

# ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

## INFORMATION AND COMMUNICATION TECHNOLOGIES

DOI: 10.22363/2313-0660-2025-25-2-236-250

EDN: MQQFIS

*Научная статья / Research article*

### Информационное противоборство в многополярном мире

С.В. Базавлук<sup>1</sup>, А.А. Ковалев<sup>2</sup>✉<sup>1</sup>Национальный исследовательский институт развития коммуникаций, Москва, Российская Федерация<sup>2</sup>Северо-Западный институт управления — филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Санкт-Петербург, Российская Федерация  
✉kovalev-aa@ranepa.ru

**Аннотация.** Формирование нового миропорядка в XXI в. находится в стадии становления, а нарастающее противоречие между международными акторами продолжает усиливаться. США, стремясь сохранить однополярность и противодействуя многополярности, придерживаются концепции информационного противоборства, вовлекая в этот процесс остальной мир. Конфликтность в международных отношениях сохраняется, а диалог часто воспринимается либо как проявление слабости, либо как спланированный маневр оппонента. Цель исследования — выявление особенностей аксиологического и технического аспектов информационного противоборства в многополярном мире. Отдельно рассмотрены два ключевых аспекта информационного противоборства: информационно-психологический и информационно-технический. Анализ применения инструментов информационного противоборства позволяет установить направленность действий глобальных акторов, основные используемые методы, преследуемые цели и достигнутые результаты. Методология исследования основана на системном и аксиологическом подходах, позволивших информационное противоборство как форму некинетического воздействия на ценностные и институциональные основы противника. В качестве метода применен герменевтический анализ первоисточников с элементами лексико-семантического разбора. Авторами сделан вывод, что информационное противоборство, главным субъектом которого остаются США, представляет серьезную угрозу формирующемуся многополярному миру и безопасности его сторонников, при этом отмечается наличие у них потенциала к сопротивлению, который, вероятно, будет раскрываться в будущем. В заключении приводятся возможные направления для дальнейших исследований, такие как практика взаимодействия союзных государств, препятствующих восстановлению однополярного мира и информационному давлению со стороны США и коллективного Запада; переход России в информационном противоборстве от оборонительных действий к наступательным; анализ новых инструментов и методов ведения информационного противоборства и другие актуальные темы.

**Ключевые слова:** когнитивная война, ментальная безопасность, стратегическая пропаганда, технологии искусственного интеллекта, deepfake, декаплинг, технологический суверенитет, цифровая манипуляция, гибридные угрозы, психосфера, ценностное воздействие, информационная дестабилизация

© Базавлук С.В., Ковалев А.А., 2025



This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by-nc/4.0/legalcode>

**Заявление о конфликте интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Вклад авторов.** Базавлук С.В.: концептуализация, разработка методологии исследования, проведение анализа, написание — подготовка черновика рукописи. Ковалев А.А.: теоретико-аналитическая проработка материала, редактирование текста, оформление библиографии, валидация источников. Оба автора ознакомлены с окончательной версией статьи и одобрили её.

**Для цитирования:** Базавлук С. В., Ковалев А. А. Информационное противоборство в многополярном мире // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2025. Т. 25, № 2. С. 236–250. <https://doi.org/10.22363/2313-0660-2025-25-2-236-250>

## Information Warfare in a Multipolar World

Sergei V. Bazavluk<sup>1</sup> , Andrei A. Kovalev<sup>2</sup>  

<sup>1</sup>National Research Institute for the Development of Communications, Moscow, Russian Federation

<sup>2</sup>North-West Institute of Management — branch of the Russian Presidential Academy of National Economy and Public Administration, St. Petersburg, Russian Federation

