняшний день требуются такие преподаватели, которые не только владеют методикой преподавания информатики и имеют высокий уровень знаний в области информационных технологий, но и в совершенстве владеют программно - техническими мерами защиты информации, хорошо осведомлены о проблемах информационной безопасности личности школьника в ИКТ-насыщенной среде.

Учитель должен знать:

- о негативных формах и способах воздействия ИКТ;
- а так же методах защиты;
- правилах и нормах сетевого этикета;
- видах отклоняющегося, зависимого поведения школьников;
- методах работы по их предупреждению и устранению.

Один из возможных путей разрешения проблемы информационной безопасности – обучение ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей. И школьникам, и родителям необходимо знать о том, что в виртуальном мире существует целый свод правил, которыми нужно руководствоваться при работе и общении в сети. Незнание, неумение использовать основные нормы поведения (в принципе, похожие на те, которыми мы руководствуемся в обычной жизни), приводит к тому, что подростки демонстрируют в виртуальном пространстве асоциальное поведение, а то и совершают правонарушения в сфере ИКТ [3] .

Кажущаяся безнаказанность, анонимность, доступность приводит к таким поступкам, на которые в реальном мире большинство детей не способны. Причем многие из них даже не задумываются о том, что данные действия могут нанести реальный моральный, экономический, или даже физический вред тому, против кого они направлены.

Преподаватель должен иметь представление как о классических методах защиты информации, так и о современных методологиях, технологиях информационной безопасности. Учителя должны уделять большое внимание учебно-воспитательной работе со школьниками, направленной на преодоление негативного воздействия ИКТ-среды.

В учебных программах, учебниках, методических пособиях по информатике для средних общеобразовательных школ РФ в той или иной степени нашли отражение следующие аспекты проблемы безопасности:

- техника безопасности при использовании компьютера,

- правовая охрана программ и данных,
- защита информации,
- проблема ложной информации,
- защита Интернет,
- свобода слова и цензура в Интернет,
- соблюдение прав человека,
- искусственный интеллект и безопасность общества,
- зависимость человека и общества от компьютера,
- качество программного обеспечения,
- надежность работы компьютера и безопасность общества.

Такого рода материалы в основном раскрывают вопросы безопасности компьютерной техники, информационных ресурсов, защиты интересов общества, но не дают ответа на вопрос, как обеспечить личную безопасность в информационном обществе. Однако информационная культура не сводится к информационным технологиям, она включает мировоззренческий, нравственный, психологический и другие гуманитарные компоненты.

1.2 Социально-педагогический аспект информационной безопасности детей и подростков в условиях школы

Для рассмотрения в социально-педагогическом аспекте угрозы информационной безопасности как совокупности условий и факторов, воздействующих на здоровье личности, духовно-нравственную сферу, межличностные отношения, создающих опасность жизненно важным интересам личности, были использованы основные положения Доктрины информационной безопасности РФ. Информация представляет угрозу при определенных условиях. Целью создания таких условий является манипуляция сознанием и психикой личности, в частности, личности школьника.

В качестве основных средств информационного воздействия на личность выделяются следующие:

- средства массовой коммуникации (в том числе: информационные системы, например, интернет и т.п.); литература (художественная, научно-техническая, общественно-политическая, специальная и т.п.);
- искусство (различные направления так называемой массовой культуры и т.п.);
- образование (системы дошкольного, среднего, высшего и среднего специального государственного и негосударственного образования, система так называемого альтернативного образования и т.п.);
- воспитание (все разнообразные формы воспитания в системе образования, общественных организаций — формальных и неформальных, система организации социальной работы и т.п.);
- личное общение.

Любое из этих средств может быть использовано на благо или во вред личности. [10]

В условиях школьного образования обеспечение информационной безопасности можно рассматривать как совокупность деятельности по недопущению вреда сознанию и психике ребёнка [7].

При этом процесс обеспечения информационной безопасности основывается на умениях личности учащегося увидеть и нейтрализовать угрозу, исходящую от информационного воздействия. Это умение может приобретаться стихийно или в процессе целенаправленного обучения учащихся. В связи с этим появилась необходимость поиска путей решения такой проблемы, как обеспечение информационной безопасности школьника [7].

Анализ изученной литературы дает основание утверждать, что процесс обучения целесообразно начинать с начальной школы. Поэтому необходимо рассмотреть информационную безопасность школьника, как педагогическую проблему, цель решения которой есть педагогически направляемый процесс

развития у ребенка знаний об информационной угрозе и умения противостоять ей для минимизации последствий психического и нравственного воздействия.

Всем обозначенным видам проблем может противостоять педагог, обучающий информационной безопасности. Педагог способен подготовить сознание детей к противодействию негативным информационным воздействиям, формировать информационную грамотность (навыки критического мышления), развивать способности к самоблокированию информации, учить отличать качественную информацию от некачественной.

Недостоверная, неэтичная, непристойная, деструктивная информация, исходящая от основных источников информации, а так же от средств информационного воздействия, оказывает определенное влияние на Получателя информации – школьника. Это влияние может нанести проблемы здоровью (переутомление, психологическая зависимость, соматические заболевания, снижение работоспособности и др.), этические проблемы (переоценка нравственных норм, снижение интереса к искусству, чтению, перенос образцов поведения из виртуальной действительности в реальность и др.), трудности в обучении (отсутствие времени на обучение, перегрузка излишней информацией, снижение успеваемости)[12].

Опираясь на труды исследователей этой проблемы (в частности, Л.Ф. Обуховой) можно утверждать, что определяющей для учащихся, особенно для младшего и среднего школьного возраста становится система «ребенок – учитель», влияющая на отношения ребенка к родителям, к одноклассникам и самому себе. Для учащихся ещё высок авторитет педагога, ребенок открыт для общения с наставником и доверяет информации, исходящей от него. Данные утверждения подкрепляются наблюдениями за учащимися в ходе экспериментальной работы[12].

Основным видом деятельности школьника является учебная деятельность, а процесс развития информационной безопасности важно организовать как процесс обучения.

В ребенке начинают формироваться зачатки нравственного поведения. Он понимает смысл понятий «плохо-хорошо», «добрый – злой», но у него отсутствует субъективное отношение к системе нравственных норм и ценностей. (Ермоленко-Сайко В.Д.). Система нравственных норм и ценностей становится оценочным регулятором жизни и деятельности учащегося и реализуется в том случае, если эти правила и нормы поведения приняты и осмыслены ребенком. Следовательно, целесообразно формировать информационную безопасность, используя категории нравственных ценностей и норм, активизировать собственные внутренние силы ребенка по самоусовершенствованию.

Развитие информационной безопасности школьника невозможно без учета его взаимодействия с другими учащимися. Процесс взаимодействия реализуется как кооперация (Цукерман Г.А.). В процессе кооперации идет постоянное преобразование ребенка в плане совершенствования и открываются определенные возможности для его культурно-познавательной жизни в глобальном информационном обществе. Именно поэтому необходимым должно быть взаимодействие школьников в форме кооперации как одно из необходимых условий развития информационной безопасности [7].

Школьный возраст, характеризуется большой мыслительной пластичностью, поэтому возможно её качественное изменение в ходе значимой для ребёнка учебно-познавательной деятельности, структура которой позволяет органично включить в её содержание педагогически управляемый процесс формирования у школьника знаний по информационной безопасности (В.И. Андреев, Л.С. Выготский, В.В.Давыдов, Л.В.Занков, Ю.М. Орлов, Г.К. Селевко, Г.А. Цукерман и др.) [7].

Анализируя приведённые здесь данные, можно утверждать, что социально – педагогическое решение проблемы информационной безопасности школьников возможно и должно проходить под руководством грамотного, специально подготовленного для этого педагога, учитывающего

все необходимые составляющие единого педагогического процесса и компьютерной безопасности учащихся в школе.

Глава 2. Система педагогических условий обеспечения информационной безопасности детей и подростков в школе

2.1 Анализ современной ситуации в области информатизации образования

Информационные и коммуникационные технологии (ИКТ) занимают особое место в современном мире. Работа на компьютере, умение использовать ИКТ в работе, умение создавать, а главное использовать информационные ресурсы, находящиеся в распоряжении человечества, являются основополагающими приоритетами нового стиля работы. Уже стало совершенно понятным, что администрация и преподаватели могут и должны владеть основами информационных технологий и методикой их использования в своей профессиональной деятельности [6].

Успех информатизации школы во многом зависит от наличия технологических (аппаратных и программных), информационных и организационных ресурсов, от продуманной политики руководства школы по формированию информационного образовательного пространства, от степени участия учащихся и их родителей в наполнении информационного образовательного пространства.

Информатизация современного общества привела к возникновению проблемы подготовки школьников к безопасному использованию компьютерной техники и информационных технологий. В связи с этим проанализируем основные факторы риска, представляющие угрозу для школьника при работе с компьютером, выясним, как обучение информатике способствует подготовке учащихся к самозащите от этих факторов риска, определим направления совершенствования содержания образования, способствующие повышению защищенности школьников в информационном обществе.

Многие традиционные проблемы безопасности человека в условиях информатизации общества претерпевают серьезные изменения. Происходит расширение, модификация, появление новых источников опасности (компьютеры, разнообразные информационные ресурсы Интернет, компьютерные игры и т.д.), факторов риска (различные сбои в работе компьютера, некачественные программные продукты, высокое электрическое напряжение, электромагнитные поля, информация порнографического характера, игровые программы псевдоспортивного содержания, действия хакеров и мошенников в информационных сетях и т.д.), защищаемых интересов и ценностей (финансовое благополучие, взгляды на вопросы добра и зла, отношений мужчин и женщин, волевые качества, коммуникативные способности, эстетические взгляды и чувства и т.д.) [10].

