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-психолога по формированию основ кибербезопасности у младших школьников

Выпускная квалификационная работа по направлению
44.04.02. Психолого-педагогическое образование

Направленность программы магистратуры
«Психология и педагогика начального образования
и инклюзивного обучения»
Форма обучения очная

Проверка на объем заимствований:
91,62 % авторского текста
Работа рекомендована к защите

«14» мая 2026 г.
зав. кафедрой ТМиМНО
_____ Волчегорская Евгения Юрьевна

Выполнила:
Студентка группы ОФ-221-290-2-1
Ермолаева Вера Владимировна

Научный руководитель:
канд. пед. наук, доцент
_____ Жукова Марина Владимировна

Челябинск
2026

СОДЕРЖАНИЕ

Введение

Актуальность темы исследования обусловлена стремительной цифровизацией образовательного пространства и жизнедеятельности современных детей, что порождает принципиально новые риски для психологического благополучия и безопасности развивающейся личности. Младшие школьники сегодня представляют собой первое поколение, для которого цифровая среда является естественной средой обитания с самого раннего возраста. Однако незрелость когнитивных механизмов, недостаточная сформированность критического мышления и ограниченный социальный опыт делают эту возрастную категорию особенно уязвимой перед многообразием киберугроз.

Проблема кибербезопасности в контексте психолого-педагогического сопровождения младших школьников приобретает статус приоритетной задачи современной образовательной системы. Массовое распространение персональных цифровых устройств, снижение возраста первого контакта ребёнка с интернет-пространством и трансформация коммуникативных практик в сторону виртуализации создают ситуацию, когда традиционные механизмы социального контроля и педагогического влияния оказываются недостаточно эффективными. Педагог-психолог в этих условиях призван выполнять функцию проводника между миром цифровых возможностей и миром психологической безопасности развивающейся личности.

Анализ научной литературы свидетельствует о нарастающем интересе исследователей к проблематике информационной безопасности детства. Вместе с тем следует констатировать фрагментарность существующих разработок и отсутствие целостной системы психолого-педагогического обеспечения кибербезопасности именно на этапе начального общего образования. Большинство превентивных программ ориентировано на подростковый возраст, тогда как сензитивные периоды формирования базовых паттернов цифрового поведения приходятся на

младший школьный возраст. Более того, существующие подходы зачастую носят технократический характер и не учитывают психологические закономерности возрастного развития, специфику познавательных процессов и эмоционально-волевой сферы детей 7–10 лет [12].

Современное состояние изученности проблемы характеризуется наличием отдельных исследований, посвящённых различным аспектам цифровой социализации детей, однако комплексные работы, интегрирующие психологический, педагогический и технологический компоненты применительно к начальной школе, представлены недостаточно. Дискуссионными остаются вопросы определения содержательных границ понятия «кибербезопасность» в детском возрасте, критериев сформированности безопасного цифрового поведения, оптимальных методов диагностики и коррекции. Противоречие между объективной необходимостью систематической работы по формированию основ кибербезопасности у младших школьников и недостаточной разработанностью научно-методического обеспечения деятельности педагога-психолога в данном направлении определяет научную и практическую значимость настоящего исследования [23].

Цель исследования: изучение теоретических аспектов проблемы формирования основ кибербезопасности младших школьников и экспериментальная проверка программы психолого-педагогического сопровождения данного процесса.

Задачи исследования:

1. Проанализировать категориальный аппарат и методологические подходы к проблеме информационной безопасности личности в психолого-педагогической науке.

2. Охарактеризовать психологические особенности младшего школьного возраста как сензитивного периода для формирования цифровой грамотности и безопасного поведения в киберпространстве.

3. Выявить специфику рисков и угроз киберпространства в условиях трансформации «цифрового детства».

4. Осуществить концептуальный анализ существующих стратегий кибербезопасности: SWOT-анализ образовательных практик и актуальные проблемы профилактики.

5. Разработать, реализовать программу психолого-педагогического сопровождения формирования основ кибербезопасности у младших школьников и оценить её результативность.

Объект исследования: кибербезопасное поведение детей младшего школьного возраста.

Предмет исследования: деятельность педагога-психолога по формированию основ кибербезопасности у обучающихся начальной школы.

Методологическая основа исследования:

– субъектно-деятельностный подход, позволивший интерпретировать процесс формирования навыков кибербезопасности как активную внутреннюю работу ребенка по усвоению норм поведения в виртуальном пространстве;

– конструктивный подход, на основе которого мы разработали вариативную программу взаимодействия, ориентированную на поэтапное формирование цифровой грамотности младших школьников;

– комплексный подход, используя который нам удалось интегрировать элементы кибергигиены в повседневную образовательную деятельность и семейное воспитание, обеспечив единство психологического и информационного воздействия.

Гипотеза исследования: формирование основ кибербезопасности у младших школьников будет результативным, если педагог-психолог реализует программу сопровождения, включающую диагностический, профилактический и развивающий компоненты с учётом возрастных

психологических особенностей обучающихся и при активном вовлечении всех субъектов образовательного процесса.

Теоретическая база исследования представлена фундаментальными положениями культурно-исторической концепции развития психики (Л. С. Выготский), деятельностного подхода в психологии и педагогике (А. Н. Леонтьев, С. Л. Рубинштейн), теории психологической безопасности образовательной среды (И. А. Баева), концепции цифровой социализации детей и подростков (Г. У. Солдатова, Е. И. Рассказова), теоретических основ возрастной и педагогической психологии (Д. Б. Эльконин, В. В. Давыдов).

Практическая значимость исследования состоит в возможности использования разработанных диагностических материалов и программы психолого-педагогического сопровождения педагогами-психологами образовательных организаций; в создании методических рекомендаций для педагогов и родителей по профилактике киберугроз и формированию безопасного цифрового поведения младших школьников.

База исследования: наше исследование проходило на базе МБОУ СОШ г. Челябинска. В исследовании принимали участие учащиеся 2–3 классов в количестве 78 человек (38 второклассников и 40 третьеклассников), педагоги образовательной организации в количестве 8 человек, родители учащихся в количестве 72 человека.

Историографическая база представлена трудами отечественных исследователей в области возрастной психологии (Л. И. Божович, Д. И. Фельдштейн), психологии безопасности (Ю. П. Зинченко, А. И. Донцов), медиапсихологии и медиаобразования (А. В. Федоров, И. В. Жилавская), цифровой педагогики (Э. Ф. Зеер, В. И. Блинов).

Нормативно-правовая база исследования: Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ, Федеральный государственный образовательный стандарт начального общего образования (приказ Минпросвещения России от 31.05.2021 № 286),

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, Концепция информационной безопасности детей, Профессиональный стандарт «Педагог-психолог (психолог в сфере образования)».

Этапы исследования:

– на первом этапе (сентябрь – октябрь 2025 г.) нами был проведен анализ научной литературы, систематизация понятийного аппарата и теоретическое обоснование проблемы;

– на втором этапе (ноябрь – декабрь 2025 г.) мы изучили текущее состояние проблемы в конкретной образовательной среде;

– на третьем этапе (январь – март 2026 г.) нами была разработана модель, внедрена программа сопровождения и верификация полученных результатов.

Методы исследования:

˜ теоретические: анализ психолого-педагогической, методической литературы и нормативно-правовых документов по проблеме исследования; синтез и систематизация научных данных; сравнительный анализ концептуальных подходов; моделирование;

˜ эмпирические: анкетирование, тестирование, констатирующий и формирующий педагогический эксперимент;

˜ математические: количественный и качественный анализ эмпирических данных, методы статистической обработки результатов исследования.

Апробация исследования:

– путем публикации результатов исследования:

1. Ермолаева В. В. Психологические особенности восприятия киберугроз детьми младшего школьного возраста / В. В. Ермолаева // Педагогический альманах. – 22.05.26. – URL: https://www.pedalmanac.ru/581749 (дата обращения: 22.05.2026).

2. Ермолаева В. В. Возрастная специфика формирования цифровой безопасности у учащихся начальной школы / В. В. Ермолаева // Молодежный научный форум : электр. сб. ст. по мат. CCCXLV междунар. студ. науч.-практ. конф. № 19 (345). – URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/19(345).pdf (дата обращения: 22.05.2026).

3. Ермолаева В. В. Развитие критического мышления младших школьников как основа кибербезопасности / В. В. Ермолаева // Молодежный научный форум: электр. сб. ст. по мат. CCCXLV междунар. студ. науч.-практ. конф. № 19 (345). URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/19(345).pdf (дата обращения: 22.05.2026).

Структура работы: состоит из введения, двух глав, заключения и списка использованной литературы.

В тексте работы 5 таблиц, 3 рисунка, 3 приложения. Список литературы представлен 42 источниками.

ГЛАВА 1. Теоретико-методологические предпосылки обеспечения кибербезопасности младших школьников в современной России

1.1 Категориальный аппарат исследования информационной безопасности личности в отечественной психолого-педагогической литературе

Концептуализация проблематики информационной безопасности личности в российской психолого-педагогической науке представляет собой относительно молодое, но стремительно развивающееся направление исследований, обусловленное трансформацией социокультурного контекста развития современного ребёнка. Терминологический аппарат данной области характеризуется множественностью подходов и отсутствием единообразия в определении ключевых понятий, что объясняется междисциплинарным характером проблемы и различием методологических оснований исследователей. Базовая категория «информационная безопасность» первоначально сформировалась в технократической парадигме и обозначала защищённость информационных систем от несанкционированного доступа, утечки или разрушения данных. Однако перенос данного понятия в психолого-педагогический дискурс потребовал существенной содержательной трансформации и наполнения антропоцентрическими смыслами [7].

В контексте образования информационная безопасность личности трактуется как состояние защищённости психики человека от деструктивных информационных воздействий, обеспечивающее сохранность базовых ценностных ориентаций, адекватность восприятия и интерпретации информации, способность к критической оценке контента и осознанному выбору стратегий поведения в информационной среде. Г. У. Солдатова и Е. И. Рассказова предлагают рассматривать информационную безопасность детей через призму трёх взаимосвязанных

компонентов: содержательного (безопасность контента, потребляемого ребёнком), коммуникативного (безопасность общения в цифровой среде) и потребительского (безопасность в ситуациях электронной коммерции и использования цифровых сервисов). Такой многоаспектный подход позволяет охватить всё многообразие рисков, с которыми сталкивается развивающаяся личность в процессе освоения цифрового пространства [34].

Понятие «кибербезопасность» в отечественной литературе зачастую используется как синоним информационной безопасности, однако ряд исследователей настаивает на необходимости их разграничения. Кибербезопасность определяется как более узкая категория, относящаяся непосредственно к защите от угроз, исходящих из компьютерных сетей и интернет-пространства. В образовательном контексте кибербезопасность обучающихся включает совокупность мер технического, организационного и педагогического характера, направленных на предотвращение или минимизацию рисков, связанных с использованием сетевых технологий. К таким рискам относятся кибербуллинг, груминг, секстинг, вовлечение в деструктивные сообщества, игровая и интернет-аддикция, мошенничество, нарушение конфиденциальности персональных данных [18].

Категория «цифровая грамотность» занимает центральное место в современном категориальном аппарате, поскольку рассматривается как основа формирования компетенций безопасного поведения в киберпространстве. Вслед за И. А. Баевой можем констатировать, что цифровая грамотность представляет собой интегративное качество личности, включающее технологический, когнитивный, этический и коммуникативный компоненты. Технологический компонент предполагает владение навыками использования цифровых устройств и программного обеспечения. Когнитивный компонент связан со способностью к поиску, критической оценке, анализу и синтезу информации. Этический компонент отражает понимание норм и правил

поведения в цифровой среде, уважение к интеллектуальной собственности и персональным границам других пользователей. Коммуникативный компонент включает умения эффективного и безопасного взаимодействия в виртуальном пространстве [3].

Применительно к младшему школьному возрасту исследователи оперируют понятием «основы кибербезопасности», подчёркивая тем самым начальный, пропедевтический характер формируемых компетенций. Основы кибербезопасности младших школьников определяются как совокупность элементарных знаний о правилах безопасного поведения в интернете, первичных навыков распознавания потенциально опасных ситуаций в цифровой среде, базовых установок на защиту личной информации и обращение за помощью к взрослым в случае столкновения с киберугрозами. Важнейшим аспектом является формирование эмоционального компонента: чувства самосохранения в цифровом пространстве, настороженности по отношению к незнакомцам в сети, ответственности за собственные действия онлайн [28].

Понятие «цифровая социализация» введено в научный оборот для обозначения процесса усвоения индивидом норм, ценностей, паттернов поведения, необходимых для функционирования в качестве члена цифрового общества. Ю. П. Зинченко отмечает двойственный характер цифровой социализации современных детей: с одной стороны, она открывает беспрецедентные возможности для познавательного развития, расширения коммуникативного опыта, самореализации; с другой стороны, содержит риски десоциализации, усвоения деструктивных образцов, формирования зависимого поведения. Младший школьный возраст характеризуется интенсификацией процессов цифровой социализации на фоне недостаточной сформированности механизмов саморегуляции и критического мышления, что актуализирует необходимость целенаправленного психолого-педагогического сопровождения [15].

Термин «киберугрозы» объединяет широкий спектр явлений, различающихся по природе, механизмам воздействия и последствиям для развития личности. В психологической литературе принято разделять киберугрозы на несколько категорий:

- контентные риски, связанные с доступом к неприемлемому или травмирующему контенту;
- коммуникационные риски, возникающие в процессе общения с другими пользователями;
- электронные риски, включающие заражение устройств вредоносным программным обеспечением;
- потребительские риски, связанные с финансовыми потерями и мошенничеством;
- риски нарушения приватности и утечки персональных данных.

Для младших школьников наиболее актуальными являются контентные и коммуникационные риски, поскольку именно в этих сферах проявляется их возрастная уязвимость [22].

Понятие «психологическая безопасность образовательной среды» в контексте цифровизации приобретает новые смысловые оттенки. И. А. Баева определяет психологическую безопасность как состояние среды, свободное от проявлений психологического насилия, способствующее удовлетворению потребностей в личностном развитии и формирующее позитивное отношение к среде. В условиях активного внедрения цифровых технологий в образовательный процесс психологическая безопасность должна обеспечиваться не только в физическом пространстве школы, но и в виртуальной образовательной среде. Это предполагает разработку и соблюдение норм сетевого этикета, предотвращение кибербуллинга, контроль за содержанием используемых цифровых ресурсов, обучение педагогов и родителей навыкам выявления признаков деструктивного влияния интернета на ребёнка [4].

Категория «медиаграмотность» тесно связана с понятием цифровой грамотности, но акцентирует внимание на способности критически воспринимать и анализировать медиатексты, понимать механизмы создания и распространения информации в массмедиа, различать факты и мнения, идентифицировать манипулятивные техники. А. В. Федоров подчёркивает, что медиаграмотность выступает защитным фактором против информационных манипуляций, фейковых новостей, пропаганды деструктивных идеологий. В начальной школе формирование медиаграмотности находится на начальной стадии и включает развитие элементарных представлений о различных типах информации, способах её представления, понимание того, что не всё размещённое в интернете является правдой [38].

Понятие «цифровая компетентность педагога» приобретает особую значимость в контексте обеспечения кибербезопасности обучающихся. В. И. Блинов определяет цифровую компетентность педагога как интегративную характеристику, включающую мотивационный, когнитивный и деятельностный компоненты, обеспечивающие готовность и способность эффективно использовать цифровые технологии в профессиональной деятельности, в том числе для обучения детей безопасному поведению в цифровой среде. Педагог-психолог должен обладать не только общей цифровой компетентностью, но и специфическими компетенциями в области диагностики рисков цифровой среды для психологического развития ребёнка, консультирования родителей и педагогов, разработки и реализации профилактических программ [6].

Термин «цифровое детство» отражает качественные изменения в условиях развития современного поколения детей, для которых цифровые технологии являются неотъемлемой частью повседневной жизни с самого раннего возраста. Г. У. Солдатова использует метафору «цифровые аборигены» для обозначения детей, родившихся в эпоху повсеместного

распространения интернета и мобильных устройств, в противовес «цифровым иммигрантам» – поколению родителей и педагогов, осваивавших технологии уже во взрослом возрасте. Это различие в цифровом опыте создаёт коммуникативный разрыв между поколениями и затрудняет осуществление традиционных форм контроля и воспитания. Педагог-психолог выступает медиатором, способствующим преодолению этого разрыва и выстраиванию конструктивного диалога между взрослыми и детьми относительно норм и правил поведения в цифровой среде [33].

