УДК 327
МРНТИ 11.25.91
https://doi.org/10.48371/ISMO.2026.63.1.004

ДЕЗИНФОРМАЦИЯ КАК ИНСТРУМЕНТ ИНФОРМАЦИОННЫХ ВОЙН И ФАКТОР УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Кошербаев Ж.Д.[1], * Махмадин А.Д.[2], Мельдибекова З.А.[3]
[1, *2] Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[3] Международный Университет Информационных Технологий, Алматы, Казахстан

Аннотация. В статье рассматривается дезинформация как один из ключевых инструментов информационных и гибридных войн, оказывающий существенное влияние на общественное сознание, политическую стабильность и национальную безопасность государств. В условиях цифровой трансформации и активного развития социальных сетей, алгоритмических платформ и технологий искусственного интеллекта дезинформация приобретает системный характер, обеспечивая быстрый и масштабный охват аудитории и усиливая деструктивный потенциал информационного воздействия.

Целью исследования является комплексный анализ дезинформации и пропаганды, распространяемых с использованием цифровых технологий, выявление методологических подходов к изучению манипулятивного информационного воздействия, оценка его социальных и политических последствий, а также разработка направлений противодействия дезинформационным практикам, угрожающим национальной безопасности. Объектом исследования выступает дезинформация как инструмент информационных войн, а предметом - механизмы её создания, распространения и воздействия в цифровой среде.

Методологическую основу исследования составляет междисциплинарный подход, включающий методы анализа и синтеза, системный и сравнительный анализ, контент-анализ медиаматериалов, кейс-стади конкретных дезинформационных кампаний, а также нормативно-правовой анализ стратегических документов Республики Казахстан. В работе обоснована гипотеза о том, что эффективность дезинформации определяется сочетанием преднамеренного искажения контента, алгоритмического усиления цифровыми платформами и недостаточной правовой регламентации ответственности за её распространение.

Научная новизна исследования заключается в предложении структурированной модели дезинформации, авторском определении

данного понятия и обосновании необходимости его законодательного закрепления. Сделан вывод о том, что противодействие дезинформации требует комплексных правовых, институциональных и образовательных мер, направленных на укрепление устойчивости информационного пространства и национальной безопасности.

Ключевые слова: дезинформация, информационные войны, национальная безопасность, манипуляция общественным сознанием, цифровые платформы, медиаграмотность, информационная безопасность

Введение

В современных условиях информация выступает не только в качестве стратегического ресурса, но и как мощный инструмент целенаправленного воздействия, способный формировать общественное мнение, оказывать влияние на политические процессы и выступать триггером конфликтов различной интенсивности. Стремительное развитие цифровых технологий - включая социальные сети, алгоритмы анализа больших данных и инструменты искусственного интеллекта - значительно упростило процессы создания, тиражирования и масштабирования дезинформации. Указанные технологии позволяют осуществлять манипуляцию массовым сознанием посредством распространения ложных, искажённых либо контекстуально трансформированных сведений с беспрецедентной скоростью и охватом аудитории.

Особую угрозу в данном контексте представляют фейковые новости и контент, созданный с использованием deepfake-технологий [1]. Подобные материалы, активно распространяемые через цифровые платформы, способны в кратчайшие сроки достигать широкой аудитории, обходя традиционные механизмы проверки достоверности информации и институциональные фильтры. В условиях информационных и гибридных войн это формирует серьёзные вызовы для системы государственной безопасности, независимой журналистики и общества в целом, подрывая доверие к информационному пространству.

В этой связи изучение механизмов информационного противоборства, а также разработка эффективных методов выявления, анализа и нейтрализации дезинформационных потоков становятся приоритетными направлениями в контексте обеспечения национальной безопасности. Распространение ложных сведений активно используется как инструмент манипуляции общественным сознанием, поскольку подобные технологии искажают представления о людях, событиях и социальных процессах, вводя аудиторию в заблуждение. Так, фальсифицированные данные или целенаправленная пропаганда способны формировать негативный образ отдельных социальных групп, государств или политических инициатив,

подрывая общественное доверие, усиливая социальную напряжённость и провоцируя поляризацию общества.

Дезинформация представляет собой преднамеренное распространение ложных либо искажённых сведений с целью манипуляции общественным мнением, дестабилизации политической и социальной обстановки или достижения определённых политических, экономических и иных стратегических целей. Она ориентирована на изменение восприятия и поведенческих установок индивидов и социальных групп, вызывая недоверие, страх либо поддержку заданных идей и нарративов. Таким образом, дезинформация не только трансформирует восприятие реальности, но и создаёт прямые угрозы национальной безопасности. Искажённые данные могут использоваться для подрыва доверия к государственным институтам, воздействия на электоральные процессы, провоцирования социальных беспорядков или эскалации международных конфликтов. В условиях гибридных войн информационные атаки становятся важнейшим элементом стратегий, направленных на ослабление противника без применения прямой военной силы. Кроме того, дезинформация активно используется для углубления политических кризисов, подрыва экономической стабильности, обострения межгрупповых противоречий и дискредитации институтов государственной власти.

