

# СИСТЕМНЫЙ АНАЛИЗ ЖИЗНЕННОГО ЦИКЛА ДЕЗИНФОРМАЦИИ В ЦИФРОВОЙ МЕДИАСРЕДЕ

## SYSTEMATIC ANALYSIS OF THE LIFE CYCLE OF DISINFORMATION IN THE DIGITAL MEDIA ENVIRONMENT

**B. Goryachkin  
D. Samoylov**

*Summary.* The article explores the phenomenon of disinformation in the digital media environment through the lens of its life cycle. It examines the key stages of disinformation from strategic intent and content creation to dissemination, entrenchment, detection, and neutralization. The mechanisms of fake news circulation across social media platforms are analyzed, with emphasis on personalization algorithms, emotional manipulation, and cognitive biases. The architecture of algorithmic disinformation detection is described, including the identification of anomalous patterns, content analysis, falsification identification, alert systems, and execution control. A structured model reflecting the cyclical and iterative nature of the process is presented. The study combines theoretical and applied approaches, integrating methods for analyzing digital content, network dynamics, and machine learning technologies. The findings may serve as a basis for the development of disinformation monitoring systems and the formation of information security strategies. The study examines disinformation as a systemic process with a defined life cycle, including creation, dissemination, entrenchment, detection, and neutralization. The findings show that its effectiveness depends on the interaction between platform algorithms and audience cognitive vulnerabilities. A multi-stage algorithmic model for disinformation detection is proposed, combining anomaly detection, content analysis, and network analysis. The results highlight the importance of integrating automated tools with expert oversight and institutional responses.

*Keywords:* disinformation, digital environment, life cycle, detection algorithms, fake news, cognitive biases, information campaigns, social media, machine learning, media literacy.

**Горячкин Борис Сергеевич**  
кандидат технических наук, доцент,  
Московский государственный технический  
университет им. Н.Э. Баумана  
bsgor@mail.ru

**Самойлов Дмитрий Евгеньевич**  
Московский государственный технический  
университет им. Н.Э. Баумана  
WardedShelf12345@gmail.com

*Аннотация.* Статья посвящена изучению дезинформации в условиях цифровой медиасреды через призму её жизненного цикла. Рассматриваются этапы функционирования дезинформационного контента от стратегического замысла и производства до распространения, укоренения, выявления и нейтрализации. Выявлены ключевые механизмы циркуляции фейков в социальных сетях, включая роль алгоритмов персонализации, эмоциональной манипуляции и когнитивных искажений. Описана архитектура алгоритмического выявления дезинформации, включающая детекцию аномальных паттернов, анализ содержания, идентификацию фальсификаций, систему оповещения и этап контроля исполнения. Представлена структурированная модель, отражающая цикличность и итеративность процесса. Работа сочетает теоретический и прикладной подход, интегрируя методы анализа цифрового контента, сетевой динамики и технологий машинного обучения. Полученные результаты можно использовать для проектирования систем мониторинга дезинформации и формирования стратегий информационной безопасности.

В работе дезинформация рассмотрена как системный процесс с выраженным жизненным циклом, включающим стадии создания, распространения, укоренения, выявления и нейтрализации. Показано, что её эффективность определяется взаимодействием алгоритмов цифровых платформ и когнитивных особенностей аудитории. Разработана многоэтапная модель алгоритмического выявления дезинформации, основанная на анализе аномальных паттернов, содержания и сетевых связей. Обоснована необходимость сочетания автоматизированных методов с экспертной оценкой и институциональными мерами противодействия.

*Ключевые слова:* дезинформация, цифровая среда, жизненный цикл, алгоритмы выявления, фейковые новости, когнитивные искажения, информационные кампании, социальные сети, машинное обучение, медиаграмотность.

### Введение

В условиях стремительной цифровизации и глобализации медиапространства проблема дезинформации достигла критического уровня. Современные коммуникационные технологии значительно упростили процессы создания и распространения информации, однако одновременно превратились в инструмент целе-

направленного воздействия на общественное сознание [1]. В этих условиях дезинформация эволюционировала из побочного эффекта информационной свободы в системный механизм манипуляции, способный оказывать влияние на политические процессы, общественные настроения, уровень доверия к государственным институтам и научному знанию.

Несмотря на развитие цифровых платформ, базовые признаки дезинформации сохраняют преемственность с классическими трактовками, дополняясь алгоритмическими и когнитивными механизмами. В отличие от случайных ошибок, дезинформация носит осознанный характер и направлена на формирование выгодных для инициатора интерпретаций действительности. Она редко проявляется в форме прямой лжи, чаще опираясь на правдоподобные фрагменты информации, вырванные из контекста и усиленные эмоциональной подачей [2].