Понятие «киберсоциализация» введено В. А. Плешаковым для обозначения процесса социализации личности в киберпространстве, приводящего к формированию специфической виртуальной идентичности. Исследователь выделяет позитивные и негативные варианты киберсоциализации в зависимости от того, способствует ли она личностному развитию или приводит к деформациям в ценностно-смысловой сфере. Для младшего школьного возраста характерна высокая пластичность и внушаемость, что делает этот период критически важным для формирования конструктивных паттернов киберсоциализации под руководством взрослых [27].

Категория «информационная культура личности» рассматривается как системное образование, интегрирующее знания о закономерностях информационных процессов, умения работы с информацией, ценностное отношение к информации как ресурсу развития, нормы информационного поведения. В контексте обеспечения кибербезопасности информационная культура выступает как внутренний регулятор, определяющий выбор стратегий поведения в ситуациях неопределённости и потенциальной угрозы. Формирование информационной культуры младших школьников предполагает воспитание уважительного отношения к чужой интеллектуальной собственности, понимания недопустимости распространения оскорбительной информации, развития навыков этичной коммуникации [11].

Таким образом, категориальный аппарат исследования информационной безопасности личности в отечественной психолого-педагогической науке представляет собой развивающуюся систему взаимосвязанных понятий, отражающих различные аспекты взаимодействия развивающейся личности с цифровой средой. Центральное место в этой системе занимают понятия кибербезопасности, цифровой грамотности и цифровой социализации, конкретизирующиеся применительно к младшему школьному возрасту через категории основ кибербезопасности и пропедевтики безопасного цифрового поведения. Анализ терминологического аппарата позволяет выделить многокомпонентную структуру феномена информационной безопасности, включающую когнитивный, деятельностный, эмоционально-волевой и ценностно-смысловой компоненты, что задаёт ориентиры для разработки диагностического инструментария и содержания программ психолого-педагогического сопровождения.

1.2 Психологическая характеристика младшего школьного возраста как сензитивного периода для формирования цифровой грамотности

Младший школьный возраст, охватывающий период с 6–7 до 10–11 лет, представляет собой качественно своеобразный этап онтогенеза, характеризующийся кардинальной перестройкой всей системы отношений ребёнка с окружающей действительностью и интенсивным развитием познавательных процессов, эмоционально-волевой сферы и личности в целом. Поступление в школу знаменует переход к новой социальной ситуации развития, в которой учебная деятельность становится ведущей, а система «ребёнок – учитель» приобретает статус центрального отношения, опосредующего все остальные связи ребёнка с миром. В контексте формирования основ кибербезопасности этот возрастной период обладает уникальным сензитивным потенциалом, обусловленным сочетанием

интенсивного когнитивного развития, становления произвольности психических процессов и сохраняющейся открытости к педагогическим воздействиям [9].

Когнитивное развитие младших школьников характеризуется переходом от дооперационального мышления к стадии конкретных операций (по Ж. Пиаже), что проявляется в развитии способности к децентрации, формировании понятий сохранения, обратимости, классификации. Ребёнок постепенно преодолевает эгоцентризм познавательной позиции и начинает учитывать множественные аспекты ситуации, что создаёт предпосылки для понимания сложности информационной среды и многообразия позиций различных коммуникаторов. Вместе с тем мышление остаётся преимущественно конкретным, привязанным к наглядным образам и реальному опыту, что затрудняет осмысление абстрактных угроз и прогнозирование отдалённых последствий действий в цифровом пространстве. Эта особенность требует использования в профилактической работе конкретных примеров, игровых ситуаций, визуализации правил безопасного поведения [14].

Развитие внимания в младшем школьном возрасте идёт по линии формирования произвольности, увеличения объёма, устойчивости и способности к переключению. Если в начале периода доминирует непроизвольное внимание, привлекаемое яркими, эмоционально насыщенными стимулами, то к концу начальной школы ребёнок уже способен к довольно длительной концентрации на учебных задачах, требующих волевого усилия. Специфика цифровой среды, изобилующей яркими, динамичными стимулами, рассчитанными на захват непроизвольного внимания, делает младших школьников особенно уязвимыми перед соблазнами бесконтрольного потребления развлекательного контента. Формирование навыков саморегуляции времени, проводимого в интернете, и осознанного выбора контента требует

специальной педагогической работы, опирающейся на зону ближайшего развития произвольности [26].

Память младшего школьника претерпевает существенную трансформацию: от преобладания механического запоминания к развитию смысловой памяти, от непроизвольного к произвольному запоминанию, от внешних мнемических средств к внутренним. Однако сохраняется высокая эффективность наглядно-образной памяти, что используется в педагогическом процессе при создании памяток, визуальных алгоритмов безопасного поведения. Особенностью памяти в этом возрасте является склонность к буквальному запоминанию без глубокого осмысления, что может приводить к формальному усвоению правил кибербезопасности без понимания их смысла. Педагог-психолог должен обеспечивать активную мыслительную переработку информации, связывание новых знаний с личным опытом ребёнка [19].

Развитие речи и мышления в младшем школьном возрасте тесно взаимосвязаны. Ребёнок овладевает письменной речью, расширяется словарный запас, совершенствуется грамматический строй. Особое значение приобретает развитие коммуникативной функции речи, умения выстраивать диалог, аргументировать свою позицию. В контексте кибербезопасности критически важным является формирование навыков безопасной коммуникации: понимания различий между реальным и виртуальным общением, осознания того, что за аватаром может скрываться кто угодно, развития осторожности в раскрытии личной информации. Младшие школьники характеризуются доверчивостью и склонностью воспринимать слова буквально, что делает их лёгкой мишенью для манипуляций со стороны злоумышленников [31].

Эмоциональная сфера младшего школьника отличается повышенной впечатлительностью, импульсивностью реагирования, недостаточной дифференцированностью эмоциональных состояний. Ребёнок ещё не всегда способен адекватно распознавать собственные эмоции и управлять ими, что

создаёт риски импульсивных действий в цифровой среде под влиянием сиюминутных эмоций. Вместе с тем именно в этот период закладываются основы эмоционального интеллекта, эмпатии, способности к рефлексии чувств. Формирование эмоционального компонента кибербезопасности предполагает развитие умения распознавать собственные эмоциональные реакции на различный контент, понимать, что определённые материалы могут вызывать дискомфорт, страх, тревогу, и в этом случае необходимо прекратить просмотр и обратиться к взрослому [8].

Социальная ситуация развития младшего школьника характеризуется расширением круга социальных контактов, выходом за пределы семьи, возрастанием значимости оценки сверстников и учителя. Формируется учебная самооценка, которая в значительной степени определяется внешними оценками со стороны значимых взрослых. Младшие школьники чувствительны к похвале и критике, стремятся соответствовать ожиданиям взрослых, что создаёт благоприятные условия для формирования социально одобряемых паттернов поведения, в том числе в цифровой среде. Важно использовать этот период для закрепления норм сетевого этикета, культуры коммуникации, уважительного отношения к другим пользователям. Вместе с тем возрастает риск кибербуллинга, поскольку дети начинают активнее взаимодействовать со сверстниками онлайн, но ещё не обладают достаточными навыками конструктивного разрешения конфликтов [21].

Развитие личности в младшем школьном возрасте связано с формированием внутренней позиции школьника, развитием мотивационной сферы, становлением самосознания. Ведущими мотивами деятельности становятся познавательные и социальные мотивы. Ребёнок стремится познавать новое, получать знания, осваивать новые виды деятельности. Это естественное любопытство может быть как ресурсом – двигателем освоения цифрового пространства и развития цифровой грамотности, – так и фактором риска, поскольку может приводить к посещению опасных сайтов, переходу по подозрительным ссылкам. Задача педагога-психолога –

направить познавательную активность в конструктивное русло, научить различать легитимные и потенциально опасные источники информации [17].

Формирование произвольности поведения – центральное новообразование младшего школьного возраста, определяющее возможность целенаправленной регуляции своих действий в соответствии с заданными правилами и нормами. Произвольность формируется в процессе учебной деятельности и постепенно распространяется на другие сферы жизни ребёнка. В контексте кибербезопасности развитие произвольности является ключевым условием способности следовать правилам безопасного поведения в ситуациях, когда непосредственный контроль взрослых отсутствует. Младшие школьники находятся в процессе становления произвольности, поэтому нуждаются во внешней поддержке – напоминаниях, визуальных подсказках, структурировании цифровой среды с помощью технических средств родительского контроля [29].

Особенности морального развития младших школьников характеризуются переходом от конвенциональной морали послушания к морали взаимности и сотрудничества (по Л. Кольбергу). Ребёнок начинает понимать, что правила существуют не произвольно, а имеют смысл для благополучия людей, учится учитывать намерения и обстоятельства при оценке поступков. Вместе с тем моральные суждения ещё достаточно ригидны, мышление категорично («хорошо – плохо»). Это создаёт основу для формирования чётких нравственных ориентиров в цифровой среде: понимания недопустимости оскорблений, распространения личной информации других людей без разрешения, использования чужих паролей. Педагог-психолог должен формировать не только знание правил, но и эмоциональное отношение к их нарушению – чувство вины, стыда, эмпатию к потенциальным жертвам кибербуллинга [24].

Идентичность младшего школьника находится в процессе становления. Ребёнок начинает осознавать себя как ученика, члена

классного коллектива, носителя определённых качеств и способностей. Цифровая среда предоставляет новые возможности для экспериментирования с идентичностью через создание профилей, аватаров, участие в онлайн-играх с принятием различных ролей. С одной стороны, это может способствовать самопознанию и развитию креативности. С другой стороны, размывание границ между реальной и виртуальной идентичностью, чрезмерное погружение в фантазийный мир онлайн-игр может препятствовать формированию целостной, интегрированной идентичности. Психолого-педагогическое сопровождение должно помогать ребёнку осмыслять свой опыт в цифровой среде, связывать его с реальной жизнью [36].

Физиологические особенности младших школьников также имеют значение для обеспечения их безопасности в цифровой среде. Зрительная система ещё продолжает развиваться, длительная работа с экранами может приводить к утомлению, ухудшению зрения. Нервная система характеризуется высокой пластичностью, но и повышенной утомляемостью. Младшие школьники нуждаются в регулярной смене видов деятельности, физической активности, полноценном сне. Чрезмерное увлечение гаджетами может приводить к нарушению режима дня, дефициту движения, проблемам со здоровьем. Педагог-психолог должен просвещать родителей и самих детей относительно гигиенических норм использования цифровых устройств, формировать установку на здоровьесберегающее поведение [13].

Таким образом, младший школьный возраст представляет собой сензитивный период для формирования основ кибербезопасности благодаря сочетанию нескольких факторов: интенсивному когнитивному развитию, создающему предпосылки для понимания сложных социальных ситуаций; становлению произвольности, обеспечивающему возможность саморегуляции поведения; высокой восприимчивости к педагогическим воздействиям и стремлению соответствовать социальным ожиданиям;

началу активного освоения цифрового пространства. Вместе с тем возрастные особенности – конкретность мышления, импульсивность, доверчивость, недостаточная сформированность критического мышления – создают специфические риски и требуют адаптации содержания и методов профилактической работы к возможностям данного возраста. Эффективное формирование основ кибербезопасности возможно лишь при глубоком понимании психологических закономерностей развития младшего школьника и опоре на зону ближайшего развития каждого компонента цифровой грамотности.

1.3 Специфика рисков и угроз киберпространства в условиях трансформации «цифрового детства»

Трансформация социокультурного контекста развития современных детей, определяемая тотальной цифровизацией всех сфер жизни, порождает принципиально новую конфигурацию рисков и угроз, качественно отличающихся от традиционных опасностей физического мира. Киберпространство характеризуется специфическими свойствами – анонимностью, глобальностью, интерактивностью, мультимедийностью, – которые создают как уникальные возможности для развития, так и многообразие потенциальных угроз для психологического благополучия и безопасности детей. Феномен «цифрового детства» отражает качественное изменение условий онтогенеза: современные дети с первых лет жизни погружены в медианасыщенную среду, для них виртуальная реальность является таким же естественным пространством существования, как и физическая [5].

Контентные риски представляют собой одну из наиболее распространённых категорий угроз для младших школьников и связаны с доступом к материалам, не соответствующим возрасту или наносящим вред психологическому развитию. К контентным рискам относятся:

– материалы сексуального характера, способные нарушить нормальное психосексуальное развитие, сформировать искажённые представления о гендерных отношениях;

– сцены насилия, жестокости, агрессии, просмотр которых может приводить к десенсибилизации, снижению эмпатии, усвоению агрессивных паттернов поведения;

– контент, пропагандирующий деструктивные идеологии, экстремизм, терроризм, способный к радикализации сознания;

– информация, побуждающая к опасному поведению (зацепинг, руфинг, участие в деструктивных играх);

– материалы, связанные с употреблением психоактивных веществ, культивирующие саморазрушающее поведение;

– контент, пропагандирующий расстройства пищевого поведения, членовредительство, суицид [30].

Особенностью контентных рисков в современном киберпространстве является их повсеместность и лёгкость доступа. Даже при использовании детских поисковых систем и образовательных платформ алгоритмы рекомендаций могут выводить ребёнка на нежелательный контент. Младшие школьники в силу возрастных особенностей не всегда способны адекватно оценить опасность материала, могут продолжать просмотр из любопытства, испытывать страх, но не обратиться к взрослым из-за боязни наказания или запрета на использование интернета. Психологическое воздействие травмирующего контента может быть отсроченным и проявляться в виде ночных кошмаров, повышенной тревожности, навязчивых мыслей, изменения поведения [16].

Коммуникационные риски возникают в процессе общения ребёнка с другими пользователями в социальных сетях, мессенджерах, онлайн-играх, чатах. Наиболее серьёзными коммуникационными угрозами для младших школьников являются:

– кибербуллинг (травля в цифровой среде) – систематические агрессивные действия со стороны сверстников или старших детей, включающие оскорбления, угрозы, распространение компрометирующей информации, социальную изоляцию;

– груминг – установление доверительных отношений взрослым злоумышленником с ребёнком с целью последующей сексуальной эксплуатации;

– киберпреследование – навязчивое внимание, слежка за активностью ребёнка в сети;

– вовлечение в деструктивные сообщества, секты, группы, пропагандирующие опасные идеи;

– социальная инженерия – манипулятивные техники, направленные на выманивание личной информации, паролей, денежных средств [25].

Младшие школьники особенно уязвимы перед коммуникационными рисками в силу свойственной возрасту доверчивости, стремления к признанию и принятию, недостаточного опыта распознавания манипуляций. Кибербуллинг может иметь разрушительные последствия для самооценки, эмоционального благополучия, академической успеваемости ребёнка. Груминг представляет чрезвычайную опасность, поскольку злоумышленники используют знание детской психологии, завоевывают доверие ребёнка, эксплуатируют потребность во внимании, постепенно втягивают в опасную ситуацию. Анонимность цифровой среды облегчает осуществление манипуляций, поскольку взрослый может выдавать себя за сверстника ребёнка [32].

Потребительские риски связаны с использованием младшими школьниками электронных сервисов, онлайн-покупок, игр с внутриигровыми покупками. К этой категории относятся:

– финансовое мошенничество, фишинг – получение доступа к банковским картам родителей, личным данным через обманные сайты;

– скрытые платежи в «бесплатных» играх и приложениях;

– навязывание ненужных покупок через агрессивную рекламу и манипулятивные техники;

– азартные игры онлайн, формирующие зависимое поведение;

– нарушение прав потребителей при онлайн-покупках [20].

Младшие школьники, как правило, не имеют собственных денежных средств и совершают покупки с помощью карт родителей. Однако они могут не понимать реальной стоимости виртуальных товаров, совершать импульсивные покупки под воздействием рекламы или желания не отстать от сверстников в игре. Случаи, когда дети тратят значительные суммы на внутриигровые покупки, не осознавая последствий, достаточно распространены. Формирование критического отношения к рекламе, понимания коммерческих интересов создателей контента, навыков рационального потребительского поведения является важной составляющей профилактической работы [37].

Технические риски включают угрозы, связанные с вредоносным программным обеспечением, утечкой персональных данных, взломом аккаунтов. Младшие школьники могут случайно загрузить вирусы, перейдя по подозрительным ссылкам, открыв вложения в письмах от незнакомцев. Использование слабых паролей, передача паролей друзьям, вход в аккаунты с чужих устройств создают риски несанкционированного доступа к личной информации. Последствия могут включать потерю данных, компрометацию аккаунта, его использование злоумышленниками для распространения спама или мошенничества [10].

Риски, связанные с нарушением приватности, приобретают особую актуальность в эпоху социальных сетей и повсеместного обмена информацией. Младшие школьники могут не понимать различия между публичным и приватным, легкомысленно делиться личной информацией – фотографиями, данными о месте жительства, учёбы, распорядке дня, отсутствии родителей дома. Эта информация может быть использована

злоумышленниками для различных целей – от таргетированной рекламы до реальных преступлений. Размещение фотографий детей родителями в социальных сетях без учёта настроек приватности также создаёт риски. Формирование культуры приватности, понимания ценности личной информации и необходимости её защиты является важным направлением работы педагога-психолога [35].

