МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Балашовский институт (филиал)

Кафедра физической культуры и безопасности жизнедеятельности

ФОРМИРОВАНИЕ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ У ОБУЧАЮЩИХСЯ В СРЕДНЕМ ШКОЛЬНОМ ВОЗРАСТЕ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 5 курса 354 группы
направления подготовки 44.03.05 «Педагогическое образование» (с двумя профилями подготовки),
профилей «Физическая культура. Безопасность жизнедеятельности»,
психолого-педагогического факультета
Судоргина Никиты Ефимовича

Научный руководитель
доцент кафедры физической культуры и безопасности жизнедеятельности,
кандидат педагогических наук
доцент _____ О.В. Бессчетнова
(подпись, дата)

Зав. кафедрой физической культуры и безопасности жизнедеятельности
кандидат педагогических наук,
доцент_____ А.В. Викулов
(подпись, дата)

Балашов 2026

ВВЕДЕНИЕ

Актуальность исследования. Информационные технологии проникают во все сферы жизни, включая образование, создавая новые возможности и вызовы. Учащиеся становятся активными участниками информационного процесса, что требует навыков безопасного и эффективного использования информации.

Формирование основ информационной безопасности у обучающихся среднего школьного возраста — актуальная задача для образовательных учреждений, родителей и общества.

Средний школьный возраст — период активного формирования личностных качеств, социальных навыков и когнитивных способностей, когда важно обеспечить знаниями о рисках и безопасном поведении.

Информационная безопасность включает технические, этические, правовые и социальные аспекты, важные для ответственного поведения в сети. Стремительное развитие цифровых технологий и увеличение угроз в информационном пространстве делают вопросы защиты личной информации особенно важными для школьников.

Теоретические аспекты помогают понять механизмы формирования осознанного отношения к информационной безопасности; практические методики обеспечивают эффективные инструменты внедрения; оценка эффективности позволяет выработать рекомендации для педагогов и образовательных учреждений

Цель исследования — разработка практических рекомендаций по формированию информационной безопасности обучающихся.

Объект исследования — учебно-воспитательный процесс в образовательной организации.

Предмет исследования — формирование основ информационной безопасности у обучающихся среднего школьного возраста.

Задачи исследования:

1. Проанализировать состояние проблемы формирования информационной безопасности у обучающихся в образовательной организации.

2. Подобрать диагностический инструментарий и определить уровень сформированности информационной безопасности обучающихся 8 класса.

3. Разработать методические рекомендации для обучающихся по правилам безопасного поведения в сети Интернет.

Методы исследования: — теоретический — анализ педагогической, психологической литературы; сравнение, обобщение, систематизация с целью уточнения содержания основных концепций и обоснования теоретических основ исследования; анализ методической документации школы для исследования наличия компонента по формированию информационной безопасности;

— эмпирические — опрос, тестирование, педагогическое моделирование, педагогический эксперимент, состоящий из трех этапов: констатирующий, формирующий, контрольный — для определения уровня сформированности информационной безопасности обучающихся 8 класса и проверки эффективности применяемых методов обучения по формированию информационно безопасности в образовательном процессе предмета ОБЗР;

— методы математической статистики для обработки полученных данных.

Структура работы: Работа состоит из введения, двух глав, заключения, списка использованных источников, включающего 23 наименования, приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе **«Теоретические аспекты формирования информационной безопасности у обучающихся в среднем школьном возрасте»** рассмотрены сущность и определение понятия «информационная безопасность», роль и значение информационной безопасности в современном обществе, классификация основных угроз в подростковой среде, а также принципы формирования информационной безопасности у детей среднего школьного возраста.

Понятие «информационная безопасность» носит сложный междисциплинарный характер и системно изучается с технической, правовой и педагогической позиций. Технический подход концентрируется на защите аппаратных средств и данных от несанкционированного доступа. Правовой подход закреплён в Федеральном законе № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Доктрине информационной безопасности Российской Федерации, где безопасность трактуется как состояние защищённости личности, общества и государства от информационных угроз. Педагогический подход, наиболее значимый для школы, фокусируется на формировании внутренних механизмов защиты самого обучающегося. Как отмечает Г. У. Солдатова, внешние запреты эффективны лишь до определённого возраста, а главным фактором безопасности становится личная цифровая компетентность.

В рамках педагогического осмысления используется категория «культура информационной безопасности личности» — интегративное качество, включающее ценности, знания, умения и устойчивые поведенческие паттерны для безопасного взаимодействия с информацией. Важно разграничить это понятие со смежными: цифровая грамотность (технические навыки), медиаграмотность (анализ контента), информационная гигиена (правила поведения), кибербезопасность (техническая защита устройств).

