Информация для цитирования:

Дискин Е. И. Концептуальные основы и правовое регулирование противодействия дезинформации: сравнительный анализ через призму междисциплинарности // Вестник Пермского университета. Юридические науки. 2025. Вып. 3(69). С. 409–429. DOI: 10.17072/1995-4190-2025-69-409-429.

Diskin E. I. Kontseptual'nye osnovy i pravovoe regulirovanie protivodeystviya dezinformatsii: sravnitel'nyy analiz cherez prizmu mezhdistsiplinarnosti [Conceptual Foundations and Legal Regulation of Countering Disinformation: A Comparative Analysis Through the Lens of Interdisciplinarity]. *Vestnik Permskogo universiteta. Juridicheskie nauki* – Perm University Herald. Juridical Sciences. 2025. Issue 3(69). Pp. 409–429. (In Russ.). DOI: 10.17072/1995-4190-2025-69-409-429.

УДК 342.95;004
DOI: 10.17072/1995-4190-2025-69-409-429

Концептуальные основы и правовое регулирование противодействия дезинформации: сравнительный анализ через призму междисциплинарности

Статья подготовлена в результате работы в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ)

Е. И. Дискин
Национальный исследовательский университет «Высшая школа экономики»
E-mail: ediskin@hse.ru

Статья поступила в редакцию 07.05.2025

Введение: *дезинформация – один из сложнейших вызовов для правового регулирования. Различные правовые системы по-разному реагируют на такие вызовы в условиях геополитической напряженности. Анализ феномена дезинформации ведется представителями разных наук, при этом с юридической точки зрения данное понятие изучено недостаточно. За рубежом термин «дезинформация» прочно занял свое место в законодательстве, активно исследуется как юристами, так и специалистами иных научных направлений. Большое значение придается противодействию дезинформации, формируется правоприменительная практика, особенно в части противодействия дезинформации в киберпространстве.* ***Цель:*** *сравнительный анализ законодательства ЕС, США и России в области противодействия дезинформации, определение юридической сущности дезинформации и выявление недостатков российского законодательства в области противодействия дезинформации.* ***Методы:*** *сравнительно-правовой метод, метод юридической герменевтики, историко-правовой метод и системный подход применяются для изучения феномена дезинформации как понятия, которое может найти отражение в различных отраслях российского права – уголовном, административном и информационном.* ***Результаты:*** *автором проанализированы законодательства ЕС, США и России, а также определения дезинформации, подходы к противодействию дезинформации учеными-юристами в сопоставлении с выводами специалистов из других областей.* ***Выводы:*** *российское законодательство в настоящее время не в полной мере соответствует*

широкому спектру вызовов, связанных с распространением дезинформации. В этом отношении законодательство ЕС значительно эффективнее в решении задач по противодействию дезинформации за счет применения различных методов регулирования, подробного изложения норм и определений. Зарубежное законодательство в данной сфере в значительной степени направлено на противодействие интересам России, что является самостоятельным вызовом для суверенитета РФ.

Ключевые слова: дезинформация; интернет-платформы; модерация; инфодемия; фейковые новости; цифровые технологии; цифровая трансформация; фейк-ньюс; Цифровой кодекс

Conceptual Foundations and Legal Regulation of Countering Disinformation: A Comparative Analysis Through the Lens of Interdisciplinarity

The article was prepared within the framework of the Fundamental Research Program of the National Research University 'Higher School of Economics' (HSE University)

E. I. Diskin

National Research University 'Higher School of Economics'
(HSE University)
E-mail: ediskin@hse.ru

Received 07 May 2025

Introduction: *disinformation is currently among the most complex challenges for legal regulation. Different legal systems respond differently to such challenges under conditions of geopolitical tension. The phenomenon of disinformation is analyzed by representatives from various scientific fields, but it has not been sufficiently explored from a legal perspective, and it has yet to find its place in domestic (Russian) legislation. At the same time, in foreign countries the term 'disinformation' has firmly established itself in legislation and is actively researched by jurists as well as representatives from other sciences. Particular importance is placed on countering disinformation, the relevant legal practices are being formed, especially these concerning countermeasures against disinformation in cyberspace.* ***Purpose:*** *the study aims to provide a comparative analysis of the legislation of the EU, the USA, and Russia in the field of combating disinformation, define the legal essence of disinformation, and identify the shortcomings of Russian legislation in this area.* ***Methods:*** *the comparative-legal method, the method of juridical hermeneutics, the historical-legal method, and a systematic approach are used to study the phenomenon of disinformation as a concept that may find reflection in various areas of Russian law – criminal, administrative, and informational law.* ***Results:*** *the author has analyzed the legislation of the EU, the USA, and Russia, examined how legal sciences in Russia and abroad define disinformation, what approaches to countering disinformation are proposed by legal scholars, and compared these findings with conclusions drawn by specialists from other fields.* ***Conclusions:*** *currently Russian legislation is not fully adequate to deal with the broad spectrum of challenges associated with the spread of disinformation. In this regard, EU legislation is significantly more effective in addressing tasks related to combating disinformation through the application of various regulatory methods, detailed formulation of norms and definitions. Foreign legislation in this sphere is largely aimed at countering Russian interests, which poses an independent challenge to the sovereignty of the Russian Federation.*

Keywords: disinformation; internet platforms; moderation; infodemic; fake news; digital technologies; Digital Code

А вам стыдно, товарищ, бегать по милициям
и вносить дезинформацию!
Кинофильм «Печки-лавочки», 1972

Введение

В условиях повсеместной компьютеризации, когда информационно-коммуникационные технологии (ИКТ) радикально меняют едва ли не все сферы социального взаимодействия, проблема ложной, недостоверной, вводящей в заблуждение информации (дезинформации) становится одной из ключевых в контексте выполнения задач по обеспечению общественной безопасности в Интернете. В то же время в России и за рубежом складываются существенно разные подходы к противодействию дезинформации – начиная с использования разного понятийного аппарата и заканчивая подходами к определению значимых признаков дезинформации как общественно опасного явления и формированию системы предупреждения ее распространения. Такое различие можно объяснить разными факторами – правовой культурой, особенностями социально-политического развития и не в последнюю очередь оценкой общественной опасности, которую несет дезинформация. Целесообразно, используя сочетание таких специфических юридических методов научного познания, как юридическая герменевтика (в том числе социально-политический и телеологический анализ соответствующих норм и правоотношений), сравнительно-правовой метод, историко-правовой метод (ограничиваясь при этом горизонтом событий XXI в.), а также комплексного (междисциплинарного) и системного подходов, определить юридическую сущность и смысл понятия «дезинформация», основные методы противодействия дезинформации в России, США и ЕС, а также дать оценку сложившемуся в России нормативно-правовому регулированию в области противодействия дезинформации в контексте соответствия рассматриваемых норм социально-политическим вызовам и стандартам защиты прав человека. Основной акцент в исследовании сделан на изучении нормативного закрепления мер по противодействию дезинформации, распространяемой в Интернете, преимущественно с использованием интернет-платформ. Это объясняется тем фактом, что именно интернет-платформы, включая социальные сети, аудиовизуальные и поисковые сервисы в настоящее время стали основными площадками для распространения дезинформации в глобальном масштабе.

Прежде всего, необходимо отметить, что в настоящий момент в российском законодательстве не используется понятие «дезинформация». Задача по защите общественной безопасности, выраженная в необходимости предупреждения распространения недостоверной информации, решается путем введения ряда дефиниций в Уголовный кодекс Российской Федерации (далее – УК РФ), Кодекс об административных правонарушениях Российской Федерации (далее – КоАП РФ), Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (далее – Закон № 149-ФЗ) и другие законодательные акты. При этом используются такие громоздкие дефиниции, как «публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» (ст. 207.1 УК РФ), «публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия» (ст. 207.2 УК РФ)[1] и т. д. Иными словами, толкование и применение соответствующих норм в рамках обеспечения защиты прав человека вызывают ряд существенных трудностей и требуют понимания социально-политического контекста, оценки тяжести деяния и наступивших последствий, что зачастую также представляет большую сложность ввиду специфики данных правоотношений.

В противоположность отечественному подходу в законодательстве ЕС, а именно в Законе о цифровых услугах ЕС (EU Digital Services Act, DSA), используется термин «дезинформация» как обобщающее понятие, включающее различные виды и подвиды дезинформации с перечислением видов правоотношений, на которые она может оказывать негативное влияние. Например, в статье 95 DSA приводится следующая формулировка: «дезинформация с реальными и предсказуемыми негативными последствиями для здоровья населения, общественной безопасности, гражданского дискурса, участия в политической жизни и равенства»[2].

Разница подходов к определению недостоверной информации заставляет обратить внимание на предпосылки к использованию тех или иных формулировок, преимущества и недостатки соответствующих законодательных актов, связанные с дефинированием понятия «дезинформация».

Изучение уголовного, административного и информационного законодательства позволяет сделать вывод, что ни в одной из этих отраслей права не используется центрального, опорного понятия, которое бы давало общее описание недостоверной информации. Соответствующие определения, перегруженные прилагательными, каждый раз исходя их новых общественно-политических вызовов безопасности создаются заново и содержательно недостаточно связаны друг с другом. Это значительно усложняет

[1] Regulation (Eu) 2022/2065 Of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065.

[2] Regulation (Eu) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

восприятие и последующее толкование каждой отдельной нормы законодательного акта, ухудшает системность кодифицированных законодательных актов, таких как УК РФ и КоАП РФ.

Обращает на себя внимание то, что в противовес отечественному подходу в ЕС в настоящее время предпринята попытка систематизировать регулирование цифровых услуг и интернет-платформ. Существенную роль в данной инициативе играет система норм о противодействии дезинформации, в частности, выделено понятие «дезинформация», а также разработаны различные механизмы противодействия ее распространению.

С учетом данных исходных различий в подходах к обеспечению общественной безопасности в России и ЕС, а также того факта, что в настоящее время Российская Федерация и Европейский союз находятся в острой стадии геополитического противостояния, представляется необходимым провести герменевтический анализ понятия «дезинформация» в законодательстве ряда государств (преимущественно недружественных на данном историческом этапе), социально-политический и сравнительно-правовой анализ с целью изучить недостатки отечественного подхода к законотворчеству в данной области, предложить новые подходы к совершенствованию законодательства по противодействию дезинформации.

С социально-политической точки зрения об угрозе дезинформации заявляют правительства и негосударственные организации разных стран. Особенно остро вопрос о наращивании усилий по совершенствованию законодательства о противодействии распространению ложных, вводящих в заблуждение сведений встал после пандемии COVID-19, когда выснилось, что данная угроза имеет одновременно национальное и глобальное измерение. Генеральный секретарь ООН Антониу Гутериш, описывая последствия распространения дезинформации, употребил выражение «первая глобальная инфодемия»[1], имея в виду специфический феномен вспышки массового распространения ложной информации о COVID-19, что не только несло витальные риски заражения опасным вирусом, но и подрывало глобальные усилия по недопущению его распространения. Яркой иллюстрацией таких угроз является международное движение антиваксеров (противников вакцинации), которое активно распространяло так называемую медицинскую дезинформацию в ходе пандемии[2]. В то же время всеобщность и масштаб угрозы, вызванной пандемией, способствовали и росту саморегулирования – модерации подобного контента ведущими интернет-платформами и их сотрудничеству с государственными органами[3], что предшествовало законодательным мерам в данной области.

Срочность, с которой принимались законодательные акты по противодействию распространению дезинформации в условиях пандемии, сказалась на их качестве. Модели такого противодействия не были в достаточной мере сбалансированы с точки зрения оценки их долгосрочного влияния на баланс между защитой общественной безопасности и правом на свободу слова и мысли, не содержали оценки их долгосрочных социально-экономических последствий. Политики ряда зарубежных стран в ходе активной фазы пандемии признали необходимость ограничить выражение индивидуальной точки зрения по вопросам здоровья (в первую очередь вакцинации)[4]. Впервые за долгое время государства с разными политическими режимами в достаточно жесткой форме ограничивали сбор и распространение ранее не запрещенной законом информации в целях защиты общественного здоровья и благополучия в соответствии с теми решениями, которые принимались на международном уровне[5]. Легитимность таких мер со временем подвергается переоценке, в том числе ввиду постепенного пересмотра основных постулатов, составлявших матрицу «правда/дезинформация» в контексте пандемии. В частности, большое значение в этом вопросе имеет доклад Специального комитета нижней палаты Конгресса США по расследованию пандемии[6] (доклад Конгресса США о COVID-19), сделавшего выводы, ранее четко

[1] Подробнее см.: Всемирная организация здравоохранения. Борьба с инфодемией на фоне пандемии COVID-19: поощрение ответственного поведения и уменьшение пагубного воздействия ложных сведений и дезинформации. Совместное заявление ВОЗ, ООН, ЮНИСЕФ, ПРООН, ЮНЕСКО, ЮНЭЙДС, МСЭ, инициативы ООН «Глобальный пульс» и МФКК. URL: https://www.who.int/ru/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation.

