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

«Педагогика и психология начального образования»

Форма обучения очная

Проверка на объем заимствований:
75,76 % авторского текста
Работа рекомендована к защите
« 26 » мая 2025 г.
зав. кафедрой ТМиМНО
_____ Волчегорская Евгения Юрьевна

Выполнила:
Студентка группы ОФ-221-151-2-1
Куксова Анастасия Игоревна

Научный руководитель:
кан. пед. наук, доцент
Жукова Марина Владимировна

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современное общество находится в состоянии стремительной трансформации, обусловленной внедрением цифровых технологий, которые оказывают глубокое воздействие на все сферы жизни человека, включая сферы образования, коммуникации и досуга. Активно взаимодействуя с широким спектром электронных устройств, подрастающее поколение становится частью цифрового пространства, где открываются возможности для активного обучения, поиска развлекательного контента, виртуального общения и самовыражения. Но вместе с тем, наряду с новыми возможностями, возникают и угрозы: психологическое давление и агрессия; действия мошеннического характера, направленные на получение конфиденциальной информации и кражу персональных данных; потенциальный контакт с нежелательным и опасным контентом.

По данным исследования «Лаборатории Касперского» на 2023 год, 92 % опрошенных детей в возрасте от трёх до шести лет, имеют в своем пользовании не только электронные устройства (телефон, компьютер и т.д.), но и доступ к сети Интернет. Для сравнения, в 2022 году доля этого показателя составляла 83 % [33]. В начальной школе, по состоянию на 2023 год, почти 89 % обучающихся имеют собственные смартфоны или планшеты [16].

Примечательно, что более половины опрошенных детей скрывают от родителей продолжительность пребывания в сети (60 %) и посещаемые ими сайты (55 %). Каждый третий (35 %) не делится, каких видеоблогеров он смотрит, а каждый пятый умалчивает от взрослых факт просмотра фильмов или сериалов, которые не предназначены для их возраста [16].

Среди опрошенных 74 % признали, что получали запросы-приглашения в друзья от незнакомцев, 20 % детей сообщают, что пожалели о публикации своей личной информации в социальных сетях. Почти треть

детей (27 %) отметили, что столкнулись с кибербуллингом в качестве свидетеля, жертвы или участника.

58 % детей в возрасте 7-12 лет сталкивались с онлайн-угрозами, при этом лишь треть (30 %) родителей уверены в цифровой грамотности своего ребёнка [16].

Проанализировав данную статистику, становится очевидно, что происходят деструктивные изменения в обществе: появление ошибочных ценностей, искажение духовности личности и нравственных норм. Надежное сопровождение детей, уязвимых большим потоком разнообразной информацию, станет залогом для формирования правильных этических представлений и успешной социализации.

Повышение степени личностной зрелости, содействие готовности к самореализации в обществе, а также качественное образование помогут преодолеть сложившуюся ситуацию. В свете этого возникает острая необходимость расширения образовательного пространства, особенно в начальном общем образовании. Это расширение должно включать добавление новых элементов, таких как основы кибербезопасности, которые помогут подрастающему поколению безопасно исследовать современное информационное пространство, но и защищать себя от потенциальных угроз.

Обучение детей базовым правилам безопасности в Интернете должно опираться на систематическую работу педагогов, которые выступают в роли наставников данного вопроса. В частности, внедряются школьные программы различной направленности – коррекционные, диагностические, а также программы психолого-педагогического сопровождения.

Работу по формированию осознанной и безопасной информационной культе необходимо выстраивать не только с обучающимися, но и с родителями, а также сотрудниками образовательного процесса.

Таким образом формирование основ кибербезопасности у младших школьников является актуальной проблемой, на которую нужно обратить

пристальное внимание и искать пути её решения. В начальной школе педагог-психолог способен организовать свою деятельность для помощи безопасной цифровой социализации школьника, обучая его противостоять информационным угрозам и отделять надежные и опасные онлайн-источники в интернет-среде.

Принимая во внимание это, следует, что педагог-психолог должен быть хорошо осведомлён о вопросах кибербезопасности и уметь адаптировать сложные понятия, например, такие как «информационная безопасность», «сетевой этикет», «кибербуллинг», для восприятия их детьми 7-12 лет. Традиционные методы обучения кибербезопасности также требуют переработки для когнитивного развития младших школьников с учетом их особенностей – наглядно-образного мышления, потребности в игровых формах, ограниченного объема концентрации внимания в учебное время и т. д.

В своих трудах проблеме защиты информации личности, формированию понятий «кибербезопасность», «информационная безопасность личности» уделяли внимание Т. В. Воробьева, Н. И. Гендина, Н. В. Гутова, Л. С. Зазнобина, Л. В. Крапивская, Т. А. Малых [38], А. А. Малюк, Д. С. Синицын [55], психологи Г. В. Грачев [21], К. Н. Дудкина, Б. Ф. Ломова, и др.

О кибербезопасности в цифровой образовательной среде, в том числе в системе начального общего образования, в своих работах указывали М. И. Бачаров [13], Е. Г. Белякова[32], А. И. Березенцева [32], А. Ю. Буров, В. Е. Быков, Э. В. Загвязинская[32], Н. Н. Паньгина, Н. И. Саттарова [38], Г. А. Цукерман и др.

Изучив труды по теме кибербезопасности в цифровой образовательной среде, мы выделили актуальность нашего исследования на трех уровнях:

– социальный уровень: работы обусловлена социальными запросами. В Российской Федерации принят ряд документов, которые направлены на

обеспечение различных аспектов национальной кибербезопасности: Доктрина информационной безопасности Российской Федерации; Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; другие документы, направленные на развитие ответственного цифрового гражданина, у которого формируется уважение к приватности, критическое мышление и этичное поведение в сети;

– практический уровень: работа обусловлена необходимостью создания программы работы педагога-психолога по формированию основ кибербезопасности у младших школьников. Также важна возможность использования полученного материала в работе педагогов-психологов при разработке программ по схожей проблеме и в целом – использование программы в образовательных учреждениях.

Проблема исследования: каково содержание программы работы педагога-психолога по формирования основ кибербезопасности у младших школьников?

В связи с актуальностью данного вопроса и выявленной проблемой мы сформулировали тему нашей работы «Работа педагога-психолога по формированию основ кибербезопасности у младших школьников».

Цель исследования: теоретически обосновать и разработать программу работы педагога-психолога по формированию основ кибербезопасности у младших школьников и дорожную карту её продвижения.

Объект исследования: процесс формирования основ кибербезопасности у младших школьников.

Предмет исследования: работа педагога-психолога по формированию основ кибербезопасности у младших школьников.

Для достижения поставленной цели были выделены следующие задачи исследования:

1. Изучить понятия «кибербезопасность», «информационная безопасность».

2. Рассмотреть особенности развития младшего школьника в процессе формирования основ кибербезопасности.

3. Выявить направления работы педагога-психолога по формированию основ кибербезопасности у младших школьников.

4. Проанализировать результаты изучения уровня сформированности основ киберобезопасности у младших школьников.

5. Осуществить анализ существующих программ по формированию основ кибербезопасности в предпроектном исследовании.

6. Разработать программу работы педагога-психолога по формирование основ кибербезопасности у младших школьников и дорожную карту её реализации.

Методологическая основа исследования:

Системно-деятельностный подход (Б. Г. Ананьев, В. Г. Афанасьев, Б. Ф. Ломов, Л. С. Выготский, Л. В. Занков, А. Р. Лурия, Д. Б. Эльконин, В. В. Давыдов), позволивший выявить взаимосвязь и структуру понятий «кибербезопасность» и «информационная безопасность», а также рассмотреть кибербезопасность младших школьников как современное общественно-значимое социальное явление.

Личностно-ориентированный подход (Ш. А. Амонашвили, В. П. Бедерханова, Е. В. Бондаревская, М. А. Викулина, Т. Ф. Иванов, М. Е. Кузнецов, М. И. Лукьянова, В. В. Сериков, В. А. Сластенин, Е. Н. Степанов, В. В. Шоган, И. С. Якиманская и др.), позволивший определить содержание программы работы педагога-психолога по формированию основ кибербезопасности в начальной школе с учетом возрастных и личностных особенностей обучающихся.

Аксиологический подход (Л. В. Блинов, А. М. Булынин, Л. В. Вершинина, Д. А. Горбачева, М. Г. Казакина, А. В. Кирьякова, И. С. Ломакина, З. И. Равкин, А. А. Ручки , В. А. Сластенин, В. П. Тугаринов

и др.), позволивший посредством работы педагога-психолога определить, как младшие школьники усваивают социальные знания о возможностях и рисках Интернета, общественных правилах поведения в сети, о приемлемых и неприемлемых формах взаимодействия, а также начальные представления о виртуальной реальности.

В нашей работе были применены следующие методы исследования: анализ и изучение психолого-педагогической литературы, проведение SWOT-анализа, тестирование, математическая обработка и интерпретации результатов (использование диаграмм и таблиц).

Практическая значимость исследования: разработанной нами программой и дорожной картой могут пользоваться педагоги-психологи, и учителя начальных классов для работы по формированию основ кибербезопасности у младших школьников.

База исследования: общеобразовательная школа г. Челябинска. В исследовании приняли участие 52 обучающихся в возрасте 10-11 лет.

Этапы исследования:

На первом этапе (2023 г.) осуществлялся выбор темы исследования, изучение степени разработки проблемы в психолого-педагогической литературе, анализ ключевых понятий и формулировка методологических основ, подбор методического инструментария.

На втором этапе (2024 г.) проводилось предпроектное исследование: поиск, обоснование и выбор проектной идеи, определение выборки и подбор диагностических материалов, описание критериев и показателей, а также обработка, анализ и интерпретация полученных данных.

На третьем этапе (2025 г.) осуществлялась разработка программы работы педагога-психолога по формированию основ кибербезопасности, описание технологии внедрения программы, а также формулировка общих выводов исследования.

Результаты исследования нашли отражение в публикациях:

1. Куксова А. И. Как педагог-психолог помогает младшим школьникам стать ответственными пользователями интернета: основы кибербезопасности / А. И. Куксова // Научное сообщество студентов XXI столетия. Гуманитарные науки: сб. ст. по мат. CXXXIX междунар. студ. студ. науч.-практ. конф. – Новосибирск: СибАК. – 2024. – № 2 (204) – С. 58–62. – URL: https://sibac.info/archive/guman/7(139).pdf (дата обращения: 26.01.2025).

2. Куксова А. И. Результаты исследования по формированию основ кибербезопасности младших школьников / А. И. Куксова // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. CCV междунар. студ. науч.-практ. конф. – Новосибирск: СибАК. – 2025. – № 2 (204) – С. 112–117. – URL: https://sibac.info/archive/meghdis/2(204).pdf (дата обращения: 20.02.2025).

3. Куксова А. И. Необходимость разработки программы внеурочной деятельности по формированию основ кибербезопасности для младших школьников: опыт педагогов-психологов / А. И. Куксова // Научное сообщество студентов XXI столетия. Гуманитарные науки: сб. ст. по мат. CXLVIII междунар. студ. науч.-практ. конф. – Новосибирск: СибАК. –2025. – № 4 (147) – URL: https://sibac.info/archive/guman/4(147).pdf (дата обращения: 15.04.2025).

В участии автора в конференциях по теме исследования:

1. 205 Международная научно-практическая конференция «Научное сообщество студентов: Междисциплинарные исследования» (30 января 2025 года), г. Новосибирск.

2. 148 Международная научно-практическая конференция «Научное сообщество студентов XXI столетия. Гуманитарные науки» (17 апреля 2025 г.), г. Новосибирск.

Структура работы: выпускная квалификационная работы состоит из введения, двух глав, выводов по главам, заключения, списка использованных источников, приложений. Работа представлена на 117

страницах, в тексте 12 таблиц и 6 рисунков, Список использованных источников состоит из 61 наименования.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАБОТЫ ПЕДАГОГА-ПСИХОЛОГА ПО ФОРМИРОВАНИЮ ОСНОВ КИБЕРБЕЗОПАСНОСТИ У МЛАДШИХ ШКОЛЬНИКОВ

1.1 Сущность понятий «кибербезопасность», «информационная безопасность»

В эпоху, отмеченную стремительным развитием сферы информационных технологий, проблемы безопасности в киберпространстве становятся особенно актуальными. С одной стороны, Интернет, являясь всемирной сетью и частью киберпространства, предоставляет современным пользователям любых возрастов возможность передачи файлов и пересылки электронных писем; кроме того, интернет-среда обеспечивает подключение к разнообразным устройствам и доступ к всевозможной информации, данным в удобных и быстрых для понимания форматах. С другой стороны, наблюдается увеличение негативного влияния информационно-телекоммуникационных сетей на подрастающее поколение [26].

В связи с этим приоритетной задачей в государственной политике многих развитых стран, включая Россию, становится решение вопросов, связанных с безопасным использованием интернет-пространства подростками и детьми, где сохраняется множество неразрешенных проблем. Возникает необходимость разработки эффективных механизмов защиты несовершеннолетних от вредоносного контента, что обуславливает актуальность совершенствования правового регулирования в сфере обеспечения безопасности молодежи [19].

В рамках современных научных исследований понятие «безопасность молодежи» в более широком понимании трактуется «как система, состоящая из множества компонентов, включающих социальные, экономические, психологические и правовые аспекты, которые в совокупности обеспечивают гармоничное развитие молодого поколения» и «как система, позволяющая успешно противостоять социальным и

индивидуальным угрозам, при этом целенаправленно реализуя основные социальные функции в качестве значимого ресурса и потенциала общества» [32].

Для предотвращения негативного информационного воздействия и для защиты детей и молодежи в правовой системе Российской Федерации разработаны и сформулированы нормативные и правовые документы [53]. Так, к таким документам, отражающим важные аспекты информационной и кибербезопасности, можно отнести:

– Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. Федеральных законов от 30.11.2024 № 438-ФЗ). В данном документе содержатся правовые нормы, определяющие порядок доступа к продукции СМИ, информационным Интернет-ресурсам на территории Российской Федерации. Согласно закону «информационная безопасность детей» – это «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [42]. Также в документе прописано, что «информация, причиняющая вред здоровью и (или) развитию детей, – информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом» [42].

– Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 (в ред. Федеральных законов от 26.12.2024 № 479-ФЗ), в которой уделяется особое внимание негативному влиянию деструктивной информации на подрастающее поколение, способствующему размыванию духовно-нравственных ценностей и национальных культурных ориентиров [44].

– Распоряжение Правительства Российской Федерации от 28.04.2023 № 1105-р «О концепции информационной безопасности детей в Российской

Федерации», главной целью которого выступает «развитие безопасного информационного пространства и защита российского общества от деструктивного информационно-психологического воздействия» [19].

– Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» (в ред. Федеральных законов от 26.12.2024 № 479-ФЗ), в рамках которого имеется комплекс ограничений при распространении рекламы, направленный на минимизацию негативного влияния на детскую аудиторию. В частности, закон предусматривает специальные меры защиты, призванные предотвратить злоупотребление доверием несовершеннолетних и защитить их от манипулятивного воздействия [19].

– Федеральный закон от 27.07.2006 № 152-ФЗ (в ред. Федеральных законов от 08.08.2024 № 233-ФЗ)) «О персональных данных».

– Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 1 декабря 2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021-2027 годы» и др [19].

Механизмы обеспечения безопасности несовершеннолетних в информационной сфере нашли отражение в ключевом документе международного уровня – Конвенции о правах ребенка (принятой Генеральной Ассамблеей Организации Объединённых Наций 20 ноября 1989 года). В данном документ установлены принципы обеспечения защиты несовершеннолетних от неблагоприятной информации, которое представляет угрозу для психологического благополучия и социализации ребенка. Согласно Конвенции статья 17, гласит о гарантии права на «доступ к информации, благоприятствующей их физическому и психическому гармоничному развитию» [15].

Однако, независимо от наличия обширной законодательной базы, сохраняются существенные пробелы, свидетельствующие о необходимости дальнейшего совершенствования правовых механизмов, регулирующих безопасности несовершеннолетних в информационной среде

Интернета [15].

Рассмотрим подробнее ключевые проблемы и причины, которые не обеспечивают информационную безопасности в России, и пути их решения:

– низкая активность в области информационно-просветительской деятельности, направленной на формирование навыков безопасного поведения в виртуальной среде (причина: недостаточный уровень цифровой грамотности среди детей и подростков). Проблема решается следующими путями: интеграция модулей по цифровой гигиене в общеобразовательные учебные планы для повышения информационной грамотности; разработка обучающий курс по основам кибербезопасности у несовершеннолетних.

– пассивность родителей в вопросе обеспечения кибербезопасности детей в виртуальной среде (причина: низкий уровень осведомлённости и интернет-грамотности среди взрослых). Проблема решается следующими путями: между участниками, которые обеспечивают кибербезопастность несовершеннолетних, должны определиться конкретные функции и обязанности в контексте защиты детей в виртуальной среде. Родительский контроль будет реализован в полной мере, если будет представлена необходимая информация и инструментарий для эффективных действий в детско-родительских отношениях. Взаимодействие законных представителей (родителей, опекунов), педагогов в целом должны поспособствовать безопасной и продуктивной эксплуатации детьми интернет-ресурсов, обеспечивая их защиту от различных рисков.

– дефицит специалистов, занимающихся вопросами кибер и информационной безопасности (причина: недостаток цифровой грамотности, сопротивление к новым цифровым технология). Проблема решается следующим путем: повышения квалификации в области развития информационной безопасности.

– ограниченное содержание образовательных программ в области развития кибербезопасности на профессионально-педагогическом уровне (причины: финансовые проблемы по внедрению современных решений в

кибербезопасности; устаревшие технологии и системы защиты; отсутсвие аудитов безопасности). Решить данную проблему можно следующими путями: разработать дидактические материалы; провести семинары, лекции, мастер-классы для преподавательского состава; внедрить дополнительные образовательные программы по кибербезопасности самих педагогов.

– отсутствие мер наказания за распространение материалов, которые влияют на правила и общественные нормы (в том числе пропаганды молодёжных суицидов в социальных сетях). (Причина: недостаточное финансирование из государственных средств для защиты от вредной информации, которая оказывает пагубное влияние на детей в сети и других медиа-ресурсах и многое другое). Решить данную проблему можно следующими путями: усовершенствовать законодательство в области киберпреступности; улучшить требования к владельцам цифровых платформ; проводить мониторинг рисков и их последствий в киберпространстве [19; 23; 58; 61].

Проанализировав данные проблемы, которые существуют в нашей стране, и пути их решения, мы решили изучить опыт зарубежных территорий.

Например, в Китае одной из значимых стратегий, направленных на защиту младших школьников, активно пользующихся Интернетом, используется метод повышения развития и осведомлённости несовершеннолетних. В 2016 году в КНР в силу вступил закон «О кибербезопасности» («Cyber security Law of the People’s Republic of China»). Закон гласит «приостанавливать деятельность лиц и организаций, ставящих в ситуацию опасности здоровье психики и физическое развитие детей» [29].

Активное внедрение интернет-технологий и повсеместное распространение информационно-коммуникационных систем привели к возникновению новых вызовов, которые требуют обеспечения их защиты, что обусловило формирование таких ключевых понятий, как «информационная безопасность» и «кибербезопасность». Предлагаем

рассмотреть сущность данных понятий подробнее. Для начала вспомним, что же подразумевается под информацией.

«Информация» (от лат. слова «informatioa» – разъяснение, высказывание, осведомлённость) в последние время слово стало приобретать статус научного термина. Ранее его воспринимали только как элемент языка, письма или коммуникации [8].

В современной терминологии «кибербезопасность» выступает ключевым направление в рамках обеспечения понятия «информационная безопасность», то есть первое понятие является частью второго. «Информационная безопасность» охватывает все аспекты безопасности информации и данных в широком контексте. А трактуя понятие «кибербезопасность» необходимо обращать внимание на защиту важных данных, в киберпространстве (электронные устройства; сервера и цифровые сети).

«Информационная безопасность личности» (информационно-психологическая безопасность) – это «состояние безопасности и защищенности, обеспечивающее возможность для личностного развития в условиях постоянного информационного обмена с окружающей средой и сохранения целостности личности как активного социального субъекта». Такую трактовку предлагает Г. В. Грачев – кандидат и доктор психологических наук [21].

Согласно определению кандидата педагогических наук, Н. И. Саттаровой понятие «информационная безопасность личности», рассматривается как «состояние защищенности её основных интересов, включая реализацию конституционных прав и свобод, но и укрепление личной безопасности, улучшение уровня качества жизни в физическом, духовном и интеллектуальном аспектах» [38].

Автор отмечает, что данные составляющие помогут создать надежный барьер, оберегающий нематериальные ценности человека – его творческие и интеллектуальные достижения – от деструктивного

воздействия киберпространства.

Определение Т. А. Малых (кандидат педагогических наук) гласит, что «информационная безопасность личности» это «состояние, при котором жизненно важные интересы человека находятся под надежной защитой. Это выражается в способности индивида обнаруживать и распознавать угрозы, связанные с информационным воздействием, а также компенсировать возможные негативные последствия такого воздействия» [38].

Существует проект Концепции стратегии кибербезопасности Российской Федерации, в котором отражены понятия «киберпространство» и «кибербезопасность». Предлагаем их рассмотреть.

«Киберпространство» представляет собой «динамически развивающаяся цифровая среда, формируемая в результате интеграции глобальных информационно-телекоммуникационных инфраструктур (включая интернет-сети) и различных форм социальных практик, реализуемых субъектами разного уровня – от отдельных граждан до институтов государственного управления».