Совершенствуются факторы безопасности (меры международных структур и государственных органов РФ в области информационных технологий, деятельность учителя в системе образования, действия самих школьников и т.д.), развиваются средства и способы обеспечения безопасности (законы в области информационных технологий, технические средства защиты от электромагнитного излучения, режим работы и отдыха при работе на компьютере и т.д.), наблюдается развитие знаний, опыта, ценностей по проблеме безопасности (политехнических, правовых, психологических и др.).

Из многообразных факторов риска к наиболее распространенным и разрушительным для физического, психического и нравственного здоровья школьников относятся некоторые разновидности компьютерных игр и непродуктивное использование ресурсов Интернет. К объективным предпосылкам причинения такого рода ущерба детям и молодежи являются расширение доступа граждан России к ресурсам Интернет, наличие на рынке компьютерных программ дешевых компакт-дисков с играми разнообразного содержания.

Различные аспекты негативного влияния компьютерных игр, «интернетизации» раскрываются в публикациях А.А. Веряева, Д. Журавлева, Н.И. Саттаровой, Т. Шишовой и других авторов. Действительно, многие современные компьютерные игры, предназначенные для детей и молодежи, наводнены монстрами, палачами, скелетами, приведениями, чудовищами, людоедами и т.д. При помощи компьютера натуралистично воспроизводятся лужи крови и мозги на стенах, жуткие вопли и скрежет ломаемых костей, оторванные головы и летящие куски окровавленной плоти. Движущиеся под музыку образы на цветном экране оказывают на игроков гипнотический эффект. В ходе игр школьники имитируют действия убийц, преступников: убивают десятками, калечат, расчленяют тела персонажей игр [3, с.12].

Под предлогом борьбы со злом дети программируются на жестокость и садизм. Смысл многих игр сводится к убийству, совершению преступлений разного рода. Ребенок приобщается к реалиям криминального мира. Иные игры фактически предполагают многократную имитацию самоубийства в сюжетах со смертельными трюками на гоночных автомобилях, мотоциклах, самолетах. Под влиянием страшных образов дети начинают пугаться темноты, жалуются на кошмарные сны, боятся оставаться в комнате без взрослых. Игроки находятся в состоянии «пассивного возбуждения», при котором удовольствие достигается без усилий, что оказывает расслабляющее влияние на личность, действует как наркотик. У детей создается ощущение собственного всемогущества [3].

Увеличивается время, затрачиваемое на компьютерные игры. Реальные дела забываются, жизненные проблемы не решаются. У некоторых школьников появляются признаки компьютерной наркомании. Нарушается общение со сверстниками, утрачиваются контакты с близкими. При отсутствии возможности играть на компьютере у заядлых игроков начинается типичная «ломка» [3].

Постепенно меняется поведение компьютерных игроков в реальной жизни. Учеба, общение, спорт, искусство занимают в их жизни все меньшее

место. Притязания детей возрастают, а готовность к преодолению трудностей не совершенствуется. Формируется аддиктивное поведение, для которого характерно стремление к уходу от реальности путем изменения своего психического состояния посредством определенных видов деятельности или приема некоторых веществ. Многообразные формы аддиктивного поведения объединяет общее аддиктивное звено – стремление к искусственному изменению психического состояния, вызыванию субъективно приятных эмоций. Причем аддикты могут легко переходить от одной формы аддикции к другой, например от Интернет-зависимости к зависимости от алкоголя или наркотиков [3].

Если ребенок не становится аддиктом, во многих случаях компьютер все равно негативно влияет на его развитие. Возрастает риск появления или прогрессирования близорукости. Возможен зрительный синдром, напоминающий конъюнктивит. Дети просто сильно устают от длительного сидения за монитором. У эмоциональных игроков возможно резкое повышение артериального давления. Пониженная двигательная активность ведет к замедлению физического развития школьников.

К причинам причинения ущерба школьникам под влиянием информатизации общества относятся несформировавшаяся система личностных ценностей, отсутствие регулирования доступа к средствам информационного воздействия, психологические особенности детского возраста, индивидуальные особенности ребенка, неразвитость информационной культуры школьников, отсутствие помощи школьникам со стороны педагогов, психологов и родителей.

В связи с тем, что информатизация общества приводит к возникновению новых факторов риска, в теории и методике преподавания информатики ставится задача формирования у школьников умения отстаивать свои права в вопросах информационной безопасности личности. Соответственно, в педагогике исследуются педагогические условия обеспечения информационной безопасности школьников . Для школьников,

их родителей, учителей разрабатываются конкретные рекомендации, призванные предупредить или свести к минимуму негативные последствия использования компьютерной техники в педагогическом процессе и в повседневной жизни.

В учебных программах, учебниках, методических пособиях по информатике для средних общеобразовательных школ РФ в той или иной степени нашли отражение следующие аспекты проблемы безопасности:

- техника безопасности при использовании компьютера,
- правовая охрана программ и данных,
- защита информации, проблема ложной информации,
- защита Интернет,
- свобода слова и цензура в Интернет,
- соблюдение прав человека,
- искусственный интеллект и безопасность общества,
- зависимость человека и общества от компьютера,
- качество программного обеспечения,
- надежность работы компьютера и безопасность общества.

Такого рода материалы в раскрывают вопросы безопасности компьютерной техники, информационных ресурсов, защиты интересов общества [3].

Единое информационное пространство образовательного учреждения – это система, в которой задействованы и на информационном уровне связаны все участники образовательного процесса: администрация - учитель- ученик – родитель.

Комплексный анализ научно-педагогических источников по проблемам информационного образовательного пространства позволил выделить следующие общие положения формирования такого пространства:

- при формировании информационного образовательного пространства необходимо решить проблему содержания образования на

современном этапе, соотношения традиционных составляющих учебного процесса и новых информационно-коммуникационных технологий, новых взаимоотношений учащегося, учителя и образовательной среды;

- информационное образовательное пространство представляет сложную многокомпонентную педагогическую систему, включающую технологические (аппаратные и программные), информационные и организационные ресурсы;
- при создании информационного образовательного пространства учреждения возрастает значимость ИКТ-компетентности педагогов, осуществляющих свою профессиональную деятельность в условиях широкого внедрения средств информационных и коммуникационных технологий в образовательное пространство школы. [6]

Решая задачи построения информационного образовательного пространства многие учебные заведения приобретают различные программные продукты, интегрирующие в себе многие функции информационных систем («КМ-Школа», «Net-School», «Школьный офис», TeachPro и др.) [14].

Инновационный продукт компании «Кирилл и Мефодий» - «КМ-Школа» завоевывает все большую популярность среди педагогов школ, позволяя перейти учреждениям образования на новый информационно-технологический уровень, позволяющий осваивать и успешно применять информационные и коммуникационные технологии, как учителям, так и учащимся и даже их родителям.

Внедрение КМ-школы позволяет решить следующие проблемы:

- хранение личных дел учащихся и учителей в электронном виде (БД);
- обеспечение коммуникации всех участников образовательного процесса (методический кабинет, сайт школы);
- наличие большого объема цифровых образовательных ресурсов (готовые уроки, Медиатека КМ-Школы, портал «Школьный клуб»);

- доступность и открытость результатов учебного процесса (интеграция ИИП «КМ-Школа» со школьным сайтом, созданным в конструкторе, что обеспечивает возможность репликации на сайт данных «КМ-Школы» — расписания уроков, списков учеников, учителей и предметов, а также данных об успеваемости)
- мониторинг качества образования (анализ и формирование отчетов по результатам обучения);
- автоматизация процессов управления учебным процессом (формирование расписания, распределение нагрузки и занятости кабинетов, формирование учебных планов);
- наличие и поддержка электронной формы документооборота;
- доступность всех нормативных документов;
- использование программной среды, формирующей школьное информационное пространство;
- командный принцип формирования ИОС;
- наличие отобранной, качественной информации (обеспечивается защита школьников от доступа к вредной информации или информации сомнительного содержания).

Новые возможности сети Интернет для образования требуют их учета при построении школьного информационного образовательного пространства, которое сегодня не может ограничиваться стенами школы. Необходима поддержка дополнительного обучения школьников дома, подготовки учителей к занятиям.

2.2 Концепция информационной безопасности школьников и педагогические условия ее реализации

Формирование информационной безопасности школьников нуждается в специальных условиях, которые создают возможности взаимодействия и взаимопонимания между педагогом и учащимся на основе тщательно

продуманного содержания занятий по информационной безопасности, имеющих смысловую значимость для школьника. Одним из главных условий успешного обучения информационной безопасности является позиция учителя, сущность которой составляет безусловное, безоценочное принятие ребенка, желание укрепить его позицию в социуме, оказать своевременную поддержку в саморазвитии школьника, оградить его от совершения неприемлемых действий, открыть путь к социализации и адаптации ребенка. Работа педагога направлена на реализацию принципов педагогики саморазвития:

- принципа взаимной открытости педагога и ребенка;
- принципа свободосообразности;
- принципа глубинного общения и
- воспитания;
- принципа социосообразности;
- принципа идеологичности;
- принципа ненасилия и непримиримости к насилию над ребенком; принципа ценности творческого непослушания [4].

