МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФАКУЛЬТЕТ ПОДГОТОВКИ УЧИТЕЛЕЙ НАЧАЛЬНЫХ КЛАССОВ
КАФЕДРА ПЕДАГОГИКИ, ПСИХОЛОГИИ И ПРЕДМЕТНЫХ МЕТОДИК

Формирование основ кибербезопасности у младших школьников во внеурочной деятельности

Выпускная квалификационная работа по направлению
44.03.01 Педагогическое образование

Направленность программы бакалавриата

«Начальное образование»

Форма обучения очная

Проверка на объем заимствований:
___50_____ __% авторского текста
Работа _рекомендована_ к защите

«07» _июня_____ 2020г.
зав. кафедрой ПП и ПМ
Волчегорская Евгения Юрьевна

Выполнила:
Студентка группы ОФ-408/070-4-2
Бобылева Ирина Олеговна

Научный руководитель:
канд. пед. наук, доцент
Кудинов Владимир Валерьевич

Челябинск
2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На современном этапе жизни общества Российской Федерации возникают новые трудности для формирования личности, которые связаны с глобализацией информационного пространства. Технические возможности способствуют мгновенному распространению информации в социальном пространстве. Однако информация часто оказывается противоречивой, агрессивной, негативной и влияет на социально-нравственные ориентиры общества, в связи с этим происходят влияющие на состояние и процессы во всех ведущих сферах жизни общества деструктивные изменения и деформация духовной сферы общества: искажаются нравственные нормы и критерии, появляются неадекватные общественные стандарты и установки, неверные ценности и ориентации. Исходя из этой ситуации возникает проблема формирования кибербезопасности, решение которой способствует полноценному развития как личности, так и общества.

Большую роль безопасности школьников отводит Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»от 29.12.2010 № 436-ФЗ. Данный закон обладает отличительной особенностью– «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию». Согласно Федеральному государственному образовательному стандарту начального общего образования (далее – ФГОС НОО) у учеников начальных классов должны быть сформированы метапредметные результаты, включающие умение активно использовать средства информационных и коммуникационных технологий (далее – ИКТ) для решения познавательных и коммуникативных задач, умение использовать различные способы поиска (в справочных источниках и открытом учебном

информационном пространстве сети Интернет), сбора, обработки, анализа, обработки, организации, передачи и интерпретации информации.

Включенные в процесс познания ребенок оказывается незащищенным от различных потоков информации. Педагогическую проблему представляют популяризация жестокость средствами массовой информации, отсутствие цензуры и возрастание роли глобальной сети Интернет. Именно качество и уровень образованности подрастающего поколения, готовности личности к самореализации в обществе, степень ее зрелости могут стать решением этой проблемы, поэтому необходимо расширять содержание начального образования, вводить в него новые компоненты для обучения основам кибербезопасности.

По нашему мнению, для полноценного становления младшего школьника важнее и продуктивнее будут занятия развитием кибербезопасности личности школьника в сравнении с созданием совершенной информационной среды. Обучение ребенка адекватно воспринимать и оценивать информацию, а также критически ее осмыслять является одним из возможных путей разрешения проблемы кибербезопасности.

Главная роль при этом принадлежит начальной школе, где возможность формирования основ кибербезопасности младшего школьника обоснована сензитивностью возраста, авторитетом учителя, а еще желанием узнавать что-то новое. Так, ребенок в младшем школьном возрасте включается в киберпространство, в основном это социальные сети и компьютерные игры.

В настоящее время освоение понятий «кибербезопасность», «информационная грамотность», «информационная культура», «информационная картина мира» находится в центре научных интересов философов Т. В. Воробьевой, Л. В. Крапивской, социологов В. П. Конецкой и др., психологов К.Н.Дудкина, Б. Ф. Ломова, педагогов Н. И. Гендиной, Н. В. Гутовой, Л. С. Зазнобинойи др. Существенный вклад

в исследование влияния информации на личность внесли Ю. Н. Усов и И. В. Челышева.

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

В нашем исследовании мы опираемся на ведущие идеи педагогов, которые занимались проблемами становления личности школьника: Е. В. Бондаревской, З. И. Васильевой, И. А. Зимней и др.

На основе анализа научной литературы мы сделали вывод о том, что в педагогической науке стали появляться различные предпосылки для решения проблемы формирования основ кибербезопасностиу обучающихся. В научных исследовательских работах нами не было выявлено концепции формирования основ кибербезопасности у младшего школьника. Формировать основы кибербезопасности можно на уроках, но более целесообразно заниматься этой работой во внеурочной деятельности, которая создана для удовлетворения потребностей учеников в досуге во внеурочное время. Для нас важно, что она организуется по интересам самих обучающихся, потому что это способствует тому, что у них появляется свобода выбора в той направленность, которая им приносит удовольствие и пользу. Вследствие, появляется потребность в обучении школьника пониманию вероятного манипулирования его поведением и сознанием с помощью информации, которая распространяется средствами массовой информации, телевидением и др. Помимо этого, в современном мире для безопасной социализации личности школьника нужно научить его противостоять информационным угрозам. В нынешнее время большое количество учеников начальной школы проводят своё свободное время в компьютерных онлайн-играх и

социальных сетях, что может привести к негативным последствиям. Детям увлекательнее виртуальный мир, чем реальный, так как телекоммуникационные сети предоставляют им большие возможности для общения, развлечения и т.п. Таким образом, актуальность данной темы обусловлена ростом числа младших школьников, вовлеченных в большой и многообразный поток информации, использование которой может отображаться на них как положительно, так и отрицательно.

На сегодняшний день сложилось противоречие между необходимостью формирования основ кибербезопасности у младших школьников с одной стороны и недостаточным методическим обеспечением формирования основ кибербезопасности у младших школьников во внеурочной деятельности.

Из противоречия выявлена следующая проблема исследования: как формировать основы кибербезопасности у младших школьников во внеурочной деятельности?

Сформулированные противоречие и проблема определили выбор темы нашего исследования: «Формирование основ кибербезопасности у младших школьников во внеурочной деятельности».

Цель исследования: теоретически рассмотреть проблему формирования основ кибербезопасности у младших школьников во внеурочной деятельности для разработки рабочей программы курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников.

Объект исследования: процесс формирования основ кибербезопасности у младших школьников.

Предмет исследования: формированиеоснов кибербезопасностиу младших школьников во внеурочной деятельности.

Задачи:

1. Рассмотреть сущность понятий «кибербезопасность», «информационная безопасность».

2. Проанализировать кибербезопасность как педагогическую проблему.

3. Изучить особенности развития младшего школьника как фактор эффективности формирования основ кибербезопасности во внеурочной деятельности.

4. Экспериментально исследовать формирование основ кибербезопасности младших школьников во внеурочной деятельности.

5. Определить содержание рабочей программы курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников.

База исследования: МБОУ «Увельская СОШ № 1» п. Увельский, количество детей 26.

Методы исследования:

1. Теоретические (анализ психолого-педагогической и методической литературы, сравнение, обобщение).

2. Эмпирические (тестирование).

3. Методы обработки и интерпретации результатов.

Практическая значимость: разработанная рабочая программа, направленная на формирование основ кибербезопасности у младших школьников во внеурочной деятельности, может быть использована в практике работы учителя.

Выпускная квалификационная работа имеет следующую структуру: введение, две главы, выводы по главам, заключение, список используемых источников, приложение. В списке литературы 46 источников, в тексте работы 6таблиц, 15 рисунков.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ У МЛАДШЕГО ШКОЛЬНИКА ВО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

1.1 Сущность понятий «информационная безопасность», «кибербезопасность»

Серьезной проблемой, с которой в настоящее время пришлось столкнуться обществу, является рост негативного воздействия информационно-телекоммуникационных сетей на подростков и детей. Решение проблем, с которыми сталкиваются они в Интернете, становится значимой политикой для большинства государств. В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, делается акцент на том, что в настоящее время происходит усиление влияния на молодёжь негативной информации, в результате чего национальные нравственные ценности стираются [23]. В частности молодое поколение нуждается в особой защите государства в современных условиях развития информационного общества, и на проблемах обеспечения информационной безопасности несовершеннолетних нужно обратить большее внимание [12]. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ раскрывает термин «информационная безопасность детей» как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [39].

На международном уровне правовую базу для защиты детей от информации, способной причинить вред их здоровью и развитию, представляет «Конвенция о правах ребенка», принятая Генеральной Ассамблеей ООН 20 ноября 1989 года. Данным правовым актом закрепляется право ребенка на доступ к информации, способствующей

правильному физическому и психическому здоровью несовершеннолетнего, и формулировка принципов защиты ребенка от неблагоприятной для него информации.

В Российской Федерации уже сформировалась группа нормативных правовых актов, целью которых является защита детей от информации, причиняющей вред их здоровью и развитию (а именно Указ Президента РФот01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2018-2023 годы», Федеральный закон от29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон от27.07.2006 N 152-ФЗ (ред. от21.07.2014) «О персональных данных» (27 июля 2006 г.), Федеральный закон от13.03.2006 № 38-ФЗ «О рекламе»). Однако большое количество проблем в данной области, которые требуют решения, наличие пробелов в праве обусловливает необходимость совершенствования правовых норм, направленных на охрану информационной безопасности несовершеннолетних [42].

Интернет – глобальная сеть, которая обеспечивает связь для пересылки сообщений электронной почты, передачи файлов, соединения с другими компьютерами и получения доступа к информации, существующей в самых различных формах. Взрослым и детям представлен широкий спектр возможностей в Интернете для выражения собственной индивидуальности, обучения и образования, по этой причине дети в особенности являются одной из наиболее быстрорастущих групп пользователей Интернет. Несмотря на положительные моменты, появляются вопросы информационной безопасности детей. Важная задача как для России, так и для всех развитых стран мира – защитить несовершеннолетних от интернет-угроз, но сеть Интернет невозможно контролировать, поэтому возникает много нерешенных разнообразных проблем.

В широком смысле термин «безопасность молодежи» определяется в научной литературе, как «совокупность условий и факторов, обеспечивающих жизнедеятельность и устойчивое развитие молодого поколения, способного противостоять социальным и индивидуальным угрозам окружающей среды, целенаправленно реализуя свои основные социальные функции, как ресурс и потенциал общества» [43].

Остановимся на некоторых проблемах, связанных с обеспечением информационной безопасности в России.

Во-первых, недостаточность информационно-просветительской работы по вопросам безопасного поведения в интернет-пространстве и, как следствие, низкие показатели уровня интернет-грамотности детей и подростков. Некоторыми факторами предлагается разработка образовательного курса по интернет-безопасности несовершеннолетних. Тенденция к интеграции интернет-грамотности в школьные программы может быть эффективным способом наделения детей знаниями и навыками, необходимыми для того, чтобы обеспечить им максимальный уровень безопасности в сети Интернет [18].

Во-вторых, нужно подчеркнуть необходимость повышения степени вовлеченности родителей в обеспечение информационной безопасности детей в сети Интернет. Политика защиты детей в Интернете должна быть основана на распределении обязанностей всех заинтересованных лиц. Поэтому важно определить участников правоотношений по обеспечению информационной безопасности несовершеннолетних и определить их роль. Чтобы действовать эффективно, родители должны быть обеспечены информацией и соответствующими инструментами, необходима разработка технических решений для родительского контроля. Родители, опекуны и попечители, педагоги и общество в целом могут и должны помочь детям извлекать полезную выгоду от использования Интернета. Однако указанные субъекты также несут ответственность за защиту несовершеннолетних от рисков в Интернете.

В-третьих, проблема отсутствия специалистов в области информационной безопасности, а также реализуемых высшими учебными заведениями дополнительных профессиональных программ для педагогических работников в области развития информационных технологий. Необходимо вводить мастер-классы, разрабатывать информационные и учебные материалы, дополнительные образовательные программы по безопасности в Интернете для учителей.

В-четвёртых, не разработан механизм ответственности за распространение материалов, направленных на отрицание общественных норм и правил со стороны отдельных лиц или групп людей; пропаганде молодежных суицидов в социальных сетях; государством не выделяется достаточно средств на разработку развивающего и обучающего контента для детей; отсутствие средств защиты несовершеннолетних от наносящей вред информации в местах, доступных для детей и многое другое [19].

Исходя из перечисленных проблем в нашей стране, мы считаем, что необходимо использовать положительный зарубежный опыт. К примеру, самым важным методом защиты детей – пользователей Интернет в Китае является метод повышения осведомлённости и навыков несовершеннолетних. В КНР в 2016 году принят закон о кибербезопасности («Cyber security Law of the People’s Republic of China»), позволяющий на законных основаниях прекратить деятельность тех, кто в сети Интернет ставит под угрозу физическое и психическое здоровье детей [25].

В начальной школе при формировании понятия «информационная безопасность» важным является формирование представлений об информации как источнике возможных угроз личности, семье, ближайшему окружению, на основе которых вырабатываются умения у младшего школьника действовать в ситуациях информационных угроз в ходе моделирования их в период учебной деятельности. Актуальность изучения понятия «информационная безопасность» в начальных классах определяется тем, что большинство современных детей рано начинают

использовать компьютер не как предмет изучения, а как удобное средство решения тех или иных повседневных задач или для развлечений. Необходимо научить ребенка правильно взаимодействовать с компьютером подобно тому, как мы учим его в школе правильно держать ручку или учим правилам соблюдения техники безопасности.

Стоит отметить, что кибербезопасность – это подмножество такого понятия как информационная безопасность. Кибербезопасность имеет более узкую направленность и изучает охрану важных данных, в то время как информационная безопасность изучает всё о безопасности информации и данных в целом. Слово «информация» происходит от латинского слова «informatio», что означает разъяснение, высказывания, осведомлённость. Само слово информация не так давно стало превращаться в научный термин. До этого информацию воспринимали как то, что присутствуют в языке, письме или передаётся при общении [8].

По Г. В. Грачеву, информационная безопасность личности – это состояние защищенности личности, обеспечивающее ее целостность как активного социального субъекта и возможностей развития в условиях информационного взаимодействия с окружающей средой.

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

Т. А. Малых, касаемо области образования, определяет информационную безопасность как состояния защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного воздействия и умении

скомпенсировать негативные эффекты информационного воздействия [20]. Согласно проекту Концепции стратегии кибербезопасности Российской Федерации киберпространство – это «сфера деятельности в информационном пространстве, образованная совокупностью Интернет и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)»; так, кибербезопасность – это «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [16].

А. С. Алпеев считает, что «кибербезопасность– условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными» [2].

В русско-американском словаре в сфере информационной безопасности термин «кибербезопасность» звучит так – это свойство киберпространства (киберсистемы) противостоять намеренным и (или) ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз [31].

Появление проблем, связанных с безопасностью использования компьютеров, смежного оборудования, введение понятий «информационная безопасность» и «кибербезопасность» является последствием применения во всех сферах жизни общества сети Интернет, активного расширения области информационных и коммуникационных технологий. Проанализировав представленные понятия, можно сказать о том, что кибербезопасность является составляющей информационной безопасности, которая изучает особенности киберобъектов, нормативную документацию, источники опасности, позволяет обеспечить правовую

защиту от возможных источников опасности. Киберобъекты и киберопасность практически каждый день могут встречаться современным детям, поскольку большую часть своего времени они проводят в Интернете. Например, дети сталкиваются с такими опасностями, как [16]:

1. Нежелательный контент: легальный контент только для взрослых– как правило, это информация сексуального характера: фотографии, фильмы, товары. Также это могут быть и сайты, пропагандирующие насилие, жестокость, применение и создание оружия, секты. В реальности доступ детей к таким материалам ограничен, а в интернете открыт.

2. Запрещенный контент: информация, запрещенная в большинстве стран мира – а именно, проповедующая нацизм, терроризм, расовую непримиримость, сексуальные извращения и любой порнографический контент.

3. К запрещенному контенту относятся также суицидальные сайты-форумы (кибер-суицид, группы по вовлечению в запрограммированное самоубийство) и наркосайты (пропаганда «пользы» употребления марихуаны, рецепты изготовления наркотических смесей: «снюс», «насвай», соль).