[2] Например, Российский фонд прямых инвестиций (РФПИ) заявил, что зафиксировал более 300 информационных атак на вакцину «Спутник». Подробнее см: URL: https://tass.ru/ekonomika/21116295.

[3] Меры саморегулирования цифровых платформ в ходе пандемии показали себя отнюдь не с идеальной стороны, так как зачастую любые озвученные профессиональными медиками и биологами сомнения в эффективности тех или иных мер по противодействию распространению COVID-19 являлись основанием для применения самых жестких ограничений по отношению к их авторам, невзирая на их профессиональный статус и заслуги. Существуют обоснованные опасения, что такие действия, в отсутствие возможности их эффективного обжалования в судебном порядке, являются цензурой, то есть противоправны.

[4] 'They're Killing People': Biden Denounces Social Media for Virus Disinformation. URL: https://www.nytimes.com/2021/07/16/us/politics/biden-facebook-social-media-covid.html.

[5] WHO updates COVID-19 guidelines on masks, treatments and patient care. URL: https://www.who.int/news/item/13-01-2023-who-updates-covid-19-guidelines-on-masks--treatments-and-patient-care.

[6] Final Report of the Select Subcommittee on the Coronavirus Pandemic Committee on Oversight and Accountability. After Action Review of the COVID-19 Pandemic: The Lessons Learned and a Path Forward. URL: https://oversight.house.gov/wp-content/uploads/2024/12/2024.12.04-SSCP-FINAL-REPORT-ANS.pdf (Далее – Доклад Конгресса США о COVID-19).

определяемые в США и ЕС как «дезинформация»[1], – например, о происхождении вируса COVID-19, который, по мнению американских законодателей, распространился в результате утечки из лаборатории в г. Ухань[2], Китай, или о неэффективности масочного режима (что было предметом мощной полемики в разгар пандемии).

В юридической науке и практике (особенно в отечественной) до сих пор не существует общепринятого определения дезинформации, что подтверждается исследованием отечественной и зарубежной научной литературы, проведенным автором. Чтобы хотя бы частично заполнить эту лакуну, мы провели анализ имеющихся дефиниций данного понятия в других научных дисциплинах, таких как социология, политология, психология, лингвистика, журналистика, компьютерные науки, и сравнили их как между собой, так и с юридическими воззрениями в контексте рассматриваемого вопроса. Такое исследование в российской юриспруденции проводится фактически впервые, направлено на восполнение существующего пробела в данной области научных знаний.

Дезинформация как объект исследования социальных наук

По мнению социологов И. Д. Пирютко и Л. Б. Кулемина, обман не является целью дезинформации, ее цель – влияние «на общественное мнение по определенному вопросу» [30, с. 329]. В период пандемии COVID-19 это было особенно заметно – так называемая «инфодемия» вряд ли сознательно разворачивалась с целью обмана. Например, многие противники вакцинации верили в то, что распространяли в цифровом пространстве, продвигали свою, отличную от официальной, позицию[3]. Инструменты искусственного интеллекта (ИИ) применялись для отслеживания сообщений в социальных сетях, чтобы бороться с дезинформацией о COVID-19 [69, с. 60]. Исследователи, изучавшие российскую инфодемию, отмечают, что социальные сети обладают особой силой в распространении обманчивого контента, называя это ключевым фактором их особой роли в тот период [24, с. 557]. В фейковых новостях, связанных с коронавирусом, часто использовались репортажи, ссылки на авторитетные источники, цитирование экспертов [24, с. 558]. Иными словами, сознательно применялись меры для придания большего веса, убедительности.

Д. А. Макурова отмечает, что «разница между дезинформацией и ложным информированием в средствах массовой информации на лингвистическом уровне довольно размыта» [21, с. 63]. Она выделяет три вида дезинформации: 1) заявления о том, что правдивая информация – ложная; 2) представление ложной информации как правдивой и 3) слухи. Последние представляют собой, по мнению исследователя, непроверенную информацию. Отметим, что с точки зрения правового регулирования этот вывод привлекает особое внимание, так как выделение трех видов дезинформации могло бы найти отражение в законодательстве, а на его основании могла бы дифференцироваться ответственность за распространение недостоверной информации. Помимо законодательных мер противодействия данный подход может быть использован в алгоритмах социальных сетей для затруднения распространения дезинформации.

Полагаем необходимым отметить, что в контексте исследований дезинформации затрагиваются элементы политологического дискурса, такие как «эпоха постправды», «фейковые новости»[4]. Последние часто определяются схожим образом со второй разновидностью дезинформации по классификации, предложенной Д.А. Макуровой, – когда ложная информация подается как правдивая. В частности, такую трактовку предложил Б. Калснес в 2018 году [46] и поддержала Н. А. Урусова в 2023 году [65, с. 20]. Некоторые авторы, например Дж. МакДугал, подчеркивают необходимость повышения медиаграмотности, считая ее своеобразным «антидотом» против дезинформации [22, с. 36]. Однако следует сделать замечание, что развитие критического мышления и повышение внимания к необходимости всесторонней проверки информации не является абсолютной защитой от ложной, искаженной информации, получаемой и распространяемой индивидуумом. Необходимо

[1] В частности, исследование, опубликованное в официальном журнале Американской медицинской ассоциации, утверждало, что теория об искусственном происхождении COVID-19 является «дезинформацией». Помимо этого, в исследовании содержится утверждение, что «по состоянию на 18 января 2023 года было подтверждено, что 1 100 000 случаев смерти, связанных с COVID-19, можно было предотвратить, если бы были выполнены рекомендации в области общественного здравоохранения». См. подробнее: Sule S., DaCosta M. C., DeCou E., Gilson C., Wallace K., Goff S. L. Communication of COVID-19 Misinformation on Social Media by Physicians in the US // JAMA Netw Open. ANGLE. 2023. Vol. 6. No. 8. P. 7. (In Eng.).

[2] Доклад Конгресса США о COVID-19. С. 1.

[3] Как мы отметили ранее, с окончанием пандемии вопрос относительно того, какие теории и утверждения относительно COVID-19 являлись однозначно ложными, а какие – могли быть предметом общественного дискурса, но были запрещены, а их авторы подверглись наказанию, не получил однозначного ответа. Упомянутый доклад Конгресса США о COVID-19 может являться основанием для пересмотра значительного числа обвинительных приговоров о распространении дезинформации. Данный факт должен рассматриваться как предостережение относительно применения слишком жестких мер по противодействию дезинформации ввиду возможного изменения взглядов на произошедшие события и их оценок.

[4] Следует отметить, что термин «фейковые новости» используется и в юридической литературе, и на уровне живых дискуссий между законодателями.

учитывать возможность когнитивных искажений, что, в свою очередь, является предметом изучения для ученых-психологов. Тем не менее меры по повышению медиаграмотности, выявлению фейков в новостном потоке всё чаще находят место в арсенале государственной политики по противодействию дезинформации во многих странах[1], а также на уровне ООН[2].

Продолжая изучение позиций специалистов в области гуманитарных наук относительно методов противодействия дезинформации, следует отметить, что не только юристы предлагают заслуживающие внимание выводы о методах именно правового регулирования в данной области. В частности, филолог В. В. Макашова выделяет три основных способа борьбы с дезинформацией: 1) правоприменительная практика, юридические запреты; 2) технологические: блокировки, замедление трафика; 3) повышение медиаграмотности [20, с. 191–192]. Отметим, что ещё до пандемии уже можно было встретить публикации на русском языке о разработке поисковых роботов и применении технологий машинного обучения для выявления дезинформации [26, с. 128–130]. Так называемая «журналистика данных» также предлагается некоторыми авторами в качестве средства борьбы с дезинформацией, на примере кейса выборов в Бангладеш [12, с. 29–32]. Под «журналистикой данных» подразумевается быстро растущая роль статистических данных в производстве и распространении информации в современном цифровом мире, «будущее журналистики» (то есть использование различных баз данных и открытых источников) [54, с. 227–48].

О. С. Иссерс называет медиафейки мистификацией и считает, что в цифровой среде их цель – не всегда введение в заблуждение [13]. В частности, она выделяет в качестве целей дезинформации так называемую «коммуникативную игру с потребителем» и даже провокационную социальную рекламу. Но часто медиафейки используются для персональной дискредитации, и современные технологии позволяют даже создать фальшивое видео (дипфейк, англ. deepfake), которое порой неотличимо от оригинала без специального программного обеспечения [Ibid]. Медийные лица, особенно политики, находятся в зоне риска, ведь чем больше видео с настоящим человеком доступно в Интернете, тем реалистичнее будет подделка. В этом отношении следует отметить, что вопрос о законодательном противодействии дипфейкам в настоящее время является одним из актуальных, требующим дополнительных изысканий.

Большое значение в анализе предпосылок для изменения законодательства о противодействии дезинформации имеет изучение феномена информационной войны, в которой дезинформация считается примером ведения боевых действий [9]. Феномен информационной войны достаточно подробно рассмотрен в отечественной политологии [23, 15] и психологии [58, 1, 3], военной науке, в том числе в работах специалистов по военному праву [5, 32, 17, 29]. В часто цитируемой статье Л. Н. Кунаковой отмечается, что «в рамках психологической парадигмы информационная война понимается как латентное воздействие информации на индивидуальное, групповое и массовое сознание при помощи методов пропаганды, дезинформации, манипулирования с целью формирования новых взглядов на социально-политическую организацию общества через изменение ценностных ориентаций и базовых установок личности» [18, с. 93].

С точки зрения совершенствования законодательства о противодействии дезинформации следует рассмотреть возможность дополнения уголовного законодательства нормой об ответственности за ведение информационной войны против Российской Федерации с опорой именно на вышеприведенное определение, которое могло бы получить отражение в примечании к соответствующей новой статье особенной части УК РФ.

Обращаясь к мнению специалистов по военному праву, следует согласиться с тезисом профессора Е. В. Калининой о том, что «основным вызовом информационной безопасности можно считать недостаточность нормативной базы, регулирующей соответствующие отношения как на национальном, так и на международном (региональном и универсальном) уровнях» [14, с. 20]. При этом число вызовов в данном отношении растет.

События, связанные с мировой геополитической напряженностью в период 2022–2024 годов, постоянно напоминают о том, что грань между военными действиями на земле, на воде и в воздухе и боевыми действиями в информационном пространстве не просто стирается. Информационная компонента средств нападения в рамках военных действий перестает быть вспомогательным инструментом, выходя на первый план. Оценивая эффективность действующей системы мер по противодействию дезинформации, следует учесть точку зрения известного специалиста по проблематике информационной войны – профессора А. В. Манойло, утверждающего следующее: «Должны быть обеспечены такие условия, при которых эти удары [информационной войны] просто не будут доходить до психики обычных людей. Если

[1] См., например: Доклад Группы европейских регуляторов по аудиовизуальным медиауслугам (European Regulators Group for Audiovisual Media Services, ERGA) “Improving Media Literacy campaigns on disinformation”, который освещает деятельность по распространению лучших практик в области медиаграмотности и противодействию дезинформации в государствах ЕС. URL: https://erga-online.eu/wp-content/uploads/2021/01/ERGA-SG2-Report-2020-Improving-Media-Literacy-campaigns-on-disinformation.pdf.

[2] Не дайте себя обмануть – новый курс ООН научит распознавать фейки. URL: https://news.un.org/ru/story/2022/11/1434332.

же они проникают через все барьеры, которые выстраиваются – или не выстраиваются – государством, и все-таки доходят до сознания граждан, то обычные люди становятся жертвами информационной войны»[1]. С юридической точки зрения важно подчеркнуть, что на государстве лежит особая ответственность за обеспечение эффективных мер по защите граждан от информационно-психологических операций противника. В настоящее время юридически эта функция не закреплена за каким-либо государственным органом, ответственность за такие деяния ограничена и может возникнуть только для исполнителей, непосредственно распространивших недостоверную информацию.

