Сапронов Ярослав Денисович
аспирант
ФГАОУ ВО «Уральский федеральный университет
им. первого Президента России Б.Н. Ельцина»
г. Екатеринбург, Свердловская область

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ ДЕЗИНФОРМАЦИИ В КОНТЕКСТЕ ФОРМИРОВАНИЯ СОЦИАЛЬНО-КУЛЬТУРНОГО ПРОСТРАНСТВА РОССИИ

Аннотация: *в статье рассматривается формирование социально-культурного пространства России через призму правовых механизмов противодействия дезинформации. Проанализировано современное состояние нормативной правовой базы Российской Федерации в сфере информационной безопасности, включая положения Стратегии национальной безопасности, закрепляющей информационную безопасность как приоритет государственной политики. Исследуются понятия дезинформации и вредоносной информации, их различия, а также механизмы их распространения и социально-политические последствия. Предложена авторская классификация мер противодействия дезинформации, включающая институциональные, технологические и образовательные подходы. Подчеркивается необходимость комплексного использования правовых, технологических и просветительских инструментов для обеспечения информационной безопасности и формирования устойчивого социально-культурного пространства в условиях цифровой трансформации общества.*

Ключевые слова: *дезинформация, информационная безопасность, правовые механизмы, социально-культурное пространство, Стратегия национальной безопасности.*

Введение.

В современном мире роль информации в жизни личности, общества и государства не просто значительно возросла, но и стала одной из ключевых основ развития. В Российской Федерации, следуя примеру ведущих мировых держав,

стартовал процесс формирования информационного общества, в основе которого лежат информация и знания.

В этих условиях цифровизации общественных процессов публичное информационное пространство становится одной из ключевых сфер обеспечения национальной безопасности. При этом распространение ложной и вредоносной информации приобретает системный характер, влияя на общественную стабильность, уровень доверия к государственным институтам и реализацию стратегических национальных приоритетов.

В своем Послании Федеральному Собранию Российской Федерации Президент РФ В.В. Путин подчеркнул, что IT-индустрия стала одной из самых быстроразвивающихся отраслей [7]. В связи со становлением информационного общества перед государством появляются новые задачи, одна из которых – обеспечение информационной безопасности при распространении информации в публичном пространстве. Вопросы обеспечения информационной безопасности включены практически во все разделы, посвященные реализации стратегических национальных приоритетов, новой редакции Стратегии национальной безопасности Российской Федерации [6].

Обозначенные в Стратегии положения получили свое развитие и в новой редакции Доктрины информационной безопасности Российской Федерации. В этом документе не только дана оценка современному состоянию информационной безопасности Российской Федерации, но и определен перечень угроз, а также совокупность средств, способных обеспечить должный уровень защиты информационной безопасности РФ [4]. Однако трансформация цифровых коммуникаций, алгоритмизация распространения контента и высокая скорость тиражирования сообщений обуславливают необходимость комплексной оценки как правовых механизмов, так и современных способов противодействия дезинформации.

В настоящее время в России практически отсутствует уголовная политика в сфере противодействия преступлениям против информационной безопасности, а административная только начинает развиваться, поэтому, одним из главных во-

просов современной информационной безопасности является борьба распространения в ложной и вредоносной информации в сети Интернет и публичном пространстве [9]. В статье предложена классификация современных методов противодействия распространению ложной и вредоносной информации, рассматривающая их как многоуровневую систему правовых, организационных, технических и информационно-коммуникационных мер.

1. *Анализ действующей нормативно-правовой базы по противодействию ложной и вредоносной информации.*

Прежде, чем начать анализ нормативно-правовой базы в РФ, разберём понятия ложной и вредоносной информации, а также, их ключевые различия.

Ложная информация – это сведения, которые не соответствуют действительности. Они могут быть созданы случайно или намеренно, но без цели нанести вред. Наиболее распространенными примерами ложной информации являются: ошибки в новостях, неверные данные, мифы, слухи.

Вредоносной считается информация, которая предназначена для специального причинения вреда людям, организациям, обществу, а главное, безопасности в публичном пространстве. Вредоносная информация может включать в себя ложную информацию, но ее цель – манипуляция, дезинформация, подрыв доверия, причинение ущерба и нанесение угрозы безопасности распространения правдивой информации в сети Интернет. Примерами вредоносной информации считается пропаганда, кибербуллинг, фейковые новости с целью вызвать панику [9].

Ключевые различия между ложной и вредоносности информацией представлены в таблице 1.