Одним из важных условий успешного обучения школьников основам информационной безопасности является осведомленность педагога в теории информационной безопасности: во-первых, в том, что именно защищается, что является объектом или предметом защиты (в нашем случае – это личность школьника; во-вторых, установление, от чего защищается личность школьника, какова угроза (опасность) - внешний по отношению к данной целостности фактор, воздействующий на школьника; в - третьих, в понимании необходимости предотвращения разрушения самооценки ребенка, дезориентации в окружающей обстановке, нарушении адекватности представлений школьника об окружающем мире и своем месте в нем, снижении самоуважения или чувства уверенности, утрате целостности Я и потере индивидуальной уникальности, крушении планов, намерений, выборе неадекватных целей и способов поведения, попадании в психологическую

зависимость от других субъектов воздействия, духовной деградации, нарушениях психического здоровья вплоть до необратимых патологических изменений психики; в-четвертых, в представлении, как избежать возможного ущерба, каким образом и чем защищаться; в-пятых, в уверенности педагога в том, что в процессе обучения именно он является субъектом защиты личности школьника, опережая в данном направлении действия общества и государства.

Условия, которые будут способствовать эффективному формированию информационной безопасности:

1) содержательное, включает содержательный компонент программы занятий для учащихся (систему внеклассных мероприятий, направленных на умение выявлять информационную угрозу);

2) процессуально-технологическое, направленное на эффективность использования методов, приемов и средств проведения занятий с учетом особенностей развития школьников.

3) психолого-педагогические условия, такие как гуманно-ориентированное и доброжелательное взаимодействие педагога и учащихся. Дополнительным условием явилась организация работы с родителями[4].

Рассмотрим более подробно выявленные условия. Сущностью первого условия является разработка и реализация программы внеклассной работы по информационной безопасности. Целью обучения школьника информационной безопасности является формирование соответствующей системы противодействия информационным угрозам[4]

Также можно выделить методы проведения внеклассных занятий по обучению информационной безопасности. Первым методом, наиболее важным для начальных этапов занятий, является объяснительно-иллюстративный, его значимость заключается в том, что на первоначальном этапе обучения, знания учащимся предлагаются в «готовом» виде, педагог различными способами организует восприятие этих знаний, учащиеся осмысливают знания, фиксируют их в памяти.

Знания учащимся об информационных видах опасностей, влиянии на здоровье и др. учитель предлагает в «готовом» виде, объясняет их, учащиеся сознательно осваивают и правильно воспроизводят полученную информацию [6].

Вторым методом является метод проблемного изложения материала, на втором этапе учащиеся еще не участники, а лишь наблюдатели хода размышлений учителя. Третий метод – частично-поисковый становится основным методом обучения на последующих этапах. В данном случае, педагог организует поиск новых знаний с помощью разнообразных средств. Учащиеся под руководством учителя решают познавательные задачи, проблемные ситуации, анализируют, сравнивают, обобщают, делают выводы.

В качестве формы организации обучения учащихся информационной безопасности предлагается занятия во внеурочное время. Проведение обучения во время внеклассных мероприятий дает педагогу возможность организации занятия в форме экскурсий, которая включит такие способы ознакомления учащихся с объектом, как разъяснение, беседа, наглядный показ, сбор наглядно-иллюстрационного материала с использованием основных положений теории.

Спецификой проведения занятий является: создание реальных ситуаций, предполагающих нравственный выбор, духовно-нравственное самоопределение, наличие наглядных пособий: детской периодической литературы, компьютерных дисков, имитированных моделей сотовых телефонов и т.д. Кроме этого, специфика развития информационной безопасности школьника состоит в учете таких особенностей, как: доверие ребенка взрослому, сверстникам, недостатке опыта осознания возможности удовлетворения своих основных потребностей и обеспеченности собственных прав в любой, даже неблагоприятной ситуации, в возникновении обстоятельств, которые могут блокировать или затруднять их реализацию. Педагоги и родители – значимые взрослые, способствующие становлению информационной безопасности. Но сами педагоги и родители

не всегда компетентны в вопросах информационной безопасности. Таким образом, возникает необходимость в разработке специальных занятий для педагогов, включающих теоретические семинары и практические занятия по теме «Информационная безопасность школьника» [8, с. 139].

2.3 Организация информационно-безопасного образовательного процесса в школе, взаимосвязь с родителями школьников в решении проблемы

Использование компьютерных технологий в учебном процессе отвечает психофизиологическому развитию учащихся, допускает простоту в организации занятий, оказывает заметное влияние на содержание, формы и методы обучения. Применение мультимедийных презентаций позволяет сделать уроки более интересными, включает в процесс восприятия не только зрение, но и слух, эмоции, воображение, помогает детям глубже погрузиться в изучаемый материал, сделать процесс обучения менее утомительным, позволяет повысить эффективность и мотивацию обучения. А ведь в настоящее время учителя сталкиваются с проблемой снижения уровня познавательной активности учащихся на уроке, нежеланием работать самостоятельно, да и просто учиться [2].

Благодаря использованию мультимедийных технологий в обучении:

1. Увеличивается активность учащихся на уроке.
2. Появляется возможность оперативного тестирования учащихся.
3. Экономится время и предоставляется возможность решения большего числа задач.
4. При проведении урока с использованием мультимедийных технологий соблюдается основной принцип дидактики – наглядность, что обеспечивает оптимальное усвоение материала школьниками, повышает эмоциональное восприятие, развивает пространственное воображение и все виды мышления у детей.

С другой стороны, стремительное развитие компьютерных технологий качественно меняет окружающую жизнь и порождает множество новых проблем, в частности, проблему формирования информационной культуры и безопасности среди подрастающего поколения.

Существуют различные мнения о том, когда нужно давать детям доступ в Интернет. Зарубежные специалисты сходятся в том, что запрет на Интернет может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования. Современные школы уже подключены к Интернет, и преподавание информатики начинается со второго класса. Компьютер и Интернет, как всякие сложные технологические продукты, наряду с неоспоримыми преимуществами могут нанести серьезный вред ребенку. Одним из главных вопросов, связанных с компьютеризацией, является изучение влияния компьютера на организм, психическое состояние и развитие ребенка [10].

При современном уровне развития техники вредными для детей и, вообще, пользователей любых возрастов, являются скорее не излучения, а умственное и нервное переутомление.

Вот выдержка из аннотации к книге Заряны и Нины Некрасовых «Как оттащить ребенка от компьютера и что с ним делать», вышедшей в издательстве «София»:

«Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей – и найти в себе силы и время общаться, играть, слушать их. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».

Взрослым важно помнить, что даже самые искушенные дети не видят опасностей Интернета и не осознают рисков его использования. Проблема

заключается в том, что у детей еще не сформированы критерии различия. Ребенку, в силу особенностей его психологического развития, интересно все. Оставить ребенка один на один с компьютером в Интернете, это все равно, что бросить его одного на улице большого и незнакомого города. Когда ребенок часами сидит один за компьютером, происходит почти то же самое – скорее всего, он слоняется по виртуальным улицам и подворотням. Поэтому родители и педагоги сначала сами должны научиться азам компьютерной безопасности, а потом научить этому своих детей [10].

Для этого нужна хорошо продуманная методика обучения основам информационной безопасности.

Организация режима доступа к образовательным ресурсам Интернет:

- проведение инструктажей по доступу к образовательным ресурсам Интернет;
- разработка методического пособия «Интернет – ресурсы для образовательного процесса»;
- установка программ-фильтров на школьные компьютеры;
- проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам;
- памятка родителям «Десять фактов, которые нужно сообщить детям ради безопасности в Интернет».

Существует множество программ, позволяющих ограничить время работы за компьютером, отфильтровать содержимое Интернета, обезопасить маленького пользователя. Они называются программами Родительского контроля. Родительский контроль встроен в Windows Vista. Это дает возможность контролировать использование компьютера ребенка в четырех направлениях:

a. ограничивать время, которое он проводит за экраном монитора,
b. блокировать доступ к некоторым сайтам,
c. блокировать доступ к другим интернет-сервисам,
d. запрещать запуск некоторых игр и программ.

При среднем уровне защиты, работает фильтр на сайты, посвященные оружию, наркотикам, разного рода непристойностям и содержащим нецензурную лексику.

Видеть в современной технике только добро или только зло – это крайности, которых следует избегать. Техника всего лишь инструмент в человеческих руках, предназначенный для достижения тех или иных целей. И как при использовании любого инструмента, работа в Интернет требует определенной техники, а точнее – культуры безопасности.

При всей важности технических средств, понятно, что они являются всего лишь частью осуществления политики информационной безопасности. Она включает воспитательные и образовательные мероприятия [10].

В проведении политики информационной безопасности школы принимают участие все заинтересованные в этом лица: педагоги, учащиеся, их родители. Документально политика использования ресурсов сети Интернет зафиксирована в «Правилах использования сети Интернет в муниципальном общеобразовательном учреждении» [10].

В школе может быть создан Общественный Совет по вопросам регламентации доступа к информации в Интернете, в состав которого входят представители администрации школы, учителя, учащиеся, родители. Основная функция Совета – контроль использования учащимися ресурсов сети Интернет. Также должен быть разработан пакет документов, регламентирующий работу Совета:

1. Положение об Общественном совете школы по вопросам регламентации доступа к информации в Интернете. Инструкция для сотрудников средней общеобразовательной школы и членов Общественного Совета школы о порядке действий при осуществлении контроля за использованием учащимися сети Интернет [10].

В помощь классным руководителям для проведения классных часов и родительского лектория могут быть разработаны:

Памятка учащимся «О чем надо знать при работе в Интернет. Памятка родителям по управлению безопасностью детей в Интернет.

