МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ПСИХОЛОГИИ И ПЕДАГОГИКИ
Кафедра общей и социальной педагогики

РЕКОМЕНДОВАНО К ЗАЩИТ
В ГЭК И ПРОВЕРЕНО НА ОБЪЕ
ЗАИМСТВОВАНИ
Заведующий кафедро
д-р пед. наук, доцен
_____ И. Н. Емельянов
25 января 2017

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

ПЕДАГОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ УЧАЩИХСЯ НАЧАЛЬНОЙ ШКОЛЫ

44.04.01 Педагогическое образование
Магистерская программа «Методология и методика социального воспитания»

Выполнил работу
студент 3 курса
заочной формы обучения — Байдель Римма Робертовна

Руководитель работы
д-р пед. наук
профессор — Белякова Евгения Гелиевна

Рецензент
доцент кафедры
психологии и педагогики
детства
кан. психол. наук, доцент — Чикова Ольга Михайловна

Нормо-контроль пройден 23.01.17

г. Тюмень, 2017

ОГЛАВЛЕНИЕ

ГЛОССАРИЙ

Информационная безопасность - состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [34].

Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [5].

Информационная безопасность личности (применительно в области образования) - состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия [37].

Информационная безопасность младшего школьника - педагогически направляемый процесс формирования у ребенка знаний об информационной угрозе и умения противостоять ей для минимизации последствий психического и нравственного воздействия [36].

Риск - возникновение ситуации, характеризующейся неопределенностью результата, вероятным или обязательным наличием неблагоприятных последствий [40].

Опасность – совокупность вероятных или реально действующих факторов, процессов и явлений, которые могут оказать деструктивное воздействие на объекты и субъекты, подвергающиеся опасному посягательству [40].

Угроза – актуализированная форма опасности в процессе ее превращения из возможности в действительность, субъективированную готовность одних людей причинить ущерб другим [40].

Медиаобразование (mediaeducation) – направление в педагогике, выступающее за изучение закономерностей массовой коммуникации (прессы,

телевидения, радио, кино, видео и т.д.). Основные задачи медиаобразования: подготовить новое поколение к жизни в современных информационных условиях, к восприятию различной информации, научить человека понимать ее, осознавать последствия ее воздействия на психику, овладевать способами общения на основе невербальных форм коммуникации с помощью технических средств [56].

Интернет-зависимость (или интернет-аддикция) - навязчивое стремление использовать Интернет и избыточное пользование им, проведение большого количества времени в сети [56] .

Аддиктивное поведение – это один из типов девиантного поведения с формированием стремления к уходу от реальности путем искусственного изменения своего психического состояния посредством приема некоторых веществ или постоянной фиксации внимания на определенных видах деятельности с целью развития и поддержания интенсивных эмоций [61].

ВВЕДЕНИЕ

Актуальность исследования. Аудитория интернета стремительно растет - дети, подростки, молодежь составляют ее значительную часть. Через интернет дети и подростки открывают для себя мир, формируют собственную личность. Интернет дает пользователю огромные возможности как высокотехнологичный источник коммуникации и как инструмент поиска и получения информации. Вырастает новое цифровое поколение пользователей интернета. В то же время новые возможности привели и к появлению новых рисков. Преследования, домогательство, грубость, шантаж, мошенничество, порнография, негативный контент - вот неполный перечень тех угроз, с которыми сталкиваются юные пользователи [51].

По данным исследования «Дети России онлайн», каждый третий ребенок сталкивается с негативным контентом. На первом месте - агрессивный контент и агрессивное поведение в Интернете: жестокость, насилие, агрессия, убийства (28 %), конфликты, оскорбления, кибербуллинг (9 %), экстремизм, терроризм, насилие на национальной почве (2 %). В целом такие аспекты тревожат и пугают 39 % всех опрошенных детей. На втором месте - порнографический контент (25 %). Информация о наркотиках и суицидах беспокоит 5 % детей. Стольких же расстраивает неэтичный контент в форме нецензурной лексики. В целом около половины опрошенных детей в возрасте 8-16 лет сталкивались с сайтами, несущими угрозу их физическому здоровью и благополучию, а также с сайтами, где пропагандируется насилие и жестокость [52].

Негативный контент в Интернете регулируется рядом действующих на территории РФ законов, запрещающих или ограничивающих распространение информации, причиняющей вред здоровью и развитию детей. Но полностью оградить детей от негативной информации невозможно, один лишь ограничительный метод бессилен. Поэтому необходимо ответственное и осознанное отношение к вредной информации [52].

В связи с чем, возникает проблема информационной безопасности личности (далее ИБЛ) младшего школьника, без решения которой невозможно полноценное развитие личности ребенка и общества в целом.

В профессиональном стандарте педагога, который вступил в силу 1 января 2017 года, сказано, что педагог должен эффективно регулировать поведение учащихся для обеспечения безопасной образовательной среды. Уметь проектировать психологически безопасную и комфортную образовательную среду, знать и уметь проводить профилактику различных форм насилия. Уметь формировать и развивать универсальные учебные действия, образцы и ценности социального поведения, навыки поведения в мире виртуальной реальности и социальных сетях, навыки поликультурного общения и толерантность, ключевые компетенции (по международным нормам), то есть если сказать проще, обучать детей основам информационной безопасности личности [60].

Информационная безопасность личности (ИБЛ) - состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия [37].

Возникает необходимость обучения основам ИБЛ уже в начальной школе, так как ребенок в этом возрасте уже осваивает интернет-пространство и является уязвимым, для всех деструктивных воздействий в силу психологических особенностей.

Анализ научной литературы показал, что в педагогической науке есть исследования, посвященные ИБЛ подростков, молодежи, но недостаточно исследований по младшему школьному возрасту. Исследования по младшему школьному возрасту сводятся к запретительному методу, т.е. к простому ограждению от компьютера и интернета, что как мы видим, не является действенным методом.

В изучение проблемных вопросов информационной безопасности большой вклад внесли Федоров А. В., Федоров Д. Ю., Герасименко В. Г., Зегжда Д. П., Малюк А. А., Сычев М. П., Расторгуев С. П. и другие.

Влияние информации на личность рассматривается Грачевым Г. В., Ливингстон С., Мельником И., Пейпертом С., правила безопасности детей в Интернете предложены в исследованиях Беляевой А. Б., Козак Т., Саттаровой Н. И., вопросами информационной безопасности при применении образовательных коммуникационных технологий занимаются Морев И., Федоров А. В. , Шариков А. В. Проблемы информационной безопасности школьника нашли отражение в работах Переломовой Н. А., Малых Т. А.

Специфику взаимодействия детей и подростков с компьютерами исследовали Пейперт С., Беляева А. В. , Коул М. , Текл Ш. , Новоселова С. Л.

Огромный вклад в изучение вопроса информационной безопасности личности вносит Фонд развития интернет и конкретно такие ученые как Солдатова Г., Зотова Е., Лебешева М., Шляпников В.

В то же время сохраняется дисбаланс в указанных направлениях, как в теории, так и в практике, это подтверждается структурой и содержанием публикаций по вопросам безопасности. Во всех исследованиях личность школьника остается в стороне, нет никаких средств, программ, методик, технологий, направленных на повышение ИБЛ.

Все это позволило выделить **противоречие** между объективно существующей потребностью личности младшего школьника в информационной безопасности и отсутствием практических основ ее становления в образовательном процессе школы.

Отсюда вытекает **проблема** в недостаточной разработанности в современной науке практических способов и средств обеспечения ИБЛ младшего школьника.

В связи с этим была сформулирована актуальная **тема исследования**: «Педагогическое обеспечение информационной безопасности личности учащихся начальной школы».

Объектом исследования стал процесс обеспечения ИБЛ учащихся начальной школы.

Предмет исследования: система обеспечения информационной безопасности личности учащихся начальной школы.

Цель исследования: теоретическое обоснование, разработка и апробация программы обеспечения информационной безопасности личности учащихся начальной школы.

Гипотеза: ИБЛ учащихся начальной школы обеспечивается при выполнении следующих условий:

1. Создание безопасной информационной среды, через ограничение вредоносного контента;

2. Профилактика информационных рисков, через развитие личностных ресурсов школьников;

3. Участие всех субъектов образовательного процесса в обеспечении ИБЛ.

Критериями оценки успешности процесса обеспечения ИБЛ младшего школьника будет служить:

1. повышение компетентности учеников, родителей и педагогов в вопросах ИБЛ: сформированность у субъектов образовательного процесса умений выявлять информационные риски, оценивать их и игнорировать неблагоприятный контент;

2. установленное специализированное программное обеспечение (родительский контроль, adguard и др.) для создания безопасной среды.

Задачи:

1. Определить сущность понятия «информационная безопасность личности» в современной науке и образовательной практике;

2. Изучить и охарактеризовать информационные риски для развития личности младшего школьника;

3. Проанализировать педагогический опыт и подходы к обеспечению ИБЛ младшего школьника;

4. Разработать модель обеспечения ИБЛ младшего школьника

5. Разработать программу, включающую систему занятий для младших школьников по информационной безопасности, работу с родителями по информационной безопасности;

6. Проверить эффективность разработанных материалов в ходе опытно-экспериментальной работы.

Теоретико-методологическую основу исследования составили:

- исследования, посвященные изучению информационной безопасности личности (Т. А. Малых, Г. В. Грачев, Н. И. Саттарова, Д. Ю. Федоров и другие);

- исследования, связанные с интернет пространством (Г. Солдатова, Е. Зотова, М. Лебешева, В. Шляпников);

- общие положения развития личности, психики, затрагивающие влияние родителей на процессы формирования личностных качеств детей (Л. С. Выготский, С. Л. Рубинштейн, К. А. Абульханова-Славская, Л. И. Божович и другие).

Избранная теоретико-методологическая основа и поставленные задачи определили **этапы исследования**, которое проводилось по следующему плану:
1. Январь 2015 года – январь 2016 года - определение цели и задач исследования, выбор объекта и предмета исследования, выдвижение основной гипотезы исследования; изучение научной, законодательной литературы в этой области по теме исследования.

2. Январь 2016 года – подбор методики для выявления текущего состояния информационной безопасности личности, констатирующий этап эксперимента. Обработка и интерпретация данных. Разработка модели обеспечения информационной безопасности личности младшего школьника.

3. Март 2016 года – декабрь 2016 года – разработка материалов для формирующего этапа, проведение формирующего этапа эксперимента по разработанной программе.

4. Декабрь 2016 – Январь 2017 года – проведение контрольного этапа эксперимента, анализ, обработка, систематизация и обобщение результатов работы, формулировка выводов, оформление результатов исследования.

Методы исследования: методы теоретического уровня (изучение психолого-педагогической и методической литературы о проблематике исследования, теоретическое моделирование); методы эмпирического уровня (опрос, беседа, наблюдение, опытно-экспериментальная работа).

Экспериментальная база исследования: исследование проводилось в период с января 2015 года по декабрь 2016 года в КГУ СШ №5 города Петропавловска, Северо-Казахстанской области, Республики Казахстан, в исследовании принимали участие учащиеся 3 класса: экспериментальная группа (3 «В» класс) – 25 учащихся, контрольная группа (3 «Б» класс) – 25 учащихся.

Научная новизна исследования заключается в том, что:

- обеспечение информационной безопасности личности младшего школьника рассмотрено с позиции личностно-ресурсного подхода;

- адаптирована и модифицирована для младших школьников методика исследования особенностей использования и восприятия интернета, разработанная фондом развития Интернет;

- разработан опрос для родителей по информационной безопасности личности.

Теоретическая значимость исследования заключается в следующем**:**

- раскрыт смысл понятия «информационная безопасность личности младшего школьника» в образовании и определены подходы к его обеспечению;

- проанализирован существующий опыт обеспечения ИБЛ в образовании;

- доказана необходимость обеспечения информационной безопасности младшего школьника в процессе взаимодействия всех субъектов образовательного процесса (младших школьников, педагогов, родителей, администрации).

Практическая значимость: разработана программа по обеспечению информационной безопасности личности младшего школьника в условиях общеобразовательной школы.

Апробация материалов исследования: основные результаты исследования были освещены в ходе выступления на 67 студенческой научной конференции, 21 апреля 2016 года.

Публикации статей по теме исследования: Байдель Р. Р. Информационная безопасность школьника [Текст] // НОВЫЕ ИДЕИ – НОВЫЙ МИР: сборник научных работ молодых ученых. – Тюмень: Издательство «Печатник», 2015. – С. 19 – 22.

Байдель Р. Р. Формирование ИБЛ младшего школьника в условиях общеобразовательной школы [Текст] // НОВЫЕ ИДЕИ – НОВЫЙ МИР: сборник научных работ молодых ученых. – Тюмень: Издательство «Печатник», 2016. – С. 21 – 24

Байдель Р. Р. Информационная безопасность как составляющая медиакультуры личности [Электронный ресурс] // В помощь педагогу – Режим доступа: http://pedagog-help.ucoz.ru/publ/17-1-0-545 (дата обращения: 17.11.2016).

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПЕДАГОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ УЧАЩИХСЯ НАЧАЛЬНОЙ ШКОЛЫ

1.1. Понятие информационной безопасности личности в современной науке и образовательной практике

Под информационной безопасностью понимается состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [34].

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность [2].

В соответствии с Конституцией Российской Федерации (ст. 80, 84) Президент Российской Федерации определяет основные направления внутренней и внешней политики, в том числе в области информационной безопасности [1].

Информационная безопасность - состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [9].

Информационная безопасность личности - обеспечение информационной безопасности личности, ее право на получение объективной информации. Предполагается, что полученная человеком из разных источников информация не препятствует свободному формированию его личности [42].

Сам термин «информационная безопасность» начал употребляться в 90-х годах. Первоначально вопросы информационной безопасности ассоциировались с безопасностью самой информации, защитой информации, в большей степени - с защитой государственной тайны, но со временем это понятие приобрело и другое значение [30].

