**УДК 327.88:351.751**

**DOI: 10.55959/MSU2070-1381-115-2026-52-65**

# Информационная безопасность России: основные меры по противодействию угрозе фейковых новостей

**Юсупов Марат Минаятович**
Аспирант, marat_yusupovv@list.ru, IusupovMM@spa.msu.ru

Факультет государственного управления, МГУ имени М.В. Ломоносова, Москва, РФ.

**Аннотация**
В статье рассматривается важная для отечественной науки и практики проблема противодействия фейковым новостям в контексте обеспечения информационной безопасности Российской Федерации. Актуальность темы обосновывается возросшей ролью информационных войн и дезинформации в современном мире, особенно в условиях проведения специальной военной операции на Украине. Методологической основой исследования служит анализ нормативно-правовых актов, регулирующих сферу информационной безопасности в России, а также изучение научной литературы по проблемам информационных войн и фейковых новостей. В статье используется также сравнительный метод для оценки различных подходов к противодействию дезинформации. В результате исследования выявляются ключевые вызовы, связанные с массовым распространением недостоверной информации в российском медиапространстве, анализируются конкретные примеры фейковых новостей и организованных кампаний по дезинформации, характерные для современного периода. Особое внимание уделяется роли зарубежных стран в генерации и распространении фейков. В заключении предлагается комплекс мер по укреплению информационной безопасности государства и общества: совершенствование законодательства в сфере противодействия фейковым новостям; повышение медиаграмотности населения; внедрение технологических решений для выявления недостоверной информации (в том числе за счет механизмов искусственного интеллекта); развитие культуры фактчекинга, а также усиление контрпропаганды. Подчеркивается необходимость сбалансированного подхода, учитывающего как требования национальной безопасности, так и конституционные принципы свободы слова и свободы распространения информации. Статья вносит вклад в понимание современных информационных угроз и способов противодействия им, что может быть полезно для исследователей, работающих в области информационной безопасности, а также для практиков, занимающихся разработкой и реализацией государственной политики в данной сфере.

**Ключевые слова**
Фейковые новости, информационные войны, информационная безопасность, дезинформация, информационно-психологические операции, медиапространство, государственное регулирование, медиаграмотность, противодействие дезинформации, специальная военная операция, цифровые технологии, фактчекинг, искусственный интеллект, контрпропаганда, социальные сети.

**Для цитирования**
**Юсупов М.М. Информационная безопасность России: основные меры по противодействию угрозе фейковых новостей //Государственное управление. Электронный вестник. 2026. № 115. С. 52–65. DOI: 10.55959/MSU2070-1381-115-2026-52-65**

# Russian Information Security: The Main Measures of Countering the Threat of Fake News

**Marat M. Yusupov**
Postgraduate student, marat_yusupovv@list.ru, IusupovMM@spa.msu.ru

School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation.

**Abstract**
The article deals with the problem of countering fake news in the context of information security policy in Russia. The relevance of the topic is substantiated by the increased role of information warfare and disinformation in the modern world, especially in the conditions of the special military operation in Ukraine. The methodological basis of the study contains the analysis of normative-legal acts, regulating the sphere of information security in Russia, as well as the study of scientific literature on the problems of information warfare and disinformation The article utilizes also a comparative method to evaluate different approaches to counteracting disinformation. The research identifies key challenges associated with the mass dissemination of inaccurate information in the Russian media space, and analyzes the key approaches to counteracting disinformation, fake news typical for the modern period. Special attention is paid to the role of foreign countries in the generation and dissemination of fakes. The conclusion proposes a set of measures to strengthen information security of the state and society: improvement of legislation in the sphere of countering fake news; improvement of media literacy of the population; introduction of technological solutions for the detection of inaccurate information (including the field of fake news); identification of inaccurate information (including through the mechanisms of artificial intelligence mechanisms); development of fact-checking culture, and strengthening of counterpropaganda. The need for a balanced approach is emphasized, taking into account both national security requirements and the constitutional principles of freedom of speech and freedom of dissemination of information. The article contributes to the understanding of modern information threats and ways to counter them, which may be useful for researchers working in the field of information security, as well as for practitioners engaged in the development and implementation of public policy in this area.

**Keywords**
Fake news, information warfare, information security, disinformation, information-psychological operations, media space, government regulation, media literacy, countering disinformation, special military operation, digital technologies, fact-checking, artificial intelligence, counter-propaganda, social media.

**For citation**
**Yusupov M.M. (2026) Russian Information Security: The Main Measures of Countering the Threat of Fake News. *Gosudarstvennoye upravleniye. Elektronnyy vestnik*. No. 115. P. 52–65. DOI: 10.55959/MSU2070-1381-115-2026-52-65**

Дата поступления/Received: 07.10.2025

### *Введение*

Актуальность обращения к разработке новых методов и форм противодействия фейковым новостям в российском информационном пространстве объясняется сегодня в первую очередь проведением специальной военной операции на Украине, в рамках которой непосредственный противник, а также его союзники из числа стран коллективного Запада стремятся нанести урон безопасности Российской Федерации не только на поле боя, но и в медиаполе. В условиях кризиса доверия к традиционным СМИ аудитория все чаще стремится потреблять новости в Интернете, где разнообразие форматов предоставления информации и каналов ее получения дает иллюзию получения объективной картины происходящего.

Цель исследования — выявление особенностей и проблем государственного регулирования в области противодействия фейковым новостям в целях укрепления информационной безопасности, а также предложение решений выявленных проблем. Для достижения поставленной цели в исследовании решаются следующие задачи:

- концептуализируется понятийный аппарат информационной безопасности и фейковых новостей в контексте современных информационных войн;
- анализируется нормативно-правовая база Российской Федерации в сфере противодействия фейковым новостям, и выявляются основные подходы государственного регулирования;
- исследуется специфика угроз информационной безопасности посредством фейковых новостей в условиях проведения специальной военной операции на Украине;
- разрабатывается комплекс организационных и технологических мер по совершенствованию системы противодействия фейковым новостям в России.