Психологические риски связаны с влиянием чрезмерного или неконтролируемого использования цифровых технологий на психическое здоровье и развитие ребёнка:

– формирование интернет-зависимости, компьютерной игровой зависимости;

– дефицит реального общения, социальная изоляция;

– нарушения сна, связанные с использованием гаджетов перед сном и ночью;

– синдром дефицита внимания, клиповое мышление, снижение способности к глубокому чтению и концентрации;

– тревожность, депрессивные состояния, связанные с социальным сравнением в социальных сетях;

– размывание границ между реальностью и виртуальностью;

– обеднение эмоциональной сферы, снижение эмпатии [39].

Младший школьный возраст является критическим для формирования саморегуляции и произвольности, развития навыков социального взаимодействия. Чрезмерное погружение в цифровую среду может препятствовать развитию этих ключевых компетенций. Замещение реальной игры и общения виртуальными активностями лишает ребёнка важного опыта социального научения, развития коммуникативных навыков, эмоционального интеллекта. Педагог-психолог должен проводить диагностику признаков формирующейся зависимости, консультировать родителей относительно здорового баланса между цифровой и офлайн-активностями ребёнка [2].

Специфика современных киберугроз усугубляется рядом факторов. Во-первых, скорость технологических изменений опережает возможности адаптации образовательной системы и родительской компетентности. Появляются новые платформы, приложения, форматы взаимодействия, которые взрослые не успевают освоить и понять. Во-вторых, алгоритмическая персонализация контента создаёт «пузыри фильтров», когда ребёнок получает рекомендации на основе предыдущего просмотра, что может приводить к погружению в деструктивный контент. В-третьих, геймификация и использование механизмов поведенческой психологии создателями контента делают цифровые продукты чрезвычайно привлекательными и вызывающими зависимость [40].

Таким образом, спектр рисков и угроз киберпространства для младших школьников чрезвычайно широк и постоянно эволюционирует вместе с развитием технологий. Эффективная профилактика требует комплексного подхода, включающего повышение цифровой грамотности детей, развитие навыков критического мышления и саморегуляции, просвещение родителей и педагогов, создание безопасной цифровой образовательной среды, техническую защиту. Педагог-психолог выполняет координирующую роль в системе обеспечения кибербезопасности, объединяя усилия всех участников образовательного процесса и адаптируя профилактические стратегии к постоянно меняющемуся цифровому ландшафту детства.

Выводы по главе 1

Таким образом, анализ существующих стратегий кибербезопасности и образовательных практик свидетельствует о необходимости интегративного подхода, сочетающего элементы различных стратегий с приоритетом психолого-педагогического направления. Оптимальная модель должна включать технологическую защиту как базовый уровень,

информационно-просветительскую работу с учётом возрастных особенностей, систематическое психолого-педагогическое сопровождение, направленное на развитие личности ребёнка, формирование внутренних регуляторов поведения, критического мышления, навыков саморегуляции. Особая роль в реализации такой модели принадлежит педагогу-психологу, способному координировать усилия всех субъектов образовательного процесса и обеспечивать индивидуализированный подход к каждому ребёнку с учётом его психологических особенностей и уровня развития цифровых компетенций.

ГЛАВА 2. Методика организации экспериментальной работы

2.1 Концептуальный анализ существующих стратегий кибербезопасности: SWOT-анализ образовательных практик и актуальные проблемы профилактики

Анализ существующих подходов к обеспечению кибербезопасности детей и подростков в образовательной среде выявляет многообразие концептуальных оснований, методологических стратегий и практических решений, различающихся по степени эффективности, системности и адаптированности к возрастным особенностям обучающихся. В российской практике можно выделить несколько доминирующих стратегических направлений: запретительно-ограничительное, информационно-просветительское, технологическое и психолого-педагогическое. Каждое из этих направлений обладает определёнными сильными и слабыми сторонами, возможностями и угрозами, что требует критического осмысления и поиска оптимальной модели интеграции различных подходов [1].

Запретительно-ограничительная стратегия базируется на идее максимального ограничения доступа детей к интернету или жёсткого контроля их цифровой активности. Сторонники данного подхода исходят из представления о киберпространстве как пространстве угроз, от которых ребёнка необходимо изолировать. Практические воплощения включают полный запрет на использование гаджетов до определённого возраста, жёсткое лимитирование времени в сети, тотальный контроль посещаемых сайтов и контактов. Сильной стороной подхода является реальное снижение вероятности столкновения ребёнка с киберугрозами в краткосрочной перспективе. Однако слабые стороны существенно перевешивают преимущества: формируется цифровая неграмотность, ребёнок не получает опыта самостоятельной навигации в цифровой среде, развивается

стремление обойти запреты, нарушаются доверительные отношения с родителями [11].

В условиях современной школы, активно внедряющей цифровые технологии в образовательный процесс, запретительная стратегия оказывается нереализуемой. Более того, она вступает в противоречие с задачами развития цифровой компетентности обучающихся, которая является одним из требований ФГОС. Угрозой данного подхода является формирование у детей ощущения беспомощности перед цифровыми вызовами, неспособности критически оценивать информацию и защищать себя самостоятельно. При ослаблении внешнего контроля (например, при переходе в подростковый возраст) такие дети оказываются особенно уязвимыми [23].

Информационно-просветительская стратегия фокусируется на предоставлении детям, родителям и педагогам знаний о киберугрозах и правилах безопасного поведения в интернете. Практические формы реализации включают уроки информационной безопасности, классные часы, родительские собрания, распространение памяток и буклетов, проведение тематических акций (например, «Неделя безопасного интернета»). Сильными сторонами данного подхода являются массовость охвата, относительная простота реализации, повышение осведомлённости о существующих рисках. Информационно-просветительские мероприятия формируют общее представление о проблеме и привлекают внимание к теме кибербезопасности [18].

Слабые стороны информационно-просветительской стратегии связаны с разрывом между знанием правил и их реальным применением в поведении. Младшие школьники могут формально усвоить информацию, но не применять её в практических ситуациях в силу импульсивности, недостаточной сформированности произвольности, особенностей ситуации. Кроме того, просветительские мероприятия зачастую носят эпизодический характер, не обеспечивают систематичности и преемственности.

Возможностью развития данного подхода является интеграция тематики кибербезопасности в содержание различных учебных предметов, создание системы непрерывного образования по цифровой грамотности на всех ступенях обучения. Угрозой является формальный подход к проведению мероприятий без учёта возрастных особенностей, использование неактуальной информации, запугивание детей без предоставления конструктивных стратегий защиты [26].

Технологическая стратегия опирается на использование программных и технических средств для обеспечения безопасности детей в цифровой среде. К таким средствам относятся:

– системы контент-фильтрации, блокирующие доступ к нежелательным сайтам;

– программы родительского контроля, позволяющие отслеживать активность ребёнка в интернете;

– антивирусное программное обеспечение;

– безопасные поисковые системы и браузеры для детей;

– образовательные платформы с проверенным контентом [29].

Сильными сторонами технологического подхода являются реальная эффективность в предотвращении доступа к опасному контенту, автоматизация контроля, возможность настройки индивидуальных параметров безопасности. В образовательных организациях обязательно должна быть установлена система контент-фильтрации в соответствии с требованиями законодательства. Слабые стороны связаны с тем, что технические средства не являются абсолютно надёжными: фильтры могут блокировать безопасный контент или, наоборот, пропускать нежелательный; дети, особенно по мере взросления, находят способы обходить ограничения; технологии не работают за пределами контролируемой среды (например, когда ребёнок использует гаджет друга). Возможностью является постоянное совершенствование технологий искусственного интеллекта для более точной идентификации опасного

контента. Угрозой выступает иллюзия безопасности, когда родители и педагоги, установив технические средства защиты, прекращают педагогическую работу по формированию навыков безопасного поведения [34].

Психолого-педагогическая стратегия рассматривает обеспечение кибербезопасности как комплексную задачу развития личности ребёнка, формирования критического мышления, навыков саморегуляции, ценностных ориентаций, медиаграмотности. Данный подход предполагает систематическую работу по развитию компетенций безопасного поведения в цифровой среде с учётом возрастных и индивидуальных особенностей обучающихся, создание психологически безопасной образовательной среды, профилактику кибербуллинга, работу с родителями. Сильными сторонами психолого-педагогической стратегии являются фундаментальность, направленность на развитие внутренних регуляторов поведения, формирование устойчивых паттернов безопасного цифрового поведения, которые будут актуальны на протяжении всей жизни в условиях меняющихся технологий [7].

Слабые стороны психолого-педагогического подхода связаны с ресурсоёмкостью: требуется высокая квалификация специалистов, систематическая работа, индивидуальный подход, что не всегда реализуемо в условиях дефицита педагогов-психологов в образовательных организациях. Эффект психолого-педагогического воздействия является отсроченным, что затрудняет оценку эффективности. Возможности развития данной стратегии связаны с повышением статуса психологической службы в образовании, разработкой научно обоснованных программ формирования основ кибербезопасности для различных возрастов, подготовкой педагогов-психологов в области медиапсихологии и цифровой безопасности детства. Угрозой является формализация психолого-педагогической работы, замена содержательной деятельности отчётностью [15].

SWOT-анализ образовательных практик обеспечения кибербезопасности в российских школах выявляет следующую картину. К сильным сторонам (Strengths) существующих практик можно отнести:

– наличие нормативно-правовой базы, обязывающей образовательные организации обеспечивать информационную безопасность;

– внедрение систем контент-фильтрации в школах;

– проведение тематических уроков и акций по безопасному интернету;

– повышение внимания к проблеме со стороны педагогического сообщества и родительской общественности;

– наличие методических разработок и программ по формированию цифровой грамотности [22].

К слабым сторонам (Weaknesses) следует отнести:

– фрагментарность и бессистемность профилактической работы;

– недостаточную подготовку педагогов в области обеспечения кибербезопасности;

– дефицит педагогов-психологов и их перегруженность;

– отсутствие преемственности в работе по формированию основ кибербезопасности на разных ступенях образования;

– слабую вовлечённость родителей и их недостаточную цифровую компетентность;

– формальный подход к проведению профилактических мероприятий;

– отсутствие системы диагностики уровня сформированности компетенций безопасного цифрового поведения;

– недостаточность материально-технических и методических ресурсов [31].

Возможности (Opportunities) развития образовательных практик включают:

- включение цифровой грамотности и кибербезопасности в содержание ФГОС всех уровней образования;
- развитие системы повышения квалификации педагогов и педагогов-психологов в области медиапедагогики;
- создание банка лучших практик и методических разработок;
- развитие межведомственного взаимодействия (образование, здравоохранение, правоохранительные органы, IT-сектор);
- использование потенциала социальных партнёров (IT-компаний, общественных организаций);
- вовлечение самих школьников в разработку правил безопасного поведения, создание системы детского самоуправления в цифровой среде школы;
- использование потенциала цифровых технологий для профилактики (интерактивные образовательные игры, симуляторы безопасного поведения) [37].

Угрозы (Threats) связаны:

- с динамичностью развития технологий, появлением новых форм киберугроз, к которым система образования не успевает адаптироваться;
- снижением возраста первого доступа детей к интернету;
- разрывом цифровой компетентности между поколениями;
- коммерциализацией детского интернета, агрессивными маркетинговыми стратегиями, направленными на детей;
- недостаточным контролем контента, создаваемого пользователями;
- возможным сокращением финансирования психологических служб в образовании;
- формализацией работы по обеспечению безопасности [40].

Актуальные проблемы профилактики кибербуллинга в начальной школе заслуживают особого внимания. Исследования показывают, что кибербуллинг «молодеет»: если ранее он был характерен для подросткового

возраста, то сегодня случаи травли в цифровой среде фиксируются и среди младших школьников. Проблема усугубляется тем, что взрослые зачастую не воспринимают конфликты детей в интернете как серьёзную угрозу, недооценивают их психологическое воздействие. Младшие школьники, столкнувшиеся с кибербуллингом, могут не сообщать об этом взрослым из-за страха, стыда, непонимания происходящего. Необходима систематическая работа по формированию навыков конструктивного общения онлайн, эмпатии, умения обращаться за помощью, а также по созданию атмосферы нетерпимости к любым формам травли в школьном сообществе [12].

Проблема цифрового разрыва между поколениями создаёт ситуацию, когда взрослые оказываются менее компетентными в цифровой среде, чем дети, что подрывает их авторитет и затрудняет осуществление контроля и воспитания. Родители и педагоги нуждаются в повышении собственной цифровой грамотности, освоении тех платформ и сервисов, которыми пользуются дети, понимании их цифровой культуры. Вместе с тем важно не впадать в другую крайность – тотальную слежку за ребёнком в сети, нарушающую его личные границы и подрывающую доверие. Задача состоит в выстраивании баланса между контролем и доверием, обучением самостоятельности и предоставлением поддержки [24].

Проблема недостаточной систематичности и преемственности профилактической работы проявляется в том, что мероприятия по кибербезопасности проводятся эпизодически, часто приурочиваются к каким-либо датам или инициируются в ответ на ЧП. Отсутствует единая концепция непрерывного образования по цифровой грамотности и безопасности, начиная с дошкольного возраста. Программы для начальной школы слабо учитывают то, что было сформировано на предыдущей ступени, и не готовят к переходу на следующую. Необходима разработка целостной системы формирования компетенций безопасного цифрового поведения на всех этапах образования [35].

2.2 Моделирование системы формирования основ кибербезопасности в образовательной среде

Проектирование целостной системы формирования основ кибербезопасности в условиях начальной школы требует структурирования разнородных компонентов образовательной среды, определения логики их взаимодействия и механизмов координации деятельности всех субъектов образовательного процесса. Моделирование как метод научного познания позволяет выделить существенные связи и отношения, создать теоретический конструкт, обладающий объяснительной и прогностической функциями, а также служащий основой для практической реализации. Разработанная нами структурно-функциональная модель системы формирования основ кибербезопасности младших школьников (рисунок 1) базируется на системном, деятельностном и личностно-ориентированном подходах и включает целевой, содержательный, организационно-деятельностный, субъектный и оценочно-результативный компоненты [5].

Целевой компонент модели определяет стратегическую направленность всей системы и конкретизируется через иерархию целей различного уровня. Генеральной целью является формирование основ кибербезопасного поведения младших школьников как интегративного личностного качества, обеспечивающего способность к безопасной, этичной и конструктивной деятельности в цифровой среде. Данная генеральная цель декомпозируется на ряд частных целей:

- формирование системы знаний о правилах безопасного поведения в интернете, типичных киберугрозах и способах защиты от них;
- развитие умений распознавания потенциально опасных ситуаций в цифровой среде и применения адекватных стратегий реагирования;
- воспитание ценностного отношения к собственной безопасности и безопасности других пользователей, формирование установок на этичное поведение в киберпространстве;

- развитие навыков саморегуляции цифровой активности, рефлексии собственного цифрового поведения;
- формирование мотивации к обращению за помощью к взрослым в случае столкновения с киберугрозами [16].

Целеполагание в системе формирования основ кибербезопасности должно осуществляться с учётом возрастных возможностей младших школьников и зоны их ближайшего развития. На начальном этапе (1–2 класс) акцент делается на формировании элементарных представлений о правилах, развитии настороженности, привычки советоваться со взрослыми. На последующих этапах (3–4 класс) возрастает доля самостоятельности, развивается способность к критической оценке информации, принятию решений в типичных ситуациях.

Содержательный компонент модели определяет, что именно должно быть сформировано у младших школьников в области кибербезопасности. Содержание структурируется в соответствии с компонентами цифровой грамотности и включает когнитивный, деятельностный, мотивационно-ценностный и рефлексивный блоки. Когнитивный блок охватывает систему знаний о:

- типах контента и способах его создания;
- правилах безопасного поиска информации;
- устройстве и функционировании основных цифровых технологий, используемых детьми (планшеты, компьютеры, интернет, социальные сети);
- понятии персональных данных и необходимости их защиты;
- видах киберугроз (кибербуллинг, груминг, мошенничество, вредоносные программы);
- правилах безопасной коммуникации онлайн;
- этических нормах поведения в цифровой среде;
- последствиях нарушения правил безопасности [28].

Деятельностный блок включает систему умений и навыков:

- безопасного использования поисковых систем;
- создания и хранения надёжных паролей;
- настройки параметров приватности в социальных сетях и играх;

- распознавания подозрительных сообщений, ссылок, писем;
- корректного реагирования на кибербуллинг (не отвечать агрессией, заблокировать обидчика, сообщить взрослым);
- обращения за помощью к взрослым в случае столкновения с киберугрозой;
- критической оценки достоверности информации;
- этичной коммуникации в цифровой среде;
- саморегуляции времени, проводимого в интернете [19].

