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

ФАКУЛЬТЕТ ДОШКОЛЬНОГО, НАЧАЛЬНОГО И КОРРЕКЦИОННОГО ОБРАЗОВАНИЯ
КАФЕДРА ТЕОРИИ, МЕТОДИКИ И МЕНЕДЖМЕНТА НАЧАЛЬНОГО ОБРАЗОВАНИЯ

Работа педагога с семьей по формированию основ кибербезопасного поведения младших школьников

Выпускная квалификационная работа по направлению
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность программы бакалавриата

«Начальное образование. Английский язык»
Форма обучения очная

Проверка на объем заимствований:
82,93 % авторского текста
Работа рекомендована к защите
« 02 » июня 2025 г.
зав. кафедрой ТМиМНО
_____ Волчегорская Евгения Юрьевна

Выполнила:
Студентка группы ОФ-521-071-5-1
Амирова Анна Тимуровна

Научный руководитель:
канд. пед. наук, доцент
_____Жукова Марина Владимировна

Челябинск
2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Век информационных технологий сделал современного человека пользователем различных цифровых устройств и потребителем информационного контента. Данный век полностью изменил привычную жизнь людей, в том числе детей. В настоящее время у каждого человека, начиная с дошкольного возраста есть доступ к компьютеру, смартфону, планшету. Дети, полностью родившиеся в 21 веке, или поколение Альфа, не представляют свою жизнь без Интернета, социальных сетей и электронных устройств. Ведь найти нужную информацию или нового друга, для них, куда проще через смартфон. Именно электронные устройства и социальные сети заменяют личное общение с окружающими, физическое чтение книг и поиска информации. Смартфоны, компьютеры и планшеты привносят в жизнь младших школьников новые возможности для реализации социальных потребностей, важных для жизни любого человека. Электронные устройства, такие как: сотовые телефоны, компьютерная техника, планшеты помогают младшим школьникам почувствовать свою необходимость и важность в обществе, показать, принадлежность к определенной социальной группе, найти контакт со сверстниками, поддержать общение, находясь в любой точке мира, самовыражаться и саморазвиваться. Таким образом, 21 век ознаменовал цифровизацию всех сфер жизни человека, в том числе и сферу образования.

Уже с 1 класса обучающиеся используют различные интернет-ресурсы, а значит и электронные устройства, которые способствуют ускорению процесса выполнения домашнего задания, повторения темы, поиска необходимой информации.

Несмотря на то, что устройства, которые являются элементами информатизации и цифровизации, прочно вошли в жизнь людей, как средства реализации важных социальных потребностей, все чаще ведут к появлению множества негативных последствий: снижение внимания и

концентрации, формирование зависимости, вред здоровью, физическому и психическому благополучию.

И именно младшие школьники, ввиду своих возрастных особенностей и недостатка жизненного опыта, больше всего подвержены формированию и развитию зависимого поведения по отношению к электронным устройствам, и, как следствие, возникновению большого количества проблем и угроз, связанных с кибербезопасностью. Как следует из аналитической справки пресс-релиза, от 17 марта 2025 года, компании АО «Лаборатория Касперского», специализирующейся на разработке систем защиты от различных киберугроз, 76 % детей указывают свой настоящий возраст в информации о пользователе в социальных сетях, что является ключевой информацией для злоумышленников, в ходе их мошеннических действий с применением социальной инженерии. Также важно отметить, что каждый пятый российский ребенок, не закрывает свою страницу от посторонних пользователей в социальной сети, что увеличивает уровень уязвимости детей в киберпространстве [28].

Огромную роль в знакомстве детей с миром информационных технологий играют взрослые: прародители, родители, дядя и тети, старшие братья и сестры, учитель. Роль родителей зачастую недооценена, ведь из-за занятости на работе, незнания возрастных особенностей детей, отсутствия необходимой информации и не умения правильно ее донести, взрослые отпускают детей в «свободное плавание», перестают контролировать их экранное время и потребляемый контент, не помогают детям адаптироваться в быстро меняющемся мире информационных технологий и неосознанно подвергают их опасным последствиям чрезмерного использования электронных устройств, Интернет игр и социальных сетей, одними из которых являются проблемы кибербезопасности. Так, только 10 % родителей знают о случаях, когда незнакомый человек пытался установить контакт с ребенком, хотя по словам детей, с такой ситуацией сталкивались 17 % опрашиваемых. Чаще всего попытка незнакомца

установить контакт с ребенком происходит через социальные сети, онлайн игры и мессенджеры [28].

Следовательно, семье нужна помощь, не меньше, чем она нужна детям. И главенствующую роль в такой ситуации должен брать на себя учитель. Это именно тот человек, который знает все о жизни детей, о существующих современных угрозах в сети Интернет, о том, как предупредить влияние этих проблем на школьников, о том, кукую информацию нужно донести до родителя, в какой форме родителю вести общение с ребенком. В решение проблем кибербезопасности и ее последствий важна совместная работа школы и семьи.

Учитель начальных классов – это посредник между миром детей и миром взрослых. Именно благодаря учителю можно решить большинство проблем младших школьников и детско-родительских отношений, передать родителям важную информацию, которая поможет в воспитании и формировании опыта у детей, в том числе опыта, связанного с кибербезопасным поведением младших школьников.

Таким образом актуальным становится работа педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Теоретические основы формирования кибербезопасного поведения младших школьников рассматриваются в трудах следующих авторов: А. Ю. Акопов, Я. И. Гилинский, Е. В. Змановская, И. С. Кон, Ц. П. Короленко, А. Е. Личко, Д. И. Фельдштейн.

Направления деятельности педагога по формированию кибербезопасного поведения младшего школьника изучали в своих работа О. Н. Арестова, Л. Н. Бабанин, М. С. Киселева, М. Коул, А. В. Худяков, К. С. Янг.

Проблемой Интернет-зависимости занимались: А. В. Ваганов, А. Е. Войскунский, А. Е. Жичкина, М. В. Жукова, В. А. Лоскутова, А. В. Минаков, А. И. Ракитов, А. С. Холл, М. А. Шоттон.

Психологические аспекты коммуникативных процессов в сети изучали:

О. М. Арестова, Ю. Д. Бабаева, А. Е. Войскунский, А. Голдберг, Д. В. Иванов, Т. В. Карабин, А. В. Смысловая, А. Н. Черемисина, Л. М. Юрьева.

Проблема исследования: каково содержание программы взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников?

Актуальность проблемы обусловила выбор *темы исследования*: «Работа педагога с семьей по формированию основ кибербезопасного поведения младших школьников».

Цель исследования: изучить теоретические аспекты проблемы работы педагога с семьей по формированию основ кибербезопасного поведения детей младшего школьного возраста для разработки программы взаимодействия педагога с семьей.

Объект исследования: формирование основ кибербезопасного поведения младших школьников.

Предмет исследования: работа педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Задачи исследования:

1. Рассмотреть сущность понятия кибербезопасность, угрозы и их последствия.
2. Выявить особенности восприятия информации и поведения младших школьников в цифровой среде.
3. Определить направления работы педагога с семьей по формированию кибербезопасного поведения младших школьников.
4. Проанализировать результаты исследовательской работы.
5. Разработать программу взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Методы исследования:

– теоретические методы: анализ психолого-педагогической, социологической, методической литературы, обобщение, систематизация, сравнение;

– эмпирические методы: тестирование, эксперимент;

– методы обработки и интерпретации результатов.

База исследования: МАОУ г. Челябинска. В исследовании приняли участие 15 обучающихся 4 класса и 15 родителей.

Этапы исследования:

1. Поисково-подготовительный этап. На данном этапе проводился теоретический анализ психолого-педагогический, методической и специальной литературы по проблеме; формулировались методологические положения исследования, подбирались методики диагностики;

2. Экспериментальный этап. Проводилось тестирование детей младшего школьного возраста и родителей на выявление проблем, связанных с отсутствием знаний об основах формирования кибербезопасного поведения младших школьников и их склонностью к интернет-зависимости. Подбирались методические материалы для создания программы взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

3. Обобщающий этап. Формулировались окончательные выводы, оформлялась выпускная квалификационная работа.

Практическая значимость работы: разработанная нами программа взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников может быть использована в работе учителей начальных классов, психологов.

Структура работы: работа состоит из введения, двух глав, выводов по главам, заключения, списка литературы. В тексте работы 8 таблиц, 1 рисунок. Список литературы представлен 32 источниками.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ РАБОТЫ ПЕДАГОГА С СЕМЬЕЙ ПО ФОРМИРОВАНИЮ ОСНОВ КИБЕРБЕЗОПАСНОГО ПОВЕДЕНИЯ МЛАДШИХ ШКОЛЬНИКОВ

1.1 Сущность понятия кибербезопасность, угрозы и их последствия

Человек никогда не стоит на месте, постоянное развитие – это необходимость, связанная с быстро меняющимся миром. С появлением Интернета, первых компьютеров и смартфонов привычная жизнь людей кардинально изменилась. Сегодня невозможно представить свою жизнь без смартфона, Интернета, компьютера, планшета, умной колонки или умного дома. Цифровизация всех сфер жизнедеятельности человека сделала нормой то, что 2 века назад еще было немыслимым.

Жизнь человека стала простой, быстрой, удобной. Хочешь поговорить с другом – позвони ему по телефону, напиши сообщение через почту или мессенджер, хочешь учиться, узнавать новое – онлайн курсы и дистанционное обучение помогут в этом, срочно нужно найти рецепт блюда – просто найди его в Интернете, решил прочитывать книгу – скачай ее онлайн. Тенденция использования простых и быстрых действий растет каждый день, появляются большое количество онлайн сервисов, работающих на базе искусственного интеллекта, совершенствуется работа компьютеров, смартфонов и планшетов, появляются новые электронные устройства: очки дополненной реальности, весы, вычисляющие важные показатели тела, специальное умное кольцо, которое может отслеживать мерцающую аритмию. Такие устройства дают надежду на то, что жизнь человека, будет становится только лучше, интереснее, практичнее. Современный человек, привык ежедневно взаимодействовать с большим количеством различных цифровых устройств. В том числе и дети, которые взаимодействуют с электронными устройствами не только дома, но и в школе.

В сфере образования роль цифровизации и информатизации огромна. Система образования в современном мире тесно связана с цифровым влиянием электронных устройств. Благодаря им, обучение в школах становится мобильным, интерактивным, увлекательным, таким образом формируя у обучающихся интерес к обучению [10]. Если еще 50 лет назад в школах не было ничего, что связано с информатизацией и цифровизацией образования, то сейчас, в большинстве школ есть все новшества современного мира: Интернет, компьютеры, интерактивные доски и проекторы, документ-камера, различные образовательные сайты и ресурсы. Школы готовы обучать в электронном и дистанционном форматах. Под электронным обучением подразумевается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников [17]. Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников [17]. Все это показывает готовность школ, педагогических работников и всей сферы образования обучать современных детей или поколение digital natives – детей, которые с самого рождения знают, что такое электронные устройства, как ими пользоваться, и для чего они нужны. Термин «digital natives» был придуман в 2001 году Марком Пренски – американским писателем и консультантом в области образования, для описания «цифрового поколения» нашего общества, которое является носителями языка: цифрового, языка компьютеров, видеоигр и Интернета [32].

