МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.П. Астафьева»
(КГПУ им. В.П. Астафьева)

Факультет начальных классов
Кафедра теории и методики начального образования

**Давтян Мери Артемовна**

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

# РАСШИРЕНИЕ ЗНАНИЙ МЛАДШИХ ШКОЛЬНИКОВ О БЕЗОПАСНОМ ПОВЕДЕНИИ В СЕТИ ИНТЕРНЕТ ПОСРЕДСТВОМ САЙТА «КИБЕРЗАЩИТНИК»

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) образовательной программы
Начальное образование и русский язык

ДОПУСКАЮ К ЗАЩИТЕ
Зав. кафедрой канд. пед. н., доцент кафедры теории и методики начального образования
Басалаева М.В._____
(дата, подпись)

Научный руководитель канд.биол. н., доцент кафедры теории и методики начального образования
Панкова Е.С._____
(дата, подпись)

Дата защиты _____
Обучающийся
Давтян М.А., группа МО-Б21А-02
_____
(дата, подпись)
Оценка
_____

Красноярск 2026

**СОДЕРЖАНИЕ**

# ВВЕДЕНИЕ

В настоящее время люди постоянно используют Интернет во всех областях жизни, включая экономику, политику, образование и бытовое общение. Данная сеть больше не является только средством, с помощью которого пользователи ищут, хранят или передают данные. С помощью Интернета создается среда, где дети развивают свои личные качества, взгляды на мир и этические принципы. На интересы учеников начальных классов сильно влияет то, как они применяют сетевые ресурсы.

По мнению М. Айкен, Интернет не имеет только положительных или только отрицательных характеристик. Его воздействие полностью определяется целями и способами применения, поэтому взрослые должны обучать детей действовать в цифровом пространстве обдуманно и отвечать за свои поступки [8].

Проведя анализ статистических данных, можно сказать о неуклонном снижении возраста первого выхода в Интернет. Дети начинают осваивать онлайн-пространство задолго до поступления в школу, а к младшему школьному возрасту многие из них уже являются уверенными пользователями различных сервисов, социальных сетей, игровых платформ и видеохостингов. При этом современные исследования фиксируют не только количественный рост присутствия детей в интернет-среде, но и качественное изменение характера этого присутствия. По оценкам специалистов, уже к 2025 году средний возраст начала активного использования гаджетов снизился до 4-5 лет, а к моменту поступления в школу многие дети имеют опыт самостоятельного взаимодействия с сетевыми сервисами, сопоставимый по интенсивности с подростковым. Данная тенденция усугубляется тем, что родительское посредничество в освоении Интернета остается фрагментарным: взрослые склонны контролировать преимущественно время использования устройств, а не содержание потребляемой информации, что создает иллюзию безопасности при фактическом отсутствии у ребенка необходимых защитных механизмов.

Младшие школьники используют Интернет не только для получения новых знаний и поиска необходимой информации для учебы. Зачастую дети не осознают, что времяпрепровождение в Сети несёт в себе немало рисков, с которыми они могут столкнуться. В силу возрастных особенностей, а именно: доверчивости, любознательности, недостаточной сформированности критического мышления, стремления к самостоятельности и неумения предвидеть последствия своих действий, учащиеся начальной школы оказываются наиболее уязвимой категорией пользователей глобальной сети. Необдуманное использование личных данных, незащищенные пароли, излишняя доверчивость к незнакомым собеседникам, неконтролируемое общение в социальных сетях, переход по подозрительным ссылкам, скачивание непроверенных файлов - всё это способно привести к серьёзным, а подчас и трагическим последствиям для младших школьников и их семей.

М. В. Арсентьев, анализируя сущность безопасности в сети Интернет, подчеркивает, что данное понятие должно рассматриваться в постоянном развитии: технологии совершенствуются, а вслед за ними эволюционируют и способы злонамеренного воздействия, что делает задачу защиты детей перманентно актуальной [9].

Таким образом, перед системой начального образования встаёт задача государственной важности: не просто познакомить ребенка с элементарными правилами поведения в Сети, но и сформировать у него устойчивые знания, позволяющие критически оценивать поступающую информацию, осознанно защищать персональные данные, противостоять манипуляциям и выстраивать ответственное поведение в онлайн-пространстве.

Как отмечает Н. А. Переломова, безопасность в сети Интернет у младшего школьника не может быть обеспечена исключительно техническими средствами контентной фильтрации; она требует системной педагогической работы, направленной на формирование у ребёнка внутренних фильтров – критического мышления, ценностных установок и осознанного отношения к личным данным [40].

Вопросами, касающимися различных аспектов безопасности личности в современном мире, в том числе и применительно к подрастающему поколению, занимались многие отечественные исследователи. Большинство существующих исследований ориентировано на подростковую и молодёжную аудиторию, в то время как младший школьный возраст является сензитивным периодом для закладки базовых установок и моделей поведения, в том числе и в сфере сетевой безопасности. Как показывают исследования последних лет, к окончанию начальной школы у значительной части учащихся так и не формируются устойчивые знания о признаках интернет-мошенничества, правилах защиты персональных данных и алгоритмах действия в ситуациях сетевых угроз. В связи с этим особую актуальность приобретает поиск эффективных педагогических средств и методов, учитывающих психологические особенности детей 7–11 лет.

Б. С. Волков подчеркивает, что личностные особенности младших школьников – высокая степень внушаемости, потребность в поощрении – должны рассматриваться как исходные условия при проектировании содержания обучения основам кибербезопасности [22].

Аналогичной позиции придерживается Г. А. Цукерман, указывающая, что в младшем школьном возрасте преобладает наглядно-образное мышление, вследствие чего абстрактные правила информационной безопасности должны быть переведены в конкретные, визуально подкрепленные ситуации, доступные пониманию ребенка [54].

Важность и государственная значимость проблемы защиты детей от деструктивной информации и расширения у них знаний о безопасном поведении в глобальной сети находят свое отражение в ряде нормативно-правовых актов Российской Федерации.

Базовым документом, регулирующим данную сферу, является Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [3]. Закон устанавливает правовые механизмы ограничения доступа несовершеннолетних к контенту, способному нанести ущерб их физическому, психическому,

духовному и нравственному развитию. В документе четко прописаны виды информации, запрещенной для распространения среди детей, а также возрастные ограничения на распространение определенных категорий информационной продукции.

К информации, причиняющей вред здоровью и (или) развитию детей, относится:

1) Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий; (в ред. Федерального закона от 18.12.2018 N 472-ФЗ)

2) Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, сжиженные углеводородные газы, содержащиеся в потенциально опасных газосодержащих товарах бытового назначения, и (или) их пары, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством; (в ред. Федеральных законов от 29.06.2015 N 179-ФЗ, от 31.07.2020 N 303-ФЗ)

3) Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) Содержащая изображение или описание сексуального насилия; (в ред. Федерального закона от 01.05.2019 N 93-ФЗ)

1) Оскорбляющая человеческое достоинство и общественную нравственность, выражающая явное неуважение к обществу, содержащая изображение действий с признаками противоправных, в том числе насильственных, и распространяемая из хулиганских, корыстных или иных низменных побуждений; (в ред. Федерального закона от 08.08.2024 N 216-ФЗ)

2) Отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи; (в ред. Федеральных законов от 29.06.2013 N 135-ФЗ, от 05.12.2022 N 478-ФЗ)

3) Пропагандирующая либо демонстрирующая нетрадиционные сексуальные отношения и (или) предпочтения; (в ред. Федерального закона от 05.12.2022 N 478-ФЗ)

4) Пропагандирующая педофилию; (в ред. Федерального закона от 05.12.2022 N 478-ФЗ)

5) Способная вызвать у детей желание сменить пол; (в ред. Федерального закона от 05.12.2022 N 478-ФЗ)

Дополнительным свидетельством государственного внимания к проблеме стало появление в 2025 году методических рекомендаций Министерства просвещения Российской Федерации, направленных на обеспечение школ оптимальным и безопасным доступом к информационным системам и сети Интернет [7]. В документе конкретизированы правила фильтрации контента, меры контроля доступа, а также порядок обучения педагогов и учащихся основам цифровой грамотности, что создает организационную основу для системной профилактической работы на уровне каждой образовательной организации.

Г. В. Краснова и А. А. Марков, анализируя современное состояние информационной безопасности, подчеркивают, что одних лишь законодательных мер недостаточно; необходима комплексная система просвещения всех участников образовательных отношений – детей, родителей и педагогов [31].

Значимым шагом в направлении интеграции вопросов сетевой безопасности в образовательный процесс стало закрепление соответствующих требований в Федеральном государственном образовательном стандарте начального общего образования [1]. В перечне личностных результатов освоения программы начальной школы, в частности в рамках предмета «Окружающий мир», прямо указано требование к обучающимся руководствоваться правилами

и нормами безопасного поведения в сети Интернет. Таким образом, формирование соответствующих компетенций из разряда факультативных и рекомендованных переходит в категорию обязательных образовательных результатов, что существенно повышает ответственность педагогического сообщества за данное направление работы.

И. П. Михнев и И. Морев обращают внимание на то, что с распространением мобильного Интернета зона риска для младших школьников значительно расширилась: ребёнок может столкнуться с угрозами в любом месте и в любое время. [36].

Е. Л. Харчевникова, исследуя педагогические условия формирования безопасного поведения, настаивает на необходимости использования интерактивных методов обучения, позволяющих моделировать реальные ситуации сетевого взаимодействия [53].

С ней согласны Л. М. Бронникова и Ю. В. Ребикова, доказывающие эффективность дидактических игр как средства формирования у младших школьников не только знаний, но и практических навыков безопасного поведения в Интернете [44].

Особое значение в контексте рассматриваемой проблемы приобретает взаимодействие школы и семьи. Л. А. Черенцова, изучавшая данную проблематику ещё в начале 2000-х годов, показала, что согласованность требований педагогов и родителей является необходимым условием формирования гуманистической направленности личности младшего школьника [56]. Применительно к сфере интернет-безопасности этот вывод сохраняет свою актуальность, поскольку без поддержки семьи педагогические усилия неизбежно оказываются фрагментарными.

О. Н. Мяэотс в свою очередь акцентирует внимание на необходимости создания в образовательном учреждении целостной системы работы по формированию безопасного поведения, охватывающей урочную, внеурочную деятельность [37].

И. В. Челышева, исследуя проблемы семейного медиаобразования, подчеркивает, что родители зачастую сами не обладают достаточными компетенциями в области сетевой безопасности и нуждаются в организованной просветительской поддержке со стороны школы [55].

Таким образом, анализ современного состояния проблемы свидетельствует о наличии объективного противоречия между высокими требованиями к интернет-безопасности личности младшего школьника, закрепленными в нормативно-правовых актах и образовательных стандартах, и недостаточной разработанностью научно-методического инструментария формирования безопасного поведения в сети Интернет с учётом возрастных особенностей учащихся начальных классов.

Цель исследования: изучить сущность понятия «Безопасное поведение в сети Интернет», определить актуальный уровень знаний младших школьников о безопасном поведении в сети Интернет и создать сайт «КиберЗащитник», направленный на его расширение.

Объект исследования: процесс расширения знаний младших школьников о безопасном поведении в сети Интернет.

Предмет исследования: актуальный уровень знаний младших школьников о безопасном поведении в сети Интернет и способы его повышения.

Гипотеза исследования: знания младших школьников о безопасном поведении в сети Интернет, характеризующиеся содержательным критерием и критерием информационной защиты, находятся преимущественно на среднем и низком уровнях и требуют дальнейшего воздействия.

В соответствии с целью были определены следующие задачи исследования:

1. Изучить основные понятия по теме исследования посредством анализа информации из различных современных и литературных источников.

2. Рассмотреть особенности расширения знаний младших школьников о безопасном поведении в сети Интернет.

3. Рассмотреть способы расширения знаний младших школьников о безопасном поведении в сети Интернет.

4. Составить диагностическую программу и провести исследование по выявлению актуального уровня знаний младших школьников о безопасном поведении в сети Интернет.

5. Обработать и проанализировать полученные результаты констатирующего эксперимента.

6. Разработать инструмент, способствующий расширению знаний младших школьников о безопасном поведении в сети Интернет.

Методы исследования: теоретический (метод теоретического анализа и синтеза), эмпирический (констатирующий эксперимент).

База исследования: МБОУ Лицей №8 г. Красноярск

# ГЛАВА I. ТЕОРЕТИЧЕСКИЙ АСПЕКТ РАСШИРЕНИЯ ЗНАНИЙ МЛАДШИХ ШКОЛЬНИКОВ О БЕЗОПАСНОМ ПОВЕДЕНИИ В СЕТИ ИНТЕРНЕТ

## 1.1 Сущность понятия «безопасное поведение в сети Интернет»

Для того чтобы выявить и определить сущностные, то есть наиболее важные и принципиальные, характеристики безопасного поведения в сети Интернет, представляется вполне целесообразным и логичным обратиться к этимологии – иными словами к существующим в науке трактовкам и определениям понятия «безопасность».

В толковом словаре С. И. Ожегова безопасность трактуется как «состояние, при котором не угрожает опасность, есть защита от опасности» [39].

Схожей позиции придерживается В. И. Даль, определяя данное состояние как «отсутствие опасности; сохранность, надежность» [28].

В словаре Д. Н. Ушакова акцентируется объективная сторона явления: «отсутствие опасности, положение, при котором нет угрозы» [51].

Фундаментальные основы безопасности личности разработаны в трудах И. А. Баевой, которая рассматривает безопасность как явление, без которого не могут нормально развиваться ни личность, ни социальная организация, ни общество, ни государство. Безопасность, в её понимании, выступает необходимым условием стабильного функционирования и поступательного развития любой системы, а потребность в защищенности является одной из базовых для человека [11].

Проблемы информационно-психологической безопасности и защищенности граждан от негативных воздействий исследуются в работах В. А. Баришпольца, который определяет безопасность в Интернете как защищенность отдельных групп и социальных слоев от негативных информационно-психологических воздействий. Исследователь подчеркивает, что в современном мире угрозы, исходящие из виртуального пространства, способны оказывать не

менее разрушительное влияние на сознание и поведение человека, чем угрозы физического характера [12].

Близкой позиции придерживается Г. В. Грачев, рассматривающий информационную безопасность личности как многогранный феномен, охватывающий защиту от дезинформации, манипуляций и нежелательного контента [26].

Значительный вклад в изучение поведенческих аспектов безопасности вносят работы Н. А. Водопьяновой, отмечающей, что безопасное поведение в Интернете представляет собой использование компьютера и глобальной сети с осознанием возможных угроз и принятием соответствующих мер по защите собственных данных и личной информации. Данный подход акцентирует внимание на осознанности действий пользователя как ключевом факторе обеспечения безопасности [20].

В свою очередь Е. Войскунский, исследуя психологию интернет-зависимости, предупреждает, что бесконтрольное погружение в интернет-среду способно не только сделать ребенка уязвимым для внешних атак, но и привести к формированию аддиктивных паттернов, разрушающих его психическое здоровье [21].

А. М. Прихожан рассматривает безопасное поведение в Интернете как такое поведение, при котором ребёнок или взрослый использует интернет-ресурсы правильно и без риска. Исследователь подчеркивает, что формирование подобного поведения требует целенаправленных педагогических усилий, поскольку навыки безопасного взаимодействия с Сетью не возникают спонтанно [43].

Эту мысль развивает Д. В. Григорьев, который указывает, что информационная культура младшего школьника, являющаяся фундаментом безопасного поведения, должна формироваться через специально организованную учебную и внеурочную деятельность, а не путем стихийного накопления опыта проб и ошибок [27].

Р. Б. Стеркина понимает под безопасным поведением - знания, обеспечивающие безопасность личности [49].

А. М. Прихожан акцентирует внимание на правильности и отсутствии риска при использовании интернет-ресурсов как ребенком, так и взрослым [43].

Несмотря на различия в формулировках, все авторы сходятся во мнении, что сущность безопасного поведения в сети Интернет заключается в защите от угроз, предотвращении потенциальных опасностей и создании условий для защищенного взаимодействия в виртуальном пространстве.

Если рассматривать онлайн-угрозы с точки зрения их источника и характера воздействия на ребенка, то специалисты, занимающиеся вопросами в области обеспечения безопасности детей в сети Интернет, выделяют несколько ключевых групп рисков, каждая из которых заслуживает отдельного внимания.

Коммуникационные риски: проявляются в процессе межличностного взаимодействия, возникающего в сети. По оценкам многих специалистов, именно данная категория представляет сегодня наибольшую и, пожалуй, самую серьезную опасность для детей младшего школьного возраста. Связано это в первую очередь с тем, что она напрямую затрагивает сферу живого, непосредственного общения – ту область, в которой ребенок еще не обладает достаточными знаниями, чтобы вовремя заметить потенциальную угрозу и адекватно на нее отреагировать.

Технические риски обусловлены уязвимостью используемых устройств и программного обеспечения. Младшие школьники, скачивая игры, дополнения к ним («читы», «моды») или иной привлекательный контент из непроверенных источников, могут загрузить на устройство вредоносное программное обеспечение. Последствиями такого заражения могут стать: кража личных данных (в том числе паролей доступа и данных банковских карт родителей).

Кроме того, не следует упускать из виду ещё одну весьма серьёзную и, к сожалению, широко распространённую в современной цифровой среде угрозу, жертвами которой дети младшего школьного возраста становятся особенно часто в силу своей естественной доверчивости и пока ещё недостаточно

развитого критического мышления. Речь идёт о так называемых фишинговых атаках. Сам механизм подобных атак строится на том, что злоумышленники создают поддельные ссылки и целые веб-страницы, которые визуально имитируют хорошо знакомые и популярные среди детей сайты – будь то игровые платформы, социальные сети или образовательные ресурсы. Ребёнок, не подозревая подвоха, переходит по такой ссылке и попадает на фальшивую страницу, которая внешне выглядит точь-в-точь как настоящая. Основная цель, которую преследуют киберпреступники в данном случае, заключается в хищении учётных данных юного пользователя: логинов, паролей, а в некоторых случаях и иной чувствительной информации.

Репутационные риски обусловлены особенностью сети сохранять и распространять информацию без временных и географических ограничений. Дети младшего школьного возраста не осознают, что любое опубликованное ими изображение, комментарий или видеозапись могут стать достоянием неограниченного круга лиц и сохраниться в сети на неопределенный срок. Необдуманные публикации способны в будущем негативно повлиять на репутацию ребенка в глазах сверстников, педагогов, а впоследствии – потенциальных работодателей.

Обобщая рассмотренные теоретические подходы, нормативные требования и специфику угроз, можно выделить следующие структурные компоненты знаний младших школьников о безопасном поведении в сети Интернет:

– содержательный компонент включает систему знаний обучающегося об особенностях сети Интернет. В содержание данного компонента входят: знание базовых понятий (персональные данные, пароль, вирус, фишинг и т.д.).

– компонент информационной защиты представляет собой совокупность специализированных знаний, формирующих основу для принятия обоснованных решений по предотвращению угроз и осуществлению защиты личной информации. В отличие от умений и навыков (т.е. автоматизированных действий), данный компонент акцентирует именно осознанную

информированность младшего школьника. Его содержание включает: знание о том, какие именно данные относятся к личным и почему их нельзя передавать третьим лицам; знание принципов создания надежного пароля и последствий его разглашения; знание о существовании механизмов конфиденциальности в играх, приложениях и соцсетях; знание о том, к кому следует обратиться за помощью (родители, учитель) при попытке посягательства на личные данные.

Таким образом, совокупность рассмотренных теоретических подходов, нормативных требований и выделенных структурных характеристик позволяет определить знания младших школьников о безопасном поведении в сети Интернет как интегративное личностное качество, базирующееся на знании потенциальных угроз, правил сетевого взаимодействия и знании основ информационной защиты (что является базой для принятия обоснованных решений по предотвращению угроз и защите личной информации). Такие знания направлены на минимизацию рисков контентного, коммуникационного, технического и потребительского характера, обеспечивая защиту физического и психологического здоровья ребенка в соответствии с требованиями Федерального государственного образовательного стандарта [1] и действующего законодательства Российской Федерации [3].

## 1.2 Особенности расширения знаний младших школьников о безопасном поведении в сети Интернет

Практика показывает, что учащиеся начальных классов представляют собой одну из наиболее уязвимых категорий пользователей глобальной сети, что обусловлено комплексом возрастных, когнитивных и социальных особенностей.

Когнитивные и социальные предпосылки уязвимости младших школьников в сети Интернет:

Младший школьный возраст (период от 7 до 11 лет) характеризуется рядом специфических особенностей, определяющих восприятие ребенком информации и его поведение в интернет-пространстве. Исследователи в области возрастной

педагогики и когнитивного развития (Л.С. Выготский, Д.Б. Эльконин, Ж. Пиаже) отмечают, что на данном этапе онтогенеза происходит переход от наглядно-образного мышления к словесно-логическому [24]. Однако данный процесс находится лишь в начальной стадии своего становления, что создает фундаментальную предпосылку уязвимости: ребенок оказывается неспособным проследить скрытые причинно-следственные связи в сети Интернет и не распознает манипулятивные схемы, поскольку абстрактные понятия («конфиденциальность», «алгоритм рекомендаций», «фишинговая ссылка») для него еще труднодоступны. Кроме того, яркое анимационное оформление, всплывающие окна и аудиосопровождение в приложениях воспринимаются им как маркеры «хорошего», безопасного контента, что напрямую эксплуатируется дизайнерами интерфейсов и злоумышленниками.

Наряду с когнитивными факторами, существуют и социальные предпосылки уязвимости, связанные с ключевыми новообразованиями данного возраста. У младшего школьника резко возрастает значимость оценки сверстников и одобрения со стороны взрослого (в том числе виртуального). В интернет-среде это трансформируется в гиперчувствительность к лайкам, количеству подписчиков и комментариям, что побуждает ребенка раскрывать личную информацию или участвовать в рискованных челленджах ради социального поощрения. При этом невербальные сигналы в онлайне отсутствуют, падает ощущение стыда и страха немедленного наказания («эффект экрана»), а любой яркий блогер или авторитетный по тону голос в подкасте воспринимается ребенком как столь же непререкаемый авторитет, как и учитель в классе.

Таким образом, сочетание незавершенного перехода к словесно-логическому мышлению (с опорой на эмоционально яркие, поверхностные признаки) и социальной ориентации на сиюминутное одобрение делает младшего школьника крайне уязвимым перед угрозами, где необходима оценка последствий и способность распознавать скрытые намерения других пользователей.

По мнению Д.Б. Эльконина, ведущей деятельностью в младшем школьном возрасте становится учебная деятельность, однако она сосуществует с сохраняющейся высокой значимостью игровой активности. Это обстоятельство имеет прямое отношение к поведению детей в интернет-среде: их привлекают красочные, динамичные ресурсы, игровые платформы, интерактивные приложения, что создает благоприятные условия для отвлечения внимания от потенциальных угроз и снижения критичности восприятия поступающей информации [57].

А.Г. Асмолов, указывает на то, что современные младшие школьники растут в условиях цифровой социализации, где интернет выступает не только инструментом получения знаний, но и средой повседневного общения и досуга. Ребенок склонен воспринимать информацию, представленную в сети, как достоверную, особенно если она подается в привлекательной визуальной форме или исходит от «авторитетного» источника (популярного блогера, персонажа игры, сверстника с высоким игровым рейтингом) [10].

Существенный вклад в понимание особенностей восприятия информации младшими школьниками внес Ю.Б. Гиппенрейтер, отмечавший, что дети 6–10 лет характеризуются высокой степенью «информационной всеядности». Они активно потребляют разнообразный контент, однако их способность к его классификации и критической оценке остается весьма ограниченной. Это создает предпосылки для некритичного усвоения информации, в том числе носящей недостоверный или потенциально опасный характер [25].