Роль информационной безопасности в современном обществе носит стратегический характер. Подростки проводят в сети более четырёх часов в

сутки, при этом лишь 14% российских пятнадцатилетних школьников способны надёжно отличать факты от мнений в медиасообщениях (данные PISA-2022). Доля детей, сталкивающихся с опасным контентом, достигает 38%. Цифровая среда стала естественным пространством обитания, что кардинально меняет механизмы социализации.

Классификация основных угроз информационной безопасности в подростковой среде включает четыре группы: угрозы психическому развитию и эмоциональному благополучию (кибербуллинг, треш-стримы, шок-контент); угрозы мировоззрению и гражданской идентичности (фейки, пропаганда, вербовка в деструктивные сообщества); угрозы физическому и интеллектуальному здоровью (интернет-зависимость, клиповое мышление); угрозы личности и приватности (фишинг, кража данных, кибергруминг). Отдельно выделяются технологии манипуляции сознанием: кликбейтные заголовки, дипфейки, алгоритмические «информационные пузыри». Средний школьный возраст (11—15 лет) является периодом максимальной уязвимости в силу кризиса, лабильности эмоциональной сферы и незавершённости формирования критического мышления.

Принципы формирования информационной безопасности у детей опираются на фундаментальные дидактические концепции И. Я. Лернера и В. В. Краевского. Ключевые принципы: возрастосообразность, системность, связь с жизнью. Целевая модель безопасного поведения включает три компонента: знаниевый (когнитивная основа), деятельностный (практические умения) и ценностный (смыслообразующий). Реализация модели невозможна без активного включения семьи как полноправного партнёра школы, поскольку 61% родителей не знают, на какие сайты заходит их ребёнок, а 47% никогда не беседовали с ним о правилах поведения в сети. Формирование информационной безопасности — это не технический инструктаж, а воспитательный процесс развития критического мышления и общей культуры личности.

Во второй главе **«Практические подходы и оценка эффективности формирования информационной безопасности учащихся»** описываются организация эксперимента и его результаты.

Исследование проходило на базе Муниципального общеобразовательного учреждения «Гимназия № 1» г. Балашова Саратовской области в 2025—2026 учебном году. В нем приняли участие обучающиеся 8-го класса в количестве 24 человек (возраст 14—15 лет).

Задачей констатирующего этапа являлось определение исходного уровня сформированности информационной безопасности по трём критериям: когнитивному, поведенческому и эмоционально-ценностному.

Методиками исследования выступали:

1. **Комплексная диагностика когнитивного критерия** — авторская анкета «Оценка рисков в сети» и адаптированный тест на медиаграмотность (бинарная оценка: 1 балл — верно, 0 — неверно).
2. **Практические кейс-задания для оценки поведенческого критерия** (моделирование реальных действий): задание на выбор легитимного сайта и задание на распознавание фишингового письма от имени администрации школы. Каждое задание оценивалось по 2-балльной системе.
3. **Диагностика эмоционально-ценностного критерия** — методика «Незаконченные предложения» и шкала цифровой эмпатии (5 утверждений, оценка от 1 до 5).

Для интерпретации результатов были установлены трехуровневые критерии: высокий уровень (80—100% правильных ответов), средний (60—79%), низкий (0—59%).

Результаты констатирующего этапа представлены в таблице 1.

Таблица 1. — Уровень сформированности информационной безопасности обучающихся на констатирующем этапе

Уровень	**Количество обучающихся (%)**
Низкий	54,2% (13 чел.)

Уровень	Количество обучающихся (%)
Средний	29,1% (7 чел.)
Высокий	16,7% (4 чел.)

Анализ показал, что более половины восьмиклассников находятся на низком уровне. Выявлены конкретные дефициты: 67% не смогли аргументированно указать признаки фейковой новости; 58% допустили ошибку при выборе легитимного сайта (перешли по фишинговой ссылке); 46% согласились перейти по ссылке из письма «администрации», а 33% ввели бы логин и пароль; 63% занимают позицию пассивного наблюдения при кибербуллинге. Констатирующий этап подтвердил наличие разрыва между теоретическими знаниями и практическими умениями.

На формирующем этапе был разработан и реализован комплекс методических материалов, направленный на повышение уровня компетентности в области информационной безопасности. Работа организована в рамках внеурочной деятельности. Участие школьников было добровольным. Использовались интерактивные формы: кейс-метод, практикумы, деловые и настольные игры, веб-квесты, формы работы с семьёй.

В рамках исследования проведено 5 мероприятий. Тематическое планирование представлено в таблице 2.

Таблица 2. — Тематическое планирование занятий, направленных на формирование у восьмиклассников компетентности в области информационной безопасности

№	Мероприятие	Цель
1	Кейс-практикум «Цифровой след»	Развить понимание того, как публичная информация формирует цифровой портрет, выявить уязвимости профиля и освоить навыки настройки приватности.
2	Практикум по распознаванию манипуляций «Анатомия кликбейта»	Сформировать алгоритм фактчекинга, научить выявлять признаки фейковых новостей и манипулятивных заголовков.