Но помимо большого количества плюсов связанных, с цифровизацией жизни школьников, присутствует и пропорциональное этому количество минусов.

В эпоху современных технологий и развития цифровой среды в жизни людей и в образование, большое внимание следует уделять интернет аддикции или зависимости от электронные устройств, такие как: смартфон, планшет, компьютер или ноутбук. Данный вид зависимого поведения затрагивает жизнь общества, начиная с младшего школьного возраста и характеризуется навязчивым желанием пользоваться всемирной паутиной и болезненную неспособность от нее отключиться. Понятие «интернет зависимость», или «Internet addiction disorder» было предложено в 1995 году Айвеном Кеннетом Голдбергом – американским психиатром и психоформакологом [31].

Аддиктивное поведение рассматривают как одну из форм отклоняющегося, девиантного, поведения с формированием стремления к уходу от реальности. Такой уход осуществляется путем искусственного изменения своего психического состояния посредством приема психоактивных веществ или специфической активности, которое приводит к фиксации внимания на определенных видах деятельности [9]. Термин аддиктивное поведение изменяется на протяжение всей истории своего существования, он дополняется и корректируется. Изначально данный термин был сформулирован М. Ландри и В. Миллером, которые раскрывали данное понятие через злоупотребление химическими веществами, ведущими к изменению психического состояния, не имея выработанной зависимости от этих веществ.

А. Е. Личко и В. С. Битенский раскрывали данный термин через ухудшение поведения, которое вызвано злоупотреблением химических веществ, в основном данная трактовка используется в отношение несовершеннолетних детей.

С. Б. Вайсов и С. А. Кулаков говорят об аддиктивном поведение, как о нарушение адаптации ребенка, из-за злоупотребления химических веществ, которые влияют на психику ребенка при этом не имея зависимости от этих веществ, но данный вид нарушения адаптации является сопутствующим с другими нарушениями поведения.

Самая распространенная трактовка определения была дана Ц. П. Короленко и Н. В. Дмитриевой. Они говорят о том, что аддиктивное поведение – это один из типов девиантного (отклоняющегося) поведения с формированием стремления к уходу от реальности путем искусственного изменения своего психического состояния посредством приема некоторых веществ или постоянной фиксации внимания на определенных видах деятельности с целью развития и поддержания интенсивных эмоций [9]. Как понятно из определений, аддиктивное поведение можно разделить на два вида: химическая аддикция и фиксация внимания на определенной деятельности. И каждый из видов делится на формы, которые и формируют аддитивное поведение.

Дети «поколения Альфа» в большей степени подвержены игровым и информационным аддикциям, то есть тем зависимостям, которые формируются при постоянном взаимодействие младшего школьника с электронными информационными устройствами.

1. Игровая зависимость.

1.1 Гэмблинг – зависимое поведение, которое возникает при частом погружении в мир азартных игр, для игроков нет ничего, кроме игры, они не чувствуют ход времени, у них отсутствуют рамки потраченных денег, но самое главное что уход от данной зависимости происходит болезненно, отказ от частой игровой деятельности проходит человеком в несколько студий: гнев, стресс, агрессия, раздражительность.

1.2 Компьютерная зависимость – данный вид зависимости возникает из-за постоянного использования сети интернет и сетевых игр с

помощью компьютера, такой вид зависимости заменяет человеку реальную жизнь и наносит вред психическому и физическому здоровью.

2. Информационные аддикции

2.1 Интернет аддикция, зависимость от социальных сетей – интернет в современном мире – это источник, который помогает узнавать новое, находить интересующее и главное общаться в социальных сетях с людьми по всему миру, но данная зависимость приводит к плачевным результатам, которые сказываются на жизни субъекта [5].

Менее распространенными, но не менее опасными, для младших школьников считаются химические аддикции, такие как: курение, зависимость от алкоголя и наркотиков, токсикомания. И нарушение пищевого поведения: переедание, голодание, отказ от еды. Ведь именно эти аддикции могут возникнуть как следствие ухода ребенка от реальности, будь то проблемы в общение, получение плохих отметок, отсутствие досуга или как следствие уже имеющихся других зависимостей, например компьютерной или зависимости от социальных сетей.

Большинство детей, в частности обучающихся начальной школы проводят все свое свободное от учебы время в социальных сетях и электронных устройствах. Дети имеют свои страницы, где выкладывают посты, информацию о своих интересах, слушают музыку, играют в игры и общаются. Это помогает им отвлечься от насущных проблем, пообщаться и просто провести время в интересной для них среде.

Виртуальный мир затягивает ребенка, он становится зависимым от электронных устройств, игр и социальных сетей, из-за чего возникает множество негативных последствий: снижение уровня самооценки, агрессия к окружающим, пассивность и одиночество, возникновение угроз кибербезопасности.

Причин возникновения такой проблемы как интернет-зависимость очень много: отсутствие внимания к школьнику со стороны взрослого, демонстрация зависимого поведения взрослого на собственном примере,

отсутствие альтернативной деятельности в жизни школьника, неблагоприятная действительность.

Ребенок будет с головой уходить в новый мир, ведь там интересно, необычно. Грань реального и онлайн с каждым днем будет стираться. Любая свободная минута и уже в руках планшет или компьютер. Как бы много плюсов не находилось, явные минусы их перечёркивают. Именно на минусы необходимо направить энергию и понять, что негативное влияние электронных устройств на младших школьников велико, а одними из самых опасных проблем являются угрозы кибербезопасности. Ведь такие угрозы влекут за собой психические, физические, эмоциональные неблагоприятные последствия. Кибербезопасность и младший школьник, два этих термина, которые явно не могут стоять рядом, но реальный мир таков, что от незнания основ кибербезопасного поведения страдают все люди, в том числе и дети. Поэтому очень важно предупреждать возникновение любых проблем и угроз связанных с кибербезопасностью и проводить просветительскую работу с обучающимися и их родителями, для формирования знаний о кибербезопасном поведение в информационном пространстве.

Кибербезопасность или компьютерная безопасность – это термин, состоящий из двух слов «кибер» и «безопасность».

Кибер – это префикс, обозначающий все, что связано с информационной и цифровой средой: Интернет, компьютер, смартфон, информационные технологии.

Безопасность – это состояние, при котором человек чувствует себя защищенным от проблем, опасностей и угроз.

Сочетание этих слов показывает, что человеку важна и нужна защита от вредоносного влияния киберпространства.

Кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, сервером, мобильных устройств, электронных систем, сетей и данных [1]. Иными словами, это совокупность

мер, которые способствуют безопасному нахождению в цифровом пространстве, при этом защищая информацию, которая хранится в компьютерных системах.

Важность понимания того, что в настоящее время Интернет и электронные устройства используются повсеместно показывает необходимость развития культуры осведомленности о кибербезопасном поведении в сети и обучения в области кибербезопасности [4]. Такое обучение необходимо начинать уже с детства, ведь именно с младшего школьного возраста начинается полноценное погружение детей в мир информации и цифровизации, и, как следствие появление проблем безграмотного использования медиа и киберпространства.

Киберобразование – это важная и неотъемлемая часть жизни каждого человека. Получать знания о киберпространстве, применять их на практике, знать об угрозах кибепространства – это надежные шаги, способствующие безопасному нахождению в мире Интернета.

Изучением понятий «кибербезопасность», «информационная грамотность» и «информационная культура» занимались такие ученые как К. Янг, А. Е. Войскунский, М. Гриффитс, А. Ю. Егорова, А. Голдберг, Ц. П. Короленко, Дж. Грохол, А. Е. Жичкина, М. Фенишел и др.

Развитие и становление направления «информационная безопасность и защита информации» в РФ связано с именами следующих отечественных ученых: В. А. Герасименко, А. А. Малюк, М. Б. Игнатьев, П. Д. Зегжда и др.

Для того, чтобы полноценно и всесторонне изучить сущность понятия кибербезопасность, нужно начать с основных понятий и определений, которые являются фундаментом для строительства кибербезопасного пространства сети Интернет.

1. Идентификация – процесс установления уникальной личности пользователя, системы или устройства в компьютерной среде. С помощью идентификации в Интернете и на разных ресурсах создается персональный доступ к данным. Это своего рода паспорт, индивидуальная и единственная

в своем роде информация о пользователе или устройстве, которая подтверждает его личность.

2. Аутентификация – процесс подтверждения подлинности идентифицированной стороны. Процесс аутентификации неразделим с процессом идентификации, потому что именно благодаря аутентификации подтверждается пользователь, его индивидуальность или наоборот отклоняется субъект, который не соответствует идентификационным данным в системе. Чаще всего, для того чтобы открыть доступ к персональным данным или другим личным ресурсам субъект использует пароль, PIN-код, различные одноразовые коды и биометрические данные. Сейчас наибольшую популярность набирает двухфакторная аутентификация – использование двух факторов, подтверждающих личность, что приводит к повышению уровня безопасности в киберпространстве.

3. Авторизация – предоставление прав и разрешений аутентифицированным пользователям, определяя какие ресурсы и действия доступны конкретному субъекту. Авторизация тоже взаимосвязана с аутентификацией. Без подтверждённой информации о субъекте, невозможно использовать ресурсы и данные системы. Авторизация помогает защитить конфиденциальную информацию от кражи и несанкционированного использования.

4. Шифрование – метод обеспечения конфиденциальности данных путем их преобразования в зашифрованный формат, может быть понятен только тем, кто обладает ключом расшифровки. Любые данные и важная информация скрыты от посторонних глаз математическим алгоритмом, который создает шифрование сети и препятствует «утечке» данных третьим лицам, являющимися злоумышленниками. Шифрование обеспечивает безопасное нахождение субъекта в сети Интернет и использование всех информационно-коммуникационными технологий без вреда для личности [2].

Таким образом, представленные выше фундаментальные термины, связанные между собой, создают безопасную атмосферу пребывания в киберпространстве. Эти шаги способствуют защите данных, и персональной уверенности субъекта в безопасном нахождение в Интернете.

Когда субъект подключается к сети Интернет, для злоумышленников появляется возможность взломать идентификационный доступ и нанести ущерб данным. Для защиты данных от внутренних и внешних угроз разработаны принципы кибербезопасности. Или другими словами «триада CIA»

1. Конфиденциальность (Confidentiality) – это принцип, гарантирующий, что личные данные будут храниться в тайне от посторонних лиц и устройств. Это значит, что данные защищены от вредоносного использования, изменения, уничтожения.

2. Целостность (Integrity) – гарантирует, что информация, отправленная от одного субъекта к другому, не будет изменена или удалена до момента получения. Для это используют хэширование, которое помогает отслеживать любые изменения в данных.

3. Доступность (Availability) – гарантирует, что информация и ресурсы доступны законным авторизованным пользователям. Это также значит, что воспользоваться данными пользователь может в любое время [14].

