Научная статья
УДК 323/327
EDN: GFNYOA

ГИБРИДНО-ИНФОРМАЦИОННАЯ ВОЙНА ПРОТИВ РОССИИ (на примере теракта в «Крокус Сити Холл»)

Александр Александрович СМЕЛОВ

Северо-Западный институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ
Санкт-Петербург, Россия
mailfordayzsub@gmail.com

Аннотация. Актуальность исследования определяется тем, что террористический акт, произошедший в «Крокус Сити Холл» стал информационным поводом для проведения деструктивных акций в отношении российского руководства со стороны стран Запада. Целью работы является изучение особенностей гибридно-информационной войны стран Запада против Российской Федерации. В работе используется дискурс-анализ и контент-анализ при интерпретации публикаций СМИ, а также высказываний отдельных личностей в медиапространстве.

В исследовании отмечается, что современные стриминговые платформы и видеохостинги не уделяют достаточного внимания контролю транслируемой информации, не ограничивают к ней доступ в условиях чрезвычайных ситуаций. Искаженно трактуемое понятие свободы слова трансформируется в «свободу контроля», которой добиваются заинтересованные субъекты, распространяя конспирологические теории и злоупотребляя подменой фактов.

Большинство отечественных мониторинговых систем противодействия вредоносному контенту не способны разрешить проблему, поскольку не имеют возможности блокировки информации в реальном режиме времени. Эффективными инструментами противодействия деструктивной информации могут стать ИС «Окулус» и «Вепрь», внедряемые Роскомнадзором.

В заключении отмечается, что, кроме внедрения современных мониторинговых систем, необходимо активное освещение официальными представителями крупных событий, вызывающих общественный резонанс.

Ключевые слова: «Крокус Сити Холл», СМИ, гибридно-информационная война, иноагент, теракт, национальная безопасность, цифровизация, Роскомнадзор.

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: *Смелов А.А.* Гибридно-информационная война против России (на примере теракта в «Крокус Сити Холл») // Вестник Поволжского института управления. 2025. Т. 25, № 3. С. 39–47. EDN: GFNYOA

Original article

HYBRID-INFORMATION WARFARE AGAINST RUSSIA (on the Example of the Terrorist Attack at Crocus City Hall)

Alexander A. SMELOV

North-West Institute of Management of the Russian Presidential Academy of National Economy and Public Administration
Saint Petersburg, Russia
mailfordayzsub@gmail.com

Abstract. The relevance of the study is determined by the fact that the terrorist act that took place in Crocus City Hall became an informational reason for destructive actions against the Russian leadership by Western countries. The purpose of the work is to study the features of the hybrid information war of Western countries against the Russian Federation. The work uses the method of discourse analysis in interpreting media publications, as well as statements of individuals in the media space.

The study notes that modern streaming platforms and video hosting sites do not pay sufficient attention to the control of broadcast information and do not restrict access to it in emergency situations. The misinterpreted concept of freedom of speech is transformed into "freedom of control", which is achieved by interested parties by spreading conspiracy theories and abusing the substitution of facts.

Most domestic monitoring systems for countering malicious content are unable to solve the problem because they do not have the ability to block information in real time. The Oculus and Vepr IP systems implemented by Roskomnadzor can become effective tools for countering destructive information.

The conclusion, it is noted that in addition to the introduction of modern monitoring systems, it is necessary for official representatives to actively cover major events that cause public outcry.

Keywords: Crocus City Hall, mass media, hybrid information warfare, foreign agent, terrorist attack, national security, digitalization, Roskomnadzor.

Conflicts of interest. The author declares no conflicts of interest.