Дополнительным фактором уязвимости, по мнению П.В. Степанова, выступает несформированность у младших школьников системы устойчивых ценностных ориентаций и мировоззренческих установок. Исследователь подчеркивает, что именно в начальной школе закладываются основы отношения ребенка к окружающему миру, в том числе к миру виртуальному. Отсутствие четких нравственных ориентиров и опыта самостоятельного принятия решений в нестандартных ситуациях делает учащихся данной возрастной группы

восприимчивыми к внешним влияниям, включая деструктивные информационные воздействия [48].

Л.Н. Макарова обращает внимание на становление в младшем школьном возрасте такого важного новообразования, как способность к рефлексии. Дети начинают анализировать собственные поступки, сравнивать свое поведение с действиями окружающих, оценивать ситуации с позиции «хорошо – плохо». Однако данная способность находится в стадии активного развития и требует целенаправленного педагогического сопровождения. В контексте интернет-безопасности это означает, что ребенок может осознавать опасность постфактум, но еще не способен в полной мере прогнозировать риски своих действий в сети и предотвращать их [34].

Таким образом, совокупность возрастных особенностей – преобладание наглядно-образного мышления над абстрактно-логическим, высокая степень доверия к внешним источникам информации, ограниченные навыки критического анализа и прогнозирования, несформированность ценностных ориентиров – обусловливает повышенную уязвимость младших школьников в цифровой среде.

Формирование у учащихся начальных классов знаний о безопасном поведении в сети Интернет представляет собой комплексную и многоаспектную педагогическую задачу, решение которой отнюдь не является простым и однозначным. В данном аспекте ключевое значение приобретает необходимость тщательного и всестороннего учета тех самых возрастных особенностей обучающихся, о которых говорилось выше. Помимо этого, эффективное решение упомянутой задачи требует последовательной интеграции соответствующих компонентов, тематических модулей непосредственно в действующее содержание начального общего образования – как в урочную, так и во внеурочную деятельность.

В научных трудах Н.Ф. Виноградовой обосновывается положение о том, что основы безопасности в сети Интернет должны закладываться в процессе изучения интегрированного курса «Окружающий мир», начиная со второго

класса. Исследователь отмечает, что данный учебный предмет обладает значительным потенциалом для формирования у младших школьников целостной картины мира, включающей представления о современной интернет-среде и знаниях о правилах безопасного взаимодействия с ней. В рамках тематических разделов, посвященных общению, источникам информации, современным средствам связи, учащиеся получают первичные знания о сети Интернет, ее возможностях и связанных с ней ограничениях [19].

Б.С. Волков акцентирует внимание на том, что младший школьный возраст является оптимальным периодом для усвоения знаний о поведении в различных средах, включая цифровую. В этот период дети проявляют выраженную готовность к соблюдению правил, особенно если эти правила представлены в доступной, наглядной форме и подкреплены авторитетом значимого взрослого – педагога или родителя. Исследователь подчеркивает важность формирования у учащихся понимания того, что правила безопасного поведения в интернете являются столь же обязательными для исполнения, как и правила дорожного движения или правила поведения в общественных местах [22].

О.А. Рыдзе, рассматривая вопросы формирования функциональной грамотности младших школьников, включает в это понятие и информационную грамотность как способность ориентироваться в современном интернет пространстве, критически оценивать получаемые сведения, использовать информацию для решения учебных и жизненных задач без ущерба для собственной безопасности. Исследователь подчеркивает, что работа в данном направлении должна носить практико-ориентированный характер и опираться на анализ конкретных ситуаций, близких и понятных учащимся начальных классов [45].

Е.В. Бунеева и О.В. Чиндилова, разрабатывая концепцию начального языкового и литературного образования, обращают внимание на возможности использования художественных текстов и коммуникативных ситуаций для формирования у детей критического отношения к информации. Обсуждение прочитанных произведений, анализ поступков персонажей, оценка

достоверности сообщаемых сведений – все это способствует развитию у учащихся способности к элементарной верификации информации, что является важной составляющей безопасности в сети Интернет [18].

П.В. Степанов, исследуя проблемы воспитания в современной школе, указывает на необходимость тесного взаимодействия образовательной организации с семьей в вопросах формирования у детей знаний о безопасном поведении в сети Интернет. Исследователь отмечает, что без согласованности требований и подходов со стороны педагогов и родителей усилия школы могут оказаться недостаточно эффективными. Родители должны быть информированы о существующих интернет-рисках, о возрастных особенностях восприятия информации детьми, о способах организации безопасного доступа ребенка к сетевым ресурсам в домашних условиях [48].

Проведенный анализ научно-педагогических источников позволяет сделать ряд существенных выводов относительно особенностей формирования безопасного поведения младших школьников в сети Интернет. Прежде всего, необходимо констатировать, что учащиеся начальных классов представляют собой категорию пользователей, обладающую повышенной уязвимостью в цифровой среде. Данная уязвимость обусловлена возрастными особенностями когнитивного развития: преобладанием наглядно-образного мышления над логическим, ограниченной способностью к критическому анализу информации, высокой степенью доверия к внешним источникам.

Современными исследователями (Н.Ф. Виноградова, М.И. Кузнецова, О.А. Рыдзе, П.В. Степанов и другими авторами, работающими в области начального образования) обосновывается необходимость целенаправленной, систематической и непрерывной педагогической работы по формированию у младших школьников знаний о безопасном поведении в сети Интернет [19; 33; 45; 48]. При этом подчеркивается, что данная работа не должна носить эпизодический или разовый характер. Напротив, она должна органично интегрироваться в содержание учебных предметов (прежде всего, в такие дисциплины, как «Окружающий мир», где темы общения, информации и правил

поведения уже заложены программой), а также реализовываться в рамках внеурочной деятельности и, что особенно важно, в тесном и систематическом взаимодействии с родителями обучающихся, поскольку именно семья остается для ребёнка первичным источником поведенческих образцов.

К окончанию начальной школы учащийся должен в полной мере владеть теоретическими знаниями о потенциальных рисках интернет-среды. Достижение указанных результатов в полном объеме соответствует требованиям Федерального государственного образовательного стандарта начального общего образования (ФГОС НОО) в части формирования личностных и метапредметных компетенций обучающихся, что, в свою очередь, является важным и необходимым условием успешной социализации младших школьников в условиях современного информационного общества [1].

## 1.3 Способы и приемы расширения знаний младших школьников о безопасном поведении в сети Интернет в начальной школе

При анализе психолого-педагогической литературы мы выявили, что одним из стимулов интереса к вопросам безопасности в Сети является содержание учебного материала о Интернет рисках.

Но, как отмечает Г.У. Солдатова: «Чтобы сформировать осознанное отношение к угрозам, информация должна быть отчасти тревожной, но не пугающей, и отчасти знакомой младшему школьнику по его повседневному онлайн-опыту». Новое значение знания о кибербезопасности приобретаются учеником тогда, когда происходит сравнение того, что он знал о безопасном поведении ранее (например, «не говорить пароль»), с тем, что он осознал сегодня (например, «почему даже знакомая ссылка может быть опасна») [46].

При анализе психолого-педагогической литературы мы выявили методы и приемы расширения уровня сформированности знаний о безопасном поведении в сети Интернет. В исследованиях большинства педагогов говорится о том, что

на познавательную деятельность огромное влияние оказывает создание ситуации успеха, подкрепленной элементами соревнования.

Рассмотрим позицию Т.Н. Сущинской и А.А. Федорова. Они полагают, что создать ситуацию успеха и удержать внимание к знаниевому компоненту кибербезопасности можно с помощью нескольких методов и приемов.

Во-первых, необходимо использовать принцип нарастающей сложности в кейс-задачах (от распознавания простой угрозы к анализу составных рисков), либо применять специальные «сдвоенные» задания: сначала предложить простое задание на узнавание термина (например, «фишинг»), направленное на актуализацию теоретической базы для понимания более сложных составных инцидентов [50].

Во-вторых, Т.Н. Сущинская пишет: «…применение карточек-консультаций, содержащих алгоритмы безопасных действий в цифровой среде, правил сетевого этикета и образцов анализа опасных ситуаций, а также других материалов, которые позволят учащемуся уверенно оперировать знаниями, не переходя к практическим действиям» [50].

По мнению Е.Н. Киселёвой и Ю.Д. Бабаевой, огромное влияние на развитие интереса к информации о безопасности оказывает включение различных форм соревновательных заданий, нацеленных на проверку и накопление знаний [30].

Также Е.Н. Киселёва пишет: «Проведение сравнения и классификации правил безопасного поведения (например, что можно публиковать, а что нельзя) по заданным или самостоятельно выделенным основаниям положительно влияет на накопление знаний в области интернет-безопасности».

Такой же позиции придерживается и Н.И. Мартишин, который говорит: «Основным средством формирования когнитивного компонента безопасного поведения в курсе “Окружающий мир” и внеурочной деятельности являются вариативные по формулировке учебные задания (объясни, почему ссылка опасна; проверь, верно ли утверждение; оцени, насколько рискованно действие;

выбери правильный вариант поведения; сравни реальную и виртуальную дружбу; найди закономерность в действиях мошенников)» [35].

В работах Л.Р. Болотовой и О.Н. Евсеевой мы видим схожие утверждения. В своих работах они доказывают, что на расширение системы знаний о безопасности наиболее успешно влияют соревновательный эффект, накопительные системы баллов и игровые викторины, также логические разминки на классификацию угроз. Они подчеркивают, что отсроченное вознаграждение в виде начисления баллов за верные ответы работает эффективнее прямого поощрения [16].

При анализе психолого-педагогической литературы мы выявили, что многие педагоги значимым мотиватором для получения знаний о безопасности в сети выделяют игровую механику с достижениями. В частности, Д.В. Воронов и Е.В. Кубанова (в исследовании «Геймификация в профилактике интернет-рисков», 2021) отмечают: «Система накопления баллов за каждое самостоятельно найденное верное решение в тестовом задании по кибербезопасности, а также выдача цифровых “значков” (например, “Хранитель паролей” или “Детектор фейков”) за достижение определённого порога знаний формирует устойчивый познавательный интерес. Знание само по себе начинает восприниматься как ресурс для получения статуса в группе» [23]. Важно, что, согласно их выводам, младший школьник стремится не столько применить правило (навык), сколько знать, как называется угроза, какой рейтинг у его теоретической подготовки и сколько наград он уже заработал.

В последние десятилетия начальное образование в России претерпело значительные изменения, связанные с переходом на новые федеральные государственные образовательные стандарты (ФГОС) и унификацией учебно-методических комплексов. Если ранее в массовой школе были широко представлены вариативные развивающие системы (например, система Л.В. Занкова), то в настоящее время наблюдается тенденция к доминированию единого УМК «Школа России», который выбирается большинством

образовательных организаций в силу своей методической простоты и преемственности с традиционным подходом.

В рамках данного исследования мы проанализировали образовательный маршрут учащихся, которые начинали обучение в 1-2 классах по системе Л.В. Занкова, но впоследствии (в 3-4 классах) перешли на УМК «Школа России».

Цель анализа: оценить, какой фундамент информационной культуры был заложен на начальном этапе обучения (1-2 классы) по системе Занкова и насколько этот фундамент соответствует современным вызовам цифровой среды, в частности – расширению знаний младших школьников о безопасном поведении в сети Интернет.

В дидактической системе Л.В. Занкова ключевым принципом является раннее развитие мышления. Информатика как отдельный предмет в 1 классе обязательно не вводится (в отличие от математики или русского языка). Вместо этого действует принцип интеграции [29].

В 1-м классе система Занкова не предполагает обязательного использования компьютера на уроках. Основной акцент делается на интегрированный курс «Математика и информатика». Учебно-методический комплект (например, авторы И.И. Аргинская, Е.П. Бененсон, С.А. Волкова, а также Н.Я. Виленкин для старших, но для начальной школы – пособия Бененсон) нацелен на развитие знаково-символической деятельности [14].

Во 2-м классе информатика может оставаться в составе интегрированного курса или (по усмотрению школы) выделяться в отдельный пропедевтический курс за счет часов внеурочной деятельности или школьного компонента [14].

Анализ календарно-тематического планирования (КТП) и известных учебных пособий (например, «Информатика. 2 класс» Е.П. Бененсон, А.Г. Паутовой) показывает, что тематика курса в 1-2 классах выглядит следующим образом [14]:

1 класс (в рамках курса «Математика и информатика»):

1. Признаки предметов (цвет, форма, размер, расположение).

2. Сравнение групп предметов (больше, меньше, столько же).

3. Построение цепочек, последовательностей (алгоритмизация в быту).

4. Понятия «истина» и «ложь» (логические высказывания).

5. Работа с таблицами (простейшее структурирование информации).

2 класс (отдельный предмет или модуль):

1. Повторение: Действия с информацией (сбор, хранение, обработка в бытовом смысле).

2. Алгоритмы: Линейные алгоритмы; исполнители (например, «Муравей» или «Черепаха» на бумаге).

3. Логика: Дерево понятий; логические рассуждения по схеме.

4. Кодирование информации: Правила записи информации (азбука Морзе, числовой код).

5. Множества: Пересечение и объединение множеств – решение задач с диаграммами Эйлера-Венна.

Как в 1-м, так и во 2-м классе по системе Занкова инструментальная деятельность с реальным цифровым устройством (компьютером, планшетом) не является обязательной.

После тщательного анализа рабочих программ, методических рекомендаций (авторов: Бененсон Е.П., Паутова А.Г. – для информатики 1-4 кл. а также материалов Федерального научно-методического центра им. Л.В. Занкова) обнаружено следующее:

В 1 классе (интегрированный курс «Математика и информатика») темы «Безопасный интернет» полностью отсутствуют.

Во 2 классе ситуация не меняется. Тематическое планирование по системе Занкова не выделяет отдельного урока или модуля по кибербезопасности. Максимум, что декларируется в общих целях программы – это «формирование информационной культуры», что в трактовке авторов (Бененсон) означает: аккуратное отношение к информации, понимание авторства, работа со справочниками. Словосочетание «Интернет» не упоминается в обязательном минимуме для 1-2 классов по системе Занкова в рамках базовой программы.

В классическом УМК «Информатика» для начальной школы системы Л.В. Занкова (1-2 классы) отсутствуют темы, посвященные знаниям о безопасном поведении в сети Интернет (такие как: защита персональных данных, общение с незнакомцами в сети, кибербуллинг, достоверность информации, компьютерные вирусы, правила выхода в сеть).

В ходе исследования был проанализирован образовательный маршрут учащихся, начавших обучение в 1-2 классах по системе Л.В. Занкова. Как было установлено ранее, в данной системе темы безопасного поведения в сети Интернет отсутствуют в принципе. Естественным следующим шагом исследования является анализ того образовательного материала, который получают дети при переходе на УМК «Школа России» (начиная с 3 класса), а также анализ стандартного содержания программ для начальной школы в целом.

Важно констатировать, что в стандартном учебном плане УМК «Школа России» информатика как отдельный обязательный предмет в 1-4 классах отсутствует. Это соответствует положениям Федерального государственного образовательного стандарта начального общего образования (ФГОС НОО), где информатика не выделяется в качестве самостоятельной предметной области на этом уровне образования [1].

Подтверждение этому факту мы находим в рабочих программах и учебных планах образовательных организаций, работающих по УМК «Школа России». В документах предметная область «Математика и информатика» представлена преимущественно математикой. Информатика же может вводиться в учебный план только при наличии соответствующих условий (кадровых, материально-технических) и только за счет часов вариативной части учебного плана или внеурочной деятельности, но не как обязательный предмет.

ФГОС НОО четко фиксирует личностные результаты, согласно которым обучающийся должен знать о правилах и нормах безопасного поведения в сети Интернет. Это положение является нормативным основанием для включения соответствующего модуля в рабочие программы. Анализ содержания курса «Окружающий мир» в рамках учебно-методического комплекса (УМК) «Школа

России» (авторская линия А.А. Плешакова) показывает последовательное, но дозированное распределение тем, касающихся безопасности в сети Интернет, с 1 по 4 класс [42].

В 1 классе, в первой части учебника «Окружающий мир» (УМК «Школа России», автор А. А. Плешаков), учащиеся знакомятся с темой «Что умеет компьютер?». На соответствующей странице представлен рисунок-схема, иллюстрирующий базовые функции компьютера: хранение информации, проигрывание музыки и видео, помощь в обучении, передача сообщений по электронной почте, игровая деятельность. В сопроводительном тексте кратко сообщается, что компьютеры прочно вошли в нашу жизнь, помогают учиться, отдыхать и общаться, а компьютерная сеть Интернет связывает людей в разных городах и странах. Таким образом, на данном этапе у учащихся формируются первоначальные представления о компьютере как о многофункциональном устройстве и средстве коммуникации, однако вопросы безопасности в сети Интернет и правила контролируемого доступа на страницах первой части учебника не затрагиваются.

Во второй части учебника «Окружающий мир» для 1 класса темы, связанные с безопасным поведением в сети Интернет, полностью отсутствуют. Несмотря на то, что примерное тематическое планирование предусматривает выделение 1 академического часа на ознакомление учащихся с темой «Безопасность в информационно-телекоммуникационной сети Интернет (электронный дневник и электронные ресурсы школы) в условиях контролируемого доступа», в содержании второй части учебника данная тема не представлена ни в виде отдельного параграфа, ни в качестве структурного элемента иных разделов.


*Рис.1. Иллюстративный материал учебника «Окружающий мир» (УМК «Школа России», 1 класс, 1 часть, с. 45, автор А. А. Плешаков), раскрывающий базовые сценарии использования компьютера и сети Интернет (хранение и передача информации, обучение)*

Это означает, что теоретическая база для проведения соответствующего занятия в учебнике отсутствует, и педагогу необходимо самостоятельно подбирать дидактический материал для реализации требований примерного тематического планирования в части ознакомления первоклассников с электронным дневником и правилами безопасного использования школьных интернет-ресурсов.

Во 2 классе, в первой части учебника «Окружающий мир» (УМК «Школа России», автор А. А. Плешаков), темы, связанные с правилами безопасного поведения в сети Интернет, а также с общими правилами пользования

компьютером, полностью отсутствуют. Ни в одном из разделов первой части учебника не представлено ни параграфов, ни отдельных структурных элементов, посвящённых вопросам цифровой гигиены, сетевого общения или техническим аспектам работы с компьютерными устройствами. Таким образом, первая половина учебного года во 2 классе не обеспечена содержательной основой для реализации требований примерного тематического планирования в части формирования у учащихся компетенций безопасного поведения в Интернете.

Во второй части учебника «Окружающий мир» для 2 класса присутствует тема «Опасные незнакомцы», входящая в раздел «Здоровье и безопасность». Однако содержание данной темы ориентировано исключительно на правила безопасного поведения в реальной жизни: учащимся разъясняется, что не следует приглашать в дом незнакомых людей, открывать им дверь, а в случае возникновения опасной ситуации необходимо звонить родителям или по номеру экстренной службы. Вопросы, касающиеся общения с незнакомцами в мессенджерах, социальных группах или иных средах интернет-коммуникации, в рамках данной темы не поднимаются. Прямых указаний на опасности, связанные с виртуальным общением, и на необходимость соблюдения правил безопасности при пользовании сетью Интернет в тексте параграфа не содержится.

Следовательно, несмотря на то, что примерным тематическим планированием на изучение темы «Правила поведения при пользовании компьютером. Безопасность в Интернете (коммуникация в мессенджерах и социальных группах) в условиях контролируемого доступа в Интернет» отводится 3 академических часа, в содержании учебника для 2 класса данная тема прямого отражения не находит.


*Рис.2. Иллюстративный материал учебника «Окружающий мир» (УМК «Школа России», 2 класс, 2 часть, с. 30, автор А. А. Плешаков). Правила безопасного поведения в реальной жизни, без выхода в интернет-среду.*

Материал о технических правилах работы с компьютером (осанка, гимнастика для глаз) и базовых нормах сетевого общения, предусмотренный программой, в учебнике отсутствует, что возлагает на педагога обязанность по самостоятельному подбору дидактических средств для проведения соответствующих занятий.

В 3 классе, в первой части учебника «Окружающий мир» (УМК «Школа России», авторы А. А. Плешаков, М. Ю. Новицкая), темы, касающиеся безопасного поведения в сети Интернет, полностью отсутствуют. Ни в одном из разделов первой части учебника не содержится параграфов или отдельных структурных элементов, посвящённых вопросам защиты персональных данных, распознавания интернет-мошенничества или правилам безопасной коммуникации.

Во второй части учебника «Окружающий мир» для 3 класса ситуация аналогична: темы, связанные с безопасным использованием информационно-телекоммуникационной сети Интернет, также отсутствуют. Несмотря на то, что примерное тематическое планирование предполагает изучение в 3 классе темы «Безопасность в Интернете (ориентировка в признаках мошенничества в сети; защита персональной информации) в условиях контролируемого доступа в Интернет», в содержании учебника данная тема не представлена ни в виде отдельного параграфа, ни в качестве составной части иных разделов. Таким образом, теоретическая основа для проведения предусмотренного программой занятия в материалах учебника отсутствует, и педагог вынужден самостоятельно изыскивать дидактические средства для реализации требований тематического планирования.

Дополнительно следует отметить, что в рамках отдельных вариативных программ внеурочной деятельности («Мир информатики») могут встречаться фрагменты, касающиеся понятия «компьютерные сети». Однако эти упоминания носят сугубо технический характер и не подкреплены выделением специальных часов на изучение социальных аспектов безопасности: признаков мошенничества, фишинга, способов защиты персональных данных. Содержательный анализ показывает, что жизненно важные для девятилетнего ребенка темы, такие как «Как распознать обман в сети» или «Почему нельзя сообщать адрес и телефон незнакомым людям в Интернете», не включены ни в содержание учебника, ни в тематические планы внеурочной деятельности УМК «Школа России». Следовательно, количество учебных часов, отводимых на обсуждение этих вопросов в рамках гарантированной государством урочной и внеурочной занятости, фактически равно нулю. Отсутствие системной работы в третьем классе означает, что младший школьник подходит к рубежу перехода в основную школу, имея за плечами три года потенциального накопления стихийного интернет-опыта при полном отсутствии педагогически организованной рефлексии этого опыта как на уроках, так и во внеурочное время.

В 4 классе в первой части учебника «Окружающий мир» для 4 класса (авторы А. А. Плешаков, Е. А. Крючкова) в разделе «Человек и его безопасность» содержится фрагмент, посвящённый безопасному поиску информации в Интернете. Данный материал представляет собой краткий информационный абзац, не сопровождающийся вопросами или заданиями для учащихся. В тексте сообщается, что для безопасного поиска образовательных ресурсов и достоверной информации следует заходить на сайты, рекомендованные учителем или родителями, как можно точнее формулировать поисковый запрос, отдавать предпочтение государственным образовательным ресурсам, официальным сайтам известных организаций, детским образовательным порталам, а также избегать информации с броскими, сенсационными заголовками, за которыми, как правило, скрываются недостоверные или ложные сведения.

2. **Безопасный поиск информации в Интернете.** Для безопасного поиска образовательных ресурсов и достоверной информации в Интернете лучше всего заходить на сайты, которые рекомендованы учителем, родителями. При работе с Интернетом нужно как можно точнее формулировать поисковый запрос. Тогда вы получите ссылки на источники именно той информации, которая вас интересует. Просмотрев эти ссылки, отдайте предпочтение государственным образовательным ресурсам, официальным сайтам известных организаций (например, музеев, заповедников, администраций городов, регионов), детским образовательным порталам или тем ресурсам, которыми вы уже успешно пользовались раньше.

Используя Интернет, избегайте информации с броскими, сенсационными заголовками. Как правило, за ними скрываются недостоверные или ложные сведения.

*Рис.3. Материал учебника «Окружающий мир» (УМК «Школа России», 4 класс, 1 часть, с. 38, автор А. А. Плешаков, Е. А. Крючкова) о безопасном поиске информации в Интернете.*

Однако следует отметить, что данный материал носит исключительно информационный характер и не подкреплён методическим аппаратом (вопросами, заданиями, проблемными ситуациями), который позволил бы организовать активную познавательную деятельность учащихся. Кроме того, темы, связанные с защитой персональных данных, распознаванием интернет-мошенничества и правилами безопасной коммуникации в мессенджерах, в

содержании данного раздела не представлены. Материал ограничивается аспектом поиска достоверной информации, в то время как другие компоненты безопасного поведения в сети Интернет остаются за рамками учебника.