«Кибербезопасность» это «совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [35].

Термин «кибербезопасность» – «свойство киберпространства (киберсистемы) противостоять намеренным и (или) ненамеренным угрозам, а также реагировать на них и восстанавливать после воздействия этих угроз» (Русско-американский словарь терминов и определений в сфере информационной безопасности) [54].

«Кибербезопасность» – «условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события вкиберпространстве, которые могли бы считаться не желательными» такую трактовку даёт А. С. Алпеев

(кандидат технических наук) [3].

Для формулирования собственного определения «кибербезопасность» и «кибербезопасность младших школьников, необходимо обратиться к понятию «безопасность» и выяснить, что под ним понимается.

«Безопасность» – это сложное явление, которое изучается специалистами, работающими в самых различных отраслях [53].

Изучив нормативные акты можно сказать, что «безопасность» рассматривается как «состояние защищенности основных интересов личности, общества и государственной системы от угроз, как внешних, так и внутренних».

В обществе принято говорить о том, что «безопасность – это «отсутствие опасности»; «отсутствие угрозы, обеспечение защиты от опасности». Под «безопасностью» понимается отсутствие возможности нанести ущерб субъекту или объекту [17].

В нашем исследования мы предлагаем понятие «кибербезопасность» трактовать как стратегическое состояние, по обеспечению защиты доступа к информации, защиты цифровых электронных устройств, а также защита интересов личности для минимизации негативных последствий информационного воздействия.

«Кибербезопасность младших школьников», в рамках нашего исследовании понимается как комплекс мер и стратегий, направленных на обеспечение безопасного и защищённого взаимодействия детей младшего школьного возраста с цифровыми технологиями и интернет-средой. Это включает в себя формирование у них навыков распознавания киберугроз, использование инструментов для защиты личности, а также обучение по обеспечению сетевого этикета в Интернете.

Поскольку, современные дети в повседневной деятельности пользуются Интернетом на данный момент возникает всё больше и больше ситуаций сталкновения их с киберугрозами и сопутствующими рисками. В

этой связи особую важность приобретает разработка эффективных образовательных и профилактических мер, направленных на минимизацию негативного воздействия киберугроз на подрастающее поколение.

Так значимость изучения понятия «кибербезопасность» в начальной школе будет заключатся в том, что ребенок младшего школьного возраста пользуется компьютером не только в учебных целях, но и для досуга и решения ключевых жизненных вопросов. Это определяет актуальность изучения понятия [14].

Младшие школьники, знакомясь с информацией в Интернете, сталкиваются с рядом опасностей:

– контентом, запрещенным в большинстве стран и представляющий собой опасность (материалы носят экстремистский характер). Например, такой контент пропагандирует идеи расовой ненависти, нацизма, терроризма, а также различные формы извращений и порнографию.

– контентом, ограниченным возрастными рамками, но который всё равно в открытом доступе (материалы предназначены для взрослой аудитории). Например, материалы сексуального характера (фотографии, фильмы, продукция для взрослых). К этой категории относятся также сайты, на которых распространяется и пропагандируется жестокость и насилие (к примеру, демонстрация оружий, сект).

– контентом, транслирующим суицидальные побуждения (включая киберсуицид – запрограммированное самоубийство) через опасные онлайн-платформы. А также к данному контенту можно отнести сайты, связанные с наркотическими веществами (пропаганда изготовления, употребления наркотических препаратов). Данные онлайн-платформы и сайты нарушают психическое и физическое здоровье.

Можно заключить, что подобный контент наносит непоправимый вред детской психике, способствует развитию аддикций разного характера, побуждает заинтересованных вступить в запрещенные группы. Ввести в заблуждение несовершеннолетних также яркие ссылки-реклама, которые

несут в себе риск нарваться на сомнительные онлайн-ресурсы [37].

Мы считаем, что необходимо с упором на культуру поведения в Интернете выстраивать в образовании детей мир цифрового взаимодействия. Эта идея заложена в проекте «Концепции стратегии кибербезопасности Российской Федерации», куда включен специальный курс по информационной безопасности [35].

Необходимо помнить, что доля детей, а также их семьи и педагоги постоянно сталкиваются с киберугрозами в повседневной жизни. Это понимание служит основой для развития у младших школьников навыков реагирования в ситуациях информационных угроз посредством их моделирования в учебной деятельности [30]. Следовательно, подобно тому, как в рамках школьной программы учат, как правильно держать ручку или соблюдению правил техники безопасности, необходимо обучить ребенка правильному взаимодействию с информацией.

Это обусловило конечную цель включения основ кибербезопасности в образовательные программы начальных классов – создание условий для формирования у детей понимания структуры и функционирования киберпространства, осознание существующих угроз, а также познания методов защиты личных данных в цифровой среде [12].

Чтобы создать условия для формирования у детей понимания структуры и киберпространства необходимо:

– ввести базовое понятие кибербезопасности, которое будет доступно для понимания детей младшего школьного возраста, через различные инструктивные материалы;

– способствовать формированию у обучающихся начальной школы навыков управления с киберугрозами через интерактивные игры либо с использованием специализированных тренажёров;

– разработать руководство по взаимодействию киберпространстве через систему прикладных задач у детей;

– создать, основываясь на обучающих и методических ресурсах,

кибербезопасное домашнее пространство [14].

Обусловленное созданием условий общества в значительной мере стремится обеспечить безопасное использование и работу технологий в киберпространстве. Особое внимание уделяется адаптации для младших школьников к этим технологиям, что способствует переходу на более высококачественный уровень. Большинство мнений указывает на то, что наше общество приближается к важному этапу трансформации, известному как информационное общество, и в более широком контексте оформившемуся как информационная цивилизация [5]. Можно сделать заключение, что обеспечение безопасной цифровой среды для пользователей, в частности младших школьников, играет ключевую роль в переходе общества к информационной цивилизации.

Проект внедрения информатизации, компьютеризации и цифровизации реализуется ещё с 2000-х годов, и не теряет своей приоритетности даже в контексте современного педагогического образования нашей страны [5].

За это время был накоплен ценный опыт в преподавании и обучении информационным технологиям, что позволило обучающимся приобрести минимальные умения к уровню их подготовки. Обучающиеся должны уметь: преобразовывать визуальные данные в словесные знаки и наоборот; находить необходимую информацию в разнообразных информационных источниках; ясно формулировать цели общения и определять характер информационных потоков; модифицировать форму, размер и знаковую систему информации с учётом потребностей целевой аудитории; находить ошибки в информации и предлагать решения для их исправления; анализировать информационные сообщения, акцентируя внимание на основных моментах и прочее[37].

Исследователи все больше подчеркивают важность детального изучения кибербезопасности, которая актуальна как для безопасности школьника на личном уровне, так и для общества и государства в целом,

судя по последним тенденциям [17].

Педагог Н. И. Саттарова в своём исследовании «Информационная безопасность школьников в образовательном учреждении» акцентирует внимание на важность безопасного интернет-взаимодействия для детей [38].

Ограничением её работы в вопросе информационной безопасности является то, что всё проводится только на уроках информатике, а предоставляемые полезные рекомендации для педагогов, учеников и родителей осуществляются только в рамках образовательного процесса.

Д. С. Синицына же исследовал, как сформировать у подростков способность защищать себя от негативных информационных воздействий в рамках психолого-педагогических условий обучения информационной безопасности [55].

В работе Е. Г. Беляковой, Э. В. Звягинской и А. И. Берененцевой утверждается, что прививать основы информационной и кибербезопасности, учить детей противостоять существующим рискам нужно, начиная с младшего школьного или даже дошкольного возраста [32].

Рассмотренные нами труды, показывают, что формирования основ кибербезопасности является педагогической и психологической проблемой. В школах дети проводят большую часть своего времени, и их основная деятельность связана с учебой. Кроме того, там работают специалисты, способные обучать компьютерной и информационной безопасности.

Следует обратить особое внимание на угрозы кибербезопасности, так как они являются негативным аспектом информационной безопасности.

Вероятность проявления различных угроз может изменяться в зависимости от обстоятельств и условий, что нередко вызывает споры среди ученых. Несмотря на трудности в логическом объяснении, некоторые специалисты трактуют угрозы как «осознание потенциальной опасности и возможность ее реализации» [59]. Но на самом деле угрозы безопасности имеют в себе совокупность условий и факторов, которые могут представлять риски для значимых интересов личности, общества и

государства в информационной сфере.

Рассмотрим несколько классификаций угроз кибер-и-информационной безопасности, которые можно разделить на следующие категории:

1. Классификация по природе (объективности) происхождения, такие как естественные (объективные), вызванные вследствие физических процессов или природных явлений, находящихся вне человеческого контроля; искусственные (субъективные), вызванные деятельностью человека и его вмешательством в информационную среду.

Искусственные угрозы также делятся на умышленные (например, вирусные программы, неправомерный доступ к конфиденциальной информации) и случайные (например, ошибки персонала, сбои программного обеспечения, технические неисправности и т.д.)

2. Классификация по месту возникновения, такие как внутренние угрозы, связанные ошибками системы и её компонентами технического характера (пример: программными ошибками и сбоями коммуникационного оборудования, которые могут использовать злоумышленники); внешние угрозы, происходят извне в ходе стихийных бедствий, через каналы связи, другими внешними воздействиями (пример: атаки хакеров, фишинг и т.д.).

3. Классификация по доступу, такие как утечка или повреждение данных (скрытые каналы воздействия), а также несанкционированный доступ (прямой доступ к системам).

4. Классификация по видимости воздействия, такие как активные, которые вносят изменения в состояния системы через прямое вмешательство (пример: повреждение базы данных, вредоносные программы); пассивные, которые не заметны, без внесения видимых изменений ПО, что делает их особо опасными (пример: считывание конфиденциальных данных или ослаблению защиты).

5. Классификация по цели реализации, такие угрозы данным,

программной среде, поддерживающей инфраструктуре и сетевому оборудованию [3; 9; 31; 39].

Угрозы можно также классифицировать по уровню и степени опасности. Наиболее серьезными считаются: несанкционированный доступ, пожары, умышленное нарушение работы систем (например, ввод неверных данных, заражение вирусами, вывод из строя техники и ее кража), а также использование программ с ошибками [38].

Изучив научные подходы к классификации угроз, становится ясно, что в настоящее время отсутствует единая и общая классификация киберугроз, особенно в образовательной сфере.

На основе классификации угроз личности мы разработали свою классификацию, поскольку в психолого-педагогической литературе эта тема недостаточно раскрыта. Можно выделить следующие ключевые группы источников киберугроз для личности как:

– государственные структуры, такие как: органы власти, а также зарубежные (по уровню управления и по ветвям власти); государственные учреждения и службы (к примеру, военная и правоохранительная);

– общественные организации, такие как: организации, связанные с различными сферами деятельности, в том числе и международные;

– социальные группы, которые делятся по видам по: численности (малые и большие), способу организации (формальные и неформальные) и социальному положению (связаны с территорией, этносом, профессией, религией, образованием);

– отдельный человек или авторитетное лицо, например, родители, любимый учитель, уважаемый взрослый, друг-сверстник и т.д.

Можно также выделить такие источники информации, которые с малых лет оказывают особое влияние на личность, а также психологическому и моральному здоровью детей; как телевидение и средства массовой информации (СМИ).

В контексте современных образовательных реалий телевидение

завоевало роль ключевого источника информации для школьников, что подтверждается обширной литературой. Исследования различают медиа по степени их значимости: Интернет находится на первом месте, за ним следует телевидение, а затем печатная пресса и радио [1].

За последние двадцать лет дети школьного возраста, особенно младшие школьники, подверглись значительному влиянию экранных искусств, где преобладают действия над эмоциональными и мыслительными процессами. В современных фильмах и компьютерных играх стали нормой элементы эротики, насилие и жестокости, а вымышленные героев стали преобладать над реалистичными[27].

Современные родители, в связи с занятостью и работой, всё больше заменяют чтение традиционных сказок, а также колыбельных на мультфильмы в Интернете или на телевизоре. Из-за чего дети с рождения оказываются погружены в информационные пространства.

Также стоит учесть то, что медиа может скрывать потенциальные угрозы за безобидной и правдоподобно представленной информацией, например, в популярном анимационном фильме или сериале может фигурировать персонаж, который демонстрирует рискованное поведение – курение и употребление каких-либо средств, что может показаться ребенку интересным. Из-за чего мощный потенциал их воздействия и манипуляций на сознание детей сложно переоценить.

Для младшего школьника, стремящегося к социальной реализации, крайне важно быть в курсе событий окружающего мира. Непрерывное взаимодействие с социальной средой, где ребенок проявляет себя как активный социальный агент, выступает критически важным условием его гармоничного развития [32]. Дети через телеэкран получают доступ к миру взрослых, наблюдая его и стремясь себя с ним ассоциировать. Это создает проблему, связанную с нарушением прав ребенка, содержащихся в документах ООН, так как медиа часто не учитывают возрастные ограничения.

Г. В. Грачев, О. В. Пристанская, А. В. Федоров и А. В. Шариков исследовали эти аспекты, подчеркивая необходимость разработки государственной политики для защиты прав детей в этой области [21].

Современные информационные технологии открыли для детей доступ в Интернет, сделав его популярным развлечением, наряду с видеоиграми. Дети все чаще выбирают такие формы досуга. Тем не менее, полностью контролировать весь интернет-контент невозможно. Родители не всегда могут уследить за тем, что видят их дети в сети. Это создает риск того, что ребенок может наткнуться на сайты, рекламирующие наркотики, алкоголь и другие вредные вещества [32]. Такие ресурсы могут нанести вред детской психике и повлиять на поведение.

С нашей точки зрения, для решения вопроса кибербезопасности, особенно в детской среде, необходим правовой контроль над средствами массовой информации, включая Интернет. Без четких законодательных рамок трудно обеспечить защиту детей от негативного влияния.

Адекватное восприятие и развитие критического мышления также играют немалую роль в создание среды, фильтрующей особо опасные информационные ресурсы. Появляется зона ответственности сфер деятельности образовательных и семейных структур.

В школах должно быть предусмотрено внедрение специализированных психолого-педагогических программ, направленных на информационною грамотность, сетевому этикету, правильное использования медиа для достижения своих желаний и целей и много другое [22].

Наличие такого объёма ненадёжной информации становится основой для формирования ложных убеждений и стереотипов, которые могут негативно сказываться как на личностном развитии школьников, так и на их взаимоотношениях со сверстниками. Страдают социальные навыки школьников из-за затруднений с коммуникацией. Избыточное потребление недостоверной информации может привести к зависимому поведению,

когда ребёнок начинает терять интерес к живому общению и предпочитает виртуальные контакты. Это может негативно сказываться на развитии эмпатии и способности понимать окружающих.

Избыточное потребление недостоверной информации может привести к зависимому поведению, когда ребёнок начинает терять интерес к живому общению и предпочитает виртуальные контакты. Это может негативно сказываться на развитии эмпатии и способности понимать окружающих.

Таким образом, основными источниками информации, влияющими на детей, являются государственные и общественные структуры, социальные группы, отдельную личность, а также СМИ и телевидение.

Кибербезопасность изучается в разных областях знаний, что показал анализ правовых и научных источников. Однако в сфере педагогики четкой концепции по этой проблематике не сформулировано. Это побудило нас обратиться к междисциплинарным исследованиям, где обнаружились разнообразные и порой противоречивые подходы к определению кибербезопасности, представленные в литературе, а также нам удалось сформулировать своё собственное определение.

Но, несмотря на то, что в педагогической литературе мало внимания уделяется понятию кибербезопасности, роль педагогов в подготовке детей к защите от негативных информационных воздействий трудно переоценить. Учителя могут поспособствовать развитию информационной грамотности, обучая выделять качественную информацию из общего потока, тем самым способствуя минимизации проблем кибербезопасности среди младших школьников [6].

1.2 Особенности развития младшего школьника как фактор эффективности формирования основ кибербезопасности

Проблематика защиты кибербезопасности в образовательных учреждениях должна рассматриваться как совокупность мер,

обеспечивающих сохранение интеллектуального и психологического здоровья обучающихся [24].

Процесс обеспечения кибербезопасности базируется на способности самих школьников распознавать и нейтрализовать риски, вызванные информационным контентом. Подобные навыки формируются либо стихийно, либо целенаправленно, посредством специально организованной системы обучения.

Исходя из вышеуказанного, возникает потребность в разработке стратегии, решающей данную актуальную задачу: каким образом обеспечить кибербезопасность для обучающихся начальной школы, минимизируя негативное воздействие на их психоэмоциональное и моральное развитие [24]?

Согласно Федеральному государственному образовательному стандарту начального общего образования, утвержденному Минпросвещения РФ 31 мая 2021 г., обучающимся предстоит освоить метапредметные результаты, включающие следующие аспекты: умение подбирать источники информации, находить нужные сведения, представленные явно или скрыто, проверять достоверность полученной информации самостоятельно или при помощи методик, предложенных учителем [46].

Отдельно подчеркивается необходимость соблюдения правил безопасного пользования сетью Интернет при поиске данных, что предполагает сопровождение и надзор со стороны взрослых, включая педагогов и законных представителей несовершеннолетних [46].

Исследование вопроса предполагает выделение специфичных черт детей младшего школьного возраста, имеющих важное значение для формирования компетенций в области кибербезопасности. Анализ научных источников позволил выявить следующие ключевые особенности детской психики и поведения младших школьников [50]:

Во-первых, значимым фактором для обучающихся начальной школы является система отношений «учитель – ребенок», определяющая качество взаимосвязей с семьей, сверстниками и собственными внутренними установками. Авторитет учителя воспринимается детьми как высокий, формируя доверительное общение и положительное восприятие передаваемых сведений.

Во-вторых, ведущая деятельность младших школьников связана с учебой, что делает целесообразным интеграцию воспитания навыков кибербезопасности в общий образовательный процесс.

В-третьих, этот возраст характеризуется началом формирования представлений о базовых категориях добра и зла, хорошего и плохого. Несмотря на наличие определенных моральных ориентиров, внутренняя позиция относительно принятых обществом норм пока отсутствует. Моральные принципы начинают играть регулирующую роль только тогда, когда ученик осмыслил и принял их лично. Понимание морального аспекта кибербезопасности способно мобилизовать внутренний потенциал ребенка и направить его на самосовершенствование [50].

Четвертый ключевой вывод состоит в том, что без учета взаимодействия с одноклассниками невозможно полноценно сформировать основы кибербезопасности у младших школьников. Взаимоотношения со сверстниками отличаются от взаимодействия со взрослыми, что оказывает уникальное влияние на внутреннее развитие личности ребенка.

Г. А. Цукерман рассматривает взаимодействие детей со сверстниками как промежуточный этап в развитии навыков, который расположен между этапом первоначального обучения вместе со взрослым и периодом полного перехода деятельности внутрь сознания ребенка, ставшего независимым [7]. Кооперативная деятельность выделяется двумя ключевыми характеристиками:

Независимость от взрослого: изначально в отношениях «учитель – ученик» взрослый исполняет роль организатора и задаёт направление

деятельности, но вскоре дети продолжают действовать автономно. В отличие от традиционных моделей фронтального обучения, где преподаватель постоянно руководит и контролирует, здесь дети обращаются к наставнику лишь в редких случаях. Связь между учеником и учителем преобразуется: дети больше не нуждаются в постоянном присутствии взрослого и предпочитают обращаться за помощью друг к другу. Такая динамика способствует пониманию чужой точки зрения и уменьшает проявления эгоцентризма, что ведёт к развитию рефлексивных навыков.

Ориентация не только на конечный результат, но и на способы выполнения действий: при кооперативной деятельности внимание уделяется не только результатам, но и процессу выполнения действий как своими силами, так и партнером. Один из примеров подобной структуры взаимодействия – ситуация, похожая на «педсовет», когда ученики разного возраста обсуждают критерии заданий, предлагаемых остальным участникам. Высокая мотивация наблюдается даже у слабоуспевающих учеников, которые становятся более активными и вовлеченными.

Кооперация между детьми в эпоху глобальной информатизации способствует постоянному обновлению и совершенствованию личностных качеств, открывая дополнительные перспективы для культурологического и интеллектуального развития. Таким образом, кооперация должна считаться обязательным элементом формирования базовых принципов кибербезопасности.

Принимая во внимание возрастные особенности младших школьников, следует обратить внимание на недостаток развития критического мышления. Педагог играет значительную роль в процессах обучения, связанных с развитием основ кибербезопасности, помогая детям осознанно подходить к оценке доступной информации [2].

Еще одной чертой младших школьников является повышенная гибкость мышления, позволяющая добиться качественных изменений. Эти

преобразования осуществляются в пределах познавательной и учебной деятельности, обладающей особым значением для ребенка. Хорошо продуманная структура учебной деятельности даёт возможность гармонично включать педагогически управляемые процессы, способствующие развитию у младших школьников знаний о кибербезопасности [49].

Под руководством педагогов дети способны приобрести основы теоретико-рефлексивного мышления, согласно мнению В. В. Давыдова. Помимо мыслительных возможностей, важно учитывать и другие способности младших школьников.

Исследования Ж. Пиаже подчеркивают различия между мышлением ребенка и взрослого, отмечая не только количественную разницу, но и качественную. Так, детская мысль сочетает осознанные и бессознательные элементы, что подчеркивает необходимость уделять внимание не только очевидным достижениям, но и тому, что еще предстоит изучить и развить в процессе обучения [56].