Проблематика дезинформации выходит за рамки сугубо академического анализа, приобретая выраженную междисциплинарную значимость и оказывая непосредственное влияние на различные сферы общественной жизни. Её актуальность затрагивает, во-первых, политических акторов, ответственных за разработку нормативно-правовых механизмов и стратегий противодействия информационным угрозам; во-вторых, профессиональное журналистское сообщество, призванное обеспечивать достоверность и проверяемость распространяемой информации; и, в-третьих, широкую общественность, которая непосредственно сталкивается с последствиями информационных манипуляций. Осознание критической значимости данной проблемы способствует формированию и развитию практик информационной гигиены, медиаграмотности и цифровой безопасности, что, в свою очередь, повышает устойчивость общества к деструктивным информационным воздействиям и укрепляет основы национальной безопасности.

В сфере международных отношений дезинформация трансформируется в инструмент информационных войн, направленных на дискредитацию государств, разжигание конфликтов и подрыв дипломатических взаимодействий. Она может использоваться для легитимации агрессивных действий, конструирования образа врага и манипулирования общественным мнением в интересах отдельных геополитических акторов, что в конечном

итоге дестабилизирует международную систему и снижает уровень доверия между государствами.

Актуальность данной темы обусловлена тем, что дезинформация в условиях информационных войн представляет собой одну из наиболее серьёзных угроз национальной безопасности. Она способствует подрыву доверия к государственным институтам, дестабилизации общественно-политической системы и манипуляции массовым сознанием. Дезинформационные воздействия могут использоваться для разжигания социальных и межгрупповых конфликтов, вмешательства в электоральные процессы, а также для легитимации агрессивных действий в сфере международных отношений. В условиях гибридных войн систематические дезинформационные кампании направлены на внутреннее ослабление государства, что обуславливает необходимость разработки комплексных и многоуровневых мер по их своевременному выявлению, анализу и нейтрализации.

Вместе с тем каждый индивид, использующий современные информационные ресурсы, становится участником глобального информационного пространства и потенциальным объектом информационного воздействия. Осознание существования дезинформации, а также развитие навыков критического мышления и медиаграмотности способствуют способности граждан распознавать ложные и искажённые сведения, избегать манипулятивных практик и сохранять психологическое и социальное благополучие. В этом контексте именно коллективные усилия общества, направленные на повышение уровня информационной культуры и цифровой грамотности, способны сформировать устойчивость к деструктивным угрозам, возникающим в условиях цифровой трансформации и интенсивного информационного противоборства.

Целью настоящего исследования является комплексный анализ влияния дезинформации и пропаганды, распространяемых с использованием цифровых технологий, а также выявление ключевых методологических подходов к изучению пропагандистского воздействия, оценка его социальных и политических последствий и разработка эффективных стратегий противодействия дезинформационным практикам, направленным на дестабилизацию глобального и национального порядка.

В рамках исследования особое внимание уделяется уточнению и систематизации понятийного аппарата, необходимого для углублённого анализа роли средств массовой информации и цифровых платформ в формировании общественного мнения, поддержании политической стабильности и обеспечении устойчивости социальной среды.

Объектом исследования выступает дезинформация как ключевой инструмент информационных войн, применяемый в целях манипуляции

общественным сознанием и дестабилизации социальных и политических процессов. Рассматривается её воздействие на национальную безопасность, включая подрыв доверия к государственным институтам, провоцирование внутренних конфликтов и вмешательство во внутриполитические процессы.

Предметом исследования являются механизмы создания и распространения дезинформации в цифровой среде, а также формы и методы её воздействия на национальную безопасность, выражающиеся в ослаблении институционального доверия, эскалации социальных противоречий и нарушении политической стабильности. В работе анализируются стратегии информационного противоборства и оцениваются потенциальные инструменты и подходы к противодействию деструктивному информационному воздействию.

Научная новизна настоящего исследования заключается в следующем:

Во-первых, дезинформация рассматривается не только как медийный феномен или элемент пропаганды, но как самостоятельный инструмент информационных войн, оказывающий комплексное воздействие на общественное сознание, политическую стабильность и национальную безопасность. Такой подход позволяет расширить традиционные трактовки дезинформации и включить её в системный анализ современных угроз безопасности.

Во-вторых, в работе впервые в рамках отечественного научного дискурса предложена структурированная модель дезинформации, включающая такие ключевые элементы, как преднамеренность создания и распространения, искажённость или ложность информации, целевая направленность воздействия и механизмы распространения в цифровой среде. Данная модель позволяет более точно анализировать дезинформационные практики и разграничивать их от смежных информационных явлений.

В-третьих, автором обоснована необходимость законодательного закрепления понятия «дезинформация» в национальной правовой системе и предложена авторская редакция данного термина, учитывающая как содержательные, так и функциональные характеристики дезинформации в условиях цифровизации и гибридных конфликтов.

В-четвёртых, проведено разграничение дезинформации, ошибочной информации и манипулятивного использования правдивых данных, что позволяет уточнить понятийный аппарат исследования и создать теоретическую основу для разработки дифференцированных механизмов противодействия различным формам информационного воздействия.

В-пятых, на основе анализа нормативно-правовых документов Республики Казахстан и международных практик противодействия дезинформации выявлены ключевые институциональные пробелы и направления совершенствования национальной системы информационной

безопасности, включая усиление ответственности цифровых платформ и развитие медиаграмотности как элемента устойчивости общества.

Основная гипотеза исследования заключается в том, что дезинформация в условиях цифровой трансформации и информационных войн выступает не стихийным побочным эффектом развития медиасреды, а целенаправленным инструментом политического и социального воздействия, систематически используемым для манипуляции общественным сознанием, подрыва доверия к государственным институтам и дестабилизации национальной безопасности.