Цифровая среда радикально усилила масштаб и скорость распространения дезинформации. Социальные сети и мессенджеры обеспечивают мгновенную дистрибуцию контента без предварительной проверки, а алгоритмы персонализации формируют замкнутые информационные пространства, повышающие восприимчивость аудитории к манипулятивным сообщениям. Эмоциональная окрашенность и апелляция к когнитивным искажениям [3] снижают критическое восприятие информации и способствуют её вирусному распространению [4].

В связи с этим возникает необходимость системного анализа дезинформации как процесса с выраженным жизненным циклом, охватывающим этапы от замысла и производства до выявления и опровержения. Цель данной статьи заключается в разработке комплексной модели жизненного цикла дезинформации в цифровом пространстве с анализом ключевых механизмов её функционирования и противодействия.

**Исследование современных каналов распространения дезинформации**

Эффективность технологий выявления дезинформации во многом определяется особенностями цифровой среды её распространения. Современное информационное пространство характеризуется доминированием онлайн-каналов, которые обеспечивают высокую скорость и масштаб циркуляции контента при отсутствии встроенных механизмов предварительной проверки достоверности. Алгоритмы социальных платформ, ориентированные на удержание внимания, усиливают распространение эмоционально окрашенных и сенсационных сообщений, что создаёт структурные преимущества для дезинформации. Дополнительным фактором выступает формирование персонализированных информационных пространств, ограничивающих доступ к альтернативным точкам зрения и снижающих критическое восприятие информации. В таких условиях ложные сообщения могут устойчиво воспроизводиться и закрепляться в общественном сознании. Наибольшую роль в распространении дезинформации играют цифровые платформы с массовой аудиторией и низкими барьерами публикации, включая социальные сети и мессенджеры. Их архитектура и высокая пользовательская активность создают благоприятные условия для быстрого тиражирования манипулятивного контента. Таким образом, анализ цифровых каналов распространения позволяет рассматривать дезинформацию как процесс с выраженной динамикой и служит основой для моделирования её жизненного цикла. Для наглядного сопо-

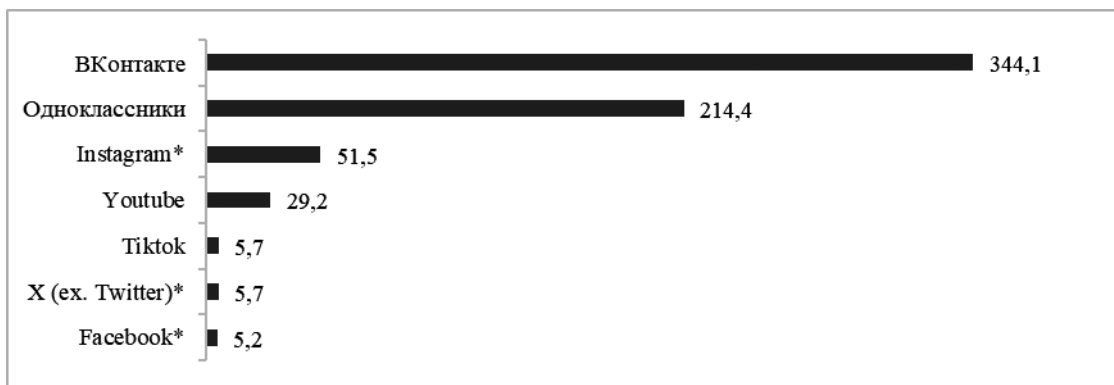


Рис. 1. Сообщений в соцсетях, млн

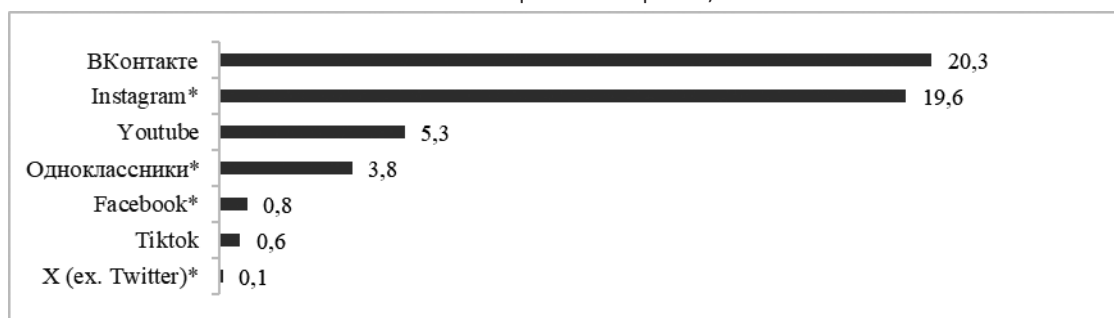


Рис. 2. Авторов соцмедиа в месяц, млн

ставления интенсивности информационных потоков в цифровой среде ниже представлено распределение объёма пользовательских сообщений и количества авторов по основным социальным платформам (рис. 1 и 2).