Во второй части учебника «Окружающий мир» для 4 класса темы, касающиеся безопасного поведения в сети Интернет, отсутствуют полностью.

Таким образом, анализ учебников «Окружающий мир» (УМК «Школа России») с 1 по 4 класс показал, что тема безопасного поведения в сети Интернет представлена фрагментарно и бессистемно.

В совокупности за четыре года обучения в начальной школе вопросам безопасного поведения в сети Интернет посвящён лишь один небольшой текстовый фрагмент в учебнике 4 класса, лишённый методического аппарата. При этом примерное тематическое планирование отводит на изучение данной темы суммарно 7 часов. Выявленное несоответствие между программными требованиями и реальным содержанием учебников свидетельствует о необходимости разработки дополнительных дидактических материалов, обеспечивающих формирование у младших школьников навыков безопасного поведения в сети Интернет.

ФГОС НОО предусматривает организацию внеурочной деятельности как обязательного компонента основной образовательной программы, направленного на достижение личностных и метапредметных результатов. Именно внеурочная деятельность является тем ресурсом, который позволяет восполнить дефицит учебного времени, отмеченный в пункте 2.1

Внеурочная деятельность, регламентированная Федеральным государственным образовательным стандартом начального общего образования (ФГОС НОО), рассматривается в теории педагогики как пространство для углубления и расширения предметных областей, формирования личностных компетенций и социализации обучающихся. На уровень начального общего образования отводится до 1350 часов внеурочных занятий. Однако практический анализ содержательного наполнения программ внеурочной деятельности, функционирующих в логике учебно-методического комплекса «Школа России»,

приводит к парадоксальному выводу: именно критическая нехватка тематических модулей и академических часов, посвященных безопасному поведению в сети Интернет, выводит данную проблему в разряд наиболее актуальных и неразрешенных противоречий современного начального образования.

Для обучающихся первых классов внеурочная деятельность в УМК «Школа России» традиционно представлена такими программами, как «Умники и умницы», «В мире книг», «Я – пешеход и пассажир». Ни в одной из указанных программ, согласно их опубликованному тематическому планированию, не содержится ни одной темы, прямо или косвенно касающейся взаимодействия ребенка с информационно-телекоммуникационной сетью Интернет. Более того, в содержании не предусмотрено даже пропедевтических бесед о существовании цифровых угроз. Количество часов, выделяемых на изучение безопасного поведения в сети Интернет в рамках внеурочной деятельности первого класса, равно нулю.

К второму году обучения перечень внеурочных занятий в УМК «Школа России» пополняется курсами «Информатика в играх и задачах» (бескомпьютерный вариант) и «Проектная деятельность». Анализ их содержания показывает, что темы, связанные с коммуникацией в мессенджерах, правилами поведения в социальных группах, защитой от незнакомцев в сети, в планировании отсутствуют. Курс информатики направлен исключительно на развитие логического мышления, а проектная деятельность не включает модуля по безопасному поиску информации. Количество часов, целенаправленно выделяемых на формирование навыков информационной безопасности во внеурочной деятельности 2 класса, составляет ноль.

В третьем классе в рамках отдельных вариативных программ («Мир информатики») могут встречаться фрагменты, касающиеся понятия «компьютерные сети». Однако эти упоминания носят сугубо технический характер и не подкреплены выделением специальных часов на изучение социальных аспектов безопасности: признаков мошенничества, фишинга,

способов защиты персональных данных. Содержательный анализ показывает, что жизненно важные для девятилетнего ребенка темы, такие как «Как распознать обман в сети» или «Почему нельзя сообщать адрес и телефон незнакомым людям в Интернете», не включены в тематические планы внеурочной деятельности УМК «Школа России».

В четвертом классе, на завершающем этапе начального образования, внеурочная деятельность в УМК «Школа России» ориентирована на проектную и исследовательскую активность («Я – исследователь»). При этом темы, связанные с поиском достоверной информации в сети Интернет, опознанием государственных образовательных ресурсов, критическим анализом контента, не выделены в самостоятельные тематические блоки.

Проведенный детальный анализ содержания программ внеурочной деятельности, функционирующих в рамках учебно-методического комплекса «Школа России» для 1-4 классов, позволяет сформулировать ряд принципиально важных выводов, касающихся представленности тематики безопасного поведения в информационно-телекоммуникационной сети Интернет.

Установлено, что в рекомендованных и наиболее распространенных программах внеурочной деятельности по всем пяти направлениям развития личности (спортивно-оздоровительному, духовно-нравственному, социальному, общеинтеллектуальному и общекультурному) полностью отсутствуют темы, прямо или косвенно посвященные вопросам безопасности в сети Интернет, цифровой гигиены, защите персональных данных, распознаванию интернет-мошенничества, противодействию кибербуллингу, поиску достоверной информации или правилам безопасной коммуникации в сети. Данный тематический вакуум прослеживается на протяжении всех четырех лет обучения в начальной школе.

Анализ содержания конкретных программ внеурочной деятельности показывает, что в них не выделены в качестве самостоятельных дидактических единиц следующие темы, необходимость изучения которых диктуется требованиями Федерального государственного образовательного стандарта

начального общего образования (ФГОС НОО) к личностным результатам и объективными вызовами современной цифровой среды:

1. Тема «Элементарные правила использования электронных ресурсов школы и сети Интернет под контролем взрослых» – отсутствует в программах для 1 класса («Умники и умницы», «В мире книг», «Я – пешеход и пассажир», «Занимательная грамматика»). Вместо этого тематические планы заполнены темами, не связанными с цифровой социализацией ребенка: «Где появились куклы», «История глиняной игрушки», «Откуда пришла тарелка», «Русские народные игры», «Путешествие к славянской азбуке».

2. Тема «Правила безопасной коммуникации в мессенджерах и социальных группах, основы сетевого этикета» – отсутствует в программах для 2 класса («Информатика в играх и задачах», «Проектная деятельность»). При наличии в проектной деятельности указания на «поиск информации в Интернете», специальные часы на обучение безопасному поиску не выделены, тема безопасной коммуникации не предусмотрена. Тематические планы вместо этого содержат проекты: «Родное село», «Красная книга», «Профессии», «Родословная», «Города России».

3. Тема «Признаки интернет-мошенничества, фишинга, способы защиты персональных данных» – отсутствует в программах для 3 класса. В рамках курса «Мир информатики» могут встречаться технические сведения о компьютерных сетях, но социально-педагогический блок, направленный на распознавание угроз и формирование навыков безопасного поведения, в тематическое планирование не включен. Вместо этого представлены темы: «Рисование на тему "Мой прекрасный сад"», «Декоративное рисование "Дивный сад на подносах"», «Художественное конструирование и дизайн».

4. Тема «Поиск достоверной информации в сети Интернет, опознание государственных образовательных ресурсов и детских развлекательных порталов, основы критического анализа контента» – отсутствует в программах для 4 класса («Праздники, традиции и ремесла народов России», «Доноведение», «Я – исследователь»). Тематические планы заполнены темами: «Наряды дам 18

века», «Причёски девушек и дам 18 века», «Дворцы Петербурга», «Балы и праздники», «Смольный институт благородных девиц», «Полезные ископаемые родного края», «Водоёмы Ростовской области».

Суммарное количество академических часов, целенаправленно выделяемых на изучение безопасного поведения в сети Интернет во внеурочной деятельности в рамках УМК «Школа России» с 1 по 4 класс, составляет ноль часов. Из общего ресурса внеурочной деятельности, достигающего 1350 часов за четыре года обучения, на формирование знаний о безопасности в сети Интернет не отведено ни одного гарантированного часа.

## Выводы по I главе

Анализ психолого-педагогической, методической и нормативно-правовой литературы показал, что в науке и образовательной практике сформировался многогранный взгляд на понятие «безопасное поведение в сети Интернет». Рассмотрев различные научные подходы, мы пришли к выводу, что безопасное поведение младшего школьника в сети Интернет – это интегративное личностное качество, базирующееся на знании потенциальных угроз, правил сетевого взаимодействия и основ информационной защиты, направленное на минимизацию рисков различного характера и обеспечение защищенности физического и психического здоровья ребенка. В дальнейшем мы решили опираться на трактовку, синтезирующую положения, сформулированные в трудах И. А. Баевой [11], Н. А. Водопьяновой [20] и А. М. Прихожан [43], и закрепленную требованиями ФГОС НОО [1]. Также данный анализ показал, что безопасное поведение представляет собой целостную структуру, содержательными компонентами которой выступают содержательный (знаниевый) компонент и компонент информационной защиты, объединяющий представления о защите персональных данных и алгоритмах действий в опасных ситуациях.

Далее мы рассмотрели особенности расширения знаний о безопасном поведении в сети Интернет у младших школьников. При анализе научных трудов Л. С. Выготского [24], Д. Б. Эльконина [57], А. Г. Асмолова [10] и других исследователей мы выявили, что специфика данного процесса тесно связана с возрастными когнитивными и личностными особенностями учащихся начальной школы.

Ключевыми факторами уязвимости младших школьников в цифровой среде являются преобладание наглядно-образного мышления над логическим, высокая степень доверия к внешним источникам информации и недостаточная сформированность критического мышления. В основе успешного формирования безопасного поведения у младших школьников лежит соблюдение педагогических условий, а именно: максимальная опора на наглядность, использование интерактивных и игровых методов обучения. Нами также было установлено, что на эффективность данной работы огромное влияние оказывает содержание учебного материала и систематичность его преподавания.

На основании проведенного анализа учебно-методического комплекса «Школа России» (авторская линия А. А. Плешакова) [42] и соответствующих методических разработок к УМК, можно констатировать отсутствие полноценных часов, посвященных вопросам безопасного поведения в сети Интернет, в учебном курсе «Окружающий мир» с 1 по 4 класс. Материал в данном УМК представлен преимущественно в форме теоретических правил и информационных справок. Проанализировав программы внеурочной деятельности указанного УМК, мы выяснили, что тематика безопасного поведения в сети Интернет, защиты персональных данных и распознавания интернет-мошенничества в них полностью отсутствует на протяжении всех четырех лет обучения. Мы можем сделать вывод, что современного дидактического материала, направленного на системное расширение знаний младших школьников о безопасном поведении в сети Интернет, представлено в ограниченном количестве.

# ГЛАВА II. ИЗУЧЕНИЕ АКТУАЛЬНОГО УРОВНЯ ЗНАНИЙ МЛАДШИХ ШКОЛЬНИКОВ О БЕЗОПАСНОМ ПОВЕДЕНИИ В СЕТИ ИНТЕРНЕТ

## 2.1 Методики оценки актуального уровня знаний младших школьников о безопасном поведении в сети Интернет

При анализе нормативно-правовой и психолого-педагогической литературы мы выяснили, что критериями оценки уровня знаний младших школьников в области безопасности в сети Интернет будут являться: содержательный и критерий информационной защиты. Рассмотрим обоснование выбора данных критериев подробнее.

Критерии были сформулированы на основе теоретической модели цифровой компетентности, разработанной Г.У. Солдатовой и Е.И. Рассказовой [46]. В их концепции цифровая компетентность понимается как сложное многокомпонентное образование, включающее четыре взаимосвязанных компонента: знания, умения, мотивацию и ответственность, которые проявляются в четырёх сферах деятельности – информационной, коммуникативной, потребительской и техносфере. Поскольку предметом нашего исследования является не сформированность практических действий, а именно система знаний младших школьников, мы опираемся на знаниевый компонент данной модели. Как отмечают авторы, «знаниевый компонент является фундаментом, на котором впоследствии выстраиваются умения и формируется ответственное отношение» [46]. Таким образом, первый критерий – содержательный – отражает совокупность знаний, обучающихся об особенностях сети Интернет, её рисках и правилах поведения.

Важность этого критерия подтверждается и положениями Федерального государственного образовательного стандарта начального общего образования (ФГОС НОО), где в требованиях к метапредметным результатам зафиксирована необходимость «освоения способов решения проблем творческого и поискового характера», а в предметной области «Технология» – «овладения

первоначальными умениями передачи, поиска, преобразования, хранения информации, использования компьютера» [1]. Именно знаниевый фундамент создаёт предпосылки для последующего формирования навыков безопасного поведения.

Второй критерий был выделен нами в качестве самостоятельного, поскольку проблема защиты персональных данных в сети Интернет приобрела особую остроту в последнее десятилетие. В концепции Солдатовой и Рассказовой данному аспекту соответствует сфера ответственности и безопасности, которая пронизывает все четыре вида деятельности в интернете. Авторы подчёркивают, что «наиболее проблемной зоной для детей и подростков остаётся именно компонент ответственности, связанный с защитой личной информации».

Значимость выделения данного критерия в отдельную единицу оценивания подтверждается нормативно-правовой базой Российской Федерации. Согласно Федеральному закону № 152-ФЗ «О персональных данных», обработка персональных данных должна осуществляться с соблюдением принципов конфиденциальности и безопасности [4]. Роскомнадзор в своих официальных разъяснениях неоднократно указывал, что «дети и подростки являются одной из наиболее чувствительных и наименее защищённых категорий субъектов персональных данных». В связи с этим, в содержание образования младших школьников необходимо включать отдельный блок знаний о способах защиты приватной информации. Критерий информационной защиты, таким образом, представляет собой совокупность знаний обучающихся, формирующих понимание того, какие сведения относятся к категории личных, почему ими нельзя делиться с посторонними и какова сущность приватности в онлайн-среде.

Выделенные критерии не являются рядоположными – они находятся в иерархической зависимости. Содержательный критерий выступает как базовый, фундаментальный: он охватывает широкий спектр знаний о цифровой среде в целом – от устройства интернета до типов мошеннических действий. Критерий информационной защиты является производным, углубляющим и

конкретизирующим один из аспектов общего содержательного поля – а именно знания о способах сохранения конфиденциальности личных данных. Взаимосвязь между критериями строится по принципу «от общего к частному»: сначала оценивается широта и полнота общих представлений обучающегося, затем – углублённое понимание наиболее значимого для безопасности младшего школьника аспекта.

Такую структуру критериального аппарата мы выстроили, опираясь на исследования Г.У. Солдатовой в области цифровой социализации. Автор отмечает, что «формирование цифровой компетентности идёт неравномерно: общая осведомлённость об интернете может быть высокой, тогда как конкретные знания в сфере защиты данных существенно западают» [47].

При выделении трёх уровней выраженности каждого критерия (низкого, среднего и высокого) мы опирались на традиционную в отечественной педагогике трёхуровневую дифференциацию, представленную в работах В.П. Беспалько [15] и развитую применительно к информационной безопасности в исследованиях Г.У. Солдатовой, Е.И. Рассказовой и Т.А. Нестика [46; 38].

В.П. Беспалько в теории педагогических систем обосновал, что освоение любого содержания проходит через несколько уровней: от узнавания (репродуктивного) до применения в новых условиях (творческого) [15]. Этот подход был адаптирован нами с учётом специфики исследования: поскольку мы оцениваем не умения и действия, а именно знания, уровни отражают степень полноты, осознанности и системности имеющихся представлений.

При определении балльных диапазонов для каждого уровня мы ориентировались на подход, предложенный Г.У. Солдатовой и Е.И. Рассказовой. В исследовании, проведённом на выборке детей 7–11 лет и их родителей, было эмпирически установлено, что средний показатель цифровой компетентности детей составляет примерно 30% от максимально возможного балла, а взрослых – 46%. С учётом возрастных познавательных возможностей младших школьников и сложности изучаемой предметной области, мы определили пороговые значения следующим образом.

Опираясь на логику, согласно которой низкий уровень должен «захватывать» зону минимальной осведомлённости (включая среднестатистические показатели по выборке), а высокий – отражать качественный скачок в осознанности знаний, мы установили следующие границы. Низкий уровень – менее 50% от максимального балла; в этот диапазон попадают дети, чьи знания фрагментарны и бессистемны. Средний уровень – от 50 до 75% от максимального балла; он охватывает обучающихся, имеющих базовые знания об основных правилах и угрозах, однако эти знания ещё не сложились в устойчивую систему. Высокий уровень – более 75% от максимального балла; эту группу составляют школьники с осознанными, систематизированными знаниями, способные ориентироваться в нестандартных ситуациях [38].

Диагностический инструмент, применяемый для оценки содержательного критерия, содержит 30 заданий, каждое из которых направлено на выявление конкретного аспекта знаний об устройстве интернета, существующих рисках и правилах безопасного поведения. Каждый верный ответ оценивается в 1 балл, неверный – 0 баллов, максимально возможный результат составляет 30 баллов. Исходя из изложенной выше логики шкалирования, были установлены следующие диапазоны.

Низкий уровень (0–14 баллов, что составляет менее 50% от максимума) характеризуется минимальной осведомлённостью. Обучающийся плохо понимает сущность интернет-опасностей, не различает, какие сведения относятся к личным данным, а какие являются общедоступными. В его представлениях отсутствует понимание рисков, связанных с мошенничеством, подозрительными ссылками и использованием публичных сетей Wi-Fi. Ребёнок не задумывается о последствиях своих действий в сети Интернет, что создаёт объективные предпосылки для попадания в ситуации, угрожающие его безопасности.

Средний уровень (15–23 баллов, диапазон 50–75% от максимума) свидетельствует о том, что у ученика сформированы базовые знания о ключевых

правилах безопасного поведения в сети Интернет. Он знает, что нельзя сообщать пароль и личные данные незнакомцам, понимает опасность, исходящую от мошенников и подозрительных ссылок. Однако эти знания ещё недостаточно систематизированы и проявляются преимущественно в типичных, стандартных ситуациях. В сложных, нестандартных обстоятельствах, требующих переноса знаний в новую плоскость, ребёнок может ошибаться, так как его представления не достигли уровня, обобщённого понимания принципов кибербезопасности.

Высокий уровень (24–30 баллов, более 75% от максимума) отражает сформированность осознанных знаний. Ребёнок хорошо разбирается в вопросах интернет-безопасности, понимает, что такое цифровой след и почему важно его контролировать. Он осознанно распознаёт угрозы различного характера, дифференцирует их и задумывается о долгосрочных последствиях своих действий в сети. Знания носят системный характер, что позволяет ученику ориентироваться не только в знакомых, но и в новых для него ситуациях.

Диагностический инструмент, используемый для оценки критерия информационной защиты, содержит 10 заданий, каждое из которых моделирует конкретную ситуацию, связанную с необходимостью принятия решения о защите или разглашении личной информации. Каждый верный ответ оценивается в 1 балл, максимально возможный результат составляет 10 баллов. Применяя тот же принцип шкалирования, мы установили следующие диапазоны.

Низкий уровень (0–4 баллов, менее 50% от максимума) указывает на отсутствие знаний о том, как следует действовать для сохранения конфиденциальности в интернете. Ребёнок считает допустимым сохранять пароли без средств защиты, сообщать коды из СМС-сообщений третьим лицам, переходить по подозрительным ссылкам, полученным от незнакомых отправителей. Его представления о приватности не сформированы, что делает его уязвимым перед целым спектром угроз, связанных с хищением персональных данных.

Средний уровень (5–7 баллов, диапазон 50–75% от максимума) свидетельствует о том, что базовые правила безопасного поведения ученику

известны. Он знает, что нельзя никому сообщать пароли и коды подтверждения, понимает риск, связанный с подозрительными сообщениями и ссылками. Однако его знания фрагментарны и касаются лишь наиболее очевидных угроз. В более сложных ситуациях – например, при необходимости настройки приватности в социальных сетях или оценке угроз, связанных с использованием публичного Wi-Fi, – ребёнок может не учесть всех факторов риска.

Высокий уровень (8–10 баллов, более 75% от максимума) демонстрирует, что обучающийся отлично знает правила безопасного поведения в сети Интернет. Он не только осознаёт, что нельзя передавать пароли и коды, но и понимает необходимость проверки источников информации, осознаёт ограничения, присущие публичным сетям Wi-Fi, и имеет правильное представление о том, что такое приватность и почему её необходимо сознательно оберегать. Знания носят устойчивый характер и проявляются вне зависимости от контекста предъявляемой ситуации.

На основании выделенных критериев и их уровневой дифференциации мы охарактеризовали следующие обобщённые уровни сформированности знаний о безопасном поведении в сети Интернет у младших школьников.

Низкий уровень в целом характеризуется познавательной пассивностью в отношении вопросов безопасного поведения в сети Интернет. Ученик не ставит перед собой задачи углубить знания об изучаемом объекте, его представления отрывочны и бессистемны. Он не идентифицирует типичные онлайн-угрозы, не осознаёт ценности личной информации и не задумывается о возможных последствиях неосторожного поведения в цифровой среде. Внимание к вопросам безопасности не сосредоточено, интерес к ним носит ситуативный, эпизодический характер и возникает лишь в результате ярких внешних впечатлений, а не внутренней познавательной потребности.

Средний уровень свидетельствует о наличии определённого фундамента знаний об основных правилах безопасного поведения в сети Интернет. Ученик демонстрирует познавательную активность в этом направлении, однако она требует периодической стимуляции со стороны педагога или родителей. Знания

ребёнка ещё недостаточно систематизированы и проявляются преимущественно в типичных, многократно разбиравшихся на занятиях ситуациях. В нестандартных обстоятельствах, когда требуется самостоятельный анализ и перенос известных правил в новую плоскость, ученик испытывает затруднения и может принять ошибочное решение.

Высокий уровень характеризуется наличием сформированной системы осознанных знаний. Ребёнок демонстрирует устойчивый познавательный интерес к вопросам кибербезопасности, стремится к расширению и углублению своих представлений. Его знания носят целостный характер, он способен дифференцировать различные типы угроз, осознаёт долгосрочные последствия неосторожного обращения с личными данными и имеет чёткое представление о том, как следует выстраивать собственное поведение в сети Интернет, чтобы минимизировать риски.

При подборе методик для диагностики каждого из выделенных критериев мы руководствовались следующими принципами, основанными на анализе теоретических источников. Во-первых, принцип возрастной адекватности: диагностический инструментарий должен соответствовать познавательным возможностям детей 7–11 лет, учитывать наглядно-образный характер их мышления и ограниченный объём произвольного внимания. Во-вторых, принцип предметной валидности: каждое задание должно диагностировать именно знаниевый компонент, а не скорость реакции, техническую грамотность или навыки навигации. В-третьих, принцип соответствия нормативной базе: содержание заданий должно опираться на актуальные требования к результатам начального образования, зафиксированные во ФГОС НОО и уточнённые в Концепции информационной безопасности детей, утверждённой распоряжением Правительства РФ от 2 декабря 2015 г. № 2471-р [6].

Концепция информационной безопасности детей, в частности, подчёркивает необходимость «формирования у детей навыков самостоятельного и ответственного потребления информационной продукции» и «повышения уровня медиаграмотности детей» [6]. Хотя в формулировках документа

используется слово «навыки», содержательный анализ показывает, что речь идёт прежде всего о когнитивной основе – знаниях, на которых эти навыки впоследствии формируются. Именно на выявление этой когнитивной основы и направлен наш диагностический инструментарий.

В соответствии с описанными выше критериями, их уровневыми характеристиками и системой оценивания была разработана диагностическая программа исследования актуального состояния знаний о безопасном поведении в сети Интернет у младших школьников. В программе в табличной форме представлены критерии, уровни, балльные диапазоны для каждого критерия и перечень применяемых диагностических материалов.

## 2.2 Результаты исследования актуального уровня знаний младших школьников о безопасном поведении в сети Интернет

Цель констатирующего эксперимента – изучить актуальный уровень знаний младших школьников о безопасном поведении младших школьников в сети Интернет.

Исследование проводилось на базе МБОУ Лицей № 8 г. Красноярск. В исследовании приняли участие 28 обучающихся 2 «А» класса в возрасте 8-9 лет.