Дезинформация как объект исследования юридических наук

Для того чтобы сформировать достаточно объективное представление о том, как понятие «дезинформация» интерпретируется в отечественной и зарубежной науке, оценить вклад правовых исследований в изучение данного феномена, мы посчитали необходимым провести анализ опубликованных работ, в которых функционируют термины «дезинформация» и disinformation, с 2019 по 2024 год. Это позволит не только понять общую картину, но и выявить «горячие области», которые в настоящее время развиваются динамичнее всего, и определить «пустоты», еще не охваченные исследованиями. Данные наблюдения будут являться подтверждением новизны выводов автора о необходимости интеграции в правовой дискурс о дезинформации результатов изысканий в других научных областях и разработки конкретных рекомендаций по совершенствованию законодательства в данной области.

Исследуя наиболее цитируемые в настоящее время работы по тематике дезинформации среди российских ученых-правоведов, мы использовали данные Российского индекса научного цитирования (РИНЦ) – национальной информационно-аналитической системы, содержащей более 6 миллионов публикаций российских авторов, а также информацию о цитировании этих публикаций из более 4500 российских журналов[2]. Данная система позволяет в достаточной степени объективно с точки зрения наукометрии оценить актуальность и востребованность соответствующих публикаций по времени, тематике и цитируемости, так как содержит наибольшее число индексируемых данных относительно других отечественных электронных библиотек [34].

Обращаясь к наиболее цитируемым трудам, написанным юристами по проблематике дезинформации, можно сделать несколько выводов. В частности, по данным РИНЦ, наиболее цитируемой работой по проблемам дезинформации является статья Д. В. Бахтеева [6], в которой термин «дезинформация» упоминается вскользь, всего два раза. Следующая наиболее цитируемая работа, согласно данным РИНЦ, – статья Н. А. Головановой [11]. Это исследование носит характер обзора актуальной на тот момент (6 лет назад) законодательной базы и инициатив зарубежных государств, который достаточно объективно описывает сложившиеся тогда тенденции к определению дезинформации как ключевого вызова действующему правопорядку в государствах Европейского союза, Великобритании, США и других государствах, относящих себя к так называемому «западному миру». Отметим, что выявленные в статье тенденции значительно усилились. В то же время указанное исследование отвечает не на все вопросы о природе дезинформации и моделях борьбы с ней.

Совместная статья С. В. Андреева, Л. В. Бертовского и В. А. Образцова 2005 года исследует не проблему противодействия дезинформации, а применение дезинформации для введения преступников в заблуждение в интересах следствия и оперативно-розыскной деятельности [4]. Далее в списке наиболее цитируемых работ РИНЦ стоит исследование Е. Л. Невзгодиной и Н. Н. Парыгиной, в котором дезинформация рассматривается в контексте защиты деловой репутации. Будучи авторской концепцией, уместной в рамках узкоспециализированного изучения одного правового института, данная работа не является комплексным исследованием дезинформации как серьезной угрозы правопорядку [25]. Последней работой, входящей в сотню наиболее цитируемых трудов, индексируемых в РИНЦ, является статья С. И. Гирько, в которой дезинформация упоминается всего один раз [10].

Если сузить спектр поиска термина «дезинформация», то обнаружится, что в разделе «Информационное право» РИНЦ индексируется лишь 29 научных работ. Из них только 21 работа опубликована за последние 5 лет; 13 работ из данного перечня никогда не цитировались. Представленный количественный анализ достаточно ярко иллюстрирует состояние исследований по данному направлению. Публикаций по проблематике дезинформации в отечественной науке информационного права действительно мало, что, в свою очередь, коррелирует с достаточно хаотичным уровнем законодательного регулирования по данной проблеме, которое не получает необходимого научного анализа, что не соответствует уровню текущих вызовов и угроз с точки зрения обеспечения информационной безопасности Российской Федерации.

[1] Под снарядами вбросов: можно ли противостоять информационной войне? Интервью с профессором А. В. Манойло. URL: https://wciom.ru/expertise/pod-snarjadami-vbrosov-mozhno-li-protivostojat-informacionnoi-voine.

[2] Подробнее см.: eLIBRARY.RU - Российский индекс научного цитирования: о проекте elibrary.ru.

Относительно иностранных исследований, посвященных дезинформации, можно отметить следующее. С помощью онлайн-платформы ScienceDirect издательства Elsevier, используя для поиска по ключевым словам термин disinformation, мы обнаружили, что с 2019 года проиндексировано 1975 исследований по данной тематике. Из них по социальным наукам 810 публикаций, или 41,01 % от общего числа публикаций. По медицинским наукам без выделения конкретных направлений – 510, по иммунологии и микробиологии 96, по психологии – 221, то есть суммарно 41,87 %. Введение дополнительного поискового признака в виде термина COVID показывает, что изучению пандемии или ее последствий посвящено 581 исследование. В свою очередь введение дополнительного ключевого слова – law – дает выборку лишь 100 работ из 1975, что представляется недостаточно репрезентативным для более полных выводов.

Аналогичный поиск по базе научной литературы издательства Taylor & Francis дал более релевантные результаты. Общее число публикаций – 6947, из них 275 атрибутируются их авторами как правовые исследования, что позволяет сделать некоторые выводы на основе изучения как общего корпуса методами семантического поиска, так и наиболее цитируемых или выделяемых по определенным общим признакам работ. Отметим, что из общего корпуса индексированных исследований 2873 (41,36 %) также обращаются к теме пандемии.

Наиболее общим выводом является тот факт, что значительный импульс исследованиям по данной проблематике дан во время пандемии COVID-19. Это подтверждается количественным анализом публикаций, описанным выше.

Не имея специальных познаний в области медицины, автор не может предложить сугубо медицинский взгляд на проблематику дезинформации. Однако считаем возможным повторить: представления о том, какая теория относительно противодействия COVID-19 является «дезинформацией», а какая – предметом защищаемой правом на свободу слова дискуссии, до сих пор претерпевают серьезные изменения[1]. Это, в свою очередь, требует разработки механизмов восстановления в правах пострадавших от несправедливых ограничений и выплаты компенсаций, в том числе за ограничения, осуществляемые интернет-платформами, на основании самостоятельно разработанных политик модерации.

Анализ юридических исследований по рассматриваемой проблематике позволяет сделать некоторые выводы и определить ряд тенденций. Из 6947 работ по вопросам дезинформации, индексированных в базе данных научных исследований Taylor & Francis, 2125 имеют отсылку к России, разумеется, в негативном контексте, что в определенной степени предсказуемо с учетом геополитического фактора. Например, наиболее релевантными по мнению системы в данном поиске являются работы с такими заголовками: “The Russian Military’s Biological Warfare Disinformation Campaign and the Russo-Ukrainian War” [37]; “Fake leads, defamation and destabilization: how online disinformation continues to impact Russia’s invasion of Ukraine” [47]; “Truth with a Z: disinformation, war in Ukraine, and Russia’s contradictory discourse of imperial identity” [65]. В целом можно выделить несколько нарративов.

Во-первых, в зарубежной научной литературе даются крайне негативные оценки действий российского государства в киберпространстве. В частности, доминирующей точкой зрения является тезис о «распространении Россией дезинформации» [64; 60; 58; 45], что, в свою очередь, значительно сужает возможности для научной кооперации в исследованиях по данному направлению либо ограничивает их исследованиями в этом направлении.

Во-вторых, при оценке российского законодательства в области противодействия дезинформации, регулированию Интернета отчетливо превалируют достаточно негативные оценки, при этом наблюдаются позитивные оценки законодательства ЕС. Например, A. Peukert указывает, что «среди либеральных демократий Европейский союз принял наиболее всеобъемлющие меры по борьбе с незаконной и не противозаконной, но вредной дезинформацией различных типов» [54]. В целом дискуссия о России и дезинформации в основном сводится, по мнению Stephen C. Hutchings, к «манифестации сопротивления обманным действиям тоталитарных режимов и современных авторитарных государств, враждебно настроенных к демократическому правлению» [44].

В основе логики «противодействия дезинформации со стороны тиранических и авторитарных режимов» лежит крайне политизированная и предвзятая матрица суждений, что наглядно видно на примере таких работ, как исследование L. Marlene и K. Limonier “Beyond “hybrid warfare”: a digital exploration of Russia’s entrepreneurs of influence”, описывающее российскую политическую систему как комплекс акторов, проецирующих незаконное вмешательство в дела других государств путем распространения дезинформации [48], что снижает объективность оценок, сделанных в рамках исследований.

Однако следует отметить наличие критических голосов в западном академическом дискурсе, которые отмечают недостатки сложившегося «триумвирата», возникшего между крупными СМИ, академическими

[1] Это обстоятельство особенно ярко проявляется после прихода к власти администрации Д. Трампа, так как она отрицает весь тот набор нарративов, которые официально были утверждены администрацией Дж. Байдена. См., например: ЦРУ изменило мнение о причинах возникновения COVID. URL: https://www.rbc.ru/politics/26/01/2025/6795bb7c9a7947126718ec24.

кругами, политическими экспертами[1] и получившего самую энергичную поддержку американского политического истеблишмента, одержимого «возвращением силы распространения знаний группе “объективных привратников”» [35]. По меткому замечанию Stephen C. Hutchings, на Западе возник целое академическое сообщество вокруг изучения проблем дезинформации. Иными словами, по мнению исследователя, весь этот аппарат создается для «подавления оппозиционных знаний со стороны либерального миропорядка» [44]. Он также отмечает, что данный дискурс со стороны государственных органов и некоммерческих организаций, занимающихся «противодействием дезинформации» на Западе, обычно связан со «стиранием грани между семантическим поиском дезинформации и борьбой с “языком ненависти”» [Ibid].

Данное замечание значимо и с юридической точки зрения, поскольку позволяет проанализировать процессы, легшие в основу целеполагания при осуществлении законотворчества. Поэтому если мы имеем «своею целью раскрыть истинную волю законодателя» [7, с. 83], то нам, безусловно, приходится обращаться к телеологическому изучению исходных причин и установок, которые стали отправной точкой складывающегося на Западе корпуса законодательства по противодействию дезинформации.

Относительно понятия «дезинформация» в зарубежных исследованиях необходимо отметить, что его применение в иностранной научной и правоприменительной деятельности позволило интегрировать между собой большие массивы научной информации, что, в свою очередь, сыграло положительную роль в изучении данных по этому направлению. Анализ исследований, рассмотренных в настоящей работе, показывает, что отказ от использования указанного термина в законотворческой и правоприменительной практике в Российской Федерации может ограничивать потенциал научного исследования данной области. Это связано с тем, что правовые исследования по этому направлению пока недостаточно интегрируют достижения других наук, таких как лингвистика, психология, журналистика и военное дело. Представляется, что совершенствование законодательства о противодействии дезинформации невозможно без интеграции соответствующих изысканий других наук.

Сравнение законодательства и практик противодействия дезинформации в ЕС, США и России

1. Подходы Европейского союза к противодействию дезинформации: особенности регулирования и вызовы для России

ЕС начиная с прошлого десятилетия и по настоящее время уделяет большое внимание противодействию дезинформации на технологическом и нормативном уровнях. Регулирование в данной области можно в самом общем виде разделить на акты саморегулирования, поощряемого Еврокомиссией, и законодательство ЕС.

К значимым актам саморегулирования можно отнести Кодекс практики по дезинформации 2022 года (The 2022 Code of Practice on Disinformation, Кодекс практики)[2]. Данный акт саморегулирования примечателен своим комплексным и сложным характером. В частности, он не является официальным нормативным актом, однако Европейская комиссия предварительно издала официальное Руководство (Guidance to the Code of Practice on Disinformation)[3], которое легло в основу обновленной версии Кодекса практики 2022 года, сменившей редакцию 2018 года. Участие осуществляется присоединением к общему соглашению, что со своей стороны сделали многие крупные технологические корпорации, такие как Google, Microsoft, Adobe, TikTok, Meta*, Vimeo, Twitch. С другой стороны, в данной инициативе участвуют организации и платформы, связанные с распространением новостей и рекламы, такие как Репортеры без границ, The Global Disinformation Index, Мировая федерация рекламодателей, Европейская ассоциация коммуникационных агентств и другие игроки[4].