Данные иллюстрируют концентрацию коммуникационной активности и позволяют выявить каналы с наибольшим потенциалом для масштабного распространения информации, включая дезинформационный контент [5].

Наиболее интенсивным каналом дезинформации в последние годы стал мессенджер Telegram [5]. Его архитектура (открытые и приватные каналы, чаты с неограниченным числом участников) и политика минимальной цензуры создают благоприятные условия для запуска информационных кампаний. В Telegram фактически отсутствует центральная публичная модерация контента, анонимность каналов практически полная — что делает платформу идеальной для распространения дезинформации на широкую аудиторию. Не случайно в 2024 году порядка 33% россиян заявили, что получают новости через Telegram-каналы, то есть напрямую из неформальных источников в мессенджере [6].

Таким образом, цифровые платформы формируют коммуникационную среду, в которой дезинформация становится системным элементом информационного потока. Анализ каналов её распространения позволяет описать жизненный цикл дезинформации от первичного вброса до выявления и опровержения.

### Технологии создания и распространения дезинформации

Рассматриваемые цифровые платформы не являются нейтральной средой поскольку они активно используются субъектами дезинформации, которые целенаправленно адаптируют контент под архитектуру конкретных каналов. В современных условиях дезинформация не является результатом спонтанного или случайного производства. С момента создания она подчиняется логике предполагаемого распространения: то, как будет структурирован контент, в каком формате он появится, когда и на какой платформе будет опубликован. Всё это определяется особенностями информационного поведения аудитории и архитектурой цифровой коммуникации.

Инициаторы дезинформационных кампаний рассматривают коммуникационный процесс как управляемую систему, в которой каждый этап связан с заранее просчитанными каналами, алгоритмами платформ, а также эмоциональными и поведенческими шаблонами целевой аудитории. Такой подход позволяет не просто «запустить» сообщение, но и обеспечить его циркуляцию, репликацию, закрепление и эскалацию. Поэтому для анализа жизненного цикла дезинформации крайне важ-

но рассматривать производство и распространение как единую синхронизированную систему, в которой архитектура дистрибуции определяет характеристики самого сообщения.

Эффективность распространения дезинформации зависит от ряда устойчивых факторов, которые следует учитывать уже на стадии создания контента. Во-первых, это эмоциональная валентность: сообщения с выраженным аффективным окрасом (тревога, возмущение, сочувствие, шок) статистически вызывают более высокий уровень вовлечённости и, следовательно, превосходят по охвату нейтральные тексты. Во-вторых, алгоритмическая релевантность: разные платформы поощряют различные форматы (короткие и яркие тексты в лентах, визуально насыщенные ролики на видеохостингах, сжатые «выжимки» и цитаты в мессенджерах). Поэтому изначальная форма сообщения должна соответствовать алгоритмам ранжирования и метрикам удержания конкретной платформы.

В-третьих, пригодность к репликации: дезинформация распространяется быстрее, если её суть легко извлекается из контекста и может быть пересказана без потери основного смысла. Это требует заранее продуманных заголовков, «якорных» формулировок и самостоятельных медиафрагментов — изображений с подписями, коротких видеороликов, цитат. В-четвёртых, важна среда первичного запуска: анонимные или слабо модерлируемые точки входа (закрытые каналы, паблики, тематические сообщества) позволяют безопасно инициировать волну распространения и проверить, как реагирует аудитория. Поэтому сценарий первого вброса — это часть стратегии, а не спонтанная акция.

Наконец, адресность: лексика, визуальные метафоры и герои сообщения должны соответствовать культурному коду целевой группы. В противном случае даже алгоритмы персонализации и социальные связи не обеспечат нужную плотность репостов и обсуждений.

Продолжая рассмотрение ключевых аспектов, формирующих процесс создания и распространения дезинформации, можно выделить значимость синхронизированной структуры, в которой каждый этап обладает своими задачами и характеристиками. Анализируя этот процесс через призму BPMN-диаграммы, можно более глубоко понять, как интеграция различных факторов и стадий позволяет выстроить эффективную кампанию по распространению дезинформации (рис. 3).

Процесс начинается с чёткого определения цели. Это даёт возможность инициатору выстроить стратегию в соответствии с характеристиками нужной аудитории. На этом этапе формулируется основная задача, будь то управление общественным мнением, усиление полити-