Важно понимать, что это тот тип контента, который способен нанести непосредственный вред психике ребенка, вызвать различные расстройства, озлобить его или мотивировать вступить в какую-то запрещенную организацию. Ребенок может случайно посетить страницу такого типа, перейдя по ссылкам рекламодателей, содержащих ложную информацию.

Дети пользуются Интернетом, чтобы выполнить домашнее задание, посмотреть фильмы, поиграть в онлайн-игры и пообщаться в социальных сетях, по этой причине взрослые должны познакомить их с правилами правильного поведения в киберпространстве. Именно это подчёркивается в проекте «Концепции стратегии кибербезопасности Российской Федерации», где указано, что на сегодняшний день важно разработать и

внедрить в образовательный процесс специальный курс по информационной безопасности, включающий модули по кибербезопасности, а также формировать и развивать культуру безопасного поведения в киберпространстве и безопасного использования его сервисов [16].

Нужно учитывать в процессе обучения, что большое количество современных учеников, их родителей и учителей сталкиваются с определенными киберугрозами в их повседневной жизни. Учитывая этот факт, была сформулирована цель обучения основам кибербезопасности в начальных классах – формировать понимание структуры киберпространства у детей, принципов работы в нем, существующих угроз пользователям Интернета, знаний о правилах, которые позволят обучающимся защитить свои личные данные в Интернете. Поставленной цели можно достичь решением следующих задач: 1) введение основных понятий кибербезопасности, например, через использование инструкций, описывающих правила поведения в киберпространстве; 2) формирование у обучающихся умения действовать в киберпространстве с применением системы прикладных задач; 3) формирование у обучающихся навыков поведения в ситуациях встречи с киберугрозой путем проведения интерактивных игр или применения каких-либо тренажеров; 4) создание родителями кибербезопасной среды дома с применением учебно-методических материалов [37].

Таким образом, рассмотрев сущность понятий «информационная безопасность» и «кибербезопасность», мы пришли к выводу, что кибербезопасность не может быть полноценно направлена на защиту от всего количества угроз. Следовательно, нужно обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве, особенно для младших школьников.

1.2 Кибербезопасность как педагогическая проблема

Переход к новому качественному состоянию общества, характеризуемому резким повышением роли информационных процессов и, в частности, созданием целой системы производства информации, стало отличительной особенностью нашего времени. Существует мнение, что современное общество находится на переходе к качественно иной форме своего существования – информационному обществу и в более широком контексте – к информационной цивилизации [1].

В настоящее время, в современном педагогическом пространстве России, уже реализована задача о проведении информатизации, компьютеризации и цифровизации в рамках приоритетного национального проекта образования. Уже с 2007 года все образовательные учреждения России имеют компьютерную базу и доступ в Интернет. Отметим, что определенный опыт в преподавании и обучении обучающихся информационным технологиям накоплен, то есть школьники умеют получать информацию из Интернета, существуют минимальные требования к необходимому уровню подготовки обучающихся, основанные на умениях [7]:

– находить требуемую информацию в разнообразных источниках;

– переводить зрительную информацию в вербальную знаковую систему и наоборот;

– трансформировать информацию, модифицировать ее форму, объем, знаковую систему, носитель и пр., учитывая коммуникативное взаимодействие и особенности аудитории, для которой она предназначена;

– понимать цели коммуникации, направленность информационного потока;

– находить ошибки в получаемой информации и вносить предложения по их корректировке;

– проводить оценку информационных сообщений;

– вычленять основное из принятой информации;

– работать с передачей, получением и хранением информации и другое.

Таким образом, на данном этапе можно утверждать, что в педагогической науке разработаны основы по информационно-коммуникационным технологиям.

Исходя из анализа научной психолого-педагогической литературы по рассматриваемой проблеме, можно сделать вывод, что, несмотря на существующую значимость в данной теме, на сегодняшний день научных и практических работ недостаточно.

Так, Н. И. Саттарова в своем исследовании «Информационная безопасность школьников в образовательном учреждении»акцентирует внимание на безопасности ребенка при работе в сети Интернет. Автор предлагает рекомендации для педагогов, обучающихся и родителей, однако в работе автор уделяет внимание информационной безопасности обучающихся именно в образовательном учреждении и только на уроках информатики.

В работе Д. С. Синицына рассматриваются психолого-педагогические условия обучения информационной безопасности подростков [33].

Определенный интерес для нашего исследования представляют работы Ю. А. Дейкиной «Развитие познавательных интересов дошкольников в процессе медиаобразования» [6], Е. В. Якушиной «Методика обучения школьников с информационными ресурсами на основе действующей модели Интернет».

Мы считаем, что для эффективного и полноценного развития ребенка невозможно и не нужно создавать идеальную информационную среду, важно заниматься кибербезопасностью каждого школьника.

Формирование основ кибербезопасности является педагогической проблемой. Во-первых, большую часть своего времени ребенок проводит в

образовательном учреждении, во-вторых, обучение является основной деятельностью школьника, и в-третьих – в школе есть специалисты, которые могут обучать основам информационной безопасности и кибербезопасности.

В последнее время все больше исследователей обращают внимание на необходимость активной разработки проблематики кибербезопасности личности школьника, общества и государства в целом [17].

Проанализировав научную литературу, мы отметили, что вопросы кибербезопасности рассматриваются в различных областях знаний. В педагогической литературе мы не определили концепцию кибербезопасности, поэтому мы обратились к междисциплинарным исследованиям и обнаружили, что неоднозначные подходы к определению кибербезопасности отмечены в литературе.

Для того чтобы дать свое определение кибербезопасности, рассмотрим, что понимается под термином «безопасность». Безопасность представляет собой сложное явление и его изучением занимаются специалисты, работающие в различных отраслях знаний [5]. В законодательстве оно закреплено как «состояние защищенности жизненно важных интересов личности, общества и государства от угроз внешнего и внутреннего характера».

На уровне обыденного сознания понятие «безопасность» определяется как «отсутствие опасности», «состояние, при котором не угрожает опасность, есть защита от опасности» [9].

Исходя из этого, мы полагаем, что «безопасность» есть невозможность нанесения вреда кому-нибудь или чему-нибудь вследствие проявления угроз, то есть их защищенность от угроз.

Нами понятие кибербезопасности понимается как состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы информационного

воздействия и умение скомпенсировать негативные эффекты информационного воздействия.

Угрозы кибербезопасностимы считаем одним из важнейших аспектов информационной безопасности. Вероятность проявления опасностей может быть различной в зависимости от конкретных условий [13]. В связи с этим некоторые авторы используют понятие угрозы как отражение осознания определенной опасности и вероятности ее возникновения, хотя это логически сложно сделать. Угроза кибербезопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

В литературе выделяются различные классификации угроз кибербезопасности [3; 9; 15]. Среди них выделяют следующие:

1. По объектам:

– угрозы конституционным правам и свободам граждан, реализуемым в информационной сфере;

– угрозы духовной жизни общества;

– угрозы информационной инфраструктуре;

– угрозы информационным ресурсам.

2. По источнику угрозы:

– внешние – связанные со стихийными бедствиями, техногенными, политическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями;

– внутренние – связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения.

3. По природе возникновения:

– естественные (объективные) – вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;

– искусственные (субъективные) – вызванные воздействием на информационную сферу человека.

Среди искусственных угроз выделяют:

а) непреднамеренные (случайные) угрозы – ошибки программного обеспечения, персонала, отказы вычислительной и коммуникационной техники и т.д.;

б) преднамеренные (умышленные) угрозы –неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д.

4. По принципу воздействия:

– с использованием доступа;

– с использованием скрытых каналов.

5. По цели реализации:

– нарушение конфиденциальности;

– нарушение целостности;

– нарушение доступности.

6. По характеру воздействия:

– активные;

– пассивные.

Кроме этого, в литературе имеет место классификация основных угроз по степени их опасности: несанкционированный доступ; пожары; умышленное нарушение нормальной работы (заражение вирусами, умышленный ввод искаженных данных, умышленный вывод из строя оборудования и его хищения); использование программного обеспечения, содержащего ошибки [19].

Изучив различные точки зрения, мы можем сделать вывод, что в настоящее время не существует достаточно обоснованной и подробной общей классификации угроз кибербезопасности и их источников в образовании. Это связано с новизной и сложностью этой проблемы, а

также с тем, что сам метод и результат классификации зависят от задач, которые необходимо решить, и от причин и критериев, используемых для классификации.

В психолого-педагогической литературе отсутствует классификация источников угроз личности, поэтому мы выделили иную классификацию источников угроз. Выделим основные источники угроз кибербезопасности с позиций отдельного человека для определения способов и механизмов его защиты [22].

Мы считаем возможным выделить четыре группы источников угроз кибербезопасности личности как для ребенка, так и для общества в целом:

– государство (в том числе иностранные), органы власти и управления и прочие государственные структуры и учреждения;

– общество (различные общественные, экономические, политические и некоторые организации, в том числе и зарубежные);

– социальные группы (стабильные и случайные, формальные и неформальные, большие и малые по месту жительства, учебы, работы, службы, совместному проживанию и, проведения досуга и т.п.);

– отдельные личности (включая органов государственных и общественных структур, многообразных общественных групп и т.д.).

Также мы уверены, что существует угроза на личность младшего школьника от средств информационного воздействия:

– средства массовой информации представляют угрозу для ребенка, если негативная информация повторяется многократно, детская литература без цензуры угрожает психическому и моральному здоровью детей;

– телевидение как общественный институт в силу своих особенностей: (каждодневное, доступное, существует в зоне психологической близости ребенка) является одним из самых значительных видов опосредованного общения и становится важным фактором, влияющим на развитие личности с самого раннего детства [34].

Телевидение для современного школьника стало важнейшим источником информации о мире, в котором он живет, что подтверждается исследованиями разных авторов. Так, первое место по значимости СМИ занимает Интернет, на втором месте телевидение, на третьем также печатные издания и дополнительно радио [26].

На протяжении двух последних десятилетий школьники, особенно обучающиеся начального звена, являются объектом массового воздействия произведений экранных искусств, в которых действия предпочитаются чувствам и мыслям, трюки – историям, реальные человеческие типы – вымышленным супергероям, а насилие, жестокость и эротика, приправленная тем же насилием, стали едва ли не основным содержанием программ, фильмов и компьютерных игр [13].

Сегодня средства массовой информации в целом и телевидение в частности оказывают огромное влияние на осведомленность общественности и формирование индивидуальной личности. В современных условиях ребенок с первых месяцев жизни попадает в насыщенное информацией поле: занятые родители вместо колыбельных и сказок на ночь включают видео или телевизор. Возможности влиять на психику, подсознание людей, манипулировать сознанием с помощью средств массовой информации огромны. Даже, казалось бы, вполне достоверная информация может нести скрытую угрозу. Так, передачи о распространении наркотических веществ и алкоголя часто служат не столько средством отвращения от них, сколько указанием конкретной информации, где и у кого можно все это приобрести.

Для реализации своего социального поведения в обществе младший школьник нуждается в постоянном притоке информации. Постоянная информационная связь с окружающим миром, социальной средой, в которой он действует как активный социальный субъект, является одним из важнейших условий нормальной его жизнедеятельности [35].

Опираясь на концептуальные положения теории М. Мид, современный американский исследователь Дж. Мейровиц заметил, что, благодаря телевидению, в конце XX в. границы между взрослым миром и детским стали прозрачными. Телеэкран дает ребенку возможность наблюдать за миром взрослых, воспринимать его и идентифицировать себя с ним [19]. Речь идет и о том, что те или иные средства массовой информации практически нарушают права ребенка, определенные документами ООН, не соблюдают возрастные ограничения при демонстрации сцен насилия на экране. Этой проблеме посвящены исследования Г. В. Грачева, О. В. Пристанской, А. В. Федорова, А. В. Шарикова, касающиеся воздействия через экраны на детскую и молодежную аудиторию негативного влияния неконтролируемого потока сцен экранного насилия и необходимости создания продуманной государственной политики по отношению к защите прав ребенка в данной области.

Современные информационные технологии открыли для детей доступ к Интернету, который, наряду с видеоиграми, является популярным времяпрепровождением.

Проследить всю информацию, попадающую в Интернет, невозможно, как невозможно предвидеть может ли ребенок случайно зайти на сайт, где ему прорекламируют употребление наркотиков, алкоголя и прочих вредных для организма веществ [37].

На наш взгляд существует несколько путей решения этой актуальной проблемы:

1. Путь законодательного регламентирования деятельности всех видов СМИ, как способ защиты детей от получения вредной информации.

2. Введение в школьные программы курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников.

3. Последовательное формирование у младших школьников в процессе всех учебных предметов самостоятельного критического мышления.

Без правового регулирования средств массовой информации, в том числе Интернета, невозможно решить проблему кибербезопасности в обществе, особенно среди детей. Важно создать определенную общественную атмосферу отказа от таких продуктов. Для этого необходимо понимать и оценивать предоставленную информацию. Здесь начинается сфера деятельности образования и семьи.

В школу нужно создавать и внедрять психолого-педагогические программы, способные:

– подготовить сознание детей к противодействию неблагоприятному влиянию фильмов, рекламы, телепередач, и т.п.;

– помочь осмыслить детям их цели, потребности и способы их удовлетворения с помощью телевидения и сети Интернет;

– формировать визуальную грамотность с учетом того, что не может быть большая часть сообщений правильно воспринята и понята детьми (то есть формирование навыков критического телесмотрения и зрительской самостоятельности) [45].

Таким образом, можно сделать вывод, что в качестве основных источников информации, влияющих на ребенка, мы выделили: государство (в лице органов власти и управления, государственные структуры и организации), общество (в лице общественных, экономических, политических, религиозных и иных организаций), социальные группы (в лице сверстников, друзей и одноклассников), отдельную личность (родитель, педагог).

Разнообразная предлагаемая источниками информация может быть недостоверной, неэтичной, непристойной, деструктивной. В качестве средств информационного воздействия выступают: СМИ (телевидение,

Интернет,радио), литература, образовательные услуги (массовое, альтернативное, медиаобразование и др.), общение [17].

Информация из ненадежных источников может вызвать проблемы со здоровьем (переутомление, психологическая зависимость, снижение трудоспособности), этические проблемы (переоценка моральных норм, снижение интереса к искусству, чтению и т.д.), Проблемы с обучением (нехватка времени на обучение, перегрузка ненужной информацией, снижение успеваемости), общение (виртуальное общение, отсутствие навыков общения) у ученика начальной школы при отсутствии знаний о кибербезопасности.

В педагогической литературе не выявлено понятия кибербезопасности, однакопедагог способен подготовить сознание детей к противодействию негативным информационным воздействиям, сформировать информационную грамотность, развитие способности к самоблокированию информации, умению отличать качественную информацию от некачественной. Ведь учитель рассматривается как активный субъект общества, способный к обучению младших школьников информационной грамотности, призванный минимизировать проблемы кибербезопасности детей [2].

1.3 Особенности развития младшего школьника как фактор эффективности формирования основ кибербезопасности во внеурочной деятельности

В условиях школьного образования обеспечение кибербезопасности можно рассматривать как совокупность деятельности по недопущению вреда сознанию и психике ребёнка [27].

В то же время процесс обеспечения кибербезопасности основан на умении личности учащегося видеть и нейтрализовать угрозу, создаваемую воздействием информации. Это умение может приобретаться стихийно или в процессе целенаправленного обучения обучающихся. В связи с этим

появилась необходимость поиска путей решения такой проблемы, как обеспечение кибербезопасности младшего школьника [7].

Процесс просвещения в области безопасности при работе с информацией в сети Интернет целесообразно начинать с начальной школы. Поэтому необходимо рассматривать кибербезопасность

школьника как педагогическую проблему, целью которой является педагогический процесс развития у ребенка знаний об угрозе информации и способности противостоять ей, с тем, чтобы свести к минимуму последствия психического и нравственного воздействия.