Таблица 1

Различия ложной и вредоносной информации

Характеристика	Ложная информация	Вредоносная информация
Соответствие истине	Не соответствует (ложь или ошибка)	Может быть ложной или правдивой, но используется во вред
Намерение	Часто случайное, без умысла	Осознанное, с целью нанести вред

Цель	Может быть ошибкой, заблуждением	Вред, манипуляция, дезинформация
Примеры	Ошибочные данные, мифы	Фейковые новости, пропаганда, кибератаки
Эффект	Может вводить в заблуждение	Вредит репутации, безопасности, вызывает панику и конфликт

Таким образом, ключевым отличием вредоносной информацией от ложной является наличие цели причинить вред, путем искажения информации, в отличие от ложной, которая может быть просто ошибочной [12].

В эпоху информационных технологий и быстрого обмена данными проблема распространения ложной и вредоносной информации стала одной из важнейших для общества и государства. Неоправданное вложение фальшивых сведений, фейков, агитации, а также вредоносного контента несёт угрозу безопасности, общественному порядку и правам граждан. В связи с этим законодательные органы разных стран, включая Россию, активно разрабатывают и совершенствуют правовые нормы и механизмы борьбы с такими явлениями.

В России вопросы противодействия распространению ложной и вредоносной информации регулируются рядом законов и подзаконных актов, призванных создать контроль и ответственность за информационные действия в сети Интернет и других средствах массовой информации [3].

Указ №400 от 2 июля 2021 г. утверждает Стратегию национальной безопасности Российской Федерации, которая с точки зрения стратегического планирования является базовым документом, определяющим национальные интересы, стратегические приоритеты и цели государственной политики в области национальной безопасности [6]. В Стратегии отражена широкая концепция информационной безопасности как части национальной безопасности.

Ключевые положения, связанные с информационной безопасностью:

− информационная безопасность объявлена одной из стратегических составляющих национальной безопасности РФ. Это включает развитие безопасного информационного пространства и защиту общества от деструктивного информационно-психологического воздействия;

− определение угроз, связанных с распространением недостоверной информации, включая провокации, информационные кампании, направленные на дестабилизацию общества и угрозу общественно-политической стабильности;

− необходимость создания механизмов предотвращения, выявления и пресечения преступлений в информационной сфере, защиты российских информационных ресурсов от манипуляций и внешнего контроля, обеспечения достоверной информации как внутри страны, так и для международной общественности.

Таким образом, Стратегия формирует основу и направление последующего законодательного регулирования, в том числе через федеральные законы, подзаконные акты и ведомственные нормативы [3].

Далее представлены основные законы, описывающие и регулирующие данную сферу.

Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.) Это базовый закон регулирует отношения, связанные с информацией, устанавливает права и обязанности пользователей, операторов информации и государственных органов. В нем прописаны нормы по борьбе с распространением запрещённой информации.

Федеральный закон №97-ФЗ «О противодействии экстремистской деятельности» (2002 г.) Хотя основной фокус – экстремизм, закон затрагивает и запрещённый к распространению контент с агрессивным и провокационным характером, в том числе распространяемый в сети Интернет.

Федеральный закон №272-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (2010 г.). Закон регулирует доступ несовершеннолетних к вредной информации, в том числе ложной или манипулятивной.

Федеральный закон №436-ФЗ о защите персональных данных (2019 г.). Этот закон регулирует обработку и защиту персональных данных, что косвенно относится к противодействию распространению недостоверной информации, связанной с личными данными.

Федеральный закон №187-ФЗ «О внесении изменений в Федеральный закон «Об информации» и отдельные законодательные акты» (2021 г.). Этот закон усилил механизмы борьбы с фейками и вредоносной информацией в интернете.

Представленные законы являются основными, также есть и дополнительные российских законы и акты для борьбы с вредоносной информацией в сети Интернет, представленные в таблице 2.

Таблица 2

Примеры российских законов для борьбы
с вредоносной информацией в сети Интернет

Закон и дата	Суть и основные положения
№149-ФЗ «Об информации» (2006)	Устанавливает общие правила работы с информацией, права и ответственность за распространение запрещённого контента, санкции по делам о ложной информации
№187-ФЗ (2021)	Вводит ответственность за распространение фейковой информации, которая может вызвать вред здоровью, безопасности, или массовые нарушения общественного порядка
№436-ФЗ о защите перс. данных (2019)	Защищает персональные данные, препятствуя распространению недостоверной информации, нарушающей конфиденциальность и права граждан
Закон о Fake News (модификации 2020–2022)	Ужесточил ответственность за фейки и дезинформацию в интернете, в том числе с возможностью административных штрафов и блокировки сайтов

В настоящее время ключевые законодательные инициативы включают в себя меры по контролю распространения вредоносной информации в сети интернет и блокировке запрещенной информации в публичном пространстве, уточнение понятий «дискредитация» и ответственности за распространение информации, помогающей обходить ограничения.