Уточняющая гипотеза состоит в том, что эффективность дезинформационных кампаний определяется совокупным воздействием преднамеренного характера искажённого контента, алгоритмического усиления охвата цифровыми платформами и недостаточной нормативно-правовой регламентации ответственности за распространение дезинформации. Предполагается, что законодательное закрепление понятия «дезинформация» и внедрение комплексных правовых и институциональных мер способны снизить деструктивный потенциал данного феномена.

Материалы и методы

Методологическую основу исследования составляет междисциплинарный подход, позволяющий рассматривать дезинформацию как сложный социально-политический феномен, находящийся на пересечении политологии, теории международных отношений, медиакоммуникаций, социологии и информационной безопасности. Применение данного подхода обусловлено многоуровневым характером дезинформации, которая одновременно функционирует как инструмент политического воздействия, элемент информационных войн и фактор угрозы национальной безопасности.

В ходе исследования использовался комплекс теоретических и эмпирических методов научного анализа. Теоретические методы включали анализ и синтез, применяемые для обобщения существующих научных подходов к понятию дезинформации и выявления её ключевых структурных элементов; индукцию и дедукцию - при формировании выводов о механизмах воздействия дезинформации на общественное сознание и политическую стабильность; системный подход, позволивший рассматривать дезинформацию как элемент целостной системы информационного противоборства, включающей акторов, цели, инструменты и каналы распространения; а также сравнительно-аналитический метод, использованный для сопоставления зарубежных и отечественных трактовок дезинформации и моделей противодействия информационным угрозам.

Эмпирическая часть исследования базировалась на контент-анализе и методе кейс-стади. Контент-анализ применялся для изучения дезинформационных нарративов в цифровом информационном пространстве на основе материалов интернет-СМИ, социальных сетей, цифровых платформ, а также официальных политических заявлений и нормативных документов. Анализ осуществлялся по таким критериям, как характер искажения информации, наличие манипулятивных фреймов, целевая направленность контента, а также использование эмоциональных и когнитивных триггеров. Метод кейс-стади использовался для углублённого анализа конкретных примеров дезинформационного воздействия, включая случаи репутационного и экономического ущерба, вызванного распространением манипулятивного контента, а также примеры политически мотивированной дезинформации, направленной на формирование негативных общественных настроений, поляризацию общества и эскалацию социальных конфликтов.

Дополнительно в работе применялся нормативно-правовой анализ, в рамках которого исследовались действующие стратегические и правовые документы Республики Казахстан в сфере информационной безопасности, а также официальные заявления высших должностных лиц государства. Данный метод позволил выявить институциональные особенности и пробелы в правовом регулировании противодействия дезинформации, включая отсутствие законодательного определения данного понятия. Сравнительный анализ международных практик противодействия дезинформации использовался для выявления общих тенденций и оценки возможностей адаптации зарубежного опыта к национальному контексту.

Использование совокупности указанных методов обеспечило комплексный характер исследования, повысило обоснованность полученных выводов и позволило рассмотреть дезинформацию не только как теоретическую категорию, но и как практический инструмент информационных войн, оказывающий реальное влияние на общественное мнение, политическую стабильность и национальную безопасность.

Обзор литературы

Дезинформация в интернет-СМИ представляет собой значимый объект научного анализа, особенно в контексте её воздействия на современное информационное пространство и процессы формирования общественного мнения. Существенный вклад в изучение данного феномена внесли зарубежные исследователи, среди которых следует выделить Оливер Бойд-Барретт [2], Ноам Хомский [3], Джулия Позетти [4] и Ричард Стенгел [5]. Их работы заложили теоретические основы анализа пропаганды, медиаманипуляций и механизмов искажения информации в условиях цифровизации и глобальных коммуникаций.

В отечественной научной школе проблематика дезинформации и информационных угроз также находит отражение в трудах ряда исследователей. К числу ведущих специалистов относятся Г.С. Султанбаева [6], З. К. Буенбаева, Ш. Шакенова [7] и другие авторы. Несмотря на возрастающее внимание к данной проблеме, следует отметить, что уровень её теоретической и эмпирической проработанности остаётся недостаточным, особенно с точки зрения комплексного анализа дезинформации как инструмента информационных войн.

В последние годы наблюдается рост числа публикаций в отечественных научных журналах, что свидетельствует об усилении интереса исследовательского сообщества к данной тематике и осознании необходимости её более глубокого теоретического и прикладного осмысления. Так, в статье «Распространение фейковой и некорректной информации в социальных сетях Казахстана» анализируются алгоритмы верификации контента, социометрические показатели распространения фейковой информации, а также источники её генерации и факторы влияния на общественное сознание [6]. В работе «Проблемы медиаграмотности в развитии цифровых технологий» акцентируется внимание на значении навыков критического восприятия информации и способности граждан различать достоверные и фейковые сообщения в условиях цифровой среды [7].

Проблематика дезинформации в контексте информационных войн, как правило, исследуется с применением междисциплинарного подхода, объединяющего инструментарий политологии, социологии, психологии, теории медиакоммуникаций и кибербезопасности. Такой подход позволяет рассматривать дезинформацию не только как медийный феномен, но и как элемент более широких стратегий политического и геополитического воздействия.

Научная методология исследования дезинформации в условиях информационных войн включает теоретико-методологический анализ пропаганды и механизмов манипуляции общественным сознанием, а также эмпирические методы, в частности контент-анализ медиаматериалов и кейс-стади конкретных дезинформационных кампаний. Дополнительно применяется сравнительный анализ международных стратегий противодействия дезинформации, что позволяет оценить эффективность различных институциональных и технологических подходов к нейтрализации информационных угроз и выработке устойчивых моделей информационной безопасности.