Но все, же по прежнему общеизвестна формула безопасности, закрепленная с 1992 г. в Законе РФ «О безопасности». Она рассматривается как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [11].

Даже в стратегии национальной безопасности Российской Федерации до 2020 года (2009 г.) в понятие национальной безопасности входит «состояние защищенности личности, общества и государства от внутренних и внешних угроз» [3].

Исходя из этого, к основным объектам безопасности относятся: личность (ее права и свободы), общество (его материальные и духовные ценности), государство (его конституционный строй, суверенитет и территориальная целостность).

В Концепции национальной безопасности РФ (от 10 января 2000 г.) на основе и с учетом результатов проведенных исследований существенно дополнены и конкретизированы положения, ранее закрепленные в Законе РФ «О безопасности» (1992 г.).

В новом Федеральном законе «О национальной безопасности» заметна выработка теории практики построения целостной системы национальной безопасности и предложенные пути, в полной мере, включают информационную безопасность, не только как составной части национальной безопасности, но и как отдельной проблемы:

– национальные интересы, угрозы им и обеспечение защиты от этих угроз во всех областях национальной безопасности выражаются, реализуются и осуществляются через информацию и информационную сферу;

– человек и его права, информация и информационные системы и права на них - это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях;

– решение задач национальной безопасности связано с использованием информационного подхода как основного научно-практического метода;

– проблема национальной безопасности имеет ярко выраженный информационный характер [19].

Укрепление информационной безопасности названо в Концепции национальной безопасности Российской Федерации в числе важнейших долгосрочных задач [35].

Согласно Доктрине информационной безопасности, интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина:

– на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития;

– на защиту информации, обеспечивающей личную безопасность [30].

В Доктрине информационной безопасности РФ (2000 г.) изложены цели, задачи, принципы и основные направления обеспечения информационной безопасности. Интересы личности в информационной среде представлены реализацией конституционных прав человека, обеспечением доступа и использованием информации, а также защитой информации, обеспечивающей личную безопасность [2].

Вопрос информационной безопасности личности все чаще появляется в нормативных документах РФ, но на территории Республики Казахстан, нет, ни одного документа, который бы затрагивал вопросы ИБЛ и регулировал их.

Согласно Национальной доктрине образования в Российской Федерации до 2025 г. (2000 г.) цели образования тесно связаны с развитием общества и включают в себя «создание основы для устойчивого социально-экономического и духовного развития России, обеспечение высокого качества жизни народа и национальной безопасности». С целью решения этого вопроса Совет Безопасности Российской Федерации разработал основные направления научных исследований в области обеспечения информационной безопасности (2008 г.), тем самым подготовил почву для обеспечения ИБЛ в условиях

образовательной системы. Некоторые из приведенных в данном документе гуманитарных вопросов, предполагают обеспечение безопасности индивидуального, группового и массового сознания, а также обеспечение безопасности от деструктивных информационных воздействий [6].

Анализ действующих Федеральных государственных образовательных стандартов образования показал, что в большинстве стандартов присутствует пункт, где говорится об использовании элементарных навыков работы с компьютером, понимании сущности и значении информации в развитии современного общества, приобретении новых знаний, используя информационные технологии.

В профессиональном стандарте «Педагог», который вступает в силу 1 января 2017 года, сказано, что педагог должен эффективно регулировать поведение учащихся для обеспечения безопасной образовательной среды. Уметь проектировать психологически безопасную и комфортную образовательную среду, знать и уметь проводить профилактику различных форм насилия. Уметь формировать и развивать универсальные учебные действия, образцы и ценности социального поведения, навыки поведения в мире виртуальной реальности и социальных сетях, навыки поликультурного общения и толерантность, ключевые компетенции (по международным нормам) и так далее [60].

Собирать, обрабатывать и интерпретировать с использованием информационных технологий данные, иметь базовые знания и навыки управления информацией и представление о безопасном поведении при работе с компьютерными программами и Интернетом все это тот необходимый минимум, которым должны овладеть учащиеся [4].

Вопросы ИБЛ имеют широкое освещение в нормативно-правовой документации РФ, ее относят к составляющей части национальной безопасности, но нам необходимо также узнать как в целом, не на законодательном уровне, понимается ИБЛ.

На данный момент основные фундаментальные труды по информационной безопасности в других странах, связаны с безопасностью страны, общества, то есть не выделяется в целом информационная безопасность личности, а рассматривается как составляющая национальной безопасности [32].

В России, ученые также рассматривали информационную безопасность в контексте государственной безопасности, но со временем ситуация изменилась и информационная безопасность у нас, стала рассматриваться в контексте отдельно взятой личности.

При изучении иностранных (английского, французского и немецкого) толковых словарей было выявлено, что социум, понятие «безопасность» связывается не столько «с отсутствием угрозы», а сколько с психологическим состоянием, чувствами и переживаниями человека [18].

Так, например, словарь Чэмберса (англ. яз.), расшифровывая понятие «безопасность», на первом месте указывает «состояние, чувство или средства пребывания в безопасности». С этим же понятием в нем связывается отсутствие «тревожности или озабоченности», «уверенность», «стабильность». Оксфордский словарь говорит о состоянии «более чем уверенности», словарь современного американского языка помимо указания на «свободу от опасности, риска» выделяет «свободу от озабоченности, сомнений» [23].

По мнению ряда авторов (А. Шафрански, Р. Х. Шульц, А. Эделыптейн), в разных культурах сформировались примерно одинаковые представления о безопасности, акцент в которых делается на чувствах и переживаниях человека, связанных с его положением в настоящем и перспективами на будущее. Иными словами, для человека безопасность переживается в первую очередь как чувство защищенности от действия различного рода опасностей [23].

Проблема ИБЛ является междисциплинарной. Исследованием данного вопроса занимаются в философском (В. П. Казанцева, О. И. Немыкина, А. Ю. Моздаков), культурологическом (Е. В. Горелова, Е. А. Кошевая), социологическом (Н. К. Воронович, Л. Ф. Отверченко, Т. В. Микерина,

Т. В. Тычкова), в психолого-педагогическом аспектах (А. А. Ахметвалиева, Т. В. Харлампьева, Е. Э. Серебряник, А. Д. Тырсикова, Т. А. Малых, М. А. Кузнецова, Н. И. Саттарова).

Таким образом, вопрос обеспечения ИБЛ в образовании осознан и отражен в современных нормативных документах, является предметом изучения гуманитарных наук, в том числе психолого-педагогических исследований.

По Грачеву Г. В., 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 [20].

Саттарова Н. И. в своей работе, под ИБЛ понимает состояние защищенности основных интересов личности, 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 [49].

Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [5].

Малых Т. А. определяет ИБЛ в области образования как состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия [37].

Информация и информатизация проникают во все аспекты жизни. Вследствие этого информационная безопасность является одним из важнейших явлений информационного общества. Обеспечение информационной безопасности личности приобретает исключительную важность для образования, которому отводится роль обеспечения ИБЛ обучающихся, их защите от вредных информационных потоков.

Соответственно, мы должны ориентироваться на формирование таких качеств, которые бы позволили обеспечить безопасность при взаимодействии с негативными информационными потоками, должны иметь представление о возможных информационных опасностях и способах противодействия им через обеспечение ИБЛ.

Информационная безопасность младшего школьника - педагогически направляемый процесс формирования у ребенка знаний об информационной угрозе и умения противостоять ей для минимизации последствий психического и нравственного воздействия [36].

Стабильный рост информатизации требует не только развития компьютерной грамотности, но также необходимость развития ИБЛ, как обязательного в условиях информационного общества качества, позволяющего учащимся полностью реализовать себя в информационном обществе. Сущность формирования информационной безопасности школьника состоит в том, чтобы научить ребенка выявлять информационную угрозу; определять степень ее опасности; уметь предвидеть последствия информационной угрозы и противостоять им [7].

В целом сегодня, в науке и системе образования, сложились две тенденции рассмотрения определения понятия и структуры информационной безопасности личности. Информационная безопасность личности как качество личности и как качество образовательного процесса.

Иными словами, информационная безопасность личности - это:

а) состояние защищенности, при котором отсутствует угроза причинения вреда информации, которой владеет личность;

б) состояние и условие жизнедеятельности личности, при которых отсутствует угроза нанесения вреда личности информацией [16].

И отсюда следует разделить информационную безопасность на информационно-идеологическую и информационно-техническую. При этом под информационно-технической безопасностью личности следует понимать защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба личности, а под информационно-идеологической безопасностью - защищенность личности от преднамеренного или непреднамеренного информационного воздействия, имеющего результатом нарушение прав и свобод в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами, противоречащих нравственным и этическим нормам, оказывающих деструктивное воздействие на личность, имеющих негласный (нечувственный, неосознанный) характер, внедряющих в общественное сознание антисоциальные установки [16].

В теории и практике информационной безопасности выделяется два направления: защита информации и информационно-психологическая безопасность. Информационно-психологическая безопасность создает условия для обеспечения психического здоровья отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания, нацеленного на прогрессивное развитие общества, защита информации это защита конкретных данных [21].

Информационная безопасность личности это не просто качество или чувство защищенности, это - то состояние, которое необходимо достичь, а для того чтобы его достичь необходимо это понятие понимать как систему. Системный подход к информационной безопасности требует определения ее субъектов, средств и объектов, источников опасности, направленности опасных информационных потоков и принципов обеспечения информационной безопасности (рис. 1).

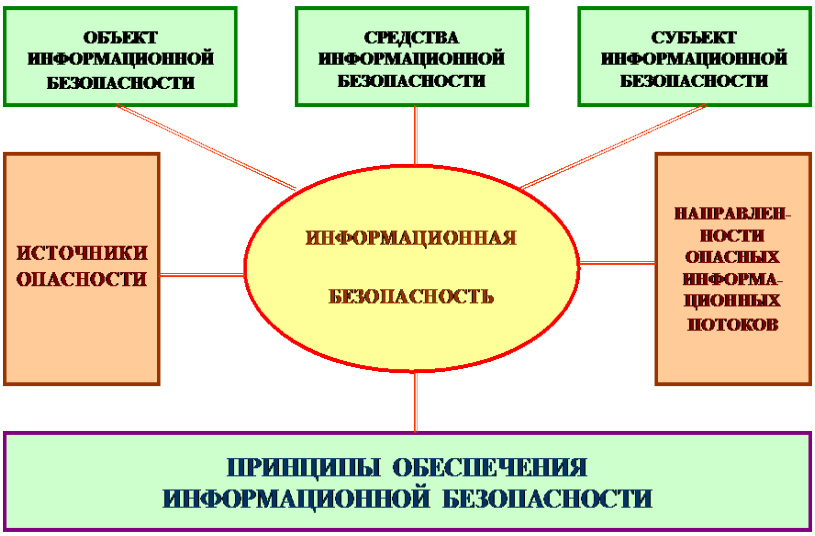

Рис. 1. Системное понимание информационной безопасности личности

Объектами опасного информационного воздействия и, следовательно, информационной безопасности могут быть: сознание, психика, личность в целом. Субъектами информационной безопасности следует считать те органы и структуры, которые занимаются ее обеспечением. Средства обеспечения информационной безопасности - это средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д. [26].

Информационная безопасность младшего школьника - педагогически направляемый процесс развития у ребенка знаний об информационной угрозе и умения противостоять ей для минимизации последствий психического и нравственного воздействия [37].

Если подвести итог всему выше сказанному, то мы можем сделать вывод, что информация – одно из сильнейших средств влияния на личность, социум и мир в целом. Поэтому и возникает проблема информационной безопасности, прежде всего именно личности, как носителя индивидуальных особенностей (способностей, характера, интересов), что в совокупности имеет влияние на национальную безопасность [43].

Сущность обеспечения информационной безопасности школьника состоит в том, чтобы научить ребенка выявлять информационную угрозу,

определять степень ее опасности, уметь предвидеть последствия информационной угрозы и противостоять им.

Мы приходим к выводу что, информационная безопасность личности рассматривается, в первую очередь, как качество присущее личности с целью защиты себя от негативного информационного воздействия. Данное качество активно влияет на жизнь социума и государства, от ИБЛ зависит национальная безопасность. В связи с этим необходима безопасная информационная среда, которая будет влиять на информационную безопасность личности. Исходя из этого, мы можем утверждать, что информационная безопасность личности это взаимосвязь среды и личности, только при их правильном взаимодействии, можно обеспечить информационную безопасность личности.

1.2. Информационные риски, опасности, угрозы развитию младшего школьника

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 способствует подготовке учащихся к самозащите от этих факторов риска, определим направления совершенствования содержания образования, способствующие повышению защищенности школьников в информационном обществе.

Для изучения проблемы обеспечения ИБЛ в образовании требуется особый понятийный аппарат. Необходимо рассматривать понятия «риск», «опасность», «угроза» как систему.

Риск как понятие представляет собой возникновение ситуации, характеризующейся неопределенностью результата, вероятным или обязательным наличием неблагоприятных последствий. Глушенко В. В. определяет риск как действующий/развивающийся фактор процесса, обладающий потенциалом негативного влияния на ход процесса [40].

В информационной безопасности риск определяется как функция трех переменных величин: вероятность существования информационной угрозы; вероятность существования незащищенности; потенциальное воздействие.

В настоящее время информационные риски уже являются не только предметом изучения, но и защиты. Информационный риск может стать причиной появления информационной опасности [40].