При анализе психолого-педагогической литературы нами были выделены следующие критерии знаний младших школьников о безопасном поведении младших школьников в сети Интернет: содержательный и информационной защиты.

Для оценки первого критерия в качестве диагностического инструментария нами была выбрана методика «Тест по кибербезопасности» (автор-составитель Булдакова Анна Васильевна) [17]. На основе данной методики, мы оценивали понимание особенностей сети, знаний её рисков, правил защиты данных, распознавания угроз и мошеннических действий.

Данная методика включает в себя тест из 30 вопросов закрытого типа (с вариантами ответа). Тестирование проводилось в рамках одного академического

часа (40 минут). Перед началом тестирования учащимся были выданы бланки с вопросами, а также сообщены правила выполнения работы. Школьникам разъяснялось, что к каждому вопросу предлагается несколько вариантов ответа, из которых необходимо выбрать один правильный. Акцентировалось внимание на том, что задание не является контрольной работой и не подлежит оцениванию с выставлением отметок, что позволило снизить уровень тревожности и получить более достоверные результаты. Время, отведённое на инструктаж, составило 2–3 минуты. За 5 минут до окончания урока было предупреждение учащихся о необходимости проверить ответы и завершить работу. После сигнала об окончании времени бланки собирались и проверялись на комплектность сданных материалов и наличие подписей (фамилия, имя, класс) на каждом бланке.

Оценивание производилось следующим образом: диагностический тест содержит 30 вопросов, каждый верный ответ оценивается в 1 балл. Максимально возможное количество баллов – 30. На основе набранной суммы баллов, учащиеся были распределены по трём уровням в соответствии с описанной ранее шкалой:

1. Если ученик набрал от 0 до 14 баллов – низкий уровень (менее 50% от максимального балла);

2. Если ученик набрал от 15 до 23 баллов – средний уровень (50–75% от максимального балла);

3. Если ученик набрал от 24 до 30 баллов – высокий уровень (более 75% от максимального балла).

Полученные результаты мы отобразили на рисунке 4.

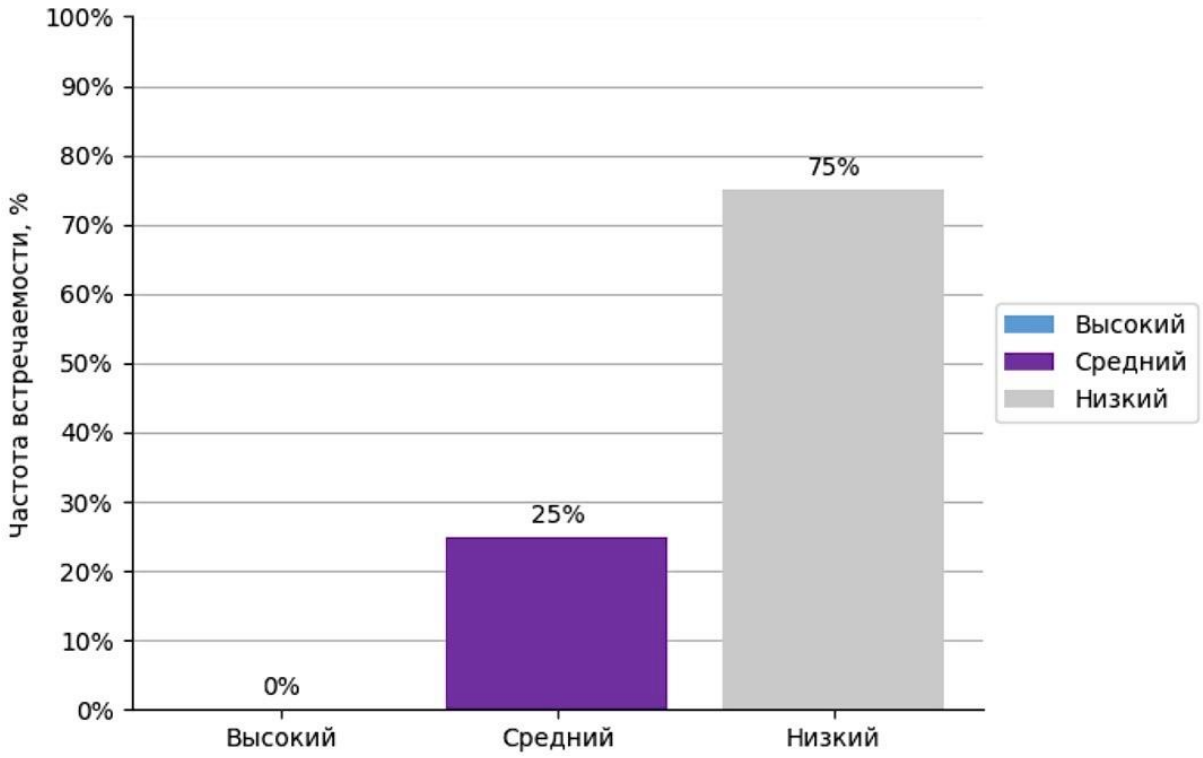



*Рис. 4. Результаты исследования актуального уровня знаний о безопасном поведении в сети Интернет у учащихся 2 класса по критерию «Содержательный»*

Проанализировав рис.4, мы выяснили, что содержательный уровень развития выглядит следующим образом:

75 % учащихся находятся на низком уровне развития содержательного критерия. Это означает, что у учащихся данной группы отсутствует система знаний об особенностях сети Интернет и её рисках. Они плохо понимают сущность интернет-опасностей, не различают, какие сведения относятся к личным данным, а какие являются общедоступными. Учащиеся не идентифицируют действия мошенников, могут переходить по подозрительным ссылкам и не осознают риски, связанные с использованием публичных сетей Wi-Fi.

25 % учащихся находятся на среднем уровне развития содержательного критерия. В данном случае у учащихся наблюдаются базовые знания о ключевых правилах безопасного поведения. Ученики знают, что нельзя сообщать пароль и личные данные незнакомцам, понимают опасность, исходящую от мошенников

и подозрительных ссылок. Однако эти знания ещё недостаточно систематизированы и проявляются преимущественно в стандартных ситуациях. В сложных, нестандартных обстоятельствах, требующих переноса знаний в новую плоскость, учащиеся могут ошибаться, так как их представления не достигли уровня обобщённого понимания принципов кибербезопасности.

0 % учащихся находятся на высоком уровне развития содержательного критерия.

При проверке работ по содержательному критерию было выявлено следующее: общая осведомлённость учащихся об интернете и его безопасности оценивается как недостаточно высокая. Наибольшие затруднения у учащихся вызвали вопросы, связанные с понятиями «цифровой след», «фишинг» и правилами использования публичного Wi-Fi. При этом большинство учащихся верно определили, что такое личные данные и почему нельзя сообщать свой адрес незнакомым людям, что свидетельствует о наличии первичных, но ещё не систематизированных представлений в данной области.

При проверке работ учащихся 2 класса по критерию информационной защиты нами были получены следующие результаты. Тестирование проводилось в течение 20 минут, отведённых от урока. Использовалась методика № 2 – тест «Работа с персональными данными» (7–11 лет), рекомендованный Роскомнадзором.

Оценивание производилось следующим образом: диагностический тест содержит 10 вопросов, каждый верный ответ оценивается в 1 балл. Максимально возможное количество баллов – 10. На основе набранной суммы баллов, учащиеся были распределены по трём уровням в соответствии с описанной ранее шкалой:

1. Если ученик набрал от 0 до 4 баллов – низкий уровень (менее 50 % от максимального балла);

2. Если ученик набрал от 5 до 7 баллов – средний уровень (50–75 % от максимального балла);

3. Если ученик набрал от 8 до 10 баллов – высокий уровень (более 75 % от максимального балла).

Полученные результаты мы отобразили на рисунке 5.

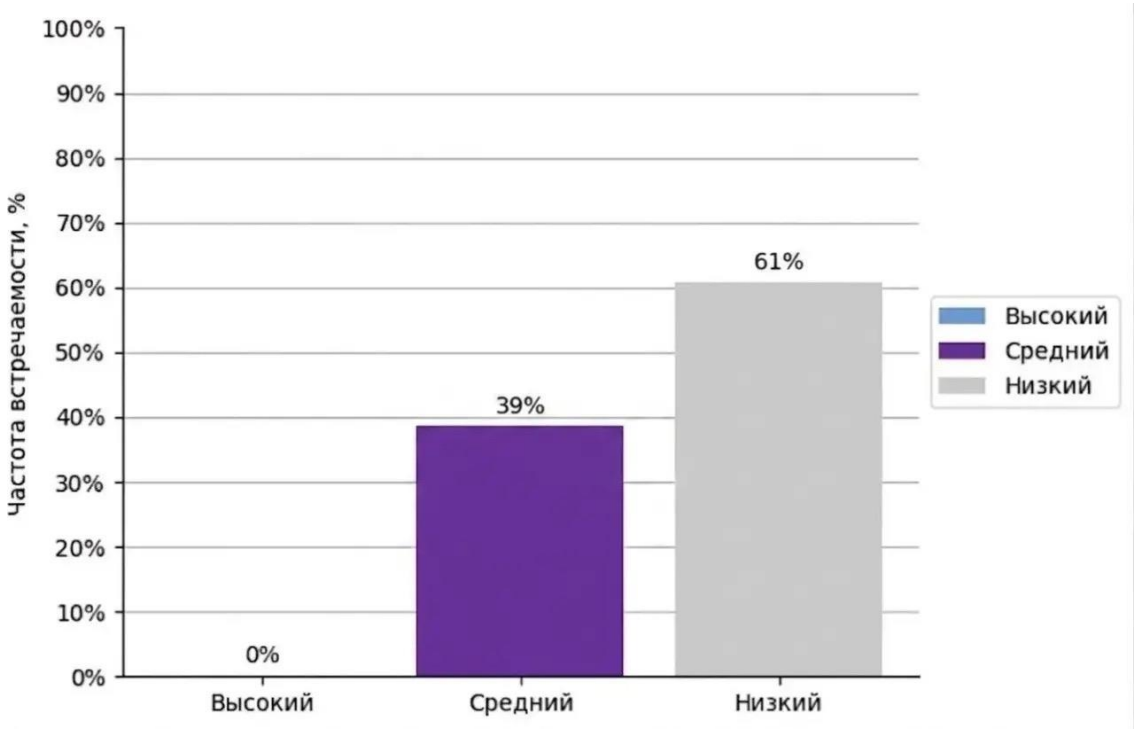



*Рис. 5. Результаты исследования актуального уровня знаний о безопасном поведении в сети Интернет у учащихся 2 класса по критерию «Информационная защита».*

Проанализировав рис. 5, мы выяснили, что уровень развития информационной защиты выглядит следующим образом:

61% учащихся находятся на низком уровне развития критерия информационной защиты. Низкий уровень (0–4 баллов, менее 50 % от максимума) указывает на отсутствие знаний о том, как следует действовать для сохранения конфиденциальности в интернете. Учащиеся данной группы считают допустимым сохранять пароли без средств защиты, сообщать коды из СМС-сообщений третьим лицам, переходить по подозрительным ссылкам, полученным от незнакомых отправителей. Их представления о приватности не сформированы, что делает их уязвимыми перед целым спектром угроз, связанных с хищением персональных данных.

39% учащихся находятся на среднем уровне развития критерия информационной защиты. Средний уровень (5–7 баллов, диапазон 50–75 % от максимума) свидетельствует о том, что базовые правила безопасного поведения учащимся известны. Они знают, что нельзя никому сообщать пароли и коды подтверждения, понимают риск, связанный с подозрительными сообщениями и ссылками. Однако их знания касаются лишь наиболее очевидных угроз. В более сложных ситуациях – например, при необходимости настройки приватности в социальных сетях или оценке угроз, связанных с использованием публичного Wi-Fi, – учащиеся могут не учесть всех факторов риска.

0% учащихся находятся на высоком уровне развития критерия информационной защиты. Высокий уровень (8–10 баллов, более 75 % от максимума) демонстрирует, что обучающиеся отлично знают правила безопасного поведения в сети Интернет. Они не только осознают, что нельзя передавать пароли и коды, но и понимают необходимость проверки источников информации, осознают ограничения, присущие публичным сетям Wi-Fi, и имеют правильное представление о том, что такое приватность и почему её необходимо сознательно оберегать. Знания носят устойчивый характер и проявляются вне зависимости от контекста предъявляемой ситуации.

При проверке работ по критерию информационной защиты было выявлено следующее: большинство учащихся продемонстрировали понимание базовых правил защиты личной информации, однако вопросы, связанные с тонкостями настроек приватности, особенностями геолокации в метаданных файлов и правилами безопасного поведения при получении подозрительных сообщений от имени знакомых, вызвали у детей заметные затруднения. Это говорит о том, что знания учащихся в области информационной защиты ещё не достигли необходимого уровня системности и требуют дальнейшего углубления.

Исходя из общего количества баллов, полученных учащимися по двум методикам, определялся общий уровень сформированности знаний о безопасном поведении в сети Интернет. Суммирование баллов производилось следующим образом: баллы, набранные учащимся по содержательному критерию (максимум

– 30 баллов), и баллы, набранные по критерию информационной защиты (максимум – 10 баллов), переводились в единую трёхуровневую шкалу. Общий уровень определялся на основании принадлежности результатов учащегося к тому или иному уровню по каждому из критериев. Если результаты учащегося по двум критериям относились к разным уровням, итоговый уровень определялся по наименьшему из них, поскольку пробелы в каком-либо одном аспекте знаний уже создают реальные риски для информационной безопасности ребёнка.

Обобщённые уровни сформированности знаний о безопасном поведении в сети Интернет представлены следующим образом:

1. Низкий уровень – у учащегося преобладают фрагментарные, бессистемные представления, он не осознаёт ценности личной информации и не идентифицирует типичные онлайн-угрозы;

2. Средний уровень – учащийся владеет базовыми правилами цифровой гигиены, однако его знания недостаточно систематизированы и проявляются преимущественно в стандартных ситуациях;

3. Высокий уровень – учащийся демонстрирует сформированную систему осознанных знаний, способен дифференцировать риски и имеет целостное представление о безопасном поведении в сети.

Полученные результаты мы отобразили на рисунке 6.

В результате проведения констатирующего эксперимента мы установили, что у учащихся 2 класса высокий уровень сформированности знаний о безопасном поведении в сети Интернет не выявлен ни в одной работе (0 %). Средний уровень наблюдается в работах, составивших 25 % по содержательному критерию и 39 % по критерию информационной защиты, что в обобщённом значении даёт примерно 32 % от общего числа учащихся – то есть лишь около трети класса обладает базовыми знаниями о правилах безопасного поведения в сети Интернет. Низкий уровень зафиксирован в работах, составивших 75 % по содержательному критерию и 61 % по критерию информационной защиты, что в обобщённом значении составляет примерно 68 % учащихся класса.

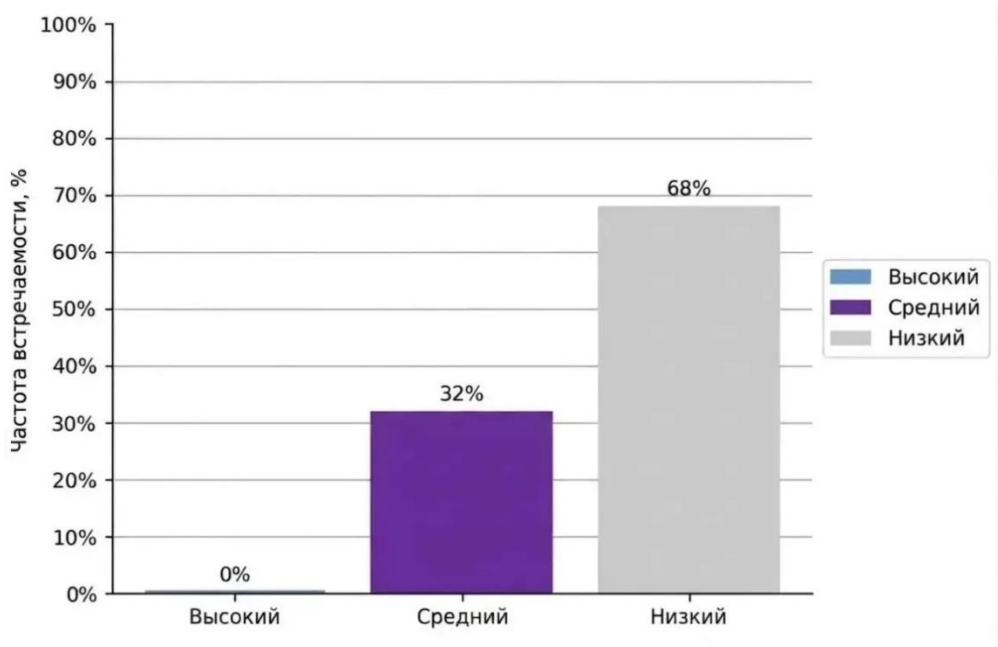



*Рис. 6. Обобщённые результаты исследования актуального уровня знаний о безопасном поведении в сети Интернет у учащихся 2 класса.*

Анализ работ, выполненных учениками 2 класса, позволил нам заметить, что преимущественно уровень знаний о безопасном поведении в сети Интернет находится на низком уровне. Учащиеся относительно успешно справляются с самыми очевидными, часто обсуждаемыми дома и в школе угрозами (например, запрет на сообщение адреса незнакомцам), но демонстрируют серьёзные пробелы в понимании более тонких механизмов защиты данных – таких как настройки приватности, геолокация в метаданных, риски синхронизации паролей с облачными сервисами.

Кроме того, отсутствие учащихся с высоким уровнем знаний по обоим критериям говорит о том, что целостной системы знаний о безопасном поведении в сети Интернет нет ни у кого из обследованных детей. Даже те учащиеся, которые показали средний уровень по одному из критериев, по другому критерию зачастую оказывались на низком уровне. Это свидетельствует о неравномерности и фрагментарности имеющихся знаний: ребёнок может, к примеру, хорошо знать, что нельзя сообщать пароль, но при этом не понимать, почему опасно использовать публичный Wi-Fi без дополнительной защиты.

Таким образом, результаты констатирующего эксперимента подтверждают актуальность выбранной нами темы и свидетельствуют о необходимости разработки и внедрения целенаправленной системы работы по формированию у младших школьников знаний о безопасном поведении в сети Интернет.

## 2.3 Разработка сайта для расширения знаний младших школьников о безопасном поведении в сети Интернет

Проведённый эксперимент позволил нам выявить уровень знаний о безопасном поведении в сети Интернет по следующим критериям: содержательный и информационной защиты. По результатам исследования выполненных работ мы можем сказать, что высокий уровень знаний не выявлен ни у одного учащегося (0 %), средний уровень наблюдается примерно у 32 % учеников, низкий уровень – примерно у 68 % учеников класса.

При анализе результатов диагностических методик мы наблюдаем следующий ряд проблем: низкий уровень знаний об особенностях сети Интернет и её рисках; низкий уровень знаний о способах защиты личной информации и сохранения конфиденциальности; фрагментарность и бессистемность имеющихся представлений, при которой даже знание отдельных правил цифровой гигиены не складывается в целостную картину безопасного поведения.

По словам Г.У. Солдатовой: «Цифровая компетентность должна формироваться не стихийно, а целенаправленно, через специально организованную образовательную среду, учитывающую возрастные особенности детей» [47]. Тем самым мы подтверждаем, что у большинства учащихся уровень знаний о безопасном поведении в сети Интернет находится на низком уровне именно по причине отсутствия систематической, специально организованной работы в данном направлении. Таким образом, мы можем выявить направления работы, в рамках которой следует проводить коррекцию актуального состояния знаний о безопасном поведении в сети Интернет у младших школьников.

По результатам констатирующего эксперимента возникла необходимость в создании образовательного сайта, направленного на расширение знаний о безопасном поведении в сети Интернет у учащихся младшего возраста.

При анализе психолого-педагогической литературы и нормативно-правовых документов мы выяснили, что на повышение уровня знаний о кибербезопасности влияет: создание ситуации успеха, интерактивные и разнообразные по форме задания, опора на игровую деятельность как ведущую в младшем школьном возрасте, а также регулярное повторение и закрепление изученного материала в новых контекстах.

Также при анализе мы выявили, что огромное влияние на формирование знаний о безопасности в интернете оказывает включение в образовательный процесс элементов геймификации: баллов, достижений, соревновательных моментов, визуальных подтверждений прогресса. Как отмечает А.В. Булдакова, «игровые механики позволяют удерживать внимание младших школьников и превращают изучение сложных правил в увлекательный процесс, что особенно важно при работе с абстрактными понятиями, такими как приватность, цифровой след или шифрование данных» [17].

Учитывая всё вышесказанное, мы предположили, что для расширения уровня знаний о безопасном поведении в сети Интернет следует разработать и внедрить в программу начальной школы образовательный сайт, состоящий из тематических модулей. Каждый модуль посвящён отдельной теме, которая вытекает из содержания диагностических тестов и охватывает ключевые аспекты кибербезопасности: личные данные и приватность, пароли и защита аккаунтов, фишинг и подозрительные ссылки, публичный Wi-Fi и безопасность соединения, кибербуллинг и безопасное общение, цифровой след и репутация в сети.

Для создания ситуации успеха каждый модуль будет содержать теоретический материал, адаптированный под возраст учащихся 1–4 классов и изложенный в доступной форме. После каждого модуля учащимся предлагается пройти квест – интерактивное испытание, которое позволяет в игровой форме проверить и закрепить полученные знания.

Для стимулирования познавательного интереса на сайте предусмотрена система достижений: за успешное прохождение квеста учащийся получает баллы и виртуальные награды (значки, отметки о завершении модуля). Накопление баллов позволяет отслеживать индивидуальный прогресс.

КиберЗащитник– это интерактивный обучающий сайт, направленный на расширение у младших школьников знаний о безопасном поведении в сети Интернет. В нем ученик становится героем виртуального мира и, проходя теоретический материал и квесты по темам интернет-безопасности, зарабатывает баллы, открывает новые уровни, соревнуется с одноклассниками и получает реальные знания о том, как защитить себя в сети.

Цель: Расширить у младших школьников знания о безопасном поведении в сети Интернет, а также о возможных онлайн-угрозах и способах их распознавания и правильного реагирования на них, сочетающими информационный и игровой подход.

Задачи:

1. Ознакомить детей с основными возможностями интернета (поиск информации, общение, обучение, игры) и потенциальными рисками (вредоносное ПО, мошенничество, кибербуллинг, утечка личных данных).

2. Представить базовые правила кибербезопасности, такие как нераспространение личной информации, проверка безопасности сайтов, использование надёжных паролей, и избегание подозрительных ссылок.

3. Обеспечить знания о важности критического мышления при работе в интернете – способность анализировать контент, различать надёжные источники и распознавать фейковые ресурсы и фишинг.

4. Ознакомить с информацией о действиях в опасных ситуациях: при столкновении с кибербуллингом, мошенничеством или подозрительными запросами.

5. Создать интерактивные форматы для закрепления знаний: квесты и игры.

Общие принципы использования:

Возрастная адаптация – контент рассчитан на детей 7–11 лет, поэтому

подача материала:

- визуальная (анимации, иконки);
- игровая (квесты, баллы, награды);
- лаконичная (короткие тексты, простые формулировки).

Модульность – каждый раздел можно использовать автономно или в связке с другими. Двусторонний доступ – отдельные блоки для детей, родителей. Гибкость форматов – подходит для фронтального, группового и индивидуального обучения.

Сайт, который мы разработали, – это прежде всего теоретическая база. Вся информация на нём – это знания, которые ребёнок должен усвоить. Но в отличие от учебника или параграфа, сайт подаёт теорию в интересном, игровом формате. Ребёнок заходит в модуль, видит яркую инфографику, короткие и понятные формулировки, проходит шаг за шагом, получает баллы и достижения. Всё это удерживает внимание и помогает запомнить даже сложные понятия. Именно этим сайт отличается от других теоретических материалов – он не просто рассказывает, он вовлекает. Баллы за прохождение модуля работают как внешняя мотивация. Достижения (звёзды, значки, уровни) дают ребёнку почувствовать себя успешным. Это чистая теория, но поданная так, что ребёнок сам хочет её освоить.