For citing: *Smelov A.A.* Hybrid-Information Warfare Against Russia (on the Example of the Terrorist Attack at Crocus City Hall) // The Bulletin of the Volga Region Institute of Administration. 2025. Vol. 25, № 3. P. 39–47. EDN: GFNYOA

Введение. Вопросы гибридно-информационного противоборства в последние годы занимают одно из важнейших мест в современной политической науке и юридических исследованиях. Среди российских авторов актуальными проблемами в данной сфере занимаются Д.А. Саидзода [1], Д.К. Григорян, Е.Н. Кондратенко [2], Ю.А. Головин, О.Е. Коханая [3], А.С. Брычков, Г.А. Никоноров [4] и другие ученые. Исследователи рассматривают теоретические концепции, раскрывая сущность информационных и гибридных войн и анализируя практические вопросы их проявления.

Зарубежные авторы, например С. Маллани, изучая проблематику гибридно-информационных войн, как правило, рассматривают Россию в качестве инициатора и активного субъекта информационного противоборства [5]. Однако Ф. Офер отмечает, что в России до обвинения ее в ведении гибридной войны не имели детального представления о ней и лишь сравнительно недавно начали изучать ее теоретические и практические аспекты [6, с. 81].

Термин «гибридная война» достаточно основательно закрепился в современном политическом дискурсе с начала украинского конфликта и чаще всего рассматривается в контексте противоборства коллективного Запада и России [7—9]. Согласно позиции западных стран гибридная война — это инструмент, широко используемый Российской Федерацией, что позволяет уменьшить дисбаланс вооруженных сил. В контексте более широкого определения гибридного противоборства лондонский Международный институт стратегических исследований предлагает следующее определение: «Использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических преимуществ, используемых в дипломатических действиях; масштабные и стремительные информационные, электронные и кибероперации, прикрытие и сокрытие военных и разведывательных действий в сочетании с экономическим давлением» [10, с. 10].

Согласно более емкому определению, гибридная война означает взаимодействие или сочетание обычных и нетрадиционных инструментов силы и диверсионных действий. Происходит синхронизованное смешение этих инструментов или средств, чтобы воспользоваться уязвимыми сторонами соперника и добиться синергетического воздействия.

В рамках проводимой против России информационной войны недружественные государства не стесняются выставлять в резко негатив-

ном ключе имидж Российской Федерацией, образ Президента России и основные направления современной российской политики [11, с. 9; 12, с. 52].

В западном информационном пространстве встречаются следующие элементы антироссийской риторики: Владимир Путин «воюет не только с Украиной, но и с собственным народом», предлагает условия мира подобно «предложенным гитлеровской Германией», а убийство Дарьи Дугиной, признанное Следственным комитетом России террористическим актом, характеризуют «самой смелой операцией СБУ на территории России» [13]. Подобные примеры направлены на искусственное создание героического образа Украины и ее руководства на фоне противостоящей ей «страны-агрессора». Именно поэтому против России ведется масштабная информационная война со стороны Запада, которая представляет угрозу ее национальной безопасности на фоне активного противоборства.

Теракт в «Крокус Сити Холл» как повод для информационной агрессии Запада. События в ТРК «Крокус Сити Холл», произошедшие в марте 2024 г., не остались без внимания со стороны западных или прозападных деструктивных акторов. Уже в первые часы после совершения теракта в мессенджере Telegram стали создаваться анонимные каналы с распространением угрозы нападения на российские школы с целью нагнетания паники. Подростки по всей стране начали получать в мессенджерах сообщения с предложением совершить теракт.

Помимо анонимных акторов в информационном сопровождении теракта участвовали запрещенные в России и имеющие статус иностранного агента Youtube-каналы, которые вели репортажи и прямые трансляции.

С первых минут репортажа, обладая минимальной информацией о происшедшем, так называемые «эксперты» высказывали конспирологические теории, указывая на «очевидную» причастность российских властей и спецслужб к теракту, обличая в этом «руку Кремля» Внушительный по меркам подобных трансляций охват аудитории позволял, используя различные технологии внушения и манипуляции, распространять ложные данные, способные дестабилизировать общественно-политическую обстановку.