Начало школьной жизни знаменует формирование нового уровня самосознания, обозначаемого термином «внутренняя позиция». Она отражает осознание ребёнком себя, своего поведения, окружающей среды и происходящих событий. Возможность вербально выразить своё отношение к различным явлениям определяет старт индивидуального личностного роста [30].

Понимание внутренней позиции связано с формированием в сознании ребёнка набора нравственных норм, которым он пытается соответствовать независимо от внешних обстоятельств. Исследования Ж. Пиаже показали, как дети разного возраста понимают и применяют моральные нормы, делая соответствующие выводы [56].

Значительный вклад в изучение морального развития внес Лоуренс Кольберг, чьи работы дополнили и обогатили идеи Ж. Пиаже. Согласно наблюдениям Л. Кольберга, на ранних стадиях морального развития дети

оценивают поступки главным образом исходя из последствий, а не намерений или сути действия [40].

На первом этапе ребёнок убеждён, что хорошее поведение определяется соблюдением установленных правил ради избегания наказания. На втором этапе появляется осознание полезности нравственных поступков, обусловленных возможностью вознаграждения или удовлетворения личных потребностей. Поведение, ведущее к выгоде или служащее интересам других, считается правильным.

При изучении основ кибербезопасности важно учитывать эти моменты и создавать ситуации, требующие от детей морального выбора. Осознанное поведение, возникающее на основе когнитивных процессов, охватывает и эмоциональную сферу, способствуя саморегуляции поведения.

Уже на третьем году обучения появляются первые признаки произвольности, хотя эта способность еще недостаточно устойчива и проявляется нерегулярно. Возрастающая способность регулировать свои эмоции впервые зарождается в конце второго-третьего годов обучения, когда младшие школьники пытаются управлять своими чувствами и стремлениями, хотя этот процесс еще несовершенен [40].

Освоение моральных норм у младших школьников проходит поэтапно, причем они чаще полагаются на авторитеты взрослых и старших товарищей. Их моральные размышления характеризуются зависимостью от внешнего воздействия и восприимчивостью к внешним факторам. Создание ситуаций успеха в обучении кибербезопасности позволит преодолеть недостатки подобного подхода [60].

Педагогическая поддержка и принцип сотрудничества являются основными факторами, способствующими формированию основ кибербезопасности у младших школьников. В возрасте от 7 до 10 лет дети сохраняют тесную связь с семьёй, проявляют любопытство к миру взрослых, постепенно обретают моральную и гендерную идентичность.

Чрезмерная доверчивость и некритичное принятие авторитетов характерны для этого этапа развития.

Согласно мнению И. П. Подласого, к шестилетнему возрасту большинство детей готовы к началу систематического обучения в школе [50]. Психологическое созревание и способность осознавать своё поведение, сравнивая себя с окружающими, позволяют считать младшего школьника уже сложившимся субъектом.

Происходит активное развитие нервной системы, повышается функциональность больших полушарий мозга, укрепляется кора больших полушарий. Интенсивное психическое развитие сопровождается изменением баланса процессов возбуждения и торможения: усиление торможения идёт параллельно с доминированием возбудимости. Улучшаются показатели точности ощущений и восприятий. Характер и темперамент ребенка тесно связаны с физиологическими особенностями организма, включая процессы полового созревания и свойства нервной системы [48].

Особенности слабости нервной системы проявляются повышенной чувствительностью и низкой выносливостью, характерные черты младшего школьного возраста: быстрота реакций, впечатлительность, легкая возбудимость и импульсивность [36].

Высокая эмоциональная подвижность и интенсивность переживаемых эмоций характеризуют младших школьников: частая смена настроений, быстрая реакция от слёз до радости. Несмотря на слабость нервной системы, организм детей обладает высоким уровнем работоспособности и быстрой восстанавливаемостью сил. К. Д. Ушинский отмечал: «Ребёнок быстро утомляется от любого длительного однотипного действия, будь то сидение, лежание, ходьба или говорение, но остаётся активным и радостным, беспрерывно двигаясь и сочетая различные виды деятельности. Даже короткий сон восстанавливает детскую энергию» [50].

Возрастные отличия проявляются и в особенностях темперамента, уровнях активности, эмоциональности и моторике. Чем старше ребенок, тем сильнее меняются его поведенческие характеристики. Старшие дети теряют некоторые ценные свойства нервной системы, присущие раннему детству [36].

Память играет центральную роль в познавательной деятельности младшего школьника. Формируются новые социальные взаимоотношения с взрослыми и сверстниками, изменяется содержание деятельности и общения, формируется социальная ориентация и общественные установки. Склонность к подражанию учителю, лёгкая внушаемость и доверчивость делают младшего школьника открытым для приобретения общественных навыков и этических норм [10].

Присоединяясь к классу, ребенок адаптируется к новым социальным нормам и ожиданиям коллектива, испытывая радость от признания и гордость за выполнение поручений. Нарушение общепринятых норм вызывает сожаление и раскаяние. Чувства дружбы, товарищества и взаимопомощи, воспринимаемые детьми как справедливые и ответственные, становятся неотъемлемой частью их повседневных отношений. Взрослые остаются главными фигурами авторитета и примером для подражания [11].

Обычным поведением младших школьников является сочетание незрелой воли и ярко выраженных эмоций, приводящее к необдуманным поступкам. Рациональные доводы уступают сильным переживаниям и ощущениям, затрудняя принятие взвешенных решений. Этот период насыщен множеством противоречий и сложных явлений, что требует тщательной организации обучения и повседневной жизни [10].

Для успешного обучения основам кибербезопасности необходима особая атмосфера взаимодействия и взаимопонимания между учителем и учеником, основанная на хорошо спланированном содержании занятий, значимых для младшего школьника. Основным условием эффективности

обучения является позиция педагога-наставника, построенная на полном принятии ребенка, содействии его социальному приспособлению и личностному развитию, ограждении от нежелательных воздействий.

Работа учителя основывается на принципах открытой двусторонней связи («учитель – ученик»), активного социального взаимодействия, глубокой психологической близости, свободы самовыражения и абсолютной нетерпимости к насилию по отношению к ребенку [10].

Одним из важнейших факторов успешного формирования основ кибербезопасности у младших школьников является глубокое понимание учителем самой природы кибербезопасности.

Первое, что необходимо понять педагогу, – это объект защиты, то есть кто именно подлежит охране. В данном случае объектом защиты является личность младшего школьника.

Второе – выявление конкретных угроз, от которых следует защитить ребенка. Угроза понимается как внешний фактор, потенциально опасный для ребенка.

Третье – осознание важности сохранения здоровой самооценки ребенка и недопущения разрушающих её факторов, которые ведут к дезориентированности в окружающем мире, искажению мировосприятия и самовосприятия. Среди негативных эффектов выделяются потеря уверенности в себе, разрушение целостного образа «Я», неверный выбор жизненных целей, риск возникновения зависимости и возможное нарушение психического здоровья, доходящее до необратимых патологий.

Четвёртое – разработка оптимальной стратегии минимизации рисков и выяснение, какие меры и методы окажутся наиболее действенными для защиты ребенка.

Пятое – осознание учителем своей особой миссии как защитника личности младшего школьника в образовательном процессе, понимаемой как превентивные действия, предшествующие усилиям общества и государства [56].

Изучив данные аспекты, мы пришли к ряду следующих особенностей: педагог – значимая личность в жизни ребенка; ведущая деятельность – учебная; ситуация взаимодействие, сотрудничества среди младших школьников; пластичное мышления, выражающаяся в способности к адаптации и применению творческих способностей; внутренняя позиция, включающая понимание и принятие себя и других.

Проанализировав указанные аспекты, можно сделать вывод, что интеграция основ кибербезопасности в жизнь младших школьников неразрывно связана с развитием их личности и индивидуальности.

Выделенные нами в ходе анализа научных источников особенности младшего школьного возраста следует учитывать при работе педагога-психолога. Эти особенности легли в основу предлагаемых нами направлений работы педагога-психолога к формированию основ кибербезопасности у младших школьников.

1.3 Направления работы педагога-психолога по формированию основ кибербезопасности у младших школьников

Современное научное сообщество сравнительно недавно стало проявлять интерес к вопросам кибербезопасности. И особенно актуальным это стало в контексте интеграции кибербезопасности как нового направления в систему начального образования. Важно отметить, что этот интерес обусловлен стремительно возрастающей ролью цифровых технологий в повседневной жизни и необходимостью адаптации учебных программ для удовлетворения новых потребностей общества [34].

Также такое внимание обусловлено значительными сдвигами в образовательной методологии, которые наблюдаются в последнее время. Внедрение компьютерных и информационных технологий всё чаще заменяет традиционные модели формирования у обучающихся знаний, умений и навыков [28].

Анализ научных исследований и рассмотренные психологические, возрастные особенности детей младшего школьного возраста позволили нам выдвинуть необходимость проведения работы педагога-психолога по формированию основ кибербезопасности.

Рассмотрим основные направления работы педагога-психолога по нашему вопросу.

В своей исследовательской работе мы основывались на трудовых функциях, определенных профессиональным стандартом «Педагог-психолог (психолог в сфере образования)», который был утверждён приказом Министерства труда и социальной защиты Российской Федерации от 24.07.2015 года № 514н [45].

Данный нормативный документ определяет требования к компетенциям и к квалификации специалистов, работающих в области педагогики и психологии. Стандарт обобщает знания, умения и навыки, которые необходимы педагогам-психологам для эффективного исполнения своих обязанностей в образовательных учреждениях.

В рамках трудовой функции «Психолого-педагогическое и методическое сопровождение реализации основных и дополнительных образовательных программ» [45], нами было выделено *организационное направление* работы педагога-психолога, а именно:

1. Организация профилактики предотвращение кибербуллинга, профилактики безопасного онлайн-поведения и других видов профилактики, необходимые для плана работы службы психолого-педагогической сопровождения.

2. Усиленный контроль выявленных «зон риска», чтобы обеспечить безопасность и поддержку обучающихся в образовательной среде.

Следующие трудовые функции «Психологическая экспертиза (оценка) комфортности и безопасности образовательной среды образовательных организаций», «Психологическая диагностика детей и

обучающихся» [45] нашли своё отражение в *диагностическом направлении* работы педагога-психолога.

В данном направлении работы осуществляется:

– проведение мониторинга (диагностики) для выявления «группы риска» (тех обучающихся, кто подвергся онлайн-мошенничеству, интернет-травле, обману в социальных сетях или онлайн-играх, а также столкнулся с недостоверными источниками информации);

– диагностика выявления безопасного использования интернета детьми в семье, а также анализ и интерпретация полученных данных и др.

Также в данном направлении осуществляется проведение анкетирования, тестирования, опросов участников образовательного процесса (педагогов, родителей и детей) на темы «Как защитить себя от опасных ситуаций в Интернете?», «Ложная информация» и пр.

Помимо этого, педагог-психолог проводит тестирование обучающихся 1-4 классов для оценки уровня тревожности, агрессивности, самооценки и других психологических характеристик.

Педагог-психолог может отслеживать прогресс детей в освоении навыков безопасного использования Интернета, вносить коррективы в свою работу на основе полученных результатов. Такая работа позволяет ему адаптировать методы и подходы под потребности каждого ребёнка, способствуя более эффективному развитию их интернет-грамотности.

Из трудовой функции «Коррекционно-развивающая работа с детьми и обучающимися, в том числе работа по восстановлению и реабилитации» [45], было выдвинуто *индивидуально-коррекционное направление*, которое является важной составляющей деятельности педагога-психолога. Ключевыми в данном направлении выступают:

1. Психологическая работа с обучающимися, направленная на формирование навыков самоконтроля и саморегуляции, то есть на умение контролировать своё поведение в Интернете.

2. Психологическая работа с обучающимися, направленная поддержку эмоционального развития, то есть для преодоления отрицательных последствий, связанных с негативными высказываниями и критикой в сети; для формирования у детей позитивного отношения к Интернету и понимания его роли в их жизни.

3. Психологическая работа с обучающимися, направленная развитие критического мышления, то есть для формирования умения критически оценивать информацию, которую они получают из Интернета.

Просветительское направление в работе педагога-психолога, выделенное нами из трудовых функций «Психологическое консультирование субъектов образовательного процесса», «Психологическое просвещение субъектов образовательного процесса» [45], можно рассмотреть в таких видах деятельности, направленных на повышение психологической компетентности учителей, учеников и родителей, как:

1. Выступление на родительских собраниях (темы для родительских собраний, которые может предложить педагог-психолог: «Цифровая грамотность для родителей: как понять мир ребенка?», «Кибербуллинг: как распознать, предотвратить и помочь?», «Развитие критического мышления: как научить детей безопасно фильтровать информацию?» и др.).

2. Подготовка рекомендаций для участников образовательного процесса на такие темы:

– для обучающихся: «Опасности онлайн-знакомств: что нужно знать перед тем, как делиться личной информацией», «Киберэтикет: хорошие манеры в виртуальном мире», «Если кто-то тебя обидел в сети: что делать?» и др.;

– для учителей: «Создание безопасного образовательного онлайн-пространства в классе», «Введение в основы кибербезопасности для детей: с чего начать?», «Распознавание признаков кибербуллинга среди учеников» и др.;

– темы для родителей: «Первый шаг к безопасности: как говорить с детьми об интернет-угрозах», «Что делать, если ваш ребенок стал жертвой кибербуллинга?» и др.

3. Разработка и организация занятий, в том числе посвящённых темам таким, как «Интернет-зависимость», «Антивирусное программное обеспечение: ваш цифровой щит», «Безопасные игры: выбор, настройка и ограничения», «Мир фейков: как отличить правду от лжи в интернете», «Защита личных данных» и др.

На своих занятиях педагог-психолог может применять инновационные технологии, такие как:

– сторителлинг – использование увлекательных историй или иллюстративных комиксов для донесения ключевых идей и принципов кибербезопасности. Эта технология помогает младшим школьникам легко воспринимать информацию благодаря простоте и наглядности. [25];

– технологии исследовательской деятельности, направленные на развитие интеллектуально-творческого потенциала ребёнка через развитие навыков исследовательского поведения, развитие творческой активности;

– тренинговые технологии, где рассматриваются актуальные вопросы кибербезопасности, способы защиты личных данных и пр. К примеру тренинг для родителей и педагогов, на тему «Стратегии по взаимодействию с детьми на тему безопасности в Интернете».

Применение этих технологий делает занятия более интересными и эффективными, помогая детям развивать критическое мышление и навыки, необходимые для безопасного существования в цифровом пространстве.

4. Внесение изменений и усовершенствование школьного сайта, создание раздела с размещением информации для всех участников образовательного процесса, а также самих обучающихся, такой как:

– инструкции по защите личной информации онлайн,

– рекомендации по безопасной навигации в интернете,

– информационные брошюры,

– вебинары по актуальным угрозам в сети.

5. Информирование о возможности получения психологической помощи в городе, включая возможность телефонных консультаций.

Трудовая функция «Психопрофилактика (профессиональная деятельность, направленная на сохранение и укрепление психологического здоровья обучающихся в процессе обучения и воспитания в образовательных организациях)» [45] нашла отражение в *аналитическом направлении*:

– анализ эффективности проведенных мероприятий,

– оценка результативности индивидуально-коррекционной работы,

– результаты наблюдения,

– разрешения конфликтных ситуаций, опроса педагогов,

– составление программы профилактических мероприятий на следующий учебный год.

Таким образом возможно осуществить эффективное взаимодействие всех участников образовательного процесса, в особенности обучающегося с педагогом-психологом, что поспособствует развитию у первых безопасного поведения в цифровой среде, а также сформирует критическое мышление и эмоциональную стабильность. Это в свою очередь, поможет младшим школьникам эффективно противостоять угрозам, возникающим в онлайн-пространстве. Благодаря профессиональным усилиям педагога-психолога в совокупности с усилиями всех субъектов образовательного процесса, младшие школьники сформируют навыки ответственного интернет-пользователя, что значительно повысит уровень их безопасности в виртуальной среде.

Выводы по главе 1

В первой главе мы рассмотрели теоретические аспекты работы педагога-психолога по формированию основ кибербезопасности у младших школьников и выяснили следующее.

Изучение понятий «кибербезопасность» и «информационная безопасность в психолого-педагогической литературе, позволило нам понимать кибербезопасность, как составляющую важной области информационной безопасности, которая уделяет особое внимание исследованию специфики киберобъектов, потенциальных цифровых угроз, создавая основу для формирования у молодежи навыков безопасного и ответственного поведения в цифровом пространстве, тем самым защищая их от различных угроз, связанных с виртуальной средой.

Под информационной безопасностью понимается системная область мер, обеспечивающая защиту, состоящая из методов, средств и процессов предотвращение некорректного и противозаконного доступа к информации (из бумажных и электронных носитетей), которая стремится к конфиденциальности, целостности и доступности.

Были выделены основные источники информации, влияющие на детей, такие как государственные структуры, общество, социальные группы-объединения, авторитетное лицо (личность). Очень часто, данные источники могут транслировать подрастающему поколению недостоверную, и даже противоречащую этике информацию. Межличностные контакты, печатная и цифровая литература, СМИ, образовательные услуги, как средства информационного воздействия, играют значительную роль в формировании мировосприятия и ценностной системы каждого человека [27].

Эффективному формированию основ кибербезопасности у младших школьников способствуют такие особенности развития, как: психологические – критическое мышление, гибкость мышления, хорошая память и высокая эмоциональная восприимчивость; возрастные – взаимодействие со сверстниками, состояние утомляемости.

Важно учитывать и то, что социальная ситуация развития, заключается в значительном количестве времени проводимым ребенком в образовательном учреждении, где ведущей деятельностью младшего

является учебная деятельность, а учитель имеет значимость и авторитет. Выделенные нами особенности младшего школьного возраста следует учитывать при организации работы педагога-психолога.

Обучение основам кибербезопасности играет важную роль в информировании детей о потенциальных угрозах и способах защиты в цифровой среде, где главная роль отводиться педагогу-психологу, как авторитетному лицу для обучающихся.

На основе профессионального стандарта «Педагог-психолог (психолог в сфере образования выделили основные направления работы педагога-психолога по формированию основ кибербезопасности, как:

– организационное (профилактика безопасного онлайн-поведения, контроль «зон риска»);

– диагностическое (проведение мониторингов и диагностик детей «групп риска», диагностика выявления безопасного использования интернета детьми в семье, анкетирования и тестирования);

– просветительское (выступление на родительских собрания, подготовка рекомендаций для участников образовательного процесса, проведение занятий и их разработка, усовершенствование школьного сайта и т.д.);

– индивидуально-коррекционное (психологическая работа с обучающимися, направленная на поддержку эмоционального развития, развитие критического мышления, формирования навыков самоконтроля и саморегуляции);

– аналитическое (анализ эффективности деятельности) [45].

ГЛАВА 2. ОРГАНИЗАЦИЯ И РЕЗУЛЬТАТЫ ПРЕДПРОЕКТНОГО ИССЛЕДОВАНИЯ ПРОБЛЕМЫ ФОРМИРОВАНИЯ ОСНОВ КИБЕРБЕЗОПАСНОСТИ У МЛАДШИХ ШКОЛЬНИКОВ

2.1 Цели и задачи предпроектного исследования, характеристика используемых методик. Результаты исследования и их интерпретация

Проектная идея, лежащая в основе данного исследования, заключается в изучении путей эффективного обучения младших школьников принципам кибербезопасности. Исследование выявляет трудности, с которыми сталкиваются дети при освоении этих основ, и подчеркивает необходимость разработки программ педагогов-психологов, направленных на облегчение этого процесса.

Для понимания сути работы по формированию кибербезопасности в теоретической части исследования рассмотрели понятия: «информационная безопасность» и «кибербезопасности», особенности младших школьников и направления работы педагога-психолога по нашей теме.

Тематика нашего исследования освещает педагогическую проблему, связанную с возрастание, как положительной, так и отрицательной роли глобальной сети Интернет. Кроме того, средства массовой информации способствуют распространению жестоких образов, что дополнительно осложняется отсутствием адекватных мер цензуры.

Проблема формирования кибербезопасности становится критически важной задачей, так как ее решение способствует гармоничному развитию как личности, так и общества в целом. Формирование базовых навыков кибербезопасности у младших школьников является актуальной задачей, требующей пристального внимания и нахождения эффективных путей её решения [22].

В начальной школе эту задачу могут решать учитель, педагог-психолог и другие сотрудники образовательного учреждения, обладающие необходимой компетентностью в обучении детей противостоять

информационным угрозам и отличать позитивный контент от негативного в потоке разнообразной информации.

С этой точки зрения основная цель нашего исследования заключается в выявлении различий в уровне сформированности кибербезопасности у младших школьников, посещающих и не посещающих тематические занятия и мероприятия для оценки эффективности практики педагогов в данной теме.

Для достижения поставленной цели, нами были выявлены следующие задачи исследования:

1. Сформировать выборку исследования;

2. Осуществить подбор диагностических методик для исследования основ кибербезопасности у младших школьников.

3. Применить выбранные методики для измерения уровня формирования основ кибербезопасности для понимания культуры безопасного поведения младших школьников в сети Интернет.

4. Провести анализ результатов исследования и практики педагогов-психолога по формированию основ кибербезопасности у младших школьников.

5. Разработать программу работы педагога-психолога, направленную на формирование основ кибербезопасности у младших школьников.

Предпроектное исследование, в соответствии с поставленной целью и задачами, проводилось в *4 этапа:*

1. Подготовительный этап: постановка цели и задач, поиск базы исследования, подбор соответствующих методик, подготовка к исследованию.

