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

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

Деятельность учителя по формированию кибербезопасного поведения у младших школьников

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

Направленность программы бакалавриата

«Начальное образование. Дошкольное образование»
Форма обучения очная

Проверка на объем заимствований:
87,43 % авторского текста
Работа рекомендована к защите
« 14 » мая 2026 г.
Зав. кафедрой ТМиМНО
_____ Волчегорская Евгения Юрьевна

Выполнила:
студентка группы ОФ-521-071-5-1
Романова Арина Ильинична
Научный руководитель:
канд. пед. наук, доцент
_____Жукова Марина Владимировна

Челябинск
2026 год

Оглавление

ВВЕДЕНИЕ

На сегодняшний день развитие современной образовательной системы в Российской Федерации подчеркивает необходимость воспитания навыков кибербезопасного поведения у младших школьников. Глобальное расширение информационного пространства приводит к новым проблемам для развития как общества, так и личности. В основу образования вложен постоянный процесс поиска информации из различных источников, однако стоит помнить, что не весь доступный материал имеет положительный характер, что приводит к потенциально небезопасному контенту, особенно среди детей младшего школьного возраста, которые мало осведомлены о кибербезопасности. Следовательно, в настоявшее время появилась острая потребность в организации процесса формирования кибербезопасного поведения среди младших школьников со стороны учителей, поэтому данное направление набирает обороты для устранения проблемы.

Значительное внимание безопасности учащихся отводит Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ. Этот закон характеризуется уникальной особенностью, он трактует кибербезопасность как «…состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [33].

Кибербезопасность в образовании является важной задачей, которая требует совместных усилий всех участников образовательных отношений. Принимая необходимые меры, можно защитить учащихся и образовательные организации от киберугроз и обеспечить их безопасность в цифровом мире [31, с.135].

Данные статистических исследований свидетельствуют: среди детей, которым сейчас 7-10 лет, большинство (77%) познакомились с гаджетами до школы. В других возрастных группах ситуация несколько иная: среди детей,

которым сейчас 11-14 лет, до школы с гаджетами были знакомы 46%, для 15-18 лет этот показатель составляет 29% [6]. Таким образом, наблюдается динамика снижения возрастной группы среди пользователей информационной средой. Процентный показатель за последнее десятилетие доказывает активный рост технического прогресса среди младших школьников.

У детей младшего школьного возраста не в полной мере сформированы представления об источниках киберугроз. Они могут не увидеть опасность, не распознать риски того или иного действия в сети Интернет, а также иногда принимают всю информацию за действительность, не понимая, что она может нести определённый вред. По нашему мнению, ответственность педагога заключается в обучение младших школьников определенным навыкам восприятия материала из различных технических ресурсов.

Сущность и особенности кибербезопасного поведения детей младшего школьного возраста освещены в работах А. А. Аверкиева, М. М. Безкаравайного, К. И. Воробьева, С. В. Исаева, Б. В. Сергеева и других.

Формы работы педагогов по формированию кибербезопасного поведения младших школьников рассмотрены в трудах Ю. С. Дащенко, А. В. Калач, А. В. Калинченко и другие.

Проблема исследования: какие формы и методы работы могут быть использованы учителем начальных классов в процессе формирования кибербезопасного поведения детей младшего школьного возраста?

Актуальность исследования и проблема позволили сформулировать тему нашего исследования: «Деятельность учителя по формированию кибербезопасного поведения у младших школьников».

Цель исследования: изучение теоретических аспектов проблемы деятельности учителя по формированию кибербезопасного поведения младших школьников для составления «банка» методических материалов педагогам.

Объект исследования*:* процесс формирования кибербезопасного поведения младших школьников.

Предмет исследования: направления деятельности учителя по формированию кибербезопасного поведения младших школьников.

Задачи исследования:

1. Изучить понятие и специфику формирования кибербезопасного поведения детей младшего школьного возраста.
2. Рассмотреть направления деятельности учителя начальных классов по формированию кибербезопасного поведения младших школьников.
3. Провести и проанализировать результаты исследовательской работы.
4. Составить «банк» методических материалов, направленных на формирование кибербезопасного поведения младших школьников.

Практическая значимость исследования состоит в том, что результаты исследования могут быть использованы учителем начальных классов в работе по формированию кибербезопасного поведения младшего школьника.

База исследования: наше исследование проходило на базе МАОУ средней общеобразовательной школы в г. Златоуст. В исследовании принимали участие учащиеся 4 класса в количестве 25 человек и педагоги образовательной организации в количестве 7 человек.

Этапы исследования:

1. На первом этапе исследования изучалась степень изучения проблемы в психолого-педагогической литературе, анализировались основные понятия, формулировались методические положения исследования, подбирался диагностический инструментарий.
2. На втором этапе проводилось изучение уровня кибербезопасного поведения и анализировались результаты.
3. На третьем этапе создавался «банк» методических материалов для работы учителя по формированию кибербезопасного поведения у младших школьников.

Методы исследования:

- теоретические: анализ психолого-педагогической и методической литературы по исследуемой проблеме, моделирование, синтез, обобщение;
- эмпирические: анкетирование;
- методы обработки и интерпретации результатов.

Структура работы: наше исследование состоит из введения, 2 глав, выводов по 2 главам, заключения, списка использованных источников, приложений. В тексте работы 2 приложения. Список литературы представлен 36 источниками.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ УЧИТЕЛЯ ПО ФОРМИРОВАНИЮ КИБЕРБЕЗОПАСНОГО ПОВЕДЕНИЯ МЛАДШИХ ШКОЛЬНИКОВ

1.1 Понятие и специфика кибербезопасного поведения детей младшего школьного возраста

Современный мир технологий ставит перед младшими школьниками новые испытания, среди которых особенно остро встают вопросы кибербезопасности, «… прежде чем перейти к анализу психологических ресурсов кибербезопасности человека, следует определить основные понятия, связанные с предметом настоящего исследования, появившиеся в научной литературе в конце 90-х гг. XX в.: кибербезопасность, киберугрозы» [8, с.151].

А. А. Аверкиев отмечал: «Кибербезопасность – практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Термин также известен как безопасность информационных технологий или электронная информационная безопасность» [1, с.567].

М. М. Безкоровайный указывает, что в проекте Концепции говорится следующее: «…кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями» [4, с. 25].

С. В. Исаев трактует: «Кибербезопасность (безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве» [13, с.293].

С. Н. Виноградский определил: «Киберугроза (киберопасность) – незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей» [7, с.229].

Кибербезопасность представляет собой комплекс мер и практик, направленных на защиту компьютерных систем, сетей, устройств и данных от

различного рода вредоносных атак и несанкционированного доступа. Понятие «кибербезопасность» охватывает широкий спектр мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации в цифровом пространстве. В свою очередь, термин «киберугроза» подразумевает угрозу незаконного вторжения или атаки на виртуальное пространство с целью реализации определенных намерений, включая политические и социальные мотивы.

Соответственно, кибербезопасность понимается как система методов и подходов, которая направленна на обеспечение информационной безопасности, сохранность и защиту персональных данных пользователей. Она включает меры по защите инфраструктуры и данных от разного рода риска и атак. В связи с ростом количества киберугроз особое внимание уделяется разработке эффективных механизмов защиты, особенно применительно к детям младшего школьного возраста.

Кибербезопасность находится на стыке технологий и психологии. Она представляет собой с одной стороны защиту технического средства от внешних кибератак, с другой стороны защиту человека в киберпространстве, то есть его репутацию, умение отстаивать личные границы.

Сегодняшняя реальность демонстрирует острую проблему, оказывающую значительное воздействие на разные поколения, особенно затрагивая учащихся начальных классов, которые пока недостаточно осознают потенциальные угрозы, исходящие от информационно-коммуникационных сетей.

Б. В. Сергеева отмечет, что исследователи-педагоги подчеркивают резко возросшую информированность детей. Раньше для ребенка школа была основным источником получения информации о мире, человеке, обществе, природе, а сегодня СМИ оказываются существенным фактором формирования у детей картины мира. Расширение кругозора, высокий рост эрудиции – несомненное преимущество современных детей. По мнению современных педагогов, уже на первой ступени обучения система образования должна в полной мере использовать новые возможности – современные образовательные технологии,

формирующие умения работать с информацией, в том числе информационно-коммуникационные технологии, информационный потенциал Интернета, различные дистанционные формы обучения и др. [28].

Формирование грамотного поведения в информационной среде у детей младшего школьного возраста важно по нескольким причинам:

1. Активный рост популярности цифрового мира. Современные технологии позволяют быстро распространять любую информацию, однако эта информация бывает разной: интересной, полезно, но в последнее время чаще всего вредной, опасной и недостоверной для пользователей.

2. Глобальная вовлеченность младших школьников в онлайн-пространство. Дети младшего школьного возраста стали активнее пользоваться Интернетом и социальными сетями, и, хотя это открывает много возможностей для развития и познания нового, но оно же создает риски негативного влияния.

3. Высокий уровень риска для детей начальной школы. Когда младший школьник начинает осваивать компьютер или телефон, он легко сталкивается с разными проблемами в Интернете, такими как мошенничество, вредные советы или агрессия, потому что младший школьник в этом возрасте уязвим и восприимчив.

Кибербезопасное поведение детей младшего школьного возраста предполагает умение безопасно пользоваться цифровыми ресурсами, защищая своё здоровье, психическое, физическое, нравственное и духовное развитие.

Опираясь на изученную литературу, мы выделили рекомендации по формированию кибербезопасного поведения:

1. Защита личной информации. Младшим школьникам важно понимать, что размещение чрезмерного количества сведений о себе в Интернете либо передача персональной информации неизвестным / малоизвестным / посторонним лицам небезопасны.

2. Обновление паролей. Следует обговорить и договориться с младшим школьником о регулярной смене паролей ко всем учетным записям, например, дважды в год или сразу после предупреждения о взломах.

3. Бдительность в социальных сетях. Следует рассказать детям младшего школьного возраста, насколько внимательно нужно подходить к размещаемым фотографиям и личным данным, поскольку неуместная информация способна сильно повлиять на репутацию и благополучие. Рекомендуется рассказать о том, что такая информация в любой момент может стать доступной для всех пользователей сети Интернет, даже после её удаления.