Всем обозначенным видам проблем может противостоять педагог, обучающий кибербезопасности. При определении эффекта воздействия на ребенка информационной продукции обоснована необходимость учета краткосрочного (немедленного) и долгосрочного эффекта. Последний представляется особенно опасным с точки зрения обеспечения информационной безопасности, поскольку картина мнимого благополучия дезориентирует родителей, педагогов и воспитателей и ограничивает возможность компенсации ущерба, нанесенного развитию и здоровью ребенка [33].

Для нашего исследования важно выявить, какие особенности этого возрастного периода могут способствовать эффективному формированию основ кибербезопасности. Для этого нами был проведен анализ научной психолого-педагогической литературы и определены значимые факторы развития личности младшего школьника [20].

Во-первых, определяющей для обучающихся младших классов становится система «ребенок – учитель», влияющая на отношения ребенка к родителям, к одноклассникам и самому себе. Для обучающихся начальных классов высок авторитет педагога, ребенок открыт для общения с наставником и доверяет информации, исходящей от него.

Во-вторых, основным видом деятельности младшего школьника является учебная деятельность, а процесс формирования кибербезопасности важно организовать как процесс обучения.

В-третьих, в ребенке начинают формироваться зачатки нравственного поведения. Он понимает смысл понятий «хорошо - плохо», «добро– зло», но у него отсутствует субъективное отношение к системе нравственных норм и ценностей. Система нравственных норм и ценностей становится оценочным регулятором жизни и деятельности обучающегося и реализуется в том случае, если эти правила и нормы поведения приняты и осмыслены ребенком. Следовательно, целесообразно формировать основы кибербезопасности, используя категории нравственных ценностей и норм, активизировать собственные внутренние силы ребенка по самоусовершенствованию [20].

Формирование основ кибербезопасности младшего школьника невозможно без учета его взаимодействия с другими обучающимися. Процесс взаимодействия реализуется как кооперация со сверстниками, которая воздействует на процесс интериоризации иначе, чем кооперация со взрослым. Г. А. Цукерман рассматривает кооперацию со сверстниками как связующее звено между началом формирования нового действия при работе со взрослым и полностью самостоятельным внутрипсихическим концом формирования.

При качественном анализе взаимодействий детей Г. А. Цукерман выделяла две характеристики этой деятельности [24]:

1. Независимость от взрослого. Взрослый организует работу, «запускает», а затем дети работают самостоятельно (в отличие от фронтального обучения, при котором учитель побуждает, направляет, контролирует, оценивает и т.д.). При этом дети обращаются к учителям очень редко – в крайних ситуациях.

Таким образом, меняются отношения «ученик – учитель»: дети не стремятся к постоянному сотрудничеству со взрослым, работают

самостоятельно. Можно отметить обращенность ребенка, прежде всего к партнеру. Это обеспечивает учет позиции партнера, его точки зрения, способствует децентрации. Все это приводит к развитию рефлексивных действий.

2. Обращенность детей не столько на результат, сколько на способ своих и партнера действий. В этой работе взаимодействие детей строилось в форме «ситуация педсовета»: дети-учителя в разных классах, они обсуждают между собой, на какие правила дать задания тому или другому классу. Отмечается высокий мотивационный уровень участников кооперации. Особенно это видно по слабым ученикам – они становятся активными и заинтересованными.

В процессе кооперации идет постоянное преобразование ребенка в плане его совершенствования, и открываются некоторые возможности для его культурной и познавательной жизни в глобальном информационном обществе. Именно поэтому взаимодействие младших школьников в форме кооперации должно быть необходимым как одно из обязательных условий формирования основ кибербезопасности.

Анализируя возрастные особенности, мы учитываем недостаточность развития у младшего школьника самостоятельного критического мышления, поэтому, в процессе занятий по формированию основ кибербезопасности, учитель помогает ребенку в осознанном проявлении критического отношения к увиденному или услышанному [32].

В-четвёртых, младший школьный возраст характеризуется большой мыслительной пластичностью, вследствие чего возможно ее качественное изменение в ходе значимой для ребенка учебно-познавательной деятельности, структура которой позволяет органично включить в ее содержание педагогически управляемый процесс развития у младшего школьника знаний по кибербезопасности [20].

В. В. Давыдов считал, что уже в младшем школьном возрасте при создании необходимых условий дети могут овладеть основами разумно-теоретического, рефлексирующего сознания и мышления.

Для нашего исследования по кибербезопасности, характеризуя внеурочную деятельность, необходимо отметить и мыслительные способности и возможности младшего школьника.

Для дальнейшего рассмотрения данного вопроса важными для нас стали труды Ж. Пиаже, который отмечал, что ребенок вовсе не маленький взрослый человек, и ум его вовсе не маленький ум взрослого.

Обобщая позицию Ж. Пиаже, выделим следующее: детскую мысль отличает осознанность и подсознательная интуитивность, поэтому при обучении младших школьников основам кибербезопасности важно отмечать, что им осознано и принято, а что еще не осознано.

Система моральных норм, свойственная ребенку, которая влияет на способность выявлять информационную угрозу, крайне важна для нашей работы. Мы будем строго полагаться на систему нравственных норм и активизировать его внутренние усилия по самосовершенствованию.

На пороге школьной жизни возникает новый уровень самосознания детей, наиболее точно выражаемый словосочетанием «внутренняя позиция». Эта позиция представляет собой осознанное отношение ребенка к себе, поведению, к окружающим людям, событиям – такое отношение, которое он четко может выразить словами и делами. Возникновение внутренней позиции становится переломным моментом в судьбе ребенка, определяя собой начало его индивидуального, в какой-то степени самостоятельного личностного развития [30].

Факт становления данной позиции внутренне проявляется в том, что выделяется в сознании ребенка система нравственных норм, которым он следует или пытается следовать всегда и везде, независимо от возникающих обстоятельств. Благодаря исследованиям, которые провел

Ж. Пиаже, мы понимаем, как судят дети разного возраста о нормах морали, каких нравственно-оценочных суждений они придерживаются.

Для нашего исследования представляют интерес работы по развитию нравственных суждений у детей Л. Колберга, который расширил, конкретизировал и углубил идеи Пиаже. Он установил, что на до конвенциональном уровне развития морали дети чаще дают оценки поведению только по его следствиям, а не на основе анализа мотивов и содержания поступков человека. Сначала, на первой стадии этого уровня развития ребенок считает, что человек должен соблюдать правила для того чтобы избежать наказания за их нарушение.

На второй стадии возникает мысль о полезности нравственных действий, сопровождающихся поощрениями. В это время нравственным считается любое поведение, за которое можно получить поощрение, или такое, которое не мешает удовлетворять свои другому человеку, удовлетворяя личные потребности какого-либо человека.

Таким образом, при работе по формированию основ кибербезопасности эту особенность необходимо учитывать, в занятиях по внеурочной деятельности использовать такие ситуации, которые предполагают нравственный выбор обучающихся. Произвольность поведения из области когнитивных процессов и добровольное регулирование поведения в младшем школьном возрасте распространяется на область чувств. У детей 3-4 классов отмечаются первые попытки, хотя и неуспешные, ограничить эмоции, непосредственные желания и побуждения. Наряду с этим, примерно начиная с 3 класса у младших школьников можно отметить проявление настойчивости как волевой черты характера.

В этом возрасте дети достаточно полно еще не способны развивать свои собственные моральные убеждения. Усваивая то или иное моральное требование, младший школьник до сих пор полагается на авторитет учителей, родителей и старшеклассников. Относительная

несамостоятельность морального мышления и большая внушаемость младшего школьника определяют его легкую подверженность как положительному влиянию, так и отрицательному. Поэтому на занятиях по кибербезопасности во внеурочной деятельности необходимо создать ситуацию успеха.

Анализ разработанных теоретических положений позволил установить, что формирование основ кибербезопасности наиболее эффективно во внеурочной деятельности, но оно должно быть построено на принципах сотрудничества. Эти характеристики позволили нам понять особенности организации работы с младшим школьником.

Семи-десятилетние дети обладают сильным чувством семьи [38]. Они только начинают развивать чувство своей моральной и половой индивидуальности и обычно интересуются жизнью старших детей. Они доверчивы и не сомневаются в авторитетах.

И. П. Подласый считает, что к 6 годам ребёнок в основном готов к систематическому школьному обучению [27]. О нём можно говорить уже как о личности, поскольку он осознаёт своё поведение, может сравнивать себя с другими. К началу школьного периода формируется ряд новых психических образований:

– стремление к общественно значимой деятельности;
– способность управлять своим поведением;
– умение делать простые обобщения;
– практическое овладение речью;
– умение налаживать взаимосвязи и сотрудничество с другими людьми.

В 6-7 летнем возрасте у ребёнка первая крупная перемена в жизни. Ведущей деятельностью становиться учение, изменяется уклад жизни, появляются новые обязанности, новыми становятся и отношения ребёнка к окружающим [30].

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

В младшем школьном возрасте улучшается нервная система, интенсивно развиваются функции больших полушарий головного мозга, усиливается соматическая функция коры. Психика ребёнка быстро развивается. Связь между процессами возбуждения и торможения меняется: процесс торможения становится сильнее, но процесс возбуждения все еще доминирует – младшие ученики очень возбудимы. Повышается точность органов чувств. Несомненно, возрастные изменения темперамента находятся в прямой зависимости от полового созревания и развития детского организма, прежде всего мозговых основ психики, свойств нервной системы.

Детей отличают некоторые признаки слабости типа нервной системы, что означает не только малую выносливость, но и более высокую чувствительность. Именно возрастная слабость нервной системы может обусловливать в ранние годы особую яркость восприятия, детскую впечатлительность и такие черты, как лёгкость перехода к возбуждению, импульсивность [44].

Интенсивность эмоциональных переживаний и их нестабильность также характерны для младших школьников. Весьма обычны стремительные переходы от горестных слёз к улыбке, веселью. Слабость нервной системы удивительным образом сочетается в годы детства с быстрым возобновлением энергии. Об этом своеобразии работоспособности ребёнка К. Д. Ушинский писал: «Заставьте ребёнка

сидеть, он очень скоро устанет, лежать – то же самое; идти он долго не может, не может долго ни говорить, ни петь, ни читать, и менее всего долго думать; но он резвится и движется целый день, переменяет и перемешивает все эти деятельности и не устаёт ни на минуту; а крепкого детского сна достаточно, чтобы возобновить детские силы» [26].

Нельзя не учитывать, что существуют возрастные особенности темперамента: в каждом детском возрасте – своя специфика активности, эмоциональности и моторики. В младшем школьном возрасте характерные черты активности – это лёгкость пробуждения интереса и недостаточная длительность состояния сосредоточенности, связанные с той же слабостью нервной системы. И эмоциональность в эту пору жизни, и моторика, иные, чем в последующих школьных возрастах. С годами происходит как увеличение возможностей нервной системы, так и ограничение, утрата её ценных детских свойств [21].

Большую роль в познавательной деятельности школьника играет память. Становление личности маленького школьника происходит под влиянием новых отношений со взрослыми и сверстниками, новых видов деятельности и общения, включения в целую систему коллективов. У младших школьников складываются элементы социальных чувств, вырабатываются навыки общественного поведения. Младший школьный возраст предоставляет больше возможности для развития нравственных качеств личности. Этому способствует гибкость и привычная внушаемость школьников, их доверчивость, склонность к подражанию, а главное огромный авторитет, которым обладает учитель. В этом возрасте ребёнок входит в школьный коллектив и должен соблюдать его требования, как и требования соседей, улицы, лагеря. Он может выполнять как индивидуальные задания, так и серьёзные дела для семьи, узнаёт школьный распорядок. Но, освоив законы «общежития», он пытается их нарушить, но искренне сожалеет о своих поступках. Некоторые ребята не любят дружбы со сверстниками и беспокоятся, если друг заводят нового

друга. Они любят игры, ответственно относятся к своей роли, к понятию справедливости. Учитель для него является авторитетом [30].

Воля младшего школьника не сформирована, мотивы не осознаются. Повышенная чувствительность, способность глубоко и сильно переживать превалируют над доводами разума, школьник совершает множество необдуманных действий. Развитие младшего школьника – очень сложный и противоречивый процесс. В этом возрасте растущий человек должен очень многое понять, а поэтому нужно максимально использовать каждый день его жизни [30].

Анализ научной литературы позволил нам выделить особенности младшего школьного возраста, которые следует учитывать при организации занятий во внеурочной деятельности по кибербезопасности. Мы учитывали эти особенности при выделении педагогических условий формирования основ кибербезопасности у младшего школьника.

Нами выяснено, что для формирования основ кибербезопасности на начальном этапе обучения нужны специальные условия, которые создают возможности взаимодействия и взаимопонимания между учителем и обучающимся на основе тщательно продуманного содержания занятий во внеурочной деятельности по кибербезопасности, которые значимы для младшего школьника.

На наш взгляд, одним из главных условий успешного формирования основ кибербезопасности представляется позиция учителя-наставника, суть которой заключается в безусловном, без оценочном принятии ребенка, стремлении укрепить его позицию в социуме, оказать своевременную поддержку в саморазвитии младшего школьника, открыть путь к социализации и адаптации ребенка, защитить его от совершения недопустимых действий. Работа учителя ориентирована на реализацию принципов педагогики саморазвития: взаимной открытости учителя и ребенка, свободосообразности, социосообразности, глубинного общения и

воспитания, идеологичности, ценности творческого непослушания, ненасилия и непримиримости к насилию над ребенком[46].

Мы считаем, что одной из важнейших предпосылок успешного формирования основ кибербезопасностиу младших школьников является осведомленность учителем в теории кибербезопасности:

Во-первых, в том, что именно защищается, что является объектом или предметом защиты (в нашем случае – это личность младшего школьника).

Во-вторых, установление, от чего защищается личность младшего школьника, какова угроза (опасность) – внешний по отношению к данной целостности фактор, воздействующий на младшего школьника.

В-третьих, в понимании необходимости предотвращения разрушения самооценки ребенка, дезориентации в окружающей обстановке, нарушении адекватности представлений младшего школьника об окружающем мире и своем месте в нем, снижении чувства уверенности, утрате целостности Я и индивидуальной уникальности, разрушении намерений, планов, выборе неадекватных целей и способов поведения, попадании в психологическую зависимость от других субъектов воздействия, нарушениях психического здоровья до необратимых патологических изменений психики, внутренней деградации.

В-четвертых, в представлении, как избежать возможного ущерба, каким образом и чем защищаться.

В-пятых, в уверенности педагога в том, что именно он является субъектом защиты личности младшего школьника в процессе обучения, опережая в данном направлении действия общества и государства [44].

Проанализировав данный параграф можно утверждать, что эффективность формирования основ кибербезопасности у младших школьников во внеурочной деятельности связана с развитием личности и ее индивидуальных особенностей.

Так, мы выделили следующие особенности:

– значимость педагога в жизни ребенка;

– ведущая деятельность – учебная;

– сотрудничество детей друг с другом;

– пластичность (гибкость) мышления, то есть умение ребенка приспосабливаться, адаптироваться, при этом используя творческие способности; умение нестандартно мыслить;

– внутренняя позиция ребенка, то есть осознанное принятие себя к окружающим.

Выводы по главе 1

Изучение кибербезопасности у младших школьников стало предметом внимания совсем недавно. Возникновение понятия кибербезопасности связано с изменением парадигмы образования; от усвоения знаний, умений, навыков к развитию личности обучающихся.

В Российской Федерации уже сформировалась группа нормативных правовых актов, целью которых является защита детей от информации, причиняющей вред их здоровью и развитию (а именно Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий винтересах детей на 2012-2017 годы», Федеральный закон от29.12.2010 № 436-ФЗ «О защите детей отинформации, причиняющей вред ихздоровью иразвитию», Федеральный закон от27.07.2006 N 152-ФЗ (ред. от21.07.2014) «О персональных данных» (27 июля 2006 г.), Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе») [38; 39; 40; 41].