Все эти принципы взаимосвязаны между собой и играют важную роль в обеспечение безопасности всех объектов и пользователей в киберпространстве.

Объектов кибербезопасности огромное количество.

1. Информация – ценный объект, который может быть представлен в разных формах: текстовые сообщения, изображения, аудио и видео записи. Утечка информации влечет за собой проблемы финансовой безопасности и репутационные угрозы.

2. Данные – это информация, представленная в виде чисел и фактов. Данные являются основой для формирования информации. Искажение и удаление данных приводит к потере части важной информации.

3. Системы – это комплексы взаимосвязанных элементов. Такие системы как операционная, приложения, база данных – обрабатывают, хранят и передают всю информацию. А хакерское воздействие может привести к нарушению работы этих систем, искажению данных и потери доступа к информации.

4. Сети – это вид систем, которые соединяют несколько устройств и способствуют быстрому и безопасному обмену данными. Атаки на сеть негативно влияют на данные и информацию.

5. Устройства – это физическое оборудование, благодаря которому возможен доступ к информации и данным. Такие устройства как компьютеры, смартфоны, планшеты, серверы при воздействии кибератак являются дверью в мир персональной информации и данных [30].

Все эти объекты нуждаются в защите, которая будет способствовать сохранению информации и ее дальнейшему безопасному использованию.

Необходимо разбираться в том, как злоумышленники проникают в устройства и крадут ценную информацию в личных целях.

Для это важно знать классификацию существующих угроз кибербезопасности и их последствия.

Классификация угроз кибербезопасности:

1. Вредоносное программное обеспечение или Malware: вирусы, троянские кони, черви, вымогательское ПО, шпионское ПО. Такие виды угроз заражают файлы, маскируются под полезные программы и крадут информацию.

2. Фишинг – это атаки, которые хакеры скрывают под привычными и надежными источниками. Чаще всего информацию ворует

через электронные письма и сайты. Злоумышленники получают информацию о паролях и номерах банковских карт.

3. DDoS-атаки или Distributed Denial of Service: такой вид угрозы кибербезопасности скрывается за мнимым спросом, обманчивой перегрузкой серверов огромным количеством запросов, приводящих к отказу системы в обслуживании пользователей.

4. Социальная инженерия – это вид манипуляции людьми, который приводит недоброжелателей к получению конфиденциальной информации. Данный вид угрозы подразумевает воздействие мошенников на эмоциональное и психическое состояние человека.

5. Уязвимости ПО подразумевают изначальное наличие в программном обеспечение дыр, ошибок, через которые злоумышленники могут проникнуть в сеть и украсть данные. Поэтому своевременное обновление ПО играет огромную роль в сохранение безопасного киберпространства.

6. Взлом паролей: целенаправленная работа хакеров для получения конфиденциальной информации учетной записи пользователя. Злоумышленники используют подбор паролей, специальное вредоносное ПО и брутфорс, то есть перебор всех возможных вариантов [8].

Понимание различных типов угроз кибербезопасности способствует предупреждению вредоносного воздействия на сети, устройства и конфиденциальную информацию. Именно поэтому очень важно изучать проблемы, связанные с воздействием угроз кибербезопасности и их последствиями для субъекта сети Интернет, будь то взрослый или ребенок.

Для современных детей электронные устройства – это обыденность. Привычка жить в цифровом и информационном окружение сделала детей еще более доверчивыми ко всему, что связано с киберпространством. Ведь «жизнь» в сети играет для них важную роль.

К сожалению, дети, как и взрослые подвержены угрозам кибербезопасности, которые помимо вредоносного воздействия на

информацию, сеть и устройства влекут за собой негативные последствия для эмоционального, психического и физического состояния детей.

Угрозы безопасности для детей младшего школьного возраста и их последствия можно разделить на три категории: незнакомцы, сверстники, самостоятельно. Эти категории можно разделить на следующие виды:

1. Фишинг: вид обмана, при котором дети передают личные данные (логины, пароли, данные банковских карт) мошенникам под видом доверенных сайтов или приложений. Очень часто недоброжелатели выдают себя за реально существующих людей, используют их фотографии, личную информацию для того, чтобы общение выглядело правдиво, таких мошенников называют кэтфишерами.

Последствия: финансовые потери для родителей и семьи в целом, использование существующего аккаунта ребенка и его личной информации в других мошеннических схемах [3].

2. Контакт с незнакомцами: общение младших школьников и подростков с людьми, которые скрывают свои истинные намерения, чаще всего негативного подтекста. Наибольшую угрозу представляют: шантажисты, вербовщики, манипуляторы и мошенники.

Последствия: кража личных данных, шантаж, вымогательство, похищения. Дети могут раскрыть информацию, которая будет использована против них или их семьи, а также пойти на личный контакт с мошенником [11].

3. Кибербуллинг: нападки, травля, оскорбления, унижения, распространение слухов в интернете. Это многократно повторяющееся поведение лица или группы лиц, другими словами, буллеров, направленное на то, чтобы специально доставить чувство тревоги и дискомфорта жертве буллинга в сети. Очень часто буллинг и кибербуллинг могут происходить одновременно. Формы кибербуллинга различны: флейминг, троллинг, киберсталкинг, аутинг и др.

Последствия: пониженная самооценка, депрессия, тревожность, социальная изоляция, проблемы с учебой, психосоматические заболевания [27].

4. Контент не по возрасту: случайное или намеренное столкновение с информацией, содержащий треш-контент, насилие, сцены жестокости, пропаганду наркотиков и другие материалы, не предназначенные для их возраста.

Последствия: страхи, ночные кошмары, эмоциональные расстройства, искаженное восприятие мира, агрессивное поведение.

5. Нежелательный контент: всплывающая реклама, спам, вирусы, которые могут повредить устройство или украсть данные.

Последствия: потеря данных, заражение устройств вредоносным ПО, финансовые потери, нарушение работы устройств [22].

6. Распространение личной информации: Дети могут не понимать важности конфиденциальности и распространять личную информацию (адрес, номер телефона, фотографии, реальный возраст, социальные связи, геопозиция, события) в интернете.

Последствия: риск стать жертвой преследования, доксинга (публикация личной информации с целью травли) [24].

Все вышеперечисленные угрозы кибербезопасности и их последствия являются актуальными и показывают проблему плохой осведомленности детей начальной школы, о возможных проблемах, которые могут возникнуть из-за отсутствия знаний о кибербезопасном поведение в сети Интернет. Как было сказано выше большую роль в этом играет жизненный опыт и знания младших школьников. Но, помимо этого, немаловажными являются возрастные особенности детей младшего школьного возраста и их особенности восприятия информации и поведения в цифровой среде, которые способствуют возникновению зависимого поведения от электронных устройств, и как следствие повелению угроз в киберсреде.

1.2 Особенности восприятия информации и поведения младших школьников в цифровой среде

Младший школьный возраст – это период в жизни ребенка, в котором происходит развитие психики на основе ведущего вида деятельности – учения. При этом происходит изменение в психике ребенка и развитие психических процессов, подготавливающие ребенка к новому этапу его развития [7]. Младшие школьник, ввиду своих возрастных особенностей имеют отличающиеся от других возрастов особенности восприятия информации и особенности поведения в информационной и цифровой среде.

Возрастные особенности младших школьников можно разделить на физиологические особенности, то есть те, которые связаны с внешними факторами развития: рост, увеличение размеров сердца, окостеневание позвоночника, приспособление нервной системы к новой окружающей среде. Психологические особенности: непроизвольное внимание, наглядно-образное мышление, эмоциональность, развитие речи и памяти, развитие самооценки. Социальные особенности: адаптация к школе, новому коллективу, развитие навыков коммуникации, освоение социальных норм и правил [29].

Наибольшую роль в восприятии информации и особенностях поведения младших школьников в сети Интернет играют психологические и социальные возрастные особенности младших школьников.

Для того, чтобы собрать полную картину изменений, способствующих определенному восприятию информации и поведению младших школьников в киберсреде, нужно подробнее изучить психологические и социальные особенности этого возраста. Как известно, возрастные особенности младших школьников таковы, что несут в себе множество возможностей для формирования привычек и зависимого

поведения к Интернету, социальным сетям и онлайн играм, что в свою очередь влияет на появление проблем кибербезопасности.

Психологические и социальные особенности:

– эмоциональность младшего школьного возраста: ребенок проявляет сильную реакцию ко всему новому и интересному или же наоборот, отсутствие реакции, сдерживание эмоций, присутствие внутренних переживаний [23]. Данная психологическая особенность участвует в формирование зависимого поведения, потому что ребенка интересует все новое, то есть социальные сети, а взаимодействие со сверстниками влечет за собой эмоциональную ответную реакцию на новшества среды и участие в жизни класс для его эмоционально стабильного фона – необходимо;

– проявления устойчивости поведения под действием среды: происходит быстрое формирование привычек, которые в последствие очень стойко входят в жизнь ребенка. Таким образом зависимость от социальных сетей появляется из-за привычки находится в смартфоне и сети при любой возможности;

– способность к саморегуляции личности: школьник учится следить за собой, за своими эмоциями, за своим поведением. Но социальные сети и зависимое поведение, которое они вызывают влекут за собой нарушение саморегуляции, эмоциональный фон становится негативным: агрессия, стресс, зависть, депрессия. Появляется заниженная самооценка, которую вызывает низкая ответная реакции в сети, не соответствующая ожиданиям. В виртуальном мире нет необходимости выражать свои эмоции, именно это делает ребенка замкнутым и влечет за собой дискоммуникацию личности в жизни;

– реализация коммуникативных способностей: человек, особенно ребенок, не может существовать без общества. Поэтому общение со взрослыми и сверстниками очень важны. Но нехватка общения в семье и в классе, отстраненность от сверстников и непринятие ребенка в малой

группе, влечет за собой уход от реальности в социальные сети, и как следствие вырабатывается зависимость от них. Ведь социальные сети способны дать ребенку то, чего в реальной жизни у него нет;

– особенности взаимодействия в первичном коллективе: школьный класс – это коллектив, в котором выработаны свои нормы, ценности и находясь в нем, ребенок должен быть его частью. Здесь следует говорить об эффекте подражания, когда все делают, значит и я должен делать. Таким образом сам коллектив прививает школьнику необходимость нахождения в социальных сетях;

– произвольность внимания: внимание – это сосредоточенность сознания на конкретном объекте. Объектом может быть как другой человек, предмет, чувства или внутренний мир субъекта. Ребенок может концертировать внимание на чем-то одном определённое количество времени, чаще всего внимание задерживается на том, что интересно и актуально для младшего школьника [25]. Взрослея, время концентрации внимания увеличивается, этот процесс распространяется как на учебную деятельность, так и на досуговую, в которой и проявляется концентрация внимания на определенный вид деятельности – нахождение в социальных сетях. Данный тип внимания помогает в развитии зависимости от социальных сетей;

– особенности строения мозга: разработчики социальных сетей давно шагнули вперед, и используют особенности мозга для привлечения внимания и управлением поведения людей и детей. Красный цвет уведомления подает в мозг сигнал, побуждающий к действие, то есть моментальной ответной реакции на увиденное. Данный цвет активизирует часть мозга, которая не воспринимает другие цвета. Бесконечная прокрутка ленты, данная функции развивает зависимое поведение, ведь в мозг не подаются сигналы, которые свидетельствуют об остановке, и так можно часами прокручивать ленту новостей. Так же дизайнерский подход,

красочность и удобность сетей заманивает пользователей, развивает зависимость.