4. Обращение за помощью. Важно сформировать доверительное отношение к взрослым, чтобы младший школьник знал: если возникает какая-либо ситуация в Интернете, родители и учителя всегда будут рядом и окажут поддержку. Стоит показать, что взрослые всегда готовы пойти на помощь.

Выделим основные умения, способствующие кибербезопасному поведению младших школьников:

- использование только проверенных и надежных источников;
- рациональное и бережное отношение к своим личным данным;
- самостоятельное управление временем, проводимым за экранами гаджетов;
- создание сложных и уникальных паролей, позволяющих обезопасить личные данные.

Стоит отметить практические рекомендации по обеспечению кибербезопасности:

1. Рекомендации для педагогов.
2. Способы повышения осведомленности детей младшего школьного возраста о правилах безопасного поведения в сети.
3. Организация семейного контроля над использованием киберпространства.

Исходя их вышеизложенного, нами было принято решение опираться на определение «…сохранение конфиденциальности, целостности и доступности информации в киберпространстве», предложенное С. В. Исаевым, поскольку оно наилучшим образом отражает содержание понятия «кибербезопасность». Обучение детей младшего школьного возраста правилам безопасного поведения

в киберпространстве направлено на охрану их здоровья и безопасности в сложной цифровой среде. Крайне важно, чтобы младшие школьники четко и ясно представляли себе значение правильной оценки информации, которая может оказать как положительный, так и отрицательный эффект.

1.2 Направления деятельности учителя начальных классов по формированию кибербезопасного поведения младших школьников

Проблема обеспечения информационной безопасности детей младшего школьного возраста в сети Интернет приобретает особую остроту в младшем школьном возрасте, когда у ребёнка формируются первые устойчивые модели поведения в цифровой среде, но при этом критическое мышление и навыки саморегуляции находятся на начальном этапе развития. В связи с этим перед педагогом стоит задача не просто информировать обучающихся о потенциальных киберугрозах, а создать условия для присвоения норм кибербезопасности как личностно значимых. Решение данной задачи требует использования разнообразных форм воспитательной и образовательной работы, учитывающих возрастные особенности младших школьников: переход то наглядно-образного к словесно-логическому мышлению, более развита наглядно-образная память, ведущая деятельность – учебная, эмоционально отзывчивы и ориентация на мнение авторитетного взрослого.

А. В. Калач заметил: «Формирование культуры кибербезопасности возможно только тогда, когда субъект в полной мере знает и понимает, чему служит цель соблюдения правил, иначе он будет их игнорировать» [15, с. 30]. Действительно, если же младший школьник не осознаёт значимости выполняемых действий, он подвергается пренебрежительно относиться к правилам, воспринимая их как формальность. Задача взрослого – не следить и ограничивать, а объяснять и убеждать: «это не запрет ради запрета, а способ защитить твои личные границы, твоё право на безопасность и твоё спокойствие». Только тогда правила становятся внутренним ориентиром, а не внешним раздражителем.

Изучив и проанализировав литературу, можно выделить несколько направлений работы педагогов по формированию кибербезопасного поведения младших школьников:

1. Тематические классные часы, внеклассные мероприятия и интерактивные игры. Здесь важно не просто перечислять и обсуждать киберугрозы, а именно проживать их вместе с детьми. Например, в формате квеста или путешествия по «безопасному Интернету» дети сами находят выход из сложных ситуаций. Проигрывание ситуаций (например, «Разговор с незнакомцев в сети», «Подозрительная ссылка от друга») позволяет эмоционально закрепить верные поведенческие действия. Таким образом, дети лучше запоминают принципы кибербезопасного поведения.

2. Онлайн-тренажёры и стимуляторы. Цифровая среда позволяет создать почти реальную ситуацию киберугрозы, но без настоящего риска. Младший школьник учится реагировать: стоит ли переходить по ссылке, можно ли отвечать незнакомцу, как выглядит фишинг, кибербуллинг, коммуникативные провокации. Этот подход продуктивен, так как такой опыт остаётся в памяти надолго.

3. Проектная деятельность. Создание стенгазет, памяток, буклетов или коротких видеороликов – всё это помогает детям не только заполнить информацию, но и осмыслить её. В ходе проектной работы происходит не просто воспроизведение информации, но её осмысление, структурирование и творческая переработка. Например, разрабатывая маршрут безопасного поведения в социальной сети, младший школьник вынужден системно осмыслить все возможные риски и способы из предотвращения.

4. Работа с родителями. Без включенности родных и близких все школьные усилия могут ослабнуть. Эффективными формами здесь выступают тематические родительские собрания с элементами тренинга, совместные детско-родительские мероприятия (например, квизы или конкурсы), распространение памяток, чек-листов. Родителям важно дать понятные инструменты: как говорить с ребёнком о кибербуллинге, какие настройки родительского контроля работают,

куда обращаться за помощью. Важно не просто проинформировать родителей о существовании киберугроз, но и предложить конкретные, понятные и реалистичные способы защиты ребёнка, выстроив единую воспитательную позицию школы и семьи.

5. Привлечение специалистов МВД и IT-сферы. Сотрудники полиции на доступных примерах объяснят младшим школьникам юридические последствия киберугроз, а IT-эксперты проведут практические мастер-классы по созданию надежных паролей и настройкам приватности. Такие встречи могут проходить в формате интерактивных бесед, игр и уроков цифровой гигиены, что делает информацию о рисках в сети более убедительной и понятной для детей младшего школьного возраста. Совместная работа специалистов и педагогов поможет сформировать у школьников конкретные навыки защиты и критическое отношение к опасным ситуациям в Интернете.

Следовательно, формирование кибербезопасного поведения младших школьников обеспечивается комплексным применением различных форм работы: игровых и интерактивных занятий, цифровых стимуляторов, проектной деятельности и просветительской работы с родителями. Только системный подход, при котором знания подкрепляются практическим опытом и единой позицией значимых взрослых, способен сформировать у ребёнка осознанное и ответственное отношение к собственной безопасности в глобальной сети. Настоящая кибербезопасность начинается там, где за каждым правилом стоит понимание его ценности – и у ребёнка, и у взрослого.

Выводы по главе 1

Анализ психолого-педагогической литературы позволил нам прийти к следующим выводам.

Проведённое в первой главе теоретическое исследование позволило системно рассмотреть проблему формирования кибербезопасного поведения младших школьников как одну из приоритетных задач современного начального образования. Мы установили, что цифровая среда перестала выполнять

исключительно вспомогательную функцию, превратившись в самостоятельное пространство социализации, развития и повседневной активности ребёнка. В связи с этим обеспечение безопасности в киберпространстве приобретает статус педагогической проблемы, требующей целенаправленной воспитательной работы.

Теоретический анализ позволил нам уточнить ключевые понятия нашего исследования. Опираясь на позицию С. В. Исаева, мы рассматриваем кибербезопасность как состояние защищённости информации и личности в цифровой среде, обеспечиваемый сохранением конфиденциальности, целостности и доступности данных. В свою очередь, кибербезопасное поведение младшего школьника представляет собой интегрированное качество личности, проявляющееся в осознанном, ответственном и безопасном взаимодействии с ресурсами сети Интернет, владении алгоритмами распознавания угроз и способности применять защитные стратегии в различных цифровых ситуациях.

Выделены также ключевые критерии компетенций в области кбербезопасности, необходимых учащимся начальных классов: информационно-познавательных (умение оценивать достоверность информации, осуществлять безопасный поиск), технико-защитные (создание надёжных паролей, настройки приватности, распознавание фишинга), коммуникативные (безопасное взаимодействие в социальных сетях, противодействие кибербуллингу) и поведенческие (своевременное обращение за помощью к взрослым, выход из опасной коммуникации). Освоение данных навыков обеспечивает ребёнку возможность не только избегать цифровых угроз, но и продуктивно использовать потенциал информационной среды для самообразования, творчества и досуга.

Отдельное внимание уделено анализу форм и методов педагогической работы в исследуемом направлении. Установлено, что наибольший воспитательный потенциал несут интерактивные и эмоционально насыщенные форматы: игровое моделирование ситуаций, квесты, онлайн-тренажёры, проектная деятельность, родительские мероприятия. Именно данные подходы

позволяют перевести знание о правилах кибербесопасности во внутренний план действий, сделать их личностно значимыми и эмоционально приятными.

Стоит отметить, что проведённый анализ позволил зафиксировать проблемную зону существующей педагогической практики. Несмотря на призвание значимости формирования кибербезопасного поведения, на сегодняшний день наблюдается дефицит методически проработанного инструментария для реализации данной работы.

Таким образом, теоретическое исследование подтвердило актуальность и практическую значимость проблемы формирования кибербезопасного поведения младших школьников, а также выявило объективную необходимость в создании и систематизации «банка» методических материалов по данному направлению.

ГЛАВА 2. ПРАКТИЧЕСКИЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ УЧИТЕЛЯ ПО ФОРМИРОВАНИЮ КИБЕРБЕЗОПАСНОГО ПОВЕДЕНИЯ МЛАДШИХ ШКОЛЬНИКОВ

2.1 Организация и методы исследования

Наше исследование проводилось на базе МАОУ средней общеобразовательной школы в г. Златоуст. В нашем исследовании приняли участие учащиеся 4 класса в количестве 25 человек и преподаватели начального общего образования в количестве 7 человек.

Цель исследования: определение уровня сформированности кибербезопасного поведения младших школьников и отношения педагогов к использованию элементов обучения для формирования кибербезопасного поведения детей начальной школы.

Задачи:

1) определить базу и выборку нашего исследования;

2) подобрать диагностический материал, направленный на выявление уровня сформированности кибербезопсного поведения младших школьников и отношения педагогов к использованию элементов обучения для формирования кибербезопасного поведения детей младшего школьного возраста;

3) выявить уровень сформированности кибербезопасного поведения младших школьников и отношения педагогов к использованию элементов обучения для формирования кибербезопасного поведения младших школьников.

4) составить «банк» методических материалов, направленных на формирование кибербезопасного поведения младших школьников.

Первым направление нашего исследования было выявление уровня сформированности кибербезопасного поведения младших школьников. Нами была использована анкета.