Поэтому сайт можно использовать в трёх вариантах, и все три абсолютно самостоятельны. Первый – ребёнок проходит модули дома с родителями. Это идеальный вариант, потому что тема безопасности в интернете требует доверительного разговора, и родитель выступает главным проводником. Второй – учитель даёт базовое знание на уроке, называет явление и правило. Третий – закрепление на внеурочной деятельности или классном часе в формате квеста или игры. Все три варианта не зависят друг от друга. Можно выбрать один, можно совместить любые два, можно использовать все три. Сайт – ядро с теорией, а вокруг него выстраиваются формы подачи в школе и дома.

Функциональные разделы сайта «КиберЗащитник» представлены в таблице 1.

Таблица 1 – Функциональные разделы сайта «КиберЗащитник»

| Раздел | Назначение | Ключевые функции | Целевая аудитория | Ожидаемый результат |
|---|---|---|---|---|
| 1. Главный экран | Навигация и мотивация | – Индикатор прогресса (процент пройденных модулей);<br>– кнопка «Начать обучение»;<br>– доступ к разделу достижений; | Дети, родители | Быстрый доступ ко всем функциям; визуализация прогресса. |
| 2. Обучение (основные модули) | Поэтапное освоение правил кибербезопасности | – 3 тематических блока;<br>– интерактивный квест после каждого модуля; | Дети 7–10 лет | Системное усвоение базовых знаний о правилах онлайн-безопасности. |
| 3. Квесты и проверка знаний | Оценка усвоения материала | – Итоговый квест по каждой теме из модуля. | Дети, педагоги | Объективная оценка уровня знаний. |
| 4. Личный кабинет ребёнка | Персонализация обучения | – Профиль с аватаркой;<br>– история пройденных уроков;<br>– коллекция достижений (значки, медали); | Дети | Осознание личной ответственности за безопасность; геймификация процесса |
| 5. Раздел для родителей | Поддержка взрослых в обучении детей | – Памятки по настройке родительского контроля;<br>– сценарии семейных бесед о безопасности;<br>– чек-листы для проверки устройств;<br>– рекомендации по ограничению экранного времени | Родители | Умение контролировать и поддерживать безопасное использование интернета |
| 6. Достижения и награды | Мотивация через геймификацию | – Система баллов за выполненные задания;<br>– виртуальные медали за прохождение модулей;<br>– сертификаты при завершении. | Дети | Стимулирование регулярного обучения; чувство успеха |

Интеграция в Окружающий мир (1–4 классы, УМК «Школа России»)

Окружающий мир – основной предмет для внедрения теоретических знаний с сайта. В учебниках Плешакова есть темы, которые прямо или косвенно касаются безопасности, правил поведения, устройства окружающего мира. Именно в них логично встраивать по одному модулю сайта. Времени на уроке тратится немного – от пяти до десяти минут на одном из этапов. Этого достаточно, чтобы учитель назвал явление, дал правило и связал его с темой урока.

В первом классе есть тема «Что вокруг нас может быть опасным?». На этом уроке разбираются источники опасности вокруг ребёнка: огонь, дорога, острые предметы, незнакомые люди на улице. Учитель перечисляет всё это, а затем добавляет ещё один источник – незнакомец в телефоне или планшете. Объясняет просто: ты же не будешь разговаривать на улице с чужим человеком и рассказывать ему, где ты живёшь? Вот и в телефоне делать этого нельзя. Это и есть модуль сайта 3.2 Общение с незнакомцем. Ребёнок получает знание о том, что незнакомцы бывают не только во дворе, но и в интернете, и правило поведения одинаковое: не рассказывать о себе и сразу сообщить взрослым.

Вторая тема первого класса – «Зачем нужны компьютеры?». Урок напрямую про компьютеры: что это такое, из чего состоит, что умеет делать. Здесь абсолютно логично добавить знание о вирусах. Учитель говорит: компьютер, как и человек, может заболеть. Только у него болезнь не от микробов, а от вредных программ – вирусов. Вирус маскируется под игру или красивую картинку. Ты хочешь поиграть, а на самом деле запускаешь программу, которая ломает компьютер. Это модуль 1.4 Вирусы в Интернете. Вирус – мастер маскировки. Ребёнок получает знание о существовании компьютерных вирусов и правило: ничего не открывать и не нажимать в компьютере без разрешения взрослых.

Во втором классе есть тема «Ты и твои друзья». Урок о том, как общаться, как дружить, какие правила действуют между друзьями и в классе. На этом уроке вводится понятие «личные данные». Учитель объясняет: друзьям мы можем рассказать что-то о себе, а незнакомцам – нет. В интернете ты не видишь, кто с тобой общается на самом деле. Поэтому есть вещи, которые нельзя писать никому: полное имя, домашний адрес, номер школы, телефон, фотографии семьи. Это модуль 3.1 Личные данные и приватность в социальных сетях. Ребёнок получает знание о том, что такое личные данные и почему их нужно охранять.

Вторая тема второго класса – «На воде и в лесу». Урок о правилах безопасности на природе. Разбираются скрытые опасности: красивые, но

ядовитые грибы и ягоды, незнакомый водоём с омутами, топкое болото, которое выглядит как обычная поляна. Всё это с виду безобидно, но на самом деле опасно. Учитель проводит параллель с интернетом: там тоже много интересного и полезного, но есть скрытые угрозы. Яркая реклама может вести на плохой сайт. Безобидная просьба незнакомца в игре может оказаться обманом. Это модуль 2.1 Информация в Интернете: возможности и риски. Ребёнок получает знание о том, что не всё в интернете так безопасно, как кажется на первый взгляд.

В третьем классе есть тема «Умей предупреждать болезни». Урок про защиту здоровья: закаливание, гигиена, правильное питание. В том числе говорится и о душевном здоровье: обиды и насмешки могут сделать человека больным не меньше, чем простуда. Здесь вводится понятие кибербуллинга. Учитель объясняет: в интернете тоже обижают, это называется кибербуллинг – травля в сети. Обидные слова в чате или комментариях ранят очень сильно, даже если ты не видишь обидчика в лицо. Правило: не отвечать агрессору, сделать скриншот и показать родителям или учителю. Это модуль 3.3 Агрессия в Интернете, кибербуллинг. Ребёнок получает знание о том, что травля в сети существует, это неправильно и нужно обязательно обращаться за помощью.

Вторая тема третьего класса – «Опасные места». Урок разбирает, какие места в городе считаются опасными и почему: пустырь, стройка, заброшенный дом, тёмный парк ночью. С виду это обычные места, но заходить туда нельзя. Учитель переносит этот принцип на интернет: там тоже есть опасные места – сайты с непроверенной информацией. Они выглядят обычно, но содержат ложь или обман. Ложная информация называется фейк. Чтобы не попасть в ловушку, нужно проверять: спрашивать у родителей, смотреть в книгах, сравнивать с другими источниками. Доверяй, но проверяй. Это модуль 2.2 Достоверность информации в Интернете. Доверяй, но проверяй! Надежные сайты.

В четвёртом классе специальных тем про интернет нет, но в конце учебника есть обобщающий урок «Правила безопасной жизни». На нём собираются все правила безопасности, изученные за четыре года: правила дорожного движения, поведение при пожаре, безопасность дома, на воде, в лесу.

В этот урок логично добавляется блок про безопасность в сети Интернет. Учитель говорит: вы уже знаете правила безопасности в реальном мире, но сегодня мы живём ещё и в цифровом мире, и там тоже есть свои правила. Первое – это правило про публичный Wi-Fi. Бесплатная сеть в кафе, торговом центре или транспорте – это удобно, но небезопасно. Открытая сеть – как незакрытая дверь. Через неё злоумышленник может увидеть всё, что ты вводишь на своём устройстве: пароли, переписки, данные карты родителей. Поэтому никогда нельзя вводить личные данные и пароли, если ты подключён к публичному Wi-Fi. Это модуль 1.2 Безопасное подключение. Публичный Wi-Fi.

Второе правило на том же уроке – про фишинг. Учитель объясняет: вам может прийти сообщение с незнакомой ссылкой, например, «Ты выиграл приз, перейди по ссылке» или «Твой аккаунт взломан, срочно введи пароль». Это уловка, которая называется фишинг. Слово произошло от английского fishing – рыбная ловля. Мошенник забрасывает крючок в виде заманчивой или тревожной ссылки и ждёт, пока кто-то клюнет и введёт свои данные. Внешне сайт может выглядеть как настоящий, но на самом деле это подделка. Правило: никогда не переходить по ссылкам от незнакомцев. Даже если ссылка пришла от друга, сначала нужно спросить, точно ли он её отправил, потому что его аккаунт могли взломать. Это модуль 3.4 Фишинг: кто присылает подозрительные ссылки?

На этом интеграция в Окружающий мир заканчивается. Важно подчеркнуть: на уроках даются только знания. Это не практикум, не лабораторная работа, не отработка навыков. Учитель объясняет явление и правило. Ребёнок запоминает. А дальше – может пройти модуль сайта дома с родителями и получить баллы, чтобы закрепить пройденный материал.

Русский язык и Литературное чтение

Здесь подход другой. Русский язык в начальной школе не предназначен для того, чтобы впервые знакомить детей с безопасностью в интернете. Но он отлично подходит для того, чтобы уже полученное знание закрепить. Ребёнок что-то узнал на Окружающем мире или дома через сайт, а на уроке русского языка он это повторяет через письменную или устную работу. Это называется

пропедевтика – подготовка к более сложным формам работы в средней школе. Но база для этого закладывается в начальной школе, когда ребёнок учится работать с простыми текстами-правилами, списывать их, составлять из них предложения, писать короткие рассуждения.

Во втором классе на уроках русского языка дети учатся списывать текст с доски без ошибок. Вместо не связанных между собой предложений можно дать списать два-три предложения, которые одновременно являются правилами безопасности. Например: «Я не называю свой адрес незнакомцам в интернете. Я всегда спрашиваю разрешения у родителей». Ребёнок тренирует навык списывания и одновременно повторяет правило из модуля 3.1 Личные данные и приватность в социальных сетях, которое он уже узнал на Окружающем мире.

В третьем классе дети учатся составлять предложения из разрозненных слов. Даётся набор слов, из которых нужно собрать инструкцию. Слова могут быть такими: «Не отвечай», «сделай скриншот», «расскажи взрослым», «агрессору». Ребёнок собирает правильный порядок и получает алгоритм действий при кибербуллинге. Это повторение модуля 3.3 Агрессия в Интернете, кибербуллинг через работу с языком.

В четвёртом классе дети знакомятся с текстом-рассуждением. Можно дать задание написать короткий текст из трёх-четырёх предложений на тему «Почему нельзя переходить по ссылкам от незнакомцев». Ребёнок формулирует мысль, подбирает аргументы. Здесь работает модуль 3.4 Фишинг: кто присылает подозрительные ссылки, который до этого был изучен на итоговом уроке Окружающего мира.

В первом классе русский язык не задействуется. В этот период дети только осваивают написание букв, многие ещё читают с трудом. Им рано работать с текстами. Но во втором, третьем и четвёртом классах русский язык становится хорошим инструментом для повторения и закрепления знаний через письменную речь.

Математика

С математикой в начальной школе ситуация похожая, поэтому она может использоваться минимально – тоже как элемент пропедевтики.

В четвёртом классе дети работают с таблицами как формой представления информации. Можно дать задание заполнить таблицу: в одном столбце перечислить опасные ситуации в интернете, а в другом – соответствующие правила безопасности.

ОРКСЭ (Основы религиозных культур и светской этики, 4 класс)

ОРКСЭ – это предмет, где обсуждаются этические вопросы: как правильно поступать, что такое хорошо и плохо, как строить отношения с людьми. Здесь темы безопасности в интернете ложатся абсолютно естественно, потому что цифровой мир – это среда, где тоже действуют нравственные нормы.

В теме «Правила общения для всех» уместно обсуждение того, что правила вежливости и осторожности едины для реального мира и для интернета. Не разговаривать с незнакомцами, не грубить, не раскрывать личную информацию – всё это относится и к общению в сети. Это модуль 3.2 Общение с незнакомцем.

В теме «Мой класс – мои друзья» разбирается ситуация кибербуллинга. Обсуждается вопрос: как поддержать друга, если его обижают в общем чате класса? Важно подчеркнуть, что молчание наблюдателей – это тоже форма поддержки агрессора. На этом уроке можно создать «Кодекс безопасного поведения класса», куда войдут правила общения в интернете. Это модуль 3.3 Агрессия в Интернете, кибербуллинг.

В теме «Достойно жить среди людей» говорится об уважении к личным границам. Обсуждается, что у каждого есть право на личное пространство и личную информацию. Публиковать чужие фотографии без спроса, читать чужие переписки, передавать личные данные третьим лицам – это нарушение границ. Это модуль 3.1 Личные данные и приватность в социальных сетях.

В теме «Простые школьные и домашние правила этикета» можно обсудить этикет в интернете. В частности, правило не пересылать непроверенную информацию, не пугать друзей фейковыми новостями, не распространять слухи.

Это модуль 2.2 Достоверность информации в Интернете. Доверяй, но проверяй! Надежные сайты.

ОРКСЭ не даёт технических навыков, но формирует отношение. Ребёнок понимает: безопасное поведение в интернете – это не только вопрос защиты от вирусов, но и вопрос нравственного выбора.

Внеурочная деятельность и классные часы

Это завершающий элемент модели. Здесь нет привязки к конкретному учебному предмету или теме. Классный час или занятие внеурочной деятельности – это время, когда можно собрать воедино все модули сайта и дать детям прожить их в неформальной, игровой обстановке. Именно здесь теоретические знания с сайта закрепляются через квесты, игры, командные задания.

Квест можно пройти и без предварительного изучения модулей, потому что правила объясняются на каждой станции коротко. Но если ребёнок уже прошёл модуль сайта дома или получил знание на уроке Окружающего мира, то квест становится именно закреплением – он вспоминает то, что уже знает, и применяет в игре.

Эффект от внеурочной деятельности двойной. Во-первых, закрепляются знания в весёлой, нешкольной обстановке. Во-вторых, на квест можно пригласить родителей, и тогда тема безопасности в интернете переходит из школы в семью. Родители проходят станции вместе с детьми, обсуждают правила, и после квеста им проще продолжить разговор дома – например, открыть сайт и пройти модули ещё раз вместе.

Сайт с модулями безопасности – это теоретическая основа, поданная в увлекательной форме с баллами и достижениями. Именно это отличает его от обычного учебного текста. Вокруг сайта выстраивается система интеграции в учебный процесс начальной школы. Окружающий мир берёт на себя задачу первого знакомства с понятиями – учитель на подходящей теме урока за несколько минут даёт знание и правило. Русский язык и математика работают

как инструменты повторения и закрепления через письменную речь и работу с числами и таблицами, закладывая основы для более сложной аналитической работы в средней школе. ОРКСЭ добавляет этическое измерение – формирует отношение к цифровым угрозам как к нравственной проблеме. Внеурочная деятельность замыкает систему, позволяя ребёнку в игре и вместе с родителями прожить все полученные знания.

Методические приёмы для повышения эффективности:

Фронтальная работа:

1. Прохождение теории с последующим обсуждением;

2. коллективное решение квестов на интерактивной доске;

3. «мозговой штурм» по теме «Что такое персональные данные?».

Групповая работа:

1. создание плакатов «Правила безопасности в сети Интернет»;

2. разбор кейсов (например, «Как поступить, если друг просит пароль?»).

Индивидуальная работа:

1. прохождение квестов с автоматической проверкой;

Проектная деятельность:

1. создание памятки «5 правил безопасного общения» для младших классов;

2. исследование «Какие угрозы встречаются в моей любимой социальной сети?».

Обратная связь и рефлексия:

– обсуждение в кругу: «Что нового я узнал?», «Как я могу применить это завтра?»;

– награждение сертификатами за прохождение модулей.

Примечание:

1. Все разделы адаптированы под мобильные устройства и ПК.

2. Интерфейс содержит крупные кнопки, минимум текста, яркие иконки для детей 7–10 лет.

Таким образом, сайт способствует формированию у детей знаний о безопасном поведении в Интернете:

– для детей – через игровые материалы, визуальные объяснения и практические примеры;

– для взрослых – через инструкции, сценарии и рекомендации по контролю.

## Выводы по II главе

Вторая глава посвящена описанию констатирующего эксперимента, проведение которого позволило нам сделать вывод об актуальном уровне знаний младших школьников о безопасном поведении в сети Интернет.

Для проведения экспериментального исследования, руководствуясь теоретической моделью цифровой компетентности Г. У. Солдатовой и Е. И. Рассказовой, а также требованиями ФГОС НОО, нами были выделены два критерия оценки: содержательный и критерий информационной защиты. В соответствии с этими критериями была составлена диагностическая программа, включающая тест по кибербезопасности (30 вопросов) и тест «Работа с персональными данными» (10 вопросов). Исследование проводилось на базе МБОУ Лицей № 8 г. Красноярска среди 28 учащихся 2 «А» класса.

На основе полученных данных мы можем сказать следующее: по содержательному критерию низкий уровень знаний об особенностях сети Интернет и её рисках продемонстрировали 75 % учащихся, средний – 25 %, высокий уровень не выявлен ни у одного ученика (0 %). По критерию информационной защиты низкий уровень зафиксирован у 61 % учащихся, средний – у 39 %, высокий уровень вновь не обнаружен (0 %).

В результате обобщения данных мы установили, что ни один учащийся класса не обладает высоким уровнем знаний о безопасном поведении в сети Интернет. Примерно у 32 % учеников наблюдается средний уровень, а у 68 % –

низкий. Следовательно, можно сделать вывод о том, что наша гипотеза оказалась верна: знания младших школьников о безопасном поведении в сети сформированы преимущественно на низком уровне. Данные результаты позволяют понять, что у учащихся наблюдается фрагментарность и бессистемность имеющихся представлений, в особенности это касается понимания механизмов защиты персональных данных, правил использования публичного Wi-Fi и распознавания фишинговых атак.

Одним из способов решения этой проблемы может стать внедрение в образовательный процесс начальной школы разработанного нами сайта «КиберЗащитник», поскольку его содержание, построенное на принципах геймификации и наглядности, позволит системно формировать у учащихся знания о группах интернет-рисков и способах их предотвращения, а также восполнит выявленный в ходе анализа УМК «Школа России» дефицит дидактических материалов по данной теме.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы была изучена психолого-педагогическая и методическая литература, была обозначена суть понятия «безопасное поведение в сети Интернет» и его структурные компоненты: содержательный и компонент информационной защиты. Также были изучены и описаны психовозрастные особенности младшего школьника и особенности расширения знаний о безопасном поведении в сети Интернет у обучающихся начальной школы.

На основании проведенного анализа УМК «Школа России» и соответствующих методических разработок было установлено, что тема безопасного поведения в сети Интернет в учебниках «Окружающий мир» с 1 по 4 класс представлена фрагментарно и бессистемно. Материал ограничивается единственным информационным абзацем в учебнике 4 класса о правилах безопасного поиска информации, который не сопровождается вопросами или заданиями. Проанализировав программы внеурочной деятельности данного УМК, мы выяснили, что тематика безопасного поведения в сети Интернет, защиты персональных данных и распознавания интернет-мошенничества в них полностью отсутствует на протяжении всех четырех лет обучения. Нами также были проанализированы другие разработки по данному вопросу. Мы можем сделать вывод, что современного дидактического материала, который направлен на формирование знаний о безопасном поведении в сети Интернет, представлено в ограниченном количестве. Это позволило нам прийти к выводу, что проблема формирования знаний о безопасном поведении младших школьников в сети Интернет актуальна и требует дальнейшего исследования.

В ходе исследования нами был проведен констатирующий эксперимент, в процессе проведения которого был определен актуальный уровень знаний о безопасном поведении в сети Интернет у младших школьников (обучающиеся 2 класса). Основными критериями оценки являлись: содержательный и критерий информационной защиты.

Констатирующий эксперимент проводился на базе муниципального бюджетного общеобразовательного учреждения МБОУ Лицей № 8 г. Красноярска. В исследовании приняли участие обучающиеся второго класса в количестве 28 человек.

В ходе эксперимента обучающиеся выполняли задания по выделенным нами критериям. Для определения уровня по содержательному критерию была использована методика «Тест по кибербезопасности» (автор-составитель Булдакова Анна Васильевна). На основе данной методики мы оценивали понимание учащимися особенностей сети Интернет, знаний её рисков, правил защиты данных, распознавания угроз и мошеннических действий. Для определения уровня по критерию информационной защиты был использован тест «Работа с персональными данными», рекомендованный Роскомнадзором. Обе методики проводились в форме тестирования.

На констатирующем этапе эксперимента мы установили, что по содержательному критерию 75 % обучающихся находятся на низком уровне,25 % – на среднем, высокий уровень не выявлен ни у одного ученика. По критерию информационной защиты 61 % обучающихся показали низкий уровень, 39 % – средний, высокий уровень также не зафиксирован. В результате обобщения данных было установлено, что ни один учащийся не обладает высоким уровнем знаний о безопасном поведении в сети Интернет, примерно у 32 % учащихся наблюдается средний уровень, а у большинства (68 %) – низкий уровень. Данные исследования представлены в виде таблиц и диаграмм.

В ходе анализа данных эксперимента было выявлено, что у большинства младших школьников преобладают низкие показатели знаний о безопасном поведении в сети Интернет. Учащиеся особенно затрудняются в понимании таких аспектов, как фишинг, правила использования публичного Wi-Fi, настройки приватности и цифровой след. Наша гипотеза оказалась верна.

На основании результатов констатирующего эксперимента и анализа методической литературы мы разработали образовательный сайт «КиберЗащитник», который направлен на расширение знаний о безопасном

поведении в сети Интернет. Данный сайт содержит тематические модули, охватывающие ключевые аспекты кибербезопасности: личные и приватность, пароли и защита аккаунтов, фишинг и подозрительные ссылки, публичный Wi-Fi, кибербуллинг, цифровой след. Теоретический материал изложен в доступной для младших школьников форме с использованием визуальных образов. Для закрепления знаний после каждого модуля предусмотрен интерактивный квест, а система достижений (баллы и награды) стимулирует познавательный интерес учащихся.

Использовать материалы сайта можно как в учебной деятельности во время уроков «Окружающий мир», русского языка, математики и ОРКСЭ, так и во внеурочной деятельности и классных часах. Предполагаем, что данное практическое пособие будет способствовать изменению уровня сформированности знаний о безопасном поведении в сети Интернет у младших школьников.

# СПИСОК ЛИТЕРАТУРЫ

1. Федеральный государственный образовательный стандарт начального общего образования: утвержден приказом Министерства просвещения Российской Федерации от 31.05.2021 № 286 (зарегистрировано в Минюсте России 05.07.2021 № 64100). – Текст: электронный // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 15.04.2026).

2. Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 286 «Об утверждении федерального государственного образовательного стандарта начального общего образования» (зарегистрировано в Минюсте России 05.07.2021 № 64100) // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 15.04.2026).

3. Российская Федерация. Законы. О защите детей от информации, причиняющей вред их здоровью и развитию : Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. – 2010. – № 52 (ч. I). – Ст. 7000.

4. Российская Федерация. Законы. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) // Российская газета. – 2006. – 1 августа (№ 165).

5. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.12.2021 № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021–2027 годы» // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 15.04.2026).

6. Распоряжение Правительства Российской Федерации от 02.12.2015 № 2471-р «Об утверждении Концепции информационной безопасности детей» // Собрание законодательства РФ. – 2015. – № 49. – Ст. 7055.