Вышеперечисленные психологические и социальные возрастные особенности напрямую связаны с восприятием информации и поведением в цифровой среде младших школьников.

Восприятие информации в младшем школьном возрасте играет важную роль, ведь почти через все, что окружает младшего школьника он получает новые знания, умения и навыки.

Существует несколько видов восприятия информации младшими школьниками:

1. Наглядно-образное мышление: мир младшего школьника – это мир конкретных образов. Абстрактные понятия им даются с трудом. Визуальная информация (картинки, анимация, видео) воспринимается ими легче и быстрее, чем текст. Именно поэтому игры и интерактивные приложения так привлекательны – они предлагают яркий, динамичный, визуально насыщенный контент.

Злоумышленники могут использовать эту особенность, создавая красочные сайты или приложения с вредоносным содержанием. Ребенок, привлеченный визуальной составляющей, может не заметить признаков опасности (например, подозрительных ссылок, неадекватных предложений) и стать жертвой мошенничества, фишинга или скачать вирус.

2. Клиповое мышление: младшим школьникам сложно воспринимать большие объемы информации, особенно текстовой. Их внимание быстро рассеивается, они предпочитают короткие, динамичные фрагменты информации, «клипы» [21]. Это связано с особенностями развития их нервной системы и недостатком опыта аналитической обработки информации.

Клиповое мышление делает детей уязвимыми к манипуляциям, основанным на коротких, броских, но ложных сообщениях. Они могут не

критически проанализировать информацию и поверить фейковым новостям, провокационным лозунгам, рекламным трюкам.

3. Доверчивость: младшие школьники более доверчивы, чем подростки или взрослые. Доверие и доверчивое отношение к людям – это важный аспект межличностного взаимодействия ребенка с окружающим его миром. Дети, склонны верить информации, полученной из интернета, не всегда понимая, что не все источники достоверны. Они могут поверить обещаниям выигрыша в онлайн-играх, советам незнакомых людей в чатах, фейковым историям. Мошенники, зная эту особенность будут стараться подружиться с ребенком, втереться в доверие, развить чувство симпатии к себе со стороны ребенка [6].

Доверчивость делает детей легкой мишенью для мошенников, которые могут выманить у них личную информацию, деньги или втянуть их в опасные ситуации.

4. Недостаточная критичность мышления: у младших школьников еще не сформированы навыки критического мышления. Им сложно анализировать информацию, выделять главное, сравнивать разные точки зрения, отличать факты от мнений [12].

Недостаток критического мышления делает детей уязвимыми к манипуляциям, пропаганде, дезинформации. Они могут принимать на веру ложную информацию, не умея ее проверить и оценить.

5. Быстрая утомляемость: нервная система младших школьников еще незрелая, поэтому они быстро утомляются от длительного пребывания за экраном. Это приводит к снижению концентрации внимания, ухудшению усвоения информации, повышенной раздражительности.

В состоянии утомления дети становятся более внушаемыми и менее бдительными, что повышает риск стать жертвой онлайн-угроз.

Помимо особенностей восприятия информации, важно знать особенности поведения младших школьников в цифровой среде:

1. Игровая мотивация: для младших школьников цифровой мир – это прежде всего игровая площадка. Они используют гаджеты преимущественно для игр и развлечений. Даже обучающие программы и приложения должны содержать игровые элементы, чтобы привлечь и удержать их внимание.

Игровая мотивация может быть использована злоумышленниками. Вредоносные программы или фишинговые ссылки могут маскироваться под игры или игровые предметы. Дети, увлеченные игровым процессом, могут не заметить подвоха и подвергнуть себя опасности. Также существует риск развития игровой зависимости.

2. Подражательность: младшие школьники склонны подражать поведению взрослых, особенно родителей, а также популярных персонажей из мультфильмов, фильмов и игр. Они могут копировать манеру общения, стиль одежды, действия, увиденные в интернете. Подражание доставляет ребенку удовольствие, является целью для ребенка [13].

Если ребенок видит в интернете агрессивное поведение, ненормативную лексику или опасные действия (например, в играх или видеороликах), он может начать воспроизводить это в реальной жизни. Также дети могут подражать блогерам или персонажам игр, которые рекламируют небезопасные товары или услуги, или разглашают личную информацию.

3. Эмоциональность: младшие школьники очень эмоциональны. Они остро реагируют на события в цифровой среде: радуются победам в играх, расстраиваются из-за проигрышей, болезненно воспринимают конфликты с другими игроками или негативные комментарии.

Эмоциональность делает детей уязвимыми к кибербуллингу. Обидные комментарии, оскорбления, исключение из онлайн-групп могут нанести им серьезную психологическую травму. Также эмоциональная реакция на проигрыш в игре может быть использована мошенниками,

которые предлагают «легкие» способы победы за деньги или личную информацию.

4. Недостаточное понимание рисков: младшие школьники еще не до конца понимают потенциальные опасности онлайн-мира. Они не всегда осознают, что за аватаром в игре может скрываться злоумышленник, что не вся информация в интернете достоверна, что распространение личной информации может быть опасным.

Недостаточное понимание рисков повышает вероятность столкновения с различными онлайн-угрозами: кибербуллингом, контактом с незнакомцами, мошенничеством, фишингом, вредоносным ПО.

5. Стремление к общению: интернет становится для младших школьников важным пространством для общения со сверстниками. Они общаются в чатах, играют в онлайн-игры, делятся фотографиями и видео в социальных сетях.

Стремление к общению может привести к контакту с опасными незнакомцами. Дети могут довериться человеку, с которым познакомились в онлайн-игре или социальной сети, и раскрыть ему личную информацию, которая может быть использована в злонамеренных целях. Также в онлайн-общении дети могут столкнуться с кибербуллингом или нежелательным контентом.

Перечисленные выше особенности восприятия информации и поведения младших школьников в цифровой среде зависят от возрастных особенностей, характерных для этого возраста, а также от индивидуальных особенностей школьников, их характера, темпа развития и восприятия мира. Поэтому важно наблюдать за младшими школьниками со стороны и заблаговременно информировать их о проблемах кибербезопасности и путях их решения.

1.3 Направления работы педагога с семьей по формированию основ кибербезопасного поведения младших школьников

Совместная работа школы и семьи, направленная на предупреждение проблем, связанных с угрозами кибербезопасности для детей младшего школьного возраста очень важна. Обучающиеся начальной школы часто сталкиваются с проблемами кибербезопасности, из-за отсутствия опыта и критичности мышления по отношению к различным ситуациям в сети. Родители и учителя, установив доверительные отношения с детьми смогут обсудить любые проблемы, в том числе онлайн-безопасности. Взрослые должны научить детей распознавать опасности в Интернете, устанавливать четкие правила нахождения в онлайн пространстве и быть опорой и поддержкой в любой ситуации. В России существует ряд федеральных законов, направленных на защиту детей от информации, которая может навредить их психическому и физическому здоровью, репутации ребенка и семьи в обществе и распространения конфиденциальной информации о ребенке, как пользователя сети Интернет. Эти законы являются фундаментом для построения совместной работы школы и семьи.

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ. Данный закон устанавливает классификацию информационной продукции по возрастным маркировкам, четко прописаны критерии и требования, которым должна соответствовать Интернет-продукция для детей, а также оговорены экспертиза и контроль выполнения условий [15].

Федеральный закон «Об основных гарантиях прав ребенка в Российской Федерации» от 24.07.1998 № 124-ФЗ (ред. от 28.12.2024). Содержание закона устанавливает гарантии прав и интересов ребенка. В законе описаны основные направления обеспечения и защиты прав и законных интересов ребенка в Российской Федерации, в том числе описаны различные меры, которые касаются области образования,

профессиональной ориентации, охраны здоровья, в том числе, защита ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию. Сюда входит защита от: национальной, классовой нетерпимости, реклама алкогольной, табачной, никотинсодержащей продукции, и информации, пропагандирующей это, а также распространение аудио- и видеоматериалов, содержащих сцены насилия и жестокости [18].

Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. Данный закон направлен на создание правовой основы для защиты информации всех пользователей киберпространства, как взрослых, так и детей. Закон требует от сайтов, приложений, онлайн-сервисов получать согласие на обработку персональных данных. Обязывает операторов обеспечить безопасность личной информации. Закон дает право на удаление данных, если она используется неправомерно, а также предусматривает ответственность за нарушение правил обработки персональных данных пользователей [16].

Государство заинтересовано в том, чтобы дети поколения Альфа жили в безопасном мире и делает все для того, чтобы обеспечить эту безопасность. Семья и школа – это проводники ребенка в мир информации. Совместная работа включает в себя несколько направлений и видов работы педагога с семьей. Такая работа состоит из отдельной работы педагога с родителями, педагога с младшими школьниками, педагога и совместной деятельности родителей и детей. Следовательно, все направления и виды мы рассматриваем, через отдельные категории участников образовательного процессе, из которых состоит совместная работа школы, в частности педагога, и семьи по формированию основ кибербезопасного поведения младших школьников. Только работая вместе родители и учитель смогут создать безопасную киберсреду для детей младшего школьного возраста и помочь им развить навыки самостоятельного и защищенного нахождения в киберпространстве.

Таким образом, для того чтобы обеспечить формирование основ кибербезопасного поведения младших школьников, необходимо всесторонне изучить направления работы педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Нами были выделены категории участников образовательного процесса и направления работы педагога с семьей.

Категории участников образовательного процесса, совместная работа которых играет важную роль в формирование основ кибербезопасного поведения детей в начальной школе:

1. Дети младшего школьного возраста.
2. Родители или законные представители.
3. Педагог.

Работу педагога с семьей по формированию основ кибербезопасного поведения можно разделить на три группы:

– работа педагога с родителями/законными представителями;
– работа педагога с младшими школьниками;
– работа педагога с родителями и детьми вместе.

В ходе этого взаимодействия достигаются следующие направления:

1. Информационно-просветительская работа: ознакомление родителей и детей с актуальной информацией, связанной с киберугрозами, важности знаний о кибербезопасной среде, способах защиты детей в онлайн-пространстве.

1.1 Работа педагога с родителями: родительское собрание, мини-лекция, рассылка по электронной почте или мессенджеру, круглый стол, создание информационного уголка для родителей, включающего различные памятки, буклеты, информативные рисунки.

1.2 Работа педагога с младшими школьниками: классный час, просмотр мультфильмов по теме и обсуждение содержания, викторина, выставка рисунков, создание стенда для младших школьников.

1.3 Работа педагога с родителями и детьми вместе: семейный семинар-практикум, семейный творческий конкурс, викторина.