Кроме стриминговых площадок и live-трансляций медиаканалов деструктивным потенциалом обладают популярные мессенджеры и социальные сети Telegram, Tumblr, Reddit. Вопрос использования данных цифровых платформ с целью политического воздействия также активно обсуждается в политической науке. Новостные каналы

социальных сетей эффективно транслируют релевантные события внешней и внутренней политики на широкую, преимущественно молодую, аудиторию. Так, согласно данным, приводимым А.И. Крисюком, «примерно трое из десяти мужчин США в возрасте от 18 до 29 лет (29%) говорят, что их взгляды на политический или социальный вопрос изменились за последний год благодаря социальным сетям» [14, с. 53].

Следует отметить, что с начала специальной военной операции с помощью платформы Telegram украинскому населению навязывается единый нарратив: «Россия — кровавый агрессор» [15]. В отношении же теракта в «Крокус Сити Холл» распространенным нарративом, навязываемым распространяемым западными СМИ, стал тезис о том, что американская сторона предупреждала российские спецслужбы о вероятной террористической угрозе, однако эти разведданные были проигнорированы, что привело к трагедии [16]. Однако заметим, что на фоне политической враждебности «предупреждавших» государств отличить намерения по сотрудничеству в области борьбы с международным терроризмом от попыток провокации достаточно сложно [17]. При этом некоторые медиаканалы и стриминговые площадки нередко предоставляют коммуникативную площадку представителям террористических организаций — например, Русскому добровольческому корпусу (террористическая организация, запрещенная на территории России), а также некоторым украинским политтехнологам, что обусловливает необходимость дополнительного контроля над подобными ресурсами в онлайн-формате в условиях чрезвычайных ситуаций.

Инструменты противодействия вредоносному контенту. За последние годы в сфере противодействия противозаконному и вредоносному контенту можно наблюдать определенную тенденцию. Если ранее большинство ресурсов с содержанием, не соответствовавшим требованиям российского законодательства, блокировалось в судебном порядке, то в последнее время практикуется блокировка путем внесения в реестр Роскомнадзора [18]. Так, под жесткий контроль попала социальная сеть Discord и видеохостинг Youtube, подвергшийся замедлению, что вызвало неоднозначную реакцию у пользователей. Однако очевидна малая эффективность в ограничении доступа к контенту, которая проявляется в широком спектре способов обхода блокировок. Пользователи активно прибегают как к VPN-сервисам, так и к альтернативным вариантам программного обеспечения, позволяющим получать доступ к любому заблокированному элементу сети.

Если учитывать, что процедуры внесения в реестр и дальнейшей блокировки со стороны Роскомнадзора требуют достаточно длительного времени, то в условиях live-трансляций подобное вероятное ограничение доступа находится под вопросом. Ограничением контента в режиме реального времени в связи с жалобами пользователей преимущественно занимаются модераторы самих видеохостингов и стриминговых площадок, однако часто в трансляциях СМИ-иноагентов нарушения с точки зрения сервисов отсутствуют.

В связи с этим возникает проблема ограничения деятельности экстремистских структур в режиме реального времени в период чрезвычайных ситуаций, хотя колоссальные усилия направляются на блокировку контента, доступного на постоянной основе. Блокировки, инициированные Роскомнадзором, не всегда имеют весомые основания и проводятся на основании отдельных жалоб на размещенный контент, ответственность за который потенциально несут конкретные пользователи, но не платформа. Более того, преобладающая часть подобного контента публикуется вне общедоступных ресурсов (в приватных чатах, закрытых серверах и прочих, далеких от массовости виртуальных пространствах). К тому же нередко эти же блокировки становятся причиной сбоя работы интернет-платформ у добросовестных пользователей, в том числе Вооруженных сил РФ.

Помимо ограничения доступа к деструктивному контенту в режиме онлайн, должен своевременно решаться вопрос о привлечении к ответственности лиц, причастных к противоправной, противозаконной деятельности, если состав преступления усматривается соответствующими органами. Несмотря на право Роскомнадзора проводить расследования, оценки, анализ и экспертизы с задействованием соответствующих специалистов, в документах ведомства не зафиксированы случаи, при которых следует прибегать к подобным действиям [19, с. 123]. Кроме того, требуется и релевантная теоретическая основа своевременного упреждающего воздействия на представляющие угрозу материалы в сети «Интернет». Подобное воздействие должно иметь локальный характер, не нарушая стабильность общей информационной инфраструктуры.