В помощь учителям-предметникам могут разработаны методические рекомендации:

1. Памятка по оформлению методических материалов для размещения на сайте.
2. Памятка по составлению мультимедийной презентации [10].

Формирование информационной культуры и безопасности – процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Но он может превратиться и в зловещую паутину, губящую людей, если люди будут искать в ней нечистоты и превращать ее во всемирную помойку. Задача взрослых (педагогов, родителей) – формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности.

Глава 3. Практическая реализация программы информационной безопасности школьника

3.1 Современные подходы к решению проблемы информационной безопасности школьника

С развитием информационно-коммуникативных технологий в системе образования все больше используется опыт, накопленный сетевыми сообществами в обучении и приобщении учителей и школьников к участию в жизни таких сообществ, существующих на базе сетевых центров науки, искусства, здравоохранения, профессионального образования, бюджетной сферы и бизнеса. Развитие сетевых сообществ в образовательной среде будет способствовать формированию новых и развитию имеющихся профессиональных сообществ прежде всего за счет овладения в учебном процессе методологией, культурой, безопасностью работы в сетевых сообществах, что в общей сложности отвечает принципам развития информационного общества в Российской Федерации:

- принципу партнерства государства, бизнеса и гражданского общества;
- свободы и равенства в доступе к информации и знаниям;
- поддержки отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;
- содействия развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;
- обеспечения национальной безопасности в информационной сфере [1].

Сетевое сообщество (Net Community, Virtual Community) — это группа людей, поддерживающих общение и ведущих совместную деятельность при помощи компьютерных сетевых средств. Компьютерная сеть (Интернет) и программное обеспечение (социальные сервисы) связывают между собой не

только компьютеры и документы, но и людей, которые пользуются этими компьютерами, документами и сервисами. Основу сетевого сообщества составляют три компонента: простые действия участников; обмен сообщениями; социальные сервисы, представляющие собой сетевое программное обеспечение (прежде всего это современные средства Web 2.0), поддерживающее групповые взаимодействия [2. С. 5—6, 11—12]. В средней школе особенно необходимо создание свободно-образовательного, но не учебно-обязательного режима и упрочение его статуса.

Профессиональная деятельность учителей в сети Интернет — это прежде всего деятельность, направленная на учащихся, на развитие интереса к предмету, на развитие их мышления, творчества, коллективизма. Учитель организует своих учеников для участия в дистанционных олимпиадах, викторинах, конкурсах, направляет деятельность учащихся в телекоммуникационных проектах и формирует культуру общения в сетевых сообществах. Профессиональная деятельность учителей в сети Интернет включает деятельность, направленную на самих учителей, на самообразование, деятельность, связанная с повышением квалификации [4]. Профессиональным сетевым сообществом можно назвать форму деятельности, применяемую для построения организаций, предполагающих обмен знаниями среди людей, объединенных общими профессиональными интересами. Мотивами для вступления в сетевое профессиональное сообщество могут быть желание самореализации, свободы общения, профессионального развития и получение возможности обмена опытом без каких-либо дополнительных условий, а также принадлежность к профессиональной группе, приобретение известности в ее рамках и достижение некоторой социальной успешности [5].

Использование школьниками сети Интернет для получения новых знаний и установления лично значимых социальных контактов, направленных на повышение их уровня готовности к профессиональному самоопределению, способствует развитию информационной культуры

подростков и положительно влияет на их ценностные ориентиры. Для обеспечения организационно-педагогической и информационной поддержки профессионального самоопределения старших школьников могут использоваться социальные сети и возможности технологий Web 2.0. Участвуя в блогах, организованных в социальных сетях, школьники имеют реальную возможность общения в интерактивном режиме с представителями различных профессиональных сообществ. От них подростки могут получать информацию о личных и профессиональных качествах, необходимых специалистам данной сферы деятельности, о путях получения той или иной профессии [6].

Сеть — это множество разнородных элементов, находящихся в различных взаимоотношениях и объединенных между собой различными типами связей. Под такое определение попадает не только множество компьютеров, но и множество цифровых устройств (фотоаппаратов, видеокамер и т.д.), веб-документов, научных публикаций и сеть текстов вообще, экологические цепи и цепочки внутриклеточного метаболизма. Важной характеристикой перечисленных сетей является их постоянный рост и развитие. Протекающие в сетях процессы, например, процессы метаболизма, распространение инфекционных заболеваний, поведение групп людей и животных, развитие сети Интернет и сети веб-документов, имеют между собой много общего. Все перечисленные образования являются сетями, внутри которых работают общие принципы и стратегии. Социальная сеть состоит из множества людей, связанных между собой различными социальными отношениями [7]. Нетрудно прогнозировать, что с последующим развитием информационных образовательных технологий в области большей интерактивности, активного вовлечения обучаемого в познавательный процесс, с созданием образовательных сред наподобие современных социальных сетей вопросы обеспечения информационной безопасности в данной сфере будут поставлены более остро [8].

В законах Российской Федерации, документах Федеральной службы по техническому и экспортному контролю (ФСТЭК), а также государственных стандартах России (ГОСТ Р 50922-96, ГОСТ Р 51275-99 и др.) под информационной безопасностью (ИБ) понимается состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности [9]. Такое определение отражает прежде всего технологический аспект обеспечения информационной безопасности и требует дополнения применительно к сфере образования.

По Г.В. Грачеву, информационная безопасность личности — это состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможностей развития в условиях информационного взаимодействия с окружающей средой. В качестве технологической основы формирования психологической самозащиты личности выделяют следующие компоненты: общая установка, ориентировка в ситуации, определение потенциала воздействия, выявление признаков угроз информационно правовой безопасности личности, организация защитного поведения [10. С. 30].

Н.И. Саттарова под информационной безопасностью личности понимает состояние защищенности ее основных интересов, которые состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии, от угроз, вызываемых информационным воздействием на психику и социокультурное развитие человека разнообразными социальными субъектами и информационной средой общества [11. С. 34].

Т.А. Малых применительно к области образования дает понятие информационной безопасности как состояния защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и

идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия. Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере. Обеспечение информационной безопасности есть совокупность деятельности по недопущению вреда сознанию и психике личности. При этом процесс обеспечения информационной безопасности основывается на умениях личности учащегося увидеть и нейтрализовать угрозу, исходящую от информационного воздействия. Это умение может приобретаться стихийно или в процессе целенаправленного обучения учащихся [12. С. 10—11].

Членство в сообществе является добровольным, репутация основывается на доверии участников сообщества, а направление и задачи сообщества складываются из поведения отдельных участников. Для группы плохо, если человек использует свои мыслительные ресурсы и информационные сервисы исключительно в личных целях. В этом случае он занят только приведением в порядок своих собственных мыслей, записей и закладок, к которым у остальных нет доступа. Еще хуже, если человек использует информационные возможности только для коммуникаций. В этом случае он использует и свои и чужие мыслительные и временные ресурсы только для общения [2. С. 12]. И совсем плохо, когда человек, не задумываясь об информационной безопасности, своими необдуманными действиями в сетевом сообществе может нанести значительный ущерб как самому себе, так и другим членам сообщества.

Глобальная сеть наряду с уникальными возможностями, которые с ее помощью открываются для системы образования, таит в себе и чрезвычайную опасность. Опасность эта кроется не в самом компьютере (например, свойствах излучения: они не больше, чем у телевизора), а именно в информации, которая размещается в сетях, доступ к которой открыт для всех желающих. Все больше школьников пользуются информацией

Всемирной паутины, которая сказывается на интеллектуальном, нравственном развитии детей, их психическом и физическом здоровье [13]. Разработчики порталов, предоставляющие информационные сервисы для детей, озабочены вопросами информационной безопасности своих пользователей. Некоторые разработчики размещают правила, которыми необходимо пользоваться при работе с предоставляемыми сервисами для обеспечения своей безопасности, например: «Обязательно скажи взрослому, если кто-то в Сети надоедает тебе или хочет говорить о сексе; сразу прекращай контакт с любым, кто пытается давить для получения информации о тебе (имени, возраста, роста и размера, фотографий, адреса, информации о семье)» и др. [14]. Особенности восприятия информации в детском возрасте, когда значительное место занимает непосредственный интерес к теме, ее эмоциональная окраска, доминирование иррационального мышления во многих случаях не позволяют детям отнестись серьезно к рекомендуемым правилам обеспечения информационной безопасности и самостоятельно оценить их важность.

Последовательному формированию у школьников самостоятельного критического мышления может способствовать введение в школьные программы курса медиаобразования. Медиаобразование — это предметная область, изучающая специфику языка различных средств массовой информации, в первую очередь телевидения, радио, прессы, Интернета. Базовым умениям работы с информацией необходимо обучать учащихся, начиная с начальной школы (уметь выделять главную мысль в тексте, сделать вывод, дать оценку событию и т.д.). Это должна быть системная работа. Вся система обучения должна быть настроена на формирование этих базовых умений. Мировая педагогическая общественность давно осознала значимость этой проблемы не только для интеллектуального развития человека, но и для его информационной безопасности. Так, проблема информационной безопасности ребенка перерастает в проблему концепции системы образования, системы подготовки педагогических кадров [13].