Мотивационно-ценностный блок направлен на формирование:

- ценностного отношения к собственной безопасности и здоровью;
- установки на соблюдение правил безопасного поведения в интернете;
- уважительного отношения к другим пользователям, эмпатии;
- нетерпимости к кибербуллингу, готовности защищать жертв;
- понимания ценности реального общения и офлайн-активностей;
- мотивации к использованию интернета для обучения и развития, а не только для развлечений [32].

Рефлексивный блок предполагает развитие:

- способности к осознанию собственного цифрового поведения;
- умения оценивать свои эмоциональные реакции на различный контент;
- навыков анализа последствий своих действий в цифровой среде;
- критического отношения к собственным цифровым привычкам [21].

Организационно-деятельностный компонент модели определяет формы, методы, средства и этапы реализации системы формирования основ кибербезопасности. Процесс формирования носит поэтапный характер и включает:

- диагностический этап (выявление исходного уровня цифровой грамотности и информационной культуры младших школьников, их родителей и педагогов);

- проектировочный этап (разработка программы психолого-педагогического сопровождения с учётом результатов диагностики и особенностей образовательной организации);
- реализационный этап (внедрение программы, включающей работу с обучающимися, родителями, педагогами);
- оценочно-коррекционный этап (оценка результативности, внесение корректив, разработка рекомендаций для дальнейшей работы) [36].

Формы работы дифференцируются по субъектам:

- с обучающимися: групповые развивающие занятия, психологические тренинги, деловые игры, квесты, проектная деятельность, индивидуальное консультирование детей группы риска;
- с родителями: родительские собрания, семинары-практикумы, индивидуальное консультирование, разработка информационных материалов (памяток, буклетов);
- с педагогами: методические семинары, супервизия, разработка методических рекомендаций по интеграции тематики кибербезопасности в содержание уроков и внеурочной деятельности [8].

Методы работы включают:

- интерактивные методы (дискуссии, ролевые игры, драматизация);
- метод кейсов (анализ конкретных ситуаций);
- метод проектов (создание правил безопасного класса, плакатов, памяток);
- арт-терапевтические методы (рисование правил, создание коллажей);
- игровые методы (дидактические игры, компьютерные образовательные игры-симуляторы);
- психогимнастика, релаксация (для профилактики негативных эмоциональных состояний, связанных с цифровой активностью);
- тестирование и анкетирование (диагностические методы) [27].

Средства включают:

- мультимедийные презентации;

- видеоролики и мультфильмы по тематике кибербезопасности;
- интерактивные образовательные платформы и игры;
- рабочие тетради и пособия для младших школьников;
- диагностические методики;
- визуальные средства (плакаты, памятки, пиктограммы) [14].

Субъектный компонент модели отражает многосубъектный характер системы формирования основ кибербезопасности и определяет роли и функции каждого участника. Центральная координирующая роль принадлежит педагогу-психологу, который:

- проводит диагностику уровня цифровой грамотности и информационной культуры обучающихся;
- разрабатывает и реализует программу психолого-педагогического сопровождения;
- консультирует родителей и педагогов по вопросам кибербезопасности;
- осуществляет индивидуальную работу с детьми группы риска;
- координирует деятельность всех субъектов образовательного процесса по обеспечению кибербезопасности;
- проводит мониторинг эффективности системы [37].

Классный руководитель:

- интегрирует тематику кибербезопасности в содержание классных часов и внеурочной деятельности;
- организует просветительскую работу с родителями;
- осуществляет наблюдение за поведением обучающихся, выявляет признаки столкновения с киберугрозами;
- взаимодействует с педагогом-психологом при выявлении проблемных ситуаций [11].

Учителя-предметники:

- интегрируют элементы медиаобразования и формирования информационной культуры в содержание преподаваемых дисциплин;

- используют возможности уроков информатики для формирования технических навыков безопасной работы в интернете;
- на уроках литературного чтения, окружающего мира формируют критическое мышление, навыки анализа информации [23].

Родители:

- осуществляют контроль за цифровой активностью ребёнка в домашних условиях;
- используют технические средства родительского контроля;
- обсуждают с ребёнком его опыт в цифровой среде, интересуются, во что он играет, с кем общается;
- собственным примером демонстрируют культуру цифрового поведения;
- обращаются к педагогу-психологу при возникновении проблемных ситуаций [30].

Сами младшие школьники выступают не только объектами психолого-педагогического воздействия, но и активными субъектами, способными участвовать в создании правил безопасного поведения в цифровой среде класса, обучать друг друга, создавать информационные продукты (плакаты, памятки), рефлексировать свой опыт [38].

Оценочно-результативный компонент модели определяет критерии, показатели и методы оценки сформированности основ кибербезопасности у младших школьников. Мы выделяем три уровня сформированности: высокий, средний, низкий, – которые оцениваются по каждому из компонентов (когнитивному, деятельностному, мотивационно-ценностному, рефлексивному), что можно видеть в таблице 1.

Таблица 1 – Критерии и показатели сформированности основ кибербезопасности у младших школьников

Компонент	Критерии	Показатели высокого уровня	Показатели среднего уровня	Показатели низкого уровня
Когнитивный	Полнота и системность	Знает и может объяснить	Знает основные	Знания фрагментарны,

Компонент	Критерии	Показатели высокого уровня	Показатели среднего уровня	Показатели низкого уровня
	знаний о правилах кибербезопасности	правила, приводит примеры	правила, затрудняется с примерами	не может объяснить
Деятельностный	Владение навыками безопасного цифрового поведения	Самостоятельно применяет навыки в различных ситуациях	Применяет навыки с напоминанием или в знакомых ситуациях	Не применяет навыки даже с помощью взрослого
Мотивационно-ценностный	Ценностное отношение к безопасности, установки на этичное поведение	Устойчивая мотивация к безопасному поведению, эмпатия	Ситуативная мотивация, не всегда проявляет эмпатию	Отсутствие мотивации, эгоцентрическая позиция
Рефлексивный	Способность к осознанию и анализу собственного цифрового поведения	Самостоятельно анализирует свои действия, делает выводы	Анализирует с помощью взрослого, выводы поверхностные	Не способен к рефлексии цифрового поведения

Методы оценки включают:

- анкетирование обучающихся для выявления уровня знаний и установок;
- наблюдение за поведением в ситуациях использования цифровых устройств;
- анализ продуктов деятельности (выполнение практических заданий по безопасному поиску информации, созданию паролей);
- беседы для оценки понимания правил и способности к рефлексии;
- кейс-метод (предъявление описаний проблемных ситуаций и анализ выбранных стратегий реагирования);
- анкетирование родителей для оценки изменений в поведении ребёнка дома [40].

Принципами функционирования системы формирования основ кибербезопасности являются:

- принцип систематичности и последовательности (регулярная, а не эпизодическая работа, постепенное усложнение содержания);

- принцип возрастосообразности (учёт психологических особенностей младшего школьного возраста);
- принцип активности и субъектности (вовлечение детей в активную деятельность, развитие их самостоятельности);
- принцип интеграции (включение тематики кибербезопасности в различные формы образовательной деятельности);
- принцип социального партнёрства (взаимодействие школы, семьи, внешних организаций);
- принцип индивидуализации (учёт индивидуальных особенностей и уровня цифровой грамотности каждого ребёнка);
- принцип практикоориентированности (опора на реальные ситуации, формирование практических навыков) [2].

Условиями эффективного функционирования системы являются:

- нормативно-правовое обеспечение (включение направления в основную образовательную программу, план работы педагога-психолога);
- организационное обеспечение (распределение функций между субъектами, координация деятельности);
- кадровое обеспечение (наличие квалифицированного педагога-психолога, повышение компетентности педагогов);
- материально-техническое обеспечение (наличие оборудования, методических материалов, диагностических инструментов);
- информационное обеспечение (доступ к актуальной информации о киберугрозах, лучшим практикам);
- мотивационное обеспечение (заинтересованность администрации, педагогов, родителей в решении проблемы) [13].

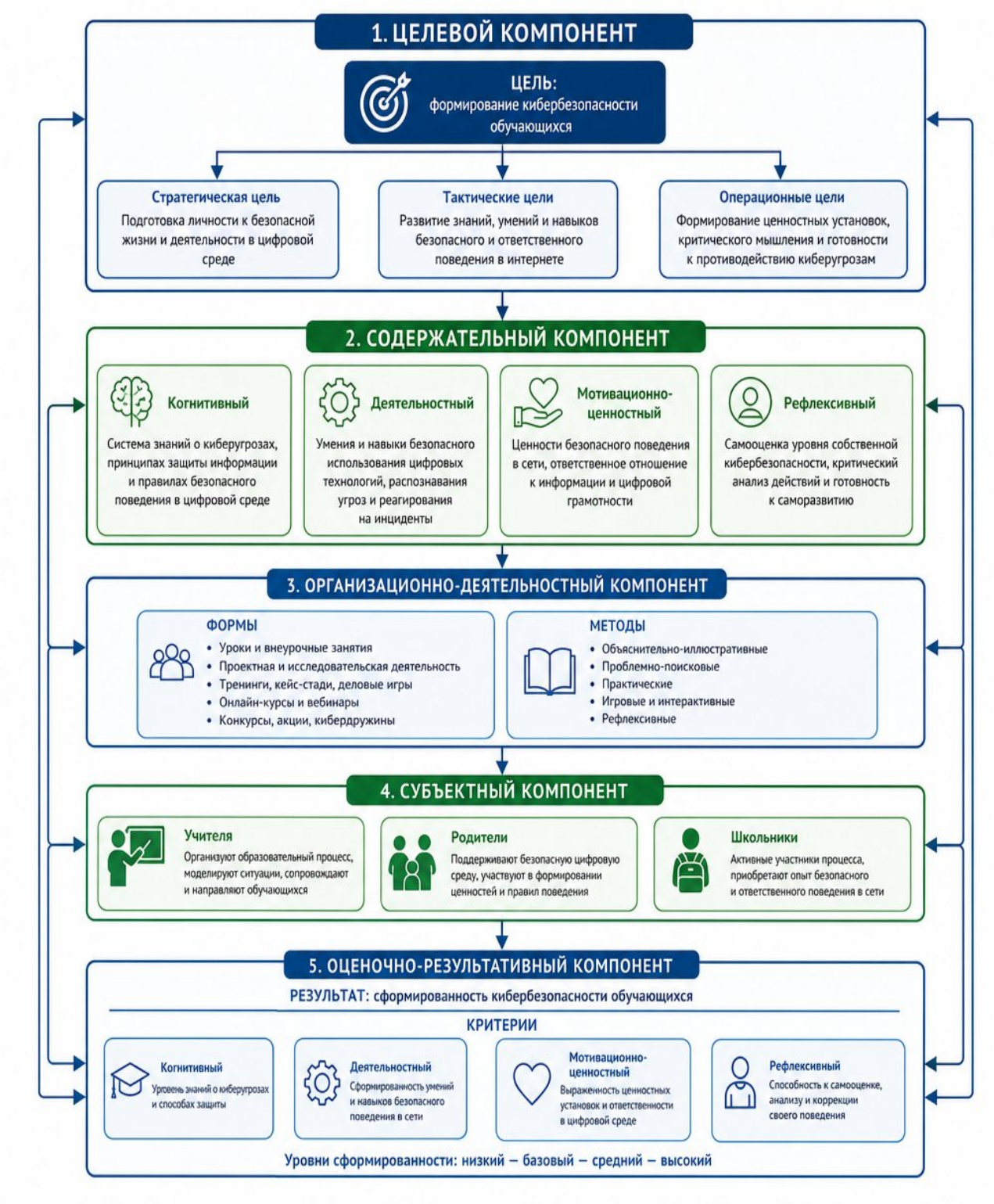

Рисунок 1 – Структурно-функциональная модель системы формирования основ кибербезопасности младших школьников

Выводы по главе 2

Таким образом, разработанная структурно-функциональная модель системы формирования основ кибербезопасности в образовательной среде

начальной школы представляет собой целостный, теоретически обоснованный конструкт, определяющий цели, содержание, организацию, субъектов и ожидаемые результаты деятельности по обеспечению безопасности младших школьников в цифровой среде. Модель носит открытый характер и может адаптироваться к специфическим условиям конкретной образовательной организации, предоставляя при этом общую рамку для проектирования и реализации системной работы в данном направлении.

ГЛАВА 3. Анализ и интерпретация результатов исследования

3.1 Диагностика и анализ уровня сформированности информационной культуры субъектов образовательного процесса

Диагностический этап является основой для проектирования программы психолого-педагогического сопровождения и предполагает комплексное изучение исходного уровня информационной культуры и цифровой грамотности всех субъектов образовательного процесса. В соответствии с разработанной моделью диагностика должна охватывать младших школьников как основных адресатов профилактической работы, родителей как ключевых агентов социализации и контроля, педагогов как участников формирования основ кибербезопасности. Многосубъектный характер диагностики позволяет получить объёмную картину ситуации и выявить зоны наибольшего риска, требующие первоочередного внимания [4].

Диагностика младших школьников направлена на выявление уровня сформированности когнитивного, деятельностного, мотивационно-ценностного и рефлексивного компонентов основ кибербезопасности. Для оценки когнитивного компонента использовалась разработанная нами анкета «Что я знаю о безопасности в интернете», содержащая вопросы о правилах безопасного поведения, типах киберугроз, способах защиты. Анкета включает закрытые вопросы с выбором варианта ответа и открытые вопросы, требующие самостоятельной формулировки. Примеры вопросов:

- можно ли сообщать незнакомым людям в интернете свой адрес и телефон;
- что нужно делать, если кто-то в интернете тебя обижает;
- какой пароль является надёжным;
- можно ли переходить по ссылкам в письмах от незнакомых людей [17].

Оценка деятельностного компонента осуществлялась с помощью метода наблюдения за поведением детей в процессе выполнения практических заданий на компьютере (поиск информации по заданной теме с использованием детской поисковой системы, создание пароля для воображаемого аккаунта, определение, какие из предъявленных изображений можно размещать в интернете, а какие содержат личную информацию). Фиксировались степень самостоятельности, уверенность действий, обращение за помощью, соблюдение правил безопасности без напоминания. Использовалась структурированная схема наблюдения с заранее определёнными категориями поведения [25].

Для оценки мотивационно-ценностного компонента применялась методика незаконченных предложений, адаптированная к тематике кибербезопасности. Детям предлагалось закончить предложения:

- интернет нужен для того, чтобы…;
- когда я в интернете, я чувствую…;
- если друг попросит меня сказать пароль от моего аккаунта, я…;
- если я увижу, что кого-то обижают в интернете, я…;
- больше всего в интернете меня пугает…

Анализ ответов позволял выявить ценностное отношение к цифровой среде, уровень эмпатии, осознание рисков [33].

Рефлексивный компонент оценивался в процессе индивидуальных бесед, в ходе которых детям предлагалось рассказать о своём опыте использования интернета, о том, что они обычно делают онлайн, были ли ситуации, когда они чувствовали себя некомфортно, как поступили в этих ситуациях, что бы сделали иначе. Фиксировалась способность к осмыслению собственного опыта, критичность по отношению к своим действиям, понимание причинно-следственных связей [9].

Диагностика родителей имела целью выявить уровень их цифровой компетентности, осведомлённости о киберугрозах, практик контроля за

цифровой активностью ребёнка. Использовалась анкета «Ребёнок и интернет: позиция родителя», включающая блоки вопросов:

- о наличии у ребёнка доступа к интернету, типах используемых устройств;
- видах цифровой активности ребёнка (игры, просмотр видео, общение в соцсетях, обучение);
- продолжительности времени, проводимого ребёнком в интернете;
- наличии правил использования интернета дома;
- применении технических средств родительского контроля;
- осведомлённости родителей о том, что делает ребёнок онлайн;
- знании родителей о киберугрозах для детей;
- обсуждении с ребёнком правил безопасного поведения в интернете;
- случаях столкновения ребёнка с негативными ситуациями в сети [20].

Анализ результатов позволял выделить типы родительской позиции по отношению к цифровой активности ребёнка:

- контролирующая (жёсткий контроль, ограничения, использование технических средств, низкая степень доверия);
- партнёрская (совместная деятельность в интернете, обсуждение опыта, баланс контроля и свободы);
- попустительская (отсутствие интереса к цифровой активности ребёнка, минимальный контроль);
- тревожная (высокий уровень беспокойства, но недостаточная компетентность для эффективного контроля) [35].