Рассмотрев теоретические аспекты формирования основ кибербезопасности у младших школьников во внеурочной деятельности, мы изучили понятия «информационная безопасность» и «кибербезопасность».

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ раскрывает термин «информационная безопасность детей» как «состояние защищенности

детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию».

Согласно проекту Концепции стратегии кибербезопасности Российской Федерации «кибербезопасность – это совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

Изучая кибербезопасность как педагогическую проблему, можно сказать то, что, во-первых, большую часть времени проводит ребенок в образовательном учреждении, во-вторых, обучение является основной деятельностью школьник, и в-третьих – в школе есть профессионалы, которые способны обучать основам информационной безопасности и кибербезопасности.

Особенностями развития младшего школьника как фактор эффективности формирования основ кибербезопасностиво внеурочной деятельности являются: мыслительная пластичность, критическое мышление, память и моторика, интенсивность эмоциональных переживаний и т.д.

Так, мы сделали краткие выводы по теоретической части нашей работы, теперь перейдем к экспериментальной.

ГЛАВА 2. ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПО ФОРМИРОВАНИЮ ОСНОВ КИБЕРБЕЗОПАСНОСТИ МЛАДШИХ ШКОЛЬНИКОВ ВО ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

2.1 Организация исследования

В теоретической части нашего психолого-педагогического исследования были рассмотрены и раскрыты представления о сущности понятий «информационная безопасность», «кибербезопасность», кибербезопасность как педагогическая проблема, а также особенности развития младшего школьника как фактор эффективности формирования основ кибербезопасностиво внеурочной деятельности.

С целью изучения формирования основ кибербезопасности младших школьников во внеурочной деятельности было проведено исследование на базе МБОУ «Увельская СОШ №1».

В исследовании приняли участие 26 учеников 4 класса в возрасте от 9 до 10 лет, из которых 12 мальчиков и 14 девочек.

Обучающимся был выдан тест с вопросами по данной теме:

Уважаемые респонденты, мы проводим исследование на тему: «Формирование основ кибербезопасности младших школьников во внеурочной деятельности. Просим Вас ответить на ряд вопросов. Вам необходимо выбрать вариант, который Вы считаете правильным.

Вопросы теста представлены в таблице 1, критерии оценивания – в приложении 1.

Таблица 1 – Тест для младших школьников по информационной безопасности

№ п/п	Вопрос	Варианты ответа
1	*2*	*3*
1	На адрес электронной почты пришел файл с игрой от неизвестного пользователя. Как Вы поступите?	a. Скачать файл и начать играть. b. Не открывать файл. c. Отправить файл своим друзьям.

Продолжение таблицы 1

1	*2*	*3*
2	В социальной сети с Вами познакомился ученик из Вашей школы, которого Вы ни разу не видели, и он пригласил Вас на встречу с ним. Ваши действия?	a. Пойти на встречу. b. Пойти на встречу с родителями. c. Не пойду на встречу вообще.
3	Как поступить, если злоумышленники взломали Ваш аккаунт, поменяв пароль и адрес электронной почты, к которой был привязан профиль?	a. Ничего страшного не произошло, нет необходимости восстанавливать аккаунт, проще завести новый. b. Обратиться к администрации того сайта о том, чтобы Вам восстановили доступ к аккаунту. c. Попросить злоумышленников, чтобы они вернули Вам доступ к аккаунту. d. Обратиться к знающему человеку, который сможет взломать Ваш аккаунт и вернуть доступ Вам. e. Доступ к взломанному аккаунту невозможно вернуть.
4	Что такое «родительский контроль» в рамках Интернета?	a. Программа специального назначения, контролирующая использование компьютера ребенком. b. Скрытая камера, которая установлена к комнате ребенка. c. Постоянное нахождение родителей вместе с ребенком.
5	Может ли мошенничеством являться электронным риском?	a. Может, так как мошенники часто прибегают к помощи технических средств для достижения своих целей. b. Не может, потому что в Интернете нет мошенников.
6	С помощью чего пользователь может попасть в Интернет?	a. Гиперссылки. b. Веб-страницы. c. Браузера.
7	Что нужно делать, чтобы антивирусная программа была продуктивной?	a. Обновлять антивирусную базу. b. Не посещать сайты, где нет уверенности, что сайт находится под защитой. c. Не отключать антивирусную программу. d. Выполнять всё вышеперечисленное.
8	Всегда ли можно быть уверенным, что сообщения в Интернете приходят от указанного отправителя?	a. Нет, так как данные отправителя можно подделать. b. Да, если Вам знаком отправитель.
9	Какой лучше выбрать пароль из указанных вариантов?	a. ViKATOi55 b. Sasha11111 c. Дата рождения родственника/друга
10	Какой из представленных паролей самый сложный?	a. Alexandr96 b. Ar!nA_12.96

Продолжение таблицы 1

1	*2*	*3*
		c. angelina96
11	Знаете ли Вы, что такое детская банковская карта?	a. Да. b. Нет.
12	Из каких источников Вы узнали про детскую банковскую карту?	a. От друзей/знакомых. b. От родителей. c. Из СМИ.
13	Хотели бы Вы приобрести детскую банковскую карту?	a. Нет. b. Да. c. У меня уже есть такая.
14	С какой целью Вы бы хотели приобрести детскую банковскую карту?	a. Оплата покупок. b. Накопление и сохранение денежных средств. c. Ведение бюджета. d. Всё вышеперечисленное.
Спасибо за внимание!		

Так, предложенный тест, состоящий из 14 вопросов, позволяет нам проследить то, насколько дети вовлечены в информационно-коммуникационную сеть Интернет; как они могут защитить себя и свою информацию от угроз в Интернете и, что нужно предпринять родителям и педагогам для того чтобы обезопасить их в глобальном информационном пространстве. Также, данный тест можно дополнить другими различными вопросами, касаемо этой темы.

2.2 Анализ результатов исследования

С помощью данного тестирования мы интерпретировали результаты обучающихся 4 класса. Нами были получены следующие результаты, представленные в таблице 2:

Таблица 2 – Индивидуальные результаты исследования уровня сформированности основ кибербезопасности

№ п/п	Вопросы теста	Правильные ответы (кол-во опрашиваемых)	Соотношение в %
1	2	3	4
1	На адрес электронной почты пришел файл с игрой от неизвестного пользователя. Как Вы поступите?	24	92

Продолжение таблицы 2

1	*2*	*3*	*4*
2	В социальной сети с Вами познакомился ученик из Вашей школы, которого Вы ни разу не	21	80
	видели, и он пригласил Вас на встречу с ним. Ваши действия?		
3	Как поступить, если злоумышленники взломали Ваш аккаунт, поменяв пароль и адрес электронной почты, к которой был привязан профиль?	19	73
4	Что такое «родительский контроль» в рамках Интернета?	19	73
5	Может ли мошенничеством являться электронным риском?	22	84
6	С помощью чего пользователь может попасть в Интернет?	15	57
7	Что нужно делать, чтобы антивирусная программа была продуктивной?	22	84
8	Всегда ли можно быть уверенным, что сообщения в Интернете приходят от указанного отправителя?	25	96
9	Какой лучше выбрать пароль из указанных вариантов?	18	69
10	Какой из представленных паролей самый сложный?	17	65
11	Знаете ли Вы, что такое детская банковская карта?	20	77
12	Из каких источников Вы узнали про детскую банковскую карту?	20	77
13	Хотели бы Вы приобрести детскую банковскую карту?	26	100
14	С какой целью Вы бы хотели приобрести детскую банковскую карту?	26	100

Проанализировав результаты проведенного исследования, выяснилось, что большинство опрошенных нами обучающихся имеют высокий и средний уровень пользования сетью «Интернет». Более подробно рассмотрим данные результаты на диаграммах.

В ходе тестирования был задан первый вопрос: «На адрес электронной почты пришел файл с игрой от неизвестного пользователя. Как Вы поступите?». Полученные ответы представлены на рисунке 1.

Рисунок 1 – Результаты ответов респондентов на вопрос: «На адрес электронной почты пришел файл с игрой от неизвестного пользователя. Как Вы поступите?»

Исходя из рисунка 1, мы видим, что 92 % (24 человека) сделают правильное решение и не откроют файл с игрой от неизвестного пользователя, 4 % (1 человек) – скачает файл и начнет играть, 4 % (1 человек) – отправит данный файл своим друзьям.

Нас интересовал вопрос: «В социальной сети с Вами познакомился ученик из вашей школы, которого Вы ни разу не видели, и он пригласил Вас встретиться с ним. Что делать?», результаты которого представлены на рисунке 2.

Рисунок 2 – Результаты ответов респондентов на вопрос: «В социальной сети с Вами познакомился ученик из вашей школы, которого Вы ни разу не видели, и он пригласил Вас встретиться с ним. Что делать?»

По рисунку 2 видно, что 80 % (21 ученик) не пойдет на встречу, 11 % (3 ученика) пойдет на встречу вместе с мамой или папой, 9 % (2 ученика) пойдет на встречу.

Следующий заданный вопрос обучающимся: «Как поступить, если злоумышленники взломали ваш аккаунт на онлайн-ресурсе и поменяли пароль и адрес почтового ящика, к которому был привязан аккаунт?», результаты которого представлены на рисунке 3.

Рисунок 3 – Результаты ответов респондентов на вопрос: «Как поступить, если злоумышленники взломали ваш аккаунт на онлайн-ресурсе и поменяли пароль и адрес почтового ящика, к которому был привязан аккаунт?»

Исходя из рисунка 3 видно, что 73 % (19 человек) опрошенных обратились бы к администрации с просьбой вернуть доступ к аккаунту; 13 % (3 человека) – завели бы новый аккаунт, не восстанавливая старый; 7 % (2 человека) – обратились бы к злоумышленникам с просьбой вернуть аккаунт; 7 % (2 человека) – попросили бы знакомого хакера взломать аккаунт и вернуть его; 0 % - вернуть аккаунт невозможно.

Далее был задан вопрос: «Что такое «родительский контроль» в Интернете?», результаты которого видны на рисунке 4.

Рисунок 4 – Результаты ответов респондентов на вопрос: «Что такое родительский контроль?»

Судя по рисунку 4, 73 % (19 учеников) знают, что такое «родительский контроль» в Интернете; 20 % (5 учеников) считают, что это постоянное нахождение родителей с ребенком; 7 % (2 ученика) думают, что это скрытая камера.

Следующий заданный нами вопрос: «Может ли мошенничество быть электронным риском?», результаты которого представлены на рисунке 5.

Рисунок 5 – Результаты ответов респондентов на вопрос: «Может ли мошенничество быть электронным риском?»

По данному рисунку можно сделать такой вывод, что 84 % (22 школьника) ответили верно «да, может», 16 % (4 школьника) ответили неверно.

Далее был задан вопрос: «С помощью чего пользователь может попасть в Интернет?», результаты которого изображены на рисунке 6.

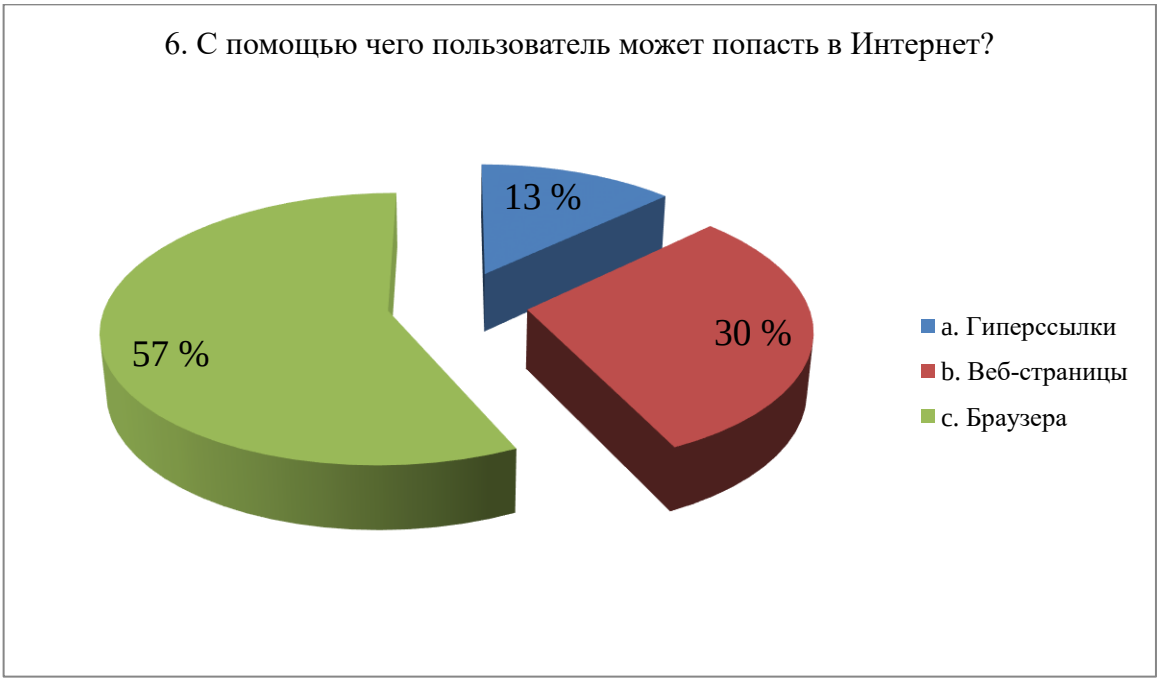


Рисунок 6 – Результаты ответов респондентов на вопрос:
«С помощь чего пользователь может попасть в Интернет?»

По данным рисунка 6 видно, что 57 % (15 учеников) выбрали верный вариант – браузера; 30 % (8 учеников) ошиблись, выбрав вариант – веб-страницы и 13 % (3 ученика) также ошиблись, выбрав вариант – гиперссылки.

Далее был задан следующий вопрос: «Что надо делать, чтобы антивирусная программа была эффективной?», результаты которого показаны на рисунке 7.

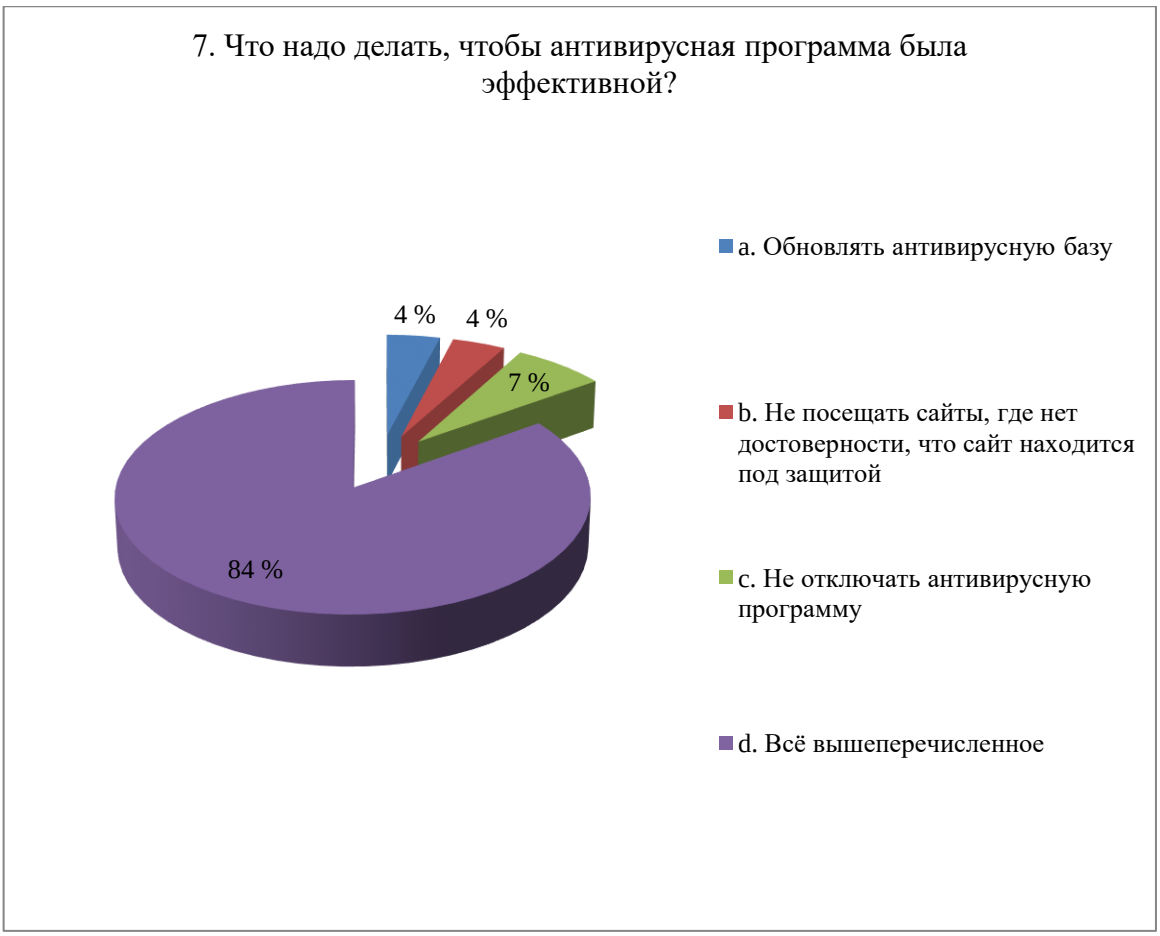


Рисунок 7 – Результаты ответов респондентов на вопрос:
«Что надо делать, чтобы антивирусная программа была эффективной?»