Авторская гипотеза состоит в том, что в данных условиях характерный для России реактивный подход к минимизации ущерба от фейковых новостей, а также приоритет мер государственной «репрессии» (разработка и реализация мер юридической ответственности за распространение таких новостей) недостаточно эффективны: необходимо вырабатывать комплексную стратегию из разноплановых по своему характеру мер, вплетенную в более широкий контекст политики информационной безопасности. Лишь в этом случае принимаемые меры будут сбалансированы с точки зрения и ценностей свободы распространения информации, и национальной безопасности страны.

### *Концептуальные основы информационной безопасности*

Проблематика исследований в области информационной безопасности, которые были начаты еще с появлением первых компьютеров в середине XX века, обострилась после окончания холодной войны, когда стало понятно, что Интернет и широкомасштабная компьютеризация делают информацию принципиально более серьезным инструментом воздействия на массовое сознание и, следовательно, требуется трансформация привычных подходов к пониманию данного феномена.

Так, если изначально термин «информационная безопасность» использовался для обозначения проблем безопасности компьютеров и компьютерных сетей, то с 1990-х гг. он приобрел значительно более широкий смысл, выходящий за рамки исключительно технологической сферы и включающий вопросы контроля над информационными потоками, обладающими

дестабилизирующим потенциалом в масштабах общества, государства и международной системы [Зиновьева 2017, 85].

Следуя подходу, поддержанному в актах стратегического планирования Российской Федерации[1], информационную безопасность можно определить как состояние защищенности личности, общества и государства и их интересов от внутренних и внешних угроз, деструктивных и иных негативных воздействий в информационном пространстве.

В случае, когда какой-либо субъект (в особенности государство или квазигосударственное образование) сознательно актуализирует угрозы информационной безопасности, то есть посягает на эту сферу, вполне оправдано ожидать ответную, симметричную по своему характеру реакцию. Для обозначения противостояния в информационной сфере сегодня часто используется термин «информационные войны».

Само понятие информационных войн впервые полноценно концептуализировалось в зарубежной и отечественной науке в 1990-е гг. Среди отечественных ученых наиболее удачные определения этому явлению дали А.В. Манойло, А.И. Петренко и Д.Б. Фролов. Они указывают, что сутью информационной войны является конкуренция, соперничество социально-экономических систем в информационно-психологической области с целью получения влияния над определенными сферами или приобретения контроля над стратегически значимыми ресурсами. В результате такого соперничества одна сторона приобретает необходимые ей возможности для развития, то есть достигает своих целей, другая же — теряет [Манойло и др. 2018, 36].

Более лаконично выразился лауреат Нобелевской премии бывший вице-президент США А. Гор, который заявил, что информационная война — это борьба за разум, достижение внешнеполитических целей за счет манипуляций в рамках информационных атак [Гор 2008]. Показателем успешности таких атак является желаемое изменение поведения адресата. В этой связи любопытно замечание американского политолога Дж. Ная, который, комментируя соотношение концепта информационных войн со своей авторской концепцией «мягкой силы» указывал, что для человеческой истории идея использования информации для получения военно-политического преимущества не нова, однако риски такого использования повышаются именно в современном мире, когда «цифровые технологии делают информационное оружие более дешевым, быстрым, масштабным по охвату», а сами информационные операции становятся «более трудными для обнаружения и более легкими для отрицания со стороны тех, кто такие операции проводит»[2].

Использование ИКТ для агрессивного воздействия на иностранные государства с целью понудить их к определенному поведению распространилось на сеть Интернет практически сразу же после ее появления. Ведение информационной сетевой войны стало как никогда удобно: появилась возможность бесконтрольного размещения негативного и, что важно, анонимного сообщения, которое быстро распространится в Сети. Следовательно, появилась возможность не просто совмещать информационные атаки с военными действиями (гибридные войны), но в целом обеспечивать перманентное информационное сопровождение тлеющих конфликтов или просто напряженности в отношениях между государствами.

В последние годы современные цифровые технологии (искусственный интеллект, нейротехнологии, глубинный анализ больших пользовательских данных, технологии виртуальной и дополненной реальности) создали риски очередной, еще более масштабной трансформации информационной войны. Как указывает Н. Сильверстайн, сочетание технологических инноваций

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50. Ст. 7074.
[2] Nye J.S. Information warfare versus soft power // China US Focus [Электронный ресурс]. URL: https://www.chinausfocus.com/foreign-policy/information-warfare-versus-soft-power (дата обращения: 14.04.2025).

в цифровой сфере и нейробиологических открытий прямо сейчас сталкивает человечество с новой реальностью, с невиданными прежде угрозами и уязвимостями. Исследователь называет этот феномен «когнитивной войной» [Silverstein, 2019, 6].

***Фейковые новости как угроза информационной безопасности***

Ключевая для настоящей статьи категория «фейковые новости», или «фейки», является дословным переводом английского термина fake news, который получил широкое распространение в англоязычной экспертно-политической среде. Если обратиться к самому понятию fake news, то в самом общем смысле его можно определить как псевдоновости (от англ. fake — «подделка»), то есть такие новостные материалы, в которых содержится информация, намеренно вводящая в заблуждение аудиторию. Иными словами, это сфабрикованная новость, такой информационный материал, который стилистически создан как достоверная новость, но по своему содержанию носит ложный характер (полностью или частично) [Суходолов 2017, 84].