№	Мероприятие	Цель
3	Деловая игра «Кибер-Щит»	Отработать навыки реагирования на комплексную киберугрозу, развить умения быстрого анализа и принятия решений.
4	Настольная игра «Кибер-патруль»	В игровой форме закрепить правила цифровой гигиены, сформировать устойчивые поведенческие реакции на типовые онлайн-угрозы.
5	Мастер-класс для родителей «Настройка родительского контроля и безопасной цифровой среды»	Обучить родителей практическим приёмам ограничения нежелательного контента, контроля экранного времени и организации доверительного диалога с подростком.

Кейс-практикум «Цифровой след» позволил учащимся на конкретных примерах убедиться, как безобидные данные складываются в детальный цифровой портрет. Практикум «Анатомия кликбейта» сформировал устойчивую привычку проверять информацию перед репостом. Деловая игра «Кибер-Щит» моделировала комплексную кибератаку и учила скоординированным действиям. Настольная игра «Кибер-патруль» закрепила алгоритмы поведения в типовых опасных ситуациях. Мастер-класс для родителей показал, что 85% родителей после занятия изменили настройки родительского контроля или провели беседу с детьми о безопасности в сети.

После реализации комплекса проведён контрольный этап (апрель) с использованием того же диагностического инструментария. Результаты представлены в таблице 3.

Таблица 3 — Уровни сформированности информационной безопасности на контрольном этапе

Уровень	Констатирующий этап	Контрольный этап
Высокий	16,7% (4 чел.)	41,7% (10 чел.)
Средний	29,1% (7 чел.)	45,8% (11 чел.)
Низкий	54,2% (13 чел.)	12,5% (3 чел.)

Наблюдается значительная положительная динамика: доля учащихся с высоким уровнем выросла с 16,7% до 41,7% (более чем в 2,5 раза), с низким — сократилась с 54,2% до 12,5% (более чем в четыре раза). Когнитивный критерий: доля правильно идентифицирующих фишинговое письмо выросла с 58% до 92%. Поведенческий критерий: импульсивные клики по фишинговым ссылкам сократились с 79% до 21%. Эмоционально-ценностный критерий: доля учащихся, готовых вмешаться при кибербуллинге, выросла с 33% до 71%; средний балл по шкале цифровой эмпатии увеличился с 11,0 до 17,2.

На основе анализа результатов выработаны практические рекомендации: включение модуля «Основы кибербезопасности и критического мышления» во внеурочную деятельность (34 часа в год), ежегодное проведение общешкольного квеста по кибербезопасности (День безопасного интернета, 10 февраля), внедрение системы обязательных родительских практикумов (не реже двух раз в год), создание школьной группы волонтёров «Цифровой патруль» из старшеклассников, внедрение единой цифровой среды с постоянным мониторингом рисков.

ЗАКЛЮЧЕНИЕ

Анализ научно-методической литературы по теме исследования позволил сделать вывод о том, что информационные угрозы, воздействующие на подростков, делятся на несколько ключевых групп: угрозы психическому развитию (кибербуллинг, шок-контент), угрозы мировоззрению (фейки, вербовка), угрозы здоровью (интернет-зависимость, клиповое мышление) и угрозы личности (фишинг, кибергруминг). Основными причинами уязвимости выступают неконтролируемый рост цифрового контента и низкая цифровая компетентность родителей.

Исследование проходило на базе МОУ «Гимназия № 1» г. Балашова. В нём приняли участие 24 человека 8-го класса. Методиками исследования выступали: авторская анкета «Оценка рисков в сети», практический кейс-тест

(моделирование фишинга), методика «Незаконченные предложения» и шкала цифровой эмпатии.

Результаты констатирующего этапа показали наличие существенного разрыва между теоретическими знаниями и практическими навыками: низкий уровень выявлен у 54,2% обучающихся. На формирующем этапе в экспериментальной группе реализован комплекс практико-ориентированных занятий: кейс-метод «Цифровой след», фактчекинговые практикумы «Анатомия кликбейта», деловая игра «Кибер-Щит», настольная игра «Кибер-патруль», мастер-класс для родителей.

Сравнение результатов констатирующего и контрольного этапов показало выраженную положительную динамику: доля учащихся с высоким уровнем выросла с 16,7% до 41,7%, с низким — сократилась с 54,2% до 12,5%. Наиболее значимый прогресс наблюдался в поведенческом критерии (снижение кликов по фишинговым ссылкам с 79% до 21%) и когнитивном (рост распознавания угроз с 58% до 92%). Полученные результаты подтверждают эффективность разработанного комплекса методических материалов, что позволяет рекомендовать его использование в образовательном процессе общеобразовательных организаций для формирования компетентности в области информационной безопасности у обучающихся основной школы.