2. Диагностический этап: проведение диагностик, интерпретация и анализ результатов.

3. Анализ и интерпретация полученных данных, а также анализ практики педагогов-психолога по формированию основ кибербезопасности у младших школьников.

4. Конструктивный этап: программа работы педагога-психолога, по формированию основ кибербезопасности у младших школьников.

Предпроектная часть нашего исследования была проведена на базе общеобразовательной школы г. Челябинска.

В выборку предпроектного исследования вошли 52 обучающихся четвертых классов: 28 девочек, 24 мальчика. Возраст испытуемых был от 10 до 11 лет. По социальным характеристикам группы не отличаются. Учителя имеют высшее педагогическое образование.

Для исследования было выделено две независимые выборки:

Группа А: 4 класс в количестве 26 человек, посещающий занятия, мероприятия, проводимые учителем (педагогом-психологом) в тематике «Кибербезопасность: безопасного поведения младших школьников в Интернете».

Группа Б: 4 класс в количестве 26 человек, где такие занятия не проводились (т.е. основываясь только на жизненный опыт).

Были определены следующие показатели для оценки сформированности основ кибербезопасности:

1. Собственное знание правил безопасного поведения в сети Интернет.

2. Готовность практического применение знаний для поиска и обработки информации в Интернете.

3. Владения навыками защиты личной информации в сети Интернет.

Для проведения исследования нами были использованы следующие проективные методики:

1. «Как бы ты поступил?» Ю. Б. Гиппенрейтер [20].

2. «Действие с информацией» Т. В. Борисова.

3. Тестирование «Безопасно или нет?» (для младших школьников).

Чтобы лучше понимать связь между выбранными нами методиками и их показателями, мы обобщим эту информацию в таблице 1.

Таблица 1 – Обобщенная информация по методикам и показателям сформированности основ кибербезопасности:

Показатель	Методика
Собственное знание правил безопасного поведения в сети Интернет	«Как бы ты поступил?» Ю. Б. Гиппенрейтера.
Готовность практического применение знаний для поиска и обработки информации в Интернете	«Действие с информацией» Т. В. Борисова
Владения навыками защиты личной информации в сети Интернет	Тестирование «Безопасно или нет?»

Для выявления показателя уровня собственное знание правил безопасного поведения в сети Интернет нами была проведена методика «Как бы ты поступил?» Ю. Б. Гиппенрейтера [20].

Данная методика преследует цель выявления уровня компетентности младших школьников в вопросах безопасного поведения в сети Интернет. Исследование нацелено на оценку способности учащихся идентифицировать потенциальные угрозы и принимать адекватные меры предосторожности в цифровой среде.

Исследование осуществлялось по средству бланков ответов, в которых нужно было написать решение предложенной ситуации для оценки их реакции на возможные интернет-угрозы. В дальнейшем данная методика позволила произвести коллективный сбор данных и их последующий анализ.

Решение каждой ситуации оценивалось в 1 балл.

Подробное описание методики и интерпретация результатов в Приложении А.

В результате данной диагностики в группах были получены следующие данные, приведённые в таблице 2:

Таблица 2 – Результаты исследования собственное знание правил безопасного поведения в сети Интернет у младших школьников

Уровни	Группа А		Группа Б	
	Количество, чел	%	Количество, чел	%
Высокий уровень собственное знание правил безопасного поведения в сети Интернет	17	65,4 %	5	19,2 %
Средний уровень собственное знание правил безопасного поведения в сети Интернет	7	26,9 %	9	34,6 %
Низкий уровень собственное знание правил безопасного поведения в сети Интернет	2	7,7 %	12	46,1 %

Из данных таблицы следует, что в группе А, которая посещала занятия по теме «Кибербезопасности», преобладает высокий уровень (65,4 %): младшие школьники утверждают, что не готовы прийти на встречу с незнакомым человеком. Также они заявляют о намерении воздерживаться от открытия файлов на компьютере, которые поступили из неизвестного источника на электронную почту. Данное поведение отражает осознанный подход к вопросам личной безопасности в цифровой среде и свидетельствует о базовых навыках кибергигиены.

В группе Б, где не проводились занятия, преобладает низкий уровень (46,1 %) и средний уровень (34,6 %). Почти половина опрошенных не обладали знанием о том, какие действия предпринять в случае взлома их аккаунта в Интернете. Более того, они могли бы открыть сомнительное электронное письмо на их почтовом ящике. Однако определённая часть опрошенных выразила, пусть и с неуверенностью, нежелание лично встречаться с человеком, с которым они познакомились в Интернете. Данные результаты подчеркивают необходимость повышения уровня цифровой грамотности и осведомлённости о безопасности в сети.

Таким образом, можно сделать вывод, что в Группе А преобладает высокий уровень собственное знание правил безопасного поведения в сети Интернет, чем в группе А.

Для наглядности отобразим полученные результаты в виде диаграммы (рисунок 1).

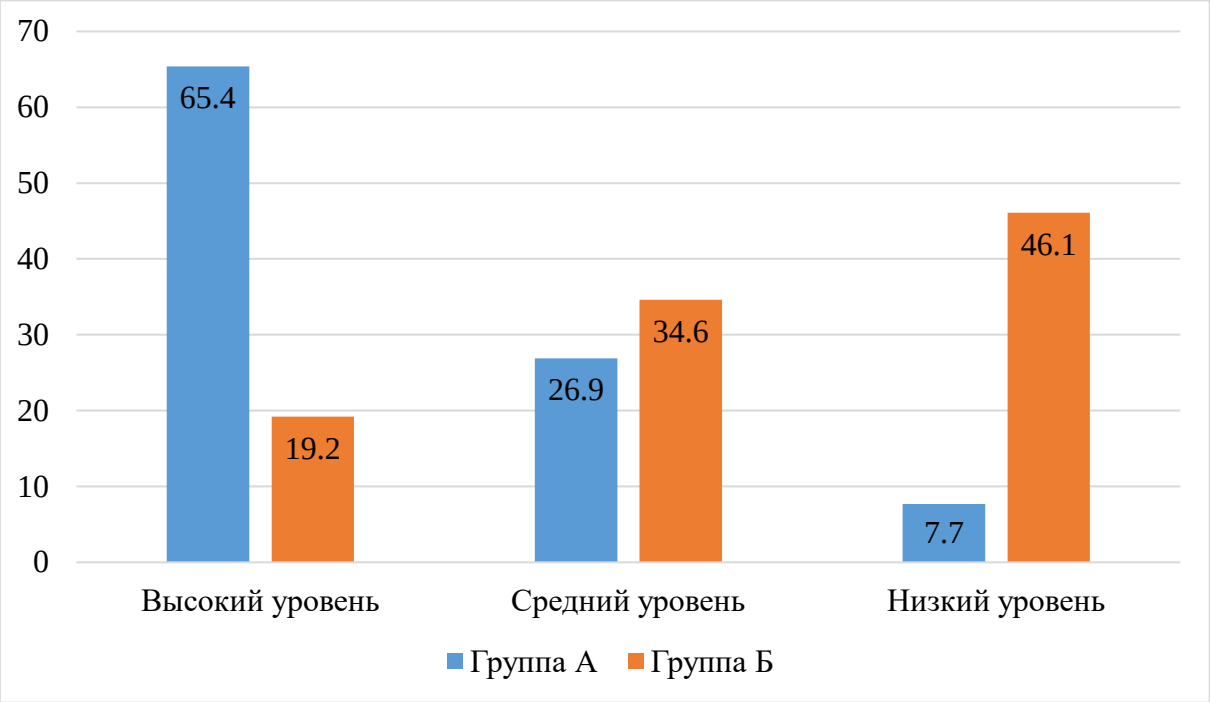

Рисунок 1 – Сравнительная диаграмма показателей уровня собственного знание правил безопасного поведения в сети Интернет

Для изучения уровня собственного знания основ безопасного поведения в сети Интернет нами был применен критерий U-критерий Манна-Уитни.

Было выполнено:

H_0: Уровень признака в группе Б не ниже уровня признака в группе А.

H_1: Уровень признака в группе Б ниже уровня признака в группе А.

В результате психодиагностического обследования групп младших школьников (Группа А – в которой, проводились занятия по кибербезопасности, и группа Б – в которой ничего не проводилось) (по 26 человек в каждой) были выявлены показатели собственного знания основ безопасного поведения в сети Интернет (в баллах).

Расчёт U-критерия Манна-Уитни по показателю собственного знания основ безопасного поведения в сети Интернет представлен в таблице 3.

Таблица 3 – Расчёт U-критерия Манна-Уитни по показателю собственного знания основ безопасного поведения в сети Интернет

№	Выборка 1 (Группа А)	Ранг 1	Выборка 2 (Группа Б)	Ранг 2
1	*2*	*3*	*4*	*5*
1	3	41,5	1	7,5
2	2	22,5	2	22,5
3	3	41,5	1	7,5
4	2	22,5	2	22,5
5	3	41,5	3	41,5
6	1	7,5	2	22,5
7	3	41,5	2	22,5
8	3	41,5	3	41,5
9	3	41,5	1	7,5
10	3	41,5	1	7,5
11	2	22,5	1	7,5
12	2	22,5	2	22,5
13	3	41,5	2	22,5
14	3	41,5	1	7,5
15	2	22,5	1	7,5
16	3	41,5	1	7,5
17	3	41,5	2	22,5
18	3	41,5	3	41,5
19	2	22,5	3	41,5
20	3	41,5	2	22,5
21	1	7,5	1	7,5
22	3	41,5	1	7,5
23	3	41,5	3	41,5
24	2	22,5	2	22,5
25	3	41,5	1	7,5

Продолжение таблицы 3

1	*2*	*3*	*4*	*5*
26	3	41,5	1	7,5
Суммы:		878		500

Сравнение выборки в таблице показывает, что значение выборки группы А несколько выше, чем выборка группы Б, поэтому первой считается выборка группы А.

Значение U-критерия Манна-Уитни мы нашли по формуле (1).

$$U = n_1 n_2 + \frac{n_x(n_x+1)}{2} - T_x, \quad (1)$$

где n_x – наибольшая из объемов выборок n_1 и n_2,

T_x– наибольшая сумма рангов.

Результат: $U_{Эмп}$ = 149.

Гипотеза Н0 о незначительности различий между выборками принимается, если $U_{кр} < U_{эмп}$. В противном случае H_0 отвергается и различие определяется как существенное. Где $U_{кр}$ – критическая точка, которую находят по таблице Манна-Уитни. Найдем критическую точку $U_{кр}$.

По таблице находим:

$U_{кр}$ (0.05) = 247.

$U_{кр}$ (0.01) = 210.

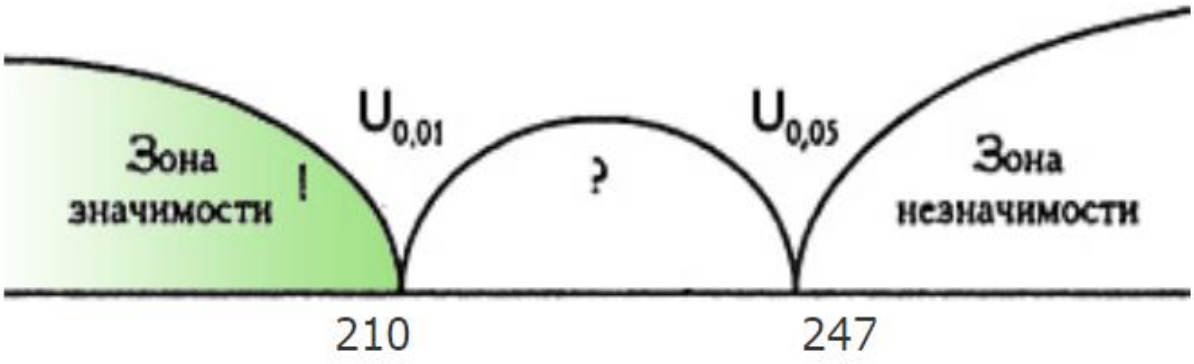

Рисунок 2 – Критерий Манна-Уитни по показателю уровня собственного знания основ безопасного поведения в сети Интернет на оси значимости

Полученное эмпирическое значение (рисунок 2) $U_{эмп}$ (149) находится в зоне значимости. Так как $U_{кр} < U_{эмп}$ – H_0 отвергается, принимается H_1 : различия в уровнях выборок можно считать существенным. Уровень

признака в группе Б ниже уровня признака в группе А, что ещё раз подтверждает полученные результаты.

Для выявления уровня готовности практического применения знаний для поиска и обработки информации в Интернете была применена следующая методика – «Действие с информацией» (Т. В. Борисова).

Методика направлена на оценку способности детей эффективно искать и обрабатывать информацию в сети Интернет. Особое внимание уделяется навыкам работы с онлайн-ресурсами и концентрации внимания на заданной теме.

Для проведения диагностики используются специализированное задание («Найди с помощью Интернета в словарях слово «потеха» и запишите его толкование?) и компьютер с доступом к Интернету.

Подборное описание методики и интерпретация результатов в Приложении Б.

В результате данной диагностики в группах были выявлены следующие данные, приведённые в таблице 4.

Таблица 4 – Результаты исследования готовности практического применение знаний для поиска и обработки информации у младших школьников

Уровни	Группа А		Группа Б	
	Количество, чел	%	Количество, чел	%
Высокий уровень готовности практического применения знаний для поиска и обработки информации в Интернете	15	57,7 %	3	11,5 %
Средний уровень готовности практического применения знаний для поиска и обработки информации в Интернете	8	30,8 %	6	23.1 %
Высокий уровень готовности практического применения знаний для поиска и обработки информации в Интернете	3	11,5 %	17	65,4 %

Из данных таблицы следует, что в группе А, где проводились занятия, преобладает высокий уровень (57,7 %) понимание ребенком как искать информацию и работать с ней в сети Интернет. Обучающиеся, принадлежащие к данной группе, демонстрируют способность оперативно и эффективно находить информацию, соответствующую заданной тематике. При этом они не отвлекаются на посторонние веб-ресурсы.

Этот навык показывает их умение сосредотачиваться на учебных задачах, а также указывает на владение методами целенаправленного поиска информации в сети.

В группе Б, где не проводились занятия, преобладает низкий уровень (65,5 %) понимание ребенком как искать информацию и работать с ней в сети Интернет. Обучающиеся испытывают затруднения в нахождении необходимой информации по заданной теме через Интернет. Вместо этого их внимание зачастую переключается на посторонние веб-страницы и изображения.

Это указывает на необходимость развития навыков критического отбора информации и целенаправленного поиска, а также умения сосредотачиваться на основной задаче.

Таким образом, можно сделать вывод, что в Группе А преобладает высокий уровень готовности практического применение знаний для поиска и обработки информации в Интернете, чем в группе Б.

Для наглядности отобразим полученные результаты в виде диаграммы (рисунок 3).

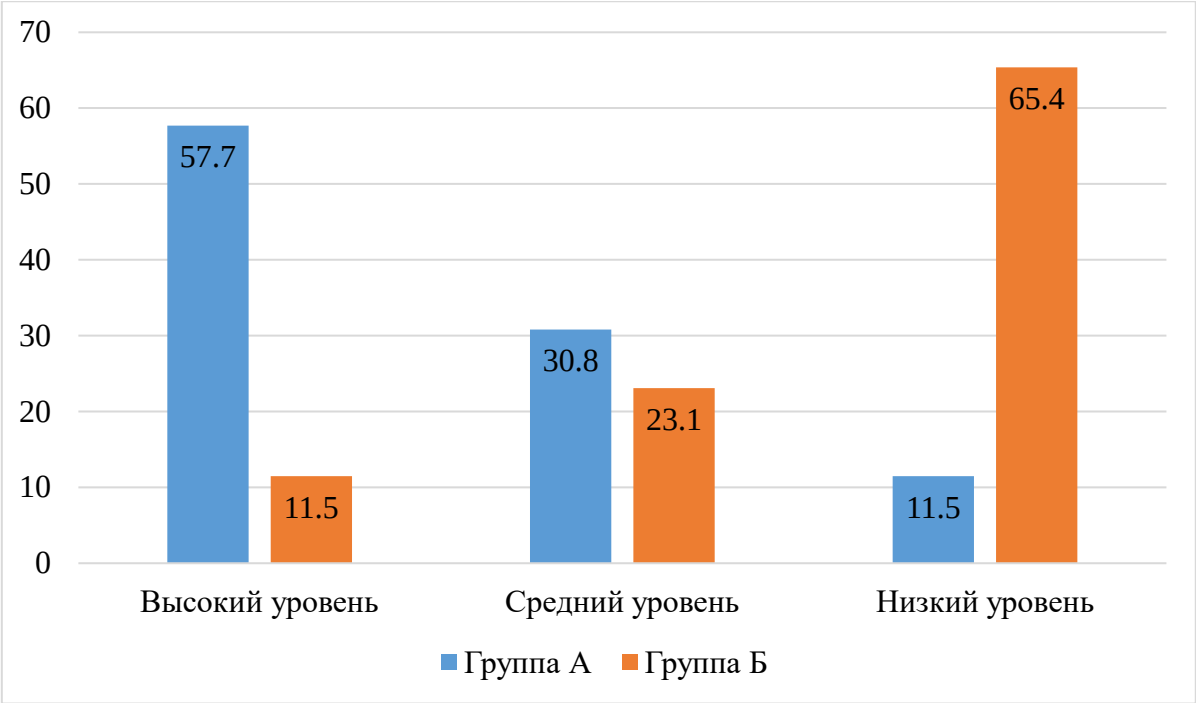

Рисунок 3 – Сравнительная диаграмма показателей уровня готовности практического применения знаний для поиска и обработки информации в Интернете

Для изучения понимание как искать информацию и работать с ней в сети Интернет применим критерий U критерий Манна-Уитни.

Значение U-критерия Манна-Уитни мы нашли по формуле (1).

Было выполнено:

H_0: Уровень признака в группе Б не ниже уровня признака в группе А.

H_1: Уровень признака в группе Б ниже уровня признака в группе А.

В результате психодиагностического обследования групп младших школьников (Группа А – в которой, проводились занятия по кибербезопасности, и группа Б – в которой ничего не проводилось) (по 26 человек в каждой) были выявлены показатели понимание как искать информацию и работать с ней в сети Интернет (в баллах).

Расчёт U-критерия Манна-Уитни по показателю собственного знания основ безопасного поведения в сети Интернет представлен в таблице 5.

Таблица 5 – Расчёт U-критерия Манна-Уитни по показателю готовности практического применения знаний для поиска и обработки информации в Интернете

№	Выборка 1.Группа А.	Ранг 1	Выборка 2. Группа Б.	Ранг 2
1	*2*	*3*	*4*	*5*
1	3	43,5	1	10,5
2	2	27,5	1	10,5
3	1	10,5	3	43,5
4	3	43,5	2	27,5
5	2	27,5	1	10,5
6	3	43,5	3	43,5
7	2	27,5	1	10,5
8	3	43,5	1	10,5
9	3	43,5	2	27,5
10	3	43,5	2	27,5
11	3	43,5	1	10,5
12	3	43,5	1	10,5
13	2	27,5	1	10,5
14	2	27,5	1	10,5
15	3	43,5	1	10,5
16	3	43,5	1	10,5
17	2	27,5	1	10,5
18	2	27,5	1	10,5
19	1	10,5	1	10,5
20	3	43,5	2	27,5
21	3	43,5	2	27,5
22	1	10,5	3	43,5
23	3	43,5	2	27,5
24	2	27,5	1	10,5
25	3	43,5	1	10,5
26	3	43,5	1	10,5
Суммы:		904		474

Сравнение выборки в таблице показывает, что значение выборки группы А несколько выше, чем выборка группы Б, поэтому первой считается выборка группы А.

Значение U-критерия Манна-Уитни мы нашли по формуле (2).

$$U = n_1 n_2 + \frac{n_x(n_x+1)}{2} - T_x, \quad (2)$$

где n_x – наибольшая из объемов выборок n_1 и n_2,

T_x– наибольшая сумма рангов.

Результат: $U_{Эмп} = 123$.

Гипотеза H_0 о незначительности различий между выборками принимается, если $U_{кр} < U_{эмп}$. В противном случае H_0 отвергается и различие определяется как существенное. Где $U_{кр}$ – критическая точка, которую находят по таблице Манна-Уитни. Найдем критическую точку $U_{кр}$.

По таблице находим:

$U_{кр}$ (0.05) = 247.

$U_{кр}$ (0.01) = 210.

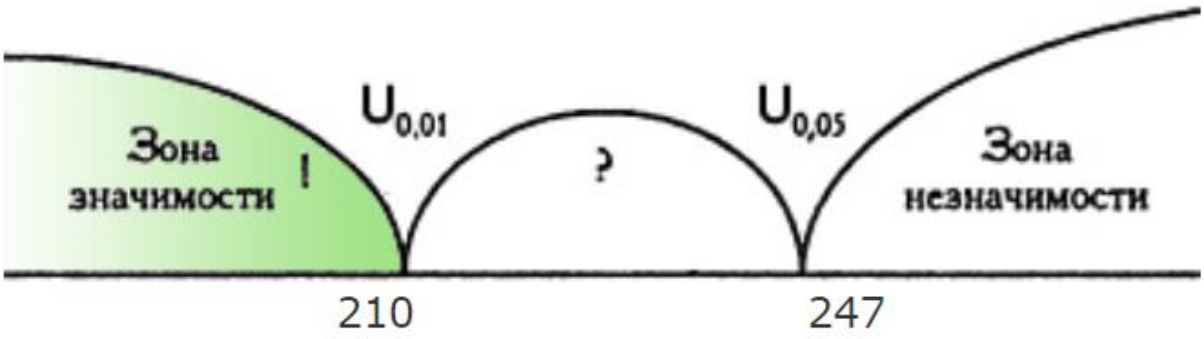

Рисунок 4 – Критерий Манна-Уитни по показателю уровня готовности практического применения знаний для поиска и обработки информации в Интернете

Полученное эмпирическое значение (рисунок 4) $U_{эмп}$ (123) находится в зоне значимости. Так как $U_{кр} < U_{эмп}$ – H_0 отвергается, принимается H_1, различия в уровнях выборок можно считать существенным. Уровень признака в группе Б ниже уровня признака в группе А, что ещё раз подтверждает полученные результаты.