Несмотря на то, что само понятие фейковых новостей появляется в англоязычной публицистике еще в XIX веке, настоящая популяризация этого термина в глобальном масштабе началась после президентских выборов в США 2016 г. Используя Twitter как инструмент новых медиа, Д. Трамп, критикуя своих оппонентов из Демократической партии США и поддерживающие их традиционные СМИ, весьма часто использовал термины «фейковые новости» и «фейковые СМИ». Как указывают зарубежные исследователи, именно Д. Трамп создал за счет этих терминов новый дискурс, который тесно вплел проблему дезинформации в медиапространстве в контекст политических противоречий и социально-экономической напряженности — проблем, которые в последнее десятилетие все более остро проявляются как в США, так и в других развитых странах [Farhall et al. 2019]. В обстановке культурных войн обвинение оппонентов в использовании такого грязного приема, как фейковые новости, оказалось довольно эффективным инструментом, и это также способствовало популярности этого термина за пределами США.

По мнению О.В. Корецкой, фейковые новости напрямую связаны с политическим контекстом, поскольку прежде всего создание и тиражирование фейков происходит в рамках информационных войн в целях «политической пропаганды и манипуляции массовым сознанием, а также создания образа врага» [Корецкая 2017, 15]. Главная цель любых фейков как инструмента информационной войны — это посеять сомнения в официальной точке зрения и убедить аудиторию в правдивости представленной информации. Задача состоит в том, чтобы дезинформировать аудиторию; пропагандировать свое видение, политику или позицию; вызвать агрессию или страх; поколебать позицию индивидуума и заставить его усомниться в своих убеждениях; посеять панику; побудить к определенному действию; активировать внимание и заинтересовать аудиторию и т. д. [Милецкий, Черезов 2020, 64]. Иными словами, распространение фейковых новостей должно вызвать в обществе определенную реакцию.

При этом важно подчеркнуть, что фейковые новости могут приобретать разнообразные формы. Сама категория «фейкньюс» в условиях современного информационного пространства приобретает весьма широкое содержание. Действительно, в современных условиях в информационных войнах могут использоваться не только фальшивые текстовые материалы, но и другие фейки. К ним можно отнести фотографии, измененные с помощью фотомонтажа; записи в блогах; мнения экспертов; инфографику; поддельные видео. Фейками называют также аккаунты вымышленных людей в социальных сетях (ботов), через которые распространяется ложная информация или стандартизированные комментарии, призванные сформировать определенный дискурс в отдельных сегментах информационного пространства [Милецкий, Никифорова 2020, 103].

В российских СМИ, как и в медиапространстве других стран, проблема фейковых новостей актуализировалась в 2010-х гг. после стремительного роста аудитории социальных сетей и, как следствие, популярности новых медиа. В качестве базовых предпосылок данной тенденции можно назвать:

— рост политической напряженности как внутри России, так и на международном уровне, нарастание полярности взглядов, ценностей и убеждений, в результате чего манипуляции и фейки стали носить характер информационного оружия, намеренной дискредитации определенных персон, событий, процессов и инициатив;

— тенденция к перепечатке, то есть к копированию одними СМИ материалов из других СМИ, что негативно сказалось на проверке достоверности сообщаемой информации;

— рост конкуренции в медиа, результатом которой стало обострение борьбы за внимание аудитории (достигаемое в том числе за счет громких заголовков, сенсаций, скандалов), в которой принцип объективности и проверки фактов несколько нивелировался;

— конвергенция гражданской журналистики и традиционных СМИ, в результате чего непроверенная, но громкая информация с мест событий стала непреднамеренно включаться в информационный мейнстрим.

Именно первая предпосылка может рассматриваться сегодня как ключевая в контексте развязанной Украиной и западными странами информационной войны против России. В рамках данного противостояния генерируется огромное количество дезинформации, которая затем распространяется как ситуативно, так и в рамках заранее организованных кампаний. С учетом высокого градуса социальной напряженности, возникающего в обществе в связи со столь чувствительной темой, как военные действия, угроза для национальной безопасности России от таких кампаний может быть довольно существенной. Ситуация обостряется тем, что фейковые новости могут распространяться на виртуальной территории, которая находится за пределами юрисдикции Российской Федерации (видеохостинг YouTube, социальные сети Facebook[3] и X, мессенджеры WhatsApp и Viber). Как следствие, не исключена возможность воздействия на эти цифровые платформы со стороны недружественных государств с целью сознательного продвижения фейков или халатного отношения руководства платформ к противодействию дезинформации подобного рода.

Применительно к проведению СВО на Украине наиболее часто в медиапространстве распространяются фейковые документы, призванные вызвать хаос и повысить социальную напряженность в российском обществе. Так, на территории республики Крым и других приграничных территориях неоднократно распространялась информация о наличии вооруженных ДРГ Украины, информация о скорых атаках на Крымский мост и другие объекты инфраструктуры, включая атомные станции [Карпович 2022, 65]. В совокупности это должно было вызвать панику в обществе.

Подобными манипуляциями не брезговали и высшие должностные лица Украины: так, с целью дестабилизации обстановки в начале 2023 г. с обращениями к гражданам России выступили министр обороны Украины А. Резников и глава Главного управления разведки Украины К. Буданов[4], в которых утверждалось, что через несколько дней российские власти начнут вторую, более масштабную волну мобилизации, а внешние границы России будут закрыты на выезд. Данные материалы были широко распространены украинскими СМИ, а далее уже транслировались рядовыми пользователями, неравнодушными к столь чувствительной теме. Отметим, что это далеко не единственные фейки, касающиеся мобилизации: в медиапространстве неоднократно

[3] Meta Platforms Inc. (владелец Facebook и Instagram) — организация признана экстремистской, ее деятельность запрещена на территории России.
[4] Внесен в список террористов и экстремистов.