Исходя из ответов по рисунку 7, можно сказать, что большая часть опрашиваемых – 84 % (22 человека) знают, что нужно для эффективности антивирусной программы; 7 % (2 человека) выбрали верный вариант, но этого недостаточно для полной эффективности; остальные респонденты – аналогично предыдущим.

Далее был представлен следующий вопрос: «Всегда ли можно быть уверенным, что электронное письмо получено от указанного отправителя?», ответы на которые показаны на рисунке 8.

Рисунок 8 – Результаты ответов респондентов на вопрос: «Всегда ли можно быть уверенным, что электронное письмо получено от указанного отправителя?»

По данному вопросу справились практически все респонденты – 96 % (25 человек); 4 % (1 человек) ошибся, выбирая ответ «да».

Затем мы спросили: «Какой из предложенных паролей лучше выбрать?», результаты представлены на рисунке 9.

Рисунок 9 – Результаты ответов респондентов на вопрос: «Какой из предложенных паролей лучше выбрать?»

Проанализировав рисунок 9, мы заметили, что у младших школьников возникли трудности при выборе пароля, так как 69 % (18 человек) только приняли правильное решение; 20 % (5 человек) допустили ошибку, потому что такой пароль не совсем надежный; 11 % (3 человека) указали дату рождения родственника, что недопустимо в целях сохранности личных данных.

Следующий заданный вопрос схож с предыдущим: «Какой пароль является самым сложным?», результаты которого показаны на рисунке 10.

Рисунок 10 – Результаты ответов респондентов на вопрос:
«Какой пароль является самым сложным?»

По данному рисунку можно сделать вывод, что некоторые дети не понимают, как нужно выбирать пароль для увеличения безопасности своего аккаунта: 65 % (17 человек) выбрали верный ответ; 24 % (6 человек) остановились на пароле среднего уровня; 11 % (3 человека) выбрали наиболее подвергаемый пароль к взлому.

Затем был задан вопрос: «Знаешь ли ты, что такое детская банковская карта?», результаты которого представлены на рисунке 11.

Рисунок 11 – Результаты ответов респондентов на вопрос:
«Знаешь ли ты, что такое детская банковская карта?»

Исходя из ответов опрашиваемых, видно по рисунку, что большинство осведомлены какой-либо информацией о детской банковской карте – 77 % (20 человек); почти четверть обучающихся – 23 % (6 человек) не знают, что такое детская банковская карта.

Следующий вопрос мы задали такой: «Из каких источников ты узнал про детские банковские карты?», результаты которого представлены на рисунке 12.

Рисунок 12 – Результаты ответов респондентов на вопрос:
«Из каких источников ты узнал про детские банковские карты?»

По данным на рисунке мы видим, что 77 % (20 человек) обучающихся узнали про детские банковские карты из разных источников: 38 % (10 человек) – от родителей; 23 % (6 человек) – от друзей/знакомых; 12 % (4 человека) – из СМИ; однако 23 % (6 человек) – не были знакомы с таким понятием.

Далее мы попросили ответить на следующий вопрос: «Хотел бы ты приобрести детскую банковскую карту?», ответы на который представлены на рисунке 13.

Рисунок 13 – Результаты ответов респондентов на вопрос «Хотел бы ты приобрести детскую банковскую карту?»

По этому рисунку можно сказать, что практически все респонденты 92 % (24 человека) хотели бы приобрести детскую банковскую карту; 8 % (2 человека) уже имеют ее.

Последний вопрос, который был задан школьникам: «С какой целью ты бы хотел приобрести детскую банковскую карту?», результаты которого показаны на рисунке 14.

Рисунок 14 – Результаты ответов респондентов на вопрос: «С какой целью ты бы хотел приобрести детскую банковскую карту?»

По данным рисунка можно сделать вывод, что 100 % респондентов определили цель использования детской банковской карты, из которых 11 % (3 человека) выбрали накопление и сохранение денежных средств; 20 % (5 человек) – ведение бюджета; 31 % (8 человек) – оплату покупок; 38 % (10 человек) – всё вышеперечисленное.

Таким образом, из данного тестирования мы выяснили, что дети знают о безопасности в сети, как защитить свою информацию и что такое детская банковская карта. Результаты исследования каждого обучающегося представлены в таблице 3 (приложение 2): из 26 опрошенных – 8 учеников имеют высокий уровень пользования сетью «Интернет», 16 учеников – средний; 2 ученика – слабый.

2.3 Рабочая программа курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников

Программа включает в себя пояснительную записку, планируемые результаты освоения программы, содержание и календарно-тематическое планирование курса «Кибербезопасность в сети», которая расположена в приложении 3.

Цель изучения «Кибербезопасность в сети»: дать общие представления о кибербезопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

Задача курса «Кибербезопасность в сети»: совершенствование школьного образования и подготовки в сфере информационных технологий, а также популяризация профессий, связанных с информационными технологиями.

Особенность данного курса заключается в том, что многие предметные знания и способы деятельности (включая использование средств ИКТ) имеют значимость для других предметных областей и формируются при их изучении.

В данном параграфе мы приведем 2 технологические карты, включенных в программу курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников на темы: «Безопасность в сети Интернет» и «Поиск информации в Интернете».

ТЕХНОЛОГИЧЕСКАЯ КАРТА №1

Класс: 4

Тема: «Безопасность в социальных сетях»

Понятия: безопасность; социальные сети; информационная безопасность; информационные угрозы.

Цели занятия:

Обучающая:

– познакомить детей с понятиями «социальные сети», «безопасность», «информационная безопасность», «информационные угрозы».

Развивающая:

– формировать коммуникативную культуру личности в информационной среде.

Воспитательная:

– формировать навыки безопасного использования сети Интернет.

Планируемые образовательные результаты:

Предметные:

– выделение информационных процессов в социальных системах.

Личностные:

– умение обеспечивать защиту значимой информации и личную информационную безопасность.

Метапредметные:

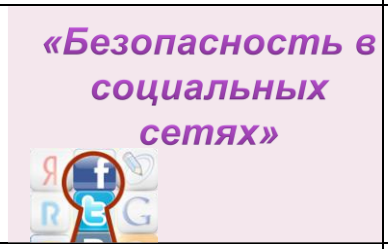
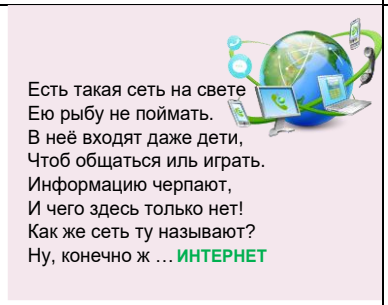
– формирование навыков повседневного использования интернета и электронных устройств, применяя правила безопасности.

Формы работы обучающихся: индивидуальная, групповая, фронтальная.

Оборудование: компьютер, мультимедийный проектор, презентация «Безопасность в социальных сетях».

Ход занятия

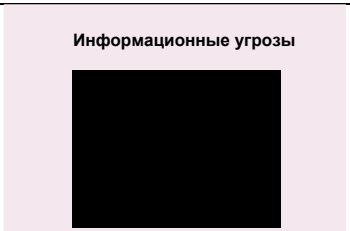
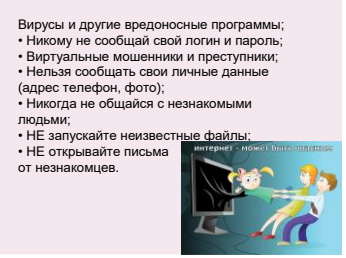
Таблица 3 – Технологическая карта №1 «Безопасность в социальныхсетях»

Этапы урока	Деятельность учителя	Деятельность обучающихся	Средства обучения	Формы работы	УУД
1	*2*	*3*	*4*	*5*	*6*
Организационный момент (1 мин)	Приветствует обучающихся, проверяет готовность к учебному занятию, организует внимание детей	Приветствуют учителя, организуют свое рабочее место		Индивидуальная	
Проверка домашнего задания (1 мин)	Отправьте свое выполненное д/з мне на почту			Индивидуальная	
Актуализация знаний (4 мин)	Показывает слайд с наглядной информацией, подводящей к понятию Интернет, читает загадку: Он знает всё и даже больше, И к нам на помощь поспешит. Любой вопрос, пусть очень сложный, Мгновенно с лёгкостью решит. Плетёт свою он паутину, Хотя, по сути, не паук. Он видит всё. Вы догадались? А, ну-ка, что это за друг? (интернет).	Слушают учителя, воспринимают предъявляемую информацию, анализируют ее и отвечают на вопрос загадки. Ответы детей: Интернет	 	Фронтальная	Познавательные УУД: Коммуникативные УУД: развитие диалогической речи

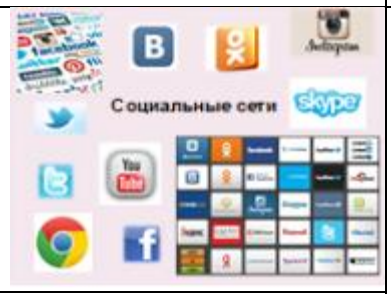
Продолжение таблицы 3

1	*2*	*3*	*4*	*5*	*6*
	Задает вопросы и ведет диалог с обучающимися. В ходе диалога показывает слайд с наглядной информацией об использовании Интернета. Вопросы: - Ребята, скажите, кто может пользоваться сетью Интернет? А с какой целью? - По-вашему мнению, есть ли какие-нибудь опасности при использовании сети Интернет? - Что вы понимаете под понятием угроза? - Откуда может исходить угроза? - Как вы думаете, что значит быть безопасным, что такое «безопасность»? - А как вы думаете, что же такое информационная угроза и информационная безопасность.	Отвечают на вопросы учителя. Воспринимают и анализируют информацию на экране. Ответы детей: Общение с друзьями, поиск информации, фильмы, игры и др. Опасно когда что то угрожает. Угроза – запугивание, намерение причинить кому-нибудь неприятность, зло или вред. От взрослых, одноклассников, знакомых при личном общении, через мобильную связь, через Интернет. Безопасность – отсутствие угроз или состояние защищенности от угроз. Ситуация, при которой не угрожает опасность кому-нибудь или чему-нибудь.			

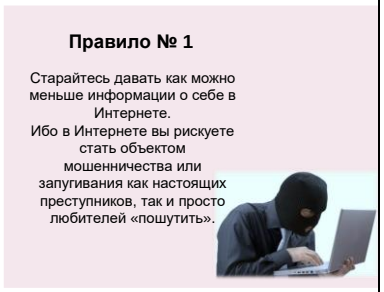
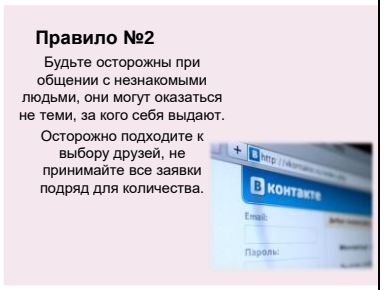
Продолжение таблицы 3

1	*2*	*3*	*4*	*5*	*6*
	Развернутые ответы: (Информационная угроза- потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации. Информационная безопасность детей – состояние, при котором отсутствует риск, связанный с причинением информацией вреда физическому, психическому, социальному, духовному и нравственному здоровью и развитию детей.	Ответы детей			
Объяснение нового материала (20 мин)	Создает условия для выделения учениками информационных угроз. Давайте, посмотрим видеоролик и каждый попробует выделить информационную угрозу.	Выделяют основные информационные угрозы.		Индивидуальная работа	Познавательные УУД: извлечение необходимой информации из видеоинформации; структурирование знаний, рефлексия способов и условий действий, Личностные УУД: развитие логического мышления, знание основных моральных норм
	Теперь сверим, о том что узнали вы и какие ещё бывают информационные угрозы.	1. Компьютерные вирусы. 2. Доступ к нежелательной информации. 3. Контакты с незнакомыми людьми с помощью чатов или электронной почты. 4. Неконтролируемые покупки.		Фронтальная работа	

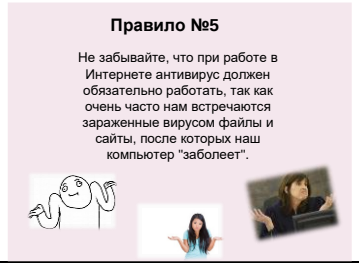
Продолжение таблицы 3

1	2	3	4	5	6
	Подводит к понятию социальные сети. Организует обсуждение, объясняя новый материал, показывая слайды презентации.	Участвуют в обсуждении, отвечают на вопросы			Познавательные УУД: извлечение необходимой информации из прослушанных текстов. коррекция полученного результата
	Вопросы: Ребята, на занятии мы говорили о том, что Интернет – это сеть, в которой компьютеры связаны между собой. За каждым компьютером сидит человек. Получается, что люди тоже связаны между собой одной сетью. Как думаете, о чем идет речь? Это сети называются социальными. Кто из вас знает, что есть в социальной сети? Кто пользовался ей? Однако люди бывают разными. И в социальных сетях можно встретить опасности, хулиганов. Чтобы не допустить этого, предлагаю нам попробовать выделить правила безопасного использования Интернета.	Ответы детей: Интернет, социальные сети. Сайты, которые созданы для объединения людей по определенному признаку или интересу, социальные взаимоотношения в Интернете (пол, интересы, профессия, деятельность, творчество, игры, музыка и пр.) Вконтакте, Одноклассники, Фейсбук, Телеграмм, Твиттер, Инстаграм и пр.			