Цель: выявить уровень сформированности кибербезопасного поведения младших школьников.

Форма (ситуация оценивания): индивидуальное анкетирование детей младшего школьного возраста.

Методика проводится в формате анкетирования.

Инструкция: Уважаемые ребята! Вам предлагается ответить на вопросы анкеты, направленной на оценку уровня сформированности навыков безопасного поведения в цифровой среде. Выберите один вариант ответа, наиболее соответствующий вашему типичному поведению. Просьба отвечать искренне.

Материал: бланк анкеты.

Анкета:

1. Знаешь ли ты правила безопасности в Интернете?

A. Да, я знаю, как вести себя в Интернете.

B. Немного знаю, но не всё.

C. Нет, я не знаю таких правил.

2. Что ты будешь делать, если незнакомый человек напишет тебе в социальной сети или в игре?

A. Отвечу, если он кажется добрым и вежливым.

B. Не буду отвечать и расскажу родителям.

C. Напишу грубость и заблокирую.

3. Как ты думаешь, можно ли сообщать свой домашний адрес, номер телефона или адрес школы новым друзьям из Интернета?

A. Думаю, что можно сообщить, если они хорошие.

B. Нет, это опасно!

C. Можно сообщить, если только очень доверяю им.

4. Ты получил(а) сообщение: «Твой друг / родственник в беде, срочно пришли деньги!». Что ты сделаешь?

A. Переведу деньги, чтобы помочь.

B. Спрошу у родителей, правда ли это.

C. Напишу обратно: «Докажи, что это правда!»

5. Какой пароль лучше для защиты своего аккаунта?

A. 123456 или дату своего дня рождения (легко запомнить).

B. Имя моего питомца (его знают только родные и близкие).

C. Случайные буквы, цифры и знаки (например, «Dk7!gA4»).

6. Если тебе в Интернете встретилось что-то страшное, непонятное или обидное, ты:

A. Никому не скажу и постараюсь забыть, как можно быстрее.

B. Закрою и пойду играть, переписываться дальше.

C. Обязательно расскажу родителям или учителю.

7. Можно ли открывать письма от незнакомцев с вложениями или ссылками?

A. Да, если там интересное название.

B. Нет, это может быть вирус.

C. Открою, но, если только компьютер защищён.

8. Как часто ты рассказываешь родителям о том, что делаешь в Интернете?

A. Всегда, мы это постоянно обсуждаем.

B. Иногда, если что-то непонятно.

C. Никогда, это мой секрет.

9. Твой друг просит логин и пароль от игры, ты:

A. Дам, ведь он мой друг!

B. Откажу, даже если обидится.

C. Попрошу у родителей / учителя совета.

10. Тебе посоветовали в Интернете игру, но для скачивания просят ввести номер банковской карты родителей. Твои действия?

A. Введу, так как мне её посоветовали знакомые, она очень интересная.

B. Спрошу разрешения у мамы или папы.

C. Попробую найти бесплатную версию.

Вторым направлением нашего исследования было выявление отношения учителей к использованию элементов обучения для формирования кибербезопасного поведения младших школьников.

Цель: оценить отношение педагогов к использованию элементов обучения для формирования кибербезопасного поведения детей младшего школьного возраста.

Форма (ситуация оценивания): индивидуальное анкетирование педагогов.

Методика проводится в формате анкетирования.

Инструкция: Уважаемые педагоги! Просим Вас принять участие в анкетировании, цель которого – изучить ваше отношение к использованию элементов обучения для формирования кибербезопасного поведения младших школьников. Ваши честные и искренние ответы помогут нам получить объективные данные.

Материал: бланк анкеты.

Анкета:

1. Считаете ли вы проблему формирования кибербезопасного поведения у младших школьников актуальной для современной начальной школы?

A. Да, проблема очень острая, требует системной работы.

B. Скорее да, но это задача скорее всего для родителей, чем для школы.

C. Нет, в этом возрасте ещё рано говорить о серьезных киберугрозах.

2. Как часто вы включаете элементы обучения кибербезопасности в свою педагогическую деятельность?

A. Регулярно, использую для работы различные формы работы (классные часы, беседы, игры).

B. Эпизодически, в основном реагирую на конкретные случае, произошедшие накануне.

C. Кране редко, так как это не входит в обязательную программу.

D. Не занимаюсь этим вопросом.

3. Какие интерактивные формы работы для формирования кибербезопасного поведения вы использовали в своей практике? (возможно выбрать несколько вариантов)

A. Ролевые и деловые игры (например, обыгрывание ситуаций с мошенниками в сети).

B. Групповые проекты и исследовательские работы на тему безопасности в Интернете.

C. Интерактивные беседы и дискуссии с разбором конкретных ситуаций (кейсов).

D. Квизы, викторины, турниры по цифровой грамотности.

E. Привлечение специалистов (МВД, IT) для интерактивного обещания с детьми.

F. Не использую интерактивные формы, предпочитаю классические беседы-лекции.

4. Оцените эффективность интерактивных форм работы (игры, кейсы, дискуссии) по сравнению с традиционными методами (беседа, инструктаж) для младших школьников.

A. Интерактивные формы значительно эффективнее, дети лучше усваивают материал через практику.

B. Они примерно одинаково эффективны, главное – интересная тема.

C. Традиционные методы надёжнее, так как позволяют четко донести правила.

D. Затрудняюсь ответить.

5. Каких ресурсов или условий Вам не хватает для более активного использования интерактивных форм работы по кибербезопасности? (возможно выбрать несколько вариантов).

A. Готовых методических разработок и сценариев (игр, кейсов, квизов).

B. Времени на подготовку и проведение таких занятий.

C. Возможность приглашать специалистов (МВД и IT-экспертов).

D. Считаю, что у меня достаточно ресурсов.

2.2 Анализ и интерпретация результатов исследовательской работы

Первым направлением нашего исследования было выявление уровня сформированности кибербезопасного поведения младших школьников. В анкетировании приняли участие 25 учащихся 4 класса. Мы получили следующие результаты.

Отвечая на первый вопрос «Знаешь ли ты правила безопасности в Интернете» 14 учащихся ответили «да, я знаю, как вести себя в Интернете», 10 учащихся ответили «немного знаю, но не всё», 1 учащийся ответил «нет, я не знаю таких правил».

На второй вопрос «Что ты будешь делать, если незнакомый человек напишет тебе в социальной сети или в игре» 3 школьников ответили «отвечу, если он кажется добрым и вежливым», 16 школьников ответили «не буду отвечать и расскажу родителям», 6 школьников ответили «напиши грубость и заблокирую».

На третий вопрос «Как ты думаешь, можно ли сообщать свой домашний адрес, номер телефона или адрес школы новым друзьям из Интернета» 3 учащихся ответили «думаю, что можно сообщить, если ни хорошие», 13 учащихся ответили «нет, это опасно», 9 учащихся ответили «можно, если только очень доверяю им».

На четвертый вопрос «Ты получил(а) сообщение: «Твой друг / родственник в беде, срочно пришли деньги!» Что ты сделаешь?» 3 школьника ответили «переведу деньги, чтобы помочь», 10 школьников ответили «спрошу у родителей, правда ли это», 12 школьника ответили «напишу обратно: «Докажи, что это правда!»».

На пятый вопрос «Какой пароль лучше для защиты своего аккаунта» 7 учащихся ответили «123456 или дату своего рождения (легко запомнить)», 10 учащихся ответили «имя моего питомца (его знают только родные и близкие)», 8 учащихся ответили «случайные буквы, цифры и знаки (например, «Dk7!gA4»)».

На шестой вопрос «Если тебе в Интернете встретилось что-то страшное, непонятное или обидное, ты:» 15 школьника ответили «никому не скажу и постараюсь забыть, как можно быстрее», 8 школьника ответили «закрою и пойду

играть, переписываться дальше», 2 школьника ответили «обязательно расскажу родителям или учителю».

На седьмой вопрос «Можно ли открыть письма от незнакомцев с вложениями и ссылками» 4 учащихся ответили «да, если там интересное название», 15 учащихся ответили «нет, это может быть вирус», 6 учащихся ответили «открою, но, если только компьютер защищен».

На восьмой вопрос «Как часто ты рассказываешь родителям о том, что делаешь в Интернете?» 2 школьника ответили «всегда, мы это постоянно обсуждаем», 5 школьников ответили «иногда, если что-то непонятно», 18 школьников ответили «никогда, это мой секрет».

На девятый вопрос «Твой друг просит логин и пароль от игры, ты:» 16 учащихся ответили «дам, ведь он мой друг», 7 учащихся ответили «откажу, даже если обидится», 2 учащихся ответили «попрошу у родителей / учителя совета».

На десятый вопрос «Тебе посоветовали в Интернете игру, но для скачивания просят ввести номер банковской карты родителей. Твои действия?» 17 школьников ответили «введу, так как мне её посоветовали знакомые, она очень интересная», 3 школьников ответили «спрошу разрешения у мамы или папы», 5 школьников ответили «попробую найти бесплатную версию».

На основании ответов младших школьников мы можем сделать следующие выводы:

В информационном пространстве 68 % младших школьников подвержены киберугрозам и кибератакам.

Учащиеся владеют информацией о кибербезопасном поведении, но не в полной мере, чтобы защитить себя и свои данное от угроз в сети Интернет.

Проведенное анкетирование о кибербезопасном поведении детей младшего школьного возраста позволяет констатировать, что уровень кибербезопасной культуры учащихся, принявших участие в проведенном исследовании средний (наблюдается угроза появления небезопасного поведения в киберпространстве).

Наглядно результаты представлены на рисунке 1.