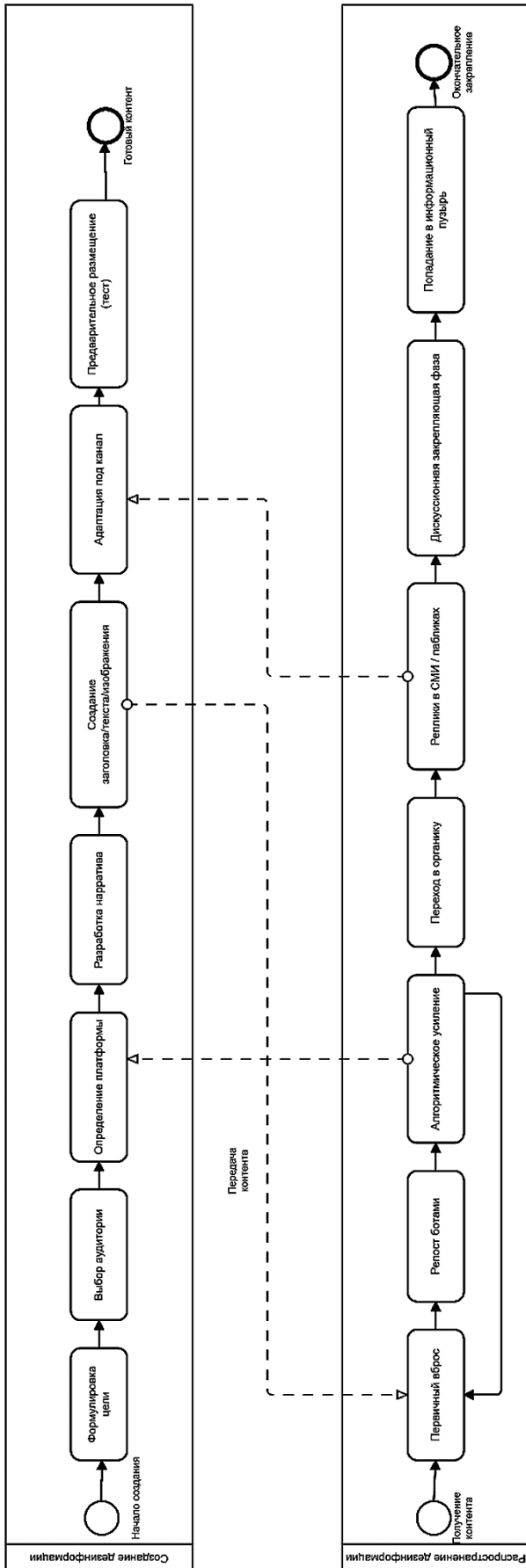


Рис. 3. VRMN диаграмма создания дезинформации

ческой нестабильности или провоцирование массового возмущения. Затем определяется целевая группа. Важно понимать, какие именно социальные слои или группы станут адресатами сообщения. Это требует предварительного анализа их поведения, интересов и модели восприятия информации.

После выбора аудитории переходит к подбору подходящей платформы. Учитываются алгоритмы и метрики вовлечённости, характерные для каждой цифровой среды. Контент адаптируется с учётом форматов, допустимой длины, визуального оформления и особенностей распространения.

На основе собранной информации создаётся основной нарратив, в котором содержится ключевое послание и эмоциональное наполнение. Цель — вызвать у аудитории сильную эмоциональную реакцию (тревогу, гнев или шок). Именно такие состояния способствуют вовлечённости и увеличивают вероятность того, что контент будет активно распространяться. Большое значение имеет формирование заголовка, текста и визуальных элементов. Заголовок должен быть выразительным, лаконичным и легко извлекаемым из контекста. Важно, чтобы такие элементы можно было быстро пересылать и воспринимать как самостоятельную информационную единицу. Это особенно актуально для мемов, коротких видео или цитат. Далее начинается адаптация материалов под формат выбранного канала. Каждый ресурс требует специфической подачи. Социальные сети лучше воспринимают короткие, эмоционально заряженные тексты, видеоплатформы — яркий визуальный контент. Перед основным запуском осуществляется пробная публикация. Это необходимо для проверки реакции аудитории. Если наблюдается положительный отклик, начинается полномасштабное распространение. Первичное размещение, как правило, происходит в закрытых или плохо модерлируемых сообществах. Это создаёт безопасные условия для оценки потенциала контента. При необходимости содержание может быть доработано. После этого в распространении начинают участвовать боты и автоматические инструменты, ускоряющие охват. Затем вступают в силу алгоритмы платформ, которые, фиксируя высокий уровень взаимодействия, автоматически усиливают видимость контента в лентах и рекомендациях. После этого начинается органическое распространение. Контент подхватывают реальные пользователи, делятся им, обсуждают, что способствует росту охвата и вовлечённости. Далее он реплицируется в СМИ и популярных пабликах, закрепляется в более широком инфопространстве. Следом наступает стадия активных обсуждений. Контент становится темой публичных дебатов, тем самым усиливая своё влияние. Затем он оказывается в так называемом информационном пузыре (замкнутом медиапространстве, где многократно воспроизводится и подтверждается, создавая иллюзию объективной реальности).

Таким образом, дезинформация представляет собой тщательно спланированную кампанию, в которой каждый этап выполняет свою функцию. BPMN-диаграмма позволяет отразить этот сложный процесс, показывая, как последовательные действия и их координация влияют на успешность распространения.