Результаты

Согласно Информационной доктрине Республики Казахстан, утверждённой Указом Президента Республики Казахстан от 20 марта 2023

года № 145, анализ развития национального информационного пространства свидетельствует о необходимости принятия системных мер по защите отечественной информационной среды от внешнего деструктивного воздействия и дезинформации, оказывающих негативное влияние на ценностно-идеологические установки граждан и создающих угрозы внутриполитической стабильности государства [8]. Данный нормативный документ подчёркивает возрастающую значимость информационной безопасности как составной части национальной безопасности в условиях цифровой трансформации и усиления информационного противоборства.

Следует отметить, что на законодательном уровне в Республике Казахстан в настоящее время отсутствует юридически закреплённое определение понятия «дезинформация». Вместе с тем в научном и прикладном дискурсе дезинформация, как правило, понимается как преднамеренно ложная либо искажённая информация, создаваемая и распространяемая с целью введения аудитории в заблуждение, манипуляции общественным мнением либо нанесения ущерба отдельным лицам, организациям или государствам.

В содержательном понимании дезинформации можно выделить три ключевых структурных элемента: преднамеренность, неточность информации и целевую направленность. Преднамеренность означает, что ложная или искажённая информация создаётся и распространяется сознательно, а не в результате ошибки, некомпетентности или случайного искажения фактов. Неточность информации предполагает её ложный или искажённый характер: для достижения поставленных целей информация может быть изначально сконструирована как недостоверная либо трансформирована путём искажения ранее существовавших правдивых данных. Целевая направленность дезинформации выражается в стремлении ввести людей в заблуждение, манипулировать общественным мнением либо нанести репутационный, политический, экономический или иной ущерб. При этом цели дезинформации могут носить политический, экономический, идеологический или военно-стратегический характер.

Отдельного внимания заслуживают средства распространения дезинформации. Несмотря на то что данный компонент не относится к числу её базовых структурных элементов, он играет ключевую роль в формировании масштабов и интенсивности деструктивного воздействия на общественное сознание. Независимо от используемых каналов - будь то традиционные средства массовой информации, искусственно формируемые «экспертные» мнения, социальные сети, мессенджеры или иные цифровые платформы - любая информация, распространяемая с намерением ввести аудиторию в заблуждение, должна рассматриваться как часть дезинформационного механизма.

Показательным примером влияния цифровых платформ на репутационные и экономические процессы является кейс «музыкант против United Airlines». После отказа авиакомпании компенсировать ущерб за повреждённую гитару музыкант создал и опубликовал песню «United Breaks Guitars» на платформе YouTube. Видеоролик набрал более 12 миллионов просмотров, что привело к существенному общественному резонансу и падению стоимости акций компании примерно на 10%, вызвав убытки акционеров, оцениваемые в около 180 миллионов долларов США [9]. Данный пример наглядно демонстрирует, что цифровые коммуникационные каналы способны оказывать значительное воздействие не только на репутацию частных корпораций, но и на их экономическую устойчивость.

Однако влияние информационного пространства не ограничивается корпоративным сектором. В последние годы дезинформация и манипулятивные практики в социальных сетях всё активнее используются в политических целях, что создаёт прямые угрозы общественной стабильности и национальной безопасности. Осознавая данные риски, Президент Республики Казахстан Касым-Жомарт Токаев на расширенном заседании Правительства 28 января 2025 года отметил: «Все чаще мы сталкиваемся со случаями дезинформации и медиавбросами, направленными на манипуляцию общественным мнением, дискредитацию власти, разжигание розни. Это создает серьезные риски для безопасности граждан и стабильности в стране» [10]. В своём выступлении глава государства также подчеркнул необходимость совершенствования законодательного регулирования и усиления ответственности интернет-платформ за распространение деструктивного контента.

Таким образом, дезинформация представляет собой серьёзную угрозу социальной стабильности и национальной безопасности, что подтверждается как результатами научных исследований, так и официальными заявлениями государственных лидеров. Рассмотрение дезинформации как сложного социально-политического феномена позволяет выделить её ключевые структурные элементы, к которым относятся преднамеренность создания и распространения, искажённость или ложность информации, целевая направленность воздействия, а также механизмы и каналы распространения. Особое значение при этом приобретает роль средств массовой информации и цифровых платформ, обеспечивающих быстрый и масштабный охват аудитории и тем самым усиливающих деструктивный потенциал дезинформационных сообщений.

В этой связи регулирование каналов распространения информации выступает неотъемлемым элементом комплексной стратегии противодействия дезинформации и необходимым условием обеспечения устойчивости государства и общества. С учётом указанных факторов

становится очевидной необходимость законодательного закрепления понятия дезинформации, а также внедрения чётких правовых механизмов, направленных на предупреждение, выявление и пресечение её распространения. Принятие нормативно закреплённого определения дезинформации и установление ответственности за её создание и распространение позволит повысить эффективность противодействия угрозам, связанным с манипуляцией информацией, и обеспечить защиту интересов государства, общества и отдельных граждан в условиях динамично трансформирующегося информационного пространства.