Диагностика педагогов была направлена на оценку их собственной цифровой компетентности и готовности к работе по формированию основ кибербезопасности у обучающихся. Использовался опросник, включающий вопросы:

- о частоте использования цифровых технологий в профессиональной деятельности;
- знании основных киберугроз для младших школьников;
- опыте интеграции тематики кибербезопасности в содержание уроков или внеурочной деятельности;
- уверенности в собственной способности обучать детей безопасному поведению в интернете;
- потребности в повышении квалификации по данному направлению [10].

Также проводилось анкетирование классных руководителей для выявления случаев столкновения обучающихся их классов с киберугрозами (кибербуллинг, доступ к неприемлемому контенту, чрезмерное увлечение играми). Это позволяло оценить масштаб проблемы в конкретной образовательной организации и выделить детей группы риска для индивидуальной работы [29].

База исследования: диагностика проводилась на базе МБОУ СОШ г. Челябинска в период с ноября по декабрь 2025 года. В исследовании приняли участие 78 обучающихся 2-3 классов (38 второклассников и 40 третьеклассников), 72 родителя, 8 педагогов (4 классных руководителя, 4 учителя-предметника).

Результаты диагностики младших школьников. Анализ ответов на анкету «Что я знаю о безопасности в интернете» показал, что большинство детей (64 %) имеют фрагментарные, несистематизированные знания о правилах кибербезопасности. Они могут назвать 1–2 правила (обычно «не общаться с незнакомцами» и «не сообщать пароли»), но не понимают глубоко их смысла и не могут объяснить, почему эти правила важны. Лишь 18 % обучающихся продемонстрировали достаточно полные и систематизированные знания, что было характерно для детей, чьи родители целенаправленно обсуждали с ними правила поведения в интернете. 18 %

детей показали крайне низкий уровень знаний, затруднялись ответить на большинство вопросов [6].

Наибольшие затруднения вызвали вопросы о надёжных паролях (только 23 % смогли объяснить, каким должен быть надёжный пароль), о действиях при столкновении с неприятным контентом (35 % выбрали правильную стратегию – закрыть страницу и сообщить взрослым, остальные выбирали варианты «продолжу смотреть из любопытства» или «расскажу друзьям»), о признаках мошеннических сайтов (менее 10 % могли назвать хотя бы один признак). Вместе с тем 78 % правильно ответили, что нельзя сообщать незнакомым людям в интернете свой адрес и номер телефона, что свидетельствует об определённой базовой осведомлённости [15].

Наблюдение за выполнением практических заданий выявило, что деятельностный компонент сформирован слабее когнитивного: даже зная правило, дети не всегда применяли его на практике. При создании пароля 52 % детей использовали простые комбинации (имя, дата рождения), несмотря на предварительное обсуждение требований к надёжным паролям. При поиске информации 41 % детей переходили по первой попавшейся ссылке, не обращая внимания на источник. Настройки приватности в учебном аккаунте социальной сети только 15 % детей установили правильно, обеспечив защиту личной информации [27].

Анализ незаконченных предложений показал, что для большинства детей (71 %) интернет ассоциируется прежде всего с развлечениями (игры, видео, мультфильмы), лишь 23 % упомянули образовательную функцию («искать информацию для уроков», «учиться»). Эмоциональное отношение к интернету в основном позитивное («интересно», «весело», «нравится»), лишь 12 % детей упомянули негативные чувства («иногда страшно», «боюсь вирусов»). Осознание рисков недостаточное: на вопрос о том, что пугает в интернете, 34 % детей ответили «ничего» [18].

Вопросы, связанные с эмпатией и этичным поведением, выявили тревожную картину: лишь 39 % детей выбрали бы просоциальную стратегию при виде кибербуллинга («защитил бы», «сказал бы учителю»), остальные выбрали пассивную позицию («не моё дело», «не знаю, что делать») или даже присоединились бы к агрессорам («это, наверное, смешно»). Это свидетельствует о необходимости специальной работы по воспитанию эмпатии и формированию нетерпимости к кибербуллингу [31].

Беседы о рефлексии цифрового опыта показали, что младшие школьники в большинстве своём (68 %) не задумываются о своём поведении в интернете, действуют импульсивно, не анализируют последствия. На вопрос «Были ли ситуации, когда ты пожалел о том, что сделал в интернете?» большинство ответили отрицательно, что может свидетельствовать как о реальном отсутствии негативного опыта, так и о недостаточной рефлексии (таблица 2) [22].

Таблица 2 – Распределение младших школьников по уровням сформированности основ кибербезопасности (констатирующий этап)

Компонент	Высокий уровень	Средний уровень	Низкий уровень
Когнитивный	18 % (14 чел.)	64 % (50 чел.)	18 % (14 чел.)
Деятельностный	15 % (12 чел.)	46 % (36 чел.)	39 % (30 чел.)
Мотивационно-ценностный	21 % (16 чел.)	53 % (41 чел.)	26 % (21 чел.)
Рефлексивный	12 % (9 чел.)	38 % (30 чел.)	50 % (39 чел.)

Результаты диагностики родителей. Анализ анкет показал, что практически все дети (97 %) имеют доступ к интернету дома, чаще всего используют планшеты (78 %) и смартфоны родителей (65 %), 43 % имеют собственные смартфоны. Среднее время, проводимое в интернете в будние дни, составляет 1,5–2 часа, в выходные увеличивается до 3–4 часов. Основные виды активности: просмотр видео на YouTube (89 %), игры (76 %), общение в мессенджерах и соцсетях (34 % третьеклассников).

Лишь 41 % родителей установили технические средства родительского контроля. Объяснение: «не знаю, как это сделать» (35 %), «доверяю ребёнку» (28 %), «нет необходимости, ребёнок ещё маленький и не делает ничего опасного» (24 %). Правила использования интернета дома

установлены у 53 % семей, но их содержание и степень соблюдения различны. Чаще всего правила касаются времени (38 %) и запрета определённых игр или сайтов (29 %). Систематические обсуждения того, что ребёнок делает в интернете, проводят лишь 36 % родителей [24].

Осведомлённость родителей о киберугрозах оказалась невысокой: 67 % слышали о кибербуллинге, но лишь 23 % правильно понимают этот термин; о груминге слышали 18 %, о фишинге – 31 %. Большинство родителей (71 %) считают, что их ребёнок слишком мал, чтобы столкнуться с серьёзными киберугрозами, и основные риски связывают лишь с «лишним временем за экраном» и «вредом для зрения». Случаи столкновения с негативными ситуациями отметили 14 % родителей: ребёнок видел пугающий контент (8 %), столкнулся с оскорблениями в игре (4 %), случайно совершил внутриигровую покупку (2 %) [36].

По типам родительской позиции распределение получилось следующим:

- контролирующая позиция – 28 %;
- партнёрская позиция – 33 %;
- попустительская позиция – 24 %;
- тревожная позиция – 15 %.

Наиболее благоприятной является партнёрская позиция, однако даже среди этой группы родителей многим не хватает специальных знаний для эффективного обучения ребёнка безопасному цифровому поведению [39].

Результаты диагностики педагогов показали, что все учителя используют цифровые технологии в своей работе (электронный журнал, мультимедийные презентации, образовательные платформы), однако уровень их цифровой компетентности различен. Знания о киберугрозах для младших школьников имеются у 75 % педагогов, но они носят общий характер. Опыт интеграции тематики кибербезопасности в уроки или внеурочную деятельность имеют лишь 37 % педагогов (в основном это проведение тематических классных часов 1–2 раза в год). Только 25 %

учителей чувствуют себя уверенно в обучении детей безопасному поведению в интернете, остальные испытывают затруднения и отмечают потребность в повышении квалификации по данному направлению (88 %) [3].

Классные руководители сообщили о следующих случаях в их классах за прошлый учебный год: конфликт между детьми, переросший в оскорбления в мессенджере (2 случая); ребёнок поделился с учителем, что увидел «страшное видео» и теперь боится (1 случай); родители обратились с жалобой на то, что их ребёнок без спроса потратил деньги на игру (1 случай). Это свидетельствует о том, что проблема кибербезопасности младших школьников является реальной, а не надуманной.

Таким образом, результаты комплексной диагностики выявили, что уровень сформированности основ кибербезопасности у большинства младших школьников является недостаточным, преобладают средний и низкий уровни. Наиболее проблемными являются деятельностный и рефлексивный компоненты. Значительная часть родителей недооценивает киберугрозы для детей младшего школьного возраста и недостаточно компетентна для эффективного контроля и обучения. Педагоги осознают важность проблемы, но испытывают дефицит методической подготовки. Полученные данные подтвердили необходимость разработки и реализации комплексной программы психолого-педагогического сопровождения, направленной на формирование основ кибербезопасности у младших школьников при активном вовлечении родителей и педагогов.

3.2 Реализация программы психолого-педагогического сопровождения и оценка её результативности

На основе результатов диагностики была разработана и реализована программа психолого-педагогического сопровождения «Безопасный мир цифровых технологий», направленная на формирование основ

кибербезопасности у младших школьников. Программа имеет комплексный характер и включает три модуля: работу с обучающимися, работу с родителями, работу с педагогами. Реализация программы осуществлялась педагогом-психологом в тесном взаимодействии с классными руководителями и родителями в период с ноября 2025 по март 2026 года на базе той же образовательной организации. Экспериментальную группу составили обучающиеся двух классов (38 человек), контрольную группу – обучающиеся двух других классов параллели (40 человек), с которыми систематическая работа по программе не проводилась [7].

Подготовительный этап педагогического эксперимента

На подготовительном этапе была осуществлена детальная разработка программы психолого-педагогического сопровождения с определением целей, задач, содержания и методов работы с каждой группой субъектов. Целью программы является формирование основ кибербезопасного поведения у младших школьников через развитие когнитивного, деятельностного, мотивационно-ценностного и рефлексивного компонентов цифровой грамотности при активном вовлечении родителей и педагогов.

Задачи программы:

- сформировать у обучающихся систему знаний о правилах безопасного поведения в интернете и типичных киберугрозах;
- развить практические навыки безопасного использования цифровых технологий;
- воспитать ценностное отношение к собственной безопасности и безопасности других, установки на этичное поведение в цифровой среде; развить способность к рефлексии собственного цифрового поведения и его последствий;
- повысить компетентность родителей в вопросах кибербезопасности детей и обучить стратегиям эффективного контроля и поддержки;

~ повысить готовность педагогов к интеграции тематики кибербезопасности в образовательный процесс [19].

Был подобран диагностический инструментарий для оценки эффективности программы (те же методики, что использовались на констатирующем этапе, для обеспечения сравнимости результатов). Подготовлены материалы для проведения занятий: мультимедийные презентации, раздаточные материалы, сценарии ролевых игр, кейсы для анализа, памятки для родителей и педагогов. Проведены организационные встречи с администрацией школы, классными руководителями, родителями экспериментальной группы для разъяснения целей и содержания программы, получения согласия на участие детей в занятиях [26].

Констатирующий этап педагогического эксперимента

На констатирующем этапе была проведена первичная диагностика в экспериментальной и контрольной группах с использованием описанного выше инструментария. Цель констатирующего этапа – установить исходный уровень сформированности основ кибербезопасности в обеих группах и убедиться в их эквивалентности до начала формирующего воздействия. Диагностика проводилась в естественных условиях в ноябре 2025 года. Использовались методы анкетирования, наблюдения, беседы, анализа продуктов деятельности.

Результаты констатирующего этапа показали отсутствие статистически значимых различий между экспериментальной и контрольной группами по всем измеряемым параметрам, что подтверждает корректность формирования выборки. В обеих группах преобладали средний и низкий уровни сформированности основ кибербезопасности, это можно видеть в таблице 3.

Таблица 3 – Результаты констатирующего этапа эксперимента (обобщённые показатели)

Уровень сформированности основ кибербезопасности	Экспериментальная группа (n = 38)	Контрольная группа (n = 40)
Высокий уровень	16 % (6 чел.)	15 % (6 чел.)
Средний уровень	50 % (19 чел.)	52 % (21 чел.)
Низкий уровень	34 % (13 чел.)	33 % (13 чел.)

Анализ связи между факторным и результативным признаками с использованием критерия χ^2 (хи-квадрат) показал отсутствие статистически значимых различий ($\chi^2 = 0{,}049$ при $df = 2$, $p = 0{,}976$). Полученное значение критерия существенно ниже критического порога для уровня значимости $\alpha = 0{,}05$ ($\chi^2_{крит} = 5{,}991$). Таким образом, нулевая гипотеза об отсутствии связи между исследуемыми признаками принимается, а выявленная зависимость признается статистически незначимой при $p > 0{,}05$.

Отобразим полученные данные с помощью диаграммы (рисунок 2).

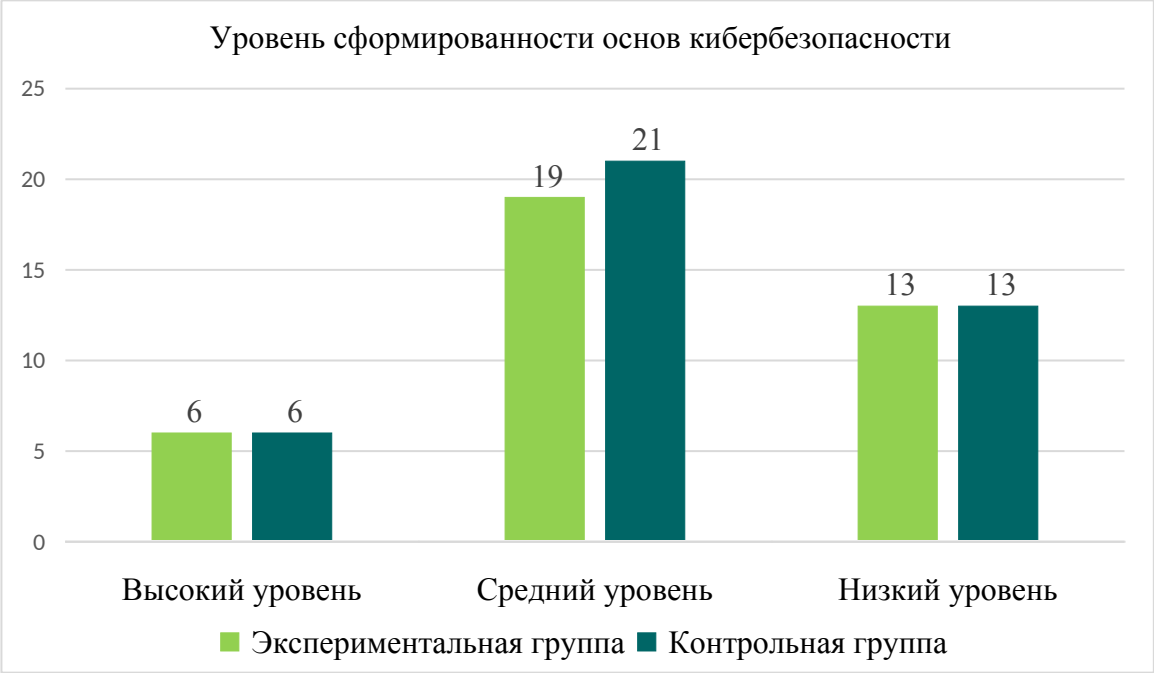

Рисунок 2 – Результаты констатирующего этапа эксперимента (обобщённые показатели)

Полученные данные подтвердили необходимость реализации формирующего воздействия и позволили конкретизировать акценты программы с учётом наиболее проблемных зон: недостаточная сформированность деятельностного и рефлексивного компонентов, низкий уровень эмпатии по отношению к жертвам кибербуллинга, формальное знание правил без понимания их смысла [14].

Формирующий этап педагогического эксперимента

Формирующий этап включал реализацию трёх модулей программы в период с ноября 2025 по март 2026 года.

Модуль 1: Работа с обучающимися экспериментальной группы

Была разработана система из 12 групповых развивающих занятий продолжительностью 35–40 минут каждое, проводившихся с периодичностью 1 раз в неделю. Занятия имели единую структуру:

- организационный момент, создание положительного эмоционального фона;
- актуализация имеющихся знаний и опыта по теме занятия;
- введение новой информации через интерактивные методы (дискуссия, просмотр видеоролика, мини-лекция);
- практическая отработка навыков через ролевые игры, решение кейсов, выполнение заданий на компьютере;
- рефлексия, обсуждение чувств и мыслей участников;
- домашнее задание (например, обсудить с родителями правила, создать плакат, понаблюдать за своим поведением) [31].

Тематика занятий:

1. «Что такое интернет и зачем он нужен» – формирование понимания структуры интернета, его возможностей и ограничений.

2. «Мой цифровой след» – знакомство с понятием цифрового следа, понимание, что информация в интернете остаётся навсегда.

3. «Личная информация: что можно и нельзя сообщать» –определение границ приватности, отработка навыков защиты персональных данных.

4. «Надёжные пароли: создаём и храним правильно» – формирование навыков создания надёжных паролей, правил их хранения.