Третья методика, направленная на выявление показателя владения навыками защиты личной информации в сети Интернет представляла собой проведение тестирования.

Тестирование «Безопасно или нет?», разработано на основании имеющихся тестирований и опросников в Интернете, для выявления уровня

знаний в сфере кибербезопасности у младших школьников. Обучающимся предлагался тест, состоящий из 10 вопросов с выбором вариантами ответа. Вопросы охватывают различные аспекты безопасного поведения в Интернете, включая выбор паролей, безопасность электронной почты, неразглашение личной информации, а также работу с интернет-устройствами и платформами. За один правильный ответ на вопрос возможно получить 1 балл.

Подробное описание методики и интерпретация результатов в Приложении В.

В результате данной диагностики в группах были получены следующие данные, приведённые в таблице 6.

Таблица 6 – Результаты исследования владения навыками защиты личной информации у младших школьников

Уровни	Группа А		Группа Б	
	Количество, чел	%	Количество, чел	%
Высокий уровень владения навыками защиты личной информации в сети Интернет	10	38,5 %	2	7,7 %
Средний уровень владения навыками защиты личной информации в сети Интернет	15	57,7 %	13	50 %
Низкий уровень владения навыками защиты личной информации в сети Интернет	1	3,8 %	11	42,3 %

Было выявлено, что обучающиеся из группы А демонстрируют более высокий уровень (38,5 %) и средний уровень (57,7 %) осознания угроз и правил безопасного поведения в сети, чем другие. Хотя из группы Б, также имеется показатель в виде среднего уровня (50 %), что свидетельствует о различиях в степени освоения кибербезопасных навыков среди младших школьников. Такая ситуация подчеркивает необходимость продолжения усилий по повышению уровня информированности всех учащихся в этом важном направлении.

Таким образом, можно сделать вывод, что в Группе А преобладает, как высокий уровень, так и средний уровень владения навыками защиты личной информации в сети Интернет, общению в сети, чем в группе Б.

Для наглядности отобразим полученные результаты в виде диаграммы (рисунок 5).

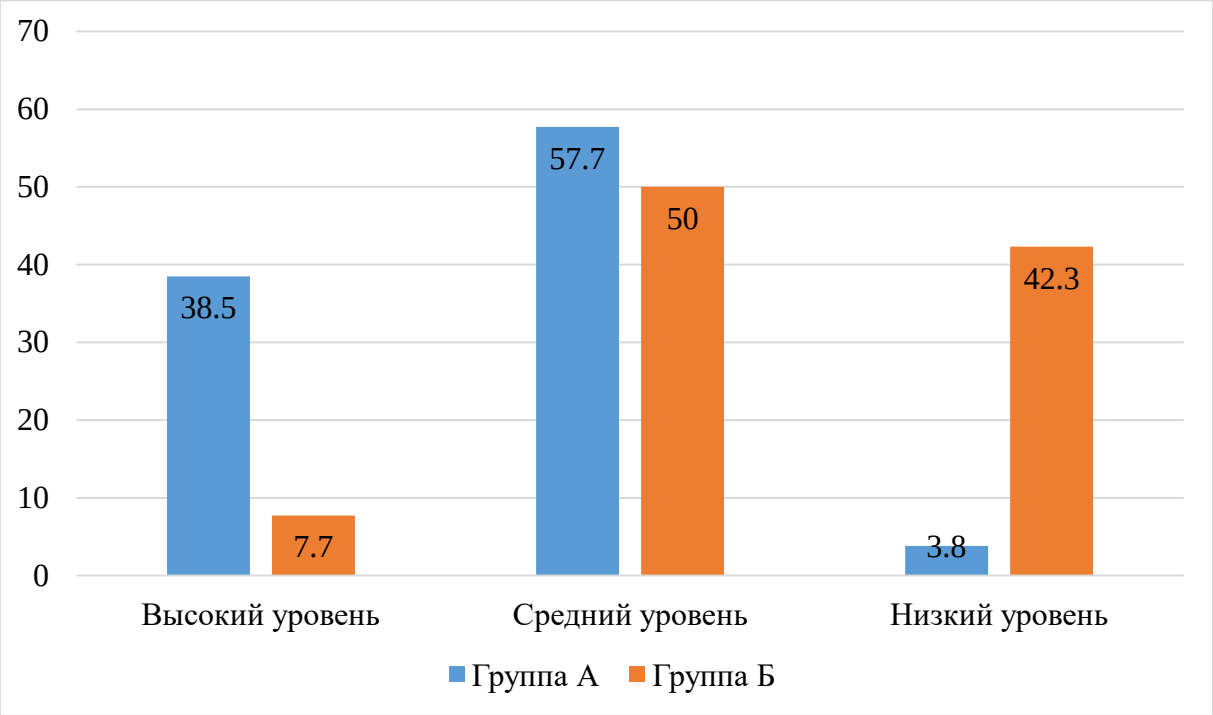

Рисунок 5 – Сравнительная диаграмма показателей уровня владения навыками защиты личной информации в сети Интернет

Для изучения знания основ безопасного поведения в сети Интернет применим критерий U критерий Манна-Уитни.

Было выполнено:

H0: Уровень признака в группе Б не ниже уровня признака в группе А.

H1: Уровень признака в группе Б ниже уровня признака в группе А.

В результате психодиагностического обследования групп младших школьников (Группа А – в которой, проводились занятия по кибербезопасности, и группа Б – в которой ничего не проводилось) (по 26 человек в каждой) были выявлены показатели понимание ребенком как искать информацию и работать с ней в сети Интернет (в баллах).

Расчёт U-критерия Манна-Уитни по показателю владения навыками защиты личной информации в сети Интернет представлен в таблице 7.

Таблица 7 – Расчёт U-критерия Манна-Уитни по показателю владения навыками защиты личной информации в сети Интернет

№	Выборка 1	Ранг 1	Выборка 2	Ранг 2
1	9	43,5	9	43,5
2	8	38,5	4	11
3	10	49,5	4	11
4	8	38,5	9	43,5
5	5	15,5	7	31,5
6	10	49,5	2	3
7	6	22,5	3	7
8	7	31,5	7	31,5
9	7	31,5	5	15,5
10	10	49,5	6	22,5
11	10	49,5	2	3
12	6	22,5	2	3
13	10	49,5	1	1
14	9	43,5	6	22,5
15	9	43,5	5	15,5
16	7	31,5	6	22,5
17	7	31,5	7	31,5
18	8	38,5	3	7
19	6	22,5	3	7
20	7	31,5	8	38,5
21	3	7	6	22,5
22	7	31,5	4	11
23	5	15,5	5	15,5
24	6	22,5	5	15,5
25	9	43,5	3	7
26	10	49,5	7	31,5
Суммы:		903,5		474,5

Сравнение выборки в таблице показывает, что значение выборки группы А несколько выше, чем выборка группы Б, поэтому первой считается выборка группы А.

Значение U-критерия Манна-Уитни мы нашли по формуле (3).

$$U = n_1 n_2 + \frac{n_x(n_x+1)}{2} - T_x, \quad (3)$$

где n_x – наибольшая из объемов выборок n_1 и n_2,

T_x– наибольшая сумма рангов.

Результат: $U_{Эмп}$ = 123,5.

Гипотеза H_0 о незначительности различий между выборками принимается, если $U_{кр} < U_{эмп}$. В противном случае H0 отвергается и различие определяется как существенное. Где $U_{кр}$ – критическая точка, которую находят по таблице Манна-Уитни. Найдем критическую точку $U_{кр}$.

По таблице находим:

$U_{кр}$ (0.05) = 247.

$U_{кр}$ (0.01) = 210.

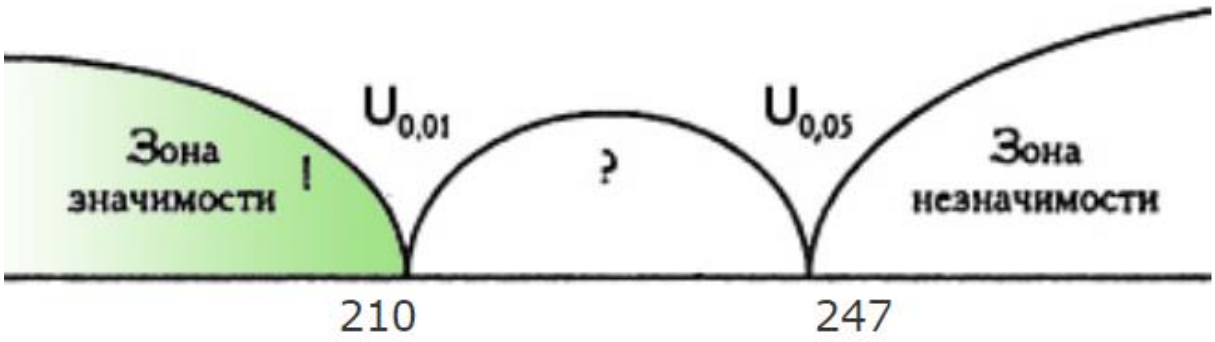

Рисунок 6 – Критерий Манна-Уитни по показателю уровня владения навыками защиты личной информации в сети Интернет на оси значимости

Эмпирическое значение (рисунке 6) $U_{эмп}$ (123,5) находится в зоне значимости. Так как $U_{кр} < U_{эмп}$ – H_0 отвергается, принимается H_1, различия в уровнях выборок можно считать существенным. Уровень признака в группе Б ниже уровня признака в группе А.

Анализ полученных данных и эффективность деятельности педагога позволили выявить, что обучающиеся из группы А демонстрируют более высокую степень осведомленности об угрозах и о правилах безопасного поведения в интернете по сравнению с группой Б. Эти результаты отражают различия в успешности формирования навыков кибербезопасности среди младших школьников и акцентируют внимание на необходимости

продолжения работы по повышению осведомленности всех обучающихся в этой области.

2.2 Анализ существующих программ процесса формирования основ кибербезопасности

В процессе предпроектного исследования работы педагога-психолога по формированию основ кибербезопасности у младших школьников, нами было принято решение проанализировать программы педагогов-психологов, учителей начальных классов по схожей теме, SWOT-анализ которых будет применен к нашему собственному продукту. Были проанализированы такие программы, как:

– «Безопасность в сети интернет» психолого-педагогическая программа г. Белгород ОГБУ «Белгородский региональный центр психолого-медико-социального сопровождения» Е. А. Викторова, К. Г. Лобынцева (https://clck.ru/3M22tY);

– Дополнительная общеразвивающая программа социально-педагогической (социально-гуманитарной) направленности «Безопасность в сети Интернет» г. Санкт-Петербург, ГБУ ДО «ЦПМСС Красносельского района, педагог-психолог Н. В. Моисеенко (https://clck.ru/3MHrsP);

– Рабочая программа по внеурочной деятельности «Информационная безопасность» 1-4 класс, МКОУ ООШ с. Мокино, учитель Т. А. Полушина (https://clck.ru/3M22h4).

Данное решение и выбор программ были обусловлены тем, что с одной стороны анализ существующих на данный момент программ не позволил бы выделить характерные особенности опыта работы педагога-психолога с младшими школьниками в виду их достаточно малого количества, из-за чего для анализа мы взяли программу внеурочной деятельности, разработанную учителем начальных классов. С другой стороны, мы считаем, что анализ программ для подростков и обучающихся старших классов позволит выявить недостатки и преимущества, для

адаптации и разработки программ для обучающихся младшего школьного возраста как с психологической, так и с педагогической стороны изучения данной проблемы.

Отметим опыт реализации психолого-педагогической программы «Безопасность в сети интернет» (для обучающихся 13-17 лет) из реестра программ Федерации психологов образования России, авторами которой являются Викторова Е.А., директор ОГБУ «Белгородский региональный центр психолого-медико-социального сопровождения» и Лобынцева К. Г., старший методист отдела диагностики, консультирования и коррекционно-развивающей работы ОГБУ «Белгородский региональный центр психолого-медико-социального сопровождения». Занятия данной программы эффективно способствовали профилактике интерне-зависимостей у обучающихся, осознанному подходу к вопросам кибербезопасности и пониманию важности соблюдения правил в интернете. Реализация программы в образовательных организациях Белгородской области показала высокие результаты: обучающиеся не только успешно осваивали материал, но и проявляли активность в обсуждениях, задавая множество вопросов. Это свидетельствует о том, что программа стимулирует интерес и желание узнать больше о информационном пространстве. Опросы родителей и учителей подтвердили положительный эффект, отмечая увеличение осведомленности детей о рисках в интернете.

Ещё одним примером служит дополнительная общеразвивающая программа социально-педагогической (социально-гуманитарной) направленности «Безопасность в сети Интернет» (для обучающихся 11-15 лет), г. Санкт-Петербург, ГБУ ДО «ЦПМСС Красносельского района, разработанная педагогом-психологом Н. В. Моисеенко, нацелена на обучение принципам безопасного поведения в интернете, охватывая как социальные, так и гуманитарные аспекты взаимодействия с цифровой средой. Программа ставит перед собой задачу содействия формированию у обучающихся компетенции, необходимой для успешной социализации. Она

акцентируется на развитии медиаграмотности и на обучении детей правильному использованию коммуникаций в цифровой среде. Таким образом, данная программа предоставляет всесторонний подход к повышению навыков интернет-безопасности у подростков, способствуя их успешной социализации и личностному развитию в цифровую эпоху. Про реализацию программы известно, что она внедрялась специалистами ГБУ ДО «ЦПМСС Красносельского района» в общеобразовательные учреждения в 2023-2024 учебном году.

Особенностью программы мы можем выделить то, что она имеет гибкость в выборе тем, которые могут быть адаптированы в соответствии с возрастными особенностями участников, в нашем случае для младших школьников.

Одним ощутимым минусом, выделенным нами из двух представленных выше программ стало то, что своей структуре программы более-менее похожи, а также что программ педагогов-психологов направлены больше на подростков и обучающихся старших классов.

Третьим примером мы выделили программу внеурочной деятельности «Информационная безопасность» 1-4 класс, МКОУ ООШ с. Мокино, разработанная учителем начальных классов Т. А. Полушиной. Эта программа была составлена с учетом законодательства Российской Федерации, включая акты «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию», а также санитарные требования, регулирующие условия образовательного процесса.

Главное новшество программы «Информационная безопасность» заключается в формировании у младших школьников как межпредметных, так и предметных компетенций через дисциплину «Информамика», связанных с безопасным и обоснованным использованием цифровых технологий и интернет-ресурсов.

Для проведения глубокого анализа программ, с акцентом на выявление их преимуществ и недостатков, а также потенциальных рисков и перспектив, связанных с их внедрением, мы использовали методику SWOT-анализ. Его результаты представлены в таблице 8.

Таблица 8 – SWOT-анализ программ, направленных на формирование основ кибербезопасности

«Безопасность в сети интернет» психолого-педагогическая программа г. Белгород ОГБУ «Белгородский региональный центр психолого-медико-социального сопровождения» Е.А. Викторова, К. Г. Лобынцева		
1	*2*	*3*
Сильные стороны	Слабые стороны	Направленность программы
Программа основана на психологической модели цифровой компетентности. Структура логична, имеется правовые аспекты, цели, задачи, список источников и т.д. Соответствие возрасту и психологическим особенностям обучающихся. Содержание и структура занятий учитывают интересы и жизненный опыт школьников. Структура программы рассчитана на 34 часа (состоит из 4 блоков, где занятия проводятся в форме лекций-бесед с элементами психологического тренинга. Наличие поурочных разработок всех 34 занятий. Имеется список литературы, перечень учебников и пособий по информационной безопасности и психологии, указаны интернет-источники, а также имеется глассарий с основными понятиями. Использование активных форм и методов обучения.	Программа требует наличия образовательной среды, соответствующей потребностям развития обучающихся. Отсутствуют количественные показатели для оценки эффективности реализации психологической программы, что затрудняет подтверждение овладения формируемых компетенций по блокам. Работа программы направлена только на обучающихся.	Программа «Безопасность в сети Интернет» направлена на обеспечение информационно-психологической безопасности детей и подростков.

Продолжение таблицы 8

1	*2*	*3*
Программа содержит достаточное количество таких методов для интеллектуального, эмоционально-волевого и личностно-мотивационного развития подростков и старшеклассников. Оценочные материалы представлены вопросами для самопроверки по различным аспектам интернета; вопросами по персональным данным, сетевому этикету и подводным камням интернета. Программа проходила апробацию в 10 образовательных организациях Белгородской области с 1 сентября 2017 г. по 25 мая 2018 г. Программа получила высокую оценку участников и педагогов.		
Возможности	Угрозы	Деятельность педагога
Предполагает реализацию в рамках программ внеурочной деятельности, в рамках программ воспитания и социализации. Предполагает диагностику обучающихся во время внедрения программы (по итогу каждого блока программы проводится опрос).	Для реализации программы необходимы определённые ресурсы и специалисты. Направлена только на подростков и старшеклассников (что требует пересмотра её структуры для внедрения её в начальное звено). Программа предполагает обеспечение гарантий прав участников, описывает сферы ответственности, основные права и обязанностей участников программы, но насколько это всё соблюдается в процессе реализации программы (чем подкрепляется).	Программа реализуется педагогом-психологом образовательной организации

Продолжение таблицы 8

Дополнительная общеразвивающая программа социально-педагогической (социально-гуманитарной) направленности «Безопасность в сети Интернет» Н. В. Моисеенко		
Сильные стороны	Слабые стороны	Направленность программы
Программа носит общеразвивающий характер и предназначена для использования в общеобразовательных организациях. Структура логична, имеется правовые аспекты, цели, задачи, список источников и т.д. Использование дистанционных образовательных технологий и электронного обучения. Наличие поурочных разработок. Проведение анкетирования и сбор отзывов учащихся, родителей и педагогов Программа предполагает обеспечение гарантий прав участников, описывает сферы ответственности, основные права и обязанностей участников программы, что подкрепляется договором между центром и образовательной организацией. Анализ результатов анкетирования и отзывов для определения результативности. Текущий контроль через наблюдение и рефлексию учащихся.	Программа требует наличия образовательной среды, соответствующей потребностям развития обучающихся. Отсутствуют количественные показателя для оценки эффективности реализации психологической программы, что затрудняет подтверждение овладения формируемых компетенций по блокам. Программа направлена на формирование медиаграмотности, хотя речь идет больше про безопасность в Интернете. Работа программы направлена только на обучающихся.	Социально-педагогическая направленность (формирование социальной компетентности и медиаграмотности)

Продолжение таблицы 8

Возможности	Угрозы	Деятельность педагога
Программа носит модульный характер, предлагаемые темы могут меняться в соответствии с возрастом учащихся. Возможность применения в сочетании с другими программами и использование ее результатов другими специалистами для групповой и индивидуальной работы.	Для реализации программы необходимы определённые ресурсы и специалисты (должны быть педагоги-психологи и социальные педагоги). Направлена только на подростков и старшеклассников (что требует пересмотра её структуры для внедрения её в начальное звено).	Программа реализуется педагогом-психологом, направленным центра психолого-педагогической, медицинской и социальной помощи в образовательную организацию.
Программа внеурочной деятельности «Информационная безопасность» 1-4 класс, Т. А. Полушина		
Сильные стороны	Слабые стороны	Направленность программы
Программа рассчитана на 4 года начальной школы. Занятия проводятся в комбинированной, теоретической и практической форме.	Темы занятий нуждаются в актуализации материалов. Отсутствие поурочных разработок. Работа программы направлена только на обучающихся.	Направлена на формирование у школьников культуры информационной безопасности в условиях цифрового мира. Она включает в себя вопросы безопасного поведения в интернете, методы предупреждения и защиты от негативного стороннего воздействия, вопросы сетевой этики и другие.
Возможности	Угрозы	Деятельность педагога
Интеграция с учебным курсом «Информатика».	Предполагает затраты на подготовку практических занятий для каждого класса. Всесторонний охват опыта младших школьников предусматривает избыточность материала и практических занятий	Реализация педагогом (классным руководителем)

Подводя итоги выше сказанному, опыт педагогов-психологов показывает, что правильно организованный процесс обучения может значительно повысить уровень осведомленности детей и помочь им научиться безопасно использовать интернет-пространство. Анализ и реализации программ среди подростков и обучающихся старших классов

позволяет выявить недостатки и преимущества, для адаптации и разработки программ для обучающихся начальной школы.

Выявленные сильные стороны программ включают их модульную структуру, соответствие возрастным особенностям, гибкость и возможность интеграции с другими образовательными программами. Среди слабых сторон были выделены: нехватка поурочных планов, необходимая система оценок, внимание только на обучающихся, затраты на подготовку занятий для каждого класса при многолетней реализации и необходимость специалистов. Также имеющийся в программах полезный материал, мы извлекли и адаптировали для нашей программы, и использовали при её реализации. Мы также признаём необходимость создания программы, подходящей для младших школьников, что обусловливает её актуальность. В ходе разработки программы работы педагога-психолога мы постарались учесть вышеизложенные выводы.