В этой связи представляется целесообразным введение на законодательном уровне определения термина «дезинформация», учитывающего её ключевые характеристики, включая преднамеренность, неточность или искажённость информации, цели её распространения, а также механизмы, посредством которых она достигает широкой аудитории. В качестве возможной редакции предлагается следующее определение:

дезинформация - это преднамеренное распространение посредством различных средств коммуникации ложной и (или) искажённой информации с целью манипуляции общественным мнением, искажения фактов, а также нанесения ущерба отдельным лицам, организациям или государствам.

Кроме того, чёткое и однозначное определение дезинформации в контексте информационных войн необходимо для её разграничения со смежными понятиями, такими как пропаганда, фейковые новости и манипулятивные информационные практики. Это, в свою очередь, создаёт основу для разработки более эффективных правовых, институциональных и технологических механизмов противодействия деструктивному информационному воздействию. Наличие точного понятийного аппарата способствует повышению эффективности деятельности государственных органов, средств массовой информации и научного сообщества в сфере обеспечения информационной безопасности, а также содействует формированию устойчивых навыков медиаграмотности и критического мышления в обществе.

Обсуждения

В современном информационном пространстве целесообразно выделять три ключевых типа информационного контента, оказывающего влияние на общественное восприятие: ошибочную информацию, распространяемую без умысла; дезинформацию, характеризующуюся преднамеренным искажающим воздействием; а также правдивую информацию, используемую в различных целях. Каждый из указанных видов способен оказывать существенное воздействие на интерпретацию событий, формирование общественного мнения и, в конечном итоге,

на политические, социальные и экономические процессы.Ошибочная информация распространяется без намерения обмануть, зачастую из-за недосмотра или ошибок, например, в журналистике. В отличие от нее, дезинформация создается с целью манипуляции, распространения ложных и/или искаженных сведений, направленных на нанесение ущерба или продвижение определенных интересов. Дезинформация часто базируется на полуправде, где ложные элементы сливаются с правдивыми, что делает ее особенно опасной, поскольку вызывает доверие и более эффективно воздействует на аудиторию. В свою очередь, распространение правдивой частной информации с целью разрушения репутации акцентирует внимание на личных данных и фактах, которые могут быть использованы против конкретных лиц или организаций.

Продолжая анализ проблемы ответственности за манипуляцию информацией, следует подчеркнуть, что в современных условиях развитие информационных технологий и социальных сетей существенно усиливает деструктивный эффект дезинформации. Высокая скорость распространения сообщений, алгоритмическое продвижение контента и возможность анонимного участия в цифровых коммуникациях значительно усложняют идентификацию источников недостоверной информации и своевременное пресечение её распространения. В этих условиях ответственность за манипуляции в информационном пространстве требует комплексного и многоуровневого подхода, включающего не только правовое регулирование, но и активное участие общественных институтов, профессионального медиасообщества и технологических платформ.

Юридическая ответственность за манипуляцию информацией может реализовываться в форме административных штрафов, гражданско-правовых санкций или уголовного преследования, особенно в случаях, когда дезинформационные действия связаны с клеветой, нарушением авторских прав, незаконным использованием персональных данных либо утечкой конфиденциальной информации. Существенное значение приобретает также наличие институциональных механизмов противодействия распространению фейковых новостей и регулирования обработки персональных данных, направленных на минимизацию рисков их использования в манипулятивных целях.

Вместе с тем исключительно правовые меры не всегда способны обеспечить эффективное решение данной проблемы, поскольку манипулятивные информационные практики зачастую не поддаются однозначной юридической квалификации. В этой связи особую роль приобретает этическая ответственность всех участников информационного процесса. Журналисты, блогеры, общественные деятели и рядовые пользователи социальных сетей должны осознавать степень своего влияния

на информационное пространство и придерживаться профессиональных и моральных стандартов распространения информации. Одновременно возрастает значимость развития медиаграмотности и критического мышления среди населения, что позволяет снижать уязвимость общества к манипулятивным воздействиям и дезинформационным кампаниям.

Таким образом, ответственность за распространение манипулятивного контента представляет собой многомерный процесс, требующий согласованных усилий законодателей, медиаиндустрии, технологических компаний и институтов гражданского общества, направленных на защиту общественных интересов и сохранение доверия к информации в условиях цифровой трансформации.

Одним из наиболее распространённых методов дезинформации является распространение ложных и (или) искажённых новостей, при котором недостоверная или сфальсифицированная информация целенаправленно используется в средствах массовой информации и цифровых платформах. Применение технологий искусственного интеллекта, получивших широкое распространение в последние годы, значительно ускоряет процессы генерации и тиражирования подобного контента, усиливая его воздействие на коллективное сознание.

Манипулятивная информация нередко становится элементом недобросовестной журналистской практики, что проявляется, в частности, в использовании кликбейтных заголовков, искажении фактов либо их намеренном вырывании из контекста. Показательным примером является так называемое «дело Лизы» в Германии, когда сообщения о пропаже несовершеннолетней сопровождались информацией о росте числа сирийских мигрантов в соответствующем районе. Несмотря на формальную достоверность отдельных фактов, их контекстуальное сочетание формировало у аудитории ложное представление о причастности мигрантов к инциденту, что способствовало росту ксенофобских настроений и социальной напряжённости [11].

Отдельного внимания заслуживает использование дезинформации в качестве инструмента провокации конфликтов и целенаправленного формирования агрессии в отношении определённых социальных групп, этнических сообществ или идеологических концептов. Одним из методов подобного воздействия выступает выборочная цензура и селективная подача информации, направленная на управление эмоциональной реакцией аудитории. В этом случае факты могут представляться в преднамеренно искажённом или фрагментированном виде с целью вызова заданных эмоций и формирования определённых общественных настроений.