5. «Безопасный поиск информации» – обучение использованию детских поисковых систем, критической оценке источников.

6. «Как отличить правду от обмана в интернете» – развитие критического мышления, навыков проверки информации.

7. «Безопасное общение онлайн» – правила общения в мессенджерах и соцсетях, распознавание попыток манипуляции.

8. «Что делать, если тебя обижают в интернете» – понятие кибербуллинга, стратегии реагирования, обращение за помощью.

9. «Я не буду обижать других» – воспитание эмпатии, понимание последствий агрессивного поведения онлайн.

10. «Полезный и вредный контент» – формирование навыков оценки контента, действия при столкновении с неприемлемым материалом.

11. «Игры и покупки в интернете: будь осторожен» – профилактика игровой зависимости и импульсивных покупок.

12. «Баланс: реальная жизнь и интернет» – формирование понимания ценности офлайн-активностей, навыков саморегуляции времени [8].

На каждом занятии использовались разнообразные методы. Ролевые игры позволяли отрабатывать навыки в безопасных условиях (например, ролевая игра «Незнакомец в чате», где один ребёнок играл роль ребёнка, другой – взрослого, выдающего себя за ровесника, остальные наблюдали и затем обсуждали, какие признаки выдали обман, как правильно поступить). Кейс-метод предполагал анализ ситуаций: «Ваня получил сообщение: “Поздравляем! Ты выиграл новый смартфон! Для получения приза перейди по ссылке и введи данные банковской карты родителей”. Что должен сделать Ваня?» Дети работали в малых группах, обсуждали варианты, защищали своё решение, педагог-психолог направлял дискуссию к правильному выводу [23].

Использовались визуальные материалы: просмотр обучающих мультфильмов из серии «Фиксики» и «Смешарики» о безопасности в интернете с последующим обсуждением, создание плакатов «Правила нашего класса в интернете». Практические задания на компьютерах включали: безопасный поиск информации на заданную тему с использованием детской поисковой системы, настройку параметров

приватности в учебном аккаунте, создание надёжного пароля с использованием техники ассоциаций [37].

Арт-терапевтические методы применялись для работы с эмоциональным компонентом: рисование «Мой интернет» (что нравится и что пугает), создание коллажей «Интернет – друг или враг». Обсуждение рисунков позволяло выявить индивидуальные страхи и проблемы детей, проработать их. Психогимнастика и релаксационные упражнения использовались в конце занятий для снятия напряжения [11].

Для повышения мотивации была введена система символического поощрения: на каждом занятии дети получали «смайлики безопасности» за активное участие, правильные ответы, выполнение домашних заданий. По окончании программы был проведён праздник «Знатоки безопасного интернета» с вручением грамот и памятных призов [20].

Модуль 2: Работа с родителями

Работа с родителями включала групповые и индивидуальные формы. Проведены три тематических родительских собрания:

1. «Цифровое детство: возможности и риски» (ноябрь 2025) – информирование о масштабах цифровой активности детей, типах киберугроз, задачах родителей.

2. «Как защитить ребёнка в интернете: практикум для родителей» (январь 2026) – обучение установке и настройке родительского контроля, правилам установления границ, способам обсуждения с ребёнком его цифрового опыта.

3. «Партнёрство семьи и школы в обеспечении кибербезопасности» (март 2026) – подведение итогов, презентация результатов работы с детьми, выработка совместных стратегий [28].

Формат собраний был интерактивным: мини-лекции чередовались с дискуссиями, работой в малых группах, просмотром видеороликов, демонстрацией технических средств. Использовались приёмы повышения вовлечённости: опросы через мобильное приложение, анонимные вопросы

на стикерах, обмен опытом между родителями. По результатам каждого собрания родителям предоставлялись методические материалы: памятки «Как говорить с ребёнком о кибербезопасности», инструкции по настройке родительского контроля, списки рекомендуемых детских ресурсов [35].

Индивидуальное консультирование проводилось по запросу родителей и по инициативе педагога-психолога в случае выявления у ребёнка признаков столкновения с киберугрозами или формирования зависимого поведения. За период реализации программы проведено 12 индивидуальных консультаций. Тематика: чрезмерное увлечение ребёнка играми, трудности установления ограничений, конфликт между ребёнком и родителями из-за интернета, случай кибербуллинга [4].

Создана группа родителей экспериментальных классов в мессенджере, где педагог-психолог регулярно размещал короткие информационные посты по тематике кибербезопасности, отвечал на вопросы, напоминал о темах занятий с детьми, предлагал задания для совместной деятельности детей и родителей дома [17].

Модуль 3: Работа с педагогами

Для педагогов проведён методический семинар «Формирование основ кибербезопасности у младших школьников: роль учителя» продолжительностью 4 часа. Семинар включал теоретический блок (психологические особенности младшего школьного возраста в контексте цифровой социализации, виды киберугроз, принципы профилактики) и практический блок (способы интеграции тематики кибербезопасности в содержание различных учебных предметов, методы выявления признаков столкновения ребёнка с киберугрозами, алгоритмы действий педагога) [25].

Разработаны методические рекомендации для учителей начальных классов «Кибербезопасность на каждом уроке: идеи для интеграции», содержащие примеры заданий по математике (решение задач о безопасном времени в интернете), русскому языку (написание сочинения «Мой друг – интернет», грамматические упражнения на материале правил

кибербезопасности), окружающему миру (изучение темы «Средства связи и коммуникации» с акцентом на безопасность), литературному чтению (обсуждение поступков героев с точки зрения этики цифрового поведения) [32].

Классным руководителям экспериментальных классов оказывалась методическая поддержка при подготовке и проведении тематических классных часов, предоставлялись материалы для работы с родителями. Проводилось супервизорство: педагог-психолог помогал учителям анализировать сложные ситуации, связанные с цифровым поведением обучающихся [9].

Контрольный этап педагогического эксперимента и анализ результатов

По завершении реализации программы в апреле 2026 года была проведена повторная диагностика в экспериментальной и контрольной группах с использованием тех же методик, что и на констатирующем этапе. Цель контрольного этапа – оценить изменения уровня сформированности основ кибербезопасности и определить эффективность программы психолого-педагогического сопровождения.

Результаты контрольного этапа в экспериментальной группе показали значительную положительную динамику по всем компонентам. Когнитивный компонент: количество обучающихся с высоким уровнем знаний возросло с 18 % до 47 %, со средним уровнем – с 63 % до 50 %, с низким уровнем снизилось с 19 % до 3 %. Дети стали демонстрировать более полные и системные знания о правилах кибербезопасности, могли объяснять смысл правил, приводить примеры. Значительно улучшилось понимание того, что такое надёжный пароль (с 23 % до 76 % правильных ответов), знание стратегий реагирования на неприятный контент (с 35 % до 84 %), осведомлённость о признаках мошенничества (с 10 % до 58 %) [22].

Деятельностный компонент показал наибольший прирост: высокий уровень возрос с 16 % до 42 %, средний – с 47 % до 52 %, низкий снизился

с 37 % до 6 %. При выполнении практических заданий дети стали действовать более уверенно и самостоятельно. При создании пароля 79 % использовали надёжные комбинации (против 48 % на констатирующем этапе). При поиске информации 82 % обращали внимание на источник и использовали безопасные детские ресурсы (против 59 %). Настройки приватности правильно установили 71 % детей (против 15 %). Это свидетельствует о том, что систематическая практическая отработка навыков является эффективной [30].

Мотивационно-ценностный компонент: высокий уровень возрос с 21 % до 39 %, средний – с 53 % до 55 %, низкий снизился с 26 % до 6 %. В ответах на методику незаконченных предложений увеличилась доля упоминаний образовательной функции интернета (с 23 % до 47 %), появились высказывания о важности безопасности («интернет – это интересно, но надо быть осторожным»). Значительно возросла эмпатия по отношению к жертвам кибербуллинга: 76 % детей выбрали просоциальную стратегию реагирования (против 39 %), что свидетельствует об эффективности специальных занятий по этой теме [36].

Рефлексивный компонент: высокий уровень возрос с 13 % до 34 %, средний – с 37 % до 58 %, низкий снизился с 50 % до 8 %. В беседах дети стали демонстрировать большую способность к осмыслению своего цифрового поведения, анализировали свои действия, могли спрогнозировать последствия, выражали намерение изменить некоторые привычки (например, «я понял, что слишком много играю, надо больше гулять», «буду спрашивать маму, прежде чем переходить по ссылкам»), информация об этом представлена в таблице 4 [12].

Таблица 4 – Сравнительные результаты констатирующего и контрольного этапов эксперимента в экспериментальной группе

Компонент	Высокий уровень (до/после)	Средний уровень (до/после)	Низкий уровень (до/после)
Когнитивный	18 % / 47 %	63 % / 50 %	19 % / 3 %
Деятельностный	16 % / 42 %	47 % / 52 %	37 % / 6 %

Компонент	Высокий уровень (до/после)	Средний уровень (до/после)	Низкий уровень (до/после)
Мотивационно-ценностный	21 % / 39 %	53 % / 55 %	26 % / 6 %
Рефлексивный	13 % / 34 %	37 % / 58 %	50 % / 8 %

В контрольной группе, с которой систематическая работа по программе не проводилась, также была проведена повторная диагностика. Результаты показали незначительные изменения, которые могут объясняться естественным взрослением детей, общим влиянием образовательной среды, эпизодическими мероприятиями (например, в рамках Единого урока по безопасности в сети Интернет). Однако динамика в контрольной группе была существенно меньше, чем в экспериментальной, данные об этом приведены в таблице 5.

Таблица 5 – Сравнительные результаты экспериментальной и контрольной групп на контрольном этапе (обобщённые показатели)

Уровень сформированности основ кибербезопасности	Экспериментальная группа (n = 38)	Контрольная группа (n = 40)
Высокий уровень	40 % (15 чел.)	20 % (8 чел.)
Средний уровень	54 % (21 чел.)	55 % (22 чел.)
Низкий уровень	6 % (2 чел.)	25 % (10 чел.)

Сравнение результатов экспериментальной и контрольной групп на контрольном этапе демонстрирует статистически значимые различия: в экспериментальной группе доля обучающихся с высоким уровнем сформированности основ кибербезопасности в два раза выше, а с низким уровнем – более чем в четыре раза ниже. Это подтверждает эффективность реализованной программы психолого-педагогического сопровождения [15].

Отобразим полученные данные с помощью диаграммы (рисунок 3).

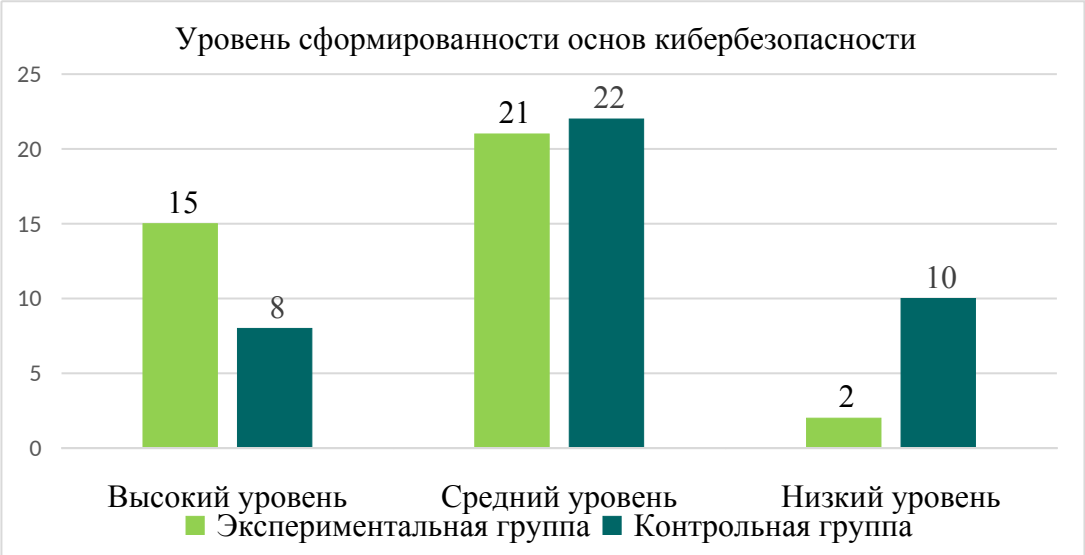

Рисунок 3 – Сравнительные результаты экспериментальной и контрольной групп на контрольном этапе (обобщённые показатели)

Как мы видим, анализ связи между факторным и результативным признаками с использованием критерия χ^2 (хи-квадрат) выявил наличие статистически значимых различий ($\chi^2 = 7{,}441$ при $df = 2$, $p = 0{,}025$). Полученное значение критерия превышает критический порог для уровня значимости $\alpha = 0{,}05$ (χ^2крит = 5,991), что позволяет отвергнуть нулевую гипотезу об отсутствии связи. Таким образом, установленная зависимость между признаками является статистически значимой на уровне $p < 0{,}05$.

Анализ результатов работы с родителями показал повышение их компетентности и изменение практик контроля. По данным итогового анкетирования родителей экспериментальной группы: установили технические средства родительского контроля 78 % (против 41 % до начала программы); регулярно обсуждают с ребёнком его цифровой опыт 71 % (против 36 %); установили правила использования интернета дома 89 % (против 53 %); считают себя достаточно информированными о киберугрозах 82 % (против 29 %). Увеличилась доля родителей с партнёрской позицией (с 33 % до 61 %) за счёт снижения доли попустительской и тревожной позиций. Родители отмечали, что дети стали сами рассказывать о том, что узнали на занятиях, инициировать обсуждения, что способствовало выстраиванию диалога [27].

Оценка результатов работы с педагогами: по данным итогового опроса, 100 % учителей, участвовавших в семинаре, оценили его как полезный; 87 % интегрировали тематику кибербезопасности в свои уроки или внеурочные занятия хотя бы один раз; 75 % чувствуют себя более уверенно в обсуждении с детьми вопросов безопасного поведения в интернете; 100 % выразили готовность к продолжению работы в данном направлении [38].

Качественный анализ изменений выявил ряд косвенных эффектов программы. Классные руководители отмечали улучшение атмосферы в классах, снижение конфликтности (в том числе потому, что дети стали более осознанно подходить к общению онлайн, научились не реагировать агрессивно на провокации). Родители отмечали, что дети стали более открыто делиться своим опытом в интернете, меньше сопротивляются установлению правил, понимая их смысл. Несколько родителей обратились за консультацией по поводу не связанных с кибербезопасностью вопросов, что свидетельствует о повышении доверия к психологической службе [18].

В ходе реализации программы выявлены факторы, способствовавшие её эффективности:

- комплексный подход, охватывающий всех субъектов образовательного процесса;
- систематичность и регулярность занятий с детьми;
- использование разнообразных интерактивных методов, обеспечивающих активность и вовлечённость;
- практикоориентированность: отработка навыков в условиях, максимально приближенных к реальным;
- учёт возрастных особенностей младших школьников (опора на наглядность, игру, эмоциональное вовлечение);
- создание положительной мотивации через систему поощрений, игровые элементы;

- вовлечение родителей как ключевых агентов закрепления навыков в домашних условиях;
- поддержка педагогов, обеспечивающих интеграцию тематики в образовательный процесс [24].

Ограничения исследования связаны с относительно небольшим объёмом выборки, коротким периодом реализации программы (5 месяцев), отсутствием отсроченного контроля (через 6–12 месяцев после завершения программы для оценки устойчивости эффектов). В дальнейшем планируется расширение программы на параллели 1–4 классов, проведение лонгитюдного исследования для оценки долгосрочных эффектов, разработка цифровой версии программы с использованием интерактивных образовательных игр [33].

Выводы по главе 3

Таким образом, результаты педагогического эксперимента подтвердили выдвинутую гипотезу: систематическая реализация программы психолого-педагогического сопровождения, включающей диагностический, профилактический и развивающий компоненты с учётом возрастных психологических особенностей младших школьников и активным вовлечением всех субъектов образовательного процесса, является эффективным средством формирования основ кибербезопасности. Значимые позитивные изменения зафиксированы по всем компонентам: когнитивному, деятельностному, мотивационно-ценностному и рефлексивному. Разработанная программа может быть рекомендована к внедрению в практику работы образовательных организаций с адаптацией к конкретным условиям.

Заключение

Проведённое исследование было посвящено актуальной проблеме формирования основ кибербезопасности у младших школьников в условиях стремительной цифровизации образования и повседневной жизни детей. В ходе работы были решены поставленные задачи, получены теоретические и практические результаты, подтверждающие выдвинутую гипотезу.