Подробное описание программы и дорожная карта её внедрения представлены в следующей параграфе.

2.3 Программа работы педагога-психолога по формированию основ кибербезопасности младших школьников и дорожная карта продвижения проекта

На основании результатов, полученных в ходе проведенного научного исследования, в данном параграфе представлена программа работы педагога-психолога по формированию основ кибербезопасности для обучающихся 4 классов. Настоящая программа разработана в результате детального анализа документов, литературы, исследовательских данных и дополнительных ресурсов, связанных с формированием основ кибербезопасности.

Программа представляет собой структурированное руководство для педагога-психолога, направленное на развитие основ кибербезопасности у младших школьников.

Новизна программы заключена в достижении формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Ниже, в таблице 9, мы представили паспорт нашей программы работы педагога-психолога по формированию основ кибербезопасности для обучающихся младшего школьного возраста.

Таблица 9 – Паспорт программы

Паспорт программы	
1	*2*
Полное наименование программы	Работа педагога-психолога по формированию основ кибербезопасности у младших школьников
Разработчик программы	Педагог-психолог
Сроки реализации программы	Реализация программы рассчитана на период с октября по апрель учебного года
Целевая аудитория программы	Обучающиеся 4 класса, их родители, педагоги, психолог образовательного учреждения
Нормативно-правовая основа программы	1.Конвенция ООН о правах ребёнка, принятая Генеральной Ассамблеей ООН 20 ноября 1989 г. 2.Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.05.2024). 3.Федеральный государственный образовательный стандарт начального общего образования, утвержденный приказом Минпросвещения России от от 31.05.2021 N 286 (ред. от 08.11.2022) «Об утверждении федерального государственного образовательного стандарта начального общего образования». 4.Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. Федеральных законов от 30.11.2024 № 438-ФЗ). 5.Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 (в ред. Федеральных законов от 26.12.2024 № 479-ФЗ) 6.Распоряжение Правительства Российской Федерации от 28.04.2023 №1105-р «О концепции информационной безопасности детей в Российской Федерации».

Продолжение таблицы 9

1	*2*
Основная цель программы	Создание условий, позволяющих наиболее эффективно выстроить формирование у обучающихся младшего школьного возраста основ кибербезопастности, базовых принципов безопасного поведения в сети Интернет и безопасности личного информационного пространства.
Основные задачи программы	–Содействовать развитию умения безопасной работы с информацией, анализировать и обобщать полученную информацию; –формировать у младших школьников базовую систему знаний о безопасном поведении и информационной этике при работе с компьютерными программами, информацией в сети Интернет; –развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий; –содействовать в усвоение сознательного и бережного отношения к вопросам собственной информационной безопасности в стенах образовательной организации, в семье; –развивать нравственные, этические, патриотические качеств личности в процессе формирования основ кибербезопасности.
Особенность программы	Программа предусматривает совместную деятельность педагога-психолога и классного руководителя (учителя) по формированию основ кибербезопасности, психологической коррекции аддиктивных проявлений в информационной среде (кибербуллинг, игровая зависимость и т.д.), консультировании родителей по стратегии минимизации рисков, связанных с онлайн-угрозами.
Принципы для построения и реализации программы	–Принцип гуманизма; –принцип единства диагностики и коррекции; –принцип развития; –принцип доступности, системности; –принцип рефлексивности; –принцип мотивации; –принцип активной включенности; принцип практико-ориентированности.

Продолжение таблицы 9

1	*2*
Ожидаемые результаты	–Повышение уровня информативности школьников, в результате владения знаниями о интернет-рисках и угрозах к информационном пространстве. –Умение анализировать и критически относиться к информации в Интернете. –Формирование мотивации к ответственному использованию информационно-коммуникационных технологий. –Умение определять наличие негативного, недостоверного, небезопасного содержания в интернет-контенте. –Владение эффективными способа защиты от не нежелательной информации, контактов в Интернете и их применение на практике. –Владение нормами интернет-этикета, приёмами эффективной коммуникации. –Развитие педагогических навыков для помощи младшим школьникам, испытывающим трудности в обучении кибербезопасности. –Формирование компетенций у родителей в области обучения младших школьников основам кибербезопасности. –Разработка рекомендаций для педагогов и родителей по эффективному педагогическому сопровождению. –Умение владеть принципами уважительного и толерантного отношения к другим пользователям при взаимодействии в сети Интернет. –Повышение осведомлённости родителей для эффективного сопровождения детей в процессе освоения информационных технологий. –Укрепление психологического здоровья.
Средства мониторинга эффективности реализации программы	–Наблюдение за поведением детей, –консультации родителей.

Программа предназначена для обучающихся 10-11 лет, рассчитанная на срок с октября по апрель учебного года обучающихся 4 классов. На реализацию курса отводится 1 час в неделю (36 занятий).

В результате мы считаем, что нами был разработан достаточно универсальный проект, призванный усилить взаимодействие педагога-психолога с обучающимися, учитывающий наиболее важные критерии по

формированию компетенций, способствующие обеспечению кибербезопасности школьников.

При разработке нашей программы мы учли все ключевые направления работы педагога-психолога, такие как организационное, диагностическое, индивидуально-коррекционное, просветительское и аналитическое.

Универсальность проекта проявляется в том, что в нем указаны ключевые направления деятельности, направленной для безопасной социализации личности младшего школьника так, чтобы научить обучающегося противостоять информационным угрозам и отделять положительное от отрицательного, среди многообразного потока информации в Интернете.

Подробное описание программы представлено в Приложении Г.

Для внедрения нашей программы работы педагога-психолога по формированию основ кибербезопасности предложим дорожную карту её внедрения.

Ключевые направления работы ориентированы на формирование информационной поддержки и осуществление педагогического мониторинга формирования основ кибербезопасности учащихся младшей школы.

Особый акцент делается на улучшении образовательной среды, способствующей формированию кибербезопасного поведения детей, с учетом их индивидуальных особенностей.

Планируемые итоги реализации: повышение уровня понимание основ кибербезопасности младших школьников; участники программы будут лучше оценивать информацию из интернет-ресурсов и критически подходить к ее использованию и т.д.

Структура дорожной карты охватывает целевой, подготовительный, организационный, контрольно-аналитический и коррекционный блоки, представленные в таблице 10.

Таблица 10 – Дорожная карта внедрения программы работы педагога-психолога

№	Наименование мероприятия	Срок реализации	Ответственные исполнители
1	*2*	*3*	*4*
Целевой			
1.	Определение целей для формирования основ кибербезопасности младших школьников.	Январь	Завуч, педагог-психолог, классный руководитель
Подготовительный			
1.	Сбор данных об имеющихся потребностях формирования основ кибербезопасности у обучающихся начальной школы с целью выявления актуальности реализации программ. С этой целью будет проведен сбор запросов (в виде анкет), как обучающихся, так и их законных представителей (родителей).	Февраль	Классный руководитель
2.	Анализ полученных результатов исследования потребностей формирования основ кибербезопасности у обучающихся начальной школы.	Февраль	Классный руководитель
Организационный			
1.	Организация и проведение педагогические заседания, посвященные вопросам подготовки к внедрению программы по формированию основ кибербезопасности. Необходимо формирование положительной психологической установки, заинтересованности субъектов образовательной организации.	Март	Завуч, педагог-психолог, классный руководитель
2.	Анализ материально- технических (ресурсного) обеспечения для реализации программы: – нормативно-правовая база (актуализация локальных актов в образовательном учреждении); – финансово-экономическое обеспечение (возможность бесплатного обучения); – организационно-управленческие механизмы (возможность сотрудничества с организациями иных видов); – информационно-аналитический комплекс (создание цифровых платформ для дистанционной реализации программы); – учебно-методическое сопровождение (наличие УМК); – кадровая политика (наличие необходимых педагогических кадров); – материально-техническая инфраструктура (наличие оснащенного кабинета / места работы).	Март	Завуч, педагог-психолог

Продолжение таблицы 10

3.	Проведение и участие педагогов в конференциях, семинарах по вопросу формирования основ кибербезопасности детей начальной школы.	Учебный год	Завуч
4.	Проведение входной диагностики детей для выявления текущего уровня основ кибербезопасности.	Сентябрь	Педагог-психолог
5.	Включение программы образовательный процесс. Организация работы с родителями в формировании основ кибербезопасноти детей младшего школьного возраста.	Октябрь-май	Педагог-психолог
6.	Включение программы образовательный процесс для проведения занятий. Организация работы с детьми по формированию основ кибербезопасности.	Октябрь-май	Педагог-психолог
Контрольно-аналитический			
1.	Диагностика и анализ результатов внедрения программы работы педагога-психолога по формированию основ кибербезопасности у младших школьников. Результатом может выступить положительные изменения в образовательных достижений обучающихся.	Май	Педагог-психолог, классный руководитель
Коррекционный			
1.	Корректировка осуществляемой деятельности с целью усовершенствования программы работы педагога-психолога по формированию основ кибербезопасности у младших школьников.	Июнь-август	Педагог-психолог, классный руководитель

Таким образом, нами предлагаются следующие мероприятия по внедрению программы работы педагога-психолога по формированию основ кибербезопасности учеников начальной школы. Главное в такой работе – включение всех участников образовательного процесса.

Результативность программы будет оценена после проведения мониторинга, организованного в виде проведения анкетирования родителей и опекунов детей младшего школьного возраста, а также классных руководителей.

Данная анкета будет отражать следующие аспекты для оценки:

1. Каковы были цели и задачи программы работы педагога-психолога по формированию основ кибербезопасности учеников начальной школы?

2. Получали ли Вы положительные отзывы детей, участников данной программы?

3. Наблюдали ли Вы какие-либо изменения в поведении или

эмоциональной сфере ребенка после реализации в этой программе?

4. Если изменения были, то какие? Опишите их подробнее.

5. Ваши впечатления относительно программы. Считаете ли Вы, что она достигла своих целей и была эффективной?

6. Укажите, пожалуйста, Ваши предложения или пожелания по улучшению программы.

Эффективность программы будет определяться её одобрением и принятием, что свидетельствует о соответствии установленным в ней целям и задачам.

Выводы по главе 2

Во второй главе мы организовали предпроектное исследование по проблеме формирования основ кибербезопасности младших школьников и описали результаты.

Исследование проводилось на базе общеобразовательной школы г. Челябинска, где, согласно двум независимым выборкам приняли участие 52 обучающихся 4 класса. Группа А – в количестве 26 человек, посещающий занятия, мероприятия, проводимые учителем (педагогом-психологом) в тематике нашего исследования, а также группа Б – в количестве 26 человек, где такие занятия не проводились (т.е. основываясь только на жизненный опыт).

В результате описанных нами методик и показателей формирования основ кибербезопасности (собственное знание правил безопасного поведения в сети Интернет; готовность практического применение знаний для поиска и обработки информации в Интернете, владения навыками защиты личной информации в сети Интернет), было выявлено, что в Группе А преобладают высокий и средний уровень сформированности основ кибербезопасности, чем в группе Б.

Эти результаты отражают различия в успешности формирования навыков кибербезопасности среди младших школьников и акцентируют

внимание на необходимости продолжения работы по повышению осведомленности всех обучающихся в этой области.

Для анализа программ по формированию основ кибербезопасности была выбрана программа внеурочной деятельности, созданная учителем начальных классов. Кроме того, были изучены программы, предназначенные для подростков и учеников старших классов, предоставляющие возможность выявить их достоинства и недостатки, что помогло в адаптации и разработке программы для младших школьников с учетом психологических и педагогических аспектов. Выявленные сильные стороны (модульная структура, соответствие возрастным особенностям, гибкость и возможность интеграции с другими образовательными программами и др.) и слабые стороны (нехватка поурочных планов, необходимая система оценок, внимание только на обучающихся, затраты на подготовку занятий для каждого класса при многолетней реализации и необходимость специалистов и др.) существующих программ, их риски, угрозы мы также отразили в ходе разработки нашей программы по формированию основ кибербезопасности.

Для повышения уровня основ кибербезопасности нами была разработана программа работы педагога-психолога по формированию основ кибербезопасности обучающихся 4 классов. Программа представляет собой структурированное руководство для педагога-психолога, направленное на развитие основ кибербезопасности у младших школьников.

Разработанный и описанный алгоритм внедрения программы работы педагога-психолога по формированию основ кибербезопасности младших школьников в педагогическую деятельность будет свидетельствовать о успешной реализации программы.

ЗАКЛЮЧЕНИЕ

Целью исследования было теоретически обосновать аспекты работы педагога-психолога и разработать программу по формированию основ кибербезопасности у младших школьников и дорожную карту её реализации.

На основании анализа психолого-педагогической литературы были изучены понятия:

– информационная безопасность, под которой понимается состояние защищенности, при котором исключаются риски, связанные с негативным влиянием информации физическое и психическое здоровье, духовное и моральное развитие детей.

– кибербезопасность, представляющая собой составляющую часть информационной безопасности, ориентированной на изучение особенностей киберобъектов, нормативную документацию, источники опасности в цифровой среде.

В нашем исследовании понятие «Кибербезопасность младших школьников» представлено как совокупность мер и стратегий, направленных на обеспечение безопасного и защищённого взаимодействия детей младшего школьного возраста с цифровыми технологиями и интернет-средой. Это включает развитие у них навыков для распознавания киберугроз, применение инструментов для защиты личных данных, а также обучение принципам безопасного поведения в онлайн-сообществах.

В рамках этих понятий были выделены основные источники информации, влияющие на детей, такие как государственные и общественные структуры, социальные группы, отдельная личность. Эти источники могут предлагать информацию различного качества, которая может быть недостоверной или неэтичной. В качестве средств информационного воздействия выступают СМИ, литература, образовательные услуги и межличностное общение [27].

Эффективное формирование основ кибербезопасности у младших школьников тесно связано с особенностями развития, такими как критическое мышление, гибкость мышления, хорошая память и высокая эмоциональная восприимчивость. Также важно учитывать, что значительное количество времени ребенок проводит в образовательном учреждении, где учебная деятельность является его основной деятельностью для формирования комплекса норм и практических стратегии по защите от возможных атак злоумышленников в киберпространстве. Выделенные нами в ходе анализа научных источников особенности младшего школьного возраста следует учитывать при работе педагога-психолога.

На основании профессионального стандарта «Педагог-психолог (психолог в сфере образования)» выделены направления работы педагога-психолога по формированию основ кибербезопасности, такие как организационное, диагностическое, просветительское, индивидуально-коррекционное и аналитическое. Данные направления работы наладить взаимодействие всех участников образовательного процесса, способствуя формированию безопасных привычек в цифровом мире, критического мышления и устойчивого эмоционального состояния. В результате младшие школьники смогут уверенно противостоять угрозам, возникающим в онлайн-пространстве.

Изучение уровня сформированности основ кибербезопасности и культуры безопасного поведения в интернете среди младших школьников, а также анализ эффективности педагогической деятельности показали, что обучающиеся из группы А (класс, где проводились мероприятия, направленные на формирование основ кибербезопасности) имеют более высокий уровень осведомленности об интернет-угрозах и правилах безопасного поведения по сравнению с группой Б (класс, где ничего не проводилось).

Эти результаты отражают различия в успешности формирования навыков кибербезопасности среди младших школьников и акцентируют внимание на необходимости продолжения работы по повышению осведомленности всех обучающихся в этой области.

Проведя анализ существующих программ по формированию основ кибербезопасности в предпроектном исследовании, мы выделили две программы, направленные на обучающихся старших и средних классов (полезный материал которых мы можем извлечь и адаптировать в дальнейшем для нашей программы, и использовать при её реализации), а также одну программу для младших школьников.

Выявленные сильные стороны (модульная структура, соответствие возрастным особенностям, гибкость и возможность интеграции с другими образовательными программами и др.) и слабые стороны (нехватка поурочных планов, необходимая система оценок, внимание только на обучающихся, затраты на подготовку занятий для каждого класса при многолетней реализации и необходимость специалистов и др.) существующих программ, их риски, угрозы мы также отразили в ходе разработки нашей программы по формированию основ кибербезопасности.

По результатам предпроектного исследования была разработана программа работы педагога-психолога по формированию основ кибербезопасности у младших школьников и дорожная карта её реализации. Особенностью программы является совместная деятельность педагога-психолога и классного руководителя (учителя) по формированию основ кибербезопасности, психологическая коррекция аддиктивных проявлений в информационной среде (кибербуллинг, игровая зависимость и т.д.), консультирование родителей средствами проведения родительских собраний по стратегии минимизации рисков, связанных с онлайн-угрозами,

Разработанная и подробно изложенная дорожная карта реализации программы педагогов-психологов по формированию основ кибербезопасности у младших школьников станет показателем успешного

внедрения данной программы в образовательную организацию.

Таким образом, задачи нашего исследования решены, и цель нашего исследования достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Абдуразаков М. М. Современные проблемы обеспечения информационной безопасности в образовательно-педагогической сфере / М. М. Абдуразаков, З. О. Батыгов // Информатика и образование. – 2021. – № 10. – URL : https://info.infojournal.ru/jour/article/view/759 (дата обращения: 17.03.2025).

2. Аверин В. А. Психология детей и подростков: учеб. пособие / В. А. Аверин. – 2-е изд. – Санкт-Петербург : Михайлова В. А., 2018. – 379 с. – ISBN 5-8016-0034-5.

3. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность / А. С. Алпеев // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 39–42.

4. Бабаш А. В. Информационная безопасность. Лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – Москва : КноРус, 2023. –131 с. – ISBN 978-5-406-11731-6.

5. Базавлуцкая Л. М. Информатизация в системе профессионального образования : монография / Л. М. Базавлуцкая, О. Н. Шварцкоп, А. М. Рудакова. – Челябинск : Изд-во ЗАО «Библиотека А. Миллера», 2019. – 301 с. – ISBN 978-5-93162-208-8.

6. Баракина Т. В. Формирование навыков информационной безопасности у детей дошкольного и младшего школьного возраста / Т. В. Баракина // Информатика в школе. – 2017. – № 7. – URL: https://school.infojournal.ru/jour/article/view/162 (дата обращения: 13.01.2024).

7. Батюта М. Б. Возрастная психология : учеб. пособие / М. Б. Батюта, Т. Н. Князева. – Нижний Новгород : ДЕКОМ, 2018. – 240 с. – ISBN 978-5-89533-407-2, 978-5-89533-407-3.

8. Безкоровайный М. М. Кибербезопасность – подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Вопросы кибербезопасности. – 2014. – № 1(2). – С. 22–27.

9. Беленов Н. В. Формирование навыков информационной безопасности в сети интернет у обучающихся 5-9 классов / Н. В. Беленов, О. С. Самсонова //Проблемы современной науки и образования. – 2020. – № 7(37). – С. 54-57.

10. Божович Л. И. Личность и ее формирование в детском возрасте / Л. И. Божович. – Москва: Питер, 2022. – 400 с. – ISBN 978-5-4461-1955-4.

11. Бордовская Н. В. Педагогика: учеб. пособие. / Н. В. Бордовская, Е. А. Кошкина. – Москва : КноРус, 2022. – 456 с. – ISBN 978-5-406-09235-4.

12. Босова Л. Л. Об информационной безопасности в общеобразовательной школе / Л. Л. Босова, А. Ю. Босова // Информатика в школе. – 2017. – № 7 (130). – URL : https://school.infojournal.ru/jour/article/view/150 (дата обращения: 03.11.2024).

13. Бочаров М. И. Сетевые сообщества и информационная безопасность в непрерывном образовании средней общеобразовательной и профессиональной школы / М. И. Бочаров // Вестник Российского университета дружбы народов. Серия: Информатизация образования. – 2009. – № 4. – С. 20–27.

14. Букина Е. Ю. Формирование у младших школьников навыков безопасной работы в сети Интернет / Е. Ю. Букина // Информатика в школе. – 2014. – № 5 (98). – С. 40–49.

15. Ведерникова О. Н. Международно-правовые основы противодействия преступлениям против детей в сети Интернет / О. Н. Ведерникова // Международное уголовное право и международная юстиция. – 2022. – № 2. – С. 2–5.

16. Взрослые и дети в интернете: аналитический отчёт 2023 // Kids Safe Media: [сайт]. – 2023. – URL:

https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_analiticheskiy_otchet_2023 (дата обращения: 13.03.2025).

17. Вишнякова С. М. Профессиональное образование: словарь. Ключевые понятия, термины, актуальная лексика. / С. М. Вишнякова. – Москва : НМЦ СПО, 1999. – 538с. – ISBN 5-89714-013-8.

18. Волчегорская Е. Ю. Подверженность кибербуллингу детей младшего школьного возраста /Е. Ю. Волчегорская, М. В. Жукова, Е. В. Фролова, К. И. Шишкина // Ученые записки университета им. П. Ф. Лесгафта. – 2019. – №10 (176). – С. 412–416.

19. Гафарова Е. А. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Е. А. Гафарова. – Челябинск : Изд-во ЗАО «Библиотека А. Миллера»,2019. –127 с. – ISBN 978-5-93162-170-8.

20. Гиппенрейтер Ю. Б. Как бы ты поступил? Сам себе психолог : Психология для детей / Ю. Б. Гиппенрейтер, А. Н. Рудаков. – Москва : АСТ, 2022. – 128 с. – ISBN 978-5-17-101287-8.

21. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – Москва : Изд-во РАГС, 1998 – 120 с. – ISBN 5-7729-0030-7.

22. Дащенко Ю. С. Воспитание информационной безопасности как необходимый компонент формирования информационной культуры детей младшего школьного возраста / Ю. С. Дащенко, С. А. Новоселов // Педагогическое образование в России. – 2020. – № 6. – С. 80–86.

23. Диденко К. В. Некоторые проблемы выявления и предупреждения киберпреступлений / К. В. Диденко // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2020. – № 3. – С. 20–24.

24. Диков А. В. Как учителям и ученикам не запутаться в сетях Всемирной паутины / А. В. Диков // Школьные технологии. – 2019. – № 6. – С. 99–104.

25. Диков А. В. Онлайн-безопасность в сетях сторителлинга / А. В. Диков // Школьные технологии. – 2018. – № 6. – С. 51–58.

26. Добринская Д. Е. Киберпространство: территория современной жизни / Д. Е. Добринская // Вестник Московского университета. Серия 18. Социология и политология. – 2018. – Т. 24. – № 1. – С. 52–70.

27. Дороженко Е. К. Преступления против несовершеннолетних в цифровой среде: обзор проблемы и пути противодействия / Е. К. Дороженко, И. А. Биккинин // Вестник Башкирского государственного педагогического университета им. М. Акмуллы. – 2022. – Т. 3. – № 1(62). – С. 178–180.

28. Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н. З. Емельянова, Т. Л Партыка, И. И. Попов. – Москва : ФОРУМ, 2021. – 368 с. – ISBN 978-5-00091-466-3.

29. Ефимова Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : монография / Л. Л. Ефимова, С. А. Кочерга. – Москва : Юнити-Дана, 2013.– 239 с. – ISBN 978-5-238-02405-9.

30. Зубалова О. А. Проблемы информационной безопасности образовательной среды в современных условиях / О. А. Зубалова // Мир науки, культуры, образования. – 2018. – № 3 (70). – С. 36–38.

31. Информационная безопасность : учеб. пособие / Кирколуп сост., Е. М. Скурыдина. – Барнаул : Алтайский государственный педагогический университет, 2017. – 313 с. – URL: https://www.iprbookshop.ru/102889.html (дата обращения: 20.05.2024). – Режим доступа: для авторизир. пользователей.

32. Информационная культура и информационная безопасность школьников / Е. Г. Белякова, Э. В. Загвязинская, А. И. Березенцева // Образование и наука. – 2017. – №8. – URL: https://cyberleninka.ru/article/n/informatsionnaya-kultura-i-informatsionnaya-bezopasnost-shkolnikov (дата обращения: 04.04.2025).

33. Исследование 2022: Взрослые и дети в интернете: альтернативные цифровые реальности // Kids Safe Media: [сайт]. – 2022. – URL: https://kids.kaspersky.ru/article/vzroslye_i_deti_v_internete_alternativnye_cifrovye_realnosti (дата обращения: 18.04.2025).

34. Киселев Г. М. Информационные технологии в педагогическом образовании : учебник / Г. М. Киселев, Р. В. Бочкова. – 5-е изд., стер. – Москва : Дашков и К., 2022. – 300 с. – ISBN 978-5-394-05073-2.

35. Концепция стратегии кибербезопасности Российской Федерации. Проект // Проект : [сайт]. – 2020 – URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (дата обращения: 13.01.2025).

36. Кулагина И. Ю. Возрастная психология: Развитие человека от рождения до поздней зрелости : учеб. пособие для студентов высших специальных учебных заведений / И. Ю. Кулагина, В. Н. Колюцкий. – 2-е изд. – Москва : Творческий центр «Сфера», 2008. – 463 с. – ISBN 978-5-89145-075-2.

37. Макаров С. Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете / С. Макаров. – Москва : Ростелеком, 2022. – URL: https://www.company.rt.ru/social/cyberknowledge/book_cybersecurity/files/_SMakarov_fullBook_light_.pdf (дата обращения: 17.02.2025).

38. Малых Т. А. Педагогические условия развития информационной безопасности младшего школьника : автореф .дис. … канд. пед. наук : 13.00.01 / Малых Татьяна Александровна ; ПИ ИГУ. Иркутск, 2008. – 23 с.

39. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для студентов вузов по спец. «Информационные системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков . – 5-е изд., стер. – Москва : Академия, 2011. – 331 с. – ISBN 978-5-7695-7738-3.

40. Мухина В. С. Возрастная психология : феноменология развития, детство, отрочество : учебник для студентов, обучающихся по пед. специальностям / В. С. Мухина. – Москва : Академия, 2007. – 640 с. – ISBN 978-5-4468-2273-7.

41. Мухина В. С. Возрастная психология: Феноменология развития и бытия личности. В 2 т. Т. 1 : учебник для студентов ВУЗов / В. С. Мухина. – 18-е изд., перераб. и доп. – Москва : Наука, 2022. – 671 с. – ISBN 978-5-02-040903-3.

42. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024). – Контур Норматив [сайт]. – 2010. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=489460 (дата обращения 27.09.2024).

43. Об образовании в Российской Федерации : Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 01.05.2024) // Консультант Плюс: [сайт]. – 2023. – URL: https://www.consultant.ru/document/cons_doc_LAW_140174/38e6fc208f73b94f1595dbebf3aafb62c3f41281/ (дата обращения: 12.11.2024). – Режим доступа: по подписке СПС КонсультантПлюс.

44. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 5 декабря 2016 г. № 646. – Контур Норматив [сайт]. – 2016. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=284857 (дата обращения 21.02.2025).

45. Об утверждении об утверждении профессионального стандарта «Педагог-психолог (психолог в сфере образования)» : Приказ Минтруда России от 24.07.2015 № 514н. – Контур Норматив [сайт]. – 2015. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=258098#h226 (дата обращения 27.04.2024).

46. Об утверждении Федерального государственного образовательного стандарта начального общего образования (ред. от 22.01.2024) : Приказ Министерства просвещения Российской Федерации от 31.05. 2021 № 286. – Контур Норматив [сайт]. – 2021. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=477741 (дата обращения 13.12.2024).

47. Опрос: «Взрослые и дети в интернете: цифровая грамотность» // Kaspersky Safe Kids: [сайт]. – 2020. – URL: https://kids.kaspersky.ru/article/opros_vzroslye_i_deti_v_internete_cifrovaya_gramotnost (дата обращения: 13.01.2024).

48. Особенности психического развития детей 6-7-летнего возраста : монография / ред. Д. Б. Эльконин, А. Л. Венгер. – Москва : Педагогика, 1988. – 136 с. – ISBN 5-7155-0042-7.

49. Педагогика : учебник и практикум для вузов / под редакцией П. И. Пидкасистого – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 408 с. – ISBN 978-5-534-01168-5.

50. Подласый И. П. Педагогика : учебник для вузов / И. П. Подласый. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 575 с. – ISBN 978-5-534-03772-2.

51. Постановление Главного государственного санитарного врача РФ от от 28 сентября 2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20 Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» // Система ГАРАНТ : [сайт]. – 2020. – URL : https://base.garant.ru/75093644/ (дата обращения: 21.12.2024).

52. Развитие цифровой грамотности школьников в условиях создания цифровой образовательной среды / Т. А. Бороненко, А. В. Кайсина, В. С. Федотова // Перспективы науки и образования. – 2019. – №2. – С. 167– 193.

53. Родичев Ю. А. Информационная безопасность: нормативно правовые аспекты: учеб. пособие / Ю. А. Родичев. – Санкт-Петербург : Питер, 2018. – 272 с. – 978-5-388-00069-9.

54. Русско-американский словарь терминов и определений в сфере информационной безопасности // Всё о цифровой экономике и цифровой политике : [сайт]. – 2018. – URL: https://digital.report/cybersecurity-terminology (дата обращения: 01.05.2025).

55. Синицын Д. С. Обучение подростков информационно-психологической безопасности / Д. С. Синицын// Человек и образование. – 2005. – № 1. – С. 50–52.

56. Сластенин В. А. Педагогика : учебное пособие для студентов образовательных учреждений среднего профессионального образования, обучающихся по педагогическим специальностям / В. А. Сластенин, И. Ф. Исаев, Е. Н. Шиянов. – 7-е изд., стер. – Москва : Академия, 2015. – 490 с. – ISBN 978-5-4468-1536-4.

57. Уроки кибербезопасности // Проект «Кибер Забота»: официальный сайт. – 2021. – URL: https://cyber-care.ru/lessonscybersecurity (дата обращения: 15.02.2024).

58. Шварцкоп О. Н. Информационная безопасность в профессиональном образовании : учебно-метод. пособие / О. Н. Шварцкоп, Ф. Х. Хабибуллин ; Южно-Уральский государственный гуманитарно-педагогический университет. – Челябинск : Изд-во ЗАО «Библиотека А. Миллера», 2020 – 75 с. – ISBN 978-5-93162-403-7.

59. Шевчук М. В. Методика обучения основам сетевой кибербезопасности в школьном курсе информатики / М. В. Шевчук, В. Г. Шевченко, А. А. Масленникова. // Педагогическое образование и наука. – 2020. – № 6. – URL: https://www.elibrary.ru/item.asp?id=45791678 (дата обращения: 15.11.2024).

60. Эльконин Д. Б. Избранные психологические труды : [детская и педагогическая психология] / Д. Б. Эльконин. – Москва : Педагогика, 1989. – 560 с. – ISBN 5-7155-0035-4.

61. Ярочкин В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. – 5-е изд. – Москва : Академический Проект, 2020. – 544 с. – ISBN 978-5-8291-3031-2.

ПРИЛОЖЕНИЕ А

Диагностическая методика №1. Анкетирование

«Как бы ты поступил?» (Ю. Б. Гиппенрейтер)

Цель: изучение уровня знаний основ безопасного поведения в сети Интернет.

Материалы и оборудование: бланк ответов.

Проведение исследования производится коллективно.

Содержание: обучающимся предлагались следующие три ситуации:

Ситуация 1. В социальной сети с Вами познакомился ученик Вашей школы, которого Вы ни разу не видели, и он пригласил Вас на встречу с ним. Ваши действия?

Ситуация 2. На адрес электронной почты пришел файл с игрой от неизвестного пользователя. Как Вы поступите?

Ситуация 2. Как поступить, если злоумышленники взломали Ваш аккаунт, поменяв пароль и адрес электронной почты, к которой был привязан профиль?

Ответы анализировались в соответствии со следующими уровнями:

– низкий уровень знаний основ безопасного поведения в сети Интернет (1 балл): школьник не знает, как поступать в случае взлома его аккаунта в Интернете, также он готов прийти на встречу с незнакомым человеком, назначенную через Интернет, и открыть на компьютере файл, пришедший с незнакомого почтового адреса;

– средний уровень знаний основ безопасного поведения в сети Интернет (2 балла): школьник не знает, как поступать в случае взлома его аккаунта в Интернете, однако он не готов прийти на встречу с незнакомым человеком, назначенную через Интернет, и не станет открывать на компьютере файл, пришедший с незнакомого почтового адреса;

– высокий уровень знаний основ безопасного поведения в сети Интернет (3 балла): школьник знает, как поступать в случае взлома его

аккаунта в Интернете, также он не готов прийти на встречу с незнакомым человеком, назначенную через Интернет, и не станет открывать на компьютере файл, пришедший с незнакомого почтового адреса.

ПРИЛОЖЕНИЕ Б

Диагностическая методика № 2

«Действие с информацией» (Т. В. Борисова)

Цель: умение грамотно искать информацию в сети Интернет и работа с данной информацию.

Материалы: задание, компьютер.

Ход диагностики: обучающемуся предлагается следующее задание: «Найди с помощью Интернета в словарях слово «потеха» и запишите его толкование?

1. орфографический – _____

2. словарь ударений – _____

3. толковый – _____

4. фразеологический – _____

Оценка результатов осуществлялась следующим образом:

– 3 балла – высокий уровень: ребенок смог быстро и без отвлечения на посторонние сайты найти информацию по заданной теме с помощью Интернета;

– 2 балла – средний уровень: ребенок смог найти информацию по заданной теме с помощью Интернета, однако это заняло более 15 минут. Ребенок отвлекался на посторонние сайты;

– 1 балл – низкий уровень: ребенок не смог найти информацию по заданной теме с помощью Интернета. Ребенок отвлекался на посторонние сайты.

ПРИЛОЖЕНИЕ В

Диагностическая методика № 3 «Безопасно или нет?»

(Тест с выбором вариантами ответами)

Цель: диагностика уровня сформированности отношения к безопасному поведению в сети Интернет».

Материалы: тест.

Методика «Безопасно или нет?» Тест с вариантами ответами

Цель: диагностика уровня сформированности отношения к безопасному поведению в сети Интернет».

Материалы: тест.

Ход диагностики: ребенку предлагается тест с выбором вариантами ответа.

Фамилия, Имя _______

Класс_____

Тестирование «Безопасно или нет?» (по теме «Кибербезопасность младшего школьника» 1 триместр)

1. Какой из предложенных паролей лучше выбрать для своей электронной почты?

а) дата рождения;

б) K_83_vv6Q;

в) 12345.

2. Тебе на электронную почту пришло письмо от незнакомого человека, представившегося знакомым твоей мамы, в котором он просит пройти по ссылке и проголосовать за его проект. Что ты сделаешь?

а) пройду по ссылке и посмотрю, что за проект;

б) напишу в ответ письмо и спрошу, откуда он знает мою маму;

в) удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам.

3. Укажи устройство для подключения компьютера к сети:

а) модем;

б) монитор;

в) сканер.

4. Какую информацию нельзя разглашать в Интернете?

а) свои увлечения;

б) свой псевдоним;

в) свой домашний адрес.

5. Какие данные из нижеперечисленных можно сообщать по электронной почте?

а) номера банковских карт твоих родителей;

б) секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта;

в) свои имя и фамилию.

6. Когда можно доверять письму от неизвестного отправителя?

а) Отправитель ссылается на твоих друзей;

б) К тебе обращаются по имени;

в) Никогда нельзя доверять письму от неизвестного отправителя.

7. Что НЕ поможет защитить твою электронную почту от взлома?

а) Создавать разные надежные пароли от своих аккаунтов;

б) Не открывать сообщения с незнакомых и подозрительных адресов;

в) Сказать свой пароль родителям.

8. Что такое СПАМ:

а) агрессивное поведение на форумах;

б) массовая рассылка рекламы и прочих объявлений;

в) цепочка непонятных, нелогичных объяснений.

9. Какое правило безопасного поведения в сети Интернет позволит уберечь себя от спама?

а) Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета;

б) Не добавляй незнакомых людей в свои контакты;

в) Общаясь в Интернете, будь дружелюбен. Не пиши грубых слов!

10. Какие из этих поисковых систем являются детскими поисковыми системами?

а) www.yandex.ru, www.rambler.ru;

б) www.kids.quintura.ru, www.agakids.ru;

в) www.google.ru, Апорт.

Ответы на тестирование:

1	2	3	4	5	6	7	8	9	10
Б	В	А	В	В	В	В	Б	А	Б

Оценка результатов осуществлялась следующим образом:

0-5 правильных ответов – низкий уровень.

5-8 правильных ответов – средний уровень.

9-10 правильных ответов – высокий уровень.

Интерпретация результатов:

– Обучающиеся с низким уровнем знаний (0-5 правильных ответов) представляет собой наиболее уязвимую категорию пользователей. Они демонстрируют серьезные пробелы в понимании основных принципов кибербезопасности, что делает их легкой мишенью для кибератак. Эта категория включает людей, недостаточно осведомленных о рисках, связанных с использованием технологий и интернета, а также о мерах предосторожности, необходимых для защиты своих данных.

– Обучающиеся, набравшие от 5 до 8 правильных ответов, находятся на среднем уровне знаний. Эта группа демонстрирует некоторое понимание ключевых аспектов кибербезопасности, однако им все еще не хватает глубины знаний, чтобы чувствовать себя полностью защищенными в цифровом пространстве. Они могут осознавать некоторые угрозы, но недостаточно подготовлены к адекватному реагированию на них.

– Группа с высоким уровнем знаний (9-10 правильных ответов) показывает уверенное понимание основ кибербезопасности. Эти участники

способны распознавать различные виды угроз и имеют представление о том, как защитить себя и свои данные в сети. Они являются образцовыми пользователями интернет-пространства, способными не только защищать себя, но и предупреждать других о возможных угрозах.

ПРИЛОЖЕНИЕ Г

Программа работы педагога-психолога по формированию основ кибербезопасности для обучающихся 4 классов

Пояснительная записка

Программа работы педагога-психолога по формированию осснов кибербезопасности (далее – Программа) разработана в результате детального анализа документов, литературы, исследовательских данных и дополнительных ресурсов, связанных с формированием основ кибербезопасности; программа соответствует требованиями Федеральных государственных образовательных стандартов начального общего образования и трудовым функциям профессионального стандарта «Педагог-психолог (психолог в сфере образования)».

Программа представляет собой структурированную работу педагога-психолога, направленную на развитие основ кибербезопасности у младших школьников.

Актуальность программы обусловлена тем, что проблемы безопасности детей в сети Интернет последние годы являются особенно актуальными, в связи с бурным развитием IT-технологий и со свободным использованием детьми современных информационно коммуникационных технологий (Интернет, мобильная связь).

Программа имеет высокую актуальность и отражает важные вопросы безопасной работы: потребность в защите персональной информации, потребность в работе с ресурсами для досуга (компьютерные игры, видео и цифровое телевидение, СМИ), а также поиск познавательной и учебной информации, общение в социальных сетях, получение и передача файлов.

При реализации требований безопасности в сети Интернет для любого пользователя (школьник или учитель), образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к

противоправной негативной информации. Но включение школьников в Интернет наиболее активно осуществляется вне школы самостоятельно, уже без надлежащего надзора со стороны взрослых.

Следовательно, необходимо проводить непрерывную работу не только с обучающимися, но и с семьей, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере киберпространства, в том числе внимательно относиться к использованию личных устройств мобильной связи, домашнего компьютера с Интернетом, использовать программные средства защиты.

Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет.

Ведь важно формировать на качественно новом уровне культуры умственного труда и взаимодействия с окружающими, ответственного отношения к вопросам информационной безопасности и кибербезопасности.

Нормативно-правовая основа программы разработана в соответствии с требованиями:

1. Конвенция ООН о правах ребёнка, принятая Генеральной Ассамблеей ООН 20 ноября 1989 г.

2. Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (с изм. и доп., вступ. в силу с 01.05.2024).

3. Федеральный государственный образовательный стандарт начального общего образования, утвержденный приказом Минпросвещения России от от 31.05.2021 № 286 (ред. от 08.11.2022) «Об утверждении федерального государственного образовательного стандарта начального общего образования».

4. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в ред. Федеральных законов от 30.11.2024 № 438-ФЗ).

5. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 (в ред. Федеральных законов от 26.12.2024 № 479-ФЗ)

6. Распоряжение Правительства Российской Федерации от 28.04.2023 №1105-р «О концепции информационной безопасности детей в Российской Федерации».

7. Постановления Главного государственного санитарного врача РФ от 28 сентября 2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20 Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

Общая характеристика программы

Цель Программы: создание условий, позволяющих наиболее эффективно выстроить формирование у обучающихся младшего школьного возраста основ кибербезопастности, базовых принципов безопасного поведения в сети Интернет и безопасности личного информационного пространства.

Задачи Программы:

– содействовать развитию умения безопасной работы с информацией, анализировать и обобщать полученную информацию;

– формировать у младших школьников базовую систему знаний о безопасном поведении и информационной этике при работе с компьютерными программами, информацией в сети Интернет;

– развивать компьютерную грамотность и информационную культуру личности в использовании информационных и коммуникационных технологий;

– содействовать в усвоение сознательного и бережного отношения к вопросам собственной информационной безопасности в стенах образовательной организации, в семье;

– развивать нравственные, этические, патриотические качеств личности в процессе формирования основ кибербезопасности.

Принципы для построения и реализации Программы:

– принцип гуманизма;

– принцип единства диагностики и коррекции;

– принцип развития;

– принцип активной включенности;

– принцип практико-ориентированности.

При разработке программы были учтены все ключевые направления работы педагога-психолога, такие как организационное, диагностическое, индивидуально-коррекционное, просветительское и аналитическое.

Особенность Программы: программа предусматривает совместную деятельность педагога-психолога и классного руководителя (учителя) по формированию основ кибербезопасности, психологической коррекции аддиктивных проявлений в информационной среде (кибербуллинг, игровая зависимость и т.д.), консультировании родителей по стратегии минимизации рисков, связанных с онлайн-угрозами.

Психолог становится полноправным участником образовательного процесса. У него появляется возможность тесно сотрудничать с педагогами в решении проблем и задач развития конкретных детей и ученического коллектива в целом, прежде всего – с классным руководителем.

Содержание программы

Целевой аудиторией Программы являются обучающиеся 10-11 лет (4 класс), а также родители (законные представители), педагоги, классные руководители.

В связи с чем, мероприятия программы деятельности педагога–психолога по формированию основ кибербезопасности младших школьников (далее – Программа) включают в себя разделы:

1. Работа с младшими школьниками по формированию основ кибербезопасности (классные часы, викторины, квесты).

2. Работа с родителями младших школьников по формированию основ кибербезопасности (консультации, родительские собрания).

3. Работа с педагогическим коллективом по формированию информационной компетентности учителей в сфере основ кибербезопасности начальной школы (лекции, собрания). Подробнее вся работа описана в таблице Г.1.