Большой интерес для изучения возможных моделей саморегулирования, которые пока не применяются в России, представляет система мер, предусмотренная Кодексом практики – он содержит 44 обязательства и 128 специальных мер по недопущению распространения дезинформации. Наиболее значимые из них: недопущение монетизации для распространителей дезинформации, прозрачность политической рекламы, сотрудничество в период выборов и использование структурных индикаторов. Необходимо отметить, что данный Кодекс практик носит отнюдь не декларативный, а глубоко прикладной характер, что

[1] Данный феномен, получил неофициальное название «BigDisinfo». Термин BigDisinfo является отсылкой к терминам BigPharma и BigTech, отражающему феномен влияния на принимаемые решения в области здравоохранения крупных корпораций, производящих лекарственные препараты. В данном случае имеется в виду большое влияние на дискурс о дезинформации мейнстримовых СМИ и работающих с ним в паре аппарата аналитических и политических центров.

[2] The 2022 Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[3] Commission presents guidance to strengthen the Code of Practice on Disinformation. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585.

[4] Полный список подписантов соглашения доступен по ссылке. URL: https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

* Компания Meta признана экстремистской в Российской Федерации, её деятельность запрещена в Российской Федерации по решению суда.

обеспечивает глубокую интеграцию интернет-платформ в систему противодействия дезинформации, выстраиваемую Еврокомиссией. Данная система включает в себя большое количество инициатив, направленных на побуждение к саморегулированию путем опубликования таких документов, как План действий по противодействию дезинформации (2018 Action Plan Against Disinformation)[1], ежегодные отчеты об оценке выполнения Кода практик и др. Другим направлением саморегулирования является создание «зонтичных организаций», таких как European Digital Media Observatory (EDMO), которая является негосударственной организацией, объединяющей и синхронизирующей работу организаций и платформ, осуществляющих фактчекинг (проверку фактов на достоверность), поддерживающих исследования, осуществляющих мониторинг эффективности практик по противодействию дезинформации[2].

Большую роль в регулировании противодействия дезинформации на уровне ЕС играет упомянутый ранее Закон о цифровых услугах ЕС (Digital Services Act, DSA)[3]. Обращает на себя внимание тот факт, что уже в преамбуле этого документа (ст. 2) в качестве основных угроз названы «противоправный контент и онлайн дезинформация». В целом термин «дезинформация» упоминается в тексте Закона о цифровых услугах ЕС 13 раз, что дает достаточно подробное представление о смысле данного понятия. С точки зрения его нормативного толкования, исходя из содержания текста DSA, прежде всего следует обратить внимание на статью 95, которая указывает на то, какую именно угрозу общественной безопасности несет дезинформация: «…с реальным и предсказуемым негативным воздействием на общественное здоровье, общественную безопасность, гражданский дискурс, участие в политической жизни и равенство». Статья 104 DSA говорит о «возможных негативных последствиях, проистекающих из системных рисков для общества и демократии, таких как дезинформация или манипулятивная и злоупотребительная деятельность или любые неблагоприятные последствия для несовершеннолетних». Согласно тексту Digital Services Act (ст. 84) дезинформация – это обманчивая, или вводящая в заблуждение, или манипулятивная информация, распространение которой несет для общества и демократии системный риск возникновения реального и предсказуемого негативного воздействия на общественное здоровье, общественную безопасность, благополучие несовершеннолетних, гражданский дискурс, возможность участвовать в политической жизни и проведение в жизнь начал равенства. Безусловно, данное определение достаточно громоздко, однако оно в полной мере отражает текстуальный смысл, заложенный законодателем в понятие дезинформации. Тем не менее, давая оценку системе мер ЕС по предупреждению распространения дезинформации, следует учитывать выводы, сделанные в предыдущем разделе, о том, что регуляторные меры по противодействию дезинформации в своей сути, в своем исходном целеполагании направлены на установление контроля над распространением информации на территории ЕС, в том числе путем «поглощения» информационного суверенитета отдельных государств-участников, так как именно бюрократический аппарат Европейского совета благодаря DSA получает практически всю полноту контроля за общим информационным пространством ЕС (ст. 2 DSA).

Для полноты телеологического толкования данного структурно сложного, комплексного закона и сопутствующего ему регулирования следует обратить внимание на неформальные практики Европейской комиссии, связанные с противодействием дезинформации. В частности, представляется необходимым изучить конфликт между руководством Еврокомиссии и владельцем платформы X (бывш. Twitter) Илоном Маском, который 12 июля 2024 г. заявил, что Европейская комиссия предложила платформе X тайную сделку с целью установления цензуры на платформе в обмен на отказ от применения штрафных мер. Он также отметил, что «другие платформы пошли на эту сделку»[4]. Сказанное Илоном Маском можно соотнести с проанализированным Кодексом практик, а серьезные штрафные меры действительно предусмотрены DSA. Подтверждают слова И. Маска и другие факты. В частности, 23 декабря 2023 г. в отношении X было открыто предварительное расследование относительно несоблюдения положений Digital Services Act о запрете «темных практик» (dark patterns), доступе для исследователей к внутренним данным платформы и распространении дезинформации. Дополнительно Еврокомиссия пригласила сотрудников X на условиях анонимности сообщать о нарушениях законодательства ЕС, чтобы помочь расследованию[5]. В целом X грозит штраф в размере до 6 % глобального годового оборота, если компания будет признана виновной в рассматриваемых правонарушениях.

[1] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation (JOIN (2018) 36 final). URL: https://digital-strategy.ec.europa.eu/en/library/action-plan-against-disinformation.

[2] URL: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065.

[4] European Commission offered secret censorship to X social network — Musk. URL: https://tass.com/economy/1816441.

[5] Commission sends preliminary findings to X for breach of the Digital Services Act. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761.

Позднее, 25 августа 2024 г., во Франции был арестован основатель и генеральный директор Telegram Павел Дуров по ряду тяжких обвинений, которые напрямую связаны с претензиями французских властей к качеству модерации контента в мессенджере Telegram[1]. 29 августа того же года появилась информация о том, что Еврокомиссия ведет предварительное расследование относительно возможного занижения числа пользователей мессенджера в Европе[2]. После своего ареста П. Дуров неоднократно заявлял о необходимости усиления качества модерации мессенджера, что в итоге стало его «личным приоритетом»[3].

Данные примеры показывают, что в рамках противодействия дезинформации ЕС применяет не только официальные, но и неофициальные меры, затрагивающие интересы Российской Федерации в информационном пространстве.

2. Подходы Соединенных Штатов Америки к противодействию дезинформации: особенности регулирования и вызовы для России

Структура законодательства США в отношении регулирования оборота информации значительно отличается от таковой в странах Европы. Не будет преувеличением сказать, что в Соединенных Штатах сложилась по-своему уникальная традиция защиты свободы слова, основанная на широком доктринальном понимании ее границ, проистекающая не только из текста Первой поправки к Конституции США, но и из многочисленных судебных прецедентов, постоянно уточняющих границы и практические особенности реализации права на высказывание и самовыражение [40]. Тем не менее, с учетом обострения политической борьбы в США, когда поляризация политических позиций населения США начинает делить страну на два всё менее готовых соглашаться друг с другом лагеря[4], взгляды на вопрос о том, должен ли сохраняться бескомпромиссный взгляд на защиту свободы слова, начинают претерпевать изменения [36].

Кульминацией описанных процессов является первое избрание президентом США Дональда Трампа в 2016 году, которое многократно усилило дискурс о том, насколько крупные интернет-платформы способны влиять на общественное мнение, выборы, внутреннюю и внешнюю политику, насколько интернет-платформы могут быть эффективным инструментом внешнего вмешательства путем распространения злонамеренными акторами дезинформации и каковы последствия и ответственность за такие действия [63]. Весь этот процесс в каком-то смысле длится до сих пор, каждый раз получая новый импульс, как это было после событий 6 января 2021 г., приведших к такому знаковому событию, как синхронная блокировка аккаунтов действующего Президента США на всех крупных интернет-платформах[5]. Этот случай подчеркивает уровень автономии, который получили интернет-платформы в США в части возможности интерпретировать границы свободы слова и осуществлять саморегулирование. Чтобы оценить его масштаб, можно обратиться к такой цифре – только в 2020 году Facebook* удалил около 12 млн отдельных сообщений в приватных группах, 87 % которых были определены как запрещенные правилами без участия в процессе человека[6]. В целом корпорация уделяет большое внимание борьбе с дезинформацией путем запрета «скоординированного недостоверного поведения» (Coordinated Inauthentic Behavior, CIB). В 2018 году было дано публичное определение данного понятия: «скоординированное недостоверное поведение не разрешено, потому что мы не хотим, чтобы люди или организации, создающие сети учетных записей, вводили в заблуждение других о том, кем они являются, или что они делают»[7]. Иными словами, речь идет о противодействии организованным кампаниям по дезинформации, причем на официальном уровне не сообщается о коммуникации по данному вопросу со специальными службами каких-либо государств, включая сами США (презюмируется, что такая коммуникация отсутствует). Анализируя ряд других заявлений представителей Facebook*, можно сделать вывод, что скорее всего взаимодействие со спецслужбами западных стран имеет место. Следует отдельно подчеркнуть, что никакой эффективной судебной процедуры обжалования мер в области модерации контента в США не существует. Это особенно актуально для российских пользователей, которые регулярно подвергаются ограничениям со стороны крупных онлайн-платформ[8]. В качестве доказательства данного тезиса можно привести в пример тот факт, что федеральный суд отказал даже

[1] Источник заявил о соответствии ареста Дурова Акту о цифровых услугах ЕС. URL: https://tass.ru/obschestvo/21682013.

[2] ЕС расследует, не занижал ли Telegram число европейских пользователей. URL: https://3dnews.ru/1110155/bryussel-podozrevaet-telegram-v-sokritii-kolichestva-polzovateley-es.

[3] Личный телеграм-канал Павла Дурова. URL: https://t.me/durov/342.

[4] Americans see little bipartisan common ground, but more on foreign policy than on abortion, guns. Pew Research. URL: https://www.pewresearch.org/short-reads/2024/06/25/americans-see-little-bipartisan-common-ground-but-more-on-foreign-policy-than-on-abortion-guns/

[5] Twitter bans President Trump permanently. URL: https://edition.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html.

[6] Our Latest Steps to Keep Facebook Groups Safe. URL: https://about.fb.com/news/2020/09/keeping-facebook-groups-safe/.

[7] Removing Bad Actors on Facebook. URL: https://about.fb.com/news/2018/07/removing-bad-actors-on-facebook/.

[8] Роскомнадзор потребовал прекратить цензуру российских СМИ от Facebook и Google. URL: https://www.gazeta.ru/tech/2020/10/28/13336639/censorship.shtml.

* Продукт корпорации Meta, признанной в России экстремистской организацией, чья деятельность запрещена в России на основании решения суда.

действующему президенту США Дональду Трампу в восстановлении его аккаунта после блокировки в ходе событий 6 января 2021 г.[1]

Отметим, что такой уровень автономии онлайн-платформ возможен ввиду особенностей федерального законодательства Соединенных Штатов. В частности, ключевым для регулирования правоотношений между интернет-платформами, пользователями и исполнительной властью в США является подраздел 230 раздела 47 (Section 230 Title 47) Акта о Пристойности Телекоммуникаций 1996 года (Communications Decency Act of 1996 – CDA; далее – подраздел 230), который дает интернет-платформам статус «издателя» (publisher), что в силу устоявшегося толкования Первой поправки к Конституции США (Билль о правах) наделяет их правами, аналогичными праву СМИ определять собственную редакционную политику, то есть публиковать какую-либо информацию исключительно на основании собственной редакционной политики. Сложившийся своеобразный status quo значительно повышает значимость саморегулирования интернет-платформ, в том числе в вопросе определения того, что является дезинформацией, как осуществляется ее удаление и ограничение, какие меры воздействия применяются к нарушителям.

Тем не менее было бы ошибочным считать, что в США не существует средств воздействия на интернет-платформы с точки зрения выбора направления модерации дезинформации. Например, технологический предприниматель Илон Маск, который в 2023 году приобрел корпорацию Twitter, сообщил, что предыдущие владельцы социальной сети на еженедельной основе проводили секретные совещания с представителями ФБР, Министерства внутренней безопасности (Department of Homeland Security, DHS), а также директората национальной разведки (Directorate of National Intelligence, DNI). Исходя из представленных Маском данных Twitter получал от ФБР прямые запросы на удаление информации и аккаунтов вместе с другими крупными социальными сетями и технологическими компаниями. Признание в том, что ФБР оказывало давление на Meta* в части направления требований об удалении дезинформации на ее платформах сделал и Марк Цукерберг в своем открытом письме Конгрессу США. При этом он отметил, что в ряде случаев удаление контента и аккаунтов было «ошибочным», о чем он сожалеет в свете появления новой информации[2].