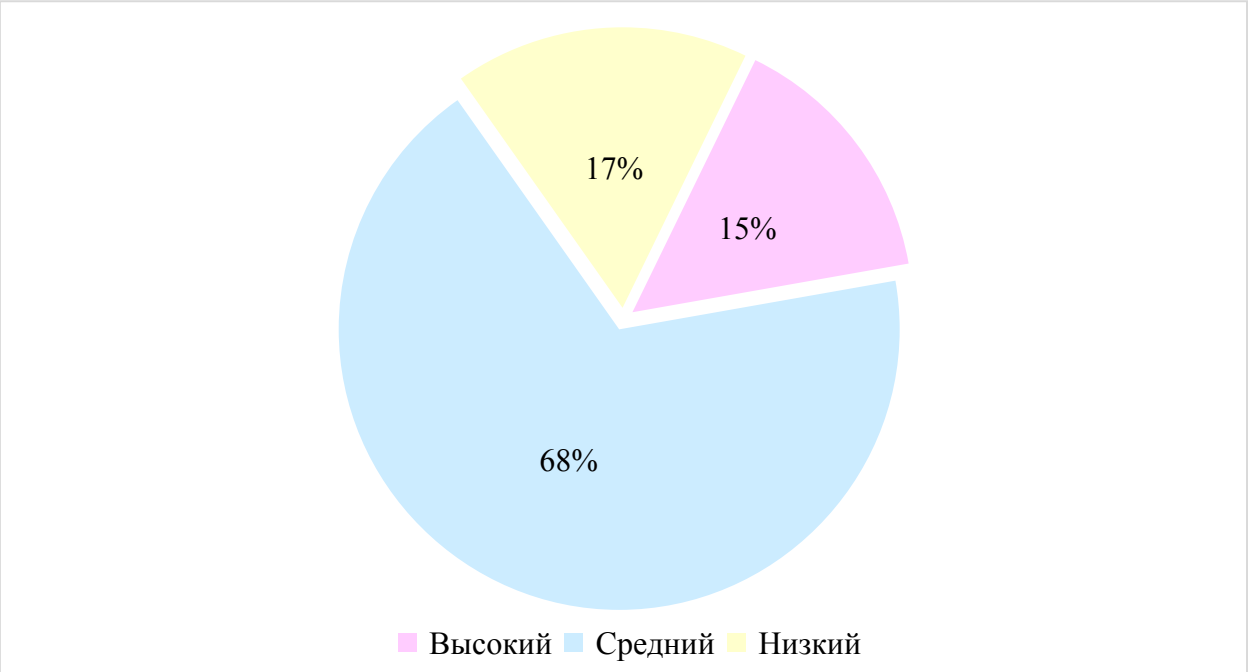


Рисунок 1 – Распределение испытуемых по уровню сформированности кибербезопасного поведения

Вторым направлением нашего исследования было выявление отношения учителей к использованию элементов обучения для формирования кибербезопасного поведения детей начальной школы. В анкетировании приняли участие 7 преподавателей начальных классов. Мы получили следующие результаты.

Отвечая на первый вопрос «Считайте ли вы проблему формирования кибербезопасного поведения к младшим школьникам актуальной для современной начальной школы» 7 педагогов ответили «да, проблема очень острая, требует системной работы», ни один педагог не выбрал вариант «скорее да, но это задача скорее всего родителей, чем для школы», ни один педагог не выбрал вариант «нет, в этом возрасте ещё рано говорить о серьёзных киберугрозах».

На второй вопрос «Как часто вы включаете элементы обучения кибербезопасности в свою педагогическую деятельность» 2 педагога ответили «регулярно, использую для работы различные формы работы (классные часы, беседы, игры)», 5 педагогов ответили «эпизодически, в основном реагирую на конкретные случае, произошедшие накануне», ни один педагог не выбрал вариант «не занимаюсь этим вопросом».

На третий вопрос «Какие интерактивные формы работы для формирования кибербезопасного поведения вы использовали в своей практике» позиция «ролевые и деловые игры (например, обыгрывание ситуаций с мошенниками в сети)» была выбрана 2 педагогами, позиция «групповые проекты и исследовательские работы на тему безопасности в Интернете» – не выбрана, позиция «интерактивные беседы и дискуссии с разбором конкретны ситуаций (кейсов)» выбрали 7 педагогов, позиция «квизы, викторины, турниры по цифровой грамотности» – 2 педагогами, позиция «привлечение специалистов (МВД, IT) для интерактивного общения с детьми» – не была выбрана, позиция «не использую интерактивные формы, предпочитаю классические беседы-лекции» – 1 педагог.

На четвертый вопрос «Оцените эффективность интерактивных форм работы (игры, кейсы, дискуссии) по сравнению с традиционными методами (беседа, инструктаж) для младших школьников» 5 педагогов ответили «интерактивные формы значительно эффективнее, дети лучше усваивают материал через практику», 2 педагога ответили «они примерно одинаково эффективны, главное – интересная тема», ни один педагог не выбрал «традиционные методы надежнее, так как позволяют четко донести правила», ни один педагог не выбрал «затрудняюсь ответить».

На пятый вопрос «Каких ресурсов или условий Вам не хватает для более активного использования интерактивных форм работы по кибербезопасности» позиция «готовых методических разработок и сценариев (игр, кейсов, квизов)» была выбрана 6 педагогами, позиция «времени на подготовку и проведение таких занятий» была выбрана 7 педагогами, позиция «возможность приглашать специалистов (МВД и IT-экспертов)» – 6 педагогов, позиция «считаю, что у меня достаточно ресурсов» – не выбрана.

На основании ответов педагогов мы можем сделать следующий вывод:

Учителя сталкиваются с рядом трудностей, включая нехватку времени на подготовку и проведение занятий, недостаток готовых методических разработок, а также проблему невозможности приглашать специалистов из МВД и IT. Эти

факторы приводят к тому, что 71,4 % педагогов нерегулярно включают элементы обучения кибербезопасности в свою педагогическую деятельность.

Наглядно результаты представлены на рисунке 2.

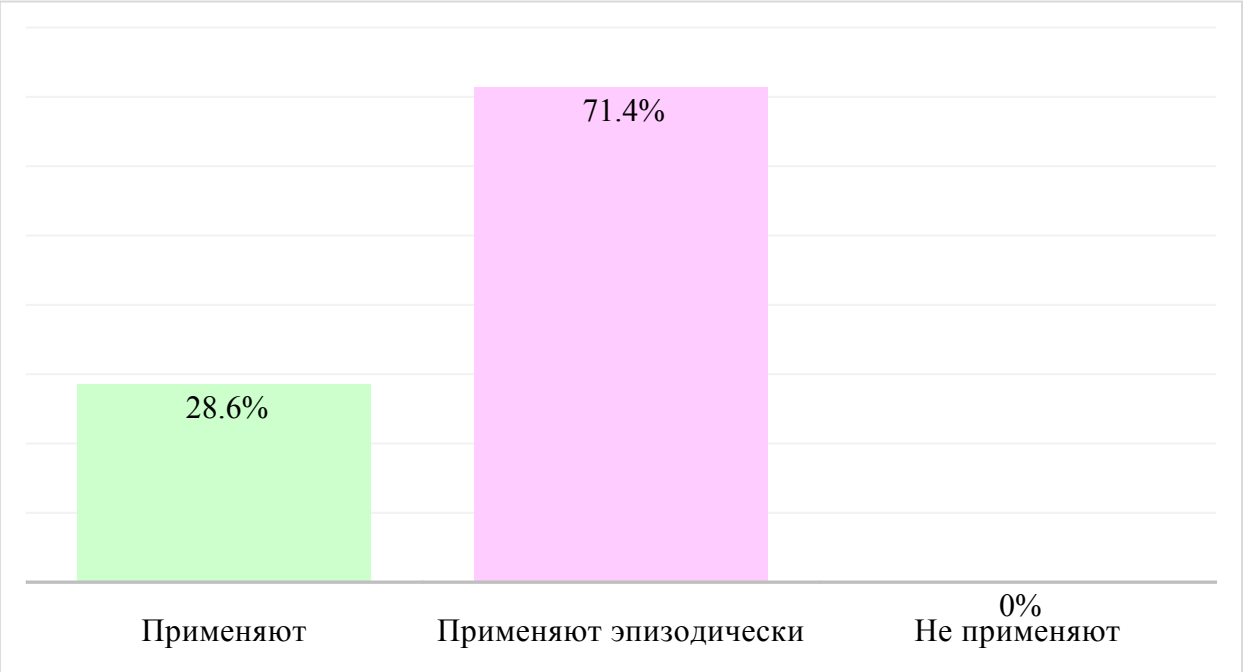


Рисунок 2 – Распределение отношения учителей к использованию элементов обучения для формирования кибербезопасного поведения детей начальной школы

Полученные нами результаты свидетельствуют о том, что необходимо создать «банк» методических материалов, направленных на формирование кибербезопасного поведения младших школьников.

2.3 Содержание «банка» методических материалов, направленных на формирование кибербезопасного поведения младших школьников

Целью является составление «банка» методических материалов, направленных на формирование кибербезопасного поведения младших школьников, которые могут быть использованы в практике учителя начальных классов.

Содержательное наполнение такого «банка» должно отвечать современным вызовам цифровой социализации, опираться на учёт возрастных особенностей детей младшего школьного возраста, включать разнообразные интерактивные

игры и предполагать активное вовлечение родителей как полноправных участников воспитательного процесса.

Первое направление работы по формированию кибербезопасного поведения – это совместная деятельность с младшими школьниками.

Игра по станциям «Цифровая ловкость»

Интегрированная игра, которая совмещает знания по информационной безопасности и физическую активность младших школьников. Участники делятся на команды, каждая команда проходит последовательно станции, зарабатывая баллы за правильные ответы и выполнение физических упражнений.

Правила:

1. Команды состоят из 4-6 человек;
2. Каждая команда получает маршрутный лист, где указаны порядок посещения станций, их название и местоположения.
3. Каждая станция включает задание на знание теории кибербезопасности и одно физическое упражнение.
4. За каждый верный ответ начисляется +1 балл команде.
5. После каждого задания участники выполняют физическое упражнения, зарабатывая дополнительные очки.
6. На прохождение одной станции отводится не более 3 минут.

Побеждает команда, набравшая наибольшее количество баллов.

Станция № 1: Пароли и шифры.

Задание: Какое правило составления пароля считается наиболее безопасным?

A. Использовать имя своего питомца.

B. Повторять один пароль для всех аккаунтов.

C. Применять длинные случайные комбинации букв, цифр и символов.

D. Записывать пароль на листочке рядом с компьютером.

Физическое упражнение: отжимания – столько раз, сколько участников в вашей команде.