циркулировали «секретные документы» Минобороны РФ и других ведомств, содержащие дезинформацию о дополнительных наборах в армию среди подлежащих призыву граждан[5].

Заметную часть материалов составляют и фейки, прямо направленные на дискредитацию действий российских солдат на территории Украины. Из «радиоперехватов», «взломанных переписок» и других «источников» аудитории сообщается о военных преступлениях, пытках гражданских и пленных, наркомании, мародерстве и т. п. В некоторых таких материалах сообщается ложная информация о смерти или ранении российских солдат. Подобные кампании призваны очернить руководство и личный состав Вооруженных сил Российской Федерации не только в глазах российской аудитории, но и среди собственных граждан для эффекта сплочения, а также среди граждан иностранных государств.

В еще большей степени распространены фейковые новости в традиционных СМИ, которые нередко перепечатываются зарубежными медиа и посвящены ходу боевых действий. Эксперты отмечают, что с содержательной точки зрения такие фейки могут касаться численности погибших и раненых, показателей уничтоженной техники, успехов или неуспехов в контроле над территорией и т. п.[6] В результате искажается реальная картина проведения СВО, создаются предпосылки для изменения общественных настроений и, следовательно, политических решений.

Массовый характер распространения подобных фейковых новостей в условиях СВО (по оценкам экспертов газеты «Известия», только за первый год в медиапространстве циркулировало более 1,5 млн материалов[7]) объясняется нетипичным для мировой практики явлением — наличием открыто действующей организационной системы по созданию и распространению фейков с прямо поставленной целью проведения информационно-психологических операций. Так, на Украине за такие действия ответственен 72-й центр информационно-психологических спецопераций Украины (ЦИПсО), который является структурным подразделением Сил специального назначения Вооруженных сил Украины[8]. Таким образом, создание фейковых новостей с целью воздействия на российское медиапространство — официальная цель иностранного государства, неотъемлемая часть вооруженного противостояния.

На основании вышеизложенного можно констатировать, что фейковые новости, в особенности те, которые распространяются в рамках информационной войны, представляют собой существенную угрозу информационной безопасности, на которую государство обязано реагировать. Сегодня в России созданы как концептуальные, так и нормативные основы такого противодействия. Рассмотрим их более подробно.

***Концептуальные и нормативно-правовые механизмы противодействия фейковым новостям***

Так, в Разделе IV («Обеспечение национальной безопасности») Стратегии национальной безопасности Российской Федерации, содержится отдельная глава, посвященная вопросам информационной безопасности[9]. В частности, здесь подчеркивается, что ИКТ все чаще используются для вмешательства во внутренние дела суверенных государств, причем происходит это не только

[5] «Будут дискредитировать ВС РФ»: зачем ЦИПсО создал фейковые сайты городских военкоматов // Татар Информ [Электронный ресурс]. URL: https://www.tatar-inform.ru/news/budut-diskreditirovat-vs-rf-zacem-cipso-sozdal-feikovye-saity-gorodskix-voenkomatov-5935126 (дата обращения: 20.04.2025).
[6] Хроника зверской лжи: Как Киев и Запад погружали мир в паутину фейков о спецоперации // Комсомольская Правда [Электронный ресурс]. URL: https://www.kp.ru/daily/27470.5/4725079/ (дата обращения: 20.04.2025)
[7] Около 1,5 млн фейков появилось с начала операции на Украине // Экспертный клуб [Электронный ресурс]. URL: https://expert-club.online/news/okolo-15-mln-feykov-poyavilos-s-nachala-operatsii-na-ukraine (дата обращения: 20.04.2025).
[8] Военное обозрение: Центры информационно-психологических операций ССО Украины // Военное обозрение [Электронный ресурс]. URL: https://topwar.ru/192979-centry-informacionno-psihologicheskih-operacij-sso-ukrainy-razgrom-blizok.html (дата обращения: 20.04.2025).
[9] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ от 05 июля 2021 г. № 27 (часть II). Ст. 5351.

в военно-политических или экономических целях, но и для дестабилизации внутренней обстановки. Примечательно, что упоминается и проблема фейковых новостей («недостоверная информация, в том числе заведомо ложные сведения»), правда, лишь применительно к информации о террористических актах.

В Стратегии также прямо перечислены задачи, стоящие перед государством, для обеспечения информационной безопасности, некоторые из которых представляется целесообразным рассматривать и как конкретные направления деятельности по противодействию негативному влиянию фейковых новостей:

— формирование безопасной среды оборота достоверной информации (прямая связь с противодействием фейковым новостям и манипуляциям);

— развитие сил и средств информационного противоборства (абстрактное положение, в котором можно усмотреть цель создания инструментов контрпропаганды);

— противодействие попыткам террористических организаций, а также разведок иностранных государств оказывать «деструктивное информационное воздействие на граждан и общество»;

— доведение до российской и зарубежной общественности достоверной информации о внутренней и внешней политике России (формирование собственной позитивной повестки).

Другой акт концептуального характера — принятая в 2016 г. Доктрина информационной безопасности РФ[10], тоже указывает на расширение практик информационного воздействия со стороны иностранных спецслужб в целях разрушительного влияния на внутриполитическую ситуацию в различных странах, в частности России. Давление в информационной сфере может осуществляться как путем распространения предвзятой и негативной информации о России и ее политических действиях, так и путем притеснения отечественных СМИ за рубежом. Информационное противодействие (в том числе и фейковым новостям) признается одним из ключевых элементов противостояния давлению Запада.