В 2023 г. Роскомнадзор начал тестировать систему «Вепрь», предназначенную для выявления «точек информационной напряженности» в сетевых СМИ и прочих ресурсах, а в ноябре 2024 г. система мониторинга была зарегистрирована в Роспатенте [20]. При этом «Вепрь» входит в единую систему мониторинга информационного

пространства вместе с системой «Окулус», которую с января 2023 г. начали интегрировать с уже существующими мониторинговыми системами.

Главная задача ИС «Окулус» заключается в выявлении нарушений российского законодательства в изображениях и видеороликах. Подобная система распознает изображения и символы, противоправные сцены и действия, а также анализирует текст на фотоснимках и видеоматериалах. До разработки системы операторам Главного радиочастотного центра приходилось анализировать изображения и видео главным образом вручную, обрабатывая 106 изображений и 101 видео в день. «Окулус» анализирует более 200 тысяч изображений в сутки (около трех секунд на одно изображение) [21].

Общемировой практикой является применение современных информационных систем для борьбы с угрозами в Сети: в зарубежных странах такие ИС используются уже давно. Аналогичные системы существуют в Китае, Сингапуре, США и других странах. При этом рассматриваемые российские системы считаются мониторинговыми, так как «сердцем» данных систем является искусственный интеллект. Они не будут блокировать доступ к информации, а значит, не смогут ущемлять свободу граждан, являясь более прогрессивными, чем аналогичные зарубежные продукты.

Заключение. В условиях гибридного противоборства с Западом события в «Крокус Сити Холл» стали поводом информационной агрессии в российском виртуальном пространстве. Главной задачей внешних акторов информационной войны против России являлось распространение недостоверной информации и запугивания населения в период проведения специальной военной операции. С одной стороны, проявляется стремление показать слабость правоохранительных структур, их неспособность контролировать ситуацию, с другой стороны — инспирируются точки зрения о причастности к преступлению российских спецслужб. В условиях недостаточной информации от официальных источников подобные вбросы в информационное пространство, особенно в режиме онлайн, способны дестабилизировать общественно-политическую обстановку в период терактов и других крупных происшествий. В связи с этим необходимо регулярное освещение подобных событий со стороны официальных лиц в СМИ и в социальных сетях, которые пользуются наибольшей популярностью у населения, а также внедрение мониторинговых систем, способных блокировать деструктивную информацию, в том числе в режиме реального времени.

Список источников

1. *Саидзода Д.А*. Информационная война: теоретический и концептуальный анализ // Endless Light in Science. 2024. С. 69–77.

2. *Григорян Д.К., Кондратенко Е.Н*. Характерные особенности современных информационных войн политической направленности // Государственное и муниципальное управление. Ученые записки. 2024. № 2. С. 178–183. DOI: 10.22394/2079-1690-2024-1-2-178-183. EDN: CIRDUE.

3. *Головин Ю.А., Коханая О.Е.* Журналистика и процессы трансформации медиасреды в эпоху информационных войн // Знание. Понимание. Умение. 2024. № 2. С. 155–167. DOI: 10.17805/zpu.2024.2.12. EDN: YTZUYU.

4. *Брычков А.С., Никоноров Г.А*. Российское информационное пространство в эпоху «гибридной войны»: защита или нападение // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2024. № 2. С. 53–60. EDN: PGHCAH.

5. *Маллани С*. В потоке: Формы и тактики российской информационной войны в Украине и США с 2014 по 2020 г. // Cyber Defense Review. 2022. № 4. С. 193–212.

6. *Офер Ф*. «Гибридная война» понятий // Вестник МГИМО Университета. № 5 (50). 2016. С. 79–85. DOI: 10.24833/2071-8160-2016-5-50-79-85.