Станция № 2: Кибермошенничество.

Задание: Какие признаки указывают на возможное мошенничество в Интернете?

A. Сайт запрашивает личные данные.

B. Предлагают быстрые деньги или подарки.

C. Все выше перечисленное верно.

D. Все выше перечисленное неверно.

Физическое упражнение: приседания – столько раз, сколько участников в вашей команде умноженное на два.

Станция № 3: Мифы о вирусах.

Задание: Верно ли утверждение: вирусы распространяются только через социальные сети?

A. Да, это правда.

B. Нет, вирус можно «поймать» и через другие источники (сайты, электронная почта, приложения).

C. Только при скачивании неизвестных файлов.

D. Антивирус всегда защитит меня, поэтому невозможно вирусам попасть на мой смартфон или компьютер.

Физическое упражнение: наклоны вперед – количество наклонов равняется возрасту младшего участника команды.

Станция № 4: Приватность в сети.

Задание: Что лучше всего предпринять, чтобы защитить личную информацию?

A. Регулярно проверять настройки конфиденциальности.

B. Устанавливать публичные профили везде, так ка хочу набрать популярность.

C. Постоянно делиться информацией о себе с друзьями.

D. Всё выше перечисленное.

Физическое упражнение: скручивания («пресс») – количество скручиваний равняется возрасту самого старшего участника команды.

Заключение игры.

Победители награждаются дипломами или небольшими призами. Остальные участники получают сертификаты участия.

Такая форма игры развивает командный дух, укрепляет физическое здоровье и формирует важные знания по кибербезопасности.

Интерактивный квест «Шпионские тайны»

Данный квест направлен на изучение основ защиты личных данных и конфиденциальности онлайн. Участники проходят ряд этапов, исследуя правила защиты персональных данных, распознавая риски в сети и соблюдая принципы конфиденциальности. Для перехода к следующему этапу каждой команде предстоит правильно отвечать на вопросы и успешно справляться с испытаниями.

I. «Тайный агент».

Команда получает зашифрованное послание с инструкциями о следующем пункте назначения. Чтобы расшифровать письмо, участникам необходимо разгадать кроссворд на тему «Безопасность данных».

Вопросы для этого этапа:

1. Как называется программа, защищающая компьютер от вирусов? (антивирус)
2. Чем опасна публикация фотографий документов в социальных сетях?
3. Назовите два типа вредоносных писем? (спам, фишинг)

Задание к переходу на следующий этап: переходить передвижными прыжками.

II. «Опасные следы».

Участникам предлагают серию картинок с изображениями различных ситуаций, связанных с нарушением безопасности в Интернете. Нужно выбрать наиболее опасные ситуации и объяснить причины своего выбора.

Примеры ситуаций:

1. Пользователь публикует фото паспорта.
2. Человек вводит данные карты на подозрительном сайте.
3. Кто-то выкладывает контактные данные друга в открытом доступе.

Задание к переходу на следующий этап: преодолеть полосу препятствий (например, пролезть через туннель или выбраться через верёвочную лестницу).

III. «Правильные решения».

Команда получает карточку с ситуацией, и им нужно принять решение, какое действие правильное в плане сохранения свой конфиденциальности. Важно, чтобы каждый участник высказал свое мнение.

Пример ситуации:

Вы получили письмо, в котором указано, что оно отправлено от администрации сайта, на котором зарегистрирован, с просьбой подтвердить пароль. Ваши действия?

1. Сразу введёте пароль.
2. Проверите достоверность письма через официальный сайт сервиса.
3. Проигнорируете письмо.
4. Попросите о помощи у родителей или учителя.

Задание к переходу на следующий этап: дойти гуськом.

IV. «Эстафета цифровых следов».

Команды участвуют в эстафете, в которой нужно передать друг другу конверт с секретным сообщением, избежав столкновений и повреждений содержимого. Конверт представляет собой метафору личной информации в сети Интернет.

Физическая активность данного этапа заключается в том, что участник бежит до определенной точки и обратно через различные препятствия (например, перепрыгивая бруски, обегая конусы, проходя по канату), аккуратно перенося конверт и не теряя его содержимое.

Завершающий этап: проверка полученных знаний.

Вопросы включают темы защиты личных данных, создание сложных паролей, методы борьбы с фековыми новостями.

Поведение итогов квеста. Победителями становится команды, которые быстро и правильно справились с заданиями. Призёры награждаются медалями,

дипломами и сертификатами, подтверждающими статус экспертов по защите личных данных.

Спектакль «Виртуальная опасность»

Цель: создание условий для воспитания культуры общения в социальных сетях.

Действующие лица:

1. А. – ученик, который активно пользуется социальными сетями.
2. Е. – подруга А., осторожная и ответственная в социальных сетях.
3. О. – одноклассник, распространяющий недостоверную информацию ради шуток.
4. Мама – ученика А.
5. Хакер – персонаж, который олицетворяет угрозы виртуального мира за кадром.
6. Учитель.
7. Ведущий.

Сцена № 1: Утро перед школой.

А.: «Ого! Я проснулся знаменитым! Посмотрите, сколько просмотров собрал мой пост!».

Е.: «Но там ведь твоя фотография с домашним адресом …».

А.: «Да, ладно тебе, ничего же страшного … Это забавно!».

О.: «Ага, забавно! Вот теперь посмотрим, кто первый взломает твою страницу и устроит розыгрыш!»

Хакер (за кадром): «Ха-ха-ха… Доверчивые дети попадутся прям в мои руки…»

Сцена № 2: Школа, перемена.

Учитель: «Дети, будьте внимательны! Если информация попадает в Интернет, вернуть её невозможно».

О.: «А., слышал новость? Твой кот съел мышеловку!»

А.: «Что?! Нет, конечно, нет!»

О.: «Да-да … Просто решил пошутить. Репостнул (повторно опубликовал) сообщение от какого-то незнакомца.»

Е.: «Ты понимаешь, что такие шутки могут испортить репутацию?»

Хакер (за кадром): «Отличный повод проверить систему защиты вашей страницы».

Сцена № 3: Дома вечером.

Мама: «А., почему твою страницу в социальной сети заблокировали? Что случилось?»

А.: «Ой, мама, я сам не понял… Просто вдруг исчезли все мои посты и комментарии…»

Мама: «Похоже, что кто-то воспользовался твоей доверчивостью и опубликовал ложную информацию. Теперь репутация испорчена, а доверие утрачено.»

Хакер (за кадром): «Следующий этап моего плана – сбор ваших личных данных…»

Сцена № 4: Комната А. поздно вечером – видеосвязь.

А.: «Почему я раньше не задумывался обо всё этом серьёзно? Ведь это действительно опасно …»

Е. (по видеосвязи): «Давай будем осторожнее. Важно помнить, что информация в сети остаётся навсегда. Даже удалённые посты могут сохраняться.»

А.: «Спасибо, Е. Завтра начну исправлять ситуацию. Удалю лишние фотографии, проверю настройки приватности, сменю пароли.»

Хакер (за кадром): «Хмм.. Этот парень стал умнее. Придется придумать новый способ атаки!»

Финал спектакля:

Все персонажи вместе выходят на сцену.

Ведущий: «Помните, друзья, что ваши поступки в социальной сети влияют на вашу жизнь и окружающих вас людей. Будьте аккуратны, думайте наперёд и берегите свою безопасность в цифровом пространстве!»

Игра-Квиз «Цифровой мир»

Игра состоит из нескольких раундов, где участники отвечают на вопросы, решают кейсы и проходят тесты. За каждое успешное прохождение раунда игроки получают баллы.

Ход игры:

Раунд 1: «Парольные замки».

Тип вопроса: открытые вопросы с несколькими вариантами ответов.

Задача: игроки выбирают категорию сложности (легко/средне/сложно) и отвечают на вопросы о создании надёжных паролей и принципах управления ими.

Примеры вопросов:

Легко: Сколько знаков рекомендуется иметь надежному паролю?

a) 6-8 знаков;

b) 8-12 знаков

c) Более 12 знаков;

d) Не имеет значения, главное его не забыть.

Средне: Как часто надо менять пароль к важным учетным записям?

a) каждые полгода;

b) каждые две-три недели;

c) один раз в месяц;

d) никогда, так как пароль и так уже сложный.

Сложно: Почему пароли вида «123456» / «Дружок» / «10.11.2012» считаются ненадежными?

a) Они короткие;

b) Их легко угадать – методом подбора;

c) Из-за редкого использования специальных символов (например, !,*,%);

d) Они состоят только из букв или цифр.

Раунд 2: «Социальные сети и приватность».

Тип вопроса: решение практических кейсов.

Задача: участникам предлагается набор жизненных ситуаций, связанных с общением в социальных сетях. Команды должны предложить наилучшее решение

исходя из принципов безопасности и этического поведения. Они также защищают своё решение и объясняют выбранные действия.

Примеры кейсов:

1. Вы выложили фотографию с прогулки, где видны номера машин соседей. Ваши действия?

2. Ваш знакомый попросил поделиться ссылкой на важный документ, находящийся в закрытом чате. Какие будут ваши действия?

3. Вы получили предложение дружбы от совершенного незнакомого человека. Что вы сделаете?

Раунд 3: «Тест на скорость».

Тип вопроса: быстрая серия простых вопросов.

Задача: за ограниченный промежуток времени (2 минуты) команды отвечают на максимально количество вопросов о базовых принципах кибербезопасности.

Примеры вопросов:

1. Что такое пароль?

2. Какие правила нужно соблюдать при выборе пароля? как часто нужно менять пароль?

3. Можно ли делиться своим паролем с друзьями?

4. Почему важно использовать сложные пароли?

5. Нужно ли сообщать своё Интернет-имя незнакомым людям?

6. Что делать, если получили подозрительное сообщение или письмо?

7. Зачем нужны антивирусные программа?

8. Как обезопасить свои личные данные в Интернете?

Завершение игры: подсчет очков, объявление победителя и вручение наград.

Классный час «Профилактика зависимости от компьютерных игр»

Цель: создать условия для формирования у детей младшего школьного возраста пользы и вреда компьютерных игр, развитие навыков самоконтроля и осознанного отношения к использованию компьютера.