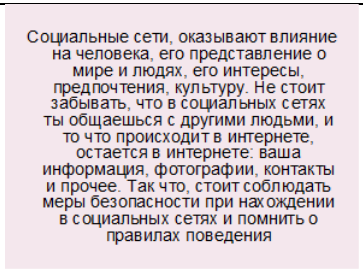
Продолжение таблицы 3

1	2	3	4	5	6
	Ставит задачу (выделение правил) перед обучающимися, инструктирует по порядку выполнение работы. Каждая группа прорабатывает правило по безопасности в социальных сетях на одной остановке, затем перемещаются на следующую и дополняют написанное, предыдущей группой, но, не изменяя ничего, переходят на другую остановку, пока снова не вернутся на свою начальную остановку. (На каждую остановку дается 3 минуты) Корректирует деятельность обучающихся, отвечает на возникшие вопросы.	Выполняют задания в группах. Осуществляют перемещение по остановкам и и прорабатывают правила. Ответы детей: (Не сообщайте свой электронный адрес никому, кроме людей, которым доверяете. Тщательно обдумайте, какую информацию о себе стоит загружать в Интернет. Осторожно подходите к выбору друзей, не принимайте все заявки подряд. Не открывайте доступ к своим личным страницам незнакомым людям. Обязательно установите антивирус, обновляйте его регулярно. Будьте осторожны при общении с незнакомыми людьми. Нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы родителей и т.д.;)	Ватман, карандаши, фломастеры.   	Групповая работа	Коммуникативные УУД: Ориентация на партнера по общению, умение слушать собеседника, умение аргументировать свое мнение, убеждать и уступать Регулятивные УУД: планирование своей деятельности для решения поставленной задачи, контроль полученного результата,

Продолжение таблицы 3

1	2	3	4	5	6
			 		
	Организует проверку выполнения заданий.	Каждая группа выступает с выполненным заданием.			
Физкультминутка (1 мин)	Это лёгкая забава – Повороты влево-вправо. Нам известно всем давно – Там стена, а там окно. (Повороты туловища вправо и влево.) Приседаем быстро, ловко. Здесь видна уже сноровка. Чтобы мышцы развивать, Надо много приседать. (Приседания.) А теперь ходьба на месте, Это тоже интересно. (Ходьба на месте.)	Выполняют физминутку.			

Продолжение таблицы 3

1	*2*	*3*	*4*	*5*	*6*
Первичное закрепление знаний (10 мин)	Проводит тест, чтобы закрепить полученные знания.	Самостоятельно выполняют тест	Раздаточный материал каждому на листочках	Индивидуальная работа	Личностные УУД: развитие логического мышления. Познавательные УУД: структурирование знаний, рефлексия способов и условий действий, контроль и оценка процесса и результатов деятельности.
Итоги занятия. Рефлексия (2 мин)	*Подводит итог урока. Обеспечивает рефлексию обучающихся. Оценивает работу детей.* *Вопросы:* *- Какие правила нужно соблюдать в Интернете?* *- Что из себя представляет Интернет?* *- Можно ли доверять любой информации, полученной из Интернета?* *- Как защитить компьютер при работе в Интернете?* *- Является ли занятие полезным для тебя?* *Раздает памятки и кратко поясняет их.*	*Оценивают свои результаты. Анализируют информацию. Фиксируют выводы.* *Отвечают на вопросы учителя*	 ПАМЯТКА Это важно знать! - Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей. - Я никогда не передам по Интернет своей фотографии. - Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.	Фронтальная	Коммуникативные УУД: построение речевого высказывания в устной форме. Личностные: контроль и оценка процесса и результатов деятельности. Регулятивные УУД: контроль полученного результата, коррекция полученного результата

Продолжение таблицы 3

1	*2*	*3*	*4*	*5*	*6*
			- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате. - Я буду разговаривать об Интернет с родителями. - Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал вИнтернет.		
Домашнее задание (1 мин)	Задает домашнее задание. Инструктирует обучающихся по выполнению домашнего задания. Выражает благодарность за работу в классе.	Записывают домашнее задание.	 Спасибо за внимание!!! 		

Тест на тему: «Безопасность в социальных сетях»:

1. Что такое Интернет?

а) вычислительная сеть

б) всемирная сеть

в) компьютерная игра

2. Нужно ли в интернете всем сообщать свою фамилию, имя, адрес, номер школы?

а) всем виртуальным друзьям нужно рассказать о себе

б) никогда не сообщать личную информацию

в) сообщать только вымышленную информацию

3. Можно ли отправлять SMS или оставлять свой номер телефона с незнакомого сайта, чтобы получить код доступа к игре или подарку?

а) никогда не следует отправлять SMS или давать свой номер телефона

б) всегда оставлять номер телефона, а SMS слать нельзя

в) всегда отправлять сообщение и давать номер, чтобы получить код доступа

4. Виртуальный друг предлагает встретиться, ваши действия:

а) встретиться с виртуальным другом в торговом центре

б) сообщить родителям о встрече

в) встретиться с виртуальным другом в заброшенном, таинственном месте

5. На вашу электронную почту пришло письмо от неизвестного адресата, вы:

а) сохраните в черновики и откроете позднее

б) откроете немедленно

в) никогда не открываете писем от неизвестных адресатов

6. В сети вы встретились с дразнилками и оскорблениями, вы:

а) отвечаете грубостью

б) заблокируете этого человека и сообщите родителям

в) никому об этом не говорите

7. Антивирусная программа – ...

а) программа обнаружения вирусов на вашем компьютере

б) название журнала о компьютерах

в) программа закаливания организма

8. Сколько времени детям, по мнению специалистов, можно проводить за компьютером?

а) пока не выиграешь в любимую игрушку

б) пока не подготовишься к урокам

в) не более часа в день

ТЕХНОЛОГИЧЕСКАЯ КАРТА №2

Класс: 4

Тема: «Поиск информации»

Понятия: «сеть»; «поиск; «система поиска»

Цель: обеспечить формирование у обучающихся навыков и умений поиска заданного фрагмента и замены его на другое знаний о процессе поиска и замене информации;

Планируемые образовательные результаты:

Предметные:

– сформировать представление о поиске информации.

Метапредметные:

– ученик научится использовать средства информационных технологий для преобразования текстовой информации;

– ученик получит возможность самостоятельно производить поиск, сбор и выделение существенной информации из различных источников или файлов.

Личностные:

– формирование умения наблюдать, анализировать, сравнивать, делать выводы;

– навык построения таблиц с применением текстового процессора.

Формы работы обучающихся: фронтальная, индивидуальная, групповая (парная).

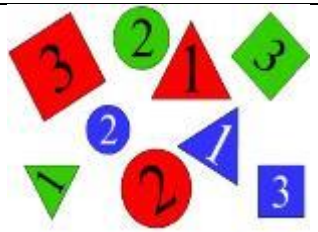
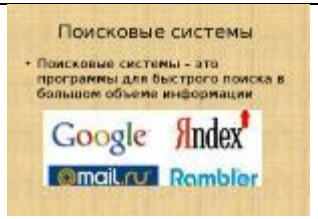
Оборудование: компьютер, мультимедийный проектор, презентация «Поиск информации в Интернете».

Ход занятия

Таблица 4 – Технологическая карта №2 «Поиск информации»

Этапы урока	Деятельность учителя	Деятельность обучающихся	Средства обучения	Формы работы	Формируемые УУД
1	*2*	*3*	*4*	*5*	*6*
Организационный момент (1 мин)	Приветствует обучающихся, проверяет готовность к занятию, организует внимание детей	Приветствуют учителя, проверяют наличие учебного материала на столах, организуют свое рабочее место		Индивидуальная	Коммуникативные: планирование учебного сотрудничества со сверстниками Личностные: психологическая готовность обучающихся к уроку, самоопределение
Актуализация знаний и формулирование темы и целей занятия (4 мин)	Для начала давайте вспомним, что мы рассматривали на прошлом занятии. Задания на слайдах (Предположите, что можно сделать с данной информацией: сортировка по фамилии, сортировка по группам, сортировка по размеру планет, сортировка по положению планет) Задание показать в учебнике определение обработки информации. А какой обработкой информации вы сейчас занимались?	Анализ и интерпретация информации, сохранение и передача информации Дети пытаются сделать задание, но у них возникают затруднения Поиск информации	 	Фронтальная	Познавательные: структурирование знаний, рефлексия способов и условий действий, контроль и оценка процесса и результатов деятельности Регулятивные: – развитие умения формулировать тему и цель урока в соответствии с задачами и нормами русского языка Коммуникативные: Ориентация на партнера по общению, умение слушать собеседника, умение аргументировать свое мнение, убеждать и уступать Личностные: развитие логического мышления, знание основных моральных норм

Продолжение таблицы 4

1	2	3	4	5	6
	А благодаря чему вы смогли найти определение? Если вы помните на схеме видов обработки информации поиск стоит рядом с систематизацией. Так, систематизация и поиск информации тесно связаны между собой.	Систематизации информации			
	- Скажите, а где в наше время можно найти практически любую информацию?	Интернет			
	Сформулируйте тему занятия.	Записываем в тетрадь тему занятия и число. Поиск информации в Интернете			
Усвоение новых знаний (7 мин)	Как вы думаете, информация в Интернете систематизирована? Чем же тогда нужно воспользоваться для поиска информации? (Показ поисковых систем на слайде) Что такое поисковая система? Как используем? Что и куда будем писать?	Нет Записывают в тетрадь: «Для поиска информации в сети Интернет используются поисковые системы» Записывают определение поисковой системы. Строка поиска, запроса Делают вывод по теме занятия		Индивидуальная	решения поставленной задачи, контроль полученного результата, коррекция полученного результата Личностные: развитие внимания, зрительной и слуховой памяти, возможность самостоятельно осуществлять деятельность обучения Коммуникативные: умение работать в группах, развитие диалогической речи

Продолжение таблицы 4

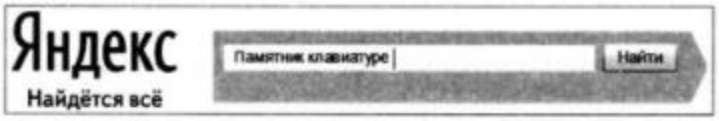
1	*2*	*3*	*4*	*5*	*6*
Первичное закрепление материала (9 мин)	Замечание. Я совершил ещё одну ошибку. Пользоваться нужно как минимум двумя поисковыми системами. Но мало найти информацию, нужно ещё её уметь сохранить. И последнее, если вы собираетесь использовать как либо, найденную информацию, вы обязаны указать источники информации.	Например, кубик Рубика Копирование текста, сохранение рисунков		Индивидуальна, парная	Познавательные: выбор наиболее эффективных способов выполнения задания Личностные: формирование умений систематизации объектов
Практическая работа (15 мин)	Предлагает выполнить задание практической работы (рис. 15)	Выполняют парами задание практической работы. Закрепляют навыки поиска, систематизации и сохранения информации. Получают помощь в выполнении заданий, если она требуется при затруднении.		Парная	Личностные: формирование навыков работы в текстовом редакторе; закрепление умений поиска и систематизации информации.
Итоги занятия. Рефлексия (3 мин)	На какую тему мы с вами сегодня разговаривали? Вам было легко? С какими трудностями вы столкнулись? Что у вас получилось лучше всего и без ошибок? Какое задание было самым интересным и почему? Как бы вы оценили свою работу?	Отвечают на вопросы учителя		Фронтальная	Познавательные: Построение речевого высказывания в устной форме, контроль и оценка процесса и результатов деятельности Регулятивные: контроль и оценка своей деятельности в рамках урока Коммуникативные: умение слушать и вступать в диалог,

Продолжение таблицы 4

1	*2*	*3*	*4*	*5*	*6*
					формулирование и аргументация своего мнения Личностные: рефлексия способов и условий действия, контроль и оценка процесса и результатов деятельности
Домашнее задание (1 мин)	Выучить записи в тетради	Работа с дневниками		Индивидуальная	Личностные: формирование навыков самоорганизации - формирование навыков письма

Задание 1

1. **Подключитесь к Интернету.**
2. **Выберите одну из поисковых систем.**
3. **Зайдите на один из сайтов поисковых систем: google.ru, yandex.ru, mail.ru, rambler.ru.**
4. **Введите в специальное окно свой поисковый запрос «Памятник клавиатуре» и щёлкните мышью на кнопке Найти.**



5. **Результат поиска — ссылки на огромное количество найденных Интернет-страниц. Каждая ссылка сопровождается кратким описанием имеющейся на странице информации. Сначала идут ссылки на страницы, содержание которых наиболее полно и точно соответствует запросу. Говорят, что страницы отсортированы по релевантности. Зайдите на 2–3 сайта из верхней части списка. Прочитайте информацию о памятнике клавиатуре.**
6. **В текстовом редакторе откройте документ Клавиатура.rtf из папки Заготовки:**

Памятник клавиатуре

Место расположения памятника	
Дата открытия памятника	
Материал, из которого изготовлен памятник	
Описание внешнего вида	
Графическое изображение	
Размеры	
Автор проекта памятника	

7. **Заполните таблицу на основании найденной вами информации. Можете выделять и копировать нужную информацию с Интернет-страниц.**
8. **Под таблицей укажите информационный источник — адрес сайта (сайтов), на котором вы нашли нужную информацию.**
9. **Сохраните файл в личной папке под тем же именем и закройте программу.**

Рисунок 15 – Практическая работа

Выводы по главе 2

На основе теоретических положений, изложенных в первой главе, во второй главе представлены результаты проведенного исследования, а также разработка программы курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников и подробное изложение двух занятий.

Мы определили, что обучающиеся 4 класса имеют хорошие навыки пользования Интернетом, осведомлены о том, как нужно себя обезопасить в Глобальной сети и что нужно предпринять в случае информационной угрозы. Большинство младших школьников (16 человек) показали средний уровень сформированности основ кибербезопасности, меньшая часть (8 человек) – высокий уровень, и только лишь 2 респондента показали слабый уровень. Данные показатели позволили нам сделать вывод о том, что дети начальной школы всё же подвержены различным опасностям в сети «Интернет», несмотря на то, что многие знают, что нужно делать в той или иной ситуации. Однако, и для тех, кто более опытный в данной сфере, и для тех, кто наиболее всего подвержен информационным угрозам, нужно оказать помощь и контроль в этом направлении. Это необходимо для того чтобы дети умели правильно пользоваться электронными источниками, владеть информацией, правильно ее анализировать и отбирать. В связи с этим, мы считаем, что внедрение модуля по формированию основ кибербезопасности у младших школьников во внеурочной деятельности, является неотъемлемой частью обучения детей, как для их безопасности в Интернете, так и для всестороннего развития каждого обучающегося. Поэтому мы предлагаем разработку курса программы внеурочной деятельности по формированию основ кибербезопасности у младших школьников, рассчитанную на 1 учебный год (36 часов), включающую в себя календарно-тематическое планирование, а также 2 занятия по данному направлению.

Таким образом, мы выяснили, что данные разработки помогут обучающимся в том, что они смогут лучше разбираться в информационной среде, быть продвинутыми пользователями и владеть необходимыми базовыми знаниями и умениями по данному направлению; их родителям – в том, что они могут быть более уверенными в безопасности своих детей от информационных угроз и различных уловок мошенников; а также и педагогам, которые смогут оказать помощь во время внеурочных занятий и не только, если у учеников возникнут какие-либо вопросы, получив нужную информацию, благодаря этому модулю.

ЗАКЛЮЧЕНИЕ

Подводя итоги данной работы, важно отметить, что изучение основ кибербезопасности будет более эффективным, если внедрить данный модуль в начальной школе в рамках внеурочной деятельности.

Проблема информационной безопасности и кибербезопасности личности действительно существует, нарушая состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, отсюда появляется необходимость активной разработки проблематики кибербезопасности.

Для эффективного и полноценного развития ребенка не нужно создавать соответствующую информационную среду, необходимо заниматься кибербезопасностью личности обучающегося, т.е. научить ребенка жить в информационной среде, видеть опасности, исходящие от информации, уметь предвидеть и реагировать на информационную угрозу в СМИ.

Проблемам кибербезопасности в психолого-педагогической литературе, учебных программах не уделено достаточно внимания, вследствие чего, младших школьников не обучают умению выявлять информационную угрозу и противостоять ей. Отсутствие законодательства в области информационной политики детей и подростков предполагает активное участие педагогов в обучении школьников информационной безопасности.

Рассмотрев теоретические аспекты формирования основ кибербезопасности у младших школьников во внеурочной деятельности, мы изучили следующие задачи:

1. Рассмотрели сущность понятий «кибербезопасность», «информационная безопасность».

Так, в проекте Концепции стратегии кибербезопасности Российской Федерации кибербезопасность – это «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

По мнению А. С. Алпеева, это «кибербезопасность– условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными».

И еще выделили одно понятие из русско-американского словаря, в котором в сфере информационной безопасности термин «кибербезопасность» звучит так – это свойство киберпространства противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз.

2. Проанализировали кибербезопасность как педагогическую проблему.