2. Образовательная работа: формирование у родителей и детей практических навыков для обеспечения кибербезопасности. Данное направление играет ведущую роль в формирование знаний о киберсреде.

2.1 Работа педагога с родителями: практикум, мастер-класс, тренинг, семинар.

2.2 Работа педагога с младшими школьниками: практическое занятие, игра-тренинг, проект.

2.3 Работа педагога с родителями и детьми вместе: мастер-класс, практикум, семейный проект, игровой тренинг.

3. Психолого-педагогическая работа: помощь родителям и детям в понимании психологических аспектов безопасности в сети, развитие навыков уверенного поведения в онлайн среде, преодоление и предупреждение интернет-зависимости, работа с последствиями киберугроз, влияющих на психическое здоровье.

3.1 Работа педагога с родителями: индивидуальная консультация, групповой тренинг, семинар, родительское собрание с участием психолога, создание родительского клуба для обмена опытом.

3.2 Работа педагога с младшими школьниками: классный час, тренинг, ролевая игра, беседа с психологом, круглый стол.

3.3 Работа педагога с родителями и детьми вместе: ролевая игра, семейная консультация с участием психолога, круглый стол.

Таким образом, все вышеперечисленные направления работы педагога с семьей помогают всесторонне изучить проблемы кибербезопасности, научить родителей и детей распознавать угрозы онлайн-среды и бороться с ними правильно, а также способствуют совместной работе взрослых и детей, и как итог, в совокупности, помогают сформировать основы кибербезопасного поведения младших школьников.

Выводы по I главе

В первой главе мы проанализировали литературу психологической и педагогической направленности, благодаря который нам удалось рассмотреть теоретические аспекты проблемы работы педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Ключевыми моментами I главы являются следующие теоретические аспекты изучения данной проблемы:

Дети младшего школьного возраста, ввиду своих возрастных особенностей и недостатка жизненного опыта, больше всего подвержены формированию и развитию зависимого поведения по отношению к электронным устройствам, и, как следствие, возникновению большого количества проблем и угроз, связанных с кибербезопасностью.

В знакомстве детей с миром информационных технологий большую роль играют взрослые: родители и учитель. Но чаще всего родители не могу уделить должное внимание проблемам кибербезопасности, поэтому ведущую роль в этом вопросе берет на себя учитель, который является посредником между миром детей и миром взрослых. Именно учитель формирует базу знаний и умений, которыми будут пользоваться родители и дети в изучении киберпространства и его угроз. Таким образом формируя основы кибербезопасного поведения младших школьников.

Дети «поколения Альфа» в большей степени подвержены игровым и информационным аддикциям, то есть тем зависимостям, которые формируются при постоянном взаимодействие младшего школьника с электронными информационными устройствами. Негативное влияние электронных устройств на младших школьников велико, а одними из самых опасных проблем являются угрозы кибербезопасности.

Кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, сервером, мобильных устройств, электронных систем, сетей и данных.

В настоящее время Интернет и электронные устройства используются повсеместно, что показывает необходимость развития культуры осведомленности в области кибербезопасности. Понимание различных угроз киберсреды, способов их предупреждения и предотвращения играют ключевую роль во взаимодействии детей и онлайн-пространства.

Еще одним важным фактором возникновения проблем кибербезопасности являются возрастные особенности, в частности особенности восприятия информации, младших школьников и особенности поведения детей начальной школы в цифровой среде.

Для того, чтобы обезопасить младших школьников от пагубного влияния киберсреды, нужно проводить комплексную работу по всестороннему изучению проблем возникновения угроз кибербезопасности. Данная работа задействует всех участников образовательного процесса: учителя, родителей и самого обучающегося. Предупреждение возникновения любых проблем и угроз связанный с киберпространством – это полноценная осведомлённость темой кибербезопасность, угрозы и последствия для младших школьников.

Только такая работа поможет оградить ребенка от угроз кибербезопасности и сформировать основы кибербезопасного поведения младших школьников.

ГЛАВА 2. ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА ПО ИЗУЧЕНИЮ УРОВНЯ СФОРМИРОВАННОСТИ ЗНАНИЙ О КИБЕРБЕЗОПАСНОМ ПОВЕДЕНИИ У ДЕТЕЙ МЛАДШЕГО ШКОЛЬНОГО ВОЗРАСТА

2.1 Ход исследовательской работы. Характеристика используемых методик

Исследовательская работа проводилась с учетом теоретических сведений, представленных в первой главе. Для работы по изучению уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста было проведено тестирование обучающихся МАОУ г. Челябинска и родителей. Всего в исследовательской работе участвовало: 15 детей – учащихся 4 класса и 15 родителей.

Цель исследовательской работы: выявить уровень сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста и склонности детей к интернет-зависимости со стороны родителей, и, на основании полученных результатов, разработать программу взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Задачи исследовательской работы:

1. Подобрать методики, способствующие выявлению уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста и выявлению склонности к интернет-зависимости у детей начальной школы со стороны родителей.
2. Провести исследовательскую работу по выявлению проблем уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста и их склонности к интернет-зависимости со стороны родителей.

3. Обработать результаты тестирования младших школьников и родителей и выявить детей, с проблемами сформированности знаний о кибербезопасном поведении и склонностью к интернет-зависимости.

4. Разработать программу взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Исследовательская работа по выявлению проблем уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста и склонности детей к интернет-зависимости со стороны родителей состояла из двух частей.

Первоначально исследовательской работе подверглись родители. Им был предоставлен тест на детскую интернет-зависимость для родителей, автором которого является С. А. Кулаков (Приложение № 1). Суть исследовательской работы заключалась в том, что родитель должен был ответить на 20 вопросов теста, выбирая тот ответ, который подходит к описанию реальной ситуации, связанной с уровнем проявления интернет-зависимости у его ребенка. Тест имеет интерпретацию, благодаря которой можно выявить склонность детей к интернет-зависимости со стороны родителей. Ключ к интерпретации теста предполагает три стадии интернет-зависимости: отсутствие зависимости, стадия увлеченности, стадия зависимости (Приложение № 2).

Вторая часть исследовательской работы состояла из проведения теста «Это нормально или опасно?» для младших школьников, от IT-компании «Лаборатория Касперского». Суть исследовательской работы заключалась в том, что младший школьник должен был ответить на 10 вопросов, выбирая тот ответ, который он считают верным. Каждый вопрос предлагает 4 варианта ответа с возможностью одиночного выбора, в зависимости от правильности ответов можно выявить уровень сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста (Приложение № 3). Ключ к интерпретации теста предполагает три уровня сформированности знаний о кибербезопасном поведении: низкий уровень

сформированности знаний, средний уровень сформированности знаний, высокий уровень сформированности знаний (Приложение № 4).

2.2 Анализ результатов исследовательской работы

При определении склонности младших школьников к интернет-зависимости со стороны родителей, по тесту на детскую интернет-зависимость для родителей, были получены результаты (таблица 1).

Таблица 1 – Индивидуальные результаты родителей (по тесту на детскую интернет-зависимость для родителей)

№	Возраст участника	Результат
1	41	45
2	44	31
3	39	62
4	42	44
5	48	55
6	40	58
7	36	81
8	49	35
9	38	77
10	44	62
11	39	67
12	37	83
13	42	53
14	45	78
15	36	81

По результатам теста на детскую интернет-зависимость, можно увидеть, что группа родителей содержит в себе участников разных возрастов: от 36 до 49 лет. Индивидуальные показатели представлены в приложении 5.

При определении уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста, по тесту «Это нормально или опасно?», были получены следующие результаты (таблица 2).

Таблица 2 – Индивидуальные результаты детей по тесту «Это нормально или опасно?»

№	Номер родителя в таблице	Результат
1	Родитель 7	1
2	Родитель 4	3
3	Родитель 6	4
4	Родитель 12	5
5	Родитель 14	0
6	Родитель 15	6
7	Родитель 1	9
8	Родитель 10	5
9	Родитель 3	2
10	Родитель 5	7
11	Родитель 11	1
12	Родитель 8	1
13	Родитель 9	8
14	Родитель 2	7
15	Родитель 13	6

Исходя из полученных результатов, мы видим, что в тесте участвовали дети 4 класса. Всего 15 обучающихся. Ответы обучающихся соотносятся с ответами их родителей.

Благодаря полученным результатам мы можем составить сравнительную таблицу расположения детей по уровням проявления интернет-зависимости и уровнем сформированности знаний о

кибербезопасном поведении у детей младшего школьного возраста (таблица 3).

Таблица 3 – Распределение детей по уровням проявления интернет-зависимости и сформированности знаний о кибербезопасном поведении

	Уровень проявления интернет-зависимости		Уровень сформированности знаний о кибербезопасном поведении	
	N	Доля (%)	N	Доля (%)
Низкий уровень	4	27	6	40
Средний уровень	8	53	5	33
Высокий уровень	3	20	4	27

Графический результат сравнения расположения детей по уровням проявления интернет-зависимости и сформированности знаний о кибербезопасном поведении представлен на рисунке 1.

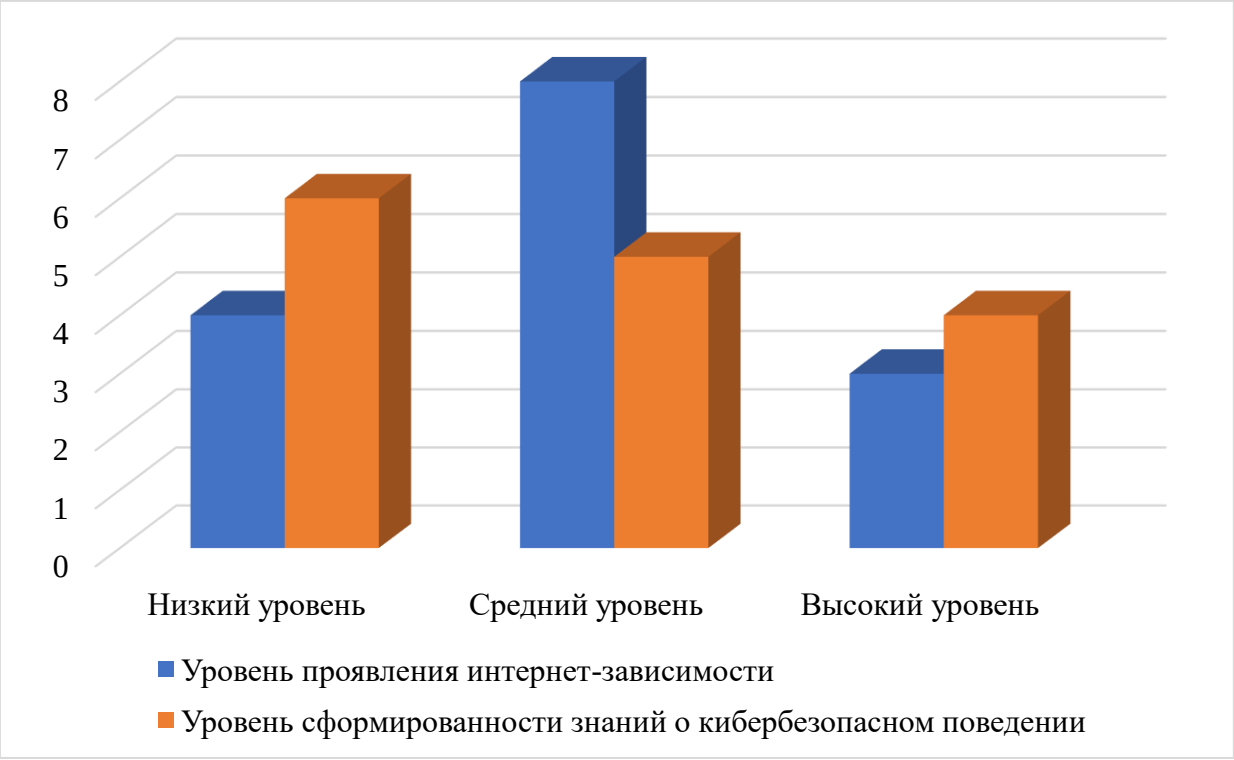

Рисунок 1 – Распределение детей по уровням проявления интернет-зависимости и сформированности знаний о кибербезопасном поведении

Исходя из данных тестов, мы видим, что показатели уровня проявления интернет-зависимости и уровня сформированности знаний о кибербезопасном поведении у младших школьников отличаются.