В наиболее обобщенном виде опасность представляет собой совокупность вероятных или реально действующих факторов, процессов и явлений, которые могут оказать деструктивное воздействие на объекты и субъекты, подвергающиеся опасному посягательству. В зависимости от своей природы, количественной и качественной характеристик, продолжительности действия опасность способна оказать значительное отрицательное воздействие на субъекты опасности. Информационная опасность, заключается как в действиях самого субъекта информационной сферы, своими непрофессиональными, самонадеянными, ошибочными действиями или в результате информационного риска нанесшего вред собственным интересам в данной сфере (внутренний аспект), так и в спонтанном (неумышленном) или преднамеренном нанесении вреда интересам субъекта в информационной сфере внешней стороной (внешний аспект). Здесь важно учесть, что субъект информационной среды никогда не ставит цели нанесения вреда своим информационными правам и интересам, предполагая потенциально или реально возникающую информационную опасность (риск) предусмотреть или преодолеть. Способность подобного преодоления всецело относится к личностным характеристикам субъекта. На наш взгляд, информационная опасность более всего представляет собой побуждение к определенному действию (бездействию), которое, в принципе, можно предвидеть, а значит, своевременно предотвратить или минимизировать вред и ущерб от его реализации и тем самым обеспечить защиту интересов субъекта информационной сферы [40].

Угроза в общем понятии представляет собой намерение реализовать вероятную опасность. Само понятие «угроза» не имеет четкого единого определения и многими авторами трактуется по-разному. Например, угроза определяется как «высказанное в любой форме намерение нанести физический, материальный или иной вред общественным и личным интересам». Ряд авторов считают, что угроза – это «совокупность факторов и условий, представляющих опасность жизненно важным интересам личности, общества и государства». Другие полагают, что угроза – это «наиболее конкретная и непосредственная форма опасности, создаваемая целенаправленной деятельностью откровенно враждебных сил» [40].

Барабин В. В. представляет угрозу как актуализированную форму опасности в процессе ее превращения из возможности в действительность, субъективированную готовность одних людей причинить ущерб другим.

Образно говоря, угрозу можно охарактеризовать как последнее предупреждение, за которым и последует само действие. Информационная угроза, по сути, представляет собой умысел с целью намеренного нанесения вреда субъекту информационной сферы. В отличие от информационного риска и частично информационной опасности, информационная угроза направлена против интересов субъекта в данной сфере.

Учитывая нынешнее развитие информационно-коммуникационных технологий и информационных ресурсов, возрастающее и неуклонное влияние информации на жизнедеятельность личности, общества и государства, а также происходящие процессы глобализации человечества, можно утверждать, что информационные угрозы способны не только воздействовать на информационную безопасность, но также в тех или иных параметрах оказывать деструктивное влияние на человека в целом.

Таким образом, квалифицируя исследованные выше информационные риски, опасности и угрозы, можно сделать вывод: информационные риски и отчасти информационные опасности (без наличия умысла) представляют собой потенциально вредные намерения и действия, способные нанести

определенный ущерб субъектам информационной сферы. Информационные угрозы являют реальную готовность нанесения вреда и желание наступления негативных последствий для субъектов информационной и иных сфер жизнедеятельности личности, общества и государства. При этом следует уточнить: информационные риски и опасности могут стать причиной появления информационной угрозы безотносительно того, умышленны они или нет. Информационные угрозы представляют наибольшую проблему в обеспечении информационной безопасности личности, так как содержат в себе качественные квалифицирующие признаки повышенной потенциальной и реальной деструкции [40].

Информационные угрозы могут быть преддверием последующих действий, которые выражаются в таких формах как: информационная война, информационная атака, информационный шантаж, хакерство, нарушение или вывод из строя технических и информационно-коммуникационных систем, несанкционированный доступ в компьютерные системы собственника или владельца информации, шпионаж, публичное разглашение секретных и конфиденциальных сведений, нарушение права на частную жизнь, кража персональных данных, фальсификация данных, умышленная негативная информация с целью нанесения ущерба имиджу личности, клевета, фальсификация и уничижение национальных и государственных институтов, приоритетов, святынь, проектов, идеологии и др., пропаганда асоциальных и аморальных установок и норм, разрушение духовно-нравственных ценностей социума и т. д. Виды угроз информационной безопасности Российской Федерации обстоятельно представлены в ее Доктрине информационной безопасности [2].

Согласно классификации Фонда Развития Интернет собственно информационные риски и опасности делятся на контентные, коммуникационные, потребительские и электронные (рис.2) [57].

Рис. 2. Классификация интернет рисков и угроз

Хлопьев А. Т. выделяет основные факторы информационной среды, которые могут стать факторами риска. К ним относятся объем, полнота, количество циркулирующей информации, адекватность потоков информации перцептивным параметрам органов чувств, свойствам внимания, памяти, мышления, наличие в информационных потоках специфических элементов, целенаправленно изменяющих психофизиологическое состояние больших масс людей или лиц, принимающих важные для социума решения (слова, образы, сообщения, воздействующие на подсознательном уровне) [58].

Информационная опасность имеет различные формы своего проявления: зависимость от сетевых и компьютерных, азартных игр, интернета, наркотиков, плагиат, пропаганда насилия, жестокости, агрессии, нетерпимости, расовой ненависти, безответственного поведения, азартных игр, суицида, булимии, деятельности различных сект, неформальных молодежных движений, угроза жизни, психическому здоровью личности, развитие агрессивной потребительской идеологии, непристойные выражения, миксофилия - стремление к многообразию жизнедеятельности, миксофобия - страх перед увеличивающимся многообразием стилей жизни и опасностей, криминальная и террористическая информация молодежных движений, кибербуллинг (запугивание, унижение, травлю, физический или психологический террор) [10].

Из большого числа рисков, более влияющие на физическое, психическое здоровье и нравственные ценности младших школьников, компьютерные игры и непродуктивное использование ресурсов сети Интернет [40].

Аспекты негативного влияния компьютерных игр, «интернетизации» раскрываются в публикациях Веряева А. А., Журавлева Д., Саттаровой Н. И., Шишовой Т. и других авторов.

Увеличивается время, затрачиваемое на компьютер. Реальные дела забываются, жизненные проблемы не решаются. У некоторых школьников появляются признаки компьютерной зависимости. Нарушается общение со сверстниками, утрачиваются контакты с близкими. При отсутствии возможности играть на компьютере у заядлых игроков начинается типичная «ломка». 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 [59].

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 [59, С. 187].

При анализе существующих подходов к обеспечению ИБЛ в образовании, Петровой В., выделено два основных подхода – запретительный и личностно-ресурсный [46].

Запретительный подход осуществляется через запрет-ограничение потоков информации. Данный подход представлен в нормативных документах. Так для защиты детей от информации, причиняющей психический,

нравственный, физический вред была введена возрастная классификация информационной продукции с 1 сентября 2012 года [44].

Знак возрастных ограничений классифицирует информационную продукцию по возрастным категориям. Появилась и юридическая ответственность за причинение вреда с помощью информации. Постановлением Правительства Российской Федерации от 26 октября 2012 г. в сети Интернет создан Единый реестр запрещенных сайтов. Хотя сравнительно недавно Уголовный кодекс Российской Федерации (1996 г.) не предусматривал борьбы с сайтами, содержащими информацию, отрицательно влияющую на психику [13].

При поддержке Минкомсвязи РФ создана Лига безопасного интернета, организации для противодействия распространения опасного контента в сети Интернет. Члены лиги присоединяются к организации добровольно и ведут борьбу с вредным контентом. Данный подход достаточно широко представлен на дошкольном и школьном уровнях образования [53].

Но ИБЛ невозможно обеспечить одними лишь запретительными мерами. Как только исчезают внешние фильтры потоков информации, личность становится уязвимой, неспособной осмысленно относиться к информационным рискам, опасностям и угрозам. Если в ресурсах самой личности отсутствуют сформированные ценности, критерии и барьеры, которые определяют отношение и поведение человека, то риски остаются неопознанными самой личностью.

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 – все это относится к причинам причинения ущерба учащимся информацией [14].

Мы видим следующую картину: родители чаще всего не уделяют должного внимания работе детей за компьютером и в сети интернет, педагоги в

начальной школе не уделяют этому вопросу должного внимания, так как считают, что это не является проблемой, ведь в школе в начальных классах дети не часто сталкиваются с использованием ИКТ, а то, что происходит дома, за этим должны следить родители. А младшие школьники, в силу своего возраста, не понимают угроз и возможных рисков при работе с ИКТ. Не относятся к этому как к чему-то серьезному, а наоборот считают, что сетевое пространство, это пространство вседозволенности, открытости и развлечения. Также они не могут фильтровать получаемую информацию, они верят всему.

Информационных рисков, угроз, опасностей существует огромное множество, оно подстерегает младшего школьника за каждым углом. Задачи педагогов и родителей, сплотить усилия и донести до учащихся всю важность ИБЛ, показать все возможные угрозы и стараться обеспечить информационную безопасность, но не запретами, как чаще всего делается, а так, чтобы ребенок сам понимал, все, то плохое, что в себе может нести интернет и прочие источники информации.

1.3. Опыт обеспечения информационной безопасности личности в образовательном процессе

Применение информационно коммуникационных технологий (ИКТ) в образовании соответствует психофизиологическому развитию учащихся, обеспечивает удобство при проведении занятий, оказывает несомненное влияние на содержание, формы и методы обучения. Применение мультимедиа помогает сделать уроки интереснее и ярче, в процесс восприятия включается не только зрение и слух, но и эмоции, воображение, что способствует более глубокому погружению в изучаемый материал, процесс обучения становится менее утомительным, повышается эффективность и мотивация обучения [9].

Но с другой стороны, быстрое развитие ИКТ и постоянно меняющееся информационное пространство, качественно меняют окружающую действительность, что порождает множество нерешенных проблем на

сегодняшний день, одной из этих проблем является обеспечение информационной безопасности личности подрастающего поколения [54].

Учитывая информационные риски, угрозы, опасности система образования не может остаться в стороне. На сегодняшний день, система образования осознает, что перед ней стоят сложные задачи:

- поиск эффективных путей полноценного развития детей в современных условиях неограниченного доступа к информации (ТВ, Интернет и т.д.);

- поиск путей формирования информационного иммунитета, который проявляется в невосприимчивости личности к негативным информационным воздействиям, в умении выявить, идентифицировать угрозы, содержащиеся в информации и защититься от них.

Существуют различные взгляды на вопрос о том, когда нужно и можно давать детям самостоятельный доступ к сети Интернет. Иностранные специалисты солидарны в том, что запрет на Интернет может быть действенным только до тех пор, пока это не ограничивает потребности ребенка в сфере образования. Компьютер и Интернет, как всякие сложные технологические продукты, могут нанести серьезный вред ребенку. Одной из важных проблем, связанных с компьютеризацией, является изучение влияния компьютера на человека, его психическое состояние и развитие в целом [9].

В книге Заряны и Нины Некрасовых «Как оттащить ребенка от компьютера и что с ним делать» рассказывается о том, как сделать, чтобы компьютер в семье стал другом и помощником: «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» [28].

Взрослым необходимо помнить, что даже самые искушенные дети чаще не видят опасностей Интернета и не осознают рисков его использования. Проблема заключается в том, что у детей еще не сформирован некий фильтр. Ребенку, в силу особенностей его психологического развития, интересно все. Предоставить ребенку полную самостоятельность и оставить его одного с компьютером в Интернете, это все равно, что бросить его одного на улице большого и незнакомого города. Когда ребенок часами сидит в интернете, скорее всего, он слоняется по виртуальным «улицам и подворотням». Поэтому важно, чтобы родители и педагоги, владели информационной безопасностью и прививали ее детям.

В этом может помочь методика обеспечения информационной безопасности. Необходима организация режима доступа к образовательным интернет ресурсам. Нужно проводить инструктажи по доступу к образовательным ресурсам Интернет. Можно разработать методическое пособие «Интернет - ресурсы для образовательного процесса» или каталог образовательных ресурсов, перечень рекомендуемых сайтов для посещения и прочее. Важна установка программ-фильтров на школьные компьютеры и родительского контроля на домашние. Проведение лектория для родителей учащихся по режиму доступа детей к образовательным ресурсам будет не лишним, можно разработать и раздать памятки 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: ограничивать время, которое он проводит за экраном монитора; блокировать доступ к некоторым сайтам; блокировать доступ к другим интернет-сервисам; запрещать запуск некоторых игр и программ.

При среднем уровне защиты, работает фильтр на сайты, посвященные оружию, наркотикам, разного рода непристойностям и содержащим нецензурную лексику [59].

При всей важности технических средств, понятно, что они являются всего лишь частью осуществления политики информационной безопасности. Она включает воспитательные и образовательные мероприятия, которые должны быть направлены на формирование у учащихся морально-семантического фильтра, благодаря которому дети смогут проходить мимо различных сайтов с неблагоприятным контентом. Видеть угрозы и реагировать на них так, чтобы минимизировать их отрицательный эффект [47].

В проведении политики информационной безопасности школы должны принимать участие все заинтересованные в этом лица: педагоги, учащиеся, их родители и администрация заведения.

В учреждении образования может существовать организация общественного совет, которая будет консультировать по вопросам доступа к информации в Интернете, в его состав могут войти представители администрации школы, учителя, учащиеся и их родители. Основная функция совета – контроль использования учащимися ресурсов сети Интернет. Необходимо, конечно разработать документы, которые будут направлять работу совета, например, такие как положение об общественном совете школы по вопросам регламентации доступа к информации в Интернете, инструкция для сотрудников общеобразовательной школы и членов общественного совета школы о порядке действий при осуществлении контроля при использовании учащимися сети Интернет.

В помощь классным руководителям в проведении классных часов и родительского лектория могут быть разработаны памятки для учащихся «О чем надо знать при работе в Интернет и для родителей по управлению безопасностью детей в Интернет.

Педагогическое обеспечение информационной безопасности личности процесс довольно долгий и не простой, но важный и необходимый. Задача

взрослых (педагогов, родителей) формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности.

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 [38].

Последовательному формированию у школьников самостоятельного критического мышления может способствовать введение в школьные программы курса медиаобразования [39].

Медиаобразование (mediaeducation) – направление в педагогике, выступающее за изучение «закономерностей массовой коммуникации (прессы, телевидения, радио, кино, видео и т.д.). Основные задачи медиаобразования: подготовить новое поколение к жизни в современных информационных условиях, к восприятию различной информации, научить человека понимать ее, осознавать последствия ее воздействия на психику, овладевать способами общения на основе невербальных форм коммуникации с помощью технических средств [56].