kovalev-aa@ranepa.ru

**Abstract.** The formation of a new world order in the 21st century is in its infancy, and the growing contradiction between international actors continues to intensify. In an effort to preserve unipolarity and counteract multipolarity, the United States adheres to the concept of information warfare, involving the rest of the world in this process. Conflict remains a prevalent feature of international relations, and dialogue is frequently perceived either as a sign of weakness or as a planned maneuver by an opponent. The purpose of the study is to identify the features of the axiological and technical aspects of information warfare in a multipolar world. Two key aspects of information warfare are examined separately: the information-psychological and the information-technical. The analysis of the use of information warfare tools enables the identification of the direction of actions by global actors, the main methods employed, the goals pursued and the results achieved. The research methodology is based on systematic and axiological approaches, which have facilitated the conceptualization of information warfare as a form of non-kinetic influence on the value and institutional foundations of the enemy. The present study employs a hermeneutical analysis of sources, incorporating elements of lexico-semantic analysis, as a methodological approach. The main conclusion of the study asserts that information warfare, in which the United States remains the main actor, poses a serious threat to the emerging multipolar world and the security of its supporters, while acknowledging their potential for resistance, which is likely to emerge in the future. In conclusion, the following directions for further research are proposed: firstly, the practice of interaction between the allied states that prevent the restoration of a unipolar world; secondly, the information pressure from the United States and the collective West; thirdly, Russia's transition from defensive to offensive actions in the information warfare; and fourthly, the analysis of new tools and methods of conducting information warfare, as well as other relevant topics.

**Key words:** cognitive warfare, mental security, strategic propaganda, artificial intelligence technologies, deepfake, decoupling, technological sovereignty, digital manipulation, hybrid threats, psychosphere, value impact, information destabilization

**Conflicts of interest.** The authors declare no conflicts of interest.

**Authors' contributions.** S.V. Bazavluk: conceptualization, development of research methodology, analysis, writing and preparation of a draft manuscript. A.A. Kovalev: theoretical and analytical study of the material, text editing, bibliography design, validation of sources. Both authors have read the final version of the article and approved it.

**For citation:** Bazavluk, S. V., & Kovalev, A. A. (2025). Information warfare in a multipolar world. *Vestnik RUDN. International Relations*, 25(2), 236–250. <https://doi.org/10.22363/2313-0660-2025-25-2-236-250>

### Введение

Мир стремительно меняется: однополярная структура уступает место многополярности, характеризующейся распределением

центров силы. Однако страны, открыто заявившие о переходе к полицентричному устройству, сталкиваются с противодействием со стороны США. Вместо открытого

военного противостояния акцент перемещается на скрытые формы борьбы, такие как информационное противоборство.

Термин «информационное противоборство» имеет сложную этимологию и состоит из двух элементов: «информационное» (от лат. *informatio* — «разъяснение, изложение, сообщение») и «противоборство», состоящего, в свою очередь, из «против» (от старославянского *прѣтивъ* «находящийся напротив, враждебный») и «борьба» (корень «бор-» восходит к древнерусскому *боронити* — «защищать, сопротивляться»). Тем самым «информация» охватывает процессы передачи, обработки и получения данных, а «информационное» указывает на обмен сведениями или использование технологий. При этом «противоборство» подразумевает активное сопротивление и борьбу между сторонами, стремящимися достичь целей через преодоление воли оппонента. Таким образом, под информационным противоборством следует понимать активные действия в информационной сфере, направленные на достижение стратегических целей с использованием информации как ресурса или инструмента. Информационное противоборство осуществляется как в наступательных формах, таких как распространение дезинформации, так и в оборонительных, направленных на защиту от информационных угроз.

В XXI в. соперничество государств перемещается в информационную сферу, поэтому информационное противоборство стало частью стратегий национальной безопасности и военных доктрин. Оно подразумевает под собой взаимоотношения государств в различных областях (политической, экономической, военной и проч.), при котором происходит воздействие на информационную сферу противника с целью расширения зоны своего влияния (Выходец, Панцеров, 2022, с. 139). А.И. Поздняков и В.С. Шевцов в своей совместной работе, посвященной методологическим основам построения теории информационного противоборства, отмечают, что говорить об информационной войне можно только в переносном смысле, поэтому уместнее употреблять термин «информационное противоборство» («борьба») (Поздняков,

Шевцов, 2017, с. 245). Авторы также отмечают, что информационное воздействие, осуществляемое в рамках информационного противоборства, можно разделить на две большие группы: информационно-техническое и информационно-психологическое. Важно отметить, что информационно-техническое противоборство воплощается в концепции когнитивной войны, которая фокусируется на технических аспектах, основанных на достижениях когнитивной науки. С помощью этих достижений появляется возможность манипулировать и управлять процессами потребления информации человеком, тогда как информационно-психологическое противоборство раскрывается благодаря концепции ментальной войны, в которой внимание акцентируется прежде всего на изменении ценностных и мировоззренческих установок человека и общества. При этом важно понимать, что информационно-психологическое противоборство осуществляется с помощью информационно-технических систем.