Оборудование: компьютер для трансляции мультфильма и презентации, раздаточный материал.

Каждый учитель сам рассчитывает в какой момент лучше выдавать детали пазла.

Ход занятия:

1. Организационный этап

– Доброе утро! Сегодня мы поговорим об интересной теме. Нам прислали картинку, но, чтобы её рассекретить на нужно хорошо работать и за каждое выполненное задание у нас будет появляться одна часть от картинки. В конце мы увидим, что же там скрывалось. А чтобы узнать тему занятия мы сначала посмотрим мультфильм и потом обсудим его.

2. Вводная часть

Просмотр мультфильма «Маша и медведь», серия «Game over».

– Сейчас мы с вами просмотрели мультфильм, мы увидели с вами зависимость от игр – игроманию. Мишка стал агрессивным, начал плохо выглядеть, перестал со всеми общаться, а ещё Мишка не следил за своим домиком и все было разбросано. А почему так произошло?

– Всё верно. Маша и Зайчик пришли к Мишке, потому что сами не смогли разобраться, кто же будет играть следующим. Из-за этого Мишка сам увлёкся игрой и забыл про остальных. Как вы думаете, что же хорошего было показано в этой серии?

– Конечно, именно то, что Мишка подумал наперёд, представил, что же будет с ним и окружающими его друзьями, оценил последствия и понял, что игра – это не есть хорошо, он не стал играть. А позже и Маше с Зайчиком предложил подвижную игру на свежем воздухе, чему они были рады и с удовольствием побежали на улицу играть в хоккей.

– Подумайте и ответьте на вопрос «Почему многие любят играть в компьютерные игры»?

– Как вы думаете «Какие преимущества и недостатки есть в играх»? (запись на доске в два столбика по 3-5 пунктов на каждый критерий)

3. Основная и практическая часть.

– К нам пришло письмо от взволнованных родителей, в котором много неразрешённых проблем. Нас попросили помочь. Каждая группа получает ситуацию и вопрос. Нужно ответить на него.

Примеры ситуаций:

1. Петя играет каждый вечер перед сном в компьютерные игры и засыпает поздно. Утром он чувствует себя уставшим, а на уроках он бывает невнимательным. Вопрос: что можно сделать, чтобы Петя выспался и успевал играть в меру?

2. Катя стала много пропускать уроки и получать плохие оценки, потому что вечером сидит допоздна за смартфоном, играя в любимую игру. Родители ругают её за низкую успеваемость в школе. Вопрос: какие шаги должна предпринять Катя, чтобы совмещать учёбу и игры?

3. Миша проводит целый день дома, сидя за экраном ноутбука, забывая о прогулке на свежем воздухе и физических упражнениях. У него начались проблемы со зрением и осанкой. Вопрос: Как помочь Мише сохранить здоровье и поддержать баланс между играми и активностью?

4. Лиза раньше дружила со всеми ребятами в классе, ходила гулять, играла в подвижные игры. Но теперь она всё свободное время проводит одна – ей интереснее общаться с виртуальными персонажами и проходить уровни. Друзья обижаются, считая, что она забыла о настоящей дружбе. Вопрос: Почему важно уделять внимание друзьям и каким образом можно сочетать общение с ними и увлечение играми?

5. Коля начал тратить карманные деньги на покупки новых персонажей в игре и на их атрибуты. Теперь денег почти не остаётся даже на вкусности и развлечения вне компьютера. Вопрос: Нужно ли покупать вещи в играх и как разумнее распоряжаться деньгами?

– Мы послушали все ситуации, какие проблемы из них можно выделить? (потеря времени, проблемы с учёбой, потеря здоровья, плохие отношения с друзьями)

– Сейчас устроим небольшой батл по том материалу, который мы обсуждаем с начала урока, но батл будет необычным. Первый раунд – вам нужно в командах придумать другой группе кроссворд, после этого вы поменяетесь ими между собой и будете разгадывать кроссворд другой группы, далее отдаёте свой разгаданный кроссворд той команде, кто его составлял и сверяете ответы, оцените работу. В кроссворде нужно зашифровать не более 5 слов. На составление кроссворда у вас 7 минут, на разгадывание 3 минуты, на проверку 1 минута. Начинаем!

– Меняемся кроссвордами! Отгадываем ответы.

– Возвращаем себе свои составленные кроссворды и сверяете ответы! Скажите какая команда решала его и сколько правильных ответов у них получилось.

– Второй раунд! Каждая команда должна придумать занятия, которыми можно заменить время, проводимое за компьютерными играми, не менее 5. На работу 5 минут. После этого вы поочередно называете по одному придуманному занятию. Побеждает та команда, края назовет больше всего. Время пошло!

– Молодцы! Хорошо постарались. Сейчас мы станем настоящими учёными, которые создают один логотип, символизирующий вредность компьютерных игр. Для этого мы запускаем один лист бумаги, на котором каждый по очереди будет рисовать какой-либо элемент. Пока листок идет до вас или пока мы ждем последнего ученика, вы должны на отдельном листочке, который раздали, придумать загадку по нашему сегодняшнему уроку. Пример такой загадки вы увидите на экране:

Чёрный, но не уголь.
Открывается, но не книжка.
Светится, но не лампочка.
С клавишами, но не пианино.
(ноутбук)

– Посмотрите, какой красивый и познавательный логотип у нас получился. Прикрепим его к доске.

4. Подведение итогов.

– Мы поработали и собрали все элементы пазла. Теперь соберите его все вместе на первой парте. Посмотрите на нашу картинку на экране. Она символизирует наше занятия!

– Какой вывод мы можем сделать в завершение занятия?

– Таким образом, хотя компьютерные игры могут приносить радость и удовольствие, необходимо помнить о мере их использования и соблюдать правила безопасного пользования. Важно грамотно организовывать досуг, чередовать игровое время с физической активностью, чтением книг, занятием спортом и встречами с друзьями. Только тогда мы сможем гармонично развиваться и избегать возможных негативных последствий увлечением виртуальным миром.

5. Рефлексивная часть.

– Предлагаю разгадать несколько загадок, написанных вами.

– Поделитесь своим впечатление о сегодняшнем занятие.

– Занятие окончено. Всего доброго!

Цикл классных часов «Кибербезопасность»

1. «Наш дом – Интернет»

Цель занятия: создать условия для осознания и понимания, что Интернет похож на большой город, где действуют законы вежливости и доброты.

Этапы занятия:

1. Разминка «Приветствие виртуальных гостей». Младшие школьники приветствуют воображаемых Интернет-гостей и вспоминают правила хорошего тона.

2. Беседа «Что такое частная жизнь в Интернете». Учитель объясняет понятие частной жизни и говорит о том, почему нельзя публиковать чужие фотографии или личную информацию без разрешения.

3. Упражнение «Чужие границы». Детям младшего школьного возраста зачитываются ситуации (например, «Вы нашли разблокированный телефон друга. Там пришло сообщение от его мамы. Ваши действия?). Младшие школьники

предлагают свои действия и объясняют почему нужно поступить именно таким образом.

4. Творческое задание «Закрытый замок». Каждому ученику нужно нарисовать замок, который символизирует частную жизнь. Внутри замка обозначаются вещи, которые не вправе нарушать.

2. «Интернет-дружба против травли»

Цель занятия: создать условия для понимания «что такое травля в Интернете» и умения противостоять негативу.

Этапы занятия:

1. Упражнение «Правильно – неправильно». Учитель показывает сюжетные картинки с нарушением границ (размещение чужой фотографии, чтение чужих сообщений). У младших школьников две карточки: красная и зелёная. Они поднимают карточку после обсуждения увиденного, а затем каждый объясняет6 «Я бы так не сделал, потому что …». Учитель помогает и подсказывает детям правильные варианты поведения.

2. Вопросы для рассуждения «Проверь свои знания». Возможные вопросы:

- Можно ли называть кого-то неприятными прозвищами в комментариях и личных сообщениях?
- Правильно ли делиться чужими фотографиями, даже если кажется это смешным?
- Что делать, если увидел издевательство над другими ребятами в школе или социальных сетях?

3. Практическое задание «Я умею помогать». Младшие школьники составляют план действий, как поддержать друга, которого начали обижать в сети Интернет.

3. «Верно-неверно: Ответственность за информацию»

Цель занятия: создать условия для умения отличать правду от вымысла.

Этапы занятия:

1. Упражнение «Кто прав». Дети младшего школьного возраста просматривают реальные примеры размещения ложно информации в киберпространстве. Далее рассуждают, как такая информация влияет на других людей.

2. История с продолжением «Сказка про ложную информацию». Учитель рассказывает историю про мальчика, разместившего в Интернете неправдивую информацию о другом ребенке. Младшие школьники продолжают сюжет и пытаются исправить ситуацию.

3. Кроссворд «Честность». Дети младшего школьного возраста разгадывают термины, связанные с ответственностью за контент в сети Интернет (например, правда, информация, комментарии, честность).

4. Изготовление листовок «Будь честным». Младшие школьники создают небольшие буклеты с советами, как избежать распространения недостоверной информации.

Второе направление работы по формированию кибербезопасного поведения – это взаимодействие с родителями младших школьников.

Формирование кибербезопасного поведения младших школьников строится на принципе «доверительные и доброжелательные отношения» со взрослыми. Стоит отметить, что невозможно полностью оградить детей младшего школьного возраста от киберпространства, однако возможно превратить его цифровую среду в контролируемое и безопасное использования сети Интернет. Самое необходимое – это регулярное родительское участие в онлайн-жизни младшего школьника.

Родительское собрание «Кибербезопасность младших школьников в киберпространстве»

Цель: создать условия для понимания родителями о важности киберугроз и кибератак для необходимости формирования у младших школьников навыков кибербезопасности.

Задачи:

1. Огласить существенные риски для детей младшего школьного возраста в сети Интернет.

2. Рассказать о правилах контроля.

Ход выступления:

1. Вступительное слово.

– Уважаемые родители! Современные дети не представляют свою жизнь без использования смартфонов, компьютеров и выходов в сеть Интернет. Однако их доверчивость в информационном пространстве может стать объектом для мошенников, людей, которые настроены против ребёнка и опасного, незащищенного контента. Сегодня рассмотрим угрозы младших школьников и как из пребывания может стать безопасным в киберпространсте.