2. *Анализ механизмов распространения ложной и вредоносной информации в публичном информационном пространстве.*

2.1. *Технологии искусственного интеллекта.*

С развитием технологий искусственного интеллекта, в частности генеративных нейросетей, широкое распространение получила технология deepfake. Она позволяет создавать высоко-реалистичные аудио- и видеоматериалы с подменой лица, и голоса конкретных лиц [5].

Использование deepfake создает угрозу для:

− политической стабильности (дискредитация лидеров государств);

− репутации публичных персон;

− коммерческой безопасности компаний (создание ложных заявлений руководства);

− национальной безопасности (информационные провокации).

Особую опасность представляют синхронизированные информационные атаки, при которых фальсифицированные материалы распространяются одновременно на нескольких платформах с целью создания иллюзии достоверности.

2.2. *Боты и автоматизированные аккаунты.*

Использование автоматизированных аккаунтов (ботов) в социальных сетях является распространённым инструментом манипуляции общественным мнением. Боты способны:

− массово тиражировать ложные сообщения;

− формировать искусственную поддержку определённых позиций;

− провоцировать информационные конфликты;

− искажать результаты онлайн-опросов и обсуждений.

Координированные сети ботов (botnets) применяются для создания эффекта «информационного большинства», что психологически влияет на пользователей через механизм социального доказательства.

2.3. *Фишинг и социальная инженерия.*

Фишинговые атаки представляют собой форму целенаправленного обмана, основанного на принципах социальной инженерии. Злоумышленники, выдавая себя за доверенные организации или должностных лиц, направляют пользователям электронные письма или сообщения с целью получения конфиденциальной информации [13].

Такие атаки могут быть направлены:

− на частных пользователей (кража персональных данных);

− на корпоративные структуры (получение доступа к коммерческой тайне);

− на государственные учреждения (компрометация служебной информации).

Эффективность фишинга обусловлена использованием психологических механизмов доверия, страха, срочности и авторитета.

2.4. *Целенаправленные информационные кампании.*

В условиях глобализации информационного пространства дезинформация нередко используется как инструмент достижения политических и экономических целей [8]. Государственные факторы, а также крупные корпоративные структуры могут инициировать информационные кампании, направленные на:

− влияние на электоральные процессы;

− дискредитацию политических и экономических оппонентов;

− формирование выгодной интерпретации событий;

− создание искусственного информационного повода;

− продвижение идеологических установок.

Подобные кампании нередко сочетают в себе использование фальсифицированного контента, сетей ботов, таргетированной рекламы и аналитики больших данных.

Распространение дезинформации оказывает комплексное воздействие на общественные процессы.

В социальной сфере:

− снижение уровня доверия к средствам массовой информации и государственным институтам;

− рост поляризации общества;

− формирование искаженной картины реальности.

В политической сфере:

− вмешательство в избирательные процессы;

− усиление протестных настроений;

− подрыв легитимности органов власти.

В экономическая сфере:

− репутационные потери компаний;

− финансовые убытки вследствие панических настроений;

− манипуляции фондовыми рынками.

В сфере информационная безопасности:

− утечка конфиденциальных данных;

− кибератаки, сопровождаемые информационным давлением;

− дестабилизация критической инфраструктуры.

3. *Классификация современных методов противодействия распространению ложной и вредоносной информации в публичном информационном пространстве.*

Комплексное противодействие дезинформации предполагает следующее:

− развитие цифровой грамотности населения;

− совершенствование нормативно-правовой базы;

− внедрение технологий автоматической проверки фактов;

− развитие международного сотрудничества в сфере кибербезопасности;

− создание механизмов ответственности за распространение заведомо ложной информации.

Особое значение приобретает междисциплинарный подход, объединяющий усилия специалистов в области информационных технологий, права, социологии и политологии [2].