Далее мы изучили кибербезопасность как педагогическую проблему и пришли к тому, что школа способна реально действовать в решении данной проблемы, создавая и внедряя психолого-педагогические программы, способные подготовить сознание детей к противодействию негативным воздействиям информации, помочь осознать младшим школьникам их цели, потребности и способы их удовлетворения с помощью телевидения, сети Интернет, формировать визуальную грамотность и навыки критического осмысления информации и информационнуюсамостоятельность.

3. Изучили особенности развития младшего школьника как фактор эффективности формирования основ кибербезопасности во внеурочной деятельности.

Мы выделили следующее:

– для младших школьников высок авторитет учителя, следовательно, дети полностью доверяют информации, исходящей от него;

– познавательные интересы детей сформированы, он готов к восприятию материалашкольной программы;

– углубленная и умственная работа зависит от усидчивости, сдерживания эмоций и внимания, младшим школьникам необходимы занятия по безопасности в классах, в игровых комнатах с учетом возрастных особенностей, с использованием социально-психологических ролей;

– так как сотрудничество является необходимым условием психического состояния ребенка, в обучении кибербезопасности ребенок в тех или иных ситуациях осваивает новое, через методы и формы обучения, при этом воздействия адресованы ребенку, учитывая его индивидуальные особенности;

– учитывая слабое развитие у младшего школьного возраста самостоятельного мышления, присутствует необходимость в занятиях по кибербезопасности, которые помогают формировать критическое отношение к предлагаемой информации.

4. Провели экспериментальную работу поформированию основ кибербезопасности младших школьников во внеурочной деятельности.

Выяснили, что информационная безопасность и кибербезопасность играет большую роль в развитии младших школьников. Мы определили уровень сформированности основ кибербезопасности у младших школьников и сделали вывод, что большинство обучающихся 4 класса имеют средний и высокий уровень. Это позволяет утверждать то, что дети менее подвержены к угрозам в Интернете. Они достаточно осведомлены о возможной опасности в сети; знают, как справляться с различными вирусами и взломщиками. Однако, несмотря на это, есть ребята, имеющие слабый уровень, соответственно они наиболее подвержены к

недостоверной информации в Интернете, могут делиться своими данными, не подразумевая о том, что это может быть опасно.

Исходя из этого, мы считаем, что формировать основы кибербезопасности у младших школьников во внеурочной деятельности необходимо.

5. Определили содержание рабочей программы курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников.

В ней мы предоставили курс, включающий в себя содержание и календарно-тематическое планирование занятий, рассчитанный на 1 учебный год на 36 часов 1 раз в неделю. А также привели примеры2 технологических карт по темам: «Безопасность в сети Интернет» и «Поиск информации в Интернете», чтобы вкратце показать, как во внеурочной деятельности модуль «Кибербезопасность в сети» реализуется на практике.

Развитие ребенка в информационном пространстве на начальных этапах обучения в школе позволит ему в будущем оценивать и воспринимать информацию с учетом полученных знаний благодаря эффективности обучения школьников основам кибербезопасности.

Таким образом, цель работы достигнута, поставленные задачи выполнены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алигулиев, Р. М. Вопросы защиты детей школьного возраста от интернет-зависимости [Текст] / Р.М. Алигулиев, Р.Ш. Махмудова, Р. Ш. Махмудов. // Дистанционное и виртуальное обучение, Москва, 2011. – № 5. – С. 97–107.

2. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность [Текст] / А. С. Алпеев. – Москва, 2014. – № 5. – С. 39–42.

3. Будунов, Г. М. Компьютерные технологии в образовательной среде: «за» и «против» [Текст] / Г.М. Будунов. – Москва:Аркти. – 2006. – 192 с.

4. Букина, Е. Ю. Формирование у младших школьников навыков безопасной работы в сети Интернет [Текст] / Е.Ю. Букина // Информатика в школе, Москва, 2014. – № 5 (98). – С. 40–49.

5. Давыдова, М. С. Формирование навыка работы с информацией у младших школьников [Текст] / М.С. Давыдова // Управление начальной школой, Москва, 2016. – № 4. – С. 27–31.

6. Дейкина, А. Ю. Развитие познавательных интересов дошкольников в процессе медиаобразования [Электронный ресурс] // автореф. дис. кан. пед. наук / А.Ю.Дейкина: [сайт] [2000]. URL:https://zh.b-ok.cc/book/516419/3d7122.

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

8. Жидкова, А. В. Понятие «информационная безопасность» на пропедевтическом этапе обучения информатике в школе [Текст] / А. В. Жидкова, Москва, 2017. – № 10. – С. 31–34.

9. Жолобова, С. И. Информационная безопасность современного школьника [Электронный ресурс] // Социальная сеть работников

образования: [сайт] [2013]. URL: http://nsportal.ru/shkola/klassnoe-rukovodstvo/library/2013/10/26/informatsionnaya-bezopasnost-sovremennogo-shkolnika.

10. Инфоурок [Электронный ресурс] // Технологическая карта урока «Безопасность в сети Интернет»: [сайт].[2017]. URL: https://infourok.ru/tehnologicheskaya-karta-uroka-bezopasnost-v-socialnih-setyah-1938688.html.

11. Инфоурок [Электронный ресурс] // Технологическая карта урока «Поиск информации»: [сайт].[2018]. URL:https://infourok.ru/tehnologicheskaya-karta-po-temepoisk-informacii-2796505.html.

12. Ищенко, А. Н., Прокопенко, А. Н., Страхов, А. А. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасностиРоссии информационной сфере [Текст] / А. Н. Ищенко, А. Н.Прокопенко, А. А. Страхов // Проблемы правоохранительной деятельности, Москва, 2017. – № 2. – С. 55–62.

13. Калуга, Д. Д. Информационная безопасность школьников [Электронный ресурс] // Д.Д. Калуга // Первое сентября. Открытый урок: [сайт]. [2003].URL: http://festival.1september.ru/articles/652762.

14. Киселев, Г. М. Информационные технологии в педагогическом образовании [Текст] / учебник / Г.М. Киселев, Р.В. Бочкова. – Москва: Дашков и К. – 2012. – 308 с.

15. Климонтова, Г. Н. Защита информации для современных школьников [Текст] / Г. Н. Климонтова// Воспитательная работа в школе. – 2013. – № 8. – С. 74–81.

16. Концепция стратегии кибербезопасности Российской Федерации. Проект [Электронный ресурс] // Проект [сайт] [2020]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf.

17. Кузьмина, М. В. Как формировать медиакультуру учащихся [Текст] / М.В. Кузьмина // Управление начальной школой, Москва, 2016. – № 9. – С. 12–16.

18. Магдилов, М. М., Магдилова, Л. В. Особенности формирования образовательного курса по интернетбезопасности несовершеннолетних [Текст] / EUROPEAN RESEARCH. Сборник статей XVIII Международной научно-практической конференции ; Под общ.ред. к.э.н. Г.Ю. Гуляева. – Москва: Наука и просвещение. – 2019. – 199 с.

19. Малых, Т. А. Педагогические условия развития информационной безопасности младшего школьника [Электронный ресурс] // автореф. дис. кандпед. наук / Т.А. Малых: [сайт]. [2008]. URL: http://www.ifap.ru/library/book296. pdf.

20. Малых, Т. А. Педагогические условия развития информационной безопасности младшего школьника [Текст]: автореф. дисс. канд. пед. наук Основы безопасности детей и молодежи в Интернете/ Интерактивный курс по интернет – безопасности. –Москва: Иркутск. – 2015. – 56 с.

21. Некрасова, З. В., Некрасова, Н. Н. Как оттащить ребенка от компьютера и что с ним делать [Текст] / З.В. Некрасова, Н.Н. Некрасова // Книга для родителей. – Москва: София. – 2007. – 256 с.

22. Новосельцев, В. И. Компьютерные игры: детская забава или педагогическая проблема? [Текст] / В. И. Новосельцев // Директор школы. – Москва, 2003. – № 9. – С. 13–18.

23. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. N 646 [Текст] / Собрание законодательства РФ, 12.12.2016, N 50, ст. 7074.

24. Обухова, Л. Ф. Возрастная психология: учебник для бакалавров [Текст] / Л. Ф. Обухова. – Москва: Юрайт. – 2013. – 460 с.

25. Остроушко, А. В., Букалеров, А. А., Букалеров, С. А. Защита информационной безопасности несовершеннолетних в КНР [Текст] / LegalBulletin, Москва,2018. –Т. 3. – № 1-2. –С. 56–60.

26. Пидкасистый, П. И. Педагогика: учебник для студентов высших учебных заведений, обучающихся [Текст] / П. И. Пидкасистый, В. А. Мижериков, Т. А. Юзефавичус ; под ред. П.И. Пидкасистого. - 2-е изд., перераб. и доп. – Москва: Академия. – 2014. – 619 с.

27. Подласый, И. П. Педагогика начальной школы [Текст] / И. П. Подласый. – Москва: Владос. – 2008. – 464 с.

28. Распоряжение Правительства от 7 февраля 2008 г. № Пр.-212 «Об утверждении Стратегии развития информационного общества в Российской Федерации»[Электронный ресурс] // [сайт]. [2014]. URL: https://www.garant.ru/products/ipo/prime/doc/92762.

29. Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014-2020 гг. и на перспективу до 2025 г.» [Электронный ресурс] // [сайт]. [2014]. URL: https://base.garant.ru/70498122.

30. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие [Текст] / под ред. Ю.А. Родичев. — Санкт-Петербург: Питер.– 2008. – 272 с.

31. Русско-американский словарь терминов и определений в сфере информационной безопасности [Электронный ресурс] // Всё о цифровой экономике и цифровой политике: [сайт]. [2018]. URL:https://digital.report/cybersecurity-terminology.

32. Синицын, Д. С. Психолого-педагогические условия обучения информационно-психологической безопасности подростков. Дис. канд. пед. наук [Текст] / Д. С. Синицын : 13.00.01 / Рос.гос. пед. ун-т им. А. И. Герцена. – Санкт-Петербург. – 2005. – 19 с.

33. Соболева, Б. Влияние телевизора и компьютера на душу ребенка [Текст] / Б. Соболева // Женское здоровье: сборник научных трудов, Москва, 2000. – № 7. – С. 16–19.

34. Сонькин, В. Н. Чем занимаются наши дети [Текст] / В. Н. Сонькин // Здоровье детей, Москва, 2003.– № 21.– С. 5–10.

35. Стрельцов, А. А. Обеспечение информационной безопасности России [Текст] / А.А. Стрельцов // Теоретические и методологические основы под ред. В. А. Садовничего и В. П. Шерстюка. – Москва:МЦНМО. – 2002. – 86 с.

36. Тверитинова, А. В. Информационно еаудиопространство и безопасность личности (Скрытая угроза FM) [Текст] / А. В. Тверитинова // Психолого-педагогические проблемы влияния телевидения и других СМИ на детей и молодежь, Материалы научно-практической конференции. –- Санкт-Петербург. – 2002. – 51 с.

37. Троицкая, О. Н., Ширикова, Т. С., Безумова, О. Л., Лыткина, Е. А. Концептуальная модель обучения основам кибербезопасности в основной школе [Электронный ресурс] // Современные проблемы науки и образования. – № 5: [сайт] [2018]. URL:https://www.science-education.ru/ru/article/view?id=28073.

38. Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на2012-2017 годы»[Электронный ресурс] // [сайт]. [2014]. URL:https://base.garant.ru/70183566.

39. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью иразвитию» [Текст] / Собрание законодательства РФ. – 2011. – № 1. – Ст. 48.

40. Федеральный закон от13.03.2006 № 38-ФЗ «О рекламе» (принят Государственной Думой 22 февраля 2006 года, одобрен Советом Федерации 3 марта 2006 года, в ред. приказов от 1 мая 2019 г. №89-ФЗ) [Электронный ресурс] // [сайт]. [2014]. URL: https://base.garant.ru/12145525/#friends.

41. Федеральный закон от27.07.2006 № 152-ФЗ«О персональных данных» (принят Государственной Думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года, вред. приказов от31 декабря 2017 г. № 498-ФЗ) [Электронный ресурс] // [сайт]. [2014]. URL: https://base.garant.ru/12148567.

42. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ РФ «Об образовании в Российской Федерации», п. 34 ст. 2. [Электронный ресурс] // Основные понятия, используемые в настоящем Федеральном законе: [сайт]. [2020]. URL: http://www.consultant.ru/document/cons_doc_LAW_140174/b819c620a8c698de35861ad4c9d9696ee0c3ee7a.

43. Фомченкова, Г. А. Научный журнал Проблема становления института безопасности молодежи: результаты нормативно-правового анализа [Текст] / Гуманитарные, социально-экономические и общественные науки, Москва,–2014. – № 9.– С. 77–79.

44. Якушина, Е. В. Подростки в Интернете [Текст] / Е. В. Якушина// Педагогика, Москва,2001.– № 4. – С. 55–62.

45. Янушкявичене, О. Л. Компьютерное обучение в младшей школе [Текст] / О.Л. Янушкявичене, Р.В. Янушкявичюс // Школьные технологии, Москва, 2015. – № 3. – С. 25–27.

46. Ярочкин, В. И. Информационная безопасность: учебное пособие для студентов вузов [Текст] / В.И. Ярочкин // Компьютерная безопасность. –Москва:Междунар. Отношения. – 2000. – 400 с.

ПРИЛОЖЕНИЕ 1

Тест для младших школьников

по информационной безопасности (6-11 лет)

В 2019 году в Российской Федерации прошел Единый урок по безопасности в сети «Интернет», который представляет собой цикл мероприятий, направленных на повышение уровня информационной безопасности детей, и направлен на обеспечение внимания родительской и педагогической общественности к проблеме обеспечения безопасности и развития детей в информационном пространстве.

Инициатором Единого урока выступила спикер Совета Федерации Федерального Собрания Российской Федерации В.И. Матвиенко.

На основании проведения Единого урока был создан тест для младших школьников по информационной безопасности, включающий в себя 10 вопросов, которые имеют только один правильный ответ, и 4 вопроса добавлены нами по осведомленности и использовании обучающимися детскими банковскими картами.

Критерии оценивания участников:

13-14 правильных ответов – высокий уровень сформированности основ кибербезопасности;

10-12 верных ответов – средний уровеньсформированности;

7-9 правильных ответов – слабый уровень;

Менее 6 верных ответов – пользователи, которые сильно подвергнуты к информационным угрозам.

ПРИЛОЖЕНИЕ 2

Таблица 2.1–Индивидуальные результаты исследования обучающихся 4 класса

№ п/п	Имя участника исследования	Количество правильных ответов	Уровень сформированности основ кибербезопасности
1	Алина	11	Средний
2	Вероника	12	Средний
3	Виктория	10	Средний
4	Александра	13	Высокий
5	Артем	9	Слабый
6	Артур	11	Средний
7	Валерия	10	Средний
8	Данил	13	Высокий
9	Софья	10	Средний
10	Екатерина	12	Средний
11	Максим	11	Средний
12	Ольга	13	Высокий
13	Станислав	10	Средний
14	Сергей	11	Средний
15	Марина	10	Средний
16	Тихон	13	Высокий
17	Ульяна	12	Средний
18	Яна	11	Средний
19	Андрей	13	Высокий
20	Светлана	13	Высокий
21	Матвей	11	Средний
22	Алексей	12	Средний
23	Дарья	10	Средний
24	Ксения	9	Слабый
25	Федор	13	Высокий
26	Александр	13	Высокий

ПРИЛОЖЕНИЕ 3

Рабочая программа курса внеурочной деятельности по формированию основ кибербезопасности у младших школьников

Пояснительная записка

Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, что также означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В проекте Концепции стратегии кибербезопасности Российской Федерации киберпространство определяется как «сфера деятельности в информационном пространстве, образованная совокупностью Интернета и других телекоммуникационных сетей и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)», а кибербезопасность – как «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями». В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективудо2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются [28;29]:

– обеспечение различных сфер экономики качественными информационными технологиями;

– обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Компьютерные технологии применяются при изучении практически всех школьных дисциплин уже с младших классов, поэтому, как указано в «Стратегии развития отрасли информационных технологий в Российской Федерации»: «Необходимо совершенствовать современную профессиональную подготовку учителей и преподавателей дисциплин в сфере информационных технологий», а значит, и в сфере кибербезопасности. Киберугрозы существуют везде, где применяются информационные технологии, следовательно, учитель может в профессиональной деятельности столкнуться и со спамом, и с вирусами, и со взломом компьютера и с многими другими проблемами, на которые нужно не только оперативно реагировать, но и насколько возможно уметь предотвращать их появление, а значит, постоянно упоминать в контексте занятия различные аспекты организации информационной безопасности и кибербезопасности. Учитель должен иметь представление о современном уровне развития вычислительной техники, информационный сетей, технологий коммуникации и навигации.