7. Методические рекомендации Министерства просвещения Российской Федерации по обеспечению оптимального и безопасного доступа к

информационным системам и сети Интернет в образовательных организациях. – М., 2025. – 48 с.

8. Айкен, М. Кибербезопасность для детей: как защитить ребёнка в цифровом мире / М. Айкен; пер. с англ. Т. О. Новиковой. – М.: Эксмо, 2020. – 256 с.

9. Арсентьев, М. В. К вопросу о понятии «информационная безопасность» в современной науке / М. В. Арсентьев // Информационное общество. – 2019. – № 6. – С. 45–52.

10. Асмолов, А. Г. Социокультурная модернизация образования: личностный подход / А. Г. Асмолов. – М.: ФИРО, 2018. – 256 с.

11. Баева, И. А. Психологическая безопасность в образовании: монография / И. А. Баева. – СПб: СОЮЗ, 2002. – 271 с.

12. Баришполец, В. А. Информационно-психологическая безопасность: основные положения / В. А. Баришполец // Безопасность Евразии. – 2013. – № 1. – С. 45–58.

13. Беляева, А. Б. Методические рекомендации для родителей по профилактике интернет-рисков у детей / А. Б. Беляева, А. Н. Карасев, Е. А. Никонова // Образование и наука. – 2020. – № 8. – С. 92–108.

14. Бененсон, Е. П. Информатика. 2 класс: учебное пособие / Е. П. Бененсон, А. Г. Паутова. – М.: Академкнига/Учебник, 2015. – 128 с.

15. Беспалько, В. П. Слагаемые педагогической технологии / В. П. Беспалько. – М.: Педагогика, 1989. – 192 с.

16. Болотова, Л. Р. Игровые технологии как средство формирования информационной культуры младших школьников / Л. Р. Болотова, О. Н. Евсеева // Начальная школа. – 2020. – № 4. – С. 25–29.

17. Булдакова, А. В.Тест по кибербезопасности для младших школьников / А. В. Булдакова // Педагогическая копилка. – 2022. – № 5. – С. 12–16.

18. Бунеева, Е. В. Концепция начального языкового и литературного образования / Е. В. Бунеева, О. В. Чиндилова. – М.: Баласс, 2014. – 144 с.

19. Виноградова, Н. Ф. «Окружающий мир» в начальной школе: методические рекомендации / Н. Ф. Виноградова. – М.: Вентана-Граф, 2019. – 192 с.

20. Водопьянова, Н. А. Информационная безопасность личности в цифровой среде / Н. А. Водопьянова // Психология и педагогика. – 2021. – № 3. – С. 34–41.

21. Войскунский, А. Е. Психология и интернет: монография / А. Е. Войскунский. – М.: Акрополь, 2010. – 439 с.

22. Волков, Б. С. Психология младшего школьника / Б. С. Волков. – М.: Академический проект, 2020. – 208 с.

23. Воронов, Д. В. Геймификация в профилактике интернет-рисков / Д. В. Воронов, Е. В. Кубанова // Информационная безопасность: вчера, сегодня, завтра. – 2021. – № 2. – С. 45–53.

24. Выготский, Л. С. Мышление и речь / Л. С. Выготский. – М.: Национальное образование, 2016. – 368 с.

25. Гиппенрейтер, Ю. Б. Общаться с ребенком. Как? / Ю. Б. Гиппенрейтер. – М.: АСТ, 2018. – 304 с.

26. Грачев, Г. В. Информационная безопасность личности: теория и методология / Г. В. Грачев. – М.: Академия, 2015. – 240 с.

27. Григорьев, Д. В. Внеурочная деятельность школьников: методический конструктор / Д. В. Григорьев. – М.: Просвещение, 2020. – 223 с.

28. Даль, В. И. Толковый словарь живого великорусского языка: в 4 т. / В. И. Даль. – М.: Русский язык, 1989. – Т. 1. – 699 с.

29. Занков, Л. В. Избранные педагогические труды / Л. В. Занков. – М.: Педагогика, 1990. – 424 с.

30. Киселева, Е. Н. Дидактические игры в обучении школьников основам кибербезопасности / Е. Н. Киселева, Ю. Д. Бабаева. – М.: ВЛАДОС, 2019. – 128 с.

31. Краснова, Г. В. Информационная безопасность в образовании: практическое пособие / Г. В. Краснова, А. А. Марков. – М.: Флинта, 2020. – 188 с.

32. Крышалович, В. Г. Проектная деятельность как средство формирования безопасного поведения в сети Интернет / В. Г. Крышалович, О. Л. Борисюк // Информатика и образование. – 2021. – № 7. – С. 34–42.

33. Кузнецова, М. И. Основы информационной грамотности младших школьников / М. И. Кузнецова // Начальное образование. – 2020. – № 3. – С. 12–18.

34. Макарова, Л. Н. Рефлексивные технологии в начальной школе / Л. Н. Макарова // Педагогические исследования. – 2021. – № 2. – С. 56–63.

35. Мартишин, Н. И. Задания на развитие когнитивного компонента безопасного поведения в сети / Н. И. Мартишин // Начальная школа. – 2021. – № 11. – С. 24–28.

36. Михнев, И. П. Мобильный интернет и безопасность школьников / И. П. Михнев, И. Морев // Педагогическое обозрение. – 2020. – № 5. – С. 67–73.

37. Мяэотс, О. Н. Создание целостной системы работы по формированию безопасного поведения в школе / О. Н. Мяэотс // Педагогическое образование и наука. – 2020. – № 3. – С. 34–39.

38. Нестик, Т. А. Отношение к угрозам информационной безопасности у детей и подростков / Т. А. Нестик // Психологические исследования. – 2018. – Т. 11, № 61. – С. 8–19.

39. Ожегов, С. И. Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений / С. И. Ожегов. – 3-е изд., стереотип. – М.: Мир и Образование, 2015. – 1375 с.

40. Переломова, Н. А. Проблемы информационной безопасности школьника / Н. А. Переломова. – М.: НИЦ «Инфра-М», 2019. – 208 с.

41. Пиаже, Ж. Психология интеллекта / Ж. Пиаже; пер. с фр. А. М. Пятигорского. – М.: АСТ, 2021. – 288 с.

42. Плешаков, А. А. Окружающий мир. 1–4 классы: учебники в 2 ч. / А. А. Плешаков, М. Ю. Новицкая, Е. А. Крючкова. – М.: Просвещение, 2023. – 120 с.

43. Прихожан, А. М. Информационная безопасность и развитие информационной культуры личности / А. М. Прихожан // Мир психологии. – 2010. – № 4. – С. 135–141.

44. Ребикова, Ю. В. Дидактические игры в формировании безопасного поведения младших школьников / Ю. В. Ребикова, Л. М. Бронникова // Начальная школа плюс До и После. – 2021. – № 6. – С. 14–18.

45. Рыдзе, О. А. Формирование функциональной грамотности в начальной школе / О. А. Рыдзе. – М.: Просвещение, 2021. – 160 с.

46. Солдатова, Г. У. Цифровая компетентность и безопасность детей в интернете / Г. У. Солдатова, Е. И. Рассказова // Психологические исследования. – 2013. – Т. 6, № 27. – С. 3–15.

47. Солдатова, Г. У. Цифровая социализация в культурно-исторической парадигме: изменяющийся ребенок в изменяющемся мире / Г. У. Солдатова // Социальная психология и общество. – 2018. – Т. 9, № 3. – С. 71–80.

48. Степанов, П. В. Воспитание в современной школе: теория и практика / П. В. Степанов. – М.: Педагогический поиск, 2020. – 224 с.

49. Стеркина, Р. Б. Безопасность жизнедеятельности: учебник для начальной школы / Р. Б. Стеркина. – М.: Просвещение, 1998. – 127 с.

50. Сущинская, Т. Н. Кейс-задачи и алгоритмы как средства формирования безопасного поведения / Т. Н. Сущинская, А. А. Федоров // Начальное образование. – 2020. – № 5. – С. 30–35.

51. Ушаков, Д. Н. Толковый словарь русского языка: в 4 т. / Д. Н. Ушаков; под ред. Б. М. Волина. – М.: Астрель, 2005. – Т. 1. – 848 с.

52. Федоров, А. В. Медиаобразование и информационная безопасность школьников / А. В. Федоров. – М.: Флинта, 2021. – 160 с.

53. Харчевникова, Е. Л. Педагогические условия сформированности безопасного поведения младших школьников в сети Интернет / Е. Л. Харчевникова // Образование и наука. – 2021. – № 1. – С. 55–62.

54. Цукерман, Г. А. Психолого-педагогические особенности младших школьников / Г. А. Цукерман. – М.: Просвещение, 2019. – 224 с.

55. Челышева, И. В. Кибербезопасность школьников в интернет-пространстве и проблемы семейного медиаобразования / И. В. Челышева // Crede Experto: транспорт, общество, образование, язык. – 2016. – № 4. – С. 45–55.

56. Черенцова, Л. А. Взаимодействие школы и семьи в формировании гуманистической направленности личности младшего школьника: дис. канд. пед. наук: 13.00.01 / Черенцова Лариса Александровна. – М., 2002. – 174 с.

57. Эльконин, Д. Б. Детская психология: учебное пособие / Д. Б. Эльконин. – 5-е изд., стереотип. – М.: Академия, 2011. – 384 с.

Приложение А

Тест на Содержательный критерий, Методика №1

(Булдакова Анна Васильевна)

Дорогой ученик!

Перед тобой тест из 30 вопросов. Все сделано для того, чтобы ты смог показать, что знаешь. Читай внимательно каждый вопрос и выбирай один правильный ответ. Успехов!

**1. Что значит «красный замок» в браузере?**

· Подключение к сайту не защищено, данные могут перехватить

· Сайт требует особого разрешения для входа

· Сайт временно недоступен из-за проблем с безопасностью

· Сайт использует устаревший дизайн, который браузер не поддерживает

· Браузер предупреждает, что на сайте много рекламы

**2. Что из этого – личные данные?**

· То, что помогает узнать конкретного человека

· То, что человек любит делать в свободное время

· То, что человек выбирает для развлечения

· То, что человек часто упоминает в переписке

· То, что человек публикует в своём профиле чаще всего

**3. Что можно выкладывать в интернет открыто?**

· Информацию, по которой сложно определить автора

· Контакты, если они нужны для общения

· Данные, которые не жалко показать всем

· То, что уже публиковали другие пользователи

· То, что не запрещено правилами конкретной платформы

**4. Почему нельзя писать свой адрес?**

· Чужие люди могут найти, где ты живёшь

· Адрес сложно проверить на правдивость

· Его могут случайно использовать не по назначению

· Адрес может измениться, и информация устареет

**5. Какой пароль лучше?**

· Тот, который сочетает разные типы символов

· Тот, который легко запомнить и быстро ввести

· Тот, который связан с важными датами

· Тот, который ты используешь только на одном устройстве

· Тот, который ты меняешь часто

**6. Почему плохо использовать один пароль везде?**

· При утечке одного пароля под угрозой все аккаунты

· Пароли могут перестать подходить после обновлений

· Сложно отслеживать, где какой пароль использовался

· Одинаковые пароли занимают больше места в памяти браузера

· Браузеры могут автоматически заменять одинаковые пароли на разные

**7. Что такое фишинг?**

· Способ выманить личную информацию через поддельные сообщения

· Вид рекламы, который появляется в неожиданных местах

· Ошибка, из-за которой сайт работает неправильно

· Метод быстрого поиска информации в нескольких источниках

· Система автоматической проверки подлинности сайтов

**8. Почему нельзя нажимать на странные ссылки?**

· Они могут перенаправить на сайт, который крадёт данные

· Они могут замедлить работу устройства

· Они могут не соответствовать тому, что обещали

· Они могут открыть сайт на иностранном языке

· Они могут активировать режим экономии трафика на устройстве

**9. Что такое публичный Wi-Fi?**

· Сеть, к которой может подключиться любой человек

· Интернет, который работает без пароля дома

· Личное подключение, которое раздаёт телефон

· Сеть, которую предоставляет государство для бесплатного доступа

· Сеть с повышенной скоростью для всех пользователей

**10. Чем он может быть опасен?**

· Через такую сеть злоумышленники могут получить доступ к твоим данным

· В публичных сетях чаще случаются сбои связи

· Подключение к такой сети требует дополнительных настроек

· Публичный Wi-Fi быстрее расходует заряд батареи устройства

· Публичный Wi-Fi автоматически удаляет историю просмотров

**11. Что такое кибербуллинг?**

· Систематические оскорбления и давление через интернет

· Споры и разногласия в онлайн-играх

· Обычное общение с элементами критики

· Автоматическая блокировка пользователей за нарушение правил

· Официальное предупреждение от администрации платформы

**12. Что значит «защита личных данных»?**

· Ограничение доступа посторонних к твоей информации

· Полное удаление всей истории действий в сети

· Публикация данных только для проверенных людей

· Регулярная смена паролей и никнеймов в аккаунтах

· Публикация данных только в закрытых группах по интересам

**13. Почему не стоит отправлять фото незнакомым?**

· Получатель может использовать изображение без твоего согласия

· Фотографии занимают место в памяти устройства

· Не все люди умеют правильно оценивать чужие фото

· Фотографии низкого качества могут испортить репутацию отправителя

· Фотографии могут не открыться у получателя из-за формата

**14. Кто такие интернет-мошенники?**

· Люди, которые обманом получают деньги или данные

· Игроки, которые ищут преимущества в онлайн-играх

· Администраторы, которые удаляют подозрительные аккаунты

· Пользователи, которые часто меняют никнеймы в играх

**15. Что лучше сделать с письмом от незнакомого человека?**

· Внимательно проверить отправителя и не переходить по ссылкам

· Написать ответ, чтобы узнать цели обращения

· Сразу удалить письмо, не читая содержания

· Переслать письмо другу, чтобы он помог оценить его содержание

· Сохранить письмо в отдельной папке для будущего анализа

**16. Что значит «https» у сайта?**

· Передача данных между тобой и сайтом зашифрована

· Сайт загружается быстрее обычного

· Доступ к сайту не требует оплаты

· Сайт прошел официальную регистрацию в государственном реестре

· Сайт автоматически переводит текст на твой язык

**17. Что нельзя писать в игре незнакомым?**

· Информацию, которая помогает найти тебя в реальной жизни

· Никнейм, который ты используешь в играх

· Предпочтения по жанрам игр

· Стратегию прохождения сложного уровня

· Секретные коды, которые ты нашёл в интернете

**18. Зачем нужен антивирус?**

· Чтобы вовремя обнаруживать и блокировать вредоносные программы

· Чтобы ускорить запуск игр и приложений

· Чтобы автоматически сортировать файлы на устройстве

· Чтобы создавать резервные копии важных документов

· Чтобы автоматически обновлять все приложения на устройстве

**19. Что такое «цифровой след»?**

· Совокупность всех действий, которые ты оставляешь в интернете

· Список установленных и удаленных приложений

· Отпечаток пальца для разблокировки смартфона

· История поиска, которую можно очистить в настройках

**20. Почему важно думать перед тем, как что-то выложить?**

· Опубликованное может сохраниться в сети надолго и стать доступным многим

· Контент может не понравиться друзьям и подписчикам

· Публикация требует времени на подготовку и оформление

· Посты с большим количеством лайков привлекают внимание мошенников

· Публикация в неподходящее время снижает количество просмотров

**21. Почему нельзя вводить данные карты на незнакомом сайте?**

· Злоумышленники могут скопировать данные и потратить деньги

· Платежная система может временно не работать и деньги не вернут на счёт

· Сайт может не подтвердить успешность операции

· Данные карты могут не подойти для иностранной валюты

· Сайт может потребовать подтверждение через СМС, которое придет с задержкой

**22. Как безопаснее платить в интернете?**

· Совершать покупки только на проверенных ресурсах и с согласия взрослых

· Выбирать самый удобный способ оплаты без дополнительных проверок

· Платить сразу, чтобы не упустить выгодное предложение

· Использовать карту с минимальным балансом для любых покупок

· Платить только в приложениях, которые скачаны из официального магазина

**23. Почему нельзя тратить деньги в игре без разрешения?**

· Внутриигровые покупки списывают реальные деньги с карты

· Игра может потерять прогресс после покупки

· Виртуальные предметы быстро теряют свою ценность

· Покупки в игре могут конфликтовать с обновлениями

· Игра может временно заблокировать аккаунт после крупной покупки

**24. Какой аватар безопаснее?**

· Изображение, которое не раскрывает информацию о тебе

· Фотография, сделанная в знакомом месте

· Картинка, которая нравится большинству друзей

**25. Чем опасны фото с геолокацией?**

· По меткам на фото можно определить твоё местоположение

· Такие фотографии занимают больше места в памяти

· Геолокация может исказить цвета на снимке

· Фото с геолокацией сложнее отредактировать в фоторедакторе

· Фото с геолокацией автоматически публикуются в открытых альбомах и тебя могут заметить знакомые или родители

**26. Что может быть, если выкладывать много личных фото?**

· Кто-то может скачать и использовать их в своих целях

· Фотографии автоматически удалятся через время

· Аккаунт станет более популярным среди незнакомцев

· Большое количество фото может замедлить загрузку профиля

· Фотографии могут быть использованы в искусственном интеллекте

**27. Почему нельзя идти на встречу с интернет-другом одному?**

· Человек в реальности может оказаться не тем, за кого себя выдавал

· Встреча может потребовать дополнительных расходов

· Добираться до места встречи может быть неудобно

· Первая встреча всегда проходит в людном месте, где сложно говорить

· На встрече может не быть бесплатного интернета для связи, и ты не сможешь связаться с родителями

**28. Что важно помнить про людей в интернете?**

· Пользователь может представляться не тем, кто он есть на самом деле

· Все участники общения проходят обязательную проверку

· Люди в сети всегда пишут только правду о себе

· Никнеймы в интернете регистрируются на одного человека

· Пользователи с большим количеством подписчиков всегда честны

**29. Почему информации о человеке в интернете нельзя всегда верить?**

· Данные в профиле легко изменить или выдумать полностью

· Информация в интернете обычно слишком краткая

· Информация в интернете быстро устаревает из-за обновлений

**30. Что может быть опасным в общении?**

· Просьбы поделиться личной информацией или договориться о встрече ✓

· Обсуждение общих интересов, таких как фильмы или музыка

· Длительная переписка на разные темы, в том числе, о секретах

· Использование смайликов и сокращений в сообщениях, можно не так понять собеседника

Приложение Б

Тест на критерий Информационной защиты, Методика №2 (Роскомнадзор)

Дорогой ученик!

Перед тобой тест из 10 вопросов. Все сделано для того, чтобы ты смог показать, что знаешь. Читай внимательно каждый вопрос и выбирай один правильный ответ. Успехов!

**1. Браузер предлагает сохранить пароль от почты. Как поступить?**

A) Отказаться, так как синхронизация с облаком создаёт риск утечки при взломе аккаунта браузера

B) Сохранить, но только если включена двухфакторная аутентификация в браузере и установлен мастер-пароль

D) Записать пароль в текстовый файл на рабочем столе с именем «notes.txt», чтобы не доверять браузеру

**2. На сайте есть замочек и HTTPS. Можно ли вводить данные карты?**

A) Да, HTTPS гарантирует, что сайт легальный и проверен

B) Нет, HTTPS лишь шифрует трафик, но не подтверждает легитимность владельца сайта

**3. Звонят из «службы безопасности» и требуют код из СМС для отмены операции по списанию денег, которые вы не производили, ваши действия?**

A) Не называть код, положить трубку, попросить родителей перезвонить в банк по номеру с официальной карты

B) Назвать код, но сразу после звонка заблокировать карту и попросить родителей выпустить новую

C) Не называть код, но перейти по ссылке, которую продиктуют, чтобы проверить операцию

D) Назвать последние 4 цифры кода, этого достаточно для «подтверждения личности»

**4. Выкладываешь фото рядом с парком у кафе в котором часто проводишь время. Что опаснее?**

A) Встроенная геолокация кафе в метаданных файла.

B) Визуальные маркеры: вывеска кафе, номер дома, уникальная архитектура

C) Время публикации фото

**5. Ты в кафе с публичным Wi-Fi. Включил инкогнито. Что это даёт?**

A) Полную анонимность: провайдер не увидит сайты

B) Защиту только на устройстве: история не сохранится локально, но трафик виден в сети

C) Защиту от вирусов

**6. Телефон предлагает обновиться. Когда соглашаться?**

A) Только если в описании указано «исправление уязвимостей безопасности»

B) Всегда сразу, так как любые обновления включают патчи безопасности

C) Через неделю, чтобы другие пользователи проверили стабильность

D) Только при подключении к Wi-Fi, чтобы не тратить трафик

**7. Друг просит пароль от игры потому что у тебя больше скинов.**

A) Дать пароль, но только после того, как друг пообещает не менять настройки

B) Не давать пароль, но разрешить играть через функцию «Семейный доступ» или на твоём устройстве

C) Дать пароль, но сменить его сразу после того, как друг поиграет

D) Создать второго персонажа и дать пароль от него

**8. Представь, ты поругался с другом и удалил переписку. Что произошло?**

A) Они исчезли у всех участников диалога

B) Они удалились только у тебя, у собеседника остались и могут быть заскриншочены

C) Они удалятся у всех через 30 дней

D) Друг не сможет доказать, что в переписке я, так как у меня её нет

**9. Ты создаешь аккаунт в социальной сети. Ты сделаешь общедоступный профиль или закрытый?**

A) Оставить открытым, но не публиковать личную информацию

B) Сразу закрыть профиль, так как даже публичные посты собираются для создания цифрового досье

C) Оставить открытым на месяц для набора подписчиков, потом закрыть

D) Разрешить просмотр только друзьям друзей

**10. Представь, тебе пришло сообщение на электронную почту от родителей, но они сейчас на работе. В письме следующее сообщение:**

**«Нашла твою детскую фотографию, взгляни». Твои действия:**

A) Перейду по ссылке и посмотрю, что отправили родители, зачем им меня обманывать

B) Позвоню и уточню у родителей, почему отправили сообщение, а не показали лично

C) Скопирую ссылку и зайду через второй аккаунт

Приложение В

Таблица 2 – Диагностическая программа исследования актуального уровня знаний младших школьников о безопасном поведении в сети Интернет

| Параметр | Критерий | Уровни сформированности безопасного поведения в сети Интернет | | |
|---|---|---|---|---|
| | | Низкий | Средний | Высокий |
| Методика № 1<br>Тест по кибербезопасности<br>(7-11 лет)<br>Булдакова А.В. | Содержательный | 0-14 баллов:<br>Обучающийся плохо понимает сущность интернет-опасностей, не различает, какие сведения относятся к личным данным, а какие являются общедоступными. В его представлениях отсутствует понимание рисков, связанных с мошенничеством, подозрительными ссылками и использованием публичных сетей Wi-Fi. Ребенок не задумывается о последствиях своих действий в сети Интернет, что создает объективные предпосылки для попадания в ситуации, угрожающие его безопасности. | 15-23 баллов:<br>У ученика сформированы базовые знания о ключевых правилах безопасного поведения в сети Интернет. Он знает, что нельзя сообщать пароль и личные данные незнакомцам, понимает опасность, исходящую от мошенников и подозрительных ссылок. Однако эти знания ещё недостаточно систематизированы и проявляются преимущественно в типичных, стандартных ситуациях. В сложных, нестандартных обстоятельствах, требующих переноса знаний в новую плоскость, ребёнок может ошибаться, так как его представления не достигли уровня, обобщенного понимания принципов кибербезопасности. | 24-30 баллов:<br>Ребёнок хорошо разбирается в вопросах интернет-безопасности, понимает, что такое цифровой след и почему важно его контролировать. Он осознанно распознает угрозы различного характера, дифференцирует их и задумывается о долгосрочных последствиях своих действий в сети. Знания носят системный характер, что позволяет ученику ориентироваться не только в знакомых, но и в новых для него ситуациях. |

| | | | | |
|---|---|---|---|---|
| Методика № 2. Тест «Работа с персональными данными» (7-10 лет). Роскомнадзор. | Критерий информационной защиты | 0-4 баллов: Ребенок считает допустимым сохранять пароли без средств защиты, сообщать коды из СМС-сообщений третьим лицам, переходить по подозрительным ссылкам, полученным от незнакомых отправителей. Его представления о приватности не сформированы, что делает его уязвимым перед целым спектром угроз, связанных с хищением персональных данных. | 5-7 баллов: Ребенок знает, что нельзя никому сообщать пароли и коды подтверждения, понимает риск, связанный с подозрительными сообщениями и ссылками. В более сложных ситуациях – например, при необходимости настройки приватности в социальных сетях или оценке угроз, связанных с использованием публичного Wi-Fi, – ребёнок может не учесть всех факторов риска. | 8-10 баллов: Ребенок не только осознаёт, что нельзя передавать пароли и коды, но и понимает необходимость проверки источников информации, осознаёт ограничения, присущие публичным сетям Wi-Fi, и имеет правильное представление о том, что такое приватность и почему её необходимо сознательно оберегать. Знания носят устойчивый характер. |