**Жизненный цикл дезинформации: от замысла до опровержения**

Если BPMN-диаграмма отражает операционную логику создания и распространения дезинформации, то жизненный цикл позволяет рассмотреть данный процесс в более широком аналитическом контексте, от формирования замысла до этапов выявления и опровержения. Исследовательская группа по технологиям и социальным изменениям (TaSC) в Центре Шоренштейна Гарвардской школы имени Кеннеди использует подход ситуационного исследования для составления карты жизненного цикла кампаний по манипуляции СМИ. Этот методологический подход направлен на анализ порядка, масштаба и сферы охвата кампаний по манипуляции, отслеживая артефакты СМИ в пространстве и времени, объединяя множественные связи для сортировки запутанного беспорядка. В рамках этой работы был разработан обзор жизненного цикла кампании по манипуляции СМИ, который полезен для журналистов, когда они пытаются идентифицировать, отслеживать и разоблачать манипуляции СМИ и дезинформацию (рис. 4).

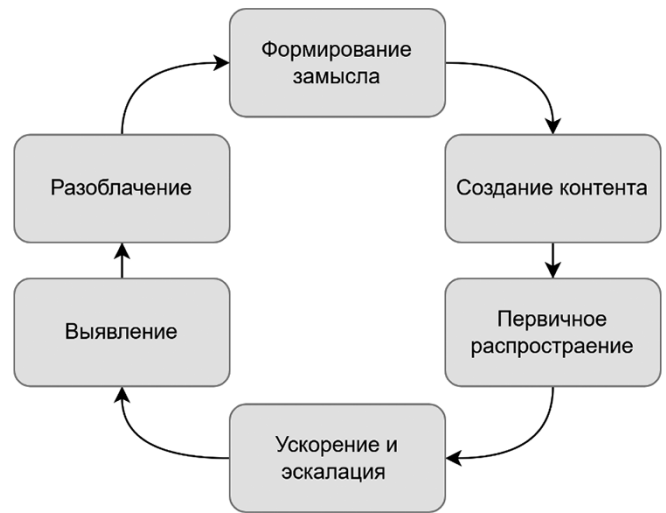


Рис. 4. Жизненный цикл дезинформации

Жизненный цикл дезинформации начинается с этапа формирования замысла, на котором осуществляется концептуализация будущего информационного воздействия. Различные акторы, включая государственные структуры, частные лица, активистские группы и коммерческие организации, формулируют цели дезинформационной кампании. Эти цели могут быть связаны с дискредитацией оппонентов, формированием чувства

страха или недоверия, а также с влиянием на массовое поведение. На данном этапе проводится анализ целевой аудитории с целью выявления её социально-культурных особенностей и когнитивных уязвимостей, которые могут быть использованы для усиления манипулятивного эффекта. Существенную роль играет работа с эмоциональными триггерами, такими как тревога, чувство несправедливости или групповая идентичность. Параллельно формируется содержательная основа дезинформации, определяются ключевые нарративы, меседжи и формы подачи, при этом особое внимание уделяется правдоподобию и эмоциональной вовлечённости. Часто используются гибридные тактики, сочетающие достоверные элементы с искажёнными или ложными интерпретациями.

На следующем этапе замысел материализуется в виде конкретного контента. Дезинформация приобретает форму текстовых публикаций, фальшивых новостей, манипулятивных визуальных материалов, мемов, поддельных документов или видеозаписей. В современных условиях всё чаще применяются технологии искусственного интеллекта и глубоких подделок, позволяющие создавать высокореалистичный контент, способный имитировать высказывания публичных фигур или визуальные доказательства. Одновременно осуществляется выбор каналов распространения, ориентированных на максимальный охват целевой аудитории. Приоритет отдается платформам с высокой вовлечённостью пользователей, включая социальные сети, мессенджеры и специализированные онлайн-ресурсы. После создания контента начинается стадия первичного распространения, направленная на запуск дезинформации в цифровом пространстве. Для этого используются как автоматизированные средства, включая ботов и сетевые аккаунты, так и реальные пользователи, вовлечённые в кампанию сознательно или неосознанно. Цель данного этапа заключается в достижении вирусного эффекта, при котором информация начинает распространяться органически за счёт пользовательских репостов, комментариев и реакций. Дополнительным инструментом становится искусственное создание видимости общественной поддержки через накрутку показателей вовлечённости, что усиливает доверие аудитории к распространяемому сообщению. По мере наращивания охвата дезинформация переходит в стадию укоренения и эскалации. Ложные или искажённые сведения начинают восприниматься как достоверные и воспроизводятся пользователями в рамках повседневного информационного обмена. Это сопровождается ростом эмоциональных реакций, усилением поляризации и формированием устойчивых интерпретаций событий. Важной особенностью данного этапа является то, что попытки опровержения нередко способствуют дальнейшему распространению дезинформации, поскольку любое упоминание усиливает её присутствие в медиaprостранстве. Манипуляторы мо-