Курс медиаобразования будет способствовать обучению учащихся базовым умениям работы с информацией. Необходимо обучать учащихся, начиная с начальной школы, должна быть системная работа.

При поступлении ребенка в школу угроза ИБЛ возрастает, так как ребенок свободен от наблюдения и контроля со стороны родителей, начинает разграничиваться сфера влияния семьи, школы, системы дополнительного образования, социума. Из-за нерешенности проблемы обеспечения информационной безопасности школьников и методики ее реализации на уровне семьи и школы, ответственность за информационную безопасность

ребенка педагоги часто перекладывают на родителей, а родители - на педагогов.

Исходя из этого, мы можем выделить ряд задач по обеспечению информационной безопасности школьников:

1. Необходимо выделить уровни обучения ИБЛ школьников. В школе можно выделить три уровня обучения ИБЛ, соответствующие:

- начальной школе,
- неполной средней школе,
- средней общеобразовательной и профессиональной школе, с целью непрерывного обеспечения ИБЛ.

2. Классифицировать угрозы на каждом этапе обучения ИБЛ, от простого к сложному, то есть от объяснения возможности личных угроз до угроз больших масштабов.

3. Обеспечение непрерывности в изучении ИБЛ при переходе от одного этапа обучения к другому. Обеспечение непрерывного обучения на каждом этапе и построении на его основе системы последующих положений с учетом возрастных особенностей развития и использования технических средств работы с информацией.

4. Определение содержания обучения на каждом этапе. Особенностью обучения ИБЛ является то, что недостаточно изучить только организационные и технические средства обеспечения ИБЛ, 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 ИБЛ школьников в учебно-воспитательном процессе. Необходимо разработать методические рекомендации для родителей по обеспечению информационной безопасности семьи. Организационными формами взаимодействия школы с родителями по вопросам обеспечения ИБЛ

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 ИБЛ в учебно-воспитательный процесс школы. Внедрение знаний по ИБЛ 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 [12].

Нами проанализирован опыт работы образовательного учреждения МБОУ «Гимназия №1» г. Саянска, Иркутской области по информационной безопасности личности школьника, ведь именно выше перечисленные задачи стали приоритетным направлением работы гимназии с 2005 – 2010 гг.

Хотелось бы подчеркнуть, что это направление инновационной работы впервые разрабатывалось в системе образования России, и поэтому было поддержано на федеральном уровне.

Таким образом, гимназия понимала, что педагогическое воздействие необходимо было направить не только на формирование умения работать с информацией, но и на формирование умения обучающихся защищаться от негативного ее воздействия с раннего школьного возраста.

Как это возможно сделать? Такого опыта в современной российской практике и науке не было, да и в зарубежной практике тоже. Поэтому коллектив гимназии №1 г. Саянска стал первопроходцем по разработке нового инновационного направления.

Их работа была поддержана на региональном и федеральном уровнях. Так, начавшийся в 2005 году эксперимент по разработке педагогического аспекта информационной безопасности позволил гимназии стать победителем конкурса культурно-образовательных инициатив в Москве, и приказом Министерства образования и науки Российской Федерации от 12.05.2006 №108

учреждению был присвоен статус федеральной экспериментальной площадки для реализации проекта «Педагогические аспекты информационной безопасности личности».

Педагогическим коллективом совместно с научным руководителем д.п.н. Переломовой Н. А., были разработаны:

– программа развития гимназии «Информационная безопасность участников образовательного процесса в воспитательной системе гимназии»;

– программа эксперимента «Исследования информационной безопасности личности: педагогический аспект»;

– программа воспитательной системы школы;

– программы внеклассной деятельности для обучающихся начальной школы, специальных курсов для обучающихся средней и старшей школы, направленные на формирование информационного иммунитета;

– проведена апробация данных специальных курсов [15].

Целью проводимого эксперимента являлись анализ и исследование проблем, связанных с воздействием информации на сознание и психику человека; определение путей обеспечения безопасности школьника, связанной с информационной экспансией; разработка методики работы с информацией [15].

Прежде всего, было необходимо понять, что же такое «информационная безопасность личности» и «компетентность учащихся в области информационной безопасности».

Для чего это было нужно? Для того чтобы разработать и апробировать специальные курсы для школьников 3-11-х классов. Эти курсы, должны помочь детям защититься от негативного влияния информационных потоков. Хочется подчеркнуть, что гимназией рассматривались информационные потоки не только Интернета, но и различных СМИ и т.д.

Надо было научить педагогов работать в современном информационном пространстве, несущем определенные угрозы. Отсюда и появилась

необходимость в разработке программы повышения квалификации педагогов по вопросам информационной безопасности школьника [15].

Гимназия хорошо понимала, что без поддержки семьи, только силами педагогического коллектива, эффективно сработать будет достаточно трудно. В связи с этим была разработана система работы с родителями по вопросам информационной безопасности ребенка.

Следующим шагом в экспериментальной работе являлось определение системы организационных, психолого-педагогических, научно-методических условий, способствующих эффективной реализации разработанной системы воспитания.

Достаточно долгим и ответственным этапом являлась экспериментальная проверка системы обеспечения информационной безопасности личности учащихся гимназии.

При решении поставленных задач многое было сделано впервые. Так ими, первыми, в Российской Федерации была разработана концепция информационной безопасности школьника. В ходе её реализации были успешно разработаны содержание и методики повышения квалификации педагогов в области информационной безопасности. Важным направлением работы стало включение педагогов в деятельность временных исследовательских коллективов.

За период экспериментальной работы педагогическим коллективом гимназии изданы соответствующие методические пособия, учебно-методическое обеспечение образовательного процесса регулярно дополнялось с помощью педагогов практическими материалами рефлексии своего опыта, представленных в сборниках, методических материалах и других публикациях.

Так были разработаны программы для 3-11-х классов. Реализация программы эксперимента потребовала разработки и апробации психолого-педагогической модели мониторинга эксперимента «Информационная безопасность школьника». Разработанная система мониторинга позволила отслеживать развитие информационного иммунитета у обучающихся и

профессиональной компетентности в области информационной безопасности у педагогических работников [15].

Мониторинг был сформирован как многоуровневая система повторяющихся диагностических процедур, проводимых с использованием количественных методик, позволяющих максимально объективно показывать показатели развития обучающихся и педагогов.

За период работы педагогического коллектива по инновационному направлению деятельности программы освоили 416 выпускников (охват ежегодно по всей школе - от 358 обучающихся на начало проведения эксперимента, до 537 обучающихся в 2012 году) [15].

Достигнутые результаты работы гимназии с 2005 года по настоящее время:

1. Так за это время выло выявлено, что нет гимназистов, употребляющих психоактивные вещества; отсутствуют обучающиеся, состоящие на учете по потреблению ПАВ и наркотиков.

2. Выпускники гимназии не подвержены влиянию различных религиозных сект.

3. Выявлена положительная тенденция развития информационного иммунитета у обучающихся, о чем свидетельствуют данные мониторингов:

- по информационной (психологической) стрессоустойчивости;
- по степени доверия к источникам информации;
- по информационной культуре.

4. Более того, выпускники отмечают, что изучение спецкурсов по информационной безопасности позволило им

- определиться в системе нравственных ценностей;
- успешно самоопределиться для получения дальнейшего образования (поступление в вузы 99-100%);

Кроме этого хочется отметить и другие социальные эффекты инновационной работы:

– Положительные тенденции развития образовательной среды гимназии - развитие системы социального партнёрства таких направлений как Демократизация, развитие Добровольчества.

– Положительные тенденции личностно-профессионального развития педагогов.

– Создание созидательных сообществ детей и взрослых - педагогически организованных, добровольных объединений гимназистов, их родителей, педагогов, других взрослых с учетом их общей ценностно-смысловой личностной направленности, взаимопонимания, стремления созидательно решить определенные проблемы, которые являются для них личностно значимыми (Клуб выпускников гимназии, Клуб родителей, научное общество обучающихся «Интеллектуал» и т.д.).

– Положительная тенденция развития работы коллегиальных органов управления.

– Становление гимназии ресурсным, методическим центром для других образовательных учреждений муниципалитета и региона по вопросам инновационной деятельности и научно-методической поддержки педагогических кадров.

– Условия для осуществления идеи единого воспитывающего коллектива, общности на основе гуманистических ценностей, где действует досугово-культурная сеть объединений дополнительного образования гимназии и учреждений дополнительного образования города.

– Содружество выпускников школы, родительского клуба «Единство», городской общественности, основанное на традициях первой Саянской школы.

Значимым результатом явилось освоение новой внешней среды, в том числе, плодотворное сотрудничество с учреждениями – партнёрами (ОГОУ «НПУ№16» г. Байкальска, ОГОУ «Санаторный ДД №5» г. Иркутска, МОУ «Гимназия № 2» г. Иркутска) [15].

Хочется отметить, что ежегодно педагогический коллектив гимназии представлял свои инновационные разработки для профессиональной экспертизы в Экспертный совет при Министерстве образования и науки Российской Федерации. Все они получили активную поддержку. Процессы, определяющие развитие гимназического образования на сегодняшний день, позволили получить значительные изменения в воспитательной системе, обеспечить системные, устойчивые результаты благодаря практике нововведений [15].

Учреждение регулярно информирует о своей деятельности общественность города, региона, Российской Федерации. Результатом данной работы стало участие в III Всероссийском конкурсе «Организация воспитательного процесса в образовательных учреждениях» в 2006 году, на котором гимназия стала лучшей из более 1300 участников в России и получила диплом лауреата. Кроме этого, гимназия получила диплом победителя конкурса общеобразовательных учреждений, внедряющих инновационные образовательные программы в рамках ПНП «Образование» [15].

В гимназии проходила Региональная НПК «Проблемы информационной безопасности: вызовы времени» (закрытие ФЭП; регион 15.10.2011), ставшая отчетом учреждения о проделанной работе. Проблеме информационной безопасности посвящены многочисленные публикации педагогов гимназии, ее научного руководителя.

Эксперимент завершен, но и в настоящее время в учебном плане и в плане внеурочной деятельности гимназии остаются разработанные и апробированные ранее программы для обучающихся по информационной безопасности. Они позволяют педагогическому коллективу в свете современных требований в области образования обучать школьников аналитической работе с информацией, развивать у них критическое мышление, уметь оценивать достоверность информации, своевременно обнаруживать манипуляции сознанием. Обучение этому позволяет школьникам правильно организовать информационный процесс и, тем самым, оценивать и

обеспечивать свою информационную безопасность, а в конечном итоге, возможно, здоровье и жизнь [15].

Все эти результаты были достигнуты благодаря тому, что данная гимназия стала пилотной площадкой для эксперимента по ИБЛ. Но как обстоят дела в других школах, где не проводилось данного эксперимента? На основании предоставленных данных фонда развития интернет и нашего исследования выявлен низкий уровень обеспечения ИБЛ учащихся.

Анализируя выше сказанное, мы понимаем, что только лишь комплексное решение рассмотренных задач информационной безопасности личности со стороны семьи и школы позволит значительно уменьшить риски причинения различного рода ущербов (морального, материального, здоровью и др.) ребенку, один лишь ограничительный метод обеспечения информационной безопасности личности не работает. Поэтому обеспечение информационной безопасности личности школьников должно стать одним из первоочередных направлений работы современной школы и основывается на двух подходах, личностно-ресурсном и ограничительном.

Факторами обучения информационной безопасности выступает:

– содержание программы занятий по обеспечению информационной безопасности для учащихся начальной школы;

– подготовка педагогов, разработка семинаров и занятий по теме «Информационная безопасность младшего школьника»;

– подготовка родителей включит в себя: проведение тематических родительских собраний, совместные занятия с детьми;

– программа для учащихся 1-4 классов по основам информационной безопасности личности.

Таким образом, обучение информационной безопасности педагогов, родителей и учащихся, связывая объективные и субъективные закономерности и тенденции, накопление знаний в критическую массу личностных состояний, приведет к эффекту мощных позитивных прорывов на личностном уровне, которые активизируют личностный опыт и спровоцируют внутренне избранное

ребенком и индивидуально мотивированное «поступление» и умение видеть, чувствовать информационную угрозу и уметь противостоять ей [36].

1.4. Модель обеспечения информационной безопасности личности учащихся начальной школы

Сегодня в мире неконтролируемый информационный поток, который несет в себе множество различных рисков, угроз и опасностей для личности младшего школьника. Ребенок не в состоянии справиться самостоятельно с информационными угрозами. Все это подтверждается представленным выше материалом.

Существующие подходы к обеспечению информационной безопасности личности учащихся начальной школы малоэффективны и практически нигде не реализуются. В связи с этим, вопрос обеспечения информационной безопасности личности младшего школьника стоит очень остро. Для решения данной проблемы, нами разработана модель обеспечения ИБЛ учащихся начальной школы.

ИБЛ младшего школьника зависит от всех субъектов образовательного процесса. От администрации образовательного учреждения, так именно она должна одобрить внедрение программ по обеспечению информационной безопасности, организовывать безопасную информационную среду в стенах учреждения. От родителей, так как пропаганды ИБЛ лишь в стенах школы не достаточно, родители должны быть заинтересованы в обеспечении ИБЛ, обязаны организовать безопасное информационное пространство за пределами школы. От педагогов, так как они должны обучить детей основам информационной безопасности. Дать теоретические знания, практические умения и ценностные ориентации в вопросах ИБЛ.

На рисунке 3 изображена модель обеспечения информационной безопасности личности учащихся начальной школы.