Итак, существует ряд современных теорий информационного противоборства, которые делятся на две большие взаимосвязанные группы.

В рамках анализа *информационно-технического противоборства* можно выделить, в частности, концепции сетевой войны, сетевцентрической войны и кибервойны. Так, теория сетевой войны была раскрыта в работе Дж. Аркиллы и Д. Ронфельдта (1996 г.)<sup>1</sup>, в которой отмечалось, что сетевой принцип организации современного противоборства является ведущим в войнах современности. Нарушение связи и коммуникаций противника с помощью применения новейших технологий становится, таким образом, основным способом достижения военных целей.

На рубеже XX и XXI столетий в США была разработана теория сетевцентрической войны<sup>2</sup>, при которой в единую информационную

<sup>1</sup> Arquilla J., Ronfeldt D. The Advent of Netwar. Santa Monica, CA : RAND Corporation, 1996. (Деятельность *RAND Corporation* признана нежелательной на территории Российской Федерации. — *Прим. ред.*).

<sup>2</sup> Cebrowski A. K., Garstka J. H. Network-Centric Warfare — Its Origin and Future // *Proceedings*. 1998. Vol. 124, no. 1. URL: <https://www.usni.org/magazines/>

сеть объединялись одновременно живая сила, военная техника и командование. Цель такого объединения — повысить синхронизацию действий различных боевых подразделений и увеличить скорость управления операциями на поле боя. Таким образом, иерархический способ организации и координации военных действий начал уступать сетевому принципу. В свою очередь, концепция кибервойны объединяет в себе знания о том, как с помощью компьютеров и Интернета нанести ущерб противоборствующей стороне (кибератаки позволяют делать это на расстоянии без учета национальных границ) (Clarke & Knake, 2010).

Информационно-технический аспект в настоящее время оказывает существенное влияние на формирование многополярного мироустройства, основными акторами которого являются ведущие страны мира (США, Китай, Россия и ряд других). Методы противостояния в рамках информационного противоборства постоянно совершенствуются и усложняются. Так, в рамках данного исследования будут рассмотрены, в частности, декаплинг и конкуренция за освоение технологий 4.0 (четвертой промышленной революции) в качестве эффективных методов информационно-технического противоборства как одного из основных факторов санкционной политики.

*Информационно-психологическое противоборство* является разновидностью информационного противоборства и рассматривается с позиции аксиологического подхода к системе безопасности в целом. Психика человека в войнах современности становится объектом информационного воздействия, ей наносится существенный ущерб (Hoyle et al., 2021, p. 150), именно поэтому обеспечение ментальной (когнитивной) безопасности является важной задачей стратегии национальной безопасности государств. С помощью манипуляции сознанием населения противника реализуются цели информационно-психологического противоборства (Манойло, 2019, с. 39). Обладание знаниями о механизмах влияния на общественное мнение,

условиях его возникновения и способах восприятия и обработки информации человеком позволяет эффективно осуществлять информационно-психологическое противоборство. О возможности применения психологических наработок в военной сфере еще в 1954 г. писал американский исследователь П. Лайнбарджер (1962).

Итак, информационно-психологическое противоборство реализуется в рамках ментальной войны. Данная разновидность противоборства исследуется в работах российского военного эксперта А.М. Ильницкого, который в качестве объекта воздействия называет самосознание человека (нации), национальный менталитет и в целом цивилизационные основания существования противника (Ильницкий, 2021). По сути, ментальной можно назвать такую войну (враждебные действия), в которой ценности, идеалы, образ жизни и прочие элементы (атрибуты) одной нации переносятся на другую. Тем самым можно предположить, что, по мнению А.М. Ильницкого<sup>3</sup>, если в одной нации (объекте воздействия) усматриваются характерные черты и особенности другой нации (субъекта воздействия), то имеет место ментальное вторжение. То есть о ментальной войне можно судить по ее результатам.

В последние годы в процессе информационного противоборства активно развиваются и применяются методы когнитивной войны. Организация Североатлантического договора (НАТО), возглавляемая США, в базовой концепции боевых действий выделяет следующие ключевые сферы: наземную, морскую, воздушную, космическую, информационную (киберпространство) и когнитивную<sup>4</sup>. Именно когнитивной сфере в войнах нового

<sup>3</sup> Ильницкий А. М. Ментальная война за будущее России // Звезда. 21.04.2021. URL: <https://zvezdaweekly.ru/news/20214211636-jxgHZ.html> (дата обращения: 19.01.2025).