Например, самым большим показателем уровня проявления интернет-зависимости является средний уровень, или стадия увлеченности у большинства детей. Это говорит о том, что младшие школьники действительно подвергаются воздействию электронных устройств, и присутствует большая доля вероятно возникновения зависимого поведения. При этом самым большим показателем уровня сформированности знаний о кибербезопасном поведении является низкий уровень, то есть почти полное отсутствие знаний у большинства детей. Что также подтверждает проблему отсутствия или недостатка знаний у детей, для безопасного нахождения в киберпространстве. Самым маленьким показателем уровня проявления интернет-зависимости является высокий уровень, или уровень зависимости. Но даже его минимальное наличие, среди детей младшего школьного возраста, показывает, что проблема интернет-зависимости стоит остро. Ведь такая проблема напрямую связана с угрозами кибербезопасности детей.

Данные таблицы 2 подтверждают это, показывая, что есть дети, у которых имеется высокий уровень интернет-зависимости и при этом низкий уровень сформированности знаний о кибербезопасном поведении.

Таким образом, данные методики действительно помогли выявить детей со стадиями увлеченности и зависимости от электронных устройств, или со средним и высоким уровнем проявления интернет-зависимости. А большой показатель детей с низким уровнем сформированности знаний о кибербезопасном поведении, показывает актуальность проблемы и необходимость ее решения. Именно поэтому формирование основ кибербезопасного поведения у детей младшего школьного возраста так важно. Меры, направленные на повышение уровня знаний о кибербезопасном поведении у детей, помогут остановить развитие этой проблемы и обезопасить детей от угроз киберсреды и их последствий.

2.3 Программа взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников

Дети младшего школьного возраста всегда нуждаются в поддержке взрослого, особенно если это касается зоны ближайшего развития ребенка и сформированности его знаний об основах кибербезопасного поведения. Поэтому привлечение родителей в совместную работу с педагогом и детьми очень важно. Для всестороннего изучения проблем киберпространства и включения в эту деятельность родителей, нами была разработана программа взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников, которая рассчитана на 1 учебный год. В данной программе мы описываем основные направления работы педагога с семьей, для устранения низкого уровня сформированности знаний о кибербезопасном поведении у младших школьников и привлечения родителей, для участия в совместной деятельности школы и семьи.

В состав программы входит:

– пояснительная записка,
– цель и задачи,
– общая характеристика программы,
– план реализации программы.

Пояснительная записка

Цифровизация и информатизация всех сфер жизнедеятельности человека сделали нас постоянными пользователями электронный устройств, приложений, сервисов, Интернета и потребителями информационного контента.

Последствий использования электронных устройств младшими школьниками очень много. Электронные устройства пагубно влияют на психологическое и физическое здоровье обучающихся, изменяют их сознание, приводят к нарушению социальных норм и как следствие

возникновению отклоняющегося, или, другими словами, аддиктивного поведения. Дети поколения Альфа и их частое использование электронных устройств – это доказательство возникновения новых терминов, таких как «номофобия», то есть зависимость, при которой человек испытывает страх, волнение и тревогу из-за отсутствия телефона или другого электронного устройства рядом, возможности контактировать с ним. Или «фаббинг», что означает привычку собеседника, при которой он постоянно отвлекается на смартфон. Произошло это слово от слияния двух других: «phone» – телефон и «snubbing» – пренебрежение. Большое количество факторов влияют на формирование зависимого поведения от электронных устройств, и как следствие возникновению угроз кибербезопасности. Поэтому важно вести совместную деятельность педагога, обучающегося и родителя по формированию основ кибербезопасного поведения младших школьников.

По данным российской технологичной исследовательской компании «Mediascope» на март 2025 года было зафиксировано свыше 93 млн. пользователей социальной сети ВКонтакте, а также свыше 85 млн. пользователей поисковой системы Яндекс.Поиск [26]. При этом население Российской Федерации составляет свыше 146 млн. человек. Данные о пользователях социальных сетей и поисковиков показывают, что около 64 % людей всей страны использует ВКонтакте, и около 58 % людей используют поисковик Яндекс, Поиск. Что свидетельствует о популярности данных ресурсов. Эти данные постоянно растут и показывают увеличение процента числа пользователей. Насколько эти ресурсы популярны, настолько они и опасны, ведь именно социальные сети и поисковики являются проводниками в мир информации, а значит и в мир угроз кибербезопасности.

Требования к результатам освоения основной образовательной программы начального общего образования включают в себя элементы, которые можно отнести к формированию базовых навыков работы с информацией. В действующем ФГОС НОО написано, что выпускник

начальной школы должен уметь работать с информацией: осуществлять поиск, обработку, анализ информации и работать в информационной среде. Формирование ИКТ-компетентности также подразумевается в рамках освоения познавательных УУД, так как работа с информацией напрямую связано с использованием цифровых технологий. Также в рамках отдельных предметов могут быть предусмотрены конкретные требования к использованию ИКТ [20].

Важно отметить введение «Концепции информационной безопасности» распоряжением Правительства РФ от 02.12.2015 года. Этот документ официально признает детей, как потребителей информационно-коммуникативных технологий и призван способствовать единой политике в области информационной безопасности детей [19].

Большое внимание со стороны государства к этой проблеме, показывает реальную картину взаимодействия детей и цифровой среды, которое несет опасения, связанные с возникновением зависимого поведения к электронным устройствам и угроз кибербезопасности для обучающихся начальной школы.

Теоретические основы формирования кибербезопасного поведения младших школьников рассматриваются в трудах следующих авторов: А. Ю. Акопов, Я. И. Гилинский, Е. В. Змановская, И. С. Кон, Ц. П. Короленко, А. Е. Личко, Д. И. Фельдштейн.

Проблемой Интернет-зависимости занимались: А. В. Ваганов, А. Е. Войскунский, А. Е. Жичкина, М. В. Жукова, В. А. Лоскутова, А. В. Минаков, А. И. Ракитов, А. С. Холл, М. А. Шоттон.

Изучением понятий «кибербезопасность», «информационная грамотность» и «информационная культура» занимались такие ученые как К. Янг, А. Е. Войскунский, М. Гриффитс, А. Ю. Егорова, А. Голдберг, Ц. П. Короленко, Дж. Грохол, А. Е. Жичкина, М. Фенишел и др.

Сегодня очень важно особое внимание уделять проблемам кибербезопасности младших школьников. Учителям начальных классов

необходимо формировать знаний о кибербезопасном поведение у детей младшего школьного возраста и лучше всего включать в эту деятельность родителей младших школьников.

Цель: создание условий для взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников.

Задачи:

1. Повышение уровня педагогической компетентности родителей в вопросах взаимодействия с детьми и формирования зоны их актуального развития с помощью информирования о проблемах киберпространства, в том числе угроз кибербезопасности и их последствий для семьи и младшего школьника.

2. Формирование понятия кибербезопасность и основы кибербезопасного поведения младших школьников посредством работы педагога с родителями, детьми и совместной работы родителей и детей.

3. Формирование мотивации родителей и детей для сотрудничества с учителем начальных классов.

4. Формирование системы знаний о основах кибербезопасного поведения у младших школьников.

Общая характеристика

Данная программа направленна на укрепление взаимодействия педагога с родителями и детьми, что в свою очередь будет способствовать формированию основ кибербезопасного поведения младших школьников.

Направления взаимодействия педагога с родителями и младшими школьниками: информационно-просветительская работа, образовательная работа, психолого-педагогическая работа.

Работа педагога с семьей: родительское собрание, практикум, тренинг, мастер-класс, классный час, индивидуальные консультации, круглый стол, викторина, ролевая игра, проект, конкурс.

Данная программа будет реализована в три этапа:

1. Подготовительный этап. Срок реализации: сентябрь – октябрь.

Цель: сбор информации, проведение диагностик с родителями и детьми, анализ результатов диагностических методик и подготовка теоретической базы.

2. Основной этап. Срок реализации: октябрь – апрель.

Цель: достижение основных задач программы при взаимодействии педагога с семьей, отдельно работая с родителями, младшими школьниками и работая с ними совместно.

3. Заключительный этап. Срок реализации: апрель – май.

Цель: проверка эффективной реализации программы путем проведения диагностических методик подготовительного этапа повторно.

План реализации программы

План реализации программы для взаимодействуя педагога с семьей по формированию основ кибербезопасного поведения младших школьников «Безопасная киберсреДа» представлен в таблицах 4-8. Разработанные конспекты занятий и другие методические материалы представлены в приложении 5-7.