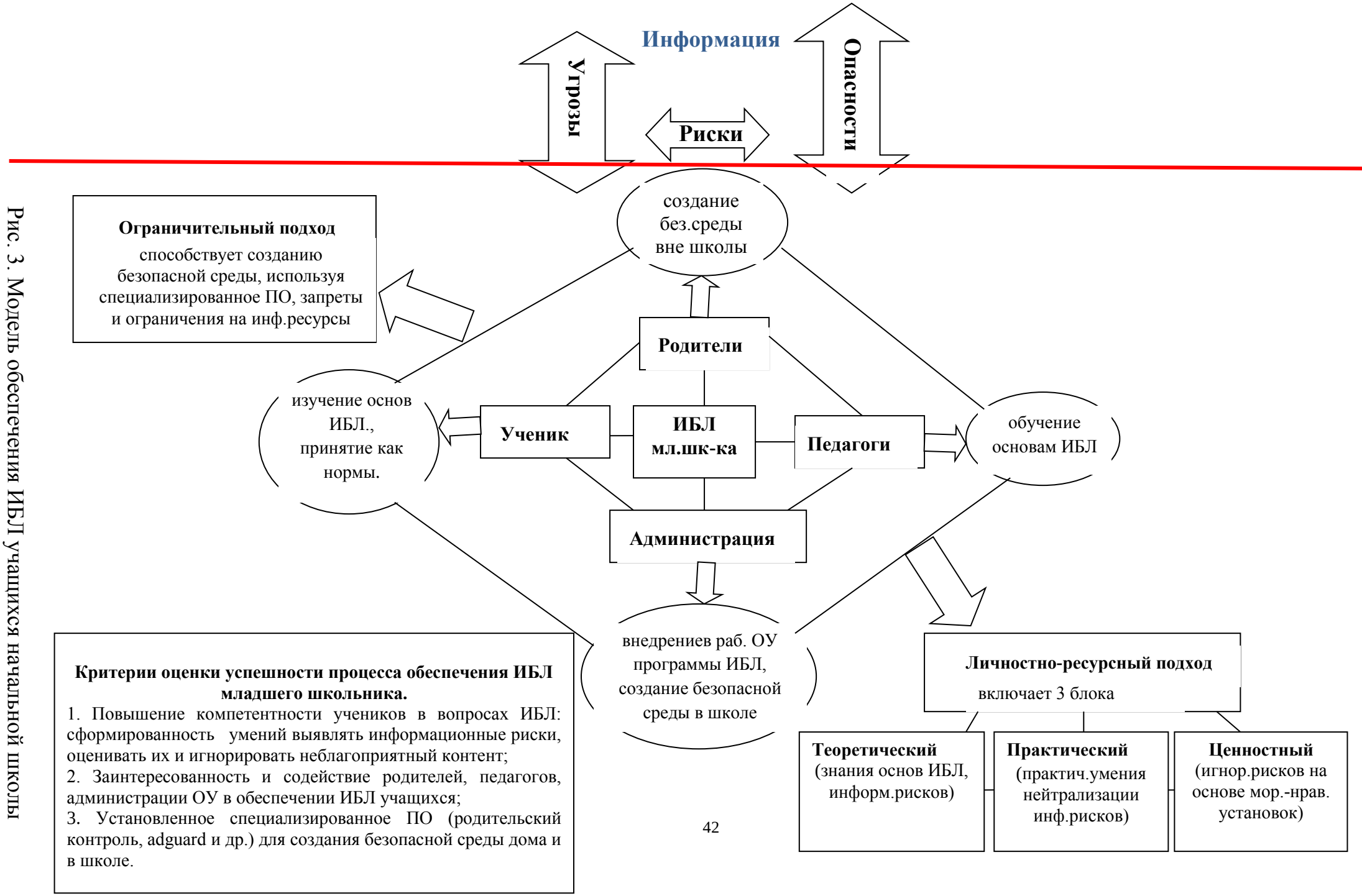

Рис. 3. Модель обеспечения ИБЛ учащихся начальной школы

Необходимо использовать два подхода к обеспечению ИБЛ младшего школьника: личностно - ресурсный и ограничительный.

Ограничительный подход способствует созданию безопасной среды, реализуется через использование специализированного программного обеспечения, запреты и ограничение на доступ к некоторым видам информационных ресурсов. Осуществляется через родителей, педагогов и администрацию учреждения.

Личностно-ресурсный подход опирается на саму личность учащегося, на его морально-нравственные принципы, чувства, знания, умения, навыки и прочие внутренние личные ресурсы. Его смысл заключается в том, чтобы ребенок понимал, что есть вредная информация (неблагоприятный контент) и не проявлял к такой информации интерес (игнорировал).

При единстве этих подходов достигается ИБЛ. Обеспечение ИБЛ в ограничительном подходе реализуется через специализированное программное обеспечение, а личностно - ресурсный строится на основе программы повышения ИБЛ личности младших школьников, которая представляет собой систему уроков, направленную на повышение знаний, практических умений и ценностных ориентиров учащихся. Иными словами включает в себя три блока: теоретический, практический, ценностный. Программа включает родительские собрания, с целью привлечения родителей к обеспечению ИБЛ младших школьников и консультирования их в вопросах ИБЛ.

Критериями оценки успешности процесса обеспечения ИБЛ младшего школьника для нас служит:

1. Повышение компетентности учеников в вопросах ИБЛ: сформированность умений выявлять информационные риски, оценивать их и игнорировать неблагоприятный контент;

2. Заинтересованность и содействие родителей, педагогов, администрации ОУ в обеспечении ИБЛ учащихся;

3. Установленное специализированное ПО (родительский контроль, adguard и др.) для создания безопасной среды дома и в школе.

Данная модель является «щитом» от информации, таящей в себе информационные риски, угрозы, опасности и способной нанести вред физическому, психическому и духовно-нравственному развитию личности.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

По данным исследований, каждый третий ребенок сталкивается с негативным контентом. Негативный контент в Интернете регулируется рядом действующих на территории РФ законов, запрещающих или ограничивающих распространение информации, причиняющей вред здоровью и развитию детей. Но полностью оградить детей от негативной информации невозможно, один лишь ограничительный метод бессилен. Поэтому необходимо ответственное и осознанное отношение к вредной информации. Это объясняет актуальность темы исследования.

В изучение проблемных вопросов информационной безопасности большой вклад внесли Федоров А. В., Федоров Д. Ю., Герасименко В. Г., Зегжда Д. П., Малюк А. А., Сычев М. П., Расторгуев С. П. и другие. Влияние информации на личность рассматривается Грачевым Г. В., Ливингстон С., Мельником И., Пейпертом С., правила безопасности детей в Интернете предложены в исследованиях Беляевой А. Б., Козак Т., Саттаровой Н. И. Вопросами информационной безопасности при применении образовательных коммуникационных технологий занимаются Морев И., Федоров А. В., Шариков А. В., проблемы информационной безопасности школьника нашли отражение в работах Переломовой Н. А., Малых Т. А. Специфику взаимодействия детей и подростков с компьютерами исследовали Пейперт С., Беляева А. В. , Коул М., Текл Ш., Новоселова С. Л. Огромный вклад в изучение вопроса информационной безопасности личности вносит Фонд развития интернет и конкретно такие ученые как Солдатова Г., Зотова Е., Лебешева М., Шляпников В.

Аспекты информационной безопасности личности находят отражение в нормативно-правовых документах РФ, в том числе и в области образования (ФГОС, профессиональный стандарт подготовки педагога, доктрина образования и прочие).

Информационная безопасность личности (ИБЛ) – состояние защищенности жизненно важных интересов личности, проявляющееся в

умении выявлять и идентифицировать угрозы информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия.

В теории и практике информационной безопасности выделяется два направления: защита информации и информационно-психологическая безопасность. Информационно-психологическая безопасность создает условия для обеспечения психического здоровья отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания, нацеленного на прогрессивное развитие общества, защита информации это защита конкретных данных.

Информационных угроз и рисков существует огромное множество (контентные, коммуникационные, потребительские, электронные). В отличие от информационного риска и информационной опасности, информационная угроза направлена против интересов субъекта в данной сфере.

При анализе существующих подходов к обеспечению ИБЛ в образовании, Петровой В., выделено два основных подхода – запретительный и личностно-ресурсный.

МБОУ «Гимназия №1» г. Саянска, Иркутской области стала федеральной экспериментальной площадкой для реализации проекта «Педагогические аспекты информационной безопасности личности». В основу данного проекта легло не только формирование умения работать с информацией, но и формирование умения обучающихся защищаться от негативного ее воздействия с раннего школьного возраста.

В своей работе мы предлагаем использовать все два подхода обеспечения. Ограничительный подход помогает создать безопасную среду и реализуется через родителей, педагогов и администрацию учреждения, а личностно-ресурсный опирается на саму личность учащегося, на его морально-нравственные принципы, чувства, знания, умения, навыки и прочие внутренние личные ресурсы. При единстве этих подходов достигается ИБЛ.

ГЛАВА 2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ПЕДАГОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ УЧАЩИХСЯ НАЧАЛЬНОЙ ШКОЛЫ

2.1. Актуальное состояние обеспечения информационной безопасности личности учащихся начальной школы

В соответствие с методологическим аппаратом исследовательской работы, нами разработан план опытно-экспериментальной работы.

План опытно-экспериментальной работы:

1. Среди классов начальной школы выделить две группы: экспериментальную и контрольную.

2. В экспериментальной группе провести опрос – анкетирование у родителей, выявляющий их уровень информированности об информационной безопасности личности, осуществить мероприятия по привлечению родителей к обеспечению ИБЛ учащихся начальной школы.

3. Провести констатирующую диагностику уровня обеспеченности информационной безопасности личности у детей двух групп.

4. Апробировать разработанную программу педагогического обеспечения информационной безопасности личности учащихся начальной школы в экспериментальной группе.

5. Осуществить контрольную диагностику обеспечения информационной безопасности личности у детей двух групп, проанализировать и сравнить результаты всех диагностик.

Характеристика выборки

Учащиеся двух классов начальной школы, 50 человек. Экспериментальная группа (3 «В» класс) – 25 человек, их родители 25, контрольная группа (3 «Б» класс) – 25 человек.

Характеристика диагностического инструментария

На начальном этапе происходит анкетирование детей и родителей.

Для детей модифицирован опросник разработанный Фондом Развития Интернет совместно с факультетом психологии МГУ имени Ломоносова М. В. и аналитическим центром Юрия Левады «Левада-Центр».

Данный опрос на основе ответов учащихся позволяет судить о сформированном уровне информационной безопасности личности, дает сведения о режиме дня школьников, об участии педагогов и родителей в обеспечении информационной безопасности личности учащихся начальной школы (см. приложение 1).

Так, например, вопросы, сколько времени, в среднем, ты проводишь в интернете в будний день и в выходной, позволяют судить о занятости учащихся, об их времяпровождении и режиме дня.

Есть вопросы, направленные на выяснение, чем занимаются дети в интернете, что они чаще всего делают в сети.

Вопрос 5,о проблемах (информационных рисках), с которыми могут столкнуться дети, выявляет, был ли у детей контакт с неблагоприятным контентом, каким именно. Ответ на данный вопрос напрямую влияет на уровень обеспеченности ИБЛ учащихся.

Имеются вопросы, которые раскрывают участие родителей и педагогов в обеспечении информационной безопасности детей.

Интерпретация результатов, происходит на основе ответов учащихся. В опросе 28 возможных ответов, которые говорят о нарушении информационной безопасности или ее недостаточном уровне. Анализируя ответы учащихся по количеству «желтых ответов», мы определяем уровень обеспечения информационной безопасности младших школьников. Низкий уровень ИБЛ, если «желтых» ответов 10 и более. Средний уровень 5-10 ответов. Высокий уровень от 0-5.

Результаты каждого ребенка, экспериментальной и контрольной групп, занесены в таблицу, которая показывает набранное количество баллов. Таблицы можно просмотреть в приложении 2.

Для удобного представления полученных данных, результаты первичного

исследования, представлены в виде диаграмм ниже.

Рисунок 4 демонстрирует результаты, полученные при первичной диагностике экспериментальной группы, в процентном соотношении.

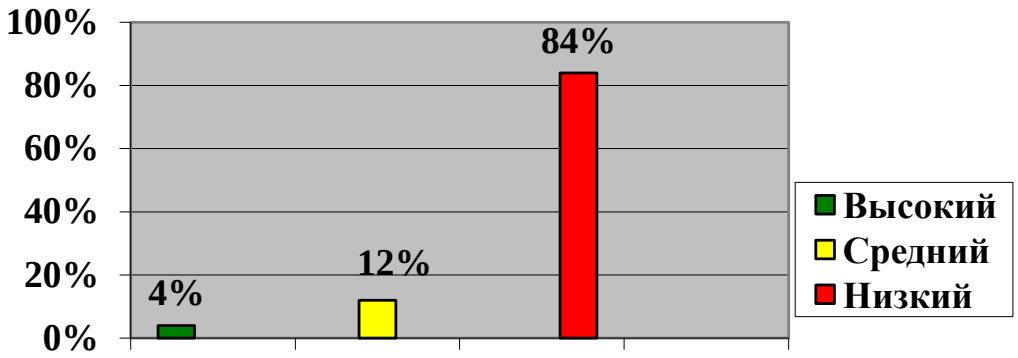

Рис. 4. Уровень информационной безопасности личности в экспериментальной группе

При первичной диагностике, в экспериментальной группе, был выявлен низкий уровень обеспеченности ИБЛ у 21 учащегося, это 84% от общего количества детей. Количество «желтых» ответов от 10 до 21. У десяти детей с низким уровнем ИБЛ, количество «желтых» ответов, превысило 15 баллов, что говорит об очень низком уровне, практически полном незнании и непонимании основ ИБЛ.

Средний уровень ИБЛ имеют 3 учащихся, от 7 до 9 баллов, это довольно большое количество баллов, поэтому этот уровень безопасности, не является оптимальным для детей, необходимо повышение, так как ребенок может столкнуться с информационными рисками и не иметь возможности с ними справиться.

Только у одного ребенка по данным диагностики высокий уровень ИБЛ. Пять баллов, это пограничное состояние, между высоким и средним уровнем, но этот ребенок более защищен, чем другие, у него больше возможностей справиться с информационными рисками и шансов обезопасить себя.

Одновременно, с диагностикой экспериментальной группы, проводилась диагностика в контрольной группе, по тому же диагностическому инструментарию.