Приложение Г

Таблица 3 – Протокол программы исследования актуального уровня знаний о безопасном поведении в сети интернет учащихся 2 «А» класса

| № | Ф.И. ученика | Критерий | | | | Общий уровень | |
|---|---|---|---|---|---|---|---|
| | | Содержательный | | Информационной защиты | | Баллы | Уровень |
| | | Баллы | Уровень | Баллы | Уровень | | |
| 1 | Александр | 12 | Н. | 3 | Н. | 15 | Н. |
| 2 | Алексей | 13 | Н. | 3 | Н. | 16 | Н. |
| 3 | Алина | 10 | Н. | 4 | Н. | 14 | Н. |
| 4 | Анастасия | 11 | Н. | 4 | Н. | 15 | Н. |
| 5 | Андрей | 14 | Н. | 4 | Н. | 18 | Н. |
| 6 | Анна | 12 | Н. | 3 | Н. | 15 | Н. |
| 7 | Артем | 13 | Н. | 2 | Н | 15 | Н. |
| 8 | Валерия | 10 | Н. | 3 | Н. | 13 | Н. |
| 9 | Виктор | 15 | С. | 5 | С. | 20 | С. |
| 10 | Виктория | 11 | Н. | 3 | Н. | 14 | Н. |
| 11 | Владимир | 14 | Н. | 5 | С. | 19 | Н. |
| 12 | Дарья | 16 | С. | 5 | С. | 21 | С. |
| 13 | Дмитрий | 12 | Н. | 4 | Н. | 16 | Н. |
| 14 | Екатерина | 13 | Н. | 4 | Н. | 17 | Н. |
| 15 | Елизавета | 14 | Н. | 2 | Н. | 16 | Н. |
| 16 | Иван | 17 | С. | 6 | С. | 23 | С. |
| 17 | Ирина | 11 | Н. | 5 | С. | 16 | Н. |
| 18 | Кирилл | 10 | Н. | 3 | Н. | 13 | Н. |
| 19 | Мария | 15 | С. | 6 | С. | 21 | С. |
| 20 | Максим | 14 | Н. | 5 | С. | 19 | Н. |
| 21 | Михаил | 16 | С. | 7 | С. | 23 | С. |
| 22 | Наталья | 12 | Н. | 4 | Н. | 16 | Н. |
| 23 | Никита | 15 | С. | 6 | С. | 21 | С. |
| 24 | Ольга | 18 | С. | 6 | С. | 24 | С. |
| 25 | Сергей | 13 | Н. | 5 | С. | 18 | Н. |
| 26 | София | 15 | С. | 7 | С. | 22 | С. |
| 27 | Татьяна | 11 | Н. | 4 | Н. | 15 | Н. |
| 28 | Юлия | 16 | С. | 7 | С. | 23 | С. |

Приложение Д

Таблица 4 – Сводная таблица результатов проведения методик

| Критерий | Уровни развития | | | | | |
|---|---|---|---|---|---|---|
| | Низкий | % | Средний | % | Высокий | % |
| Содержательный | 21 | 75 | 7 | 25 | 0 | 0 |
| Информационной защиты | 17 | 61 | 11 | 39 | 0 | 0 |
| Общее кол-во | 19 | 68 | 9 | 32 | 0 | 0 |