Значительное внимание на федеральном законодательном уровне уделяется противодействию дипфейкам, то есть аудио-, фото- и видеоматериалам, полученным с помощью инструментов искусственного интеллекта и содержащим значительные искажения и/или изменения контента с целью ввести зрителя/слушателя в заблуждение. В частности, полномочия по принятию мер, направленных на идентификацию и противодействие манипуляциям с медиаконтентом, были даны Министерству обороны США еще в 2020 году в соответствующем законе об оборонном бюджете [8, с. 220]. Тем не менее такое регулирование остается в своеобразной «серой зоне» ввиду процитированных положений Первой поправки к Конституции США, что не позволяет наделить какой-либо федеральный орган конкретными официальными полномочиями по ограничению распространения контента. Поэтому политика в этой области переходит к неформальным операциям влияния, когда соответствующие специальные службы или сотрудники президентской администрации убеждают онлайн-платформы предпринимать определенные действия в обход положений закона, фактически нарушая его.

3.3. Подходы к противодействию дезинформации в Российской Федерации

Согласно новому проекту Указа Президента России «О стратегии противодействия экстремизму в Российской Федерации» (номер проекта 01/03/07-24/00149268 от 22.07.2024)[3], подготовленному МВД России, различные методы манипулирования общественным мнением и распространения недостоверной информации, в том числе дискредитация Вооруженных Сил Российской Федерации и исполнения государственными органами Российской Федерации своих полномочий, способствующей усилению радикальных и экстремистских настроений в российском обществе, являются одними из основных способов дестабилизации общественно-политической и социально-экономической обстановки в Российской Федерации.

Президент России В. В. Путин неоднократно подчеркивал, что против России ведется информационная война. В частности, 22 мая 2022 г. он заявил, что «против России развязана настоящая агрессия, война в информационном пространстве»[4].

[1] Federal judge rejects Trump's lawsuit challenging Twitter ban. URL: https://www.pbs.org/newshour/nation/federal-judge-rejects-trumps-lawsuit-challenging-twitter-ban.

[2] Mark Zuckerberg says Meta was 'pressured' by Biden administration to censor Covid-related content in 2021. URL: https://edition.cnn.com/2024/08/27/business/mark-zuckerberg-meta-biden-censor-covid-2021/index.html.

[3] Федеральный портал проектов нормативно-правовых актов. Проект Указа президента Российской Федерации «Об утверждении Стратегии противодействия экстремизму в Российской Федерации». URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=149268.

[4] Путин заявил, что против России развязана война в киберпространстве. URL: https://tass.ru/politika/14686131.

* Корпорация Meta признана в России экстремистской организацией, ее деятельность в России запрещена на основании решения суда.

В феврале 2023 года Президент России развил свою мысль, указав на то, что «…всегда эта борьба сопровождалось противоборством в информационном поле. И это было всегда, на протяжении всей нашей истории. А то, что происходит сегодня и сопровождает специальную военную операцию, – это только обострение этой борьбы, которая велась всегда»[1]. Об угрозах дезинформации говорит пункт 52 раздела «Информационная безопасность» Стратегии национальной безопасности Российской Федерации: «в целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов»[2].

Таким образом, проблема информационной войны, распространения дезинформации как ее ключевого инструмента признается на высшем государственном уровне, а противодействие дезинформации является одной из крупнейших задач, которые стоят перед законодателями и правоприменителями на текущий момент. Тем не менее, как показывает обзор отечественной научной литературы в данной области, эта проблематика в настоящее время исследуется недостаточно. Не решена проблема совершенствования законодательства, направленного на противодействие дезинформации. Действующие меры регулирования в большей части основываются на подходах, выработанных в период пандемии, для которых характерно отсутствие системности и устойчивости, что подтверждается ранее приведенными фактами о злоупотреблениях при осуществлении противодействия дезинформации. Законодательство во многом по-прежнему носит экспериментальный характер, не подкреплено серьезными юридическими исследованиями, правоприменительной практикой, страдает от дефицита системного подхода к его формированию. Например, с 2020 года в Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (далее – Закон № 149-ФЗ) было внесено 26 поправок. Отсутствие общей нормы о противодействии дезинформации вынуждает законодателя создавать многочисленные конструкции, во многом повторяющие друг друга, громоздкие, трудно воспринимаемые как для обывателя, так и для специалистов. Данная тенденция прослеживается и в УК РФ: так, за последние годы была значительно расширена глава 24 УК РФ, также кодекс пополнился статьями:

205.2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма;

207.1. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан;

207.2. Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия;

207.3. Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации;

280. Публичные призывы к осуществлению экстремистской деятельности;

280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации.

280.3. Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, исполнения государственными органами Российской Федерации своих полномочий, оказания добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации;

Перечисленные статьи УК РФ криминализуют распространение различных видов недостоверной информации, но каждый раз предлагается новое определение вместо использования единого понятия «дезинформация». В каких-то случаях, когда речь идет о пропаганде терроризма, это оправданно (ст. 205.1 УК РФ). В других ситуациях это явно избыточно и громоздко, например в статье 207.1 УК РФ: публичное распространение заведомо ложной информации об обстоятельствах, *представляющих угрозу жизни и безопасности граждан*; в статье 207.2: публичное распространение заведомо ложной общественно значимой информации, *повлекшее тяжкие последствия*.

С распространением заведомо ложной информации связаны диспозиции и других статей УК РФ, например статья 354 «Публичные призывы к развязыванию агрессивной войны», статья 354.1. «Реабилитация нацизма», так как объективная сторона данных преступлений в основном заключается в распространении дезинформации. Представляется, что подобные преступления можно было бы выделить в от-

[1] Путин заявил, что с Россией всегда велась борьба. URL: https://tass.ru/politika/16950005

[2] О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Собр. законодательства Российской Федерации. 2021. № 27, ст. 5351 (ч. 2).

дельную главу, где были бы объединены все уголовные составы, связанные с распространением дезинформации. В данной главе можно было бы дать определение дезинформации как общего понятия, без необходимости дальнейшего повторения в составах, где объективная сторона состоит в распространении дезинформации. В таком случае можно избежать громоздких определений, ограничиться формулировками «дезинформация против Вооруженных сил», «дезинформация против государственной власти», «дезинформация в целях пропаганды деструктивной идеологии» и т. п. Аналогично тому, как это сделано в актах ЕС, в целом большинство составов можно было бы систематизировать как распространение дезинформации или распространение деструктивной информации определенного рода, выделив именно соответствующую специфику.

Из опыта ЕС можно было бы заимствовать практику направляемого государством саморегулирования, когда онлайн-платформы, журналисты и представители гражданского общества объединяются для выработки специальных кодексов практик по противодействию дезинформации. При этом важно избежать формального подхода, когда такие соглашения не требуют обязательного выполнения принятых на себя обязательств. В ЕС в аналогичных случаях используется механизм выделения специальных органов, создаваемых участниками соглашения, и наделения их соответствующими полномочиями по мониторингу и контролю взятых на себя обязательств.

Выводы

Как показывает углубленное изучение научной литературы по проблематике дезинформации, российская наука и зарубежные исследования движутся в разных направлениях. Если в России термин «дезинформация» используется достаточно ограниченно и несколько хаотично – в основном в правоприменительной практике и в СМИ, то за рубежом данному феномену, а соответственно, и термину уделяется большое внимание как на уровне законодательства, так и в научной литературе различных дисциплин. В отношении проблем противодействия дезинформации за рубежом активно развивается законодательство, ведутся научные исследования, к деятельности по противодействию дезинформации привлекаются онлайн-платформы, которые участвуют в этой работе не только как исполнители законодательства, но и как стейкхолдеры, вовлеченные в данный процесс на организационном уровне – они играют роль в формировании так называемого «мягкого права», участвуют в *со*-регулировании и саморегулировании правоотношений в данной области.

Представляется, что отсутствие должного внимания к термину «дезинформация» на научном уровне, отсутствие инициатив по внедрению данного термина на законодательном уровне в России не соответствует тем задачам, которые в настоящее время стоят перед законодателем, когда противодействие распространению недостоверной информации является одной из ключевых проблем информационного противостояния, а эффективность регулирования информационного пространства критически важна.

Анализ развития законодательства об информации, противодействии угрозам в информационном пространстве показывает, что существует дефицит системности в подготовке соответствующих законодательных инициатив. Данная проблема особенно ярко себя проявит, когда разработчики Цифрового кодекса приступят к подготовке соответствующих разделов закона, важность подготовки которого в очередной раз признал Президент Российской Федерации[1]. Уже сейчас очевидно, что текущая редакция Закона № 149-ФЗ не позволяет взять соответствующие нормы и просто перенести в новый кодекс – они не соответствуют общепринятым критериям систематизации законодательства, а именно не может быть «обеспечено системное нормативное регулирование одного вида общественных отношений путем создания единого, юридически и логически цельного, внутренне согласованного нормативного акта, выражающего содержательную и юридическую специфику структуры обособленных подразделений системы права» [2, с. 254].

Изложенное обстоятельство, как и тот факт, что сам законодатель признает необходимость кодификации нормативно-правовых актов информационного права в виде Цифрового кодекса, предопределяет необходимость перехода в законодательстве об информации к таким обобщающим понятиям, как дезинформация. Тем более что данный термин широко признан в зарубежной юридической науке, подробно освещен в других отечественных науках, таких как политология, социология, психология, журналистика и др., что подтверждается результатами настоящего исследования. Иными словами, расширение юридических исследований в области дезинформации, интеграция данного термина в законодательство и соответствующая перестройка норм, касающихся распространения недостоверной информации, не только целесообразны, но и необходимы с точки зрения процессов систематизации отечественного информационного законодательства. В противном случае качество регулирования соответствующих правоотношений не будет согласовываться с критериями кодифицированного нормативного акта, о чем уже было сказано.

[1] Путин пообещал придать дополнительный импульс разработке Цифрового кодекса РФ. URL: https://www.interfax-russia.ru/moscow/news/putin-poobeshchal-pridat-dopolnitelnyy-impuls-razrabotke-cifrovogo-kodeksa-rf.

Представляется, что необходим самостоятельный, российский взгляд на природу и понятие дезинформации в процессе введения данного понятия в законодательство. Предлагается предусмотреть в проекте Цифрового кодекса отдельный раздел, посвященный противодействию деструктивной информации, где были бы указаны виды деструктивной информации, в числе которых должна быть представлена и дезинформация. С учетом достижения других наук предлагается следующее определение дезинформации: *деструктивная информация, направленная на введение в заблуждение общества путем обмана с целью подорвать основные ценностные установки, закрепленные Конституцией Российской Федерации, нарушить общественный порядок, создать панику, дезорганизовать или дискредитировать работу органов власти и военного управления*. При этом особенно важно, чтобы законодательно была установлена гарантия свободы слова, направленная на защиту лиц, говорящих «неудобную правду», а именно сообщающих о преступлениях и злоупотреблениях, выявленных членами гражданского общества. Как известно, об этой проблеме говорилось на самом высоком уровне, однако принцип «ошибаться можно, врать нельзя» должен получить законодательное отражение[1]. В частности, предлагается закрепить в Уголовном кодексе принцип недопущения привлечения лица к уголовной ответственности, в случае распространения им сведений о готовящемся или совершенном преступлении, даже если такие сведения могут быть признаны дискредитирующими для органов власти. Однако для предупреждения злоупотреблений, в случае опровержения распространенных сведений в ходе судебного разбирательства, предлагается взыскивать с такого лица крупные штрафы. Конкретизация данных норм требует широкой научной и общественной дискуссии, однако отсутствие таких механизмов, которые формируют баланс права на свободу слова и требование защищать интересы государства и общества в информационном пространстве, сейчас ощущается особенно остро.

В целом следует отметить чрезвычайную сложность противодействия дезинформации, в том числе потому, что часто невозможно установить, является ли та или иная информация достоверной в момент ее распространения. Этот факт определяет необходимость вовлечения в работу по противодействию дезинформации структуры гражданского общества, что, в свою очередь, требует внесения изменений в раздел «Информационная безопасность» Стратегии национальной безопасности Российской Федерации, в части дополнения его конкретными шагами по предупреждению распространения дезинформации, и выделения специальной подпрограммы, привязанной к Стратегии. Предлагается дополнить ее определением дезинформации, предложенным в настоящем исследовании.