Особого внимания заслуживает анализ соответствия положений базового Федерального закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» современным реалиям информационного пространства. Принятый в начале 1990-х гг. закон формировался в принципиально иных технологических и медийных условиях, когда доминировали традиционные СМИ (печать, радио, телевидение), а интернет-технологии и социальные сети практически отсутствовали. Закон устанавливает классические принципы свободы массовой информации, недопустимости цензуры, права на получение информации, однако его категориальный аппарат и регулятивные механизмы во многом не адаптированы к реалиям цифровой эпохи.

Ключевой проблемой является то, что закон оперирует понятием «средство массовой информации» в традиционном смысле (периодическое печатное издание, радио- и телепрограмма), тогда как современное медиапространство характеризуется доминированием новых медиа — блогов, социальных сетей, мессенджеров, которые формально не подпадают под определение СМИ, но фактически выполняют аналогичные функции по распространению информации. Это создает правовые лакуны в регулировании ответственности за распространение недостоверной информации через цифровые платформы.

Кроме того, традиционные механизмы ответственности, предусмотренные законом (предупреждение, приостановление деятельности СМИ), слабо применимы к противодействию

[10] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50. Ст. 7074.

фейковым новостям в эпоху вирусного распространения информации в социальных сетях, где источник дезинформации может быть анонимным, а скорость распространения — мгновенной. Это обуславливает необходимость концептуального обновления медийного законодательства с учетом вызовов информационной безопасности в цифровую эпоху.

Выполнение задач, обозначенных в рассмотренных выше документах, может развиваться с помощью различных инструментов. В России сегодня в наибольшей степени развито применение мер государственного принуждения и юридической ответственности за распространение фейковых новостей. Количество новых правовых норм в этой сфере последние годы неуклонно возрастает.

В частности, в Кодексе об административных правонарушениях Российской Федерации (далее — КоАП РФ)[11] содержится целый ряд статей, призванных нейтрализовать угрозы информационной безопасности. В частности, ответственность установлена за публичные призывы к участию в несанкционированных публичных мероприятиях, за пропаганду либо публичное демонстрирование запрещенной атрибутики и символики, за возбуждение ненависти либо вражды, за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, за призывы к введению санкций в отношении Российской Федерации, ее граждан и юридических лиц. Неоднократно дополнялась и расширялась ст. 13.15 КоАП РФ («Злоупотребление свободой массовой информации»), которая сегодня является основным инструментом привлечения к административной ответственности за фейковые новости.

Под влиянием серьезной угрозы фейковых новостей о пандемии коронавируса COVID-19 в 2020 г. Уголовный кодекс Российской Федерации (далее — УК РФ) был дополнен статьями 207.1 и 207.2, которые устанавливают ответственность: а) за публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств; б) публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия. Это классический пример ответственности за фейковые новости, причем с точки зрения юридической техники обе статьи сформулированы довольно грамотно[12].

С весны 2022 г. в КоАП РФ и УК РФ были внесены новые поправки, призванные противодействовать недостоверной информации о действиях Вооруженных сил РФ, а также привлекать к ответственности за заведомо ложные сведения об «исполнении российскими государственными органами своих полномочий за пределами РФ» (ст. 207.3 УК РФ). Это довольно полезная мера в условиях уже отмеченной выше массированной информационной атаки со стороны ЦИПсО, однако следует учитывать, что на территории Российской Федерации чаще всего проживают распространители, а не создатели подобного контента, то есть нередки ситуации, когда они выступают жертвами, а не производителями пропаганды. Эту особенность следует принимать во внимание в процессах правоприменения. Российский правовед Н.Н. Парыгина указывает, что в целом нормы о диффамации в адрес государства как публично-правового образования нуждаются в дополнительной проработке, причем не только в рамках уголовного права [Парыгина 2025].

***Организационные и технологические меры противодействия фейковым новостям***

Признавая важность введения мер административной и уголовной ответственности в отношении распространителей фейковых новостей, важно понимать, что без комплекса других

[11] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ от 07 января 2002 г. № 1 (часть I). Ст. 1.
[12] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ от 17 июня 1996 г. № 25. Ст. 2954.

действий государство вынуждено лишь реагировать на угрозу, а не предотвращать ее или снижать связанные с ней риски негативных последствий. В этой связи эффективными инструментами противодействия фейковым новостям в условиях активизации информационной войны против России видятся также ряд мер организационного и технологического характера.

Во-первых, к таким мерам можно отнести повышение медиаграмотности. Такая мера подразумевает работу с аудиторией как реципиентом информации, с общественным сознанием как объектом защиты в рамках политики информационной безопасности. Как указывает Г.А. Арутюнов, медиаграмотность рассматривается как вид информационной грамотности, под которым понимается комплекс знаний, умений и навыков, необходимых для понимания СМИ и медиаформатов, а также умений анализировать, оценивать и создавать информацию, представленную в разных формах и форматах [Арутюнов 2013, 32]. С данным определением можно согласиться.

В ходе обучения медиаграмотности пользователям социальных сетей и аудитории традиционных СМИ должны прививаться такие полезные в информационном обществе навыки, как умение:

- распознавать источники новостей и оценивать их достоверность;
- выявлять предвзятость в конкретном материале и понимать, как она может влиять на его интерпретацию;
- различать факты и мнения;
- проверять факты, приводимые в материалах СМИ, посредством обращения к альтернативным источникам информации [Adjin-Tettey 2022, 34].

Можно позитивно оценить шаги, предпринимаемые в России в этом направлении. Так, в рамках Петербургского международного экономического форума 2022 г. Министерство просвещения России заключило соглашения с обществом «Знание», «Мегафоном» и АНО «Диалог» о проведении в школах уроков цифровой грамотности. Предполагается, что здесь будут преподаваться «основы критического мышления и привычки проверки любой информации, с которой они сталкиваются в интернете»[13]. Аналогичные учебные дисциплины вводятся и в некоторых российских вузах[14].