Рисунок 5 наглядно демонстрирует результаты, полученные в ходе первичной диагностики контрольной группы.

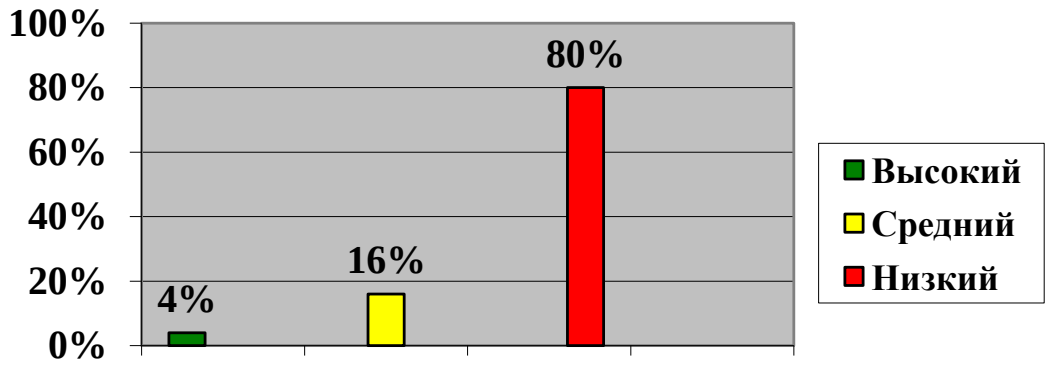

Рис. 5. Уровень информационной безопасности личности в контрольной группе

Низкий уровень обеспеченности информационной безопасности личности обнаружен у 20 учащихся, что составляет 80% от общей массы опрошенных. Результаты колеблются от 10 до 21 баллов. У 9 учащихся, количество «желтых» ответов превысило 15, это говорит об очень низком уровне ИБЛ и большой уязвимости перед информационными рисками. Средний уровень ИБЛ выявлен у 4 учащихся, высокий у одного учащегося.

При проведении сравнительного анализа результатов двух групп особых различий не выявлено. На рисунке 5 показаны результаты контрольной и экспериментальной группы в сравнении. По полученным данным можно судить о том, что учащиеся обеих групп имеют низкий уровень обеспечения информационной безопасности личности.

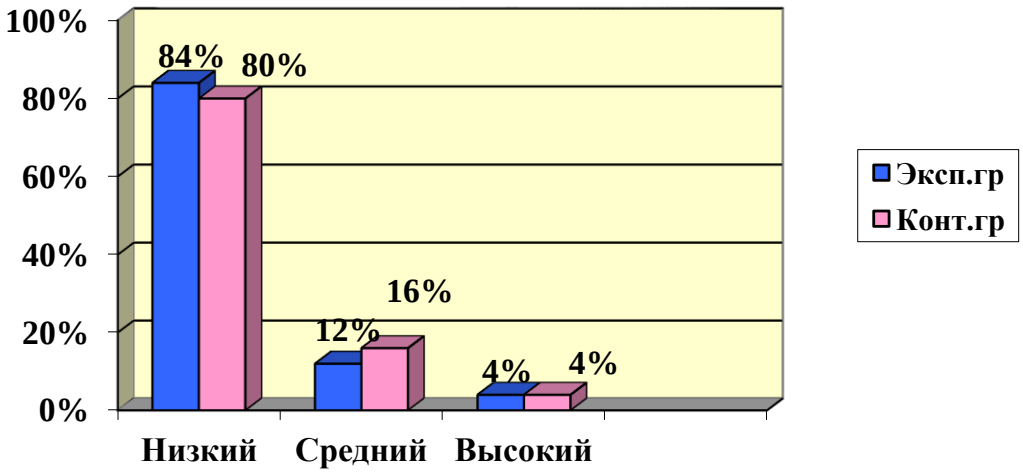

Рис. 5. Сравнение уровня ИБЛ в экспериментальной и контрольной группах на констатирующем этапе ОЭР

В экспериментальной группе 84% учащихся имеют низкий уровень ИБЛ, в контрольной 80%. Средний уровень имеют 12% в экспериментальной, 16% в контрольной группе. Высоким уровнем обладают 4% учеников, в обеих группах. В контрольной группе, результаты чуть выше, чем в экспериментальной.

Для выяснения причин такого низкого уровня обеспеченности ИБЛ младших школьников, нами разработан специальный опросник для родителей младших школьников (см. приложение 3), выявляющий общую осведомленность родителей и меры, предпринимаемые родителями для обеспечения ИБЛ ребенка. На основе ответов родителей мы делаем вывод об общем состоянии вопроса ИБЛ в семье.

Опрос включает в себя вопросы о том, что такое информационная безопасность ребёнка, чтобы выяснить имеют ли родители представление об ИБЛ. Какие меры по информационной безопасности ребёнка они предпринимают, какие знают методы и средства защиты от негативной информации и информационных рисков. Контролируют ли время, проведенное ребенком за компьютером и сайты, которые он посещает, следят ли за онлайн жизнью детей. Говорят ли с ребенком о возможных рисках и угрозах в сети.

Опрос родителей экспериментальной группы показал низкий уровень обеспечения ИБЛ младшего школьника. Опрос показал, что всего лишь 32% родителей смогли дать свое видение понятия информационная безопасность личности и эти определения не совсем соответствуют действительности.

84% родителей считают, что ограничивая время нахождения ребенка за компьютером, таким образом, принимают меры по обеспечению информационной безопасности. 8% воздержалось от ответа.

60% опрашиваемых на вопрос, знаете ли вы, как сделать общение ребёнка на компьютере безопасным и полезным ответили, нет, что свидетельствует о низком уровне осведомленности большинства родителей.

36% осведомлены о неблагоприятных факторах воздействия ИКТ на ребенка, остальные 64% оставили вопрос без ответа.

100% родителей говорит, о том, что дети проводят все свое время за компьютером, пользуясь при этом интернетом.

У 80% опрошенных не установлено никаких программных средств для обеспечения ИБЛ. У 12% стоит родительский контроль. 8% оставили вопрос без ответа.

84% опрошенных, отмечают частые конфликты с детьми из-за компьютера и доступа к сети интернет.

84% родителей следят за временем, проводимым их детьми за компьютером. 64% родителей не контролируют сайты посещаемые детьми.

Таким образом, мы видим, что дети и их родители имеют низкий уровень знаний об информационной безопасности личности. Полученные данные свидетельствуют о необходимости и важности формирующего этапа опытно-экспериментальной работы. Разработанная программа позволит привлечь родителей к обеспечению ИБЛ учащихся, а система занятий для детей будет способствовать повышению их уровня информационной безопасности личности.

2.2. Характеристика и особенности формирующего этапа

Для обеспечения информационной безопасности личности учащихся начальной школы, нами была разработана программа «Азбука безопасности». Программа представляет собой систему занятий, направленную на обеспечение информационной безопасности личности учащихся, путем привития им навыков ответственного и безопасного поведения в сети Интернет. В программу входит 31 час занятий с учащимися, где он изучают и практически прорабатывают различные аспекты информационной безопасности личности. Также в программу входят часы для родителей, 2 обязательных родительских собрания, а также раз в неделю, в рамках программы, выделен час для индивидуального консультирования родителей по вопросам обеспечения ИБЛ младшего школьника. По общей договоренности родителей и администрации школы предусмотрен рейд «Безопасный интернет дома». Программа рассчитана на проведение одного занятия раз в неделю в течение года, но в условиях опытно-экспериментальной работы, а точнее ограниченности времени, занятия проводились два раза в неделю.

Задачи программы:

1) информировать учащихся и родителей об информации, которая способна причинить вред их здоровью и развитию, а также о возможных негативных последствиях распространения такой информации;

2) обучить детей правилам ответственного и безопасного использования сети Интернет, способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях;

3) привлечь родителей к обеспечению информационной безопасности личности учащихся начальной школы.

Ожидаемый результат от использования данной программы:

- учитель получит возможность проводить уроки-безопасности, используя программу, современные методические и технологические подходы;

- родители получат практические материалы, знакомство с которыми поможет им более грамотно организовать общение с детьми при обсуждении проблем, связанных с интернетом.

- в ходе занятий учащиеся научатся делать более безопасным и полезным свое пребывание в сети Интернет и других информационно-телекоммуникационных сетях, а именно:

– критически относиться к информации, распространяемой в сети Интернет и других телекоммуникациях;

– отличать достоверные сведения от недостоверных, распознавать вредную для них информацию;

– избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;

– распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;

– критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;

– анализировать степень достоверности информации и подлинность ее источников;

– применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях [55].

Разработанная нами система занятий направлена на решение всех выше перечисленных задач и способствует получению выше изложенных результатов.

Согласно календарно-тематическому планированию, в котором отражены темы занятий, содержание и количество часов для изучения материала с учащимися, мы приступили к реализации программы «Азбука безопасности» в экспериментальной группе (см. приложение 4).

Первым нашим шагом было проведение родительского собрания для родителей учащихся экспериментальной группы. На данном собрании мы затронули вопрос о том, что такое ИБЛ, как ее обеспечить и почему это так важно. Мы рассказывали о важности обеспечения информационной безопасности детей, о возможных рисках и угрозах в сети интернет, о том, что одна школа не в состоянии до конца решить вопрос ИБЛ, необходима слаженная работа родителей и школы. Родители согласились с актуальностью этого вопроса и проявили желание и готовность участвовать в ее реализации. Обсудили возможность проведения рейда «Безопасный интернет дома», выбрали представителя от имени родителей, который будет участвовать в организации и проведении рейда.

Следующим шагом для нас стало проведение обучающих занятий с детьми и постоянное консультирование родителей в вопросах обеспечения ИБЛ, а также непосредственная организация рейда.

После согласования организационных моментов, мы приступили к проведению занятий у учащихся. Пятого сентября было проведено первое занятие. Темой занятия стала «Информационная безопасность личности: зачем и почему?» Где рассматривалось понятие информационной безопасности, зачем она нужна и цели и задачи нашего курса. Была выбрана эмблема для наших занятий.

Занятие 2. Цифровая грамотность и цифровая компетентность. Рассматривали грамотность и компетентность в информационном мире.

Занятие 3. Безопасное подключение. Будь хозяином своей безопасности. Как обезопасить свое интернет пространство. Безопасное подключение, как и зачем?

Занятие 4-5. Угрозы и опасности сети. Изучали, какие риски и угрозы существуют, как нужно вести себя в сети интернет, что бы ни накликать беду, на эту тему выделено 2 часа, так как информационных рисков и угроз существует огромное множество.

Занятие 6-7. Профилактика рисков и угроз. Способы защиты и реагирования на возможные угрозы; выработка алгоритма действий.

Занятие 8. Зависимость, какая она, от чего возникает? Люди, которые играют в игры. В данной теме, познакомились с понятием «зависимость», узнали меры по борьбе с зависимостью, рассмотрели признаки зависимости , рисовали зависимого человека и анализировали свое окружение на предмет зависимости.

В параллель работе с учащимися, мы проводили рейд «Безопасный интернет дома». По договоренности родителей и администрации школы. В школе работает мастер-программист, который на ПК и ноутбуки в домах учащихся установил специализированное программное обеспечение, способствующее защите учащихся от воздействия неблагоприятного контента. По итогам рейда, программное обеспечение было установлено в 24 квартирах, на 32 устройствах.

Занятие 9. Режим дня и место гаджетов в режиме. Планирование режима дня, гаджеты в нашей жизни. В рамках этой темы, каждый ребенок разрабатывал свой режим дня, с учетом использования различного рода гаджетов, каждый ребенок смог подсчитать, сколько времени «незаметно» он тратит на «электронных товарищей» и сделать выводы о пересмотре режима, с учетом здоровье сбережения.

Занятие 10-11. Социальные сети. Социальные сети, безопасность, поведение, правила, вот все аспекты затрагиваемой темы. На данных занятиях мы познакомились с социальными сетями, узнали, какие используют младшие школьники, обсудили возможные угрозы и правила поведения в сети, также затронули этикет в онлайн пространстве.

Занятие 12. Защита личных данных и другой конфиденциальной информации в Интернете. Как защитить личные данные и обезопасить себя. Поговорили о надежных паролях, пробовали их составлять.

Занятие 13. О чем стоит поделиться с взрослыми? Что нужно рассказать взрослым, рассмотрение ситуаций, которые ребенок не может решить без помощи взрослых, почему помощь взрослых важна? Не надо бояться.

Занятие 14. Урок-сказка «Жизнь в интернет пространстве». Повторение правил безопасного нахождения в интернете путем обыгрывание сказки с привычными героями в непривычной ситуации.

Занятие 15. Средства поиска информации в Интернете. Знакомство с поисковыми системами. С особенностями поиска в сети.

Занятие 16-17. Поиск информации в интернете. Учимся поиску в сети, выбираем лучшее.

Занятие 18. Достоверность информации . Как определить и понять, можно верить или нет? Достоверные интернет источники.

Занятие 19. Осторожно?! Интернет. Какие бывают риски и способы реагирования на них. Урок организации безопасности.

Занятие 20. Способы защиты от негативной информации. Как защитить себя от негативной информации, что относится к негативной информации.

Занятие 21-22. Онлайн общение. Правила общения в сети.

Занятие 23. Кибербезопасность. Занятие в игровой форме «интернет-турнир», а также прохождение тест на компьютерную зависимость.

Занятие 24. Интернет мошенничество. Чего ждать и как избежать неприятностей. Реклама, пиратство, взлом.

Занятие 25. Правила поведения в интернете: безопасность в твоих руках. Повторение основных видов угроз, правил поведения.

Занятие 26. Викторина «Что я знаю о безопасной работе в интернете?». Проверка усвоенных знаний, закрепление.

Занятие 27. Вирусы. Рассматриваем виды вирусных программ и как от них спастись. Эффективные средства и методы защиты от вирусов.

Занятие 28-29. Полезные сайты. Составление каталога рекомендованных сайтов для младшего школьного возраста.