Библиографический список

1. *Аблеев С. Р., Кузьминская С. И.* Медийные мистификации массового сознания как психологическое орудие информационной войны // Психология и педагогика служебной деятельности. 2023. № 2. С. 12–15.
2. *Алексеев С. С.* Общая теория права: в 2 т. Т. 1. М.: Юрид. лит., 1981. 360 с.
3. *Альджадуои А. Д. Х.* Тенденции развития методов ведения современной информационной войны // Обществознание и социальная психология. 2022. № 11 (41). С. 305–308.
4. *Андреев С. В., Бертовский Л. В., Образцов В. А.* Использование дезинформации при выявлении и расследовании преступлений // Российский следователь. 2005. № 8. С. 2–5.
5. *Аулов В. К.* Правовой инструментарий информационной войны: базовые ценности военной организации государства и юридические технологии их разрушения // Военное право. 2022. № 3 (73). С. 44–53.
6. *Бахтеев Д. В.* Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. 2018. № 2 (104). С. 43–49.
7. *Васьковский Е. В.* Цивилистическая методология: учение о толковании и применении гражданских законов. М.: Центр ЮрИнфоР, 2002. 507 с.
8. *Виноградов В. А., Кузнецова Д. В.* Зарубежный опыт правового регулирования технологии «дипфейк» // Журнал Высшей школы экономики. Право. 2024. Т. 17(2). С. 215–240. DOI: 10.17323/2072-8166.2024.2.215.240.
9. *Воронова О. Е.* Современные информационные войны: типология и технологии. Рязань: Ряз. гос. ун-т имени С. А. Есенина, 2018. 188 с.
10. *Гирько С. И.* Проблемы уголовно-процессуального статуса уголовно-исполнительной системы Российской Федерации: мифы и реальность // Ведомости уголовно-исполнительной системы. 2020. № 7 (218). С. 13–21.
11. *Голованова Н. А.* Новые формы онлайн-преступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 42–57. DOI: 10.12737/jflcl.2019.3.4.
12. *Жук Д. А., Жук Д. В., Третьяков А. О.* Методы определения поддельных новостей в социальных сетях с использованием машинного обучения // Информационные ресурсы России. 2018. № 3. С. 29–32.
13. *Иссерс О. С.* Медиафейки: между правдой и мистификацией // Коммуникативные исследования. 2014. № 2. С. 112–123.
14. *Калинина Е. В.* Дилеммы правового регулирования безопасности информационного пространства и коммуникативные медиатехнологии как инструменты ведения информационной войны //

[1] Белоусов заявил, что руководствуется принципом «ошибаться можно, врать нельзя». URL: https://tass.ru/politika/20792945.

Военно-юридический журнал. 2023. № 1. С. 19–23. DOI: 10.18572/2070-2108-2023-1-19-23.

15. *Караяни А. Г.* Теория и практика психологической войны. Организация и проведение информационных операций. URL: http://psyfactor.org/lib/psywar30.htm.

16. *Козлов В. В., Власов Н. А.* Информационные войны: история и современность // Человеческий фактор. Социальный психолог. 2017. № 1 (33). С. 98–111.

17. *Красовская Н. Р., Гуляев А. А.* Информационные войны на территории бывшего СССР // Гуманитарные проблемы военного дела. 2019. № 2 (19). С. 51–58.

18. *Кунакова Л. Н.* Информационная война как объект научного анализа (понятие и основные характеристики информационной войны) // Альманах современной науки и образования. 2012. № 6. С. 93–96.

19. *Лисичкин В. А., Шелепин, Л. А.* Третья мировая (информационно-психологическая) война. М.: Ин-т социально-политических исследований АСН, 2000. 304 с.

20. *Макашова В. В.* Дезинформация как оружие массового поражения: проблема диагностики // Современный медиатекст и судебная экспертиза: междисциплинарные связи и экспертная оценка: сб. науч. работ по итогам Междунар. науч.-практ. конф. «Современный медиатекст и судебная экспертиза: междисциплинарные связи и экспертная оценка» (г. Москва, 12–13 октября 2023 г.). М.: СОЮЗКНИГ, 2023. С. 190–204.

21. *Makurova D. A.* Media disinformation: types and characteristics // Studia Linguistica. 2021. № 30. Pp. 57–64.

22. *МакДугал Дж.* Медиаграмотность как антидот к дезинформации // СоциоДиггер. 2021. Т. 2. № 6 (11). С. 36–37.

23. *Михальченко И. А.* Информационные войны на рубеже XXI века // Безопасность информационных технологий. 1998. № 3. С. 14–15.

24. *Моногарова А. Г., Ширяева Т. А., Тихонова Е. В.* Язык вирусных фейковых новостей: корпусный подход к анализу русскоязычной дезинформации о Covid-19 // Russian Journal of Linguistics. 2023. Т. 27, № 3. С. 543–569.

25. *Невзгодина Е. Л., Парыгина Н. Н.* Гражданско-правовой механизм защиты деловой репутации в России: панорамный обзор // Lex Russica. 2018. № 1. С. 57–70. DOI: 10.17803/1729-5920.2018.134.1.057-070.

26. *Некрасов Г. А., Романова, И. И.* Разработка поискового робота для обнаружения веб-контента с фейковыми новостями // Инновационные, информационные и коммуникационные технологии. 2017. № 1. С. 128–130.

27. *Панарин И. Н.* Технология информационной войны. М.: КСП+, 2003. 320 с.

28. *Панарин И. Н.* СМИ, пропаганда и информационные войны. М.: Поколение, 2012. 260 с.

29. *Полончук Р. А., Ганиев Т. А.* Взгляды китайских военных специалистов на сущность и содержание информационной войны в современных условиях // Военная мысль. 2020. № 3. С. 133–139.

30. *Пирютко И. Д.* Социальные сети как инструмент для дезинформации и управления дезинформацией // Достижения науки и технологий-ДНиТ-11-2023: сб. науч. ст. по материалам II Всерос. науч. конференции (г. Красноярск, 27–28 февраля 2023 г.). Красноярск: Общественное учреждение «Красноярский краевой Дом науки и техники Российского союза научных и инженерных общественных объединений», 2023. Вып. 7. С. 327–331.

31. *Прокофьев В. Ф.* Тайное оружие информационной войны: атака на подсознание. М.: СИНТЕГ, 2003. 408 с.

32. *Проскурин О. Н.* Информационная совместимость — обязательное условие реализации концепции «сетецентрических войн» // Известия Российской академии ракетных и артиллерийских наук. 2011. № 4 (70). С. 45–51.

33. *Царик В. С.* Противодействие «российской информационной угрозе» в политике Европейского союза после украинского кризиса: дискурсивный и институциональный аспекты // Среднерусский вестник общественных наук. 2020. Т. 15, № 5. С. 107–123.

34. *Akoev M., Moskaleva, O., Pislyakov, V.* Confidence and RISC: How Russian papers indexed in the national citation database Russian Index of Science Citation (RISC) characterize universities and research institutes // STI 2018 Conference Proceedings. 2018. Pp. 1328–1338. DOI: 10.1887/65344.

35. *Bernstein J.* Bad news: Selling the story of disinformation // Harper's Magazine. URL: https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/.

36. *Carlson C. R.* On Shaky Ground: Reconsidering the Justifications for First Amendment Protection of Hate Speech // Communication Law and Policy. 2023. № 28 (2). Pp. 124–151. DOI: 10.1080/10811680.2023.2193571.

37. *Cigar N.* The Russian Military's Biological Warfare Disinformation Campaign and the Russo-Ukrainian War // The Journal of Slavic Military Studies. 2023. № 36(4). Pp. 361–409. DOI: 10.1080/13518046.2023.2305511.

38. *Cole M.* The Relevant EU Legal Framework for Online Content Dissemination // Cross-border Dissemination of Online Content. 2020. Pp. 53–168. DOI: 10.5771/9783748906438-53.

39. *Custers B.* New digital rights: Imagining additional fundamental rights for the digital era // Computer Law & Security Review. 2022. Vol. 44. Pp. 1–13. DOI: 10.1016/j.clsr.2021.105636.

40. *Demaske C.* Modern power and the First Amendment: Reassessing hate speech // Communication Law and Policy. 2004. Vol. 9 (3). Pp. 273–316. DOI: 10.1207/s15326926clp0903_1.

41. *Gamito M. C.* The European Media Freedom Act (EMFA) as meta-regulation // Computer Law & Security Review. 2023. Vol. 48. Pp. 1–20. DOI: 10.1016/j.clsr.2023.105799.

42. *Helberger N.* FutureNewsCorp, or how the AI Act changed the future of news // Computer Law & Security Review. 2024. Vol. 52. Pp. 1–20. DOI: 10.1016/j.clsr.2023.105915.

43. *Herbosch M.* Fraud by generative AI chatbots: On the thin line between deception and negligence // Computer Law & Security Review. 2024. Vol. 52. Pp. 1–31. DOI: 10.1016/j.clsr.2024.105941.

44. *Hutchings S.C.* Uncovering the uncoverers: identity, performativity and representation in counter-disinformation discourse // Cultural Studies. 2024. Vol. 39 (1). Pp. 1–28. DOI: 10.1080/09502386.2024.2384942.

45. *Juhász K.* European Union defensive democracy's responses to disinformation // Journal of Contemporary European Studies. 2024. Vol. 32 (4), Pp. 1075–1094. DOI: 10.1080/14782804.2024.2317275.

46. *Kalsnes B.* Fake News // Oxford Research Encyclopedia of Communication, 2018. Pp. 1–24. DOI: 10.1093/crefore/9780190228613.013.809.

47. *Karalis M.* Fake leads, defamation and destabilization: How online disinformation continues to impact Russia's invasion of Ukraine // Intelligence and National Security. 2024. № 39. Pp. 1–10. DOI: 10.1080/02684527.2024.2329418.

48. *Limonier K., Laruelle M.* Russia's African Toolkit: Digital Influence and Entrepreneurs of Influence // Orbis. 2021. Vol. 65 (3). Pp. 403–419. DOI: 10.1016/j.orbis.2021.06.005.

49. *Mantelero A., Esposito M. S.* An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems // Computer Law & Security Review. 2021. Vol. 41. Pp. 1–31. DOI: 10.1016/j.clsr.2021.105561.

50. *Marsden C., Meyer T., Brown I.* Platform values and democratic elections: How can the law regulate digital disinformation? // Computer Law & Security. 2020. Vol. 36. Pp. 1–18. DOI: 10.1016/j.clsr.2019.105373.

51. *Moyakine E., Tabachnik A.* Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology // Computer Law & Security Review. 2021. Vol. 40. Pp. 1–13. DOI: 10.1016/j.clsr.2020.105512.

52. *Nave E., Lane L.* Countering online hate speech: How does human rights due diligence impact terms of service? // Computer Law & Security Review. 2023. Vol. 51. Pp. 1–18. DOI: 10.1016/j.clsr.2023.105884.

53. *Park T. J., Rohatgi A.* Balancing the platform responsibility paradox: A case for amplification regulation to mitigate the spread of harmful but legal content online // Computer Law & Security Review. 2024. Vol. 52. DOI: 10.1016/j.clsr.2024.105960.

54. *Peukert A.* The regulation of disinformation: a critical appraisal // Journal of Media Law. 2024. Vol. 16 (1). Pp. 1–7. DOI: 10.1080/17577632.2024.2362485.

55. *Quarmal S. B., Islam M. A.* Data journalism in combating misinformation during Bangladesh national election 2018 // Russian Journal of Media Studies. 2020. № 8. Pp. 27–48. DOI: 10.17223/26188422/8/3.

56. *Rojszczak M*. Online content filtering in EU law – A coherent framework or jigsaw puzzle? // Computer Law & Security Review. 2022. Vol. 47. Pp. 1–18. DOI: 10.1016/j.clsr.2022.105739.

57. *Shahbazi M., Bunker D.* Social media trust: Fighting misinformation in the time of crisis // International Journal of Information Management. 2024. Vol. 77. Pp. 1–13. DOI: 10.1016/j.ijinfomgt.2024.102780.

58. *Silva M., Giovanini L., Fernandes J., Oliveira D., Silva C. S*. What Makes Disinformation Ads Engaging? A Case Study of Facebook Ads from the Russian Active Measures Campaign // Journal of Interactive Advertising. 2023. № 23. Pp. 221–240. DOI: 10.1080/15252019.2023.2173991.

59. *Sokolova A. A., Kalenchuk T. V., Sokolova S. N*. NEO-terrorism in the information society as a basic element of hybrid warfare strategy // Bulletin of Polessky State University. Series in Social Sciences and Humanities. 2021. № 2. Pp. 21–27.