<sup>4</sup> Таммен Дж. Базовая концепция боевых действий НАТО: в перспективе — меняющийся характер войны // Вестник НАТО. 09.07.2021. URL: <https://www.nato.int/docu/review/ru/articles/2021/07/09/bazovaya-kontseptsiya-boevykh-dejstvij-nato-v-perspektive-menyayushchisya-harakter-vojny/index.html> (дата обращения: 06.01.2025).

типа уделяется все больше внимания с точки зрения разработки и внедрения методологии ведения боевых действий. Эта сфера рассматривается как перспективное направление для дальнейших разработок. «Взлом личности» — ключевой принцип и одновременно инструмент когнитивной войны, суть которого заключается в манипулировании сознанием человека и направленном управлении его действиями<sup>5</sup>. Дестабилизация и внешнее влияние в этом случае выступают в качестве основных целей когнитивного противоборства<sup>6</sup>.

Развитие когнитивной войны во многом опирается на достижения нейронаук, которые открывают возможность более глубокого воздействия на психофизиологические процессы. В этой связи нейронауки превращаются в инструмент политической борьбы, обеспечивающий достижение масштабных стратегических целей. Борьба за человеческий разум радикально меняет представления о безопасности, которая все чаще воспринимается как игра с нулевой суммой (Ördén, 2024, p. 614).

Информационное противоборство, активным участником которого выступают США, рассматривается как нетрадиционная угроза безопасности в условиях многополярного мира. Информационно-психологическое противоборство, опирающееся на методы «мягкой силы», разворачивается в культурном пространстве с целью трансформации сознания политического оппонента, который может даже не осознавать подобного воздействия. Объектами таких атак становятся ценностные ориентиры, традиции, историческая и культурная идентичность государств (Гончарова, Ницевич, Судоргин, 2024, с. 21), а также критическая инфраструктура, военные объекты и другие ключевые элементы государства, в результате чего подвергается опасности информационно-психологическая сфера.

<sup>5</sup> Du Cluzel F. Cognitive Warfare, a Battle for the Brain. NATO Innovation Hub. 2020. URL: <https://archive.org/details/mp-hfm-334-kn-3> (accessed: 19.01.2025).

<sup>6</sup> Wanyana R. Cognitive Warfare: Does it Constitute Prohibited Force? // EJIL: Talk. January 30, 2025. URL: <https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/> (accessed: 02.02.2025).

Динамичное развитие международных процессов, обусловленное стремительным прогрессом информационно-коммуникационных технологий (ИКТ) и ростом напряженности в мире, послужило основой для данного исследования. Особую обеспокоенность в контексте информационного противоборства вызывает информационно-психологическая безопасность. Исследование посвящено анализу информационного противоборства в многополярном мире и нацелено на выявление особенностей аксиологического и технического аспектов информационного противоборства в условиях формирования многополярного мира.

Авторы исходят из критико-аналитического подхода, позволяющего трактовать информационное противоборство как форму некинетического воздействия, направленного на трансформацию ментальной и институциональной устойчивости противника. Такой ракурс отличает исследование от технократических и инфраструктурных моделей, сосредоточенных на контроле над ИКТ-средой, а также от неомарксистской интерпретации (в частности присущей работам М. Кастельса), в рамках которой внимание акцентируется на роли цифровых сетей в глобальной системе коммуникации, распределения власти и экономического влияния (Кастельс, 2000). Выбранный подход позволяет сосредоточиться на гуманитарных аспектах и ценностной уязвимости субъектов геополитического взаимодействия.

В качестве методов исследования были использованы систематизация, с помощью которой широкая дефиниция «информационное противоборство» была дифференцирована исходя из более локальных и конкретных аспектов данного противоборства в рамках функционирования международной системы; системный подход позволил выявить глубинные причины и смыслы переустройства миропорядка и выбранные способы его реализации. Также для раскрытия выбранной тематики были применены системно-деятельностный подход и входящий в него аксиологический подход, герменевтический анализ первоисточников с элементами лексико-семантического разбора текстов, благодаря

которым были изучены потенциалы информационно-технического и информационно-психологического аспектов информационно-противоборства, обозначены возможности применения технологий искусственного интеллекта (ИИ) наступательного и оборонительного характера, а также рассмотрены возможности России по сохранению своего суверенитета в современном многополярном мире.