Применение дезинформации в цифровом пространстве носит массовый характер, при этом её инициаторами могут выступать как государственные,

так и негосударственные акторы. В интересах государства дезинформация нередко используется для манипуляции общественным сознанием, воздействия на электоральные процессы, а также влияния на политическую и экономическую обстановку в стране. В качестве примера можно привести предвыборную кампанию 2016 года в США, в ходе которой кандидат в президенты Дональд Трамп активно использовал социальную сеть Twitter в качестве инструмента прямого коммуникационного воздействия на электорат.

Негосударственные акторы, в свою очередь, применяют дезинформационные практики преимущественно для достижения собственных целей, включая коммерческую выгоду, политическое влияние или продвижение идеологических установок.

Таким образом, дезинформация в цифровую эпоху представляет собой серьёзную угрозу как национальной, так и международной безопасности, оказывая существенное влияние на общественное мнение, политическую стабильность и динамику социальных процессов. Эффективное противодействие данным угрозам требует комплексного сочетания правовых, этических, институциональных и образовательных мер.

Заключение

В условиях цифровой эпохи дезинформация трансформируется в один из наиболее действенных инструментов информационного воздействия, активно используемый в информационных и гибридных войнах для манипуляции общественным сознанием, дестабилизации государств и подрыва доверия к ключевым политическим и социальным институтам. Её масштабное распространение через социальные сети, новостные ресурсы и цифровые платформы формирует прямые угрозы национальной безопасности, способствуя росту социальной напряжённости, политической поляризации и эскалации международных конфликтов. В этой связи эффективное противодействие данным вызовам требует не только развития механизмов информационной защиты, но и чёткого правового осмысления и нормативного закрепления самого понятия дезинформации.

Законодательное определение дезинформации с учётом её ключевых характеристик - преднамеренности, искажённости информации, целевой направленности и механизмов распространения - позволит повысить результативность мер противодействия информационным угрозам и сформировать правовую основу для защиты общества от манипулятивного воздействия. Чёткое разграничение дезинформации от смежных явлений, таких как пропаганда, ошибочная информация и иные формы информационного влияния, создаёт предпосылки для разработки адресных и эффективных стратегий регулирования и пресечения её распространения. В

конечном итоге это способствует укреплению национальной безопасности, защите демократических институтов и формированию устойчивой и доверительной информационной среды.

В современном мире информация перестала быть исключительно средством передачи знаний и приобрела статус стратегического ресурса, способного оказывать существенное влияние на общественное сознание, политические процессы и экономическую динамику. В этом контексте дезинформация как форма целенаправленной манипуляции представляет собой серьёзную угрозу социальной стабильности, общественному доверию и функционированию государственных институтов.

Противодействие распространению ложных и искажённых сведений требует комплексного подхода, объединяющего правовые, технологические и образовательные меры. Законодательные инициативы должны обеспечивать нормативное закрепление понятия дезинформации, её разграничение с другими формами информационного воздействия, а также разработку механизмов ответственности за манипуляцию общественным мнением. Технологические компании и медиаструктуры, в свою очередь, обязаны внедрять эффективные инструменты проверки информации, ограничивать распространение заведомо недостоверного контента и повышать прозрачность алгоритмов формирования информационной повестки.

Особую роль в обеспечении устойчивости информационного пространства играет повышение уровня медиаграмотности населения, позволяющее гражданам критически оценивать источники информации, выявлять манипулятивные практики и снижать собственную уязвимость к дезинформационным воздействиям. Ответственность за состояние информационной среды лежит не только на государственных институтах, но и на самих пользователях, осознающих необходимость проверки информации перед её распространением.

Эффективное противодействие дезинформации предполагает реализацию комплекса взаимосвязанных мер, включающих совершенствование законодательства, усиление ответственности интернет-платформ, развитие медиаграмотности, поддержку независимых фактчекинговых инициатив, а также создание специализированных государственных структур по противодействию фейковой информации. Существенное значение приобретает и международное сотрудничество в сфере информационной безопасности, направленное на противодействие трансграничным дезинформационным кампаниям и киберугрозам. Одновременно необходимо формирование культуры информационной ответственности среди журналистов, блогеров и пользователей цифровых платформ, поскольку только согласованные действия государства, гражданского

общества, научного сообщества и медиасферы способны обеспечить устойчивость информационного пространства.

Таким образом, противодействие дезинформации требует консолидации усилий общества, медиа, науки и государства. Лишь всесторонний и системный подход позволяет минимизировать деструктивное воздействие информационных войн и обеспечить устойчивость общества перед вызовами цифровой эпохи.

ЛИТЕРАТУРА

[1] Скурлатова С. Deepfake: как искусственный интеллект размывает границы между фейком и реальностью [Электронный ресурс]. – URL: https://ipquorum.ru/news/109-deepfake-kak-iskusstvennyj-intellekt-razmyvaet-granicy-mezdu-fejkom-i-realnostu (дата обращения: 18.12.2025).

[2] Boyd-Barrett J. Media Imperialism / J. Boyd-Barrett. – Bowling Green State University, 2015. – Электронный ресурс. – URL: https://www.researchgate.net/publication/348444219_Media_Imperialism (дата обращения: 22.12.2025).

[3] Chomsky N. 10 strategies of manipulation by the media [Электронный ресурс]. – URL: https://www.abovetopsecret.com/forum/thread633151/pg1/ (дата обращения: 27.12.2025).