60. *Stewart B., Jackson S., Ishiyama J., Marshall M. C.* Explaining Russian state-sponsored disinformation campaigns: who is targeted and why? // East European Politics. 2024. Vol. 40(3), Pp. 431–446. DOI: 10.1080/21599165.2024.2302597.

61. *Sun H.* Regulating Algorithmic Disinformation // The Columbia Journal of Law & The Arts. 2023. Vol. 46 (4). Pp. 367–417. DOI: 10.52214/jla.v46i3.11237.

62. *Szegda J., Tylec G.* The level of legal security of citizen journalists and social media users participating in public debate. Standards developed in the jurisprudence of the European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ) // Computer Law & Security Review. 2022. Vol. 47. Pp. 1–15. DOI: 10.1016/j.clsr.2022.105740.

63. *Tan C.* The curious case of regulating false news on Google // Computer Law & Security Review. 2022. Vol. 46. Pp. 1–14. DOI: 10.1016/j.clsr.2022.105738.

64. *Thornton R., Miron M.* Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom // Journal of Cyber Policy. 2019. Vol. 4 (2). Pp. 257–274. DOI: 10.1080/23738871.2019.1640757.

65. *Tolz V., Hutchings S.* Truth with a Z: disinformation, war in Ukraine, and Russia's contradictory discourse of imperial identity // Post-Soviet Affairs. 2023. Vol. 39 (5). Pp. 347–365. DOI: 10.1080/1060586X.2023.2202581.

66. *Urusova N. A*. The global phenomenon of fake news: Online disinformation during crisis // Communications. Media. Design. 2023. Vol. 8. № 4. Pp. 18–31.

67. *van Bekkum M., Borgesius F. Z.* Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? // Computer Law & Security Review. 2023. Vol. 48. 105770. Pp. 1–12 DOI: 10.1016/j.clsr.2022.105770.

68. *van de Weijer S., Leukfeldt R., Moneva A.* Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands // Computers & Security.

2024. Vol. 139. Pp. 1–11 DOI: 10.1016/j.cose.2023.103693.

69. *Xiao B.* Making the private public: Regulating content moderation under Chinese law // Computer Law & Security Review. 2023. № 51. Pp. 1–16. DOI: 10.1016/j.clsr.2023.105893.

70. *Khakimova A., Zolotarev O., Sharma B., Agrawal S., Jain S.* Methods for Assessing the Psychological Tension of Social Network Users during the Coronavirus Pandemic and Its Uses for Predictive Analysis // Sustainability. 2023. Vol. 15. Issue 13. Pp. 1–19. 10008. DOI: 10.3390/su151310008.

References

1. Ableev S. R., Kuz'minskaya S. I. *Mediynye mistifikatsii massovogo soznaniya kak psikhologicheskoe orudie informatsionnoy voyny* [Media Mystifications of Mass Consciousness as a Psychological Tool of Information Warfare]. *Psikhologiya i pedagogika sluzhebnoy deyatel'nosti* – Psychology and Pedagogics in Official Activity. 2023. Issue 2. Pp. 12–15. (In Russ.).

2. Alekseev S. S. *Obshchaya teoriya prava* [General Theory of Law]: in 2 vols. Vol. 1. Moscow, 1981. 360 p. (In Russ.).

3. Aljaduoi A. J. h. *Tendentsii razvitiya metodov vedeniya sovremennoy informatsionnoy voyny* [Trends in the Development of Methods of Modern Information Warfare]. *Obshchestvoznanie i sotsial'naya psikhologiya* – Social Science and Social Psychology. 2022. Issue 11 (41). Pp. 305–308. (In Russ.).

4. Andreev S. V., Bertovskiy L. V., Obraztsov V. A. *Ispol'zovanie dezinformatsii pri vyyavlenii i rassledovanii prestupleniy* [The Use of Disinformation in Detecting and Investigating Crimes]. *Rossiyskiy sledovatel'* – Russian Investigator. 2005. Issue 8. Pp. 2–5. (In Russ.).

5. Aulov V. K. *Pravovoy instrumentariy informatsionnoy voyny: bazovye tsennosti voennoy organizatsii gosudarstva i yuridicheskie tekhnologii ikh razrusheniya* [Legal Instruments of Information Warfare: Core Values of the Military Organization of the State and Legal Technologies for Their Destruction]. *Voennoe pravo* – Military Law. 2022. Issue 3 (73). Pp. 44–53. (In Russ.).

6. Bakhteev D. V. *Iskusstvennyy intellekt v kriminalistike: sostoyanie i perspektivy ispol'zovaniya* [Artificial Intelligence in Forensics: Status and Prospects of Using]. *Rossiyskoe pravo: obrazovanie, praktika, nauka* – Russian Law: Education, Practice, Researches. 2018. Issue 2 (104). Pp. 43–49. (In Russ.).

7. Vas'kovskiy E. V. *Tsivilisticheskaya metodologiya: uchenie o tolkovanii i primenenii grazhdanskikh zakonov* [Civil-Law-Science Methodology: Doctrine of Interpretation and Application of Civil Laws]. Moscow, 2002. 83 p. (In Russ.).

8. Vinogradov V. A., Kuznetsova D. V. *Zarubezhnyy opyt pravovogo regulirovaniya tekhnologii «dipfeyk»* [Foreign Experience in Legal Regulation of 'Deepfake' Technology]. *Pravo. Zhurnal Vysshey shkoly ekonomiki.* – Law. Journal of the Higher School of Economics. 2024. Vol. 17 (2). Pp. 215–240. DOI: 10.17323/2072-8166.2024.2.215.240. (In Russ.).

9. Voronova O. E. *Sovremennye informatsionnye voyny: tipologiya i tekhnologii* [Modern Information Wars: Typology and Technologies]. Ryazan, 2018. 188 p. (In Russ.).

10. Gir'ko S. I. *Problemy ugolovno-protsessual'nogo statusa ugolovno-ispolnitel'noy sistemy Rossiyskoy Federatsii: mify i real'nost'* [Problems of the Criminal Procedural Status of the Penal System of the Russian Federation: Myths and Reality]. *Vedomosti ugolovno-ispolnitel'noy sistemy* – Bulletin of the Penal System. 2020. Issue 7 (218). Pp. 13–21. (In Russ.).

11. Golovanova N. A. *Novye formy onlayn-prestupnosti za rubezhom* [New Forms of Online Crime Abroad]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* – Journal of Foreign Legislation and Comparative Law. 2019. Issue 3. Pp. 42–57. DOI: 10.12737/jflcl.2019.3.4. (In Russ.).

12. Zhuk D. A., Zhuk D. V., Tret'yakov A. O. *Metody opredeleniya poddel'nykh novostey v sotsial'nykh setyakh s ispol'zovaniem mashinnogo obucheniya* [Methods for Detecting Fake News in Social Networks Using Machine Learning]. *Informatsionnye resursy Rossii* – Information Resources of Russia. 2018. Issue 3. Pp. 29–32. (In Russ.).

13. Issers O. S. *Mediafeyki: mezhdu pravdoy i mistifikatsiey* [Media Fakes: Between Truth and Mystification]. *Kommunikativnye issledovaniya* – Communication Studies. 2014. Issue 2. Pp. 112–123. (In Russ.).

14. Kalinina E. V. *Dilemmy pravovogo regulirovaniya bezopasnosti informatsionnogo prostranstva i kommunikativnye mediatekhnologii kak instrumenty vedeniya informatsionnoy voyny* [Dilemmas of Legal Regulation of Information Space Security and Communicative Media Technologies as Tools of Information Warfare]. *Voenno-yuridicheskiy zhurnal* – Military-Law Journal. 2023. Issue 1. Pp. 19–23. DOI: 10.18572/2070-2108-2023-1-19-23. (In Russ.).

15. Karayani A. G. *Teoriya i praktika psikhologicheskoy voyny. Organizatsiya i provedenie informatsionnykh operatsiy* [Theory and Practice of Psychological Warfare. Organization and Conduct of Information Operations]. Available at: http://psyfactor.org/lib/psywar30.htm. (In Russ.).

16. Kozlov V. V., Vlasov N. A. *Informatsionnye voyny: istoriya i sovremennost'* [Information Wars: History and Modernity]. *Chelovecheskiy faktor. Sotsial'nyy psikholog* – Human Factor. Social Psychologist. 2017. Issue 1 (33). Pp. 98–111. (In Russ.).

17. Krasovskaya N. R., Gulyaev A. A. *Informatsionnye voyny na territorii byvshego SSSR* [Information Wars in the Territory of the Former USSR]. *Gumanitarnye problemy voennogo dela* – Humanitarian Problems of Military Affairs. 2019. Issue 2 (19). Pp. 51–58. (In Russ.).

18. Kunakova L. N. *Informatsionnaya voyna kak ob''ekt nauchnogo analiza (ponyatie i osnovnye kharakteristiki informatsionnoy voyny)* [Information War as an

Object of Scientific Analysis (The Concept and Main Characteristics of Information War)]. *Al'manakh sovremennoy nauki i obrazovaniya* – Almanac of Modern Science and Education. 2012. Issue 6. Pp. 93–96. (In Russ.).

19. Lisichkin V. A., Shelepin L. A. *Tret'ya mirovaya (informatsionno-psikhologicheskaya) voyna* [The Third World (Informational-Psychological) War]. Moscow, 2000. 304 p. (In Russ.).

20. Makashova V. V. *Dezinformatsiya kak oruzhie massovogo porazheniya: problema diagnostiki* [Disinformation as a Weapon of Mass Destruction: Diagnostic Issues]. *Sovremennyy mediatekst i sudebnaya ekspertiza: mezhdistsiplinarnye svyazi i ekspertnaya otsenka* [Modern Mediatext and Forensic Examination: Interdisciplinary Relations and Expert Assessment]: a collection of scientific works based on the International Scientific and Practical Conference (Moscow, October 12–13, 2023). Moscow, 2023. Pp. 190–204. (In Russ.).

21. Makurova D. A. Media Disinformation: Types and Characteristics. *Studia Linguistica*. 2021. Issue 30. Pp. 57–64. (In Eng.).

22. McDougall J. *Mediagramotnost' kak antidot k dezinformatsii* [Media Literacy as an Antidote to Disinformation]. *SotsioDigger* – SocioDigger. 2021. Vol. 2. Issue 6 (11). Pp. 36–37. (In Russ.).

23. Mikhal'chenko I. A. *Informatsionnye voyny na rubezhe XXI veka* [Information Wars at the Turn of the 21st Century]. *Bezopasnost' informatsionnykh tekhnologiy* – IT Security (Russia). 1998. Issue 3. Pp. 14–15. (In Russ.).

24. Monogarova A. G., Shiryaeva T. A., Tikhonova E. V. *Yazyk virusnykh feykovykh novostey: korpusnyy podkhod k analizu russkoyazychnoy dezinformatsii o Covid-19* [The Language of Viral Fake News: Corpus-Based Approach to Analyzing Russian-Language Disinformation about Covid-19]. *Russian Journal of Linguistics*. 2023. Vol. 27. Issue 3. Pp. 543–569. (In Russ.).

25. Nevzgodina E. L., Parygina N. N. *Grazhdansko-pravovoy mekhanizm zashchity delovoy reputatsii v Rossii: panoramnyy obzor* [Civil Law Mechanism of Protection of Business Reputation in Russia: A Comprehensive Review]. *Lex Russica*. 2018. Issue 1. Pp. 57–70. DOI: 10.17803/1729-5920.2018.134.1.057-070. (In Russ.).

26. Nekrasov G. A., Romanova I. I. *Razrabotka poiskovogo robota dlya obnaruzheniya veb-kontenta s feykovymi novostyami* [Development of a Search Robot for Detecting Web Content with Fake News]. *Innovatsionnye, informatsionnye i kommunikatsionnye tekhnologii* – Innovative, Information, and Communication Technologies. 2017. Issue 1. Pp. 128–130. (In Russ.).

27. Panarin I. N. *Tekhnologiya informatsionnoy voyny* [The Technology of Information Warfare]. Moscow, 2003. 320 p. (In Russ.).

28. Panarin I. N. *SMI, propaganda i informatsionnye voyny* [Mass Media, Propaganda, and Information Wars]. Moscow, 2012. 260 p. (In Russ.).

29. Polonchuk R. A., Ganiev T. A. *Vzglyady kitayskikh voennykh spetsialistov na sushchnost' i soderzhanie informatsionnoy voyny v sovremennykh usloviyakh* [Views of Chinese Military Specialists on the Essence and Content of Information Warfare in Modern Conditions]. *Voennaya mysl'* – Military Thought. 2020. Issue 3. Pp. 133–139. (In Russ.).