Рассмотрим ключевые способы противодействия распространению ложной информации в публичном пространстве. Например, фильтрация и блокировка сайтов является основным способом борьбы с распространим информации, угрожающей безопасности общества. Роскомнадзор имеет полномочия вносить в реестр запрещённых ресурсов сайты, распространяющие ложную, экстремистскую или вредоносную информацию.

Вторым методом противодействия распространению ложной информации является ответственность за это распространение. Административные и уголовные наказания предусмотрены за создание и распространение заведомо ложной информации, способной нанести вред.

Еще одним способом противодействия является обязательность маркировки. Закон обязывает интернет-площадки и СМИ маркировать контент, содержащий информацию, вызывающую сомнения или требующую проверки.

В целях систематизации существующих подходов предлагается *авторская классификация методов противодействия ложной и вредоносной информации*. В отличие от существующих подходов, преимущественно ориентированных либо на правовые, либо на технологические аспекты противодействия, предлагается интегративная модель, учитывающая институциональный, технологический и социокультурный уровни воздействия.

3.1. *Институциональные методы.*

Данная группа объединяет меры, реализуемые через правовые механизмы и деятельность публичных и профессиональных институтов.

3.1.1. *Государственное регулирование и правоприменение.*

Принятие и реализация нормативных правовых актов, устанавливающих ответственность за распространение заведомо ложной информации; создание механизмов мониторинга публичного информационного пространства; взаимодействие органов государственной власти с операторами связи и цифровыми платформами в целях оперативного пресечения нарушений [11].

3.1.2. *Медийные проекты контроля фактов.*

Специальные программы и проекты, осуществляющие проверку фактов, критическую экспертизу сообщений и формирование общественно доступной базы разоблачённых фейков. К числу подобных относится передача «Антифейк» на телеканале Россия 24, направленная на выявление и опровержение ложных сведений, циркулирующих в публичном пространстве.

3.1.3. *Международное сотрудничество.*

Объединение усилий государств и международных организаций для обмена информацией о новых трендах дезинформации, выработки общих стандартов реагирования и совместных стратегий регулирования.

3.2. *Технологические методы.*

Технологические методы предполагают использование цифровых инструментов для выявления, ограничения и предупреждения распространения дезинформации [14; 15].

3.2.1. *Алгоритмическое выявление недостоверного контента.*

Использование методов машинного обучения и искусственного интеллекта для анализа текстов, изображений и видео с целью выявления аномалий и признаков манипуляции (в том числе deepfake контента).

3.2.2. *Платформенные инструменты модерации.*

Внедрение цифровыми платформами автоматизированных и комбинированных (автоматических и экспертных) механизмов фильтрации контента, ограничения охвата публикаций с признаками недостоверности и блокирования координированных сетей распространения.

3.2.3. *Системы верификации источников.*

Использование систем подтверждения подлинности аккаунтов и источников информации, метаданных, цифровых подписей и иных инструментов, обеспечивающих прослеживаемость происхождения контента.

3.3. *Образовательные и социокультурные методы.*

Данная группа направлена на формирование устойчивости общества к информационным манипуляциям и снижение восприимчивости к дезинформации.

3.3.1. *Повышение медиаграмотности.*

Образовательные программы, направленные на формирование критического отношения к информации у широких слоёв населения [11]:

− обучение навыкам критического мышления;

− понимание структуры цифрового контента;

− умение различать достоверные и недостоверные источники.

3.3.2. *Этика и саморегуляция СМИ.*

Внедрение отраслевых стандартов журналистской деятельности, механизмов внутренней проверки фактов и добровольных кодексов поведения для редакций и цифровых платформ.

3.3.3. *Публичные кампании по информированию.*

Распространение публичных сообщений об угрозах дезинформации, в том числе через государственные и частные кампании, направленные на повышение осведомлённости населения.

Подводя итог, отметим, что современное информационное пространство требует комплексного подхода к борьбе с ложной и вредоносной информацией. В России для этого создана достаточно развитая нормативно-правовая база, сочетающая административные, уголовные меры, технические технологии.

Предложенная классификация отражает многоуровневый характер противодействия распространению ложной и вредоносной информации и демонстрирует взаимосвязь правовых, технологических и социокультурных механизмов в системе обеспечения информационной безопасности.

Заключение.

Современное цифровое пространство характеризуется высокой степенью открытости и доступности информации, что, с одной стороны, расширяет возможности коммуникации и участия граждан в общественной жизни, а с другой – создает условия для масштабного и ускоренного распространения ложной и вредоносной информации.