В первой главе работы был осуществлён теоретико-методологический анализ проблемы обеспечения кибербезопасности младших школьников. Изучение категориального аппарата исследования показало, что отечественная психолого-педагогическая наука активно разрабатывает понятийное поле информационной безопасности личности, однако сохраняется терминологическое разнообразие и недостаточная концептуализация применительно к начальной ступени образования. Ключевыми понятиями выступают «кибербезопасность», «цифровая грамотность», «информационная культура», «цифровая социализация», конкретизирующиеся для младшего школьного возраста через категорию «основы кибербезопасности» как интегративного личностного качества, включающего когнитивный, деятельностный, мотивационно-ценностный и рефлексивный компоненты.

Анализ психологических особенностей младшего школьного возраста позволил обосновать его сензитивный характер для формирования основ безопасного цифрового поведения. Сочетание интенсивного когнитивного развития, становления произвольности психических процессов, высокой восприимчивости к педагогическим воздействиям и начала активного освоения цифрового пространства создаёт благоприятные условия для закладки фундамента безопасного и этичного поведения в виртуальной среде.

Изучение специфики рисков и угроз киберпространства в условиях трансформации «цифрового детства» выявило многообразие киберугроз:

контентные риски (доступ к неприемлемым материалам), коммуникационные риски (кибербуллинг, груминг, манипуляции), потребительские риски (мошенничество, импульсивные покупки), технические риски (вредоносное ПО), риски нарушения приватности, психологические риски (формирование зависимости, социальная изоляция). Для младших школьников наиболее актуальными являются контентные и коммуникационные риски, а также психологические последствия чрезмерного погружения в цифровую среду.

Во второй главе был осуществлен концептуальный анализ существующих стратегий кибербезопасности и SWOT-анализ образовательных практик показали, что ни одна из стратегий (запретительно-ограничительная, информационно-просветительская, технологическая, психолого-педагогическая) не является универсально эффективной в изолированном применении. Оптимальной является интегративная модель, сочетающая элементы различных подходов с приоритетом психолого-педагогической стратегии, направленной на развитие личности ребёнка, формирование внутренних регуляторов поведения, критического мышления, навыков саморегуляции. Выявлены актуальные проблемы профилактики: фрагментарность и бессистемность работы, недостаточная подготовка педагогов, слабая вовлечённость родителей, цифровой разрыв между поколениями.

В третьей главе работы была разработана структурно-функциональная модель системы формирования основ кибербезопасности в образовательной среде начальной школы, включающая целевой, содержательный, организационно-деятельностный, субъектный и оценочно-результативный компоненты. Модель базируется на системном, деятельностном и личностно-ориентированном подходах, реализует принципы систематичности, возрастосообразности, активности, интеграции, социального партнёрства. Определены критерии и показатели

сформированности основ кибербезопасности, разработана трёхуровневая система оценки (высокий, средний, низкий уровни).

Проведённая комплексная диагностика уровня информационной культуры младших школьников, их родителей и педагогов выявила недостаточную сформированность основ кибербезопасности у большинства обучающихся (преобладали средний и низкий уровни), наиболее проблемными оказались деятельностный и рефлексивный компоненты. Значительная часть родителей недооценивает киберугрозы для детей младшего школьного возраста и недостаточно компетентна для эффективного контроля и обучения. Педагоги осознают важность проблемы, но испытывают дефицит методической подготовки.

На основе результатов диагностики была разработана и реализована программа психолого-педагогического сопровождения «Безопасный мир цифровых технологий», включающая три модуля: работу с обучающимися (12 групповых развивающих занятий), работу с родителями (родительские собрания, индивидуальные консультации, информационное сопровождение), работу с педагогами (методический семинар, супервизия, методические рекомендации). Педагогический эксперимент, реализованный на базе МБОУ СОШ г. Челябинска с участием 78 младших школьников, подтвердил эффективность разработанной программы.

Результаты контрольного этапа эксперимента показали значительную положительную динамику в экспериментальной группе по всем компонентам сформированности основ кибербезопасности. Доля обучающихся с высоким уровнем возросла с 16 % до 40 %, с низким уровнем снизилась с 34 % до 6 %. Наибольший прирост зафиксирован по деятельностному компоненту, что свидетельствует об эффективности практико-ориентированных методов работы. В контрольной группе динамика была незначительной, что подтверждает результативность именно систематического психолого-педагогического сопровождения, а не естественного взросления или эпизодических мероприятий.

Повысилась компетентность родителей: доля использующих технические средства защиты возросла с 41 % до 78 %, регулярно обсуждающих с ребёнком его цифровой опыт – с 36 % до 71 %. Увеличилась доля родителей с оптимальной партнёрской позицией. Педагоги, прошедшие обучение, стали более уверенно интегрировать тематику кибербезопасности в образовательный процесс.

Практическая значимость проведённого исследования заключается в разработке научно обоснованной, апробированной и доказавшей свою эффективность программы психолого-педагогического сопровождения, которая может быть внедрена в практику работы образовательных организаций. Разработанные диагностические материалы, конспекты занятий, методические рекомендации для педагогов и родителей представляют собой готовый инструментарий для педагогов-психологов. Результаты исследования могут быть использованы при разработке локальных нормативных актов образовательных организаций, программ повышения квалификации педагогов, содержания курсов для родителей.

На основе проведённого исследования могут быть сформулированы следующие практические рекомендации для образовательных организаций:

- включить направление формирования основ кибербезопасности в основную образовательную программу начального общего образования и планы работы педагога-психолога;
- обеспечить систематичность профилактической работы, реализуя программы на протяжении всего периода обучения в начальной школе с постепенным усложнением содержания;
- использовать разнообразные интерактивные, практико-ориентированные методы работы с детьми, обеспечивающие активность и формирование реальных навыков, а не только знаний;
- обязательно включать в систему работы родителей как ключевых агентов закрепления навыков в домашних условиях;

- повышать компетентность педагогов через систему повышения квалификации, методические семинары, обмен опытом;
- создать в образовательной организации атмосферу открытого обсуждения проблем кибербезопасности, когда дети не боятся обращаться за помощью к взрослым;
- использовать потенциал всех учебных предметов для интеграции тематики кибербезопасности;
- разработкой системы подготовки педагогов-психологов к работе в области кибербезопасности детства.

Таким образом, проведённое исследование внесло вклад в развитие теоретических представлений о кибербезопасности младших школьников, предложило практические инструменты для решения актуальной проблемы, подтвердило эффективность психолого-педагогического подхода к формированию основ безопасного цифрового поведения. Результаты исследования могут служить основой для дальнейшего совершенствования системы обеспечения безопасности детей в цифровой среде в условиях динамично меняющегося информационного общества.

Список использованных источников

1. Асмолов А. Г. Психология современности: вызовы неопределённости, сложности и разнообразия / А. Г. Асмолов // Психологические исследования. – 2018. – Т. 11. – № 60. – С. 1–10.

2. Баева И. А. Психологическая безопасность образовательной среды в условиях цифровизации / И. А. Баева, Л. А. Гаязова // Педагогика. – 2020. – № 5. – С. 39–47.

3. Белинская Е. П. Информационная социализация подростков: опыт пользования социальными сетями и психологическое благополучие / Е. П. Белинская // Психологические исследования. – 2018. – Т. 11. – № 58. – С. 6–15.

4. Божович Л. И. Личность и её формирование в детском возрасте / Л. И. Божович. – Санкт-Петербург : Питер, 2021. – 400 с. – ISBN 978-5-4461-1955-4.

5. Войскунский А. Е. Психология и интернет / А. Е. Войскунский. – Москва : Акрополь, 2019. – 439 с. – ISBN 978-5-98807-044-3.

6. Выготский Л. С. Педагогическая психология / Л. С. Выготский. – Москва : АСТ, 2005. – 672 с.– ISBN: 5-17-027239-1.

7. Гендина Н. И. Информационная грамотность и информационная культура личности: международный и российский подходы к решению проблемы / Н. И. Гендина // Открытое образование. – 2019. – Т. 23. – № 5. – С. 58–69.

8. Давыдов В. В. Психологическая теория учебной деятельности и методов начального обучения, основанных на содержательном обобщении / В. В. Давыдов. – Томск : Пеленг, 1992 – 112 с.

9. Дидактическая концепция цифрового профессионального образования и обучения / П. Н. Биленко, В. И. Блинов, М. В. Дулинов, Е. Ю. Есенина, А. М. Кондаков, И. С. Сергеев ; под науч. ред. В. И. Блинова – Москва : Перо, 2019. – 98 с. – ISBN 978-5-00150-679-9.

10. Жилавская И. В. Медиаобразование молодёжи : монография / И. В. Жилавская. – Москва : РИЦ МГГУ им. М. А. Шолохова, 2013. – 243 с. – ISBN 978-5-8288-1404-6.

11. Журавлёв А. Л. Научные подходы в современной отечественной психологии / А. Л. Журавлёв, Е. А. Сергиенко, Г. А. Виленская [и др.]; отв. ред. А. Л. Журавлёв, Е. А. Сергиенко, Г. А. Виленская. – Москва : Изд-во «Институт психологии РАН», 2023. – 759 с. – ISBN 978-5-9270-0465-2.

12. Зеер Э. Ф. Психолого-педагогические основы проектирования цифровой образовательной среды / Э. Ф. Зеер, В. С. Третьякова // Образование и наука. – 2021. – Т. 23. – № 3. – С. 15–38.

13. Зинченко Ю. П. Психология безопасности как социально-системное явление / Ю. П. Зинченко, А. И. Донцов // Вопросы психологии. – 2020. – № 1. – С. 21–31.

14. Иванова Е. В. Профилактика интернет-зависимости у младших школьников / Е. В. Иванова // Начальная школа. – 2022. – № 3. – С. 42–47.

15. Киселёва Т. Г. Формирование информационной грамотности младших школьников в условиях цифровизации образования / Т. Г. Киселёва // Начальное образование. – 2021. – № 2. – С. 18–25.

16. Клочко В. Е. Цифровая социализация и психическое развитие детей и подростков / В. Е. Клочко, Э. В. Галажинский // Образование и наука. – 2019. – Т. 21. – № 8. – С. 11–29.

17. Кулагина, И. Ю. Психология развития и возрастная психология. Полный жизненный цикл развития человека : учебное пособие для вузов / И. Ю. Кулагина, В. Н. Колюцкий. – Москва : Академический проект, 2020. – 420 с. – ISBN 978-5-8291-2748-0.

18. Леонтьев А. Н. Деятельность. Сознание. Личность : учебное пособие / А. Н. Леонтьев. – Москва : Смысл ; Академия, 2005. – 352 с. – ISBN 5-89357-153-3.

19. Малкова И. Ю. Безопасность детей в интернете: педагогические стратегии / И. Ю. Малкова, Е. А. Дорофеева // Вестник Томского государственного университета. – 2020. – № 459. – С. 201–209.

20. Мудрик А. В. Социализация человека : учебное пособие / А. В. Мудрик. – Москва : Изд-во МПСИ ; Воронеж : Изд-во НПО «МОДЭК», 2011. – 624 с. – ISBN 978-5-9770-0511-1.

21. Нассонова Е. С. Методы и приемы обучения кибербезопасности детей младшего школьного возраста / Е. С. Нассонова // Современный урок : портал педагога. — 2025. — URL: https://www.1urok.ru/categories/10/articles/106815 (дата обращения: 20.04.2026).

22. Никитина Л. Н. Развитие критического мышления младших школьников в условиях медианасыщенной среды / Л. Н. Никитина // Начальная школа плюс До и После. – 2021. – № 7. – С. 35–41.

23. Овчарова Р. В. Психология родительства : учебное пособие / Р. В. Овчарова. – Москва : Академия, 2005. – 368 с. – ISBN 5-7695-1916-9.

24. Пайцева Д. Н. Кибербезопасность и цифровая гигиена младшего школьника: методика формирования безопасного поведения в сети / Д. Н. Пайцева // Фонд «Эверест» : учебно-методические материалы. — 2025.— URL: https://everest-edu.ru/ap-6624/ (дата обращения: 20.04.2026).

25. Плешаков В. А. Киберсоциализация: социальное развитие и социальное воспитание современного человека / В. А. Плешаков // Вестник Костромского государственного университета. Серия: Педагогика. Психология. – 2018. – № 1. – С. 15–18.

26. Поливанова К. Н. Современное детство: реалии и перспективы / К. Н. Поливанова // Образовательная политика. – 2019. – № 3. – С. 22–29.

27. Психология безопасности : учебник для вузов / А. И. Донцов, Ю. П. Зинченко, О. Ю. Зотова, Е. Б. Перелыгина. – 2-е изд. – Москва : Юрайт, 2026. – 165 с. – ISBN 978-5-534-21603-5.

28. Психология развития : учебник / Т. Д. Марцинковская, Т. М. Марютина, Т. Г. Стефаненко и др. ; под ред. Т. Д. Марцинковской. – 3-е изд, стер. – Москва : Академия, 2007. 528 с. – ISBN 978-5-7695-4471-2.

29. Роберт И. В. Развитие информатизации образования на основе цифровых технологий / И. В. Роберт // Педагогическая информатика. – 2019. – № 2. – С. 108–126.

30. Рубцов В. В. Цифровые технологии в образовании: психологический контекст / В. В. Рубцов, Т. М. Марютина, Т. А. Нестик // Психолого-педагогические исследования. – 2020. – Т. 12. – № 4. – С. 3–20.

31. Рычкова Л. С. Профилактика кибербуллинга в школьной среде / Л. С. Рычкова, Ю. С. Богданова // Вестник практической психологии образования. – 2020. – № 3. – С. 48–56.

32. Семёнова Т. В. Цифровая грамотность педагога: определение и механизмы развития / Т. В. Семёнова, К. А. Вилкова // Высшее образование в России. – 2021. – Т. 30. – № 2. – С. 47–63.

33. Собкин В. С. Младший школьник в цифровом мире / В. С. Собкин, О. В. Калашникова // Современное дошкольное образование. – 2022. – № 3. – С. 22–34.

34. Собкин В. С. Подростковый интернет: информационная безопасность и социальные риски / В. С. Собкин, А. Н. Федотова // Вестник практической психологии образования. – 2019. – № 4. – С. 7–18.

35. Солдатова Г. У. Рожденные цифровыми: семейный контекст и когнитивное развитие / Г. У. Солдатова, Е. И. Рассказова, А. Е. Вишнева, О. И. Теславская, С. В. Чигарькова. – Москва : Акрополь, 2022. – 356 с. – ISBN 978-5-98807-102-0.

36. Солдатова Г. У. Цифровая компетентность российских педагогов / Г. У. Солдатова, Е. И. Рассказова // Психологическая наука и образование. – 2020. – Т. 25. – № 4. – С. 5–18.

37. Солдатова Г. У. Цифровое детство: новые риски и новые возможности / Г. У. Солдатова, Е. И. Рассказова, Т. А. Нестик // Вестник практической психологии образования. – 2021. – № 1. – С. 8–19.

Феденкина, А. А. Особенности психического развития детей и подростков в условиях цифровизации общества / А. А. Феденкина, Л. А. Регуш, О. С. Гаврилова // Психология и право. – 2025. – Т. 15. – № 3. – С. 135–150.

38. Федоров А. В. Медиаобразование и медиаграмотность : учебное пособие для вузов / А. В. Федоров. – Москва : Директ-Медиа, 2013. – 342 с. ISBN 978-5-4458-3384-0.

39. Федоров А. В. Медиаобразование: социологические опросы / А. В. Федоров. – Таганрог : Кучма, 2007. – 228 с. – ISBN 978-5-98517-054-2.

40. Фельдштейн Д. И. Психология развития человека как личности : избранные труды : в 2 томах / Д. И. Фельдштейн. – Москва : Изд-во МПСИ ; Воронеж : НПО «МОДЭК», 2005. – 568 с. – ISBN 5-89502-698-2.

41. Хуторской А. В. Цифровая дидактика: вызовы времени / А. В. Хуторской // Народное образование. – 2021. – № 6. – С. 113–121.

42. Шаров А. С. Психология культуры, образования и развития человека : учебное пособие / А. С. Шаров. – Омск : Изд-во ОмГПУ, 2013. – 300 с. – ISBN: 978-5-8268-1782-7

Приложение А

Анкета для младших школьников «Что я знаю о безопасности в интернете»

Цель: диагностика уровня сформированности знаний младших школьников о правилах безопасного поведения в интернете, типах киберугроз и способах защиты.

Возраст: 7–11 лет (1–4 класс)

Форма проведения: индивидуальное или групповое анкетирование

Время проведения: 20–25 минут

1. Можно ли сообщать незнакомым людям в интернете свой домашний адрес и номер телефона?

☐ Да, можно всегда

☐ Нет, нельзя никогда

☐ Можно, если человек кажется хорошим

☐ Не знаю

2. Какой из этих паролей самый надёжный?

☐ 123456

☐ мояфамилия

☐ Qw7!pLm#9Zx

☐ датамоегорождения

3. Ты зарегистрировался на новом сайте. Какую информацию безопасно указывать о себе?