7. Медведев заявил о развязанной против России гибридной войне [Электронный ресурс] // Известия. URL: https://iz.ru/1512017/2023-05-12/medvedev-zaiavil-o-razvi-azannoi-protiv-rossii-gibridnoi-voine

8. Путин заявил о продолжении Западом гибридной войны против России // ТАСС. URL: https://tass.ru/politika/19578029

9. Захарова заявила о гибридной войне НАТО против России // Лента. URL: https://lenta.ru/news/2024/09/04/zaharova-zayavila-o-gibridnoy-voyne-nato-protiv-rossii/

10. *Бартош А.А*. Взаимодействие в гибридной войне // Военная мысль. 2022. № 4. С. 6–23. EDN: BUJFXU.

11. *Бартош А.А.* Информационно-психологическая война как инструмент гибридной войны // Вестник Университета мировых цивилизаций. 2024. № 3. С. 6–11. DOI: 10.24412/2587-6236-2024-344-6-11.

12. *Шамак С.А*. Средства массовой информации – основное оружие информационных войн против России // Вестник Санкт-Петербургского университета МВД России. 2022. № 2. С. 47–55. DOI: 10.35750/2071-8284-2022-2-47-55.

13. США считают, что за убийством Дугиной стоит Украина // NY Times. URL: https://www.nytimes.com/2022/10/05/us/politics/ukraine-russia-dugina-assassination.html

14. *Крисюк А.И.* За пределами мейнстрима: возможности Tumblr, Reddit и других нишевых цифровых платформ для политической мобилизации граждан // Общество: политика, экономика, право. 2025. № 2. С. 52–60. DOI: 10.24158/pep.2025.2.6. EDN: QLXXZC.

15. *Черномор А.Д.* Участие Роскомнадзора в конституционно-правовом механизме обеспечения правопорядка // Академическая мысль. 2023. № 1. С. 121–124. EDN: ALVXFQ.

16. США сообщали России о возможном теракте в Крокус Сити Холле // The Washington Post. URL: https://www.washingtonpost.com/national-security/2024/04/02/us-warning-russia-isis-crocus/

17. Провал российских служб безопасности? Кремль заявляет, что ни одно государство не защищено от терроризма // Reuters. URL: https://www.reuters.com/world/europe/russian-security-failure-kremlin-says-no-country-is-immune-terrorism-2024-03-25/

18. *Чудинов А.П., Сегал Н.А*. Метафорический образ России в украинских каналах Telegram 2022–2024 гг. // Политическая лингвистика. 2024. № 3. С. 42–48. EDN: BWMBIN.

19. *Джуров А.А., Сердечный М.С., Черкесова Л.В., Ревякина Е.А.* Экспертная система регулирования доступа к деструктивным интернет-ресурсам // Инженерный вестник Дона. 2024. № 9. С. 1–22. EDN: POMUIK.

20. РКН зарегистрировал в Роспатенте систему мониторинга интернета «Вепрь», проект написан на Python 3.7 и Go 1.17 // Хабр. URL: https://habr.com/ru/news/858428/

21. *Булгаков Д.* Игра на опережение: в России планируют бороться с опасным контентом в Сети при помощи искусственного интеллекта // Известия. URL: https://iz.ru/1473572/dmitrii-bulgakov/igra-na-operezhenie-v-rossii-planiruiut-borotsia-s-opasnym-kontentom-v-seti-pri-pomoshchi

Сведения об авторе

СМЕЛОВ Александр Александрович,
аспирант кафедры международных отношений Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте РФ
Санкт-Петербург, Россия,
mailfordayzsub@gmail.com

Статья поступила в редакцию
25.02.2025

Одобрена после рецензирования
03.04.2025

Принята к публикации
28.04.2025

The author

Alexander A. SMELOV,
postgraduate student at the International Relations Department, North-West Institute of Management of the Russian Presidential Academy of National Economy and Public Administration
Saint Petersburg, Russia
mailfordayzsub@gmail.com

The article was submitted
25.02.2025

Approved after reviewing
03.04.2025

Accepted for publication
28.04.2025