Занятие 30. Игра-путешествие «Безопасный интернет». Закрепление пройденного материала.

Родительское собрание 2. Обсуждение методов и средств обеспечение ИБЛ ребенка дома. Выступление специалиста устанавливающего ПО, в котором он еще раз подробно показывает и рассказывает о том, как оно работает. Приглашение родителей на открытый урок по информационной безопасности.

Занятие 31. Обобщение: чему научились? Что узнали? Подведение итогов. Открытый урок-театрализованное представление, в ходе которого, учащиеся примеряют на себя роль членов правительства, которые отчитываются по информационной безопасности (о ее значимости и важности) в различных жизненных сферах.

Особенностью данной программы является, то, что она рассчитана на младший школьный возраст. Все занятия программы, построены с учетом интересов учащихся, используются игровые формы, а также возможность проявления самостоятельности и инициативы, поиск самостоятельных ответов, опора на личный опыт. Полностью программу, с занятиями, можно увидеть в приложении 4.

Данная программа вызвала большой интерес у учащихся, так как дети вели себя очень активно, с желанием работали на каждом занятии, делились своим опытом и задавали вопросы.

Мы отгадывали загадки, изучали правила безопасности в стихотворной форме. Смотрели тематические мультфильмы и видео, касающиеся информационной безопасности. Но помимо игр и забав, мы изучали особенности поиска, учились отличать верную информацию от неверной, составляли свой собственный каталог полезных интернет ресурсов и многое другое.

Большой успех получила игра-путешествие «Интернет безопасность», в которой был собран весь изучаемый материал, она стала своеобразным итогом нашей работы с учениками, так как задания и вопросы в ходе занятия,

требовали не только теоретических знаний, но и практических умений учащихся, которыми мы овладевали на протяжении курса наших занятий.

В ходе работы с детьми, велась постоянная консультация родителей по возникающим у них вопросам обеспечения ИБЛ детей. Еженедельно за консультацией обращалось 3-7 родителей.

2.3 Результаты опытно-экспериментальной работы

По завершению формирующего этапа опытно-экспериментальной работы нами был проведен контрольный этап. На данном этапе проводилась диагностика текущего состояния информационной безопасности личности и сравнение результатов с результатами констатирующего этапа, для определения эффективности или не эффективности разработанной нами программы обеспечения ИБЛ.

Диагностика на контрольном этапе проводилась тем же инструментарием, что на констатирующем этапе, с помощью модифицированного нами опросника, разработанного Фондом Развития Интернет совместно с факультетом психологии МГУ имени М. В. Ломоносова и аналитическим центром Юрия Левады «Левада-Центр».

Подробные результаты, полученные в ходе исследования, можно увидеть в приложении 5, а также они представлены на рисунках ниже.

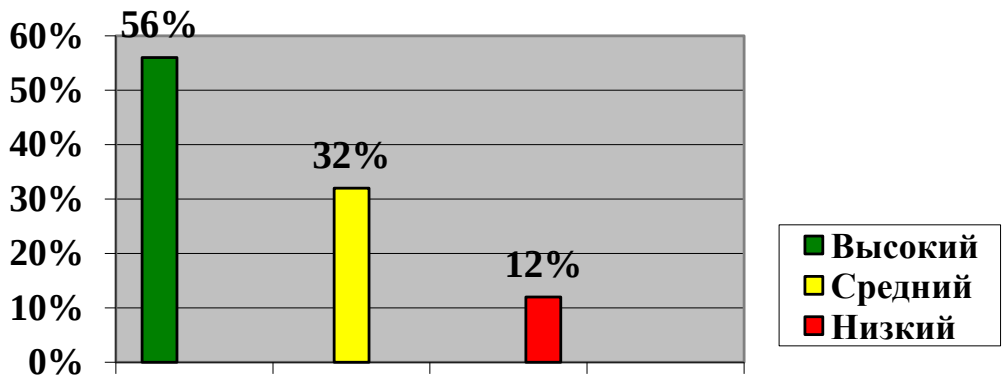

Рис. 6. Уровень информационной безопасности личности в экспериментальной группе на контрольном этапе ОЭР

Учащихся с низким уровнем информационной безопасности осталось трое, это 12% от общего количества. Средний уровень на сегодня имеют 8 учащихся. Высоким уровнем стали обладать 14 учащихся. А до начала эксперимента только лишь один ребенок имел высокий уровень обеспеченности ИБЛ. Это свидетельствует о значительном улучшении обеспечения информационной безопасности личности.

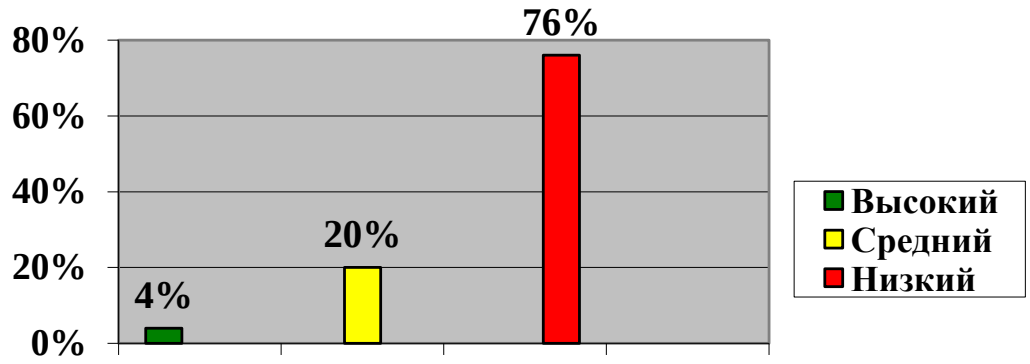

Рис. 7. Уровень информационной безопасности личности в контрольной группе на контрольном этапе ОЭР

В контрольной группе особых изменений у учащихся нет. Учащихся с низким уровнем ИБЛ 20 человек. Средний уровень имеют 4 учащихся. Высокий уровень у одного ребенка. Это подтверждает наши мысли о том, что если не предпринимать никаких мер в обеспечении информационной безопасности сама она в младшем школьном возрасте развиваться не будет.

По полученным данным в экспериментальном классе показатели обеспеченности информационной безопасности значительно выросли. В контрольном классе остались практически без изменений.

Полученные нами данные, доказывают, что если в процесс обеспечения ИБЛ включены все субъекты образования (ученики, родители, педагоги, администрация), организована безопасная информационная среда для учащихся, дома и в школе, по средствам специализированного программного обеспечения, с учащимися проводятся занятия, на которых изучаются вопросы информационной безопасности, родителям оказывается своевременная

информативная помощь в вопросах обеспечения ИБЛ детей, ведется работа по их привлечению к процессу обеспечения, все это положительно влияет на информационную безопасность личности учащихся начальной школы и повышает их уровень информационной безопасности.

Таблица 1

Сравнение результатов экспериментальной группы до и после ОЭР

Уровни	**До**	**После**
Низкий	21	3
Средний	3	8
Высокий	1	14

Если на констатирующем этапе в экспериментальном классе было учащихся с низким уровнем 21, то на контрольном осталось, лишь 3 учащихся. Учащихся со средним уровнем было 3, стало 8. Высокий уровень ИБЛ на констатирующем этапе показал 1 ребенок, после завершения опытно-экспериментальной работы высокий уровень ИБЛ у 14 учащихся.

Для наглядной демонстрации результатов работы, они представлены на рисунке 8. Он показывает результаты экспериментальной группы на констатирующем и контрольном этапах в сравнении.

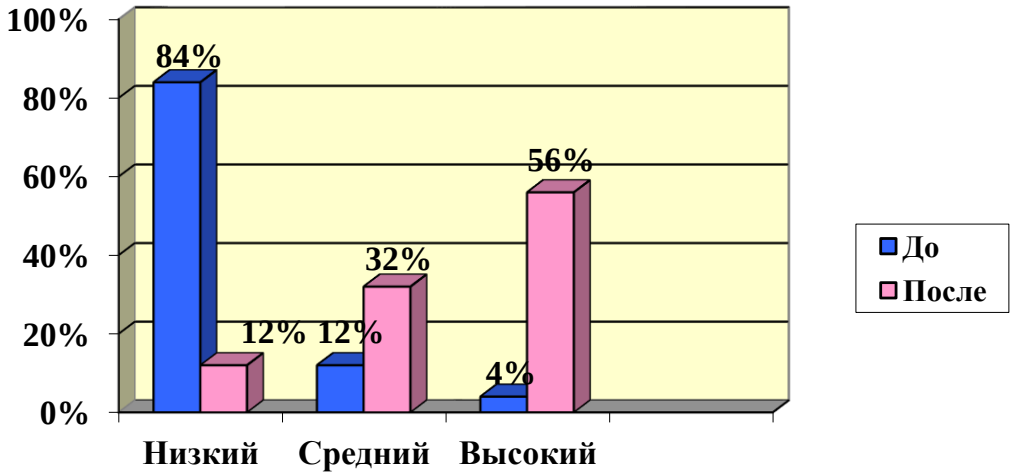

Рис. 8. Уровень информационной безопасности личности экспериментальной группы на констатирующем и контрольном этапах

Полученные результаты были достигнуты благодаря слаженной работе администрации школы (внедрение программы, проведение рейда «Безопасный

интернет дома»), педагогов (обучение учащихся и консультирование родителей в вопросах ИБЛ), родителей (активное и добровольное участие в обеспечении ИБЛ), учащихся (так как они с удовольствием и интересом изучали предлагаемый материал). Все это привело к повышению компетентности учеников, родителей и педагогов в вопросах ИБЛ. Они научились видеть информационные риски, оценивать их и игнорировать неблагоприятный контент, который приводит к возникновению таких рисков. Несомненно, большое значение, имеет установленное специализированное программное обеспечение (родительский контроль, adguard и др.) для создания безопасной среды учащихся, так оно в разы снижает возможность столкновения учащихся с неблагоприятным контентом.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

В ходе опытно-экспериментальной работы, на констатирующем этапе, разработан диагностический инструментарий и проведена диагностика уровня информационной безопасности личности у учащихся. Проведен опрос родителей, направленный на выявление осведомленности их в вопросах обеспечения ИБЛ детей.

По результатам диагностических материалов стало понятно, что осведомленность родителей и уровень обеспечения информационной безопасности находятся на очень низком уровне. Дети ежедневно сталкиваются с информационными рисками, но не в состоянии с ними справиться, родители не могут оказать детям поддержку в этих вопросах, так как не обладают нужными знаниями.

Нами разработана программа «Азбука безопасности», в рамках которой, происходит обучение учащихся и привлечение родителей к обеспечению информационной безопасности, их консультирование по вопросам информационной безопасности.

Дома и в школе создается безопасная среда по средствам специализированного программного обеспечения, которое устанавливается при проведении рейда «Безопасный интернет дома», в рамках нашей программы. В школе проводятся специализированные обучающие занятия для детей. Им рассказывают о возможных рисках, угрозах, о том, как надо себя вести в сети интернет, все это делается не только на словах, но отрабатывается практически, чтобы по окончанию занятия, у ребенка сформировался свой ценностный взгляд и появился практический опыт в создании и поддержке своей информационной безопасности.

Проводятся родительские собрания по информационной безопасности, постоянно происходит консультирование родителей в рамках программы.

После апробации программы, был проведен контрольный замер состояния ИБЛ учащихся, который выявил значительное повышение уровня информационной безопасности. Тем самым, доказывает нашу гипотезу, о том,

что если ИБЛ младшего школьника понимать как состояние защищенности личности от информационных угроз, поддерживаемое безопасностью среды и морально-ценностными установками личности и сам процесс обеспечения ИБЛ строить системно на основе сочетания двух подходов: ограничительном и личностно-ресурсном. В обеспечение ИБЛ задействовать всех субъектов образовательного процесса (детей, учителей, родителей, администрацию), то это будет способствовать созданию безопасной среды и повышению уровня обеспеченности ИБЛ начальной школы.

ЗАКЛЮЧЕНИЕ

В ходе исследования была выделена актуальная проблема, связанная с недостаточной разработанностью в современной науке практических способов и средств обеспечения информационной безопасности учащихся начальной школы.

Для разрешения данной проблемы мы теоретически обосновали, разработали и апробировали систему обеспечения информационной безопасности личности учащихся начальной школы. Определи сущность понятия «информационная безопасность личности» в современной науке и образовательной практике. Изучили и охарактеризовали информационные риски для развития личности младшего школьника, установили связь понятий: риск, опасность, угроза. Проанализировали педагогический опыт и подходы к обеспечению ИБЛ младшего школьника в образовательной практике. Разработали свою модель обеспечения ИБЛ младшего школьника. Разработали программу, включающую систему занятий для младших школьников по информационной безопасности, работу с родителями по информационной безопасности. Проверили эффективность разработанных материалов в ходе опытно-экспериментальной работы.

Выдвинутая гипотеза полностью доказана. Мы доказали, что ИБЛ учащихся начальной школы обеспечивается при выполнении следующих условий:

ИБЛ младшего школьника понимается как состояние защищенности личности от информационных угроз, поддерживаемое безопасностью среды и морально-ценностными установками личности.

Процесс обеспечения ИБЛ строится системно на основе сочетания двух подходов: ограничительном подходе, через создание безопасной среды в школе и дома, с помощью рейда «Безопасный интернет дома» в рамках программы, и личностно-ресурсном, через обучение ребенка адекватному восприятию и оценке информации, ее критическому осмыслению на основе нравственных и культурных ценностей. Данное направление реализовалось через

разработанную программу обеспечения информационной безопасности, которая включает в себя 31 занятие, направленное на обучение учащихся распознавать и реагировать на информационные угрозы, так чтобы минимизировать причинение информацией вреда их здоровью и физическому, психическому, духовному, нравственному развитию. И родительские собрания и консультации для родителей, с целью привлечения их к процессу обеспечения ИБЛ учащихся начальной школы.