Следующий элемент организационных основ противодействия фейковым новостям, направленный на снижение рисков восприятия таких материалов общественным сознанием, — это государственная политика по формированию конкурентной медиасреды с разнообразием источников информации и редакционных позиций. Это подразумевает создание условий для функционирования СМИ с различными форматами, целевыми аудиториями и редакционными подходами, что снижает риски монополизации информационного пространства. Конкретными мерами могут служить: антимонопольное регулирование медиарынка, предотвращающее чрезмерную концентрацию СМИ в руках отдельных владельцев; поддержка региональных и местных СМИ через гранты и льготы; развитие общественного вещания; стимулирование развития отраслевых и специализированных изданий. Такой подход способствует формированию медиаландшафта, где аудитория имеет доступ к различным источникам информации для сопоставления и верификации фактов, что естественным образом повышает критичность восприятия недостоверной информации.

Далее следует указать на важность такого направления, как внедрение культуры проверки фактов и разоблачения громких фейков. Как и вышеперечисленные меры, она позволяет

[13] Российских школьников и учителей научат медиаграмотности // Skillbox [Электронный ресурс]. URL: https://skillbox.ru/media/education/rossiyskikh-shkolnikov-i-uchiteley-nauchat-mediagramotnosti/ (дата обращения: 10.04.2025).
[14] Медиаграмотность // НИУ ВШЭ [Электронный ресурс]. URL: https://www.hse.ru/ba/journ/courses/920903179.html (дата обращения: 05.10.2025).

нейтрализовать негативное воздействие фейковых новостей. В современных исследованиях подчеркивается, что в условиях информационного общества распространение недостоверной или вводящей в заблуждение информации неизбежно, однако реципиент такой информации, обладающий навыками медиаграмотности, может проверить каждый из фактов, который кажется ему подозрительным. Для этого в разных странах мира создаются специальные ресурсы, позволяющие уточнить достоверность той или иной информации. Как правило, такие ресурсы создаются авторитетными СМИ или организациями гражданского общества. Некоторые из них (Google Fact Check Explorer, FactCheck.org) функционируют в рамках крупных международных интернет-платформ, другие организованы при национальных медиаресурсах или аффилированных с государством некоммерческих организациях[15].

Так, в 2022 г. АНО «Диалог» запустило проект «Лапша Медиа», цель которого — «создание безопасной информационной среды для граждан», поскольку его создатели справедливо отмечают, что фейковые новости в сети сегодня являются «угрозой не только информационной, но и национальной безопасности»[16]. Это один из первых примеров сотрудничества между государством и НКО в деле противодействия фейкам.

На уровне отдельных российских СМИ попытки создания верификации данных были предприняты еще раньше. Например, у интернет-журнала The Insider[17] существует отдельный сервис «Антифейк», посвященный разоблачению фейков при освещении внутренней и внешней политики Российской Федерации, а также международных отношений. Соответствующие рубрики все чаще применяются и в региональных СМИ. Примечателен и опыт ведения отдельных передач или рубрик, которые регулярно разоблачают наиболее громкие фейковые новости за определенный период (примеры: программа «Антифейк» на «Первом канале», а также специально посвященный разбору фейковых новостей ЦИПсО раздел на сайте «Комсомольской Правды») [Галяшина 2021, 13].

Впрочем, стоит отметить, что зачастую фактчекинг сам превращается в инструмент манипулирования общественным мнением и орудием борьбы с политическими оппонентами, подрывая тем самым доверие граждан к этой практике. Профессор Л. Грейвс, анализируя американское медиапространство в условиях предвыборной кампании в США в 2016 г., указывал, что журналисты, занимающиеся фактчекингом, должны обладать повышенным уровнем личной ответственности, поскольку их ответы выступают в качестве последней инстанции, результатом чего является принятие той или иной стороны. По сути, как указывает автор, фактчекинг — это «наиболее рискованный вид журналистики» в современном обществе[18].

В контексте формирования культуры проверки фактов важно упомянуть и технологические меры, которые тесно связаны с механизмами формирования и распространения информации в цифровом медиапространстве. В совокупности такие меры направлены на выявление и предотвращение распространения материалов, дезинформирующих аудиторию или вводящих ее в заблуждение.

Комплекс таких мер должен разрабатываться самими новыми медиа и сервисами наподобие новостных агрегаторов в рамках саморегулирования. Согласно опросу 2019 года, который был проведен по заказу аналитической компании Pew Research Center, большинство опрошенных пользователей Сети считает, что бремя ответственности за сокращение числа недостоверной

[15] Fact Check Tools // Google News Initiative [Электронный ресурс]. URL: https://newsinitiative.withgoogle.com/resources/trainings/google-fact-check-tools/ (дата обращения: 02.04.2025).
[16] Проект «Лапша Медиа» запустил кампанию по обучению молодежи проверке информации // Вечерняя Москва [Электронный ресурс]. URL: https://vm.ru/news/1248173-proekt-lapsha-media-zapustil-kampaniyu-po-obucheniyu-molodezhi-proverke-informacii (дата обращения: 01.04.2026).
[17] Включено Минюстом РФ в реестр иностранных агентов.
[18] Even trust in fact-checking is polarized // VOX [Электронный ресурс]. URL: https://www.vox.com/policy-and-politics/2016/10/19/13341000/trust-in-fact-checking-polarized (дата обращения: 14.05.2025).

информации в цифровых медиа должны нести сами площадки, удаляя подобный контент или помечая его соответствующим образом[19].