гут адаптировать стратегию, дополняя первоначальный нарратив новыми деталями, псевдодоказательствами или ссылками на фиктивных экспертов, что усложняет процесс проверки и подрывает доверие к официальным источникам. Со временем дезинформация становится объектом внимания со стороны журналистов, исследователей и организаций, занимающихся проверкой фактов. Этап выявления включает систематический анализ контента, установление первоисточников и реконструкцию путей распространения. Особое значение приобретает использование технических и аналитических методов, позволяющих обнаруживать автоматизированную активность, выявлять сетевые аномалии и фиксировать признаки технологических подделок. На стадии разоблачения предпринимаются целенаправленные меры по публичному опровержению дезинформации. Это включает публикацию аналитических материалов, проведение журналистских расследований и запуск информационных кампаний, объясняющих ложность распространяемых утверждений. Эффективность данного этапа зависит от способности донести проверенную информацию в доступной форме и обеспечить сопоставимый с дезинформацией уровень охвата. Завершающим этапом жизненного цикла становится опровержение и восстановление доверия. Он направлен на минимизацию долгосрочных последствий дезинформационного воздействия и включает выпуск разъяснительных материалов, реализацию программ по повышению медиаграмотности и внедрение платформенных механизмов фильтрации контента. Эти меры способствуют формированию критического восприятия информации и снижению уязвимости аудитории к последующим манипулятивным воздействиям.

Заключительным этапом жизненного цикла дезинформации выступает её выявление и нейтрализация, в рамках которого особое значение приобретают алгоритмические методы анализа. В условиях экспоненциального роста объёмов цифрового контента, а также ограниченных ресурсов для экспертной верификации, именно автоматизированные системы на основе методов машинного обучения становятся ключевым инструментом борьбы с ложной информацией. Применение таких алгоритмов позволяет оперативно выявлять и блокировать дезинформационные сообщения ещё до их массового распространения, существенно снижая риски информационных искажений в обществе.

Современные алгоритмические системы выявления дезинформации представляют собой многоуровневые интеллектуальные комплексы, способные функционировать в условиях непрерывного и стремительно возрастающего информационного потока. В цифровом медиaprостранстве, где объём пользовательского контента исчисляется миллионами единиц в сутки, своевременное обнаружение и пресечение фальсифицирован-

ных сообщений невозможно без автоматизированных технологий. В данном контексте алгоритм выявления дезинформации выступает как структурированный цикл, включающий последовательность этапов от мониторинга потоков данных до оценки эффективности принятых мер, с возможностью итеративного возврата к предыдущим фазам [7] (рис. 5).

### Выявление аномальных паттернов

Алгоритм запускается с мониторинга информационных потоков в цифровой среде. На этом этапе производится автоматизированный сбор данных с платформ социальных сетей, мессенджеров, новостных ресурсов и других источников. Система фиксирует статистические отклонения, которые могут сигнализировать о запуске дезинформационной кампании. К таким аномалиям относятся резкие всплески активности, синхронные публикации идентичного содержания, повторяющиеся шаблонные фразы, характерные для автоматизированных ботов, а также координированные действия подозрительных групп. Детектирование подобных паттернов осуществляется с применением методов кластеризации, графового анализа и временной сегментации, позволяющих выявить отклонения от фона в масштабе всей платформы.

### Анализ содержания

После изоляции подозрительных фрагментов информации система переходит к этапу углублённого анализа содержания сообщений. Этот процесс включает в себя оценку лингвистических и стилистических характеристик, идентификацию эмоциональной окраски, выявление признаков манипуляции и отклонений от журналистских стандартов. Применяются технологии обработки естественного языка (NLP), позволяющие проводить семантический, синтаксический и прагматический анализ текста. Особое внимание уделяется структуре изложения, фактурности информации, использованию риторических приёмов и степени односторонности подачи. Сопоставление с базами проверенных источников и фактологических данных обеспечивает контекстуальную верификацию утверждений.

### Идентификация фальсификаций

На основании результатов анализа содержания производится третий этап — идентификация фальсификаций. Это критическая фаза, в рамках которой система классифицирует сообщения на достоверные, спорные или однозначно ложные. Процесс осуществляется с помощью обученных моделей машинного обучения, в том числе нейросетевых архитектур, способных выявлять шаблоны, типичные для дезинформации. Примеры таких моделей — FakeDetector и аналогичные ему инструмен-

ты, оценивающие сообщения по множеству признаков: тема, лексика, автор, источник, характер распространения. Каждому информационному фрагменту присваивается достоверный балл. Установлено, что фейковые материалы часто содержат повторяющиеся топики, используются специфические лексемы, а источники имеют низкую медиарепутацию. На основе этих признаков и формируется решение о наличии дезинформации.