В процессе непрерывного образования личность должна получить знания, выработать умения и навыки работы с новыми информационными технологиями и средствами телекоммуникации, позволяющими выполнять социальные роли создателя и потребителя информации. Данный процесс не ограничивается только реализацией технологических проблем, он включает в себя овладение эффективными методами обучения и познания, деятельности и мышления, стоящими на верхушке пирамиды непрерывного образования, а именно: анализа, синтеза, абстрагирования, формализации, обобщения информации, связанных с креативным уровнем образования, позволяющим из множества информации строить свое представление о мире или, иначе, сформировать информационный стиль мышления и информационное мировоззрение [15].

Система непрерывного образования включает в себя государственные и негосударственные учреждения и учебные заведения, обеспечивающие организационное и содержательное единство и взаимосвязь всех звеньев образования, совместно и координировано решающих задачи общеобразовательной и профессиональной подготовки и воспитания каждого человека с учетом актуальных и перспективных общественных потребностей. Непрерывность образования подразумевает качественные изменения образовательного пространства обучающейся личности. В этой связи непрерывным может считаться образование, всеохватывающее по полноте, индивидуализированное по времени, темпам и направленности, предоставляющее каждому человеку возможность реализации собственной программы обучения [16].

В информационной сфере наблюдаются многие негативные явления, для преодоления их последствий необходимо выработать механизмы защиты психики личности, сознания, духовной жизни от информационных манипуляций и агрессии массовой культуры, воздействия недостоверной, ложной информации, дезинформации. Информационная безопасность предполагает также защиту личности от неправомерного вмешательства в

производство информации и неправомерного доступа к персональным информационным ресурсам, замены реальной жизни виртуальной (иллюзорной). Результатом непрерывного образования является формирование у личности когнитивных структур, представляющих собой относительно стабильные психологические системы репрезентации знаний, которые вместе с тем являются системами извлечения и анализа информации [15].

С момента поступления ребенка в школу угроза информационной безопасности в отношении ребенка возрастает, поскольку у него появляется свобода от наблюдения и контроля со стороны родителей, а также начинает разграничиваться сфера влияния семьи, школы, системы дополнительного образования, социума. Вследствие неразработанности проблемы обеспечения непрерывной информационной безопасности школьников и методики ее комплексной реализации на уровне семьи и школы ответственность за ребенка педагоги нередко перекладывают на родителей, а родители — на педагогов и работников системы дополнительного образования.

Таким образом, выделим следующие задачи по обеспечению информационной безопасности школьников в непрерывном общем образовании и наметим возможные пути решения поставленных задач обеспечения ИБ школьников.

1. Выявление уровней обучения ИБ школьников. В школе можно выделить три уровня обучения ИБ, соответствующие: 1) начальной школе, 2) неполной средней школе, 3) средней общеобразовательной и профессиональной школе.

2. Классификация угроз на каждом этапе обучения ИБ. На первом этапе можно выделить угрозы личной безопасности школьника, не связанные с использованием технических средств. На втором этапе выделяют угрозы личности, семье, окружающему ученика социуму, возникающие при работе с информацией на компьютере и в Интернете. На третьем этапе — изучение основ профессиональной безопасности по выбранному профилю с

использованием специальных средств записи и обработки информации. Второй и третий этапы обучения информационной безопасности непосредственно связаны с медиаобразованием.

3. Обеспечение непрерывности в изучении ИБ при переходе от одного этапа обучения к другому. Обеспечение непрерывного обучения за счет четкого выделения понятийного аппарата на каждом этапе и построении на его основе системы последующих положений с учетом возрастных особенностей развития и использования технических средств работы с информацией. Определение роли угроз исходящих от сообществ, в которые могут входить школьники на каждом этапе непрерывного образования.

4. Определение содержания обучения на каждом этапе. В зависимости от возникающих угроз ИБ (вторая задача) необходимо определить содержание обучения ИБ на каждом этапе и разработать условия безопасного использования соответствующих сервисов работы с образовательным контентом. Особенностью обучения ИБ является то, что недостаточно изучить только организационные и технические средства обеспечения ИБ, но и необходимо привить нравственность и воспитать ответственность за использование информации, которая может причинить ущерб не только личности, неумело с ней обращающейся, но и другим людям.

5. Установление способов согласования действий и распределение меры ответственности семьи, школы, системы дополнительного образования по обеспечению ИБ школьников в учебно-воспитательном процессе. Необходимо разработать методические рекомендации для родителей по обеспечению информационной безопасности семьи. Они должны содержать классификацию возможных информационных угроз. Рекомендации по ограничению доступа ребенка к информации и по обеспечению информационной безопасности для детей, находящихся за пределами школы, — в зоне ответственности родителей. Организационными формами взаимодействия школы с родителями по вопросам обеспечения ИБ как учащихся, так и семьи в целом могут быть как традиционные (родительские

собрания, заседания родительских комитетов, индивидуальные беседы учителей с родителями), так и специально организованные лекции и семинары с участием педагогов, правоохранительных органов, специалистов по защите информации.

6. Определение форм внедрения мер по обеспечению ИБ в учебно-воспитательный процесс школы. Необходимо разработать систему дидактических средств для учащихся по обеспечению ИБ на каждом этапе обучения, включающую в себя систему понятий, способы поведения, законодательство в области ИБ, и другие аспекты. Внедрение знаний по ИБ в учебный процесс школы может быть как в рамках существующих предметов, например информатики или ОБЖ, так и на специально организуемых занятиях, например, классных часах, ролевых играх, проектной деятельности учащихся.

Комплексное решение рассмотренных задач информационной безопасности со стороны семьи и школы позволит значительно уменьшить риски причинения различного рода ущербов (морального, материального, здоровью и др.) ребенку. Поэтому обеспечение информационной безопасности школьников должно стать одним из первоочередных направлений работы современной школы.

3.2 Практические советы по безопасности для детей разного возраста

(по материалам сайта Обеспечение безопасности детей при работе в Интернет (http://www.oszone.net/6213/)

Интернет это замечательное средство общения, особенно для стеснительных, испытывающих сложности в общении детей. Ведь ни возраст, ни внешность, ни физические данные здесь не имеют ни малейшего значения. Однако этот путь ведет к формированию Интернет-зависимости. Осознать данную проблему весьма сложно до тех пор, пока она не

становится очень серьезной. Да и кроме того, факт наличия такой болезни как Интернет-зависимость не всегда признается. Что же делать?

Установите правила использования домашнего компьютера и постарайтесь найти разумный баланс между нахождением в Интернет и физической нагрузкой вашего ребенка. Кроме того, добейтесь того, чтобы компьютер стоял не в детской комнате, а в комнате взрослых. В конце концов, посмотрите на себя, не слишком ли много времени вы проводите в Интернет.

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернет являются дошкольники.

В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернет.

Что могут делать дети в возрасте 5-6 лет?

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями.

Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов. Как им помочь делать это безопасно?

- В таком возрасте желательно работать в Интернет только в присутствии родителей;
- Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира;
- Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети;
- Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;

- Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

Ваши дети растут, а, следовательно, меняются их интересы.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернет ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей.

Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит Родительский контроль или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок.

Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты хотелось бы заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.

Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

Для обеспечения информационной безопасности:

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;
- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
- Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее;
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Используйте специальные детские поисковые машины, типа MSN Kids Search (http://search.msn.com/kids/default.aspx?FORM=YCHM);
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса;
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО;
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей;
- Научите детей не загружать файлы, программы или музыку без вашего согласия;

- Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах http://www.microsoft.com/rus/athome/security/email/fightspam.mspx ;
- Не разрешайте детям использовать службы мгновенного обмена сообщениями;
- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;
- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;
- Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

9-12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности в этом возрасте

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения;
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;

- Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей;
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Не забывайте беседовать с детьми об их друзьях в Интернет;
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет;
- Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними;
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;
- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам , если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;
- Расскажите детям о порнографии в Интернет;
- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами;

- Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

13-17 лет

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей. Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо боле чувствительны к сексуальным домогательствам в Интернет.

Что посоветовать в этом возрасте?

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет[1], руководство по общению в Интернет (в том числе в чатах);
- Компьютер с подключением к Интернет должен находиться в общей комнате;
- Не забывайте беседовать с детьми об их друзьях в Интернет, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством

служб мгновенного обмена сообщениями чтобы убедиться, что эти люди им знакомы;

- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю;
- Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте чтобы дети не общались в приватном режиме;
- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет;
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет;
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение;
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам , если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;
- Расскажите детям о порнографии в Интернет;
- Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры;
- Приучите себя знакомиться с сайтами, которые посещают подростки;
- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям;

- Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните что дети не могут играть в эти игры согласно закона.

Обеспечивать родительский контроль в Интернет можно с помощью различного программного обеспечения. В данной статье мы рассмотрим только некоторое ПО, в частности, Родительский контроль в Windows Vista, средства Родительского контроля, встроенные в Kaspersky Internet Security.

До выхода Windows Vista средства родительского контроля можно было обеспечить с помощью операционной системы и программного обеспечения сторонних производителей. Однако с выходом новой операционной системы Windows Vista положение коренным образом изменилось. В состав ОС были включены средства Parental Control (Родительский контроль). Это позволит родителям намного проще решать вопросы контроля за поведением своих детей и их безопасностью при работе на компьютере.

Для задания Родительского контроля вам потребуется создать ограниченную учетную запись, под которой ваш ребенок будет работать за компьютером. Кроме того, не забудьте установить устойчивый (строгий) пароль на вашу учетную запись Администратора (рис. 1).