[4] Журналистика, «фейковые новости» и дезинформация: руководство для академической и профессиональной подготовки журналистов / Серия ЮНЕСКО по журналистскому образованию. – Париж : UNESCO, 2018. – Электронный ресурс. – URL: https://unesdoc.unesco.org/ark:/48223/pf0000371785 (дата обращения: 15.12.2025).

[5] Ctengel P. Информационные войны. Как мы проиграли глобальную битву против дезинформации [Электронный ресурс]. – URL: https://adamashek.livejournal.com/1510918.html (дата обращения: 29.12.2025).

[6] Султанбаева Г., Толеген Б., Ложникова О., Буенбаева З., Тюлепбердинова Г. Распространение фейковой и некорректной информации в социальных сетях // *Вестник КазНУ. Серия журналистики*. – 2024. – Т. 72, № 2. – Электронный ресурс. – URL: https://bulletin-journalism.kaznu.kz/index.php/1-journal/article/view/1849 (дата обращения: 20.12.2025).

[7] Шакенова Ш. Проблемы медиаграмотности в развитии цифровых технологий // *Вестник КазНУ. Серия журналистики*. – 2024. – Т. 74, № 4. – Электронный ресурс. – URL: https://bulletin-journalism.kaznu.kz/index.php/1-journal/article/view/1920 (дата обращения: 24.12.2025).

[8] Об утверждении Информационной доктрины Республики Казахстан: Указ Президента Республики Казахстан от 20 марта 2023 г. № 145 [Электронный ресурс]. – URL: https://adilet.zan.kz (дата обращения: 30.12.2025).

[9] Howell L. Global Risks 2013. Eighth Edition. – Geneva : World Economic Forum, 2013. – 25 p. – Электронный ресурс. – URL: https://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf (дата обращения: 16.12.2025).

[10] Токаев К.-Ж. Выступление Главы государства на расширенном заседании Правительства Республики Казахстан от 28 января 2025 г. [Электронный ресурс]. – URL: https://www.akorda.kz/ru/vystuplenie-glavy-gosudarstva-kasym-zhomarta-tokaeva-na-rasshirennom-zasedanii-pravitelstva-2801458 (дата обращения: 19.12.2025).

[11] Жапарова Ж. Манипуляция в СМИ и соцсетях: как распознать скрытые механизмы влияния [Электронный ресурс]. – URL: https://liter.kz/manipuliatsiia-v-smi-i-sotssetiakh-kak-raspoznat-skrytye-mekhanizmy-vliianiia-1734072626/ (дата обращения: 26.12.2025).

ДЕЗИНФОРМАЦИЯ ИНФОРМАЦИЯЛЫҚ СОҒЫСТАРДЫҢ ҚҰРАЛЫ РЕТІНДЕ ЖӘНЕ ҰЛТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАУІП ФАКТОРЫ

Кошербаев Ж.Д.[1], [*] Махмадин А.Д.[2], Мельдибекова З.А.[3]
[1, *2] Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
[3] Халықаралық ақпараттық технологиялар университеті,
Алматы, Қазақстан

Аңдатпа. Мақалада дезинформация ақпараттық және гибридтік соғыстардың негізгі құралдарының бірі ретінде қарастырылып, оның қоғамдық санаға, саяси тұрақтылыққа және мемлекеттердің ұлттық қауіпсіздігіне тигізетін ықпалы талданады. Цифрлық трансформация жағдайында, әлеуметтік желілердің, алгоритмдік платформалардың және жасанды интеллект технологияларының қарқынды дамуы нәтижесінде дезинформация жүйелі сипатқа ие болып, аудиторияны жылдам әрі ауқымды қамту мүмкіндігі арқылы ақпараттық ықпалдың деструктивті әлеуетін күшейтеді.

Зерттеудің мақсаты – цифрлық технологиялар арқылы таралатын дезинформация мен пропагандаңы кешенді талдау, манипулятивтік ақпараттық ықпал етуді зерттеудің әдіснамалық тәсілдерін айқындау, оның әлеуметтік және саяси салдарын бағалау, сондай-ақ ұлттық қауіпсіздікке қауіп төндіретін дезинформациялық тәжірибелерге қарсы іс-қимыл бағыттарын әзірлеу. Зерттеу нысаны ретінде ақпараттық соғыстардың құралы ретіндегі дезинформация алынса, зерттеу пәні – оның цифрлық ортада қалыптасу, таралу және ықпал ету тетіктері болып табылады.

Зерттеудің әдіснамалық негізін пәнаралық тәсіл құрайды. Зерттеу барысында талдау мен синтез, жүйелік және салыстырмалы талдау әдістері,

медиаматериалдарға контент-талдау, нақты дезинформациялық науқандарды кейс-стади әдісімен зерттеу, сондай-ақ Қазақстан Республикасының стратегиялық нормативтік-құқықтық құжаттарына құқықтық талдау жүргізілді. Жұмыста дезинформацияның тиімділігі әдейі бұрмаланған контенттің қолданылуы, цифрлық платформалар арқылы алгоритмдік күшейту және оны таратуға қатысты құқықтық реттеудің жеткіліксіздігімен айқындалатыны туралы гипотеза негізделді.