Государство считает необходимым расширение объема преподавания информационных технологий в общеобразовательных организациях. В качестве одной из организационных мер в обеспечении кибербезопасности определена разработка и внедрение в учебный процесс образовательных организаций курса по кибербезопасности во внеурочной деятельности. Не все начальные школы включают в себя предмет «Информатика», поэтому представляется актуальным дополнить модулем по «Основам кибербезопасности» курс «Окружающий мир» и, возможно, других предметов.

С учетом роста числа угроз информационной деятельности и стремительного развития информационных технологий представляется

необходимым включить в ФГОСы соответствующие требования, что позволило бы органически дополнить образовательный процесс новыми модулями без рассогласования с имеющимися учебными планами. В число требований к результатам подготовки обучающихся необходимо включить не только «удовлетворение познавательных интересов, поиск дополнительной информации», знание«технических устройств (в том числе компьютеров)», умение «искать информацию с применением правил поиска (построения запросов) в базах данных, компьютерных сетях, пользоваться персональным компьютером и его оборудованием; следовать требованиям техники безопасности, гигиены, ресурсосбережения при работе со средствами информационных и коммуникационных технологий», но и знание основ кибербезопасности, умения соблюдать требования кибербезопасности в практической деятельности и организовывать безопасность личного информационного пространства.

В настоящее время требования ФГОС для уровней начального, общего и полного среднего образования не содержат предметной области «Кибербезопасность в сети», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» и курса внеурочной деятельности вопросы информационной безопасности обозначены:

– требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;

– умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

– понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.д.

Базой курса «Кибербезопасность в сети» является модель непрерывного информационного образования в школе, причем вопросы кибербезопасности изложены в Приказе Министерства образования Российской Федерации №1089 от 5 марта 2004 года (с изменениями на 23 июня 2015 года) «Об утверждении федерального компонента государственных образовательных стандартов начального общего, основного общего и среднего (полного) общего образования». Приказдолжны постоянно рассматривать как при изучении информатики, так и других предметов. Поэтому одна из целей курса – повышение квалификации в области кибербезопасности учителей всех дисциплин, в которых каким-либо образом используются компьютерные технологии. Наиболее очевидной является возможность дополнения вопросами кибербезопасности занятий во внеурочной деятельности.

Воспитательная цель курса – формирование на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам информационной безопасности и кибербезопасности.

Планируемые результаты освоения курса внеурочной деятельности «Кибербезопасность в сети»

Сформулированные цели реализуются через достижение образовательных результатов. Эти результаты структурированы по ключевым задачам общего образования, отражающим индивидуальные, общественные и государственные потребности, и включают в себя предметные, метапредметные и личностные результаты.

Личностные результаты:

– формирование ответственного отношения к учению, готовности и способности обучающихся к саморазвитию и самообразованию на основе мотивации к обучению и познанию;

– формирование целостного мировоззрения, соответствующего современному уровню развития науки и общественной практики;

– развитие осознанного и ответственного отношения к собственным поступкам;

– формирование коммуникативной компетентности в процессе образовательной, учебно-исследовательской, творческой и других видов деятельности [10].

В сфере развития познавательных универсальных учебных действий приоритетное внимание уделяется:

– практическому освоению обучающимися основ проектно-исследовательской деятельности;

– развитию стратегий смыслового чтения и работе с информацией;

– практическому освоению методов познания, используемых в различных областях знания и сферах культуры, соответствующего им инструментария и понятийного аппарата, регулярному обращению в учебном процессе к использованию общеучебных умений, знаково-символических средств, широкого спектра логических действий и операций.

При изучении внеурочного курса «Кибербезопасность в сети» обучающиеся усовершенствуют приобретенные на первой ступени навыки работы с информацией и пополнят их. Они смогут работать с текстами, графикой, преобразовывать и обрабатывать содержащуюся в них информацию, в том числе:

– систематизировать, сопоставлять, анализировать, обобщатьи интерпретировать информацию, содержащуюся в готовых информационных объектах;

– выделять главную и избыточную информацию, выполнять смысловое свертывание выделенных фактов, мыслей; представлять информацию в сжатой словесной форме и в наглядно-символической форме;

– заполнять и дополнять таблицы, схемы, тексты, изображения.

Обучающиеся усовершенствуют навык поиска информации в компьютерных источниках информации, приобретут навык формулирования запросов в сети Интернет. Они научатся осуществлять поиск информации в Интернете, школьном информационном пространстве, базах данных и на персональном компьютере с использованием поисковых сервисов, строить поисковые запросы в зависимости от цели запроса и анализировать результаты поиска.

Обучающиеся приобретут потребность поиска дополнительной информации для решения учебных задач и самостоятельной познавательной деятельности; освоят эффективные приемы поиска, организации и хранения информации на компьютере, в информационной среде школы и в Интернете; приобретут первичные навыки формирования и организации собственного информационного пространства.

Они усовершенствуют умение передавать информацию в устной форме, сопровождаемой аудиовизуальной поддержкой, и в письменной форме гипермедиа (т.е. сочетания текста, изображения, звука, ссылок между разными информационными компонентами).

Обучающиеся смогут использовать информацию для установления причинно-следственных связей и зависимостей, объяснений и доказательств фактов в различных учебных и практических ситуациях, ситуациях моделирования и проектирования.

Младшие школьники получат возможность научиться строить умозаключения и принимать решения на основе самостоятельно полученной информации, а также освоить опыт критического отношения к получаемой информации на основе еѐ сопоставления с информацией из других источников и с имеющимся опытом [11].

Обучающиеся научатся:

– основам реализации проектно-исследовательской деятельности;

– проводить наблюдение и эксперимент под руководством учителя;

– осуществлять расширенный поиск информации с использованием ресурсов глобальной сети Интернет;

– осуществлять выбор наиболее эффективных способов решения задач в зависимости от конкретных условий;

– давать определение понятиям;

– устанавливать причинно-следственные связи;

– обобщать понятия – осуществлять логическую операцию перехода от видовых признаков к родовому понятию, от понятия с меньшим объемом к понятию с большим объемом;

– осуществлять сравнение и классификацию, самостоятельно выбирая основания и критерии для указанных логических операций;

– строить логическое рассуждение, включающее установление причинно-следственных связей;

– объяснять явления, процессы, связи и отношения, выявляемые в ходе исследования;

– структурировать тексты, включая умение выделять главное и второстепенное, главную идею текста, выстраивать последовательность описываемых событий.

Обучающиеся получат возможность научиться:

– основам дизайна;

– ставить проблему, аргументировать еѐ актуальность;

– самостоятельно проводить исследование на основе применения методов наблюдения и эксперимента;

– выдвигать гипотезы о связях и закономерностях событий, процессов, объектов;

– организовывать исследование с целью проверки гипотез;

– делать умозаключения и выводы на основе аргументации.

Формирование ИКТ-компетентности обучающихся. Обучающиеся научатся:

– подключать устройства ИКТ к электрическим и информационным сетям;

– соединять устройства ИКТ (блоки компьютера, устройства сетей, принтер, проектор, сканер и т. д.) с использованием проводных и беспроводных технологий;

– правильно включать и выключать устройства ИКТ, входить в операционную систему и завершать работу с ней, выполнять базовые действия с экранными объектами (перемещение курсора, выделение, прямое перемещение, запоминание и вырезание);

– осуществлять информационное подключение к локальной сети и глобальной сети Интернет;

– входить в информационную среду школы, в том числе через Интернет, размещать в информационной среде различные информационные объекты;

– выводить информацию на бумагу, правильно обращаться с расходными материалами;

– соблюдать требования техники безопасности, гигиены, и ресурсосбережения при работе с устройствами ИКТ;

– осуществлять фиксацию изображений и звуков в ходе процесса обсуждения, проведения эксперимента, фиксацию хода и результатов проектной деятельности;

– учитывать смысл и содержание деятельности при организации фиксации, выделять для фиксации отдельные элементы объектов и процессов, обеспечивать качество фиксации существенных элементов;

– выбирать технические средства ИКТ для фиксации изображений и звуков в соответствии с поставленной целью;

– проводить обработку цифровыхфотографий с использованием возможностей специальных компьютерных инструментов, создавать презентации на основе цифровых фотографий;

– работать с особыми видами сообщений: диаграммами и картами;

– формулировать вопросы к сообщению, создавать краткое описание сообщения;

– избирательно относиться к информации в окружающем информационном пространстве, отказываться от потребления ненужной информации;

– создавать различные геометрические объекты сиспользованием возможностей специальных компьютерных инструментов.

Обучающиеся получат возможность научиться:

– осознавать и использовать в практической деятельности основные психологические особенности восприятия информации человеком;

– различать творческую и техническую фиксацию звуков и изображений;

– использовать возможности ИКТ в творческой деятельности, связанной с искусством.

Коммуникация и социальное взаимодействие. Обучающиеся научатся:

– осуществлять образовательное взаимодействие в информационном пространстве школы (получение и выполнение заданий, получение комментариев, совершенствование своей работы, формирование портфолио);

– соблюдать нормы информационной культуры, этики и права; с уважением относиться к частной информации и информационным правам других людей.

– формировать собственное информационное пространство;

– проектировать и организовывать свою индивидуальную и групповую деятельность, организовывать свое время с использованием ИКТ.

Обучающиеся получат возможность научиться:

– взаимодействовать с другими людьми с использованием возможностей Интернета (игровое и театральное взаимодействие).

Метапредметные результаты:

1. Умение самостоятельно определять цели своего обучения, ставить и формулировать для себя новые задачи в учебе и познавательной деятельности, развивать мотивы и интересы своей познавательной деятельности;

2. Владение основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности;

3. Умение определять понятия, создавать обобщения, устанавливать аналогии, классифицировать, самостоятельно выбирать основания и критерии для классификации, устанавливать причинно-следственные связи, строить логическое рассуждение, умозаключение (индуктивное, дедуктивное и по аналогии) и делать выводы;

4. Умение создавать, применять и преобразовывать знаки и символы, модели и схемы для решения учебных и познавательных задач;

5. Смысловое чтение;

6. Умение осознанно использовать речевые средства в соответствии с задачей коммуникации; владение устной и письменной речью;

7. Формирование и развитие компетентности в области использования информационно-коммуникационных технологий (далее ИКТ-компетенции).

Предметные результаты:

1. Умение использовать термины «информация», «сообщение», «данные», «алгоритм», «анимация», «программа», «дизайн»; понимание различий между употреблением этих терминов в обыденной речи и в информатике;

2. Умение создавать и редактировать изображения;

3. Умение создавать анимацию различными методами; умение создавать дизайн издания;

4. Умение использовать готовые прикладные компьютерные программы и работать с их описаниями;

5. Навыки выбора способа представления данных в зависимости от постановленной задачи.

Содержание курса «Кибербезопасность в сети» (36 часов,4 класс)

Техника безопасности и экология:

1. Правила поведения в компьютерном классе

2. Интернет в системе безопасности. Как защитить сам Интернет?

3. Техника безопасности при работе с компьютером. Источники питания компьютера

4. Что делать, если вода попала в компьютер или ноутбук?

5. Может ли загореться компьютер?

6. Может ли вирус сломать компьютер?

7. Первая помощь при проблемах в Интернете (службы помощи)

8. Компьютер и мобильные устройства в чрезвычайных ситуациях

9. Компьютер и зрение

10. Информационная перегрузка

11. Информация, вредная для здоровья

12. Медицинская информация в Интернете – всегда ли она полезна

Общие сведения о безопасности ПК и Интернета:

1. Как устроен компьютер и Интернет?

2. Какие программы должны быть установлены на компьютере?

3. Компьютер и системы безопасности

4. Сетевые игры как массовые развлечения. Бесплатные и платные игры

5. Кибербезопасность – что это?

Проблемы Интернет-зависимости:

1. ЗОЖ и компьютер. Виды зависимости. Как определить наличие зависимости

2. Деструктивная информация в Интернете – как ее избежать?

3. Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред?

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы:

1. Цели компьютерных вирусов

2. Способы распространения вирусов

3. Источники и причины заражения

Мошеннические действия в Интернете. Киберпреступления:

1. Киберпреступления – что это такое?

2. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.)

3. Виртуальные друзья – кто они?

Сетевой этикет. Психология и сеть:

1. «Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам?

2. Поиск информации в Интернете

3. Правила общения в Интернете. Основы сетевого этикета

4. Переписка в сети. Этикет при переписке. Что такое спам?

5. Безопасность в социальных сетях

6. Что такое форум?

7. Общение в сети и его последствия. Агрессия в сети

8. Психологическое влияние через Интернет

9. Реальная и виртуальная личность, реальные встречи с виртуальными знакомымииихопасность,угрозыиоскорбления– чемэтоможетзакончиться?

10. Как защитить себя в Интернете?

Таблица 3.1 –Календарно-тематическое планирование «Кибербезопасность в сети» (36 часов, 4 класс)

№ п/п	Тема занятия	Дата проведения
Техника безопасности и экология		
1	Правила поведения в компьютерном классе	
2	Интернет в системе безопасности. Как защитить сам Интернет?	
3	Техникабезопасностиприработескомпьютером.Источникипитания компьютера	
4	Что делать, если вода попала в компьютер или ноутбук?	
5	Может ли загореться компьютер?	
6	Может ли вирус сломать компьютер?	
7	Первая помощь при проблемах в интернете (службы помощи)	
8	Компьютер и мобильные устройства в чрезвычайных ситуациях	
9	Компьютер и зрение	
10	Информационная перегрузка	
11	Информация, вредная для здоровья	
12	Медицинская информация в Интернете – всегда ли она полезна	
Общие сведения о безопасности ПК и Интернета		
13	Как устроен компьютер и Интернет?	
14	Какие программы должны быть установлены на компьютере?	
15	Компьютер и системы безопасности	
16	Сетевые игры как массовые развлечения. Бесплатные и платные игры	
17	Кибербезопасность – что это?	
Проблемы Интернет-зависимости		
18	ЗОЖ и компьютер. Виды зависимости. Как определить наличие зависимости	
19	Деструктивная информация в Интернете – как ее избежать?	
20	Для чего может быть полезен ПК и Интернет (развивающие игры, обучение, общение и т.п.) и как польза превращается во вред?	

Продолжение таблицы 6

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы		
21	Цели компьютерных вирусов	
22	Способы распространения вирусов	
23	Источники и причины заражения	
Мошеннические действия в Интернете. Киберпреступления		
24	Киберпреступления – что это такое?	
25	Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.)	
26	Виртуальные друзья – кто они?	
Сетевой этикет. Психология и сеть		
27	«Лишняя информация» о себе и других в Интернете. Какая информация принадлежит вам?	
28	Поиск информации в Интернете	
29	Правила общения в Интернете. Основы сетевого этикета	
30	Переписка в сети. Этикет при переписке. Что такое спам?	
31	Безопасность в социальных сетях	
32	Что такое форум?	
33	Общение в сети и его последствия. Агрессия в сети	
34	Психологическое влияние через Интернет	
35	Реальная и виртуальная личность, реальные встречи с виртуальными знакомымииихопасность,угрозыиоскорбления–	
36	Как защитить себя в Интернете?	