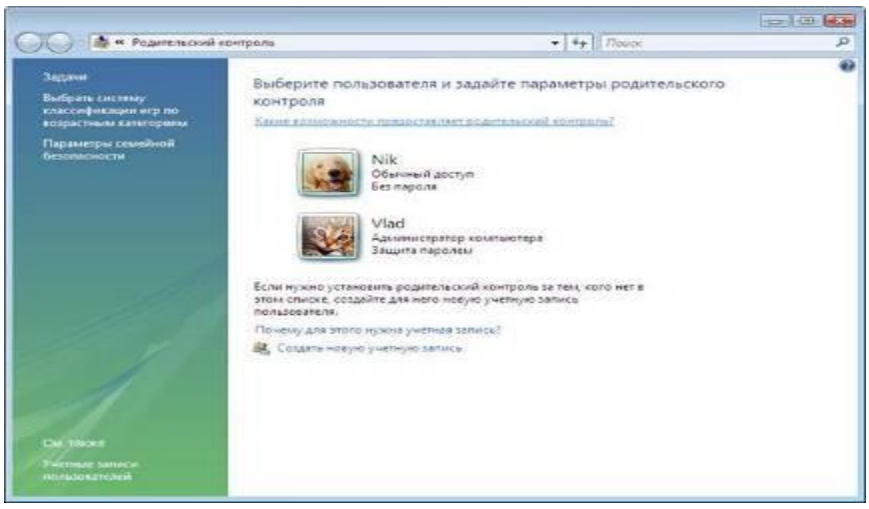

Рисунок 1 - Родительский контроль

Рассмотрим функции, решаемые с помощью родительского контроля (рис. 2):

- **Ограничение времени, проводимого ребенком за компьютером.** Можно определить время, в течение которого детям разрешен вход в систему. В частности, определить дни недели и разрешенные часы доступа в соответствующий день недели. Это не позволит детям входить в систему в течение определенного периода времени. Если в момент окончания разрешенного периода времени ребенок работает за компьютером, происходит автоматический выход из системы.
- **Установка запрета на доступ детей к отдельным играм.** Запрет можно устанавливать исходя из допустимой возрастной оценки, выбора типа содержимого или запрещая доступ к определенным играм.
- **Ограничение активности детей в Интернете.** Ограничить детей можно с помощью установки круга допустимых веб-узлов, исходя из возрастной оценки, запрета или разрешения загрузки файлов, определения условий фильтрования содержимого (т.е. вы должны определить, какое содержимое фильтры должны разрешать или блокировать). Вместе с тем можно разрешить или блокировать доступ к определенным веб-узлам.
- **Установка запретов на использование детьми отдельных программ.** Можно запретить детям доступ к определенным программам.
- **Ведение отчетов о работе ребенка за компьютером.**

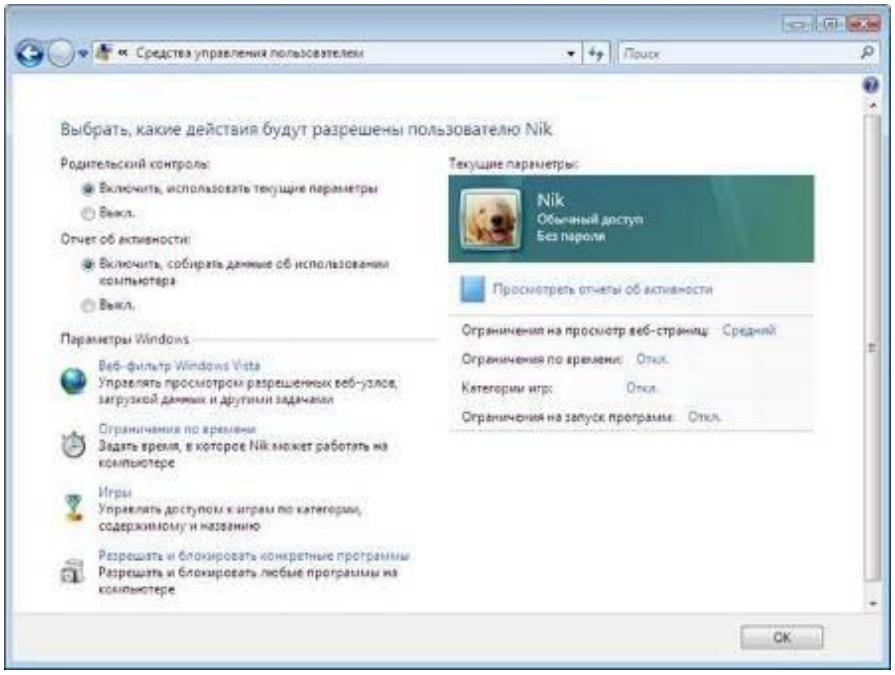

Рисунок 2 - Средства управления пользователем

Разрешенное время доступа можно определить для каждого дня недели и заблокировать при этом доступ в любое другое время (рис.3). Для этого:

- Откройте папку «Родительский контроль».
- При появлении соответствующего запроса введите пароль администратора или подтверждение пароля.
- Выберите учетную запись, для которой вы хотите задать ограничение времени.
- В группе «Родительский контроль» выберите «Вкл».
- Щелкните «Ограничение по времени».
- В появившейся сетке выберите разрешенные часы[2].

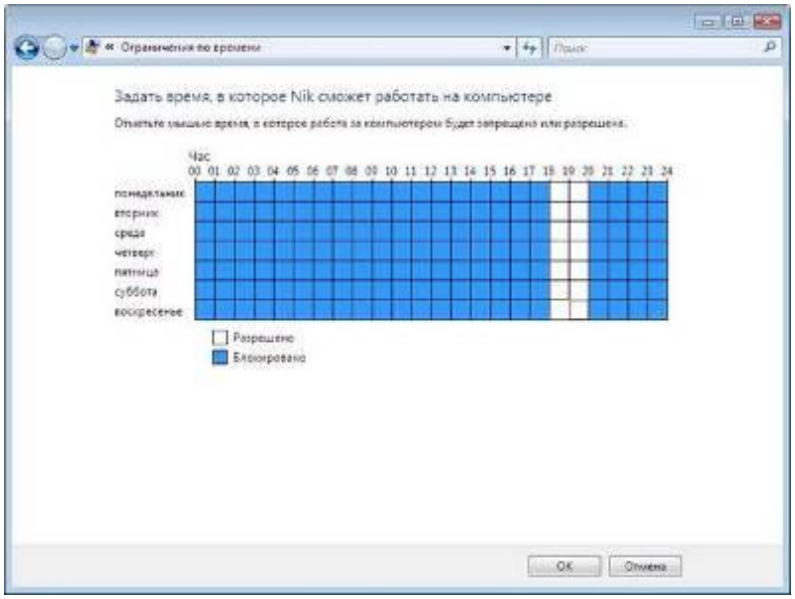

Рисунок 3 - Ограничение времени доступности компьютера для данного пользователя

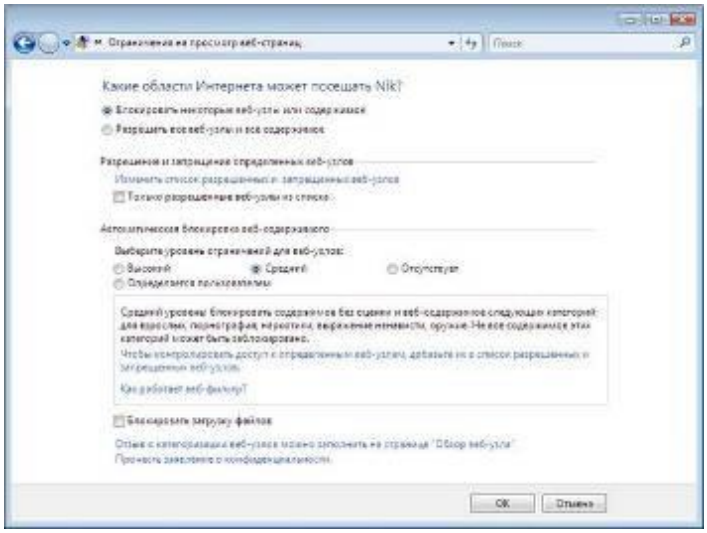

Рисунок 4 - Ограничение на просмотр веб-узлов

Веб-фильтр родительского контроля оценивает содержимое веб-узлов и может блокировать те из них, содержимое которых определено как нежелательное. Включение веб-фильтра позволит значительно уменьшить число нежелательных узлов, которые смогли бы просматривать дети, но, естественно, не гарантирует стопроцентной защиты. Так как нежелательность содержимого является субъективным критерием,

следовательно, фильтры смогут блокировать далеко не все содержимое, которое вы считаете нежелательным.

Выбор уровня ограничений для автоматической блокировки содержимого

Существует четыре уровня ограничений для обозначения содержимого, которое следует блокировать:

- **Высокий**. Веб-узлы для детей с понятным и подходящим для них содержимым. На таких узлах используется стиль изложения, понятный детям от 8 до 12 лет, а его содержимое доступно для детского понимания. Если выбран этот уровень, детям разрешается просматривать веб-узлы для детей, а также другие веб-узлы, внесенные в список разрешенных веб-узлов.
- **Средний**. Производится фильтрация веб-узлов на основании типа содержимого. В этом случае ребенок получит доступ к различной информации в Интернете, за исключением нежелательного содержимого. Чтобы узнать, какие веб-узлы ребенок посещал или пытался открыть, следует просмотреть отчет об активности в Интернете.
- **Низкий**. Содержимое веб-узлов не блокируется.
- **Особый**. Данный уровень также предусматривает блокирование веб-узлов на основании типов содержимого, но позволяет производить фильтрацию по дополнительным критериям.