2. Основная часть.

– Существуют три главные угрозы:

1) нежелательный контент, то есть это может быть пугающее видео, сцены насилия, «взрослые» рекламные баннеры (реклама о запрещенных веществах);

2) общение с незнакомцами, например, в играх просят пароль, имя, личный адрес, присылают ссылки;

3) цифровые покупки, таким образом, ребёнок случайно или намеренно тратит денежные средства с банковских карт родителей для виртуальной валюты, приобретения персонажей или атрибутов для него, а также попадаются в мошеннические схемы.

– Важно понять, что данный возраст детей не способен оценить атаки злоумышленников, достаточно часто младшие школьники верят, что выиграли смартфон и переходят по неизвестным ссылкам.

– Предлагаю ответить на несколько простых вопросов в анонимной анкете (приложение 1). После этого обсудим результаты.

– По результатам анкеты, стоит сделать вывод, что нужно больше внимания уделять ребёнку, который пользуется Интернетом, без присмотра

и контроля взрослых. Есть четыре простых правила, которые можно внедрять уже сейчас: сделать во всех учетных записях детский профиль; объяснить ребёнку, что никто не может просить у него код из СМС или номера карт родителей; безопасный просмотр видеороликов, например, включить функцию «только проверенный контент для детей»; всегда договариваться с ребёнком, не нужно ставить ультиматумы, то есть проводимое время за гаджетом – это не наказание и не награда, а также ребёнок в свою очередь обещает не отвечать незнакомцам, не открывать различные ссылки и не ставить пароли без вашего участия.

– Разберём несколько кейсов для обсуждения. Желающие вытягивают листок с ситуацией, зачитывает, говорит свой вариант разрешения ситуации, а остальные пожеланию добавляют своё мнение по данной ситуации.

Кейс 1. Ребёнок в знаменитой игре получает сообщение от неизвестного игрока, который предлагает бесплатные артефакты за пароль от аккаунта. Как вы научите ребенка реагировать на подобные сообщения?

Кейс 2. Ребёнок случайно открыл какое-либо страшное для него видео и заплакал. Ваши действия?

Кейс 3. Ребёнок попросил вас подтвердить кодом покупку персонажа. Ваш алгоритм действий?

– Вы предложили оптимальные и безопасные варианты для детей в разрешение подобных ситуаций. Можно озвучить список тех пунктов, которые стоит применять регулярно для безопасного использования детьми сети Интернет: ежедневно проверять историю запросов в информационной сети; научить ребёнка постоянно спрашивать у взрослых совета и регулярно рассказывать о страшном и непонятном; обучить вежливому общению в Интернете; объяснять ребёнку, что не стоит разглашать личные данные.

– Готова выслушать ваши вопросы и с удовольствием на них ответить.

– Дорогие родители! Технический прогресс полностью окружает нашу жизнь, поэтому мы можем только научить ребёнка пользоваться

Интернетом во благо, без нанесения вреда для него. Начинайте постепенно применять правила, о которых сегодня говорили. Спасибо за внимание!

Третье направление работы по формированию кибербезопасного поведения – это предоставление информации.

Обеспечение кибербезопасного поведения детей младшего школьного возраста в цифровом пространстве – одна из ключевых задач современного воспитания. Стоит учитывать возрастающую роль киберпространства в жизни каждого ребёнка, родителям необходимо вовремя овладеть знаниями, которые помогут обеспечить кибербезопасность младшего школьника в условиях цифровых технологий. Для этого подобран ряд памяток, направленных на повышение уровня цифровой грамотности семьи. Эти материалы помогут взрослым лучше понимать риски информационной сети и научить младшего школьника грамотно пользоваться Интернет-ресурсами (приложение 2).

Выводы по главе 2

Таким образом, для определения уровня кибербезопасного поведения младших школьников и отношение педагогов к использованию элементов обучения по формированию кибербезопасного поведения детей начальной школы были проведены анкетирования на базе МАОУ средней общеобразовательной школы в г. Златоуст. В исследовании принимали участие 25 учащихся 4 класса и 7 преподавателей начального общего образования.

Проанализировав данные, полученные в ходе проведенного исследования в 4 классе, мы смогли определить уровень кибербезопсногоо поведения младших школьников. По результатам анкетирования можно говорить о том, что наблюдается угроза появления небезопасного поведения в киберпространстве, а именно – у 68 % испытуемых, у таких младших школьников проявляются критерии: общение с незнакомцами в сети, сообщение о личном адресе или номере телефона, перевод денежных средств без выяснения нюансов, открытие писем с вложениями и ссылками от незнакомых источников, способны ответить

грубостью на грубость и не готовы делиться проблемами, с которыми сталкиваются в сети Интернет.

А также мы выявили, что 71,4 % учителей начальной школы, в которой проводилось исследование, редко применяют элементы обучения кибербезопасности в профессиональной деятельности. По итогам исследования, мы пришли к необходимости составления «банка» методических материалов, направленных на формирование кибербезопсного поведения младших школьников.

ЗАКЛЮЧЕНИЕ

В ходе изучения теоретических аспектов деятельности учителя по формированию кибербезопасного поведения младших школьников мы рассмотрели понятие и специфику кибербезопасного поведения детей младшего школьного возраста, а также направления деятельности учителя начальных классов по формированию кибербезопасного поведения младших школьников и вывили, что безопасность в сети Интернет означает использование информационных ресурсов без риска для личности. Кибербезопасные навыки младших школьников включают умение правильно обращаться с цифровыми устройствами и эффективно, без вреда искать нужную информацию. Младший школьный возраст оптимален и благоприятен для формирования основ кибербезопасного поведения. Это связано с началом активного взаимодействия детей с информационными технологии, уязвимостью, наивностью. Кибербезопасное поведение предполагает использование проверенных источников, защиту личных данных и создание надёжных паролей. Формирование культуры информационной безопасности должно включать образовательную работу и участие родителей в создание кибербезопасности младших школьников. Важно разработать актуальные методические материалы, способствующие развитию необходимых навыков.

Во второй главе «Практические аспекты деятельности учителя по формированию кибербезопасного поведения младших школьников» с помощью двух анкет рассмотрены уровень сформированности кибербезопансого поведения младших школьников и уровень отношения педагогов к использованию элементов обучения для формирования кибербезопасного поведения детей младших классов. Мы выявили, что в 4 классе у большинства младших школьников замечена угроза проявления небезопасного поведения в киберпространстве, а именно – у 68 % испытуемых. Также мы определили, что 71,4 % учителей младших классов обращаются к вопросам кибербезопасности редко в своей педагогической практике. В параграфе 2.3 мы представили

содержание «банка» методических материалов, направленных на формирование кибербезопасного поведения младших школьников.

Исходя из вышеизложенного можно сделать вывод, что формирование навыков кибербезопасности в начальной школе не только защищает младших школьников в цифровом пространстве, но и способствует их успешной адаптации в современном мире.

Таким образом, цель нашей работы достигнута, задачи решены.

Дальнейшим направление исследования могут стать создание и проверка результативности программы работы классного руководителя, направленной на формирование кибербезопасного поведения младших школьников.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Аверкиев А. А. Кибербезопасность виды и методы / А. А. Аверкиев, Д. А. Камбулов // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2022. – № 1. – С. 567–574.

2. Баранов А. П. Актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения / А. П. Баранов // Вопросы кибербезопасности. – 2015. – №1 (9). – С. 2–5.

3. Без конфликтов и ззапретов : 5 правил, которые помогут защитить ребенка в интернете – URL: https://clck.ru/3TEJXV (дата обращения: 17.04.2026).

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

5. Бородакий Ю. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2) / Ю. В. Бородакий, А. Ю. Добродеев // Вопросы кибербезопасности. – 2014. № 1 (2). – С. 5–12.

6. Взрослые и дети в интернете: аналитический отчет – URL: https://clck.ru/3T9sVz (дата обращения 02.12.2025).

7. Виноградский С. Н. Основы кибербезопасности : учебное пособие. 5 – 11 классы / С. Н. Виноградский. – Москва : Дрофа, 2019. – 238 с. – ISBN 978-5-358-22190-1.

8. Воробьева К. И. Психологические ресурсы кибербезопасности человека / К. И. Воробьева, М. В. Долгачев, Д. А. Заславский // «Социальные и гуманитарные науки на Дальнем Востоке». – 2020. – Т. 17 (4). – С. 150–157.

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

10. Джаббарова К. Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз / К. Ф. Джаббарова // АНИ: экономика и управление. – 2017. – № 2 (19). – С. 232–326.

11. Згоба А. И. Кибербезопасность: угрозы, вызовы, решения / А. И. Згоба, М. Д. Маркелов, П. И. Смирнов // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 30–38.

12. Информационная безопасность URL: https://clck.ru/3TEJYa (дата обращения: 17.04.2026).

13. Исаев С. В. К вопросу о кибербезопасности научно-образовательного учреждения / С. В. Исаев // Решетневские чтения. – 2013. – № 17. – С. 292–294.

14. Как обеспечить безопасность сайта URL: https://wishescards.ru/kak/obespechit/bezopasnost/sayta/?utm_medium=organic&utm_source=yasmartcamera (дата обращения: 17.04.2026).

15. Калач А. В. Современные технологии формирования культуры кибербезопасности / А. В. Калач, А. С. Кравченко // Ведомости УИС. – 2019. – № 11 (210). – С. 26–30.

16. Калинченко А. В. Использование сетевых образовательных технологий в процессе формирования информационной культуры младших школьников / А. В. Калинченко, Д. Ю. Калинченко // Психолого-педагогический журнал «Гаудеамус». – 2020. – Т. 19. – № 3 (45). – С. 31–36.

17. Калинченко Д. Ю. Организация работы по формированию информационной культуры младших школьников / Д. Ю. Калинченко // Азимут научных исследований: педагогика и психология. – 2021. – № 2 (5). – С. 139–142.