Проведённый анализ показал, что нормативные ориентиры противодействия деструктивному информационному воздействию закреплены в Стратегия национальной безопасности Российской Федерации и получили развитие в Доктрина информационной безопасности Российской Федерации, а также в действующем законодательстве Российской Федерации. Сформирована правовая основа реагирования на угрозы в информационной сфере, однако её эффективность во многом зависит от учёта технологических особенностей цифровой среды и динамики информационных рисков.

Исследование механизмов распространения дезинформации позволило установить, что алгоритмизация контента, использование автоматизированных сетей, технологий deepfake, фишинговых систем и координированных информационных кампаний формируют многоуровневую систему воздействия на массо-

вое сознание. Это подтверждает необходимость комплексного подхода к противодействию, сочетающего правовые, организационные, технические и информационно-коммуникационные инструменты.

Предложенная в статье классификация современных методов противодействия распространению ложной и вредоносной информации позволяет рассматривать их как взаимосвязанную систему мер, направленных не только на пресечение противоправного контента, но и на формирование устойчивости общества к информационным манипуляциям. Таким образом, обеспечение информационной безопасности в публичном пространстве требует дальнейшего развития нормативного регулирования и его согласования с технологической реальностью цифровой эпохи.

Список литературы

1. Базаркулова К.Ю. Использование приемов «медиаграмотности» для распознавания fake news / К.Ю. Базаркулова // Научные записки молодых исследователей. – 2022. – Т. 10. №5. – С. 36–45. EDN KTHWPQ

2. Бучакова М.А. Распространение деструктивной информации в информационном пространстве: проблемы и пути решения / М.А. Бучакова, А.В. Честнов // Вестник Сибирского юридического института МВД России. – 2025. – №2(59).

3. Вострецова Е.В. Основы информационной безопасности: учеб. пособие / Е.В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с. EDN TBHRSS

4. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 №646. – URL: http://www.scrf.gov.ru/documents/1/133.html (дата обращения: 15.02.2026).

5. Каширина Е.И. Дезинформация: анализ, последствия и противодействие / Е.И. Каширина, А.С. Никляева // Вестник Уральского юридического института МВД России. –2025. – №1(45). – С. 9–14. EDN DTSEBJ

6. Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» №400 от 02.07.2021 // Собрание законодательства Российской Федерации. – 2021. – №27, ч. 1. – Ст. 5351.

7. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 01.12.2026 // Кремль. – URL: http://kremlin.ru/events/president/news/53379 (дата обращения: 12.02.2026).

8. Соколов А.Ю. Правовое противодействие современным вызовам и угрозам информационной безопасности / А.Ю. Соколов // Правовая политика и правовая жизнь. – 2024. – URL: https://article/n/pravovoe-protivodeystvie-sovremennym-vyzovam-i-ugrozam-informatsionnoy-bezopasnosti/viewer (дата обращения: 06.05.2026).

9. Стернин И.А. Маркеры фейка в медиатекстах : пособие / И.А. Стернин, А.М. Шестерина. – Воронеж: РИТМ, 2021. – 60 с.

10. Стратегия национальной безопасности Российской Федерации: утв. Указом Президента РФ от 31.12.2015 №683. – URL: http://www.scrf.gov.ru/security/docs/document133/ (дата обращения: 12.02.2026).

11. Шереметьева У.М. Информационная безопасность: учеб. пособие / У.М. Шереметьева. – Томск: Изд-во ТГПУ, 2009. – 142 с. EDN OVWTGT

12. Linguistic Features and Bi-LSTM for Identification of Fake News / A.A. Ali, S. Latif, S.A. Ghauri, O.-Y. Song // Electronics. – 2023. – Vol. 12.

13. Identifying Fake News on Social Networks Based on Natural Language Processing: Trends and Challenges / N.R. de Oliveira, P.S. Pisa, M.A. Lopez [et al.] // Information. – 2021. – Vol. 12. – Article 38.

14. Dementieva D. Multiverse: Multilingual Evidence for Fake News Detection / D. Dementieva, M. Kuimov, A. Panchenko // Journal of Imaging. – 2023. – Vol. 9. No. 4. – Article 77. DOI 10.3390/jimaging9040077. EDN TQPBLJ

15. Hamed S.Kh. A Review of Fake News Detection Models / S.Kh. Hamed, M.J. Ab Aziz, M.R. Yaakub // International Journal of Advanced Computer Science and Applications (IJACSA). – 2023. – Vol. 14. No. 7.