### Система оповещения

После подтверждения ложного характера контента алгоритм инициирует механизмы оповещения. Информация о выявленной дезинформации автоматически направляется в модераторские службы соответствующей платформы. Параллельно запускаются инструменты визуального оповещения пользователей: сообщения помечаются как потенциально недостоверные, снабжаются предупреждающими баннерами или метками. При необходимости информация передаётся в верификационные организации или публикуются публичные уведомления о текущей волне дезинформации. Цель данного этапа — оперативное реагирование, информирование заинтересованных сторон и минимизация вирусного распространения ложного контента.

### Проверка выполнения и итеративная корректировка

Финальной фазой цикла выступает проверка выполнения предпринятых мер. Система отслеживает, были ли реализованы действия, рекомендованные на предыдущем этапе: удаление контента, блокировка источника, установка меток. Анализируются поведенческие метрики пользователей (просмотры, репосты, вовлеченность), чтобы оценить эффективность вмешательства. В случае отсутствия необходимой реакции или сохранения высокой активности фальсифицированного контента, алгоритм может повторно инициировать цикл анализа, скорректировав критерии фильтрации и классификации. Таким образом, реализуется итеративность процесса, обеспечивающая адаптацию системы к меняющимся стратегиям распространения дезинформации.

Именно многоаспектность подхода — использование комбинации признаков, а не опора на единичный критерий — обеспечивает высокую точность детекции дезинформации. Практика показывает, что наилучшие результаты достигаются при интеграции алгоритмического анализа с экспертной проверкой: такое человеко-машинное взаимодействие позволяет значительно повысить достоверность результатов, минимизируя как ложноположительные, так и ложноотрицательные срабатывания [8].

Следует подчеркнуть, что процесс выявления дезинформации носит не линейный, а циклический характер.