Представляется, что с учетом постоянно возрастающего количества информации в Сети (по данным Всемирного экономического форума, к 2025 году каждый день будет создаваться около 463 эксабайт данных, что эквивалентно 2,1 миллиона DVD-дисков [Войниканис и др. 2022, 12]) наиболее оптимальным будет внедрение цифровых технологий в процессы мониторинга, фильтрации и удаления фейковых новостей в социальных сетях. В первую очередь речь идет о технологии искусственного интеллекта (ИИ), чей потенциал здесь уже успешно реализовывается крупными новостными изданиями и агрегаторами как в России, так и за рубежом.

Независимо от размера или навыков команды модераторов контента в том или ином сетевом СМИ, социальной сети или новостном агрегаторе, огромное количество контента, созданного пользователями, не позволяет им обеспечить проверку всего этого массива информации. Здесь очевидным образом необходима автоматизация. Однако проверка фактов и выявление фейковых новостей — это трудоемкий процесс, на последней стадии которого пока еще в обязательном порядке должны быть задействованы люди. Таким образом, роль искусственного интеллекта на современном этапе можно охарактеризовать как вспомогательную.

Помимо этого, в рамках социальных медиа, где удаление относительно безвредного контента может расцениваться как слишком радикальная мера, ИИ может позволять ранжировать материалы по степени их достоверности или приемлемости. Такие технологии уже существуют в Facebook[20] и X, где конкретные посты могут помечаться специальными алгоритмами как содержащие информацию, требующую дополнительного подтверждения, то есть сомнительную и потенциально недостоверную.

По мере дальнейшего развития искусственного интеллекта на основе анализа больших данных в медиапотоке соответствующие технологии могут помочь в целом выявлять модели зарождения и трансляции фейковых новостей (например, по критерию использования вводящих в заблуждение заголовков, распространения известных теорий заговора, а также по критерию технологии создания контента, если он был создан с использованием ИИ — так называемые дипфейки). Это может помочь выявить потенциально фальшивые информационные материалы и предотвратить их распространение. С помощью ИИ можно также маркировать наиболее часто замеченные в их распространении средства массовой информации — с дальнейшей передачей этой информации руководству конкретного СМИ или сетевой платформы для принятия мер реагирования.

Наконец, нейтрализация угроз информационной безопасности должна осуществляться при помощи инструментов контрпропаганды, то есть собственного, ответного информационного воздействия в отношении кампаний дезинформации. Продукты контрпропаганды должны быть обращены в первую очередь к населению, которое в наибольшей степени может быть подвержено рискам воздействия фейковых новостей — это жители новых территорий Российской Федерации, оппозиционно настроенные граждане России, а также граждане других государств, включая Украину и Запад. Важность переубеждения и нейтрализации попыток сформировать образ России в негативном свете сложно переоценить в условиях, когда роль информации во внутри- и внешнеполитическом процессе столь высока.

[19] Many American Say Made-Up News is a Critical Problem that Needs to be Fixed // Pew Research Center [Электронный ресурс]. URL: https://www.pewresearch.org/journalism/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/ (дата обращения: 14.05.2025).
[20] Meta Platforms Inc. (владелец Facebook и Instagram) — организация признана экстремистской, ее деятельность запрещена на территории России.

***Заключение***

Анализ проблематики фейковых новостей в контексте информационной безопасности страны позволил прийти к выводу о том, что в современную эпоху цифровых технологий возникла необходимость в концептуализации такой сферы национальной и международной безопасности, как безопасность информационная. Под информационной безопасностью предложено понимать состояние защищенности личности, общества и государства и их интересов от внутренних и внешних угроз, деструктивных, ложных и иных негативных воздействий в информационном пространстве.

Анализ концептуальных основ российской политики в области информационной безопасности (на примере Стратегии национальной безопасности РФ, Доктрины информационной безопасности РФ, а также Концепции внешней политики РФ) показал, что эти документы должны быть более сбалансированы с точки зрения конституционных ценностей, основываться на компромиссе между объективно разными интересами государства, общества и индивида. Видится необходимой большая конкретизация угроз информационной безопасности, адаптация мер противодействия однотипным группам этих угроз под специфику этих групп, а также отказ от исключительно административно-властных, принудительных мер обеспечения информации, для чего видится необходимым более широкое вовлечение представителей информационной инфраструктуры и организаций гражданского общества в деятельность по обеспечению информационной безопасности в современной России. Наконец, необходимо уделять больше внимания разработке превентивных механизмов нейтрализации попыток применения фейковых новостей и манипуляций общественным мнением в медиапространстве, которые могут стать удачным дополнением к уже существующим механизмам ответственности за данные правонарушения.

В статье предложены две группы мер, позволяющих оптимизировать государственное управление в области противодействия фейковым новостям: организационные и технологические. Организационные меры, которые могут быть приняты для противодействия фальшивым новостям, должны разрабатываться по следующим приоритетным направлениям: просвещение населения (популяризация научного знания, курсы медиаграмотности); поощрение медиаплюрализма на государственном уровне; повсеместное внедрение процедур проверки фактов и верификации новостных материалов, включая развитие специализированных сервисов; повышение журналистских стандартов и значения журналистской этики в работе СМИ (включая меры, направленные на создание репутационных рисков для источников и распространителей фейковых новостей).

Что касается технологических мер, то они должны включать в себя разработку алгоритмов, позволяющих выявлять и отмечать потенциально фальшивые новости, а также использование искусственного интеллекта и машинного обучения для выявления моделей дезинформации с целью их дальнейшего обнаружения в информационном потоке, что особенно актуально в условиях проведения специальной военной операции.

***Список литературы:***

Арутюнов Г.А. Анализ понятия медиаграмотности как составляющей информационной грамотности личности // Вестник РМАТ. 2013. № 1(7). С. 91–94.