18. Куксова А. И. Как педагог-психолог помогает младшим школьникам стать ответственными пользователями интернета: основы киббербезопасности. – URL: https://sibac.info/studconf/hum/cxxxix/337676 (дата обращения: 18.10.2025)

19. Лопатин Д. В. Проблема безопасности школьников в сети Интернет / Д. В. Лопатин, Н. Л. Королева, М. С. Анурьева, Я. М. Пузанова, К. И. Остапчук // Вестник российских университетов. Математика. – 2017. – № 1. – С. 232–236.

20. Мазоха Д. А. История развития искусственного интеллекта в СССР в области информационной безопасности / Д. А. Мазоха, М. А. Ефремов // Современные информационные технологии и информационная безопасность. – 2024. – С. 90–94.

21. Миллер Н. В. Использование нейросетей в современном образовательном процессе: проблемы и перспективы / Н. В. Миллер // Информационные технологии и информационная безопасность в профессиональной деятельности : III Межвузовская научно-практическая конференция с международным участием. Новосибирск : Новосибирский военный ордена Жукова институт имени генерала армии И. К. Яковлева войск национальной гвардии Российской Федерации, 2024. – С. 100–105.

22. Петрова Н. Ф. Подготовка будущих практических психологов к работе с учащимися, склонными к интернет-зависимости / Н. Ф. Петрова // Мир науки, культуры, образования. – 2017. – № 3(64). – С. 288–290.

23. Правила безопасности для детей в интернете – URL: https://www.sberbank.ru/ru/person/cybersecurity/cyberkids/five_rules?ysclid=mo2u0t5znk305113859 (дата обращения: 17.04.2026).

24. Правила защиты информационных данных URL: https://clck.ru/3TEJNJ (дата обращения: 17.04.2026).

25. Пучкова Д. А. Формирование основ безопасного поведения при работе с интернет-средой у детей младшего школьного подросткового возраста / Д. А. Пучкова // Вестник ГУУ. – 2015. – № 11. – С. 333–336.

26. Ревенков П. В. Кибербезопасность в условиях Интернет вещей и электронного банкинга / П. В. Ревенков, А. А. Бердюгин // Национальные интересы : приоритеты и безопасность. – 2016. – № 11 (344). – С. 158–169.

27. Родионова В. М. Развитие кибербезопасности в эпоху цифровизации: образование в области кибербезопасности для эффективной защиты / В. М. Родионова, В. В. Козлов // Наука и образование в современных условиях : материалы Международной (заочной) научно-практической конференции. – Нефтекамск : Научно-издательский центр «Мир науки», 2023. – С. 41–48.

28. Сергеева Б. В. Формирование информационной культуры младших школьников / Б. В. Сергеева, И. В. Козырева // Молодой ученый. – 2016. – № 11 (115). – URL: https://moluch.ru/archive/115/30521?ysclid=moa4wpw221923612573 (дата обращения 16.01.2026).

29. Синица С. А. Киберугрозы цифровой экономики России / С. А. Синица // Экономика и бизнес: теория и практика. – 2023. – № 11-3(105). – С. 65–70.

30. Староверова М. В. Формирование у младших школьников модели безопасного поведения / М. В. Староверова, Д. Д. Мосинцев, И. М. Блинцова // Проблемы современного педагогического образования. – 2022. – № 76-1. – С. 277–280.

31. Тачмухаммедов А. Кибербезопасность в образовании: как защитить учащихся и образовательные организации / А. Тачмухаммедов, И. Ашыров, М. Гельдыева // Международный научный журнал «Всемирный ученый». – 2023. – № 7 (1). – С. 133–137.

32. Фасенко Т. Е. Информационная безопасность при использовании современных технологий / Т. Е. Фасенко // Информационные технологии и информационная безопасность в профессиональной деятельности : III Межвузовская научно-практическая конференция с международным участием. Новосибирск : Новосибирский военный ордена Жукова институт имени генерала армии И. К. Яковлева войск национальной гвардии Российской Федерации, 2024. – С. 148–151.

33. Федеральный закон от 29.12.2010 n 436-фз (ред. от 29.12.2025) «О защите детей от информации, причиняющей вред их здоровью и развитию» – URL: https://clck.ru/3t9tlu (дата обращения: 25.10.2025).

34. Фигуровская Ю. Е. Искусственный интеллект и информационная безопасность / Ю. Е. Фигуровская // Информационные технологии и информационная безопасность в профессиональной деятельности : III Межвузовская научно-практическая конференция с международным участием. Новосибирск : Новосибирский военный ордена Жукова институт имени генерала

армии И. К. Яковлева войск национальной гвардии Российской Федерации, 2024. – С. 151–156.

35. Челышева И. В. Кибербезопасность школьников в интернет-пространстве и проблемы семейного медиаобразования / И. В. Челышева // Международный информационно-аналитический журнал «Crede Experto: транспорт, общество, образование, язык». – 2016. – № 4 (11).

36. Челышева И. В. Стратегии развития медиакомпетентности подрастающего поколения в России / И. В. Челышева, И. А. Козаченко-Габрава // Российский журнал истории, теории и медиапедагогики. – 2013. – № 4. – С. 59–66.

ПРИЛОЖЕНИЕ 1

Анкета для родителей младших школьников.

1. Есть ли у вашего ребёнка собственный, личный гаджет с выходом в Интернет?

□ Да

□ Затрудняюсь ответить

□ Нет

2. Знаете ли Вы пароли от его социальных сетей и прочих учетных записей?

□ Да

□ Затрудняюсь ответить

□ Нет

3. Используете ли Вы родительский контроль?

□ Да

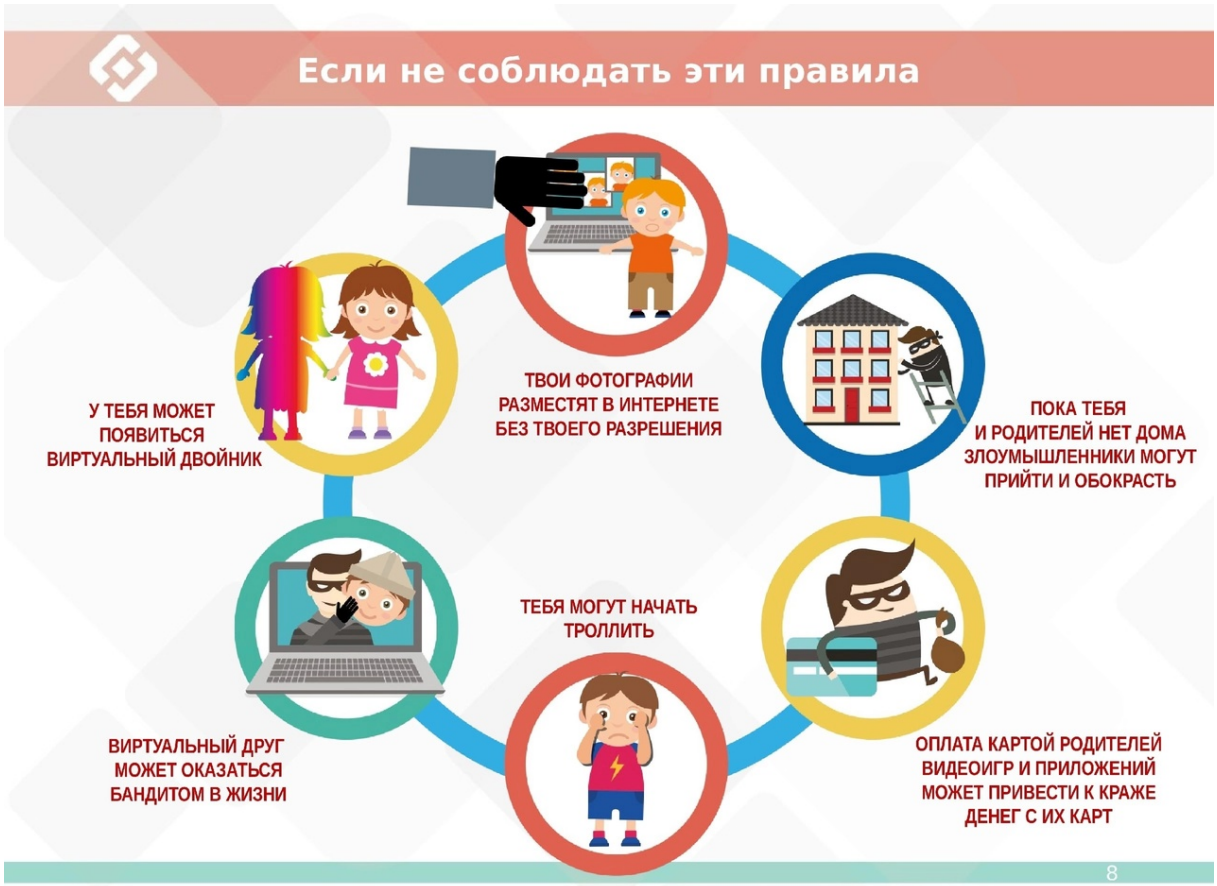
□ Нет

4. Следите ли Вы за историей просмотра вашего ребёнка?

□ Да

□ Нет

ПРИЛОЖЕНИЕ 2




ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ
рассказывай родителям, если у тебя есть страхи, связанные с Интернетом
не поддавайся на заманчивые предложения в Интернете
помни, совершая покупки в Интернете ты тратишь реальные деньги
не оставляй в публичном доступе и не отправляй незнакомцам при общении с ними свою контактную информацию или номер банковской карты
не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Сообщи родителям, если друзья из Интернета настаивают на встрече
не переходи по ссылкам в сообщениях от незнакомых адресатов. Не открывай спам-сообщения
не публикуй информацию, которая в будущем сможет скомпрометировать тебя или твоих знакомых
ИНФОРМАЦИЯ, КОТОРУЮ НЕ СЛЕДУЕТ РАЗМЕЩАТЬ НА СТРАНИЦАХ СОЦИАЛЬНЫХ СЕТЕЙ
О СВОЕМ МЕСТОПОЛОЖЕНИИ
О ПЛАНАХ НА ДЛИТЕЛЬНЫЕ ПОЕЗДКИ
ФОТО ДОРОГИХ ВЕЩЕЙ И ПОДАРКОВ
ФОТО КВАРТИРЫ ИЛИ ДОМА
СВОЙ ДОМАШНИЙ АДРЕС
ФОТО ЛИЧНЫХ ДОКУМЕНТОВ