Таблица 4 – Мероприятия подготовительного этапа

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
1	Диагностика уровня знаний родителей о проблемах и угрозах кибербезопасности и интернет-зависимости	Проведение диагностических мероприятий с целью выявления знаний родителей о существующей проблеме	Сентябрь
2	Диагностика детей младшего школьного возраста на уровень сформированности знаний о кибербезопасном поведении	Проведение диагностических мероприятий с целью выявления знаний младших школьников о кибербезопасном поведении	Сентябрь
3	Предоставление результатов данных методик родителям	Информирование родителей о проблеме низкого уровня сформированности основ кибербезопасного поведения младших школьников	Октябрь

Таблица 5 – Мероприятия основного этапа (работа педагога с родителями)

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
1	Родительское собрание «Цифровой мир наших детей: угрозы и возможности»	Знакомство с проблемой кибербезопасности, обзор основных угроз, правил безопасности и полезных ресурсов.	Октябрь
2	Практикум «Настройка родительского контроля на различных устройствах»	Обучение практическим навыкам настройки родительского контроля на компьютерах смартфонах, планшетах.	Ноябрь
3	Мастер класс «Распознаем фишинг: как защитить себя и ребенка от мошенников в сети»	Обучение распознавать фишинговые сообщения и сайты через практические упражнения	Декабрь
4	Тренинг «Как говорить с ребенком о кибербезопасности»	Обучение эффективным стратегиям коммуникации с детьми на сложные темы	Январь
5	Семинар «Психологические аспекты кибербезопасности: как формировать у ребенка ответственное отношение к онлайн-среде»	Обсуждение психологических факторы, влияющих на поведение ребенка в сети, и способов формирования ответственного отношения к онлайн-миру	Февраль
6	Родительское собрание с участием психолога «Эмоциональное благополучие ребенка в цифровом пространстве»	Обсуждение влияния интернета на эмоциональное состояние детей, способы профилактики негативных последствий	Март
7	Создание родительского клуба для обмена опытом и взаимоподдержки по вопросам воспитания детей в эпоху цифровизации	Формирование сообщества родителей, готовых делиться опытом и поддерживать друг друга. А также связь педагога и родителей по конкретным проблемам	Апрель

Таблица 6 – Мероприятия основного этапа (работа педагога с младшими школьниками)

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
1	Классный час: «Интернет-страна: путешествие с правилами»	В игровой форме познакомить детей с основными правилами поведения в интернете	Октябрь
2	Просмотр и обсуждение мультфильмов от «Лаборатории Касперского» по теме кибербезопасность	Обсудить увиденное, выделить верные действия и ошибки героев	Ноябрь
3	Викторина «Знатоки кибербезопасности»	Закрепить полученные знания в игровой форме, используя вопросы и задания по пройденному материалу.	Ноябрь

Продолжение таблицы 6

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
4	Игра-тренинг «Ловушки интернета»	Научить детей распознавать киберугрозы и правильно на них реагировать, через моделирование различных ситуаций	Декабрь
5	Проект «Моя безопасная страничка»	Дети создают макет своей странички в социальной сети, применяя знания о настройках приватности	Февраль
6	Классный час «Дружба онлайн и офлайн»	Обсудить с детьми правила безопасного общения в сети, этику онлайн-коммуникации, проблему кибербуллинга.	Март
7	Круглый стол: «Интернет и я: как найти баланс	Обсудить с детьми важность баланса между онлайн и офлайн жизнью, преимущества и недостатки использования интернета	Апрель

Таблица 7 – Мероприятия основного этапа (работа педагога с родителями и младшими школьниками вместе)

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
1	Семейный конкурс «Правила безопасного интернета для нашей семьи»	Создание совместного плаката, визуализация правил кибербезопасности, понятный детям и взрослым	Февраль
2	Семейный проект «Кибер-детективы»	Создание презентации/видеоролика или комикса о киберугрозах и способах защиты	Март
3	Ролевая игра «Что делать, если…»	Моделирование ситуаций, связанных с киберугрозами, и поиск совместных решений.	Апрель

Таблица 8 – Мероприятия заключительного этапа

№ п/п	Название и содержание мероприятия	Задачи мероприятия	Срок проведения
1	Повторное проведение диагностических мероприятий	Оценивание прогресса в работе над проблемой	Май
2	Собрание с родителями для подведения итогов работы	Обобщение изученного и подведение итогов	Май

Выводы по II главе

Во второй главе выпускной квалификационной работы с целью выявления уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста нами была проведена исследовательская работа, которая проходила на базе МАОУ г. Челябинска. В тестировании приняли участие 15 детей – учащихся 4 класса и 15 родителей в возрасте от 36 до 49 лет.

В исследовательской работе были использованы следующие методики:

1. Тест на детскую интернет-зависимость для родителей, автором которого является С. А. Кулаков.
2. Тест «Это нормально или опасно?» для младших школьников от «Лаборатории Касперского»

Первоначально исследовательской работе подверглись родители. Полученные результаты помогли определить уровень зависимости от электронных устройств, в младшем школьном возрасте.

Затем в прохождении тестирования поучаствовали обучающиеся 4 класса, их результаты были интерпретированы и помогли определить уровень сформированности знаний о кибербезопасном поведении.

Благодаря полученным данным была составлена сравнительная диаграмма, которая показала, что дети младшего школьного возраста действительно подвержены воздействию электронных устройств, что доказывает наибольшее количество опрошенных в колонке «средний уровень» или увлеченность, и в колонке «высокий уровень» или стадия зависимости. Сравнительная диаграмма также показала наибольшее количество респондентов с отсутствием или недостатком знаний о кибербезопасном поведении, в колонке «низкий уровень». Таблица 2 показывает, что есть дети, которые одновременно имеют увлеченность или зависимость от электронных устройств и недостаточность знаний о

кибербезопасном поведении. Это говорит о том, что проблема сформированности основ кибербезопасного поведения является ключевой и требует разработки программы взаимодействия педагога с семьей по формированию основ кибербезопасного поведения у младших школьников.

Именно поэтому важным этапом, после проведения исследования, считается разработка программы взаимодействия педагога с семьей.

Программа взаимодействия педагога с семьей была поделена на несколько групп: работа педагога с родителями, работа педагога с младшими школьниками, работа педагога с родителями и младшими школьниками вместе. Весь теоретический материл, практические и творческие задания охватывали следующие направления: информационно-просветительская работа, образовательная работа, психолого-педагогическая работа.

Программы взаимодействия педагога с семьей по формированию основ кибербезопасного поведения у младших школьников состоит из: диагностического материала для родителей и детей, родительских собраний, практикума, мастер-класса, тренинга, семинара, классного часа, викторины, просмотра видеоматериалов, игры-тренинг, проекта, круглого стола, конкурса, ролевой игры.

Особенностью разработанной нами программы для взаимодействия педагога с семьей является то, что она поможет учителям начальных классов в формировании основ кибербезопасного поведения у младших школьников в совместной работе с родителями.

ЗАКЛЮЧЕНИЕ

Исходя из результатов теоретической и исследовательской работы, посвященных проблеме работы педагога с семьей по формированию основ кибербезопасного поведения младших школьников, можно выделить следующие моменты:

1. Цели и задачи выпускной квалификационной работы были успешно реализованы в ходе изучения теоретических аспектов рассматриваемой проблемы, проведения исследовательской работы и разработки программы взаимодействия педагога с семьей.

2. В работе мы рассматривали проблему формирования основ кибербезопасного поведения у детей младшего школьного возраста через следующие понятия: аддитивное поведение, интернет-зависимость, электронные устройства, кибербезопасность.

3. Подобранные нами методики помогли провести тестирование родителей и младших школьников, для выявления проблемы интернет-зависимости младших школьников и отсутствия или недостатка знаний о кибербезопасном поведении у них и последующего сравнения результатов для разработки программы взаимодействия педагога с семьей по данной проблеме.

4. На основании анализа результатов исследовательской работы нами были сделаны выводы о том, что младшие школьники действительно нуждаются в формировании основ кибербезопасного поведения при участии родителей и педагога, доказана актуальность выбранной темы.

5. Нами была разработана программа взаимодействия педагога с семьей по формированию основ кибербезопасного поведения младших школьников

Таким образом актуальность данной проблемы доказана, цель достигнута, а задачи выполнены в полном объеме.

СПИСОК ЛИТЕРАТУРЫ

1. АО «Лаборатория Касперского»: официальный сайт. – Москва. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 04.02.2025).

2. Баланов А. Н. Кибербезопасность : учеб. пособие / А. Н. Баланов. – Санкт-Петербург : Изд-во Лань, 2023. – 680 с. – ISBN 978-5-507-49562-7.

3. Батюшкин М. В. «Фишинг» - компьютерное мошенничество? / М. В. Батюшкин // Символ науки. – 2021. – № 1. – С. 90–93.

4. Бекчонова Ш. Б. Актуальность образования по кибербезопасности в педагогике / Ш. Б. Бекчонова // Процветание науки. – 2022. – № 2. – С. 1–6.

5. Жукова М. В. Компьютерная зависимость как один из видов аддиктивной реализации / М. В. Жукова // Вестник Южно-Уральского государственного гуманитарно-педагогического университета. – 2013. – №11. – С. 23–26.

6. Захарченко Н. А. Проблемы изучения доверия детей младшего школьного возраста к незнакомым взрослым / Н. А. Захарченко, С. Н. Ситдикова // Russian Journal of Education and Psychology. – 2012. – № 1. – С. 1– 19.

7. Ковина М. В. Психологические особенности детей младшего школьного возраста и факторы их успешного обучения / М. В. Ковина // Материалы Всероссийской научно-практической конференции «Наука и социум». – 2020. – № 4. – С. 74–80.

8. Козлова Н. Ш. Кибербезопасность и информационная безопасность: сходства и отличия / Н. Ш. Козлова, В. А. Довгаль // Вестник Адыгейского государственного университета. – 2021. – № 3. – С. 88–96.

9. Лукичев В. В. Отклоняющееся поведение / В. В. Лукичев // Ариадна: центр психолого-педагогической реабилитации, коррекции и

образования. – 2022. – URL: https://arnar.ru/stati/lukichev-otklonyayushcheesya-povedenie (дата обращения: 23.01.2025).

10. Матвиенко С. В. Образование XXI: плюсы и минусы цифрового образования / С. В. Матвиенко, Е. В. Васильева // Образование и право. – 2022. – № 1. – С. 165–170.

11. Общение с незнакомцами онлайн: почему это опасно // Лига безопасного Интернета: [сайт]. – 2025. – URL: https://ligainternet.ru/wp-content/uploads/2022/09/obshhenie-s-neznakomtsami-onlajn-web.pdf (дата обращения 06.03.2025)

12. Онлайн программа Kidskey: официальный сайт. – Москва. – URL: https://kidskey.org/blog/critical-thinking-of-a-child (дата обращения: 13.03.2025)

13. От подражания – к независимости // Журнал для родителей и педагогов «Семья и школа» : [сайт]. – 2024. – URL: https://семьяишкола.рф/2024/01/31/от-подражания-к-независимости/ (дата обращения: 13.03.2025)

14. Платформа доступного IT образования Merion Academy: официальный сайт. – Москва. – URL: https://wiki.merionet.ru/articles/triada-cia-konfidencialnost-celostnost-dostupnost (дата обращения: 27.02.2025).

15. Российская федерация. Законы. О защите детей от информации, причиняющей вред их здоровью и развитию (ред. от 28.02.2025) : Федеральный закон № 436-ФЗ : [принят Государственной Думой 21 декабря 2010 г. : одобрен Советом Федерации 24 декабря 2010 г.]. – Москва : Кремль, 2010.

16. Российская федерация. Законы. О персональных данных: Федеральный закон № 152-ФЗ : [принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г.]. – Москва : Кремль, 2006.

17. Российская федерация. Законы. Об образовании в Российской Федерации (ред. от 28.02.2025) : Федеральный закон № 273-ФЗ : [принят

Государственной Думой 21 декабря 2012 г. : одобрен Советом Федерации 26 декабря 2012 г.]. – Москва : Кремль, 2012. – 404 с.