30. Piryutko I. D. *Sotsial'nye seti kak instrument dlya dezinformatsii i upravleniya dezinformatsiey* [Social Networks as a Tool for Disinformation and for Managing Disinformation]. *Dostizheniya nauki i tekhnologiy* [Advances in Science and Technology]: a collection of scientific articles based on the II All-Russian Scientific Conference (Krasnoyarsk, 2023, February 27-28). Krasnoyarsk, 2023. Issue 7. Pp. 327–331. (In Russ.).

31. Prokof'ev V. F. *Taynoe oruzhie informatsionnoy voyny: ataka na podsoznanie* [A Secret Weapon of Information Warfare: Attack on the Subconscious]. Moscow, 2003. 408 p. (In Russ.).

32. Proskurin O. N. *Informatsionnaya sovmestimost' — obyazatel'noe uslovie realizatsii kontseptsii «setetsentricheskikh voyn»* [Information Compatibility as a Mandatory Condition for Implementing the Concept of 'Network-Centric Wars']. *Izvestiya Rossiyskoy akademii raketnykh i artilleriyskikh nauk* – Proceedings of the Russian Academy of Rocket and Artillery Sciences. 2011. Issue 4 (70). Pp. 45–51. (In Russ.).

33. Tsarik V. S. *Protivodeystvie «rossiyskoy informatsionnoy ugroze» v politike Evropeyskogo soyuza posle ukrainskogo krizisa: diskursivnyy i institutsional'nyy aspekty* [Countering the 'Russian Information Threat' in the European Union Policy after the Ukrainian Crisis: Discursive and Institutional Aspects]. *Srednerusskiy vestnik obshchestvennykh nauk* – Central Russian Journal of Social Sciences. 2020. Vol. 15. Issue 5. Pp. 107–123. (In Russ.).

34. Akoev M., Moskaleva O., Pislyakov V. Confidence and RISC: How Russian Papers Indexed in the National Citation Database Russian Index of Science Citation (RISC) Characterize Universities and Research Institutes. *STI 2018 Conference Proceedings*. 2018. Pp. 1328–1338. DOI: 10.1887/65344. (In Eng.)

35. Bernstein J. Bad News: Selling the Story of Disinformation. *Harper's Magazine.* Available at: https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/. (In Eng.).

36. Carlson C. R. On Shaky Ground: Reconsidering the Justifications for First Amendment Protection of Hate Speech. *Communication Law and Policy*. 2023. Vol. 28 (2). Pp. 124–151. DOI: 10.1080/10811680.2023.2193571. (In Eng.).

37. Cigar N. The Russian Military's Biological Warfare Disinformation Campaign and the Russo-Ukrainian War. *The Journal of Slavic Military Studies*. 2023. Vol. 36 (4). Pp. 361–409. DOI: 10.1080/13518046.2023.2305511. (In Eng.).

38. Cole M. The Relevant EU Legal Framework for Online Content Dissemination. *Cross-Border Dissemination of Online Content*. 2020. Pp. 53–168. DOI: 10.5771/9783748906438-53. (In Eng.).

39. Custers B. New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era. *Computer Law & Security Review*. 2022. Vol. 44. Pp. 1–13. DOI: 10.1016/j.clsr.2021.105636. (In Eng.).

40. Demaske C. Modern Power and the First Amendment: Reassessing Hate Speech. *Communication Law and Policy*. 2004. Vol. 9 (3). Pp. 273–316. DOI: 10.1207/s15326926clp0903_1. (In Eng.).

41. Gamito M. C. The European Media Freedom Act (EMFA) as Meta-Regulation. *Computer Law & Security Review*. 2023. Vol. 48. Pp. 1–20. DOI: 10.1016/j.clsr.2023.105799. (In Eng.).

42. Helberger N. FutureNewsCorp, or How the AI Act Changed the Future of News. *Computer Law & Security Review*. 2024. Vol. 52. Pp. 1–20. DOI: 10.1016/j.clsr.2023.105915. (In Eng.).

43. Herbosch M. Fraud by Generative AI Chatbots: On the Thin Line Between Deception and Negligence. *Computer Law & Security Review*. 2024. Vol. 52. Pp. 1–31. DOI: 10.1016/j.clsr.2024.105941. (In Eng.).

44. Hutchings S. C. Uncovering the Uncoverers: Identity, Performativity and Representation in Counter-Disinformation Discourse. *Cultural Studies*. 2024. Vol. 39(1). Pp. 1–28. DOI: 10.1080/09502386.2024.2384942. (In Eng.).

45. Juhász K. *European* Union Defensive Democracy's Responses to Disinformation. *Journal of Contemporary European Studies*. 2024. Vol. 32 (4). Pp. 1075–1094. DOI: 10.1080/14782804.2024.2317275. (In Eng.).

46. Kalsnes B. Fake News. *Oxford Research Encyclopedia of Communication*. 2018. Pp. 1–24. DOI: 10.1093/acrefore/9780190228613.013.809. (In Eng.).

47. Karalis M. Fake Leads, Defamation and Destabilization: How Online Disinformation Continues to Impact Russia's Invasion of Ukraine. *Intelligence and National Security*. 2024. Issue 39. Pp. 1–10. DOI: 10.1080/02684527.2024.2329418. (In Eng.).

48. Limonier K., Laruelle M. Russia's African Toolkit: Digital Influence and Entrepreneurs of Influence. *Orbis*. 2021. Vol. 65 (3). Pp. 403–419. DOI: 10.1016/j.orbis.2021.06.005. (In Eng.).

49. Mantelero A., Esposito M. S. An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems. *Computer Law & Security Review*. 2021. Vol. 41. Pp. 1–31. DOI: 10.1016/j.clsr.2021.105561. (In Eng.).

50. Marsden C., Meyer T., Brown I. Platform Values and Democratic Elections: How Can the Law Regulate Digital Disinformation? *Computer Law & Security*. 2020. Vol. 36. Pp. 1–18. DOI: 10.1016/j.clsr.2019.105373. (In Eng.).

51. Moyakine E., Tabachnik A. Struggling to Strike the Right Balance Between Interests at Stake: The 'Yarovaya', 'Fake News' and 'Disrespect' Laws as Examples of Ill-Conceived Legislation in the Age of Modern Technology. *Computer Law & Security Review*. 2021. Vol. 40. Pp. 1–13. DOI: 10.1016/j.clsr.2020.105512. (In Eng.).

52. Nave E., Lane L. Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service? *Computer Law & Security Review*. 2023. Vol. 51. Pp. 1–18. DOI: 10.1016/j.clsr.2023.105884. (In Eng.).

53. Park T. J., Rohatgi A. Balancing the Platform Responsibility Paradox: A Case for Amplification Regulation to Mitigate the Spread of Harmful but Legal Content Online. *Computer Law & Security Review*. 2024. Vol. 52. DOI: 10.1016/j.clsr.2024.105960. (In Eng.).

54. Peukert A. The Regulation of Disinformation: A Critical Appraisal. *Journal of Media Law*. 2024. Vol. 16 (1). Pp. 1–7. DOI: 10.1080/17577632.2024.2362485. (In Eng.).

55. Quarmal S. B., Islam M.A. Data Journalism in Combating Misinformation During Bangladesh National Election 2018. *Russian Journal of Media Studies*. 2020. Issue 8. Pp. 27–48. DOI: 10.17223/26188422/8/3. (In Eng.).

56. Rojszczak M. Online Content Filtering in EU Law – A Coherent Framework or Jigsaw Puzzle? *Computer Law & Security Review*. 2022. Vol. 47. Pp. 1–18. DOI: 10.1016/j.clsr.2022.105739. (In Eng.).

57. Shahbazi M., Bunker D. Social Media Trust: Fighting Misinformation in the Time of Crisis. *International Journal of Information Management*. 2024. Vol. 77. Pp. 1–13. DOI: 10.1016/j.ijinfomgt.2024.102780. (In Eng.).

58. Silva M., Giovanini L., Fernandes J., Oliveira D., Silva C. S. What Makes Disinformation Ads Engaging? A Case Study of Facebook Ads from the Russian Active Measures Campaign. *Journal of Interactive Advertising*. 2023. Issue 23. Pp. 221–240. DOI: 10.1080/15252019.2023.2173991. (In Eng.).

59. Sokolova A. A., Kalenchuk T. V., Sokolova S. N. NEO-Terrorism in the Information Society as a Basic Element of Hybrid Warfare Strategy. *Bulletin of Polessky State University. Series in Social Sciences and Humanities*. 2021. Issue 2. Pp. 21–27. (In Eng.).

60. Stewart B., Jackson S., Ishiyama J., Marshall M. C. Explaining Russian State-Sponsored Disinformation Campaigns: Who Is Targeted and Why? *East European Politics*. 2024. Vol. 40 (3). Pp. 431–446. DOI: 10.1080/21599165.2024.2302597. (In Eng.).

61. Sun H. Regulating Algorithmic Disinformation. *The Columbia Journal of Law & The Arts*. 2023. Vol. 46 (4). Pp. 367–417. DOI: 10.52214/jla.v46i3.11237. (In Eng.).

62. Szegda J., Tylec G. The Level of Legal Security of Citizen Journalists and Social Media Users Participating in Public Debate. Standards Developed in the Jurisprudence of the European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ). *Computer Law & Security Review*. 2022. Vol. 47. Pp. 1–15. DOI: 10.1016/j.clsr.2022.105740. (In Eng.).

63. Tan C. The Curious Case of Regulating False News on Google. *Computer Law & Security Review*. 2022. Vol. 46. Pp. 1–14. DOI: 10.1016/j.clsr.2022.105738. (In Eng.).

64. Thornton R., Miron M. Deterring Russian Cyber Warfare: the Practical, Legal and Ethical Constraints Faced by the United Kingdom. *Journal of Cyber Policy*. 2019. Vol. 4 (2). Pp. 257–274. DOI: 10.1080/23738871.2019.1640757. (In Eng.).

65. Tolz V., Hutchings S. Truth with a Z: Disinformation, War in Ukraine, and Russia's Contradictory Discourse of Imperial Identity. *Post-Soviet Affairs*. 2023. Vol. 39 (5). Pp. 347–365. DOI: 10.1080/1060586X.2023.2202581. (In Eng.).

66. Urusova N. A. The Global Phenomenon of Fake News: Online Disinformation During Crisis. *Communications. Media. Design*. 2023. Vol. 8. Issue 4. Pp. 18–31. (In Eng.).

67. van Bekkum M., Borgesius F. Z. Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception? *Computer Law & Security Review*. 2023. Vol. 48. Pp. 1–12. DOI: 10.1016/j.clsr.2022.105770. (In Eng.).

68. van de Weijer S., Leukfeldt R., Moneva A. Cybercrime During the COVID-19 Pandemic: Prevalence, Nature and Impact of Cybercrime for Citizens and SME Owners in the Netherlands. *Computers & Security*. 2024. Vol. 139. Pp. 1–11. DOI: 10.1016/j.cose.2023.103693. (In Eng.).

69. Xiao B. Making the Private Public: Regulating Content Moderation under Chinese Law. *Computer Law & Security Review*. 2023. Issue 51. Pp. 1–16. DOI: 10.1016/j.clsr.2023.105893. (In Eng.).

70. Khakimova A., Zolotarev O., Sharma B., Agrawal S., Jain S. Methods for Assessing the Psychological Tension of Social Network Users During the Coronavirus Pandemic and Its Uses for Predictive Analysis. *Sustainability*. 2023. Vol. 15. Issue 13. Pp. 1–19. DOI: 10.3390/su151310008. (In Eng.).

Информация об авторе:

Е. И. Дискин
Кандидат юридических наук, ст. научный сотрудник Международной лаборатории цифровой трансформации в государственном управлении Национальный исследовательский университет «Высшая школа экономики»
101000, Россия, г. Москва, ул. Мясницкая, 20

ORCID: 0000-0001-9259-9820
ResearcherID: IZQ-4502-2023

Статьи в БД «Scopus» / «Web of Science»:
DOI: 10.31857/S1026945224020167

About the author:

E. I. Diskin
National Research University 'Higher School of Economics' (HSE University)
20, Myasnitskaya st., Moscow 101000, Russia

ORCID: 0000-0001-9259-9820
ResearcherID: IZQ-4502-2023

Articles in Scopus / Web of Science:
DOI: 10.31857/S1026945224020167