☐ Настоящее имя и фамилию

☐ Ник (выдуманное имя)

☐ Адрес школы

☐ Номер телефона родителей

☐ Фотографию своего дома

4. Что нужно делать, если кто-то в интернете тебя обижает, пишет неприятные сообщения?

☐ Ответить ему тем же

☐ Рассказать взрослым (родителям, учителю)

☐ Заблокировать этого человека

☐ Ничего не делать, само пройдёт

☐ Удалить свою страницу в соцсети

5. Твой друг попросил тебя сообщить пароль от твоего аккаунта в игре или в соцсети. Как ты поступишь?

☐ Скажу пароль, ведь это мой друг

☐ Не скажу, потому что пароль–это секрет

☐ Скажу, но попрошу никому не рассказывать

☐ Спрошу у родителей, можно ли это делать

6. ОТКРЫТЫЙ ВОПРОС: Если ты увидишь, что кого-то из одноклассников обижают в интернете (пишут плохие комментарии, насмехаются), что ты сделаешь? _____

7. Тебе пришло письмо от неизвестного отправителя: «Поздравляем! Ты выиграл новый телефон! Перейди по ссылке и забери приз». Что ты сделаешь?

☐ Сразу перейду по ссылке–я хочу получить приз!

☐ Покажу письмо родителям

☐ Удалю письмо, не открывая ссылку

☐ Напишу ответ и спрошу, правда ли это

8. Можно ли переходить по ссылкам в сообщениях от незнакомых людей?

☐ Да, если ссылка интересная

☐ Нет, это может быть опасно

☐ Можно, если есть антивирус

☐ Не знаю

9. Что из перечисленного может быть опасным в интернете? (Можно выбрать несколько вариантов)

☐ Вирусы и вредоносные программы

☐ Люди, которые притворяются детьми

☐ Сайты с неправдивой информацией

☐ Видео с жестокостью и насилием

☐ Реклама, которая обманывает

☐ Мошенники, которые хотят украсть деньги

☐ Ничего из перечисленного

10. Ты нашёл в интернете информацию для доклада по окружающему миру. Как проверить, правда ли это?

☐ Если написано в интернете, значит, правда

☐ Посмотреть информацию на других сайтах

☐ Спросить у учителя или родителей

☐ Проверить, кто автор информации

☐ Не нужно проверять

11. Твой друг прислал тебе смешную картинку с фотографией одноклассника и подписью, которая его высмеивает. Что ты сделаешь?

☐ Посмеюсь и отправлю другим

☐ Скажу другу, что так делать нехорошо

☐ Ничего не сделаю

☐ Расскажу учителю или родителям

12. Сколько времени в день можно проводить в интернете младшему школьнику без вреда для здоровья?

☐ Сколько хочется

☐ Не больше 1–1,5 часа

☐ 5–6 часов

☐ Не знаю

13. Что нужно делать, чтобы интернет был безопасным для тебя? (Можно выбрать несколько вариантов)

☐ Использовать сложные пароли

☐ Не общаться с незнакомцами

☐ Не открывать странные ссылки и файлы

☐ Рассказывать родителям, что я делаю онлайн

☐ Установить антивирус

☐ Быть вежливым в общении

14. ОТКРЫТЫЙ ВОПРОС: Для чего тебе нужен интернет? Напиши три главные причины.

1), 2), 3)

_____

15. ОТКРЫТЫЙ ВОПРОС: Что такое «кибербуллинг»? Объясни своими словами.

_____

16. ОТКРЫТЫЙ ВОПРОС: Представь, что твой младший брат или сестра впервые заходит в интернет. Какие три правила безопасности ты ему посоветуешь?

1), 2), 3)

_____

Приложение Б

Тест-опросник для родителей «цифровая безопасность моего ребёнка»

Цель: оценка уровня осведомлённости родителей о цифровой активности ребёнка, выявление зон риска и степени родительского контроля.

Форма проведения: индивидуальное анкетирование

Время проведения: 15–20 минут

1. Есть ли у вашего ребёнка доступ к интернету?

☐ Да, постоянный

☐ Да, но ограниченный по времени

☐ Только под присмотром взрослых

☐ Нет

2. С каких устройств ребёнок выходит в интернет? (можно выбрать несколько вариантов)

☐ Смартфон

☐ Планшет

☐ Компьютер/ноутбук

☐ Игровая приставка

☐ Умные часы

☐ Телевизор (Smart TV)

☐ Другое: _____

3. Сколько времени в день ребёнок проводит в интернете?

☐ Менее 30 минут

☐ 30 минут – 1 час

☐ 1–2 часа

☐ 2–3 часа

☐ Более 3 часов

☐ Затрудняюсь ответить

4. Чем ребёнок чаще всего занимается в интернете? (можно выбрать несколько вариантов)

☐ Онлайн-игры

☐ Просмотр видео (YouTube, TikTok и т.п.)

☐ Общение в мессенджерах и соцсетях

☐ Поиск информации для учёбы

☐ Образовательные платформы

☐ Прослушивание музыки

☐ Другое: _____

5. Знаете ли вы пароли от аккаунтов вашего ребёнка?

☐ Да, от всех

☐ Да, от некоторых

☐ Нет

☐ У ребёнка нет аккаунтов

6. Используете ли вы технические средства родительского контроля?

☐ Да, регулярно (фильтры контента, ограничение времени, мониторинг активности)

☐ Да, но не всегда

☐ Нет, не использую

☐ Не знаю, как это сделать

7. Обсуждаете ли вы с ребёнком правила безопасности в интернете?

☐ Да, регулярно

☐ Да, но редко

☐ Нет, не обсуждаем

☐ Ребёнок ещё слишком мал для этого

8. Знаете ли вы, с кем ваш ребёнок общается в интернете?

☐ Да, знаю всех

☐ Знаю некоторых

☐ Не знаю

☐ Ребёнок не общается в интернете

9. Рассказывает ли ребёнок вам о своей активности в интернете?

☐ Да, всегда делится

☐ Иногда рассказывает

☐ Редко делится

☐ Не рассказывает совсем

☐ Затрудняюсь ответить

10. Какие из перечисленных угроз в интернете вам известны? (можно выбрать несколько вариантов)

☐ Кибербуллинг (травля в интернете)

☐ Груминг (онлайн-соблазнение детей)

☐ Фишинг (кража данных через поддельные сайты)

☐ Вирусы и вредоносное ПО

☐ Интернет-мошенничество

☐ Нежелательный контент (насилие, порнография)

☐ Игромания и интернет-зависимость

☐ Кража личных данных

☐ Затрудняюсь ответить

11. Сталкивался ли ваш ребёнок с какими-либо проблемами или неприятными ситуациями в интернете?

☐ Да (опишите кратко): _____

☐ Нет

☐ Не знаю

12. Считаете ли вы себя достаточно компетентным, чтобы научить ребёнка безопасному поведению в интернете?

☐ Да, полностью

☐ Скорее да, чем нет

☐ Скорее нет, чем да

☐ Нет, мне самому нужна помощь

13. Нужна ли вам помощь школы в вопросах обеспечения цифровой безопасности ребёнка?

☐ Да, очень нужна

☐ Скорее да

☐ Скорее нет

☐ Нет, справляемся сами

14. В какой форме вы хотели бы получать информацию о кибербезопасности? (можно выбрать несколько вариантов)

☐ Родительские собрания

☐ Индивидуальные консультации

☐ Памятки и буклеты

☐ Онлайн-вебинары

☐ Статьи на сайте школы

☐ Мессенджеры (группы, рассылки)

☐ Другое: _____

15. Какие темы по кибербезопасности вас интересуют больше всего? (можно выбрать несколько вариантов)

☐ Настройка родительского контроля

☐ Защита от кибербуллинга

☐ Распознавание интернет-мошенничества

☐ Профилактика интернет-зависимости

☐ Возрастные особенности безопасного использования интернета

☐ Защита личных данных ребёнка

☐ Цифровая грамотность и критическое мышление

☐ Другое: _____

Приложение В

Анкета для педагогов «Готовность к формированию основ кибербезопасности у младших школьников»

Цель: диагностика уровня готовности учителей начальных классов к формированию основ кибербезопасности у младших школьников, выявление профессиональных дефицитов и образовательных потребностей в области цифровой безопасности.

Целевая аудитория: учителя начальных классов, педагоги дополнительного образования, работающие с детьми 7–11 лет

Форма проведения: индивидуальное анкетирование

Время проведения: 25–30 минут

1. Ваш педагогический стаж:

☐ До 3 лет

☐ 3–5 лет

☐ 6–10 лет

☐ 11–20 лет

☐ Более 20 лет

2. В каких классах Вы преподаёте в настоящее время? (можно выбрать несколько вариантов)

☐ 1 класс

☐ 2 класс

☐ 3 класс

☐ 4 класс

☐ Веду внеурочную деятельность

☐ Другое: _____

3. Проходили ли Вы за последние 3 года курсы повышения квалификации по направлению «Информационная безопасность» или «Кибербезопасность»?

☐ Да, проходил(а) целевые курсы по кибербезопасности (укажите объём программы: _____ часов)

☐ Да, данная тема частично рассматривалась в рамках других курсов

☐ Нет, не проходил(а)

☐ Планирую пройти в ближайшее время

4. Как часто Вы используете цифровые технологии и интернет-ресурсы в своей профессиональной деятельности?

☐ Ежедневно

☐ Несколько раз в неделю

☐ Несколько раз в месяц

☐ Редко (несколько раз в четверть)

☐ Практически не использую

5. Какие цифровые инструменты и сервисы Вы регулярно применяете в работе с младшими школьниками? (можно выбрать несколько вариантов)

☐ Интерактивная доска, мультимедийные презентации

☐ Образовательные платформы (Учи.ру, Яндекс.Учебник, РЭШ и др.)

☐ Онлайн-тестирование и опросы (Google Формы, Kahoot и др.)

☐ Видеоконференции и дистанционное обучение (Zoom, Teams и др.)

☐ Электронный журнал и дневник

☐ Мессенджеры для общения с родителями (Max и др.)

☐ Образовательные видеоматериалы (YouTube и др.)

☐ Другое: _____

☐ Не использую цифровые инструменты

6. Оцените свой уровень владения цифровыми технологиями:

☐ Высокий (уверенно использую разнообразные цифровые инструменты, осваиваю новые сервисы самостоятельно)

☐ Средний (использую базовые инструменты, при освоении новых иногда требуется помощь)

☐ Базовый (использую только самые простые функции, часто требуется методическая поддержка)

☐ Низкий (испытываю значительные затруднения при работе с цифровыми технологиями)

7. Сталкивались ли Вы лично или Ваши ученики с проблемами кибербезопасности? (можно выбрать несколько вариантов)

☐ Да, мои ученики сталкивались с кибербуллингом (травлей в интернете)

☐ Да, ученики получали сообщения от незнакомцев с подозрительным содержанием

☐ Да, сталкивались с вирусами или вредоносным ПО на школьных устройствах

☐ Да, ученики попадали на сайты с нежелательным контентом

☐ Да, были случаи утечки личной информации учащихся

☐ Да, я лично сталкивался(лась) с попытками мошенничества или фишинга

☐ Нет, таких ситуаций не было

☐ Затрудняюсь ответить

8. Какие из перечисленных мер защиты детей в интернете Вы считаете наиболее эффективными для младших школьников? (выберите не более 5 вариантов)

☐ Использование родительского контроля и фильтров контента

☐ Систематическое обучение детей правилам кибербезопасности

☐ Ограничение времени использования интернета

☐ Контроль со стороны взрослых за онлайн-активностью ребёнка

☐ Формирование критического мышления и медиаграмотности

☐ Доверительные отношения, при которых ребёнок делится с взрослыми своим онлайн-опытом

☐ Использование безопасных детских браузеров и поисковых систем

☐ Обучение цифровой этике и культуре общения в сети

☐ Антивирусные программы и технические средства защиты

☐ Запрет использования социальных сетей до определённого возраста

☐ Другое: _____

9. ОТКРЫТЫЙ ВОПРОС: Какие, на Ваш взгляд, киберугрозы представляют наибольшую опасность для современных младших школьников? (напишите 2–3 наиболее значимые)

1), 2), 3)

_____

10. Включаете ли Вы в содержание своих уроков или внеурочной деятельности вопросы кибербезопасности и безопасного поведения в интернете?

☐ Да, регулярно (не реже 1 раза в месяц)

☐ Да, периодически (несколько раз в четверть)

☐ Да, эпизодически (1–2 раза в год)

☐ Нет, но планирую начать

☐ Нет, не включаю

11. Если Вы включаете тематику кибербезопасности в образовательный процесс, то в рамках каких форм работы? (можно выбрать несколько вариантов)

☐ Классные часы и воспитательные беседы

☐ Интеграция в уроки информатики

☐ Интеграция в уроки окружающего мира

☐ Внеурочная деятельность (кружки, факультативы)

☐ Проектная и исследовательская деятельность учащихся

☐ Работа с родителями (родительские собрания, консультации)

☐ Участие в тематических акциях и конкурсах (например, «Неделя безопасного Рунета»)

☐ Другое: _____

☐ Не включаю данную тематику

12. Какие методы и формы работы Вы используете при обучении младших школьников основам кибербезопасности? (можно выбрать несколько вариантов)

☐ Беседы и объяснения

☐ Просмотр и обсуждение обучающих видеороликов, мультфильмов

☐ Игровые формы (ролевые игры, квесты, викторины)

☐ Решение ситуативных задач (кейсов)

☐ Создание памяток, плакатов, инфографики

☐ Моделирование ситуаций и тренинги

☐ Работа с интерактивными онлайн-ресурсами и тренажёрами

☐ Проектная деятельность

☐ Приглашение специалистов (психологов, сотрудников правоохранительных органов)

☐ Другое: _____

☐ Не использую

13. Используете ли Вы готовые учебно-методические материалы по кибербезопасности?

☐ Да, регулярно использую готовые программы и разработки

☐ Да, иногда использую отдельные материалы, адаптируя их

☐ Разрабатываю собственные материалы

☐ Комбинирую готовые и авторские разработки

☐ Нет, не использую, так как не знаю, где найти качественные материалы

☐ Нет, не использую по другим причинам (укажите):

_____

14. ОТКРЫТЫЙ ВОПРОС: Приведите пример успешного опыта интеграции тематики кибербезопасности в Вашу педагогическую практику (урок, мероприятие, проект). Если такого опыта нет, напишите «Нет опыта».

_____

15. Испытываете ли Вы потребность в повышении квалификации по направлению «Формирование основ кибербезопасности у младших школьников»?

☐ Да, испытываю острую потребность

☐ Скорее да, чем нет

☐ Затрудняюсь ответить

☐ Скорее нет, чем да

☐ Нет, не испытываю

16. Какие формы повышения квалификации по данной теме были бы для Вас наиболее предпочтительны? (выберите не более 3 вариантов)

☐ Курсы повышения квалификации (72–144 часа) с выдачей удостоверения

☐ Краткосрочные семинары и вебинары (8–16 часов)

☐ Методические мастер-классы и практикумы

☐ Онлайн-курсы и дистанционное обучение

☐ Самообразование с использованием методической литературы и интернет-ресурсов

☐ Участие в профессиональных сообществах и обмен опытом с коллегами

☐ Индивидуальные консультации специалистов

☐ Стажировка в образовательных организациях с успешным опытом

☐ Другое: _____

17. Какие конкретно темы в рамках повышения квалификации по кибербезопасности были бы для Вас наиболее актуальны? (выберите не более 5 вариантов)

☐ Современные киберугрозы для детей младшего школьного возраста

☐ Психологические аспекты цифровой социализации младших школьников

☐ Методика обучения детей безопасному поведению в интернете

☐ Разработка программ и занятий по кибербезопасности для начальной школы

☐ Диагностика уровня сформированности основ кибербезопасности у детей

☐ Использование игровых и интерактивных методов обучения кибербезопасности

☐ Работа с родителями по вопросам цифровой безопасности детей

☐ Профилактика и коррекция кибербуллинга в младшем школьном возрасте

☐ Формирование критического мышления и медиаграмотности у младших школьников

☐ Правовые аспекты кибербезопасности и защиты персональных данных

☐ Технические средства защиты детей в интернете (родительский контроль, фильтры)

☐ Цифровая этика и культура онлайн-общения

☐ Профилактика интернет-зависимости у младших школьников

☐ Другое: _____

18. Кто, на Ваш взгляд, должен нести основную ответственность за обучение младших школьников безопасному поведению в интернете?

☐ Родители

☐ Школа (учителя)

☐ Специалисты (психологи, социальные педагоги)

☐ Государственные структуры и IT-компании

☐ Ответственность должна быть общей и распределённой

☐ Другое: _____