Срок реализации программы рассчитан на 6 месяцев, начиная с октября по апрель учебного года.

Организационные условия реализации Программы:

– продолжительность занятий – 45 минут,

– количество занятий – 36,

– режим проведения занятий – 1 раз в неделю.

Методы реализации мероприятий Программы: фронтальные занятия, беседа, лекция, наглядная агитация.

Основные формы реализации работы: классный час, родительское собрание, собрание педагогического коллектива.

Приемы обучения, применяемые в процессе проведения мероприятий Программы: вопросы, загадки, игры, викторины, рассказывание, просмотр видео, проблемно-ценностное общение.

Весь материал построен с учётом возрастных особенностей, обучающихся по принципу от простого к сложному. Практические разработки примеров классных часов, конспекта родительского собрания, предложенные в содержании Программы, возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Таблица Г.1 – Календарно-тематическое планирование (перечень мероприятий) программы работы педагога-психолога по формированию основ кибербезопасности младшего школьника

№ п/п	Контингент работы	Срок проведения работы	Темы мероприятий, направленных на формирование основ кибербезопасности
1	*2*	*3*	*4*
1.	Младшие школьники	Октябрь 1-я неделя	Диагностика имеющегося уровня формирования основ кибербезопасности младших школьников *Методики (диагностики):* 1. Опросник поведения в интернете (А.Е. Жичкина) (выявление уровня активности в онлайн-пространстве, анализ мотивов нахождения в виртуальной среде, а также предпосылок развития интернет-зависимости). 2. Тест-опросник степени увлеченности младших подростков компьютерными играми (А.В. Гришина) (интерпретация для младших школьников).
		Октябрь 3-я неделя	Диагностика выявления «групп риска» (тех обучающихся, кто подвергся онлайн-мошенничеству, интернет-травле, обману в социальных сетях или онлайн-играх, а также столкнулся с недостоверными источниками информации). *Методики (диагностики):* 1. Скрининговая диагностика компьютерной (телефонной) зависимости по методике Л.Н. Юрьевой, Т.Ю. Больбот. (для выявления склонности к гаджет- зависимости и интернет-зависимости). 2. Тест «Самооценка силы воли» Н.Н. Обозов (для исследования уровня силы воли). 3. Шкала тревожности А.М. Прихожан (для определения уровня тревожности). 4. Методика исследования эмоционального состояния (по Э.Т. Дорофеевой) (для оценки эмоционального состояния ребенка).
		Ноябрь 1-я неделя	Классный час «Компьютер – как он появился, как появился Интернет».
		Ноябрь 3-я неделя	Классный час «Знакомство с Интернетом и его опасностями».
		Декабрь 1-я неделя	Викторина «Мобильные устройства. Польза и опасности мобильной связи».

Продолжение таблицы Г.1

1	*2*	*3*	*4*
		Декабрь 3-я неделя	Классный час «Что такое электронная почта? Создание электронной почты».
		Январь 2-я неделя	Классный час «Вирусы и антивирусы. Что такое антивирусная защита? Гигиена при работе с компьютером».
		Январь 4-я неделя	Классный час «Что такое Интернет-сообщество. Социальные сети. Правила безопасного использования социальных сетей».
		Февраль 1-я неделя	Классный час «Кибербуллинг (интернет-травля) и его последствия».
		Февраль 3-я неделя	Квест «Есть ли у меня игровая зависимость? Игры полезные и вредные. Признаки игровой зависимости».
		Март 1-я неделя	Изготовление стенгазеты на тему «Что такое интернет–этикет? Как вести себя в гостях у «сетевых» друзей».
		Март 3-я неделя	Классный час «Почему родители проверяют, что ты делаешь в Интернете?»
		Апрель 1-я неделя	Квест «Война миров» (Как государство защищает информацию в киберпространстве?). Памятка поведения в сети Интернет для младших школьников.
		Апрель 3-я неделя	Контрольная диагностика имеющегося уровня формирования основ кибербезопасности младших школьников. Рекомендации для младших школьников. Итоговое (повторное) проведение методики (диагностики): 1. Скрининговая диагностика компьютерной (телефонной) зависимости по методике Л.Н. Юрьевой, Т.Ю. Больбот. (для выявления склонности к гаджет- зависимости и интернет-зависимости). 2. Тест «Самооценка силы воли» Н.Н. Обозов (для исследования уровня силы воли). 3. Шкала тревожности А.М. Прихожан (для определения уровня тревожности). 4. Методика исследования эмоционального состояния (по Э.Т. Дорофеевой) (для оценки эмоционального состояния ребенка). 5. Опросник поведения в интернете (А.Е. Жичкина) 6. Тест-опросник степени увлеченности младших подростков компьютерными играми (А.В. Гришина) (интерпретация для младших школьников) и т.д.

Продолжение таблицы Г.1

2.	Законные представители младших школьников (родители)	Октябрь 1-я неделя	Родительское собрание на тему «Особенности детей младшего школьного возраста» (лекция).
		Октябрь 3-я неделя	Родительское собрание на тему «Введение в ключевые понятия информационной безопасности младших школьников» (проблемно–ценностное общение).
		Ноябрь 1-я неделя	Родительское собрание на тему «Обзор потенциальных угроз, с которыми могут столкнуться дети» (лекция).
		Ноябрь 3-я неделя	Родительское собрание на тему «Советы по предотвращению кибербуллинга и онлайн-обманов» (проблемно–ценностное общение).
		Декабрь 1-я неделя	Родительское собрание на тему «Признаки того, что ребенок может быть жертвой или свидетелем кибербуллинга (интернет-травля)» (лекция).
		Декабрь 3-я неделя	Родительское собрание на тему «Как научить детей не раскрывать слишком много в социальных сетях» (проблемно–ценностное общение).
		Январь 2-я неделя	Родительское собрание на тему «Как защитить своего ребенка от нежелательных контактов в Интернете?»» (проблемно–ценностное общение).
		Январь 4-я неделя	Родительское собрание на тему «Консультативная помощь родителям. Обратная связь».
		Февраль 1-я неделя	Родительское собрание на тему «Основные стратегии по защите личной информации в интернете» (лекция).
		Февраль 3-я неделя	Родительское собрание на тему «Средства родительского контроля и как их эффективно использовать. Найдем баланс между защитой ребенка и уважением его личного пространства».
		Март 1-я неделя	Тематический вечер с детьми «Совместные действия для создания безопасной цифровой среды».
		Март 3-я неделя	Тематический вечер с детьми «Исследование различных онлайн-игр и обсуждение их плюсов и минусов».
		Апрель 1-я неделя	Родительское собрание на тему «Совместные действия для создания безопасной цифровой среды» (проблемно–ценностное общение). Памятка для родителей по формированию основ кибербезопасности.
		Апрель 3-я неделя	День здоровья с участием детей.

Продолжение таблицы Г.1

1	*2*	*3*	*4*
3.	Педагоги, классные руководители	Октябрь 1-я неделя	Лекторий для педагогов школы «Формирование основ кибербезопасности как педагогическая проблема».
		Октябрь 3-я неделя	Лекция 1 на тему «Введение в основы кибербезопасности для младших школьников» Содержание лекции: Разбор ключевых понятий кибербезопасности, адаптированных для детей младшего возраста. Примеры простейших угроз и способы их объяснения школьникам.
		Ноябрь 1-я неделя	Лекция 2 на тему «Методы преподавания основ цифровой гигиены» Содержание лекции: Стратегии внедрения базовых навыков защиты личной информации в учебный процесс. Создание уроков, ориентированных на формирование привычек безопасного поведения в интернете.
		Ноябрь 3-я неделя	Лекция 3 на тему «Киберэтикет: онлайн-правила для маленьких пользователей» Содержание лекции: Обучение детей правилам вежливого и безопасного общения в сети. Разработка ролевых игр для освоения азов киберэтикета.
		Декабрь 1-я неделя	Лекция 4 на тему «Безопасное использование гаджетов: практические рекомендации» Содержание лекции: Уроки по безопасному использованию планшетов и смартфонов учащимися. Как формировать навыки саморегуляции в использовании цифровых устройств.
		Декабрь 3-я неделя	Лекция 5 на тему «Интерактивные методы обучения кибербезопасности» Содержание лекции: Примеры игр и упражнений, повышающих уровень цифровой грамотности. Как заинтересовать и вовлечь учеников младших классов в изучение кибербезопасности.
		Январь 2-я неделя	Лекция 6 на тему «Распознавание и предотвращение интернет-угроз» Содержание лекции: Стратегии раннего предупреждения о рисках и защите от них (фишинговые сообщения и ненадежные сайты).

Продолжение таблицы Г.1

1	*2*	*3*	*4*
		Январь 4-я неделя	Лекция 7 на тему «Создание атмосферы доверия при обучении кибербезопасности» Содержание лекции: Методы налаживания открытого диалога между учениками и учителями на тему интернет-безопасности. Обсуждение важности поддержки и мотивации для обучающихся в цифровом мире.
		Февраль 1-я неделя	Самообследование образовательной среды на предмет безопасности и комфортности.
		Февраль 3-я неделя	Психологический практикум на тему «Развитие эмпатии и навыков общения для осознанного взаимодействия в цифровой среде».
		Март 1-я неделя	Психологический практикум на тему «Психологическая поддержка и мотивация как инструмент формирования безопасного поведения в сети младших школьников».
		Март 3-я неделя	Совещание при директоре: «Организация работы по формированию основ кибербезопасности младших школьников в образовательной среде организации».
		Апрель 1-я неделя	Педагогический совет: «Основные механизмы формирования основ кибербезопасности в начальной школе».
		Апрель 3-я неделя	Новые формы работы по формированию основ кибербезопасности младших школьников.

Ожидаемые результаты Программы:

Программа работы педагога-психолога по формированию основ кибербезопасности у младших школьников направлена на достижение следующих результатов:

1. Повышение уровня информативности школьников, в результате владения знаниями о интернет-рисках и угрозах к информационном пространстве.
2. Умение анализировать и критически относиться к информации в Интернете.
3. Формирование мотивации к ответственному использованию информационно-коммуникационных технологий.
4. Умение определять наличие негативного, недостоверного, небезопасного содержания в интернет-контенте.
5. Владение эффективными способа защиты от не нежелательной информации, контактов в Интернете и их применение на практике.
6. Владение нормами интернет-этикета, приёмами эффективной коммуникации.
7. Развитие педагогических навыков для помощи младшим школьникам, испытывающим трудности в обучении кибербезопасности.
8. Формирование компетенций у родителей в области обучения младших школьников основам кибербезопасности.
9. Разработка рекомендаций для педагогов и родителей по эффективному педагогическому сопровождению.
10. Умение владеть принципами уважительного и толерантного отношения к другим пользователям при взаимодействии в сети Интернет.
11. Повышение осведомлённости родителей для эффективного сопровождения детей в процессе освоения информационных технологий.
12. Укрепление психологического здоровья.

Универсальность Программы проявляется в том, что в нем указаны ключевые направления деятельности, направленной для безопасного

обучения личности младшего школьника, чтобы научить его противостоять информационным угрозам и отделять положительное от отрицательного, среди многообразного потока информации в Интернете.

Примеры конспектов для младших школьников по формированию основ кибербезопасности, рекомендации для родителей и младших школьников, а также ссылки на полезные источники, необходимые для работы педагога-психолога представлены ниже.

План для конспекта классного часа «Знакомство с Интернетом и его опасностями»

Цель: ознакомление детей с возможностями и опасностями Интернета.

Задачи:

– понимание, что такое Интернет;

– осознание опасностей, связанных с использованием Интернета;

– формирование навыков безопасного поведения в Интернете.

Ход занятия:

1. Введение (5 минут)

– Приветствие детей и объяснение темы занятия.

– Вопросы к детям: Кто из вас уже пользовался Интернетом? Что вы знаете о нем? (обращение к опыту детей)

2. Определение понятия Интернет (5 минут)

– Объяснение, что такое Интернет и как он работает.

– Использование примеров и аналогий для более понятного объяснения.

3. Основные опасности Интернета (15 минут)

– Презентация основных опасностей Интернета: вирусы, мошенничество, кибербуллинг и т.д.

– Объяснение, как эти опасности могут повредить детям и их семьям.

4. Правила безопасного поведения в Интернете (15 минут)

– Обучение правилам безопасного поведения в Интернете: не давать личную информацию, не отвечать на подозрительные сообщения, не скачивать незнакомые файлы и т.д.

– Демонстрация примеров безопасного поведения в Интернете.

5. Заключение (5 минут)

– Подведение итогов занятия.

– Ответы на вопросы детей.

– Напоминание о важности безопасного поведения в интернете.

План для конспекта классного часа «Кибербуллинг и его последствия»

Цель: понимание опасностей кибербуллинга и развитие навыков защиты от него.

Задачи:

– осознание, что такое кибербуллинг;

– понимание последствий кибербуллинга;

– формирование навыков защиты от кибербуллинга.

Ход занятия:

1. Введение (5 минут)

– Приветствие детей.

– Объяснение темы занятия.

– Уточнение у детей, что такое кибербуллинг (обращение к опыту детей).

2. Беседа о кибербуллинге (10 минут)

– Определение кибербуллинга.

– Рассказ о том, как происходит кибербуллинг.

– Примеры кибербуллинга.

3. Последствия кибербуллинга (10 минут)

– Презентация последствий кибербуллинга (психологические проблемы, ухудшение отношений и т.д.).

– Обсуждение, как кибербуллинг может повлиять на жизнь человека.

4. Навыки защиты от кибербуллинга (15 минут)

– Обучение навыкам защиты от кибербуллинга (игнорирование сообщений, блокирование пользователя и т.д.).

– Рассказ о том, как правильно реагировать на кибербуллинг.

5. Заключение (5 минут)

– Подведение итогов занятия.

– Ответы на вопросы детей.

– Напоминание о важности безопасного поведения в интернете.

План для конспекта классного часа «Правила безопасного использования социальных сетей»

Цель: ознакомление детей с правилами безопасного использования социальных сетей.

Задачи:

– понимание, что такое социальные сети и как ими пользоваться;

– осознание опасностей, связанных с использованием социальных сетей;

– формирование навыков безопасного использования социальных сетей.

Ход занятия:

1. Введение (5 минут)

– Приветствие детей.

– Объяснение темы занятия.

– Уточнение, что такое социальные сети (обращение к опыту детей).

2. Беседа о социальных сетях (10 минут)

– Определение социальных сетей.

– Рассказ о том, как ими пользоваться.

– Примеры социальных сетей.

3. Опасности использования социальных сетей (10 минут)

– Презентация основных опасностей социальных сетей (распространение личной информации, кибербуллинг и т.д.).

– Обсуждение, какие опасности могут возникнуть при использовании социальных сетей.

4. Навыки безопасного использования социальных сетей (15 минут)

– Обучение правилам безопасного использования социальных сетей (не давать личную информацию, не добавлять незнакомых людей и т.д.).

– Рассказ о том, как правильно настроить приватность в социальных сетях.

5. Заключение (5 минут)

– Подведение итогов занятия.

– Ответы на вопросы детей.

– Напоминание о важности безопасного поведения в интернете.

Памятка поведения в сети Интернет для младших школьников (для формирования основ кибербезопасности)

Вы должны это знать:

1. Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Прежде чем начать дружить с кем-то в Интернете, спросите у родителей, как безопасно общаться.

3. Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.

4. Не отправляйте фотографии людям, которых вы не знаете. Не нужно, чтобы незнакомые люди видели фотографии Ваши, Ваших друзей или Вашей семьи.

5. Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.

7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

8. При регистрации на сайтах старайтесь не указывать личную информацию, так как. она может быть доступна незнакомым людям. Также не рекомендуется размещать свою фотографию, давая тем самым представление о том, как вы выглядите, посторонним людям.

9. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, так как. он может быть записан.

10. Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.

11. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

12. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.

13. Нежелательно размещать персональную информацию в Интернете.

14. Персональная информация – это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

15. Если вы публикуете фото или видео в Интернете – каждый может посмотреть их.

16. Не отвечайте на Спам (нежелательную электронную почту).

17. Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

18. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

19. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности.

Родительское собрание на тему «Как защитить своего ребенка от нежелательных контактов в Интернете?»

Цели родительского собрания: совместно с родителями обсудить возможные угрозы, с которыми дети могут столкнуться в Интернете, и найти способы защиты от них.

Задачи родительского собрания:

– Повысить уровень осведомленности родителей о безопасности детей в Интернете.

– Показать, какие инструменты и программы помогают защитить ребенка от нежелательных контактов в сети.

– Обсудить конкретные случаи нежелательных контактов и как на них реагировать.

– Разъяснить правила безопасного поведения младших школьников в сети Интернет и как их следовать.

– Дать рекомендации по общению с детьми на тему безопасности в Интернете.

Ход родительского собрания

1. Вступительное слово и приветствие участников.

Уважаемые родители! Я рада приветствовать вас на родительском собрании, посвященном вопросу безопасности детей в Интернете. Сегодня мы обсудим, как защитить своих детей от нежелательных контактов в сети и как предотвратить возможные опасности. Я надеюсь, что наше общее участие в этом мероприятии поможет нам стать более осведомленными и защитить наших детей от негативного влияния Интернета.

2. Определение проблемы: какие опасности могут поджидать детей в Интернете и как они могут повлиять на их жизнь.

Сегодняшние дети проводят много времени в Интернете, что может привести к нежелательным контактам, кибербуллингу, просмотру неподходящего контента и другим опасностям. Все это может повлиять на их психологическое и физическое здоровье, а также на их будущее. Поэтому очень важно обеспечить безопасность наших детей в Интернете.

3. Рассмотрение основных способов защиты ребенка: установка родительского контроля, использование специальных программ и приложений, обучение правилам безопасного поведения младших школьников в сети Интернет.

Существует несколько основных способов защиты ребенка в Интернете. Первый – установка родительского контроля на компьютере или мобильном устройстве. Это позволяет ограничить доступ к неподходящему контенту и сайтам. Второй – использование специальных программ и приложений, которые блокируют нежелательные контакты и сообщения. Третий – обучение правилам безопасного поведения младших школьников в сети Интернет. Это включает в себя объяснение детям, что они могут делать в сети, а что нет, как общаться со странными людьми и как сообщать о проблемах.

4. Обсуждение конкретных примеров нежелательных контактов и как им можно предотвратить.

Давайте обсудим конкретные примеры нежелательных контактов, которые могут поджидать детей в Интернете. Например, кибербуллинг, когда дети издеваются над другими в сети, или нежелательные контакты со странными людьми. Мы рассмотрим, как можно предотвратить такие ситуации и как правильно реагировать на них.

5. Рекомендации по общению с детьми на тему безопасности в Интернете.

Очень важно общаться с детьми на тему безопасности в Интернете. Родители должны объяснять своим детям, что они могут делать в сети, а что нет, и как правильно реагировать на нежелательные контакты. Также необходимо убедиться, что дети понимают, что они могут обратиться за помощью, если возникнут проблемы.

6. Вопросы и ответы.

Я готова ответить на все ваши вопросы и обсудить любые проблемы, связанные с безопасностью детей в Интернете.

7. Заключительное слово и пожелания участникам.

Я хотела бы поблагодарить всех участников за то, что вы пришли на это родительское собрание. Я надеюсь, что вы получили полезную информацию о том, как защитить своих детей от нежелательных контактов в Интернете. Пожалуйста, не стесняйтесь обращаться ко мне с любыми вопросами или проблемами.

Спасибо и удачи Вам в обеспечении безопасности ваших детей!

Памятка для родителей по формированию основ кибербезопасности

Чтобы помочь своим детям, Вы должны это знать:

1. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

2. Будьте в курсе того, чем занимаются ваши дети в Интернете.

3. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.

4. Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете – номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.

5. Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.

6. Объясните детям, что нельзя открывать файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото / видео с «агрессивным» содержанием.

7. Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

8. Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.

9. Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится.

10. Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Список литературы

1. Диков А. В. Как учителям и ученикам не запутаться в сетях Всемирной паутины / А. В. Диков // Школьные технологии. – 2019. – № 6. – С. 99–104.

2. Информационная безопасность : учеб. пособие / Кирколуп сост., Е. М. Скурыдина. – Барнаул : Алтайский государственный педагогический университет, 2017. – 313 с. – URL: https://www.iprbookshop.ru/102889.html (дата обращения: 20.05.2024). –Режим доступа: для авторизир. пользователей.

3. Макаров С. Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете / С. Макаров. – Москва : Ростелеком, 2022. – – URL : https://www.company.rt.ru/social/cyberknowledge/book_cybersecurity/files/_SMakarov_fullBook_light_.pdf (дата обращения: 17.02.2025).

4. Об образовании в Российской Федерации : Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 01.05.2024) // Консультант Плюс: [сайт]. – 2023. – URL: https://www.consultant.ru/document/cons_doc_LAW_140174/38e6fc208f73b94f1595dbebf3aafb62c3f41281/ (дата обращения: 12.11.2024). – Режим доступа: по подписке СПС КонсультантПлюс.

5. Об утверждении Федерального государственного образовательного стандарта начального общего образования (ред. от 22.01.2024) : Приказ Министерства просвещения Российской Федерации от 31.05. 2021 № 286. – Контур Норматив [сайт]. – 2021. – URL : https://normativ.kontur.ru/document?moduleId=1&documentId=477741 (дата обращения 13.12.2024).

6. Уроки кибербезопасности // Проект «Кибер Забота»: официальный сайт. – 2021. – URL: https://cyber-care.ru/lessonscybersecurity (дата обращения: 15.02.2024).