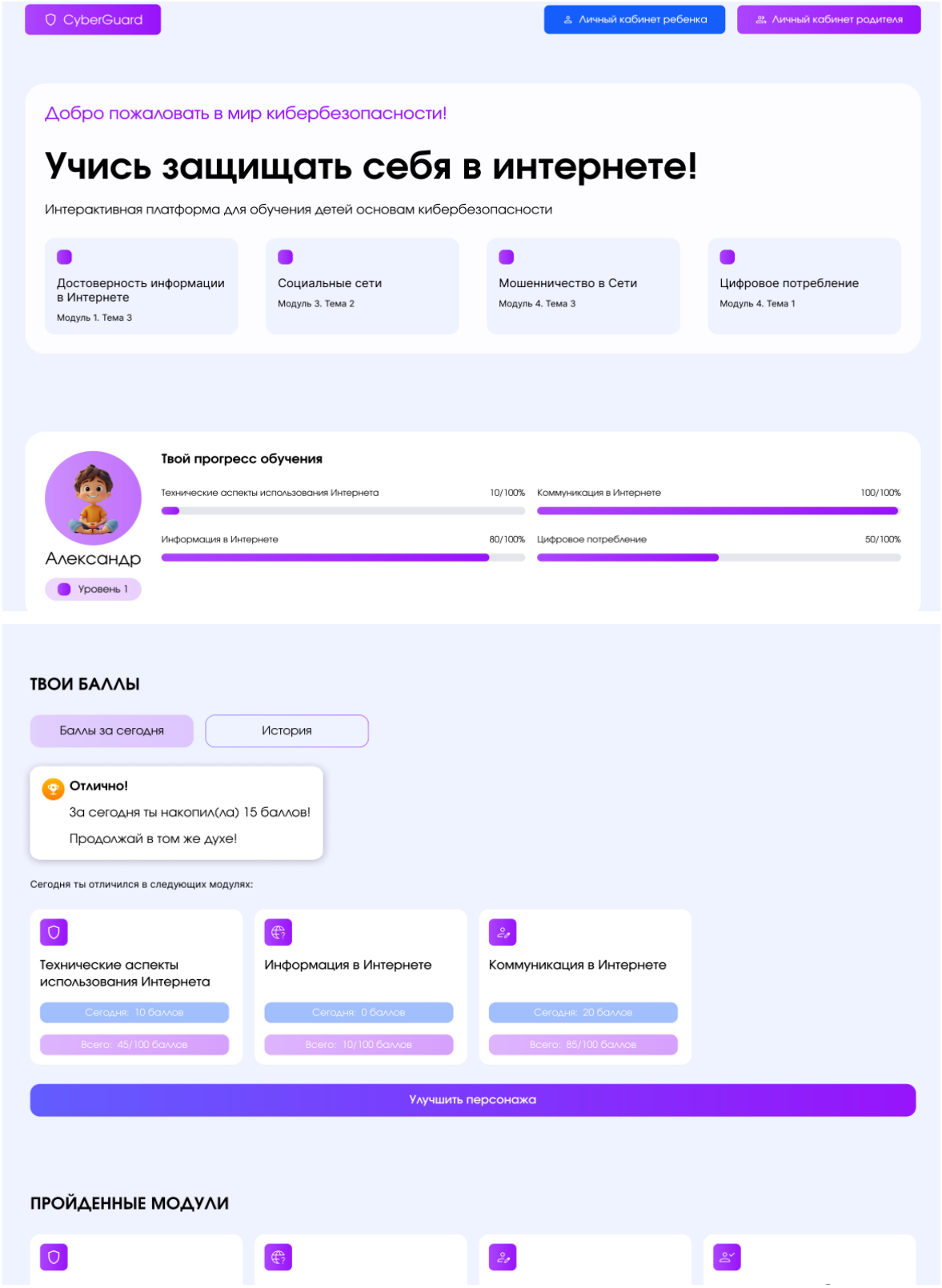



Рис. 7. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

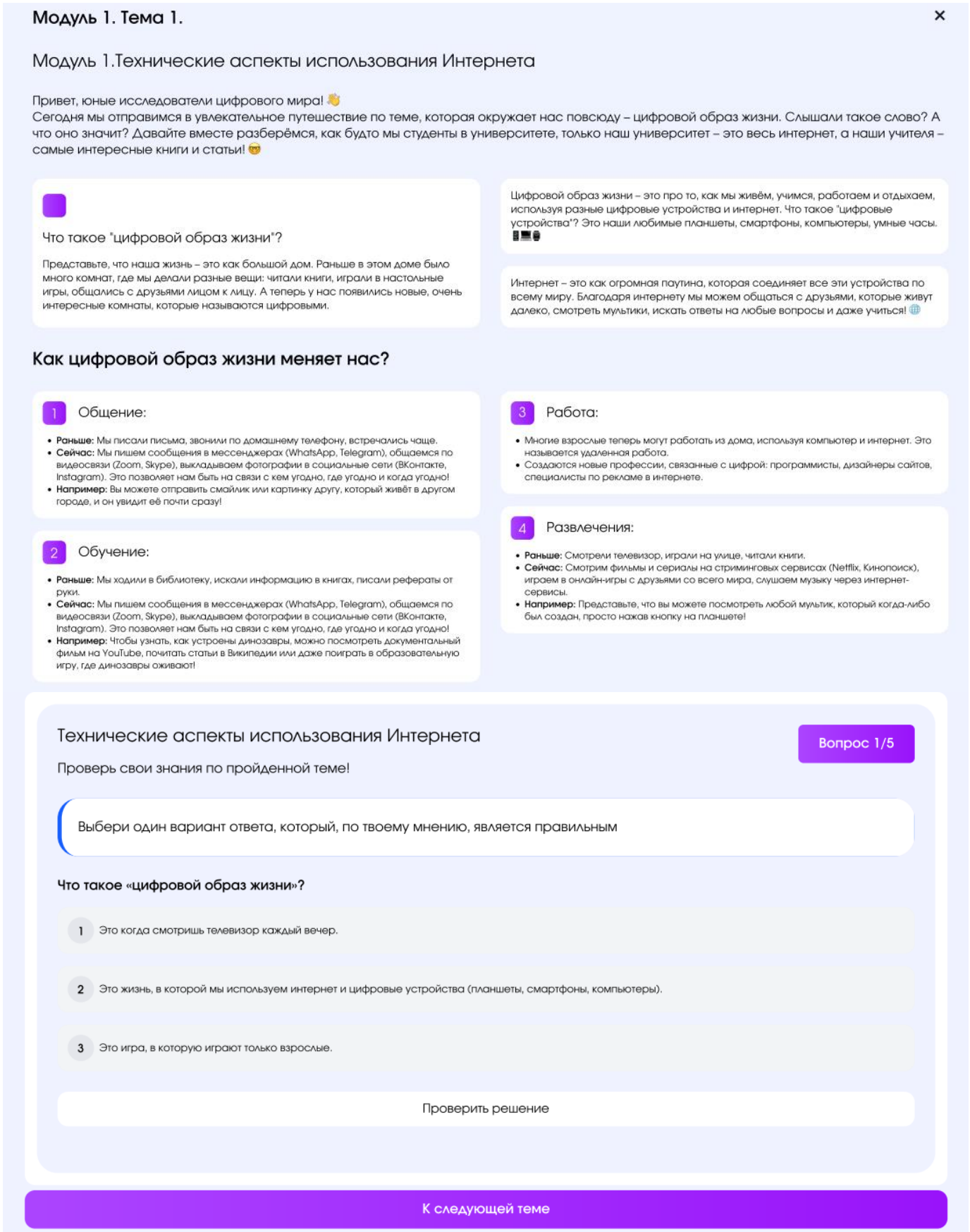



Рис. 8. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

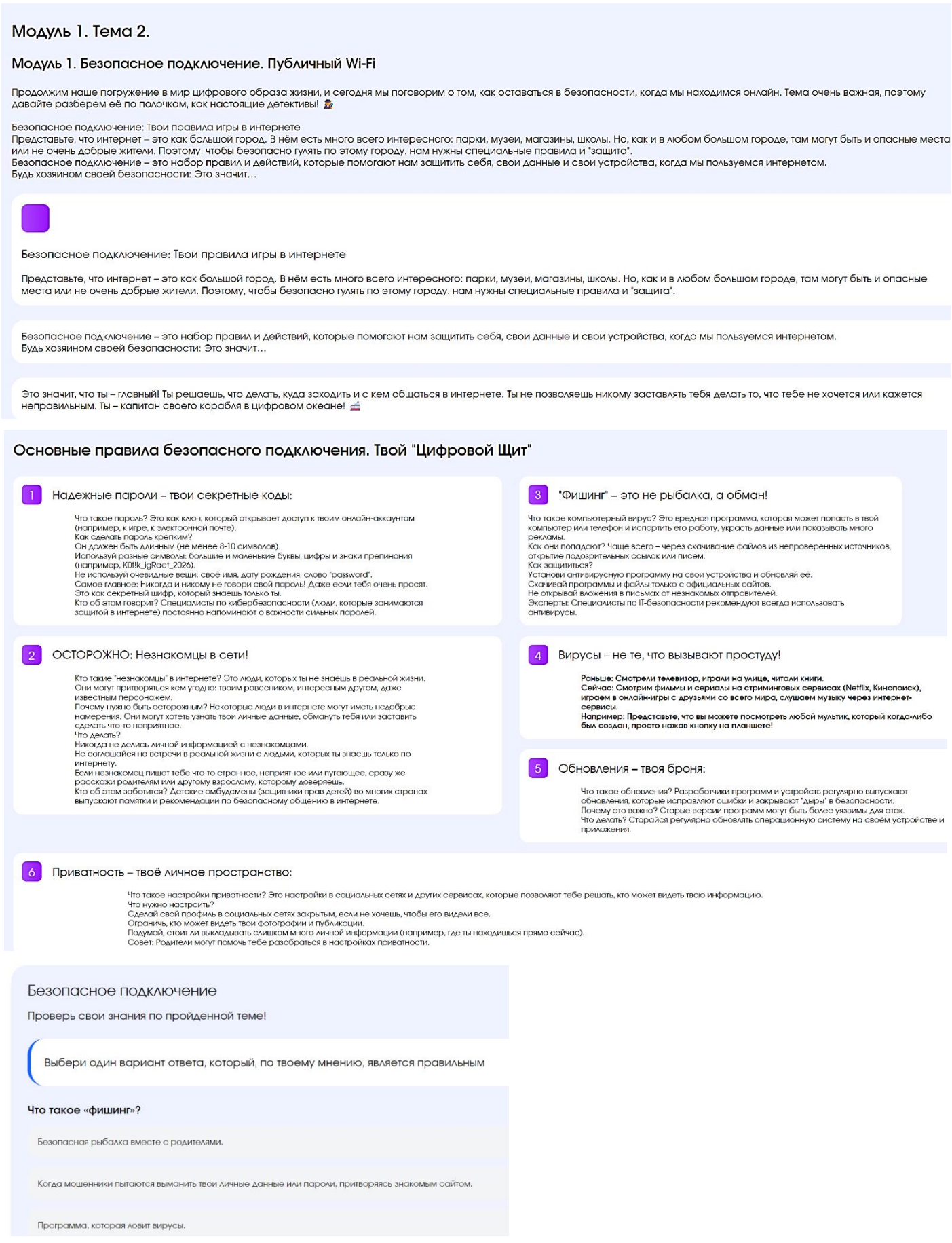



Рис. 9. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

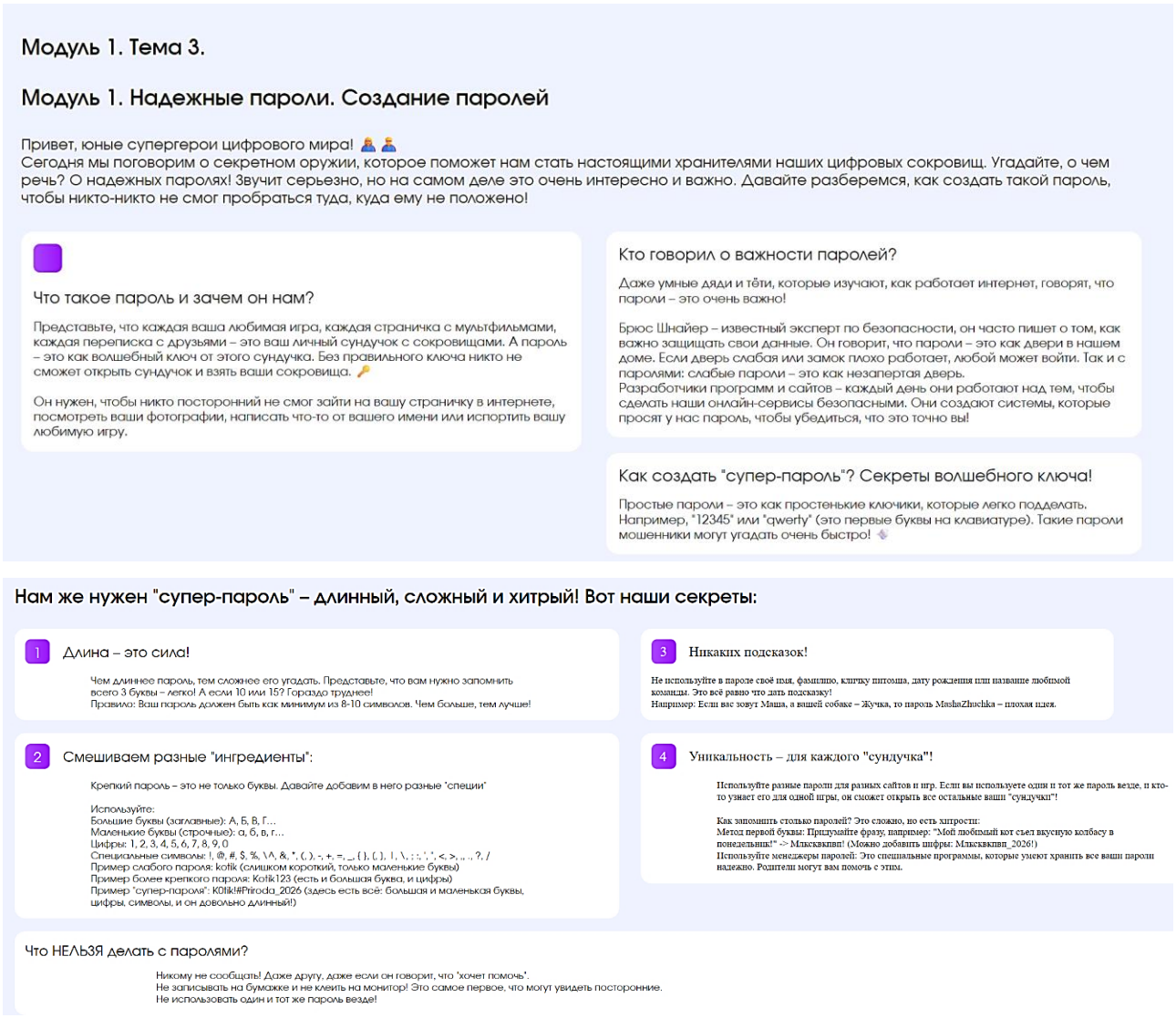



Рис. 10. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

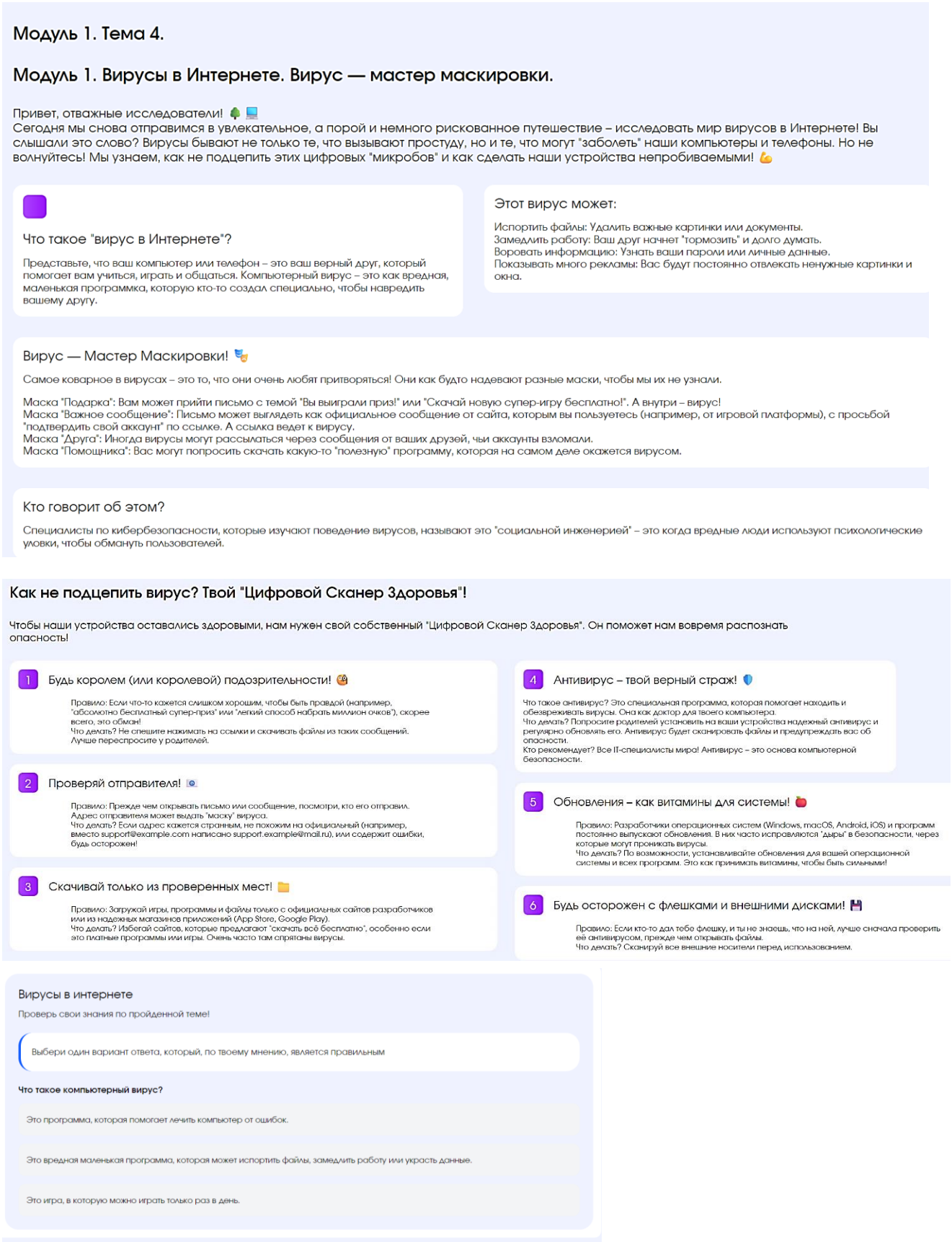



Рис. 11. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

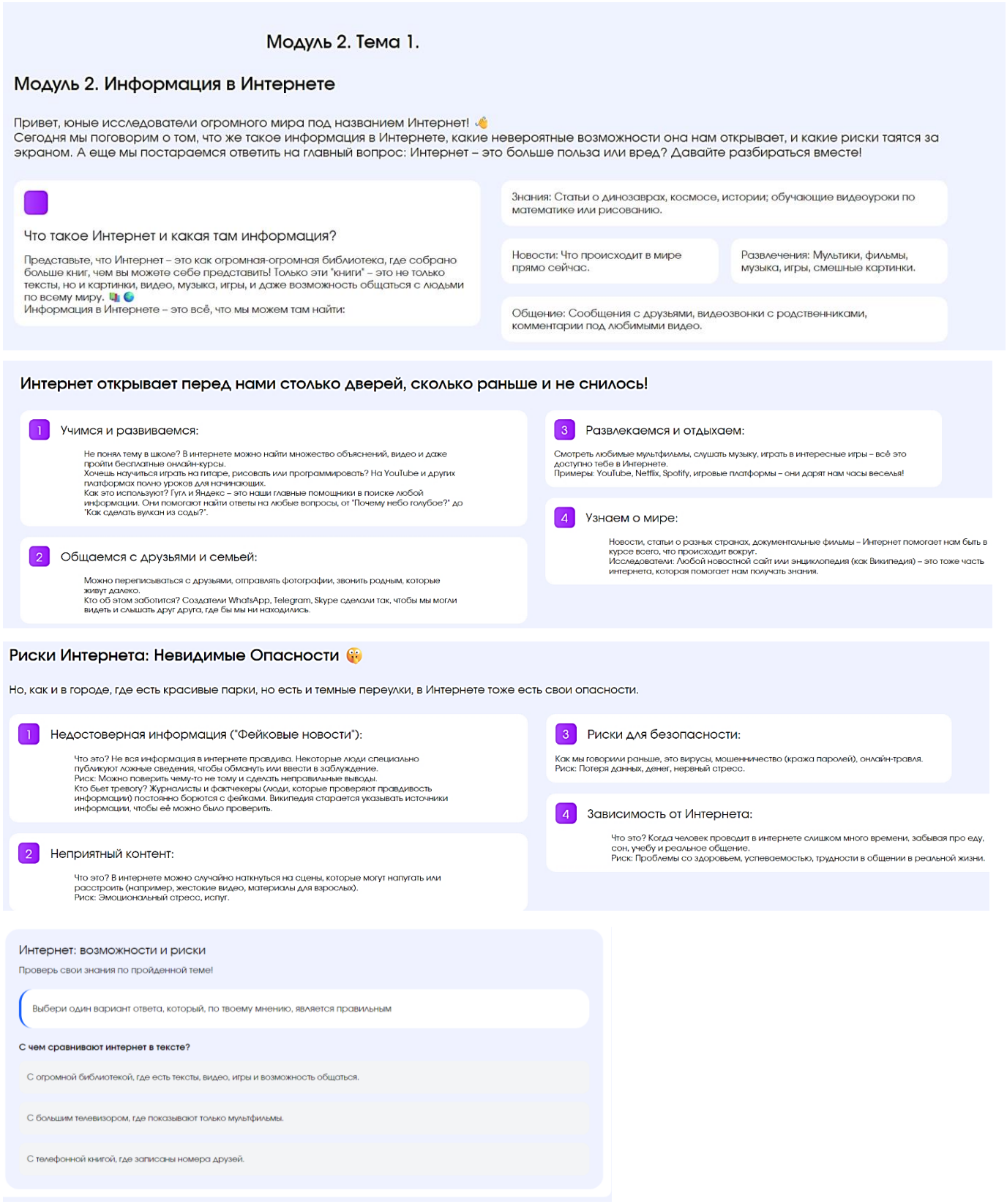



Рис. 12. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

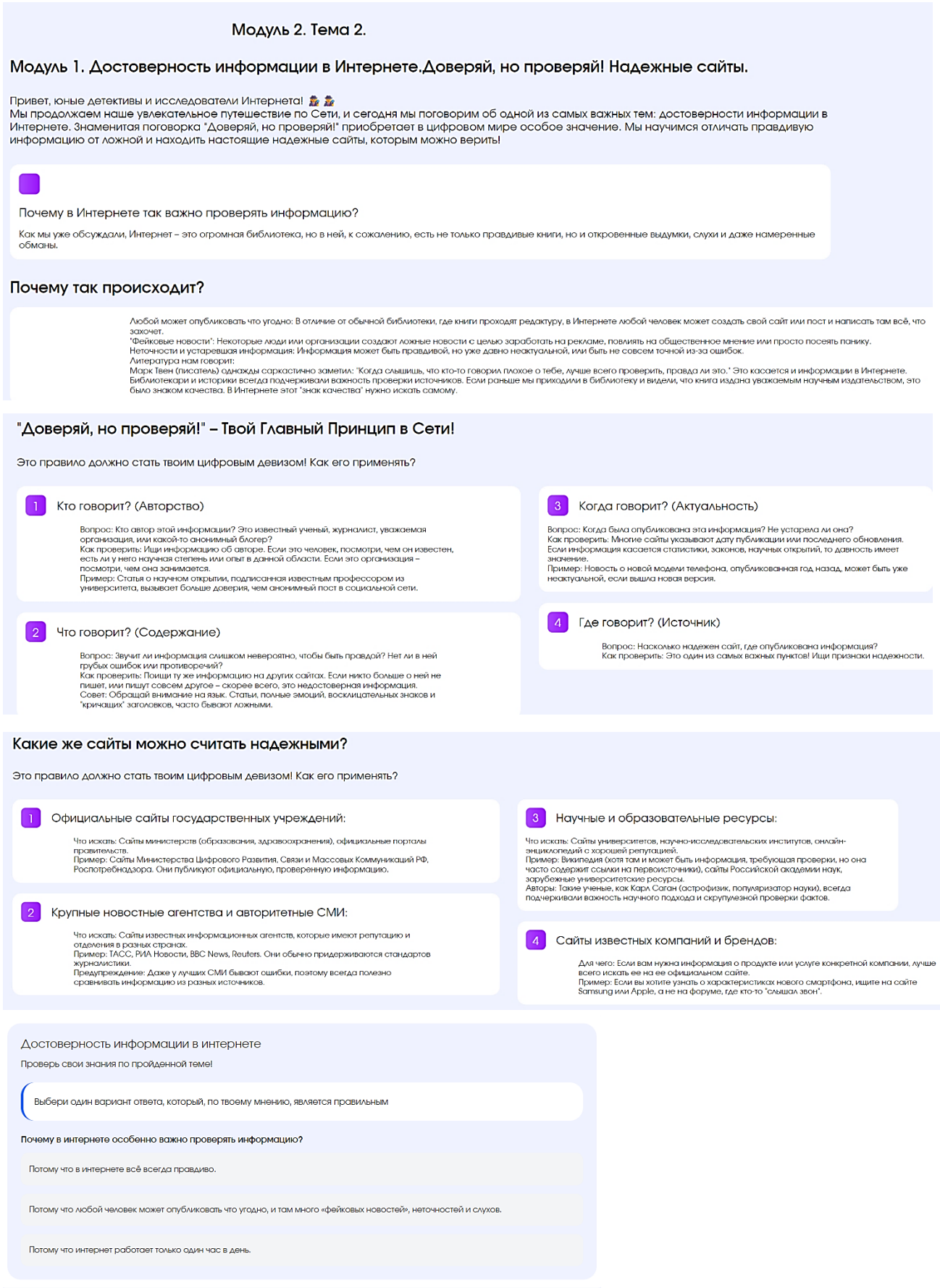



Рис. 13. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

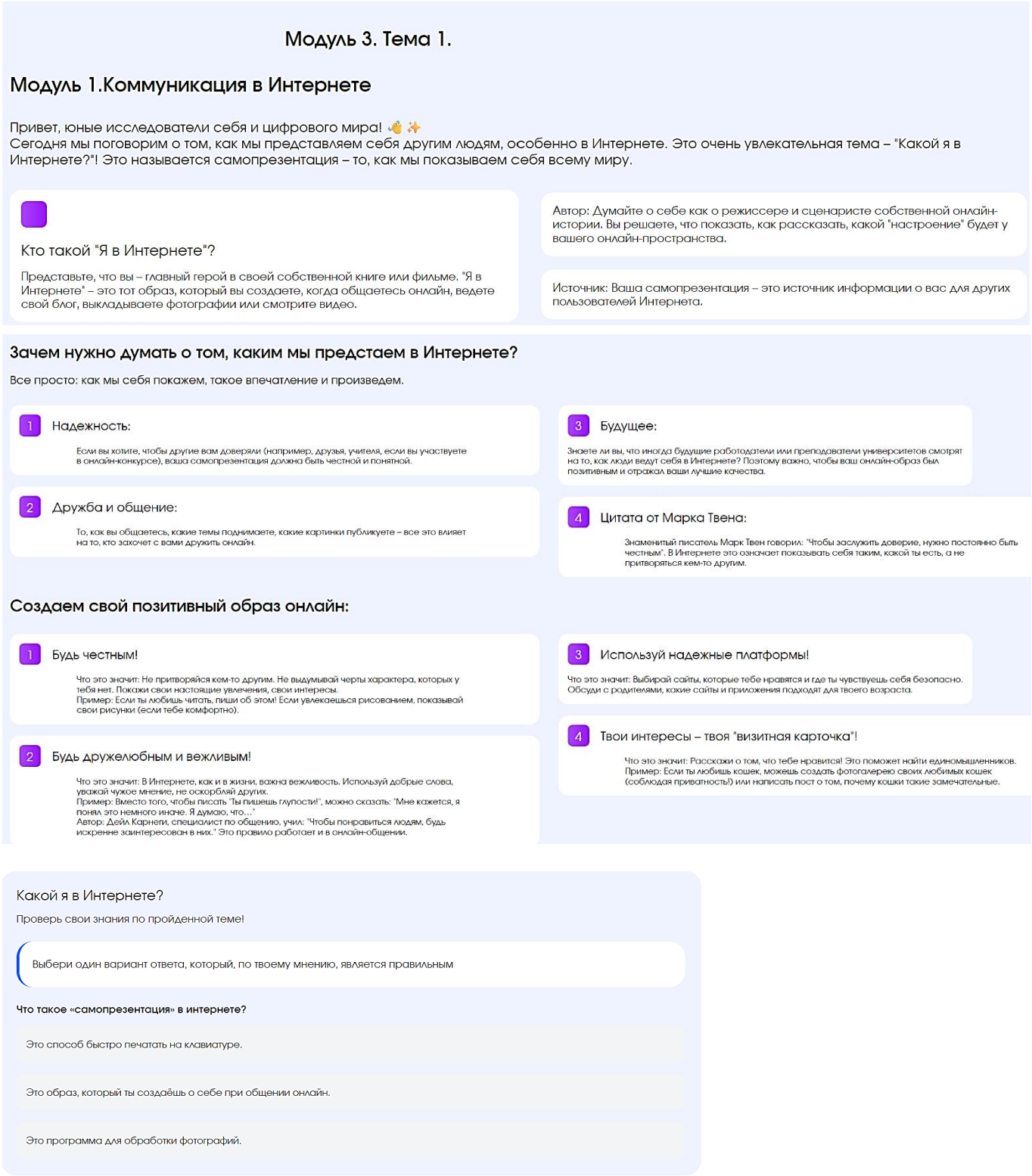



Рис. 14. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова


Рис. 15. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

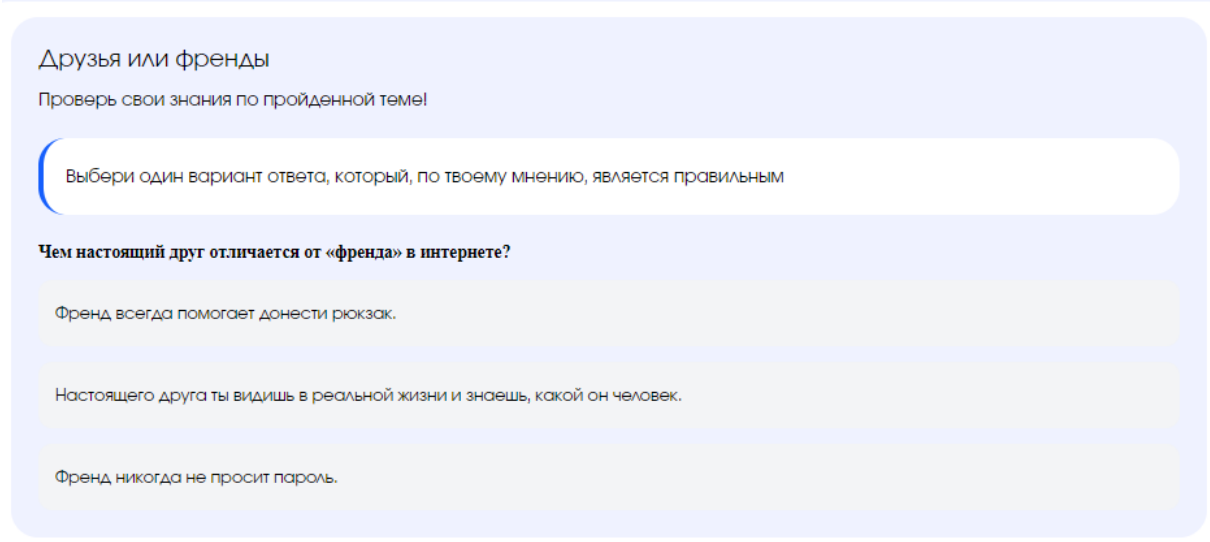



Рис. 16. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова

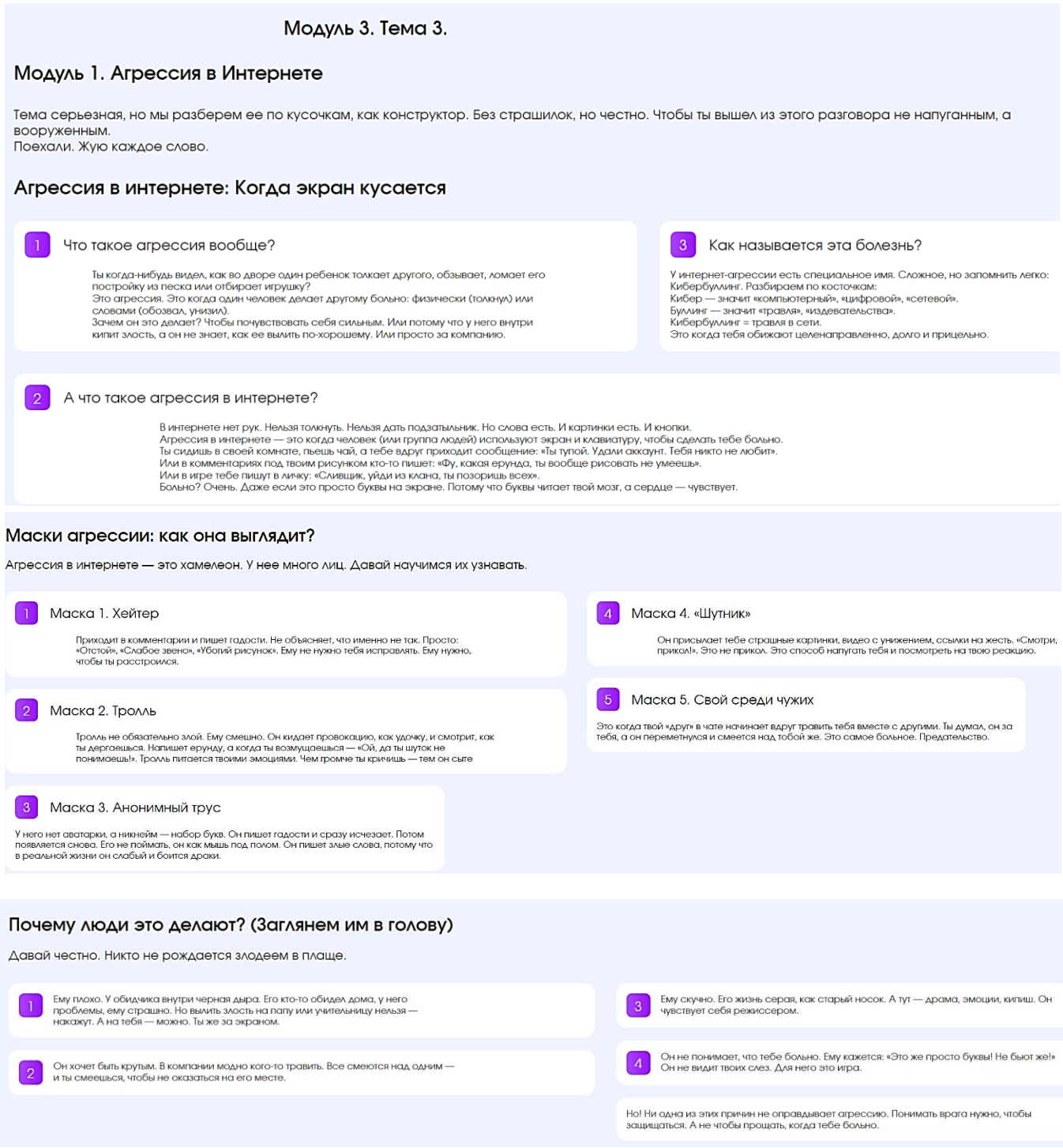
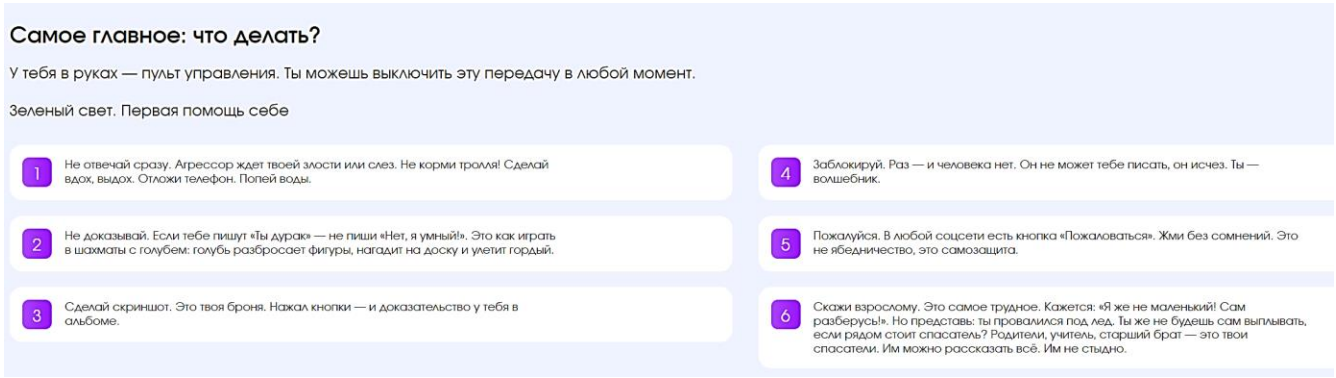
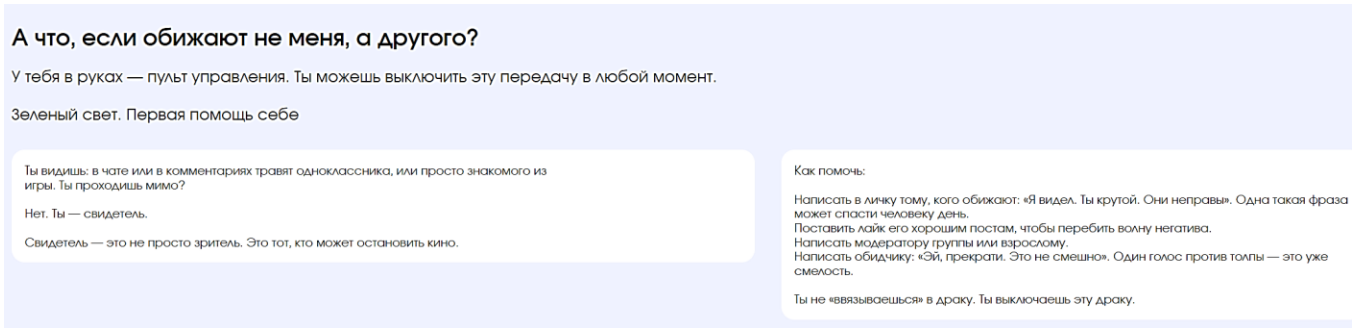



Рис. 17. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панкова



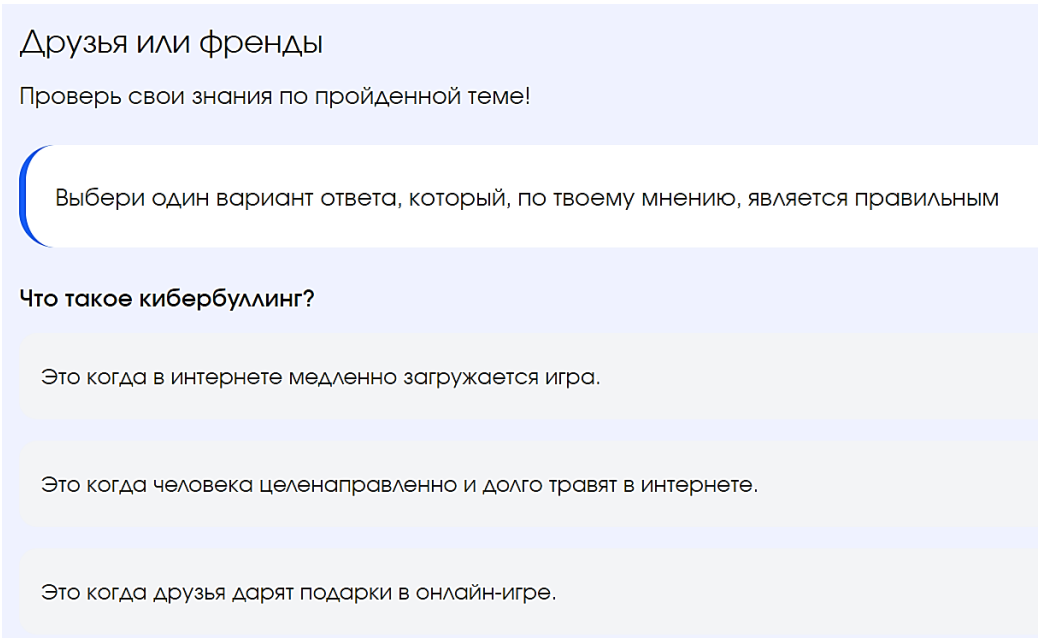




Рис. 18. Сайт «КиберЗащитник»
М. А. Давтян, Е.С. Панков

Приложение Ж

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. В. П. АСТАФЬЕВА

КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. В. П. АСТАФЬЕВА
1932

# ДИПЛОМ

*награждается*

***Давтян***
***Мери Артемовна***

*занявшая*
***III место***

*в конкурсе студенческих научных докладов секции*
*«Предметно-методические аспекты математического*
*и естественно-научного образования младших школьников»*
*на Всероссийской научно-практической конференции*
*«Современное начальное образование: проблемы и перспективы развития»*
*в рамках XXVI Международного научно-практического форума студентов,*
*аспирантов и молодых ученых «Молодёжь и наука XXI века»*

*с докладом «Формирование безопасного поведения младших школьников*
*в информационной среде»*
*(научный руководитель – Панкова Е.С., кандидат биологических наук,*
*доцент кафедры теории и методики начального образования)*

ПРОРЕКТОР ПО НАУЧНОЙ РАБОТЕ И ВНЕШНЕМУ ВЗАИМОДЕЙСТВИЮ КГПУ ИМ. В. П. АСТАФЬЕВА — Н.Ф. ИЛЬИНА

ОБЩИЙ ОТДЕЛ

КРАСНОЯРСК 2025

*17-18 апреля 2025г.*

Рис. 19.
Грамота об участии в конференции

Приложение 3

Материалы, предоставленные на конференции

Современное начальное образование: проблемы и перспективы развития: материалы Всероссийской научно-практической конференции, Красноярск, 17–18 апреля 2025 г. [Электронный ресурс] / отв. ред. Г.С. Спиридонова; ред. кол. – Электрон. дан. / Краснояр. гос. пед. ун-т им. В.П. Астафьева. – Красноярск, 2025. – С. 92–95. – (Молодежь и наука XXI века).

Доклад опубликован в сборнике:

Давтян, М.А. Формирование безопасного поведения младших школьников в информационной среде // Современное начальное образование: проблемы и перспективы развития: материалы Всероссийской научно-практической конференции, Красноярск, 17–18 апреля 2025 г. – Красноярск, 2025. – С. 92–95.