Вместе с тем стоит отметить, что можно разрешить или заблокировать отдельные узлы, добавив их в список разрешенных и блокируемых веб-узлов, независимо от выбранного уровня фильтрации.

Выбор типов содержимого для блокировки

Типы содержимого, на основании которых может производиться блокировка веб-узлов.

- **Порнография**. Веб-узел имеет содержимое откровенно сексуального характера, направленное на возбуждение полового влечения.
- **Для взрослых.** Веб-узел содержит информацию откровенно сексуального характера, не носящую медицинский или научный характер.

- **Половое воспитание.** Веб-узел содержит информацию о репродуктивной функции человека и половом развитии, заболеваниях, передающихся половым путем, контрацепции, безопасном сексе, сексуальности или сексуальной ориентации.
- **Агрессивные высказывания.** Веб-узел пропагандирует враждебность или агрессию по отношению к человеку или группе людей на основании принадлежности к определенной расе, религии, полу, национальности, этнического происхождения или иных характеристик; порочит других или оправдывает неравенство на основании вышеперечисленных характеристик либо научным или иным общепринятым методом оправдывает агрессию, враждебность или клевету.
- **Изготовление бомб.** Веб-узел пропагандирует или содержит инструкции по нанесению физического вреда людям или частной собственности при помощи оружия, взрывчатых веществ, розыгрышей или иных видов насилия.
- **Оружие.** Веб-узел продает, освещает или описывает огнестрельное или холодное оружие, а также предметы боевых искусств, либо содержит информацию об их использовании, аксессуарах или модификациях.
- **Наркотики.** Веб-узел рекламирует, предлагает, продает, поставляет, поощряет или иными способами пропагандирует незаконное использование, выращивание, производство или распространение наркотиков, медицинских препаратов, химических веществ и растений, вызывающих наркотическое опьянение, или атрибутов, связанных с употреблением наркотиков.
- **Алкоголь**. Веб-узел рекламирует или содержит предложения о продаже алкогольных напитков или средств для их производства, содержит рецепты или информацию о сопутствующих принадлежностях либо пропагандирует употребление и опьянение алкоголем.

- **Табак**. Веб-узел содержит рекламу, предложения о продаже или иными способами пропагандирует табакокурение.
- **Азартные игры.** Веб-узел позволяет пользователям делать ставки и играть на тотализаторах (в том числе лотереи) в Интернете, получать информацию, содействие или рекомендации по заключению пари, а также дает инструкции, оказывает содействие или обучает азартным играм.
- **Содержимое без оценки.** Содержимое, которое не оценивается веб-фильтром.

При помощи родительского контроля можно разрешить или запретить доступ детей к отдельным веб-узлам. Также можно заблокировать некоторые веб-узлы на основании их содержимого.

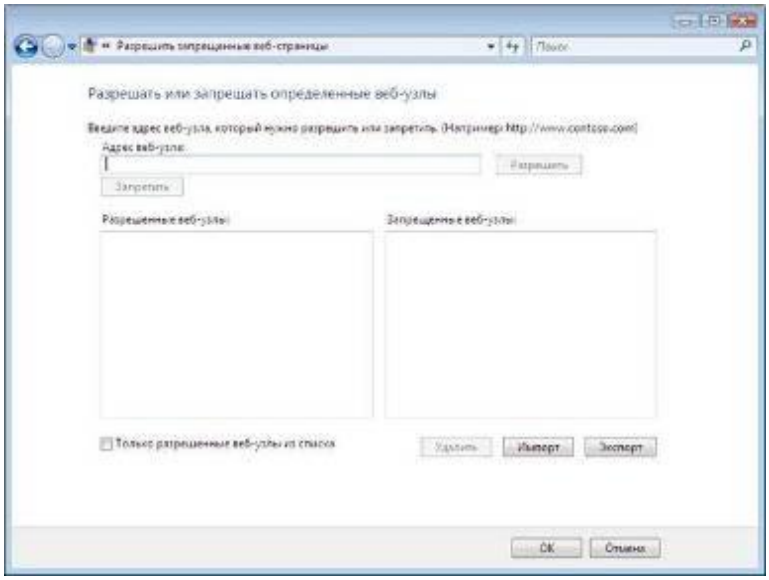

Рисунок 5 - Разрешать или запрещать определенные веб-узлы

1. Откройте «Родительский контроль».
2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
3. Щелкните имя пользователя, которому нужно установить веб-фильтр.
4. В группе Родительский контроль выберите Вкл.
5. Щелкните Веб-фильтр Windows Vista.

6. Щелкните Блокировать некоторые веб-узлы или содержимое.

7. Щелкните Изменить список разрешенных и запрещенных веб-узлов.

8. В поле Адрес веб-узла введите адрес веб-узла, доступ к которому требуется разрешить или запретить, и нажмите кнопку Разрешить или Блокировка .

Включение веб-фильтра должно значительно уменьшить число нежелательных веб-узлов, которые смогли бы просматривать дети. Однако нежелательность содержимого является субъективным критерием, и фильтр может блокировать не все содержимое, которое вы считаете нежелательным. Также в связи с постоянным появлением новых веб-узлов фильтру требуется время на анализ и оценку их содержимого.

1. Откройте «Родительский контроль».

2. Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.

3. Щелкните имя пользователя, которому нужно установить веб-фильтр.

4. В группе Родительский контроль выберите Вкл.

5. Щелкните Веб-фильтр Windows Vista .

6. Щелкните Блокировать некоторые веб-узлы или содержимое.

7. В группе Автоматическая блокировка веб-содержимого выберите необходимый уровень содержимого.

3.3 Разработка проекта информационной безопасности школьника

Актуализация качественно новых угроз безопасности учащихся, затрагивающих сущность информационной связи общества и человека, а также отсутствие педагогических условий обеспечения информационной безопасности школьника в системе образования свидетельствует об актуальности данного исследования.

Основное содержание экспериментальной работы:

Название проекта: «ПОДНИМАЙСЯ ПО ЛЕСТНИЦЕ КОМПЬТЕРНОЙ БЕЗОПАСНОСТИ»

Проект реализация модели формирования безопасной контентной информационной образовательной среды школы. Проект может быть реализован на базе ОУ.

Проект разработан для создания безопасной, комфортной информационно образовательной среды для ученика основной школы. Проект рассчитан на совместную деятельность учителей предметников, классных руководителей, администрацию образовательного учреждения, родителей и учащихся основной школы.

Проект реализован в течении первой или второй четверти. В результате проведения проекта в школе формируется школьная консультационная команда НЭО (нет электронному обману).

ПЕРВАЯ СТУПЕНЬКА. «Можно ли создать безопасную среду в Интернет для своих детей?»

Проблема: Ни родители не дети не обучены безопасной работе в Интернет, в то время как и те и другие подвержены определённому риску работая в Интернет.

Цель: Сформировать у родителей мотивацию на участие в проекте. Представить этапы, формы и условия участия в проекте совместно с детьми.

Участники: Администрация ОУ, классные руководители, родители школьников с 5 по 9 класс.

Форма проведения: Родительское собрание с элементами лекционных занятий, анкетирования, демонстраций видеороликов.

Организационно методические условия проведения: родители приглашаются на собрание по пригласительным билетам с представлением плана мероприятия. Собрание проводиться в вечернее время с использованием ТСО. Мероприятие длится не более 2 академических часов.

Ответственные и консультанты: учителя ОБЖ, информатики, зам по УВР, классные руководители.

Результат мероприятия по формированию команды НЭО: Определение микро команды от родителей 2 – 3 человека в команду НЭО.

ВТОРАЯ СТУПЕНЬКА. «Хочешь присоединиться к системе? Включай мозг !!!

Проблема: Школьники часто имеют заблуждения по поводу того, что хулиганы могут их встретить только на улице. И сидя за компьютером один на один и могут рассказать о себе всё виртуальным знакомым.

Цель: Определить востребованную школьниками ресурсов типологию Интернет ресурсов, форму представления ребят в сети.

Участники: Учащиеся 5 – 9 классов.

Форма проведения: Классный час с элементами тестирования, анкетирования, презентаций учащимися любимых Интернет порталов.

Организационно методические условия проведения: Перед проведением классного часа классный руководитель проводит анкетирование на основе которого класс разбивается на группы по принципу наиболее востребованных порталов Интернет. Проводится анализ смоделированных ситуаций имеющих место в сети.

Ответственные и консультанты: Зам. Директора по УВР, классные руководители, учитель информатики.

Результат мероприятия по формированию команды НЭО: Определение микро команды от классных руководителей 2 – 3 человека в команду НЭО.

ТРЕТЬЯ СТУПЕНЬКА. Ты собрался в Интернет? Так возьми с собой пакет!!!

Проблема: Очень часто ни дети, ни взрослые не знают каким источникам доверять?

Цель: Сформировать каталог ссылок по безопасной работе в Интернет. Создать типологию ссылок по категориям: справки, консультации, дистанционное обучение.

Участники: Школьники 5-9 классов, Родители.

Форма проведения: Самостоятельная практическая работа в Интернет на основе предложенных критериев оценки качества Интернет ресурсов.

Размещение каталога на блоге Диалоги НЭО http://dialogineo.blogspot.com

Организационно методические условия проведения: аудитория с ПК, критерии оценивания сайтов с точки зрения безопасности.

Время проведения: 1 академический час в неделю.

Ответственные и консультанты: учителя информатики. Тьюторы. Родители.