В обеспечении ИБЛ задействовались все субъекты образовательного процесса: дети, учителя, родители, администрация школы.

Критериями оценки успешности процесса обеспечения ИБЛ младшего школьника: повышение компетентности учеников, родителей и педагогов в вопросах ИБЛ: сформированность у субъектов образовательного процесса умений выявлять информационные риски, оценивать их и игнорировать неблагоприятный контент; установленное специализированное программное обеспечение (родительский контроль, adguard и др.) для создания безопасной среды в школе и дома.

Для подтверждения гипотезы, нами изучено понятие информационной безопасности личности в теории и образовательной практике. Рассмотрены и проанализированы виды информационных рисков, угроз, опасностей, установлена связь между этими понятиями. Проанализированы существующие подходы и опыт обеспечения информационной безопасности личности.

Разработана собственная модель обеспечения информационной безопасности личности. Адаптирован и модифицирован опросник для учащихся начальной школы, разработанный Фондом Развития Интернет совместно с факультетом психологии МГУ имени М. В. Ломоносова и аналитическим центром Юрия Левады «Левада-Центр». Разработан опрос для родителей по информационной безопасности. На основе разработанной модели обеспечения ИБЛ, создана программа по информационной безопасности «Азбука безопасности», включающая в себя работу с учениками и родителями, с целью привлечения их к обеспечению ИБЛ учащихся.

Полученные результаты в ходе ОЭР, доказывают, что если в процесс обеспечения ИБЛ включены все субъекты образования (ученики, родители, педагоги, администрация), организована безопасная информационная среда для учащихся, дома и в школе, по средствам специализированного программного обеспечения, с учащимися проводятся занятия, на которых изучаются вопросы информационной безопасности, родителям оказывается своевременная информативная помощь в вопросах обеспечения ИБЛ детей, ведется работа по их привлечению к процессу обеспечения, все это положительно влияет на информационную безопасность личности учащихся начальной школы и повышает их уровень обеспеченности информационной безопасности.

В дальнейшем работа может быть продолжена в обеспечении информационной безопасности личности старших школьников, в разработке курсов по ИБЛ для педагогов.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ) [Текст] // Российская газета. – 21.01.2009. – № 7.

2. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) [Текст] // Российская газета. – 28.09.2000. – № 187.

3. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года» [Электронный ресурс] / Законодательная база Российской Федерации – Режим доступа: http://zakonbase.ru/content/nav/134726 (дата обращения 15.03.2015).

4. Федеральные государственные образовательные стандарты [Электронный ресурс] / Министерство образования и науки Российской Федерации – Режим доступа: http://минобрнауки.рф/документы/336 (дата обращения 16.03.2015).

5. Федеральный закон от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Текст] // Российская газета – 2010. – №5376. – дек.

6. Национальная доктрина образования в Российской Федерации (утв. постановлением правительства РФ от 4 октября 2000 г. №751.) [Электронный ресурс] / Российская газета – Режим доступа: https://rg.ru/2000/10/11/doktrina-dok.html (дата обращения 14.03.2015).

7. Брагин, И. А., Чесноков, Н. А., Асеев, А. Ю. Педагогический аспект информационной безопасности [Текст] // Вестник Череповецкого государственного университета. – 2014. – №5 (58). – С. 89 – 92.

8. Баженова, Л. М. Медиаобразование школьника (1- 4 классы) [Текст] / Л. М. Баженова. – М.: Изд-во Ин-та художественного образования Российской Академии образования, 2004. – 55 с.

9. Батаева, И. П. Защита информации и информационная безопасность [Текст] // НиКа. – 2012. – № 1 . – С.116 – 118.

10. Басанова, Т. А. Представления студентов вуза об информационно-психологической безопасности и пути их трансформации [Текст]: Автореф. дисс. … канд. психол. наук. – Ставрополь, 2007. – 24 с.

11. Белов, Е. Б. Основы информационной безопасности: учебное пособие для высших учебных заведений [Текст] / Е. Б. Белов. – М.: Дрофа, 2006. – 544 с.

12. Богатырева, Ю. И. Непрерывная подготовка личности к обеспечению информационной безопасности [Текст] // Территория науки. – 2014. – №6. – С. 6 – 10.

13. Владимиров, В. А. Информационная безопасность личности [Текст] // Молодой ученый. – 2015. – №11. – С. 1294 – 1298.

14. Воронов, Р. В., Гусев, О. В., Поляков, В. В. О проблеме обеспечения безопасного взаимодействия с образовательными ресурсами [Текст] // Открытое образование. – 2008. – № 3. – С.18 – 21.

15. Выступление директора МБОУ «Гимназия №1» г. Саянска Иркутской области от 17.08.2012 г. Из опыта работы образовательного учреждения по информационной безопасности личности школьника [Электронный ресурс] / МОУ «Гимназия им. В. А. Надькина» – Режим доступа: http://1gim.ru/index/vystuplenie_direktora_mbou_gimnazija_1_g_sajanska_irkutskoj_oblasti_na_antinarkoticheskoj_komissi/0-81 (дата обращения 21.04.16).

16. Гафарова, Г. Г., Смелянская В. В. Информационная безопасность личности [Текст] // Сборник конференций НИЦ Социосфера. – 2012. – № 21. – С. 56 – 58.

17. Горбунова, Л. Н. Здоровье и безопасность детей в мире компьютерных технологий и интернет [Текст] / Л. Н. Горбунова. – М.: Солон-пресс, 2010. – 174 с.

18. Громов, Ю. Ю. Информационная безопасность и защита информации: Учебное пособие [Текст] / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. – Ст. Оскол: ТНТ, 2010. – 384 с.

19. Грачев, Г. В. Информационно-психологическая безопасность личности - состояние и возможности психологической [Текст] // ЛитМир, Электронная библиотека. – 31 с.

20. Грачев, Г. В. Информационно-психологическая безопасность личности [Текст]: Автореф. дис. ... док. пед. наук. – Москва, 2000. – 10 с.

21. Губанов, В. М., Михайлов, Л. А., Соломин, В. П. Чрезвычайные ситуации социального характера и защита от них [Текст] / В. М. Губанов, Л. А. Михайлов. – М.: Сфера, 2007. – 288 с.

22. Ежевская, Т. И. Психологическое здоровье как значимый ресурс информационно-психологической безопасности личности [Текст] // Гуманитарный вектор. Педагогика и психология. – 2012. – №1. – С. 205 – 210.

23. Ершов, Д. А., Аверина, С. Н. Информационная безопасность личности как цель социально-педагогической деятельности [Текст] // Актуальные проблемы семейной педагогики. – 2012. – № 1. – С. 73 – 78.

24. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография [Текст] / Л. Л. Ефимова, С. А. Кочерга. – М.: ЮНИТИ-ДАНА, 2013. – 239 с.

25. Желязков, Е. И., Авдеева, Н. В. Анализ современного состояния изучения вопросов информационной безопасности в школьном курсе [Текст] // Молодой ученый. – 2013. – № 6. – С. 666 – 669.

26. Жук, Е. И. Концептуальные основы информационной безопасности [Текст] // Наука и образование. – 2010. – №4. – апр. – С. 36 – 41.

27. Занько, Н. Г., Малаян, К. Р. Безопасность жизнедеятельности: учебное пособие [Текст] / под ред. О. Н. Русака. – 5-е изд. – СПб.: Литер, 2002. – 230 с.

28. Заряна и Нина Некрасовы Как оттащить ребенка от компьютера и что с ним делать [Текст] / Заряна и Нина Некрасовы. – София, 2007. – 56 с.

29. Ильичев, И. Е. Проблемы обеспечения информационной безопасности личности, общества и государства в современной России [Текст] // ППД. – 2015. – №2. – С.13 – 24.

30. Камышев, Э. Н. Информационная безопасность и защита информации: учебное пособие [Текст] / Э. Н. Камышев. – Томск: ТПУ, 2009. – 95 с.

31. Кисляков, П. А. Социальная безопасность личности: функциональные компоненты и направления формирования [Текст] // Современные исследования социальных проблем. – 2012. – №5. – С. 23.

32. Ковалева, Н. Н. Информационное право России: учебное пособие [Текст] / Н. Н. Ковалева. – М.: «Дашков и Ко», 2007. – 148 с.

33. Коровяковский, Д. Г. Национальная безопасность России и терроризм. Национальные интересы России в информационной сфере и их обеспечение в условиях терроризма [Текст] // Национальные интересы: приоритеты и безопасность. – 2005. – № 2. – С. 52 – 61.

34. Леончиков, В. Е. Информационная свобода и информационная безопасность в системе непрерывного образования [Текст] // Информационная свобода и информационная безопасность: Материалы междунар. научно-практич. конференции. – Краснодар, 2001. – С. 336 – 338.

35. Лопатин, В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества [Текст] / В. Н. Лопатин. – М.: Дрофа, 2000. – 428 с.

36. Малых, Т. А. Педагогические условия развития информационной безопасности младшего школьника [Текст]: Автореф. дис. … канд. пед. наук. – Иркутск, 2008. – 23 с.

37. Малых, Т. А. Педагогические аспекты информационной безопасности [Текст] // Народное образование. – 2007. – № 5. – С. 231 – 236.

38. Малых, Т. А. Наши дети во всемирной паутине Интернета [Текст] // Начальная школа плюс До и После. – 2007. – № 7. – С. 8 – 11.

39. Малых, Т. А. Информационная безопасность молодого поколения [Текст] // Профессиональное образование. Столица. – 2007. – № 6. – С. 30.

40. Марков, А. А. Понятие и характеристика информационных рисков, опасностей и угроз в современном постиндустриальном обществе [Текст] // Вестник ВолГУ. Серия 7: Философия. Социология и социальные технологии. – 2010. – №1. – С.123 – 129.

41. Непомнящий, А. В., Познина, Н. А. Перспективы повышения информационной безопасности личности путём развития сознания [Текст] // Известия ЮФУ. Технические науки. – 2010. – №11. – С. 232 – 238.

42. Нургалиева, Г. К., Есжанов, А. Е. Педагогический словарь терминов и определений в области информатизации образования [Текст] / Г. К. Нургалиева, А. Е. Есжанов. – Алматы, 2010. – 52 с.

43. Перевозчикова, М. С., Сапегин, А. Н. Способы контроля доступа школьников к компьютерным ресурсам [Текст] // Концепт. – 2014. – №10. – С. 56 – 60.

44. Петренко, С. А. Управление информационными рисками [Текст] / С. А. Петренко. – М.: Компания АйТи; ДМК Пресс, 2009. – 384с.

45. Петрова, А. К., Кобелева, Е. Е. Информационная безопасность школьника в образовательном учреждении [Текст] // Сборники конференций НИЦ Социосфера. – 2012. – №8. – С. 366 – 372.

46. Петрова, В. А. Специальные компетенции педагога «новой формации» [Текст] // НОВЫЕ ИДЕИ – НОВЫЙ МИР: сборник научных работ молодых ученых. – Тюмень: Издательство «Печатник», 2015. – С. 98 – 101.

47. Плетнев, П. В., Белов, В. М. Методика оценки рисков информационной безопасности на предприятиях [Текст] // Доклады ТУСУР. – 2012. – № 1 – 2. – С. 83 – 86.

48. Родичев, Ю. Информационная безопасность: Нормативно-правовые аспекты [Текст] / Ю. Родичев. – СПб: Лотос, 2008. – 272 с.

49. Саттарова, Н. И. Информационная безопасность школьников в образовательном учреждении [Текст]: Автореф. дис. ... кан. пед. наук. – СПб, 2003. – 13 с.

50. Серебряник, Е. Э. Формирование информационно-личностной безопасности школьника [Текст] // Вестник Балтийского федерального университета им. И. Канта. Серия: Филология, педагогика, психология. – 2010. – №11. – С.140 – 143.

51. Солдатова, Г. У., Зотова, Е. Ю., Лебешева, М., Шляпников, В. Интернет: возможности, компетенции, безопасность: Методическое пособие для работников системы общего образования [Текст] / Г. У. Солдатова, Е. Ю. Зотова, М. Лебешева, В. Шляпников. – М.: Google, 2013. – 165 с.

52. Солдатова, Г. У., Нестик, Т. А., Рассказова, Е. И., Зотова, Е. Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования [Текст] / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. – М.: Фонд Развития Интернет, 2013. – 144 с.

53. Тазин, И. И. Правовое обеспечение информационно-психологической безопасности несовершеннолетних [Текст] // Вестник ТГПУ. – 2012. – №6. – С. 220 – 225.

54. Тимошенко, Т. В. Когнитивные аспекты информационно-психологической безопасности личности [Текст] // Известия ЮФУ. Технические науки. – 2010. – №9. – С. 185 – 188.

55. Федоров, А. В. Медиаобразование: история, теория и методика [Текст] / А. В. Федоров. – Ростов-на-Дону: ЦВВР, 2001. – 708 с.

56. Федоров, А. В. Словарь терминов по медиаобразованию, медиапедагогике, медиаграмотности, медиакомпетентности [Текст] / А. В. Федоров. – Таганрог: Изд-во Таганрогского государственного педагогического института, 2010. – 64 с.

57. Фонд Развития Интернет: «Дети в информационном обществе» [Электронный ресурс] / Фонд развития Интернет – Режим доступа: http://www.fid.su/news/ (дата обращения 15.06.16).

58. Хлопьев, А. Т. Средства массовой информации как источник информационно-психологической неустойчивости [Текст] // Проблемы информационно психологической безопасности. – М.: Институт психологии РАН, 2006. – С. 47 – 52.

59. Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Текст] / А. Ю. Щербаков. – М.: Книжный мир, 2009. – 352с.

60. Ямбург, Е. А. Что принесёт учителю новый профессиональной стандарт педагога? [Текст] / Е. А. Ямбург. – М.: Просвещение, 2014. – 175 с.

61. Ярочкин, В. И. Информационная безопасность: учебник для ВУЗов [Текст] / В. И. Ярочкин. – М.: Фонд «Мир»: Акад. проект, 2010. – 639 с.