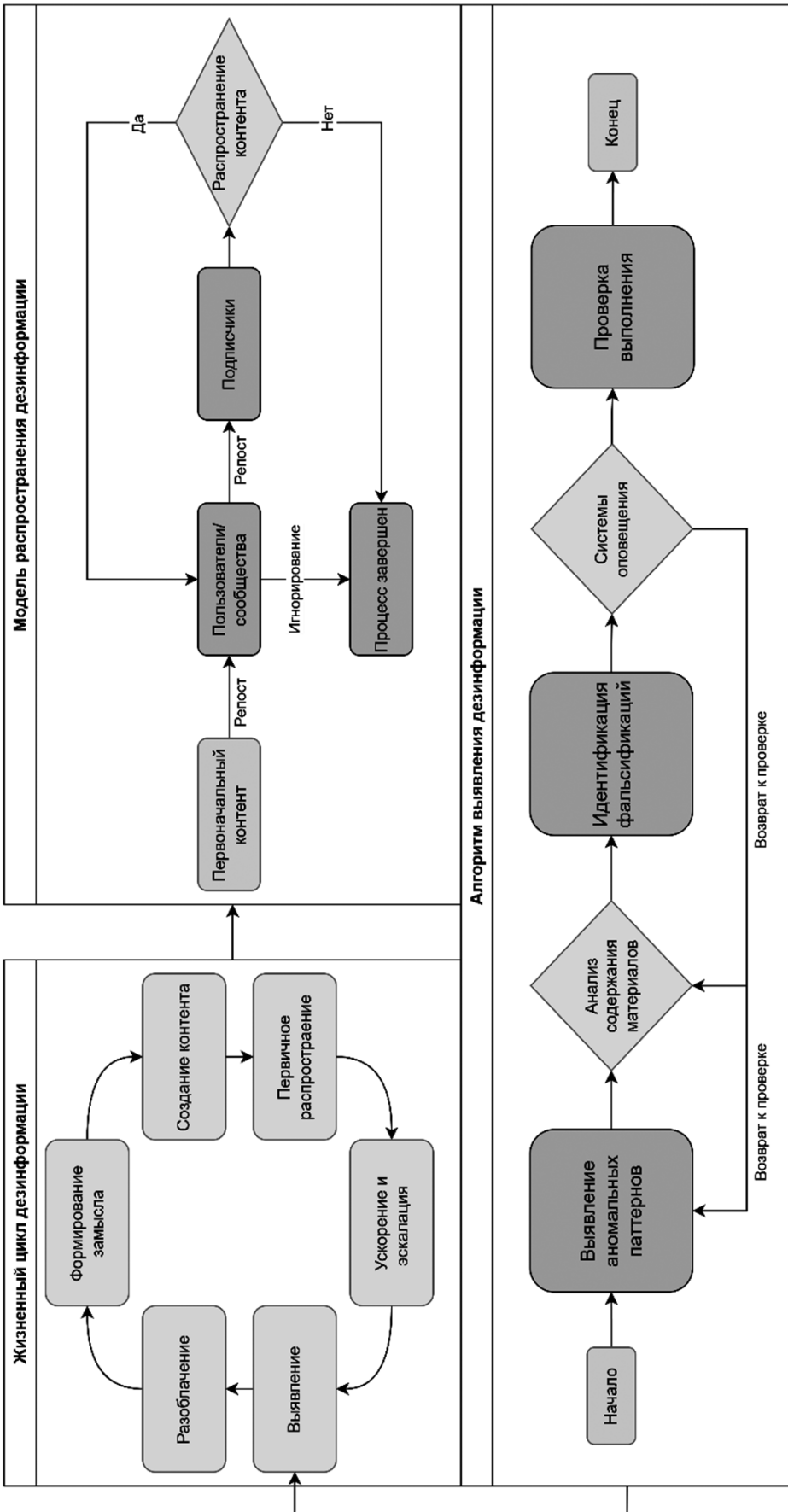


Рис. 5. Комплексная модель жизненного цикла дезинформации

Возврат к предыдущим этапам осуществляется при необходимости переоценки выявленных паттернов, уточнения классификации или доработки мер реагирования. Такая архитектура обеспечивает гибкость алгоритма и его устойчивость к быстро эволюционирующим формам дезинформации, а также к адаптации злоумышленников к противодействующим механизмам.

### Заключение

Статья посвящена системному анализу дезинформации как повторяющегося процесса с чётко выраженным жизненным циклом, включающим стадии замысла, создания, распространения, укоренения, выявления и нейтрализации. Исследование охватывает как поведенческие, так и технические аспекты функционирования фейков в цифровой среде. Особое внимание уделяется роли алгоритмов социальных платформ, эффектам информационных пузырей и когнитивным искажениям, усиливающим восприимчивость аудитории к манипулятивному контенту.

В работе представлена многоступенчатая модель алгоритмического выявления дезинформации, включающая обнаружение аномальных паттернов, анализ содержания, идентификацию фальсификаций, систему оповещений и контроль эффективности. Используются технологии машинного обучения, обработки естественного языка и графового анализа для классификации информации в реальном времени.

Подчёркивается, что эффективное противодействие дезинформации требует сочетания автоматизированных решений с институциональными мерами и развитием медиаграмотности. Предложенная модель может быть использована при разработке систем мониторинга в социальных медиа и формировании стратегий информационной безопасности. Результаты исследования вносят вклад в теоретическое осмысление цифровых угроз и прикладные практики их нейтрализации.

### ЛИТЕРАТУРА

1. Коновалов В.Н. Политология: словарь. М.: РГУ, 2010.
2. Самошкин Е.А. Институты борьбы с дезинформацией и мисинформацией в СМИ // Вестник Московского университета. Серия 10: Журналистика. 2017. № 6.
3. Ермолаева Ю.В. Типология когнитивных искажений и их влияние на проэкологическое поведение // Вестник Томского государственного университета. Философия. Социология. Политология. 2024. № 82. URL: <https://cyberleninka.ru/article/n/tipologiya-kognitivnyh-iskazheniy-i-ih-vliyanie-na-proekologicheskoe-povedenie> (дата обращения: 16.12.2025).
4. Sathianathan S., Mhd Ali A., Chong W.W. How the General Public Navigates Health Misinformation on Social Media: Qualitative Study of Identification and Response Approaches // JMIR Infodemiology. 2025. Vol. 5. e67464. DOI: 10.2196/67464.
5. Brand Analytics. Социальные сети в России: цифры и тренды. Весна 2025.
6. DataReportal. Digital 2024: Global News Report. URL: <https://datareportal.com/reports/digital-2024-global-news-report> (дата обращения: 16.12.2025).
7. Ayyasamy R.K., Ponnusamy C., Bhargavi K.N., et al. A hybrid deep learning framework for fake news detection using LSTM-CGPN and metaheuristic optimization // Scientific Reports. 2025. Vol. 15. Article 41522. DOI: <https://doi.org/10.1038/s41598-025-25311-x>.
8. Boko A. Disinformation Detection: Developing a Categorical Framework Through Thematic Analysis // Journal Media. 2024. Vol. 5. P. 1914–1924. DOI: <https://doi.org/10.3390/journalmedia5040116>.
9. Del Vicario M., Bessi A., Zollo F., Petroni F., Scala A., Caldarelli G., Stanley H.E., Quattrociocchi W. The spreading of misinformation online // Proceedings of the National Academy of Sciences of the USA. 2016. Vol. 113. No. 3. P. 554–559.
10. Garimella K., De Francisci Morales G., Gionis A., Mathioudakis M. Political discourse on social media // In: Proceedings of the 2018 World Wide Web Conference (WWW '18). New York: ACM Press, 2018. Vol. 2. P. 913–922.
11. Robertson A. Was Reddit always about free speech? Yes, and no // The Verge. June 15, 2015. URL: <https://www.theverge.com> (дата обращения: 16.12.2025).