18. Российская федерация. Законы. Об основных гарантиях прав ребенка в Российской Федерации : Федеральный закон № 124-ФЗ : [принят Государственной Думой 3 июля 1998 г. : одобрен Советом Федерации 9 июля 1998 г.]. – Москва : Кремль, 1998.

19. Российская Федерация. Концепция. Информационной безопасности детей : Концепция № 2471-р : [утверждена распоряжением Правительства РФ 2 декабря 2015 г.]. – Москва. – 2015.

20. Российская Федерация. Приказ. Об утверждении федерального государственного стандарта начального общего образования : Приказ № 286 : [утвержден Министерством просвещения Российской федерации 31 мая 2021 г.]. – Москва. – 2021. – 57 с.

21. Симанова Е. А. Клиповое мышление у младших школьников, проблемы XXI века / Е. А. Симанова // высшая школа делового администрирования. – 2022. – URL: https://s-ba.ru/conf-posts-2022-08/tpost/5jm8ufo051-klipovoe-mishlenie-u-mladshih-shkolnikov (дата обращения: 13.03.2025)

22. Симонова В. А. Защита несовершеннолетних от негативной информации в сети интернет / В. А. Симонова, Е. А. Лифинцева // Научные известия. – 2022. – № 26. – С. 128–131.

23. Смердова Е. А. Особенности эмоциональной сферы у детей младшего школьного возраста / Е. А. Смердова // Актуальные проблемы гуманитарных и естественных наук. – 2015. – № 11. – С. 1–3.

24. Солдатова Г. У. Персональные данные и дети: вопросы безопасности / Г. У. Солдатова, О. И. Теславская // Эпоха науки. – 2017. – № 12. – С. 92–101.

25. Старых А. И. Психологические особенности внимания младших школьников / А. И. Старых // Вопросы науки и образования – 2018. – № 16. – С. 84–93.

26. Технологичная исследовательская компания Mediascope : официальный сайт. – Москва, обновляется в течение недели. – URL: https://mediascope.net/data/ (дата обращения 19.03.2024).

27. Тиркашевич Г. М. Кибербуллинг среди детей: понятие, современные формы и защитные механизмы / Г. М. Тиркашевич // ORIENSS. – 2022. – № 26. – С. 84–93.

28. Три четверти детей указывают возраст в своих профилях в социальных сетях // АО «Лаборатория Касперского»: [сайт]. – 2025. – URL: https://www.kaspersky.ru/about/press-releases/tri-chetverti-detej-ukazyvayut-vozrast-v-svoih-profilyah-v-socialnyh-setyah (дата обращения: 06.03.2025).

29. Тужуева Л. А. Психологические особенности младшего школьника / Л. А. Тужуева // Вопросы науки и образования. – 2021. – № 8. – С. 53–55.

30. Что такое кибербезопасность // Российская компания Positive technologies : [сайт]. – 2022. – URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost/ (дата обращения 27.02.2025)

31. F. Saliceti. Internet Addictional Disorder / F. Saliceti // Procedia: Social and Behavioral Sciences. – 2015. – № 191. – P. 1373–1376.

32. M. Prensky. Digital Natives, Digital Immigrants / M. Prensky // On the Horizon MBC University Press. – 2001. – Vol. 9, № 5. – P. 1–6.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Тест на детскую интернет-зависимость для родителей

Автор теста – С. А. Кулаков. Тест состоит из 20 вопросов с 5 вариантами ответа, с возможностью одиночного выбора.

Инструкция: оцените каждое высказывание по пятибалльной шкале

1 – очень редко, 2 – иногда, 3 – часто, 4 – очень часто, 5 – всегда.

1. Как часто Ваш ребенок нарушает временные рамки, установленные вами для пользования сетью?
2. Как часто Ваш ребенок запускает свои обязанности по дому для того, чтобы провести больше времени в сети?
3. Как часто Ваш ребенок предпочитает проводить время в сети вместо того, чтобы провести его в кругу семьи?
4. Как часто Ваш ребенок формирует новые отношения с друзьями по сети?
5. Как часто Вы жалуетесь на количество времени, проводимые Вашим ребенком в сети?
6. Как часто учеба Вашего ребенка страдает из-за количества времени, проведенном Вашим ребенком в сети?
7. Как часто Ваш ребенок проверяет электронную почту, прежде чем заняться чем-то другим?
8. Как часто Ваш ребенок предпочитает общение в сети общению с окружающими?
9. Как часто Ваш ребенок сопротивляется или секретничает при вопросе о том, что он делает в Интернете?
10. Как часто Вы заставали своего ребенка пробивающимся в сеть против Вашей воли?
11. Как часто Ваш ребенок проводит время в своей комнате, играя за компьютером?

12. Как часто Ваш ребенок получает странные звонки от его новых сетевых «друзей»?

13. Как часто Ваш ребенок огрызается, кричит или действует раздраженно, если его побеспокоили по поводу пребывания в сети?

14. Как часто Ваш ребенок выглядит более уставшим и утомленным, чем в то время, когда у Вас не было Интернета?

15. Как часто Ваш ребенок выглядит погруженным в мысли о возвращении в сеть, когда он находится вне сети?

16. Как часто Ваш ребенок ругается и гневается, когда Вы сердитесь по поводу времени, проведенного им в сети?

17. Как часто Ваш ребенок предпочитает своим прежним любимым занятиям, хобби, интересам других нахождение в сети?

18. Как часто Ваш ребенок злится и становится агрессивным, когда Вы накладываете ограничение на время, которое он проводит в сети?

19. Как часто Ваш ребенок предпочитает вместо прогулок с друзьями проводить время в сети?

20. Как часто Вы чувствуете подавленность, упадок настроения, нервничает, когда находится вне сети, а по возвращении в сеть все это исчезает?

ПРИЛОЖЕНИЕ 2

Интерпретация результатов теста на детскую интернет-зависимость для родителей

При сумме баллов до 50 родителям не стоит волноваться, уровень влияния Интернета на жизнь младших школьников невелик, стадия зависимости не развивается.

При сумме баллов 50-79 родителям необходимо учитывать серьезное влияние Интернета на жизнь вашего ребенка и всей семьи, видно проявление стадии увлечения.

При сумме баллов 80 и выше, у ребенка с высокой долей вероятности Интернет-зависимость и ему необходима помощь специалиста.

ПРИЛОЖЕНИЕ 3

Тест «Это нормально или опасно?»

Тест на определение уровня сформированности знаний о кибербезопасном поведении у детей младшего школьного возраста, состоит из 10 вопросов с 4 вариантами ответа, с возможностью одиночного выбора.

1. Какое начало адреса сайта безопаснее?
   A. http://
   B. https//
   C. httpps://
   D. Разницы нет
2. Ты хочешь купить что-то на Avito или другом сайте с частными объявлениями. Как поступишь?
   A. Договорюсь с продавцом, переведу ему деньги на карту, буду ждать посылку
   B. Договорюсь с продавцом о встрече, отдам деньги наличными в обмен на товар
   C. Договорюсь с продавцом и попрошу встретиться с ним знакомого
   D. Перешлю ссылку на товар кому-нибудь из родителей и попрошу их купить мне эту вещь
3. Какой из этих паролей наиболее надежен для регистрации почтового ящика?
   A. 9162651798
   B. L6520g169_?!
   C. 916265oleg
   D. SuperOleg
4. Где общаться под настоящим именем и фамилией точно безопасно?
   A. Да везде, это ведь всего лишь имя и фамилия
   B. В чате со своими одноклассниками
   C. Вконтакте в группах по интересам
   D. Нигде
5. Чего не стоит делать в онлайн-играх?
   A. Вступать в гильдии
   B. Ходить в рейды
   C. Покупать игровые предметы за настоящие деньги у других игроков
   D. В них вообще играть не стоит

6. Кому разрешишь отмечать тебя на фотографиях в соцсетях?
   A. Всем
   B. Только друзьям
   C. Только друзьям с твоего согласия
   D. Никому
7. А о чем напишешь пост без всяких опасений?
   A. «Вчера смотрели интересный фильм...»
   B. «Завтра в пять иду на каток «Наш каток»...»
   C. «Отцу подняли зарплату, надеюсь, теперь куда-нибудь съездим…»
   D. «Как же бесит Петя Иванов…»
8. Тебе пришло сообщение от одноклассника - он попал в неприятности и просит срочно перевести ему денег. Как поступишь?
   A. Переведу, конечно, я же нормальный друг
   B. Проигнорирую
   C. Сначала спрошу ответным сообщением, что случилось, а потом уже переведу
   D. Позвоню и спрошу, что случилось
9. Кстати, а что будешь делать, если взломают твою страницу?
   A. Ничего
   B. Заведу новую
   C. Напишу в техподдержку. Чтобы они помогли восстановить доступ
   D. У меня такой пароль, что не взломают
10. Рассказ о какой из этих ситуаций в интернете родителям – дело вкуса, а не необходимость?
   A. Твою страницу взломали
   B. Тебе пишут гадости в комментариях
   C. У твоего блога стало больше тысячи подписчиков
   D. Тебе предлагает встретиться френд, с которым вы раньше не виделись

ПРИЛОЖЕНИЕ 4

Интерпретация результатов теста «Это нормально или опасно?»

1-3 правильных ответов: низкий уровень сформированности знаний о кибербезопасном поведении у младших школьников, отсутствие знаний подвергает их к опасному нахождение в сети.

4-7 правильных ответов: средний уровень сформированности знаний о кибербезопасном поведении у младших школьников, знания сформированы не полностью, вероятность стать жертвой мошенников есть, но меньше.

8-10 правильных ответов: высокий уровень сформированности знаний о кибербезопасном поведении у младших школьников, вероятность стать жертвой мошенника единична.

Для наглядности интерпретации результатом представлен ключ интерпретации (рисунок 4.1)

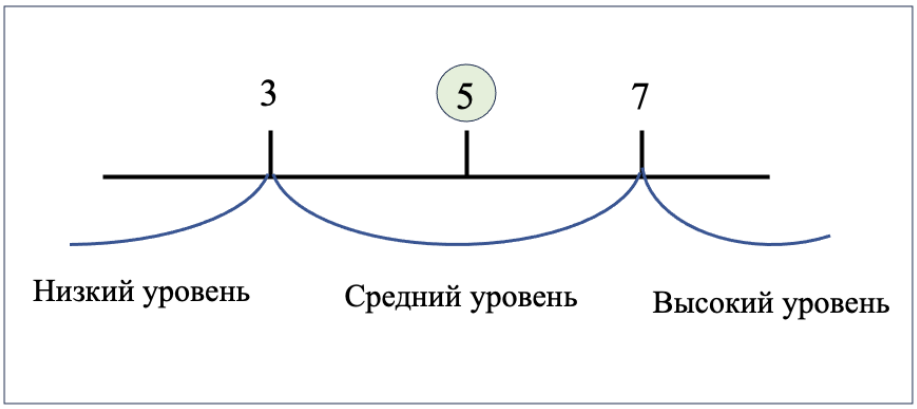

Рисунок 4.1 – Ключ интерпретации теста «Это нормально или опасно?»