Результат мероприятия по формированию команды НЭО: Пакет методической помощи школьникам по работе с сайтами различного назначения.

Определение микро команды каждой параллели: 2 – 3 человека в команду НЭО.

ЧЕТВЁРТАЯ СТУПЕНЬКА. Хочешь посмотреть на себя в Интернет!?

Проблема: Сфера интересов детей в Интернет обширна. Но отсутствую конкретные рекомендации по тому, как себя вести в определённых ситуациях, тем более важно, чтобы эти рекомендации выработаны школьниками самостоятельно, но при помощи школьной психолого – педагогикой службы.

Цель: сформировать рекомендации по представляемой в Интернет личной информации.

Участники: школьники.

Форма проведения: Психотренг.

Организационно методические условия проведения: Проведение аналитической работы по определению сфер интересов учащихся в Интернет (развлечение, досуг, образование, общение) и по возрастам. С каждой группой определить рекомендации по представлению личной информации в Интернет.

Ответственные и консультанты: Классные руководители, родители, школьники, школьные психологи.

Результат мероприятия по формированию команды НЭО: Определение специалистов психолого – педагогической службы 1 – 2 человека в команду НЭО.

ПЯТАЯ СТУПЕНЬКА. Умей пользоваться библиотекой!

Проблема: Большинство пользователей Интернет рассматривают его возможности односторонне, не предполагая, какую поддержку можно получить от Интернет для повышения квалификации, обучения по индивидуальной траектории, развития таланта.

Цель: Создать каталог ссылок по всем предметам на учебный год при помощи сервиса «Шесть шагов НЭО к безопасности», сервиса http://www.bobrdobr.ru

Участники: Учителя предметники, ученики 5 – 9 кл., родители.

Форма проведения: Уроки презентации полезных ресурсов Интернет по предмету. 1 час

Организационно методические условия проведения мероприятия: Предусмотрен предварительное знакомство в сервисом http://www.bobrdobr.ru на уроках информатики. В результате дети выполняют буклет о возможностях сервиса для образования 1 час.

Результат мероприятия по формированию команды НЭО: Определение микро команды от учителей предметников 2 – 3 человека в команду НЭО.

ШЕСТАЯ СТУПЕНЬКА. Создание блога «Диалоги С Интернет»

Проблема:многие школьники односторонне используют Интернет ресурс для разностороннего общения.

Цель: Создать блог скорой помощи для одноклассников по проблемам в сети. Люди обслуживающие данный ресурс должны быть известны школьникам и иметь доверие к себе.

Участники: Школьники 5 – 9 кл.

Форма проведения: Дистанционная поддержка школьников через блог http://dialogineo.blogspot.com/

Диалоги НЭО:

Организационно методические условия проведения мероприятия Открытие и поддержка консультационных линий по проблемам:

• Как я могу защитить своего ребенка от рисков и угроз Интернет?

• Что нового я узнал об информационной безопасности и авторском праве?

• Как определить Интернет-зависимость?

• Чем опасны виртуальные знакомства?

• Интернет-это информационная среда или часть моей жизни?

• Хулиганство в сети: как призвать к ответу недобросовестных пользователей?

Ответственные и консультанты Команда НЭО.

Подобный проект можно транслировать на любую школу. Блог Диалоги НЭО в таком случае будет поддерживаться несколькими учебными заведениями.

Участники: Учителя предметники, ученики 5 – 9 кл., родители.

Форма проведения: Уроки презентации полезных ресурсов Интернет по предмету. 1 час.

Организационно методические условия проведения мероприятия: Предусмотрен предварительное знакомство в сервисом http://www.bobrdobr.ru на уроках информатики. В результате дети выполняют буклет о возможностях сервиса для образования 1 час.

Ответственные и консультанты: Классные руководители, родители, школьники, школьные психологи.

Результат мероприятия по формированию команды НЭО: Определение микро команды от учителей предметников 2 – 3 человека в команду НЭО.

Интернет – это не безопасное место, в котором дети могут чувствовать себя защищенными. Использование только средств воспитательной работы

без организации действенного контроля – это практически бесполезное занятие. Точно так же как и использование репрессивных средств контроля без организации воспитательной работы. Только в единстве данных средств можно помочь школьникам чувствовать себя в безопасности и оградить их от влияния злоумышленников.

Заключение

В воспитании умения ненасильственно противостоять компьютерному многообразию Интернет в современном обществе очень важное прикладное значение имеют рекомендации, раскрывающие влияние психологического, нравственного, интеллектуального, коммуникативного потенциала личности на готовность человека к безопасной жизнедеятельности в информационном обществе.

Обсуждение на уроках ОБЖ, классных часах мировоззренческих, политических, идеологических, правовых, психологических, нравственных, медицинских аспектов безопасности пользователей компьютерной техники вызывает интерес учащихся, стремление осмыслить факторы риска, характер влияния этих факторов риска на человека и общество, получить представление о средствах и способах защиты, выработать собственное отношение к факторам риска информационного общества. Такого рода обсуждение направлено на формирование у школьников знаний о факторах риска и способах обеспечения информационной безопасности, убеждения о необходимости и возможности обеспечения информационной безопасности.

Учитывая, что значительная часть школьников (особенно проживающих в сельской местности) не имеет практического опыта компьютерных игр и использования ресурсов Интернета, такая воспитательная работа при учете педагогических закономерностей является превентивной − готовит учащихся к предстоящим контактам с информационными факторами риска. Что касается школьников, «приобщившихся» к компьютерным играм, то совместная работа педагогов и родителей является условием коррекции негативных тенденций в их развитии. Положительному влиянию педагогического процесса на информационную безопасность школьников способствуют сведения о влиянии уровня информационной безопасности на возможности реализации актуальных потребностей (в общении, самоутверждении и т.д.), о

социальных группах, заинтересованных в негативном влиянии информационных технологий на человека, об экономической подоплеке аморальных и криминальных компьютерных игр.

Эти рекомендации касаются широкого круга практических вопросов обеспечения безопасности: выбор и приобретение компьютера, программного обеспечения, размещение компьютера в квартире, отношения родителей и детей при использовании компьютера, гигиенические требования к деятельности с использованием компьютера, соотношение деструктивного и безопасного в общении с компьютером, способы уменьшения информационных рисков жизнедеятельности детей и т.д.

Формированию мотивации к информационной безопасности способствует предъявление сведений о путях обеспечения информационной безопасности популярным человеком (спортсменом, артистом и т.д.), с использованием образов, художественных произведений (кинофильмов, карикатур и т.д.), с участием сверстников, обладающих высоким авторитетом для школьников и т.д.

Осознание педагогическими работниками и родителями актуальности задачи совершенствования информационной безопасности школьников, наличие опыта успешной профилактики негативных тенденций в развитии информационной культуры детей свидетельствуют о наличии практических предпосылок эффективного воспитания культуры безопасности.

Совершенствованию теоретических предпосылок для решения задач повышения защищенности детей от информационных рисков будет способствовать дальнейшее исследование целей и содержания воспитания культуры безопасности в преподавании курса информатики в школе, возможностей учебного процесса и внеклассной работы в развитии и диагностике готовности школьников к безопасной жизнедеятельности в информационном обществе.

Список литературы

1. Безопасность_в_Интернет http://www.webwisekids.com // http://letopisi.ru/index.php/ .
2. Владимирова Л.П. Сетевые профессиональные сообщества учителей http://distant.ioso.ru/for%20teacher/25-11-04/sps.htm.
3. Воронов Р.В., Гусев О.В., Поляков В.В. О проблеме обеспечения безопасного взаимодействия с сетевыми образовательными ресурсами // Открытое образование. — 2008. — № 3. — С. 20—23.
4. Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: Автореф. дисс. ... д-ра психол. наук. — М., 2000.
5. Зубакина О.В. Сетевая поддержка профессионального самоопределения старших школьников // Открытое образование. — 2008. — № 2. — С. 77—85.
6. Леончиков В.Е. Информационная свобода и информационная безопасность в системе непрерывного образования // Информационная свобода и информационная безопасность: Материалы междунар. научно-практич. конференции. — Краснодар, 2001. — С. 336—338.
7. Малых Т.А. Педагогические условия развития информационной безопасности младшего школьника: Автореф. дисс. ... канд. пед. наук. — Иркутск, 2008.
8. Патаракин Е.Д. Создание профессионального сетевого сообщества http://www.soobshestva.ru/wiki/SozdanieProfessional’nogoSetevogoSoobshhestva?v=1dhl
9. Патаракин Е.Д. Социальные сервисы Веб 2.0 в помощь учителю. — М: Интуит.ру, 2007.
10. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет //

http://www.ioso.ru/distant/library/publication/infobez.htm // http://www.humanities.edu.ru/ db/msg/84168.

11. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. — СПб.: Питер, 2008.

12. Саттарова Н.И. Информационная безопасность школьников в образовательном учреждении: Дисс. ... канд. пед. наук. — СПб., 2003.

13. Старикова Л.Д. Современная трактовка непрерывности образования // Высшее образование сегодня. — 2008. — № 10. — С. 76—79.

14. Стратегия развития информационного общества в российской федерации // Российская газета: Федеральный выпуск № 4591 от 16 февраля 2008 г.

15. Утробина Е.В. О формировании сетевых профессиональных педагогических сообществ // Педагогическое образование и наука. — 2007. — № 3. — С. 64—66.

16. Эльконин Б.Д. Круглый стол / Парадоксальные результаты международных исследований оценки качества образования // Вопросы образования. — 2008. — № 1. — С. 170—171.