Зерттеудің ғылыми жаңалығы дезинформацияның құрылымданған моделін ұсынуымен, осы ұғымның авторлық анықтамасын беруімен және оны заңнамалық деңгейде бекіту қажеттігін негіздеуімен сипатталады. Зерттеу нәтижесінде дезинформацияға қарсы іс-қимыл ұлттық қауіпсіздік пен ақпараттық кеңістіктің тұрақтылығын нығайтуға бағытталған кешенді құқықтық, институционалдық және білім беру шараларын талап ететіні туралы қорытынды жасалды.

Тірек сөздер: дезинформация, ақпараттық соғыстар, ұлттық қауіпсіздік, қоғамдық сананы манипуляциялау, цифрлық платформалар, медиасауаттылық, ақпараттық қауіпсіздік

DISINFORMATION AS A TOOL OF INFORMATION WARS AND A THREAT FACTOR TO NATIONAL SECURITY

Kosherbayev Zh.D.[1], *Makhmadin A.D.[2], Meldibekova Z.A.[3]
[1, *2] Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3] International University of Information Technology, Almaty, Kazakhstan

Abstract. This article examines disinformation as one of the key instruments of information and hybrid warfare, exerting a significant influence on public consciousness, political stability, and the national security of states. In the context of digital transformation and the rapid development of social media, algorithm-driven platforms, and artificial intelligence technologies, disinformation has acquired a systemic character, enabling fast and large-scale audience reach and amplifying the destructive potential of informational influence.

The aim of the study is to provide a comprehensive analysis of disinformation and propaganda disseminated through digital technologies, to identify methodological approaches to the study of manipulative informational influence, to assess its social and political consequences, and to develop directions for countering disinformation practices that pose threats to national security. The object of the research is disinformation as a tool of information warfare, while the subject of the research includes the mechanisms of its creation, dissemination, and impact in the digital environment.

The methodological framework of the study is based on an interdisciplinary approach that integrates methods of analysis and synthesis, systemic and

comparative analysis, content analysis of media materials, case studies of specific disinformation campaigns, and normative-legal analysis of strategic documents of the Republic of Kazakhstan. The study substantiates the hypothesis that the effectiveness of disinformation is determined by the combination of deliberate content distortion, algorithmic amplification by digital platforms, and insufficient legal regulation of responsibility for its dissemination.

The scientific novelty of the research lies in the proposal of a structured model of disinformation, the formulation of an author's definition of the concept, and the substantiation of the necessity of its legislative consolidation. The study concludes that effective counteraction to disinformation requires комплексные legal, institutional, and educational measures aimed at strengthening the resilience of the information space and national security.

Keywords: disinformation, information warfare, national security, manipulation of public consciousness, digital platforms, media literacy, information security

Статья поступила / Мақала түсті / Received: 27.01.2026.
Принята к публикации / Жариялауға қабылданды / Accepted: 27.03.2026.

Сведения об авторах:

Кошербаев Жан Дуйсенбекович - кандидат исторических наук, доцент Казахского национального университета имени аль-Фараби, г. Алматы, Республика Казахстан. e-mail: Kosherbaev.zhan@gmail.com ORCID: https://orcid.org/0000-0002-1187-9837

Махмадин Алима Даулеткелдіқызы - магистрант 2 курса образовательной программы «Международные отношения» Казахского национального университета имени аль-Фараби, г. Алматы, Республика Казахстан. e-mail: alima.makhmadin@mail.ru ORCID: https://orcid.org/0009-0003-2637-9821 (*корреспондирующий автор)

Мельдибекова Зульфия Абдихалыковна - кандидат исторических наук, доцент Международного университета информационных технологий, г. Алматы, Республика Казахстан. E-mail: z.meldibekova@iitu.edu.kz ORCID: https://orcid.org/0000-0003-2042-5316

Авторлар туралы мәліметтер:

Кошербаев Жан Дүйсенбекұлы - тарих ғылымдарының кандидаты, доцент, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан Республикасы. e-mail: Kosherbaev.zhan@gmail.com ORCID: https://orcid.org/0000-0002-1187-9837

Махмадин Әлима Даулеткелдіқызы - «Халықаралық қатынастар» білім беру бағдарламасының 2-курс магистранты, Әл-Фараби атындағы

Қазақ ұлттық университеті, Алматы қ., Қазақстан Республикасы. e-mail: alima.makhmadin@mail.ru ORCID: https://orcid.org/0009-0003-2637-9821 (автор-корреспондент)

Мельдибекова Зульфия Әбдіхалыққызы - тарих ғылымдарының кандидаты, доцент, Халықаралық ақпараттық технологиялар университеті, Алматы қ., Қазақстан Республикасы. e-mail: z.meldibekova@iitu.edu.kz ORCID: https://orcid.org/0000-0003-2042-5316

Information about the Authors:

Zhan Duisenbekovich Kosherbayev - Candidate of Historical Sciences, Associate Professor at Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan. e-mail: Kosherbaev.zhan@gmail.com ORCID: https://orcid.org/0000-0002-1187-9837

Alima Dauletkeldikyzy Makhmadin - 2nd-year Master's student in International Relations, Al-Farabi Kazakh National University, Almaty, Republic of Kazakhstan. e-mail: alima.makhmadin@mail.ru ORCID: https://orcid.org/0009-0003-2637-9821 (* Corresponding author)

Zulfiya Abdhikhalykovna Meldibekova - Candidate of Historical Sciences, Associate Professor at the International University of Information Technology, Almaty, Republic of Kazakhstan. e-mail: z.meldibekova@iitu.edu.kz ORCID: https://orcid.org/0000-0003-2042-5316