Войниканис Е.А., Кольздорф М.А., Корнеев В.А., Ульянова Е.В., Шебанова Н.А. Интеллектуальное право в условиях развития технологии Big Data. База данных как объект интеллектуальных и иных прав. М.: Проспект, 2022.

Галяшина Е.И. «Фейкинг» как новая угроза медиабезопасности: лингвоюридический аспект // Этнопсихолингвистика. 2021. № 2(5). С. 7–24. DOI: 10.31249/epl/2021.02.01

Гор А. Атака на разум. СПб.: Амфора, 2008.

Карпович О.Г. Информационная война против России в условиях осуществления специальной военной операции // Вестник Академии военных наук. 2022. № 2. С. 10–13.

Корецкая О.В. Фейковые новости как объект изучения медиалингвистики (на материале англоязычных СМИ) // Филологические науки. Вопросы теории и практики. 2017. № 9–1(75). С. 118–120.

Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия, 2018.

Милецкий В.П., Никифорова О.А. Эволюция политических симулякров в цифровом обществе (на примере «фейк-ньюс» и «постправды») // Дискурс. 2020. Т. 6. № 3. С. 64–77. DOI: 10.32603/2412-8562-2020-6-3-64-77

Милецкий В.П., Черезов Д.Н. «Фейк-ньюс» в цифровом обществе как симулякры виртуального пространства // Информация–Коммуникация–Общество. 2020. № 1. С. 155–159.

Парыгина Н.Н. Категории добросовестности и противоречивого поведения в контексте диффамационных споров // Право и образование. 2025. № 2. С. 11–17.

Суходолов А.П. Феномен «Фейковых новостей» в современном медиапространстве // Евроазиатское сотрудничество: гуманитарные аспекты. 2017. № 1. С. 87–106.

Adjin-Tettey T.D. Combating Fake News, Disinformation, and Misinformation: Experimental Evidence for Media Literacy Education // Cogent Arts and Humanities. 2022. Vol. 9. Is. 1. P. 42–64. DOI: 10.1080/23311983.2022.2037229

Farhall K., Carson A., Wright S., Gibbons A., Lukamto W. Political Elites' Use of Fake News Discourse across Communications Platforms // International Journal of Communication. 2019. Vol. 13. URL: https://ijoc.org/index.php/ijoc/article/view/10677

Silverstein N. The New Geopolitical Space in the Information Era. Geneva: International Studies and Multilateral Diplomacy, 2019.

### *References:*

Adjin-Tettey T.D. (2022) Combating Fake News, Disinformation, and Misinformation: Experimental Evidence for Media Literacy Education. *Cogent Arts and Humanities*. Vol. 9. Is. 1. P. 42–64. DOI: 10.1080/23311983.2022.2037229

Arutyunov G.A. (2013) The Analysis of the Notion "Mediacompetence" ss the Component of the Individual's Information Competence. *Vestnik RMAT*. No. 1(7). P. 91–94.

Farhall K., Carson A., Wright S., Gibbons A., Lukamto W. (2019) Political Elites' Use of Fake News Discourse across Communications Platforms. *International Journal of Communication*. Vol. 13. Available at: https://ijoc.org/index.php/ijoc/article/view/10677

Galyashina E.I. (2021) «Faking» as a New Threat to Media Security: Lingua-Jurist Aspect. *Etnopsikholingvistika*. No. 2(5). P. 7-24. DOI: 10.31249/epl/2021.02.01

Gore A. (2008) *The Assault on Reason*. Saint Petersburg: Amfora.

Karpovich O.G. (2022) Information War against Russia in the Context of a Special Military Operation. *Vestnik Akademii voyennykh nauk*. No. 2. P. 10–13.

Koretskaya O.V. (2017) Fake News as the Object of Study of Media-Linguistics (by the Material of English Media). *Filologicheskiye nauki. Voprosy teorii i praktiki*. No.9–1(75). P. 118–120.

Manoylo A.V., Petrenko A.I., Frolov D.B. (2018) *Gosudarstvennaya informatsionnaya politika v usloviyakh informatsionno-psikhologicheskoy voyny* [State information policy in conditions of information-psychological warfare]. Moscow: Goryachaya liniya.

Miletskiy V.P., Cherezov D.N. (2020) “Fake news” in Digital Society as Simulacra of Virtual Space. *Informatsiya–Kommunikatsiya–Obshchestvo*. No. 1. P. 155–159.

Miletskiy V.P., Nikiforova O.A. (2020) Evolution of Political Simulacra in Digital Society (on the Examples of “Fake News” and “Post-Truth”). *Diskurs*. Vol. 6. No. 3. P. 64–77. DOI: 10.32603/2412-8562-2020-6-3-64-77

Parygina N.N. (2025) Categories of Conscientiousness and Contradictory Behavior in the Scope of Defamation Cases. *Pravo i obrazovaniye.* No. 2. P. 11–17.

Silverstein N. (2019) *The New Geopolitical Space in the Information Era*. Geneva: International Studies and Multilateral Diplomacy.

Sukhodolov A.P. (2017). The Phenomenon of “Fake News” in the Modern Media Space. *Evroaziatskoye sotrudnichestvo: gumanitarnyye aspekty*. No. 1. P. 87–106.

Voynikanis Ye.A., Kol’zdorf M.A., Korneyev V.A., Ul’yanova Ye.V., Shebanova N.A. (2022) *Intellektual’noye pravo v usloviyakh razvitiya tekhnologii Big Data. Baza dannykh kak ob’’yekt intellektual’nykh i inykh prav* [Intellectual property law in the context of the development of Big Data technology. Database as an object of intellectual and other rights]. Moscow: Prospekt.