### **Информационное противоборство в современном мире**

Термин «информационная война» впервые был упомянут в отчете ученого Томаса Роны, подготовленном по заказу Министерства обороны США в 1976 г.<sup>7</sup> В этом отчете информационная сфера обозначалась как уязвимая цель для возможных атак противника. На тот момент информационные атаки рассматривались преимущественно в экономической области, однако со временем их воздействие охватило практически все сферы жизнедеятельности. Авторство термина нередко оспаривается, поскольку еще в 1970 г. журналистка Дейл Майнор опубликовала книгу под заголовком «Информационная война» (Minor, 1970). Однако именно работа Т. Роны способствовала популяризации этого понятия как значимого феномена.

Эволюция информационного противоборства на протяжении последних десятилетий прошла путь от технических аспектов к аксиологически-антропологической сфере. В современном мире все большее значение приобретают ментальность народов, их идентичность, самосознание, коллективная память (включая коллективную травму) и идеология. В этой связи в XXI в. информационно-психологическое противоборство становится важным инструментом межгосударственного взаимодействия, применяемым для достижения целей через методы некинетических

(нефизических) форм воздействия, характерных для современных войн.

В рамках информационно-психологического противоборства используется информационно-идеологическое противостояние, в котором уникальность нации и основа ее духовного существования становятся ключевым объектом воздействия. По мнению И.Ф. Кефели и Н.А. Комлевой, информационно-идеологическое пространство в настоящее время является основным пространством борьбы, так как подобные действия носят скрытый характер и не воспринимаются обществом как агрессия. Напротив, нация-агрессор «ненавязчиво поощряет» нацию-мишень трансформироваться и пойти по восходящему пути развития. В западной риторике по-прежнему используется терминология «второй» и «третий мир», подразумевающая отсталость остального мира и необходимость следовать западным моделям развития. Такой подход подвергается критике даже внутри самого Запада как форма воспроизводства колониального мышления<sup>8</sup>. При этом «основным „оружием“ информационно-идеологических войн является совокупность оценочных мировоззренческих, или идеологических, конструктов, целенаправленно созданных с целью оправдания экспансии данного геополитического актора и осуждения экспансии актора-противника (противников)» (Кефели, Комлева, 2019, с. 57). Такая политика характерна для США, последовательно оправдывавших свое присутствие в различных регионах мира, поддержку «цветных» революций и вмешательство во внутренние дела суверенных государств<sup>9</sup>. Однако когда Россия начала специальную военную операцию (СВО) на Украине в 2022 г., США и их союзники одними из первых осудили происходящее, что

<sup>8</sup> Silver M. Memo to People of Earth: ‘Third World’ Is an Offensive Term! // NPR. January 8, 2021. URL: <https://www.npr.org/sections/goatsandsoda/2021/01/08/954820328/memo-to-people-of-earth-third-world-is-an-offensive-term> (accessed: 19.01.2025).

<sup>9</sup> GT Investigates: US Wages Global Color Revolutions to Topple Govts // Global Times. December 30, 2021. URL: <https://www.globaltimes.cn/page/202112/1240540.shtml> (accessed: 19.01.2025).

<sup>7</sup> Rona T. Weapon Systems and Information War. Office of the Secretary of Defense, Washington, DC. July 1, 1976. URL: [https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science\\_and\\_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf](https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf) (accessed: 10.01.2025).

указывает на наличие двойных стандартов в международной политике<sup>10</sup>.

Военный аналитик А.А. Бартош утверждает, что информационное противоборство, являясь ключевым элементом гибридной войны, инициировано США с целью сохранения однополярного мира и обеспечения своей гегемонии на международной арене (Бартош, 2024). В рамках первого этапа достижения глобального господства рассматривается уничтожение России через ликвидацию ее государственности, фрагментацию и установление внешнего управления. Следующим шагом обозначено установление контроля над Китаем, затем — воздействие на Индию и другие государства Евразии. Схожая логика закреплена и в официальных стратегических документах США, где Россия и Китай обозначаются в качестве главных угроз и конкурентов, подлежащих сдерживанию в рамках глобального соперничества. Такие документы прямо или косвенно фиксируют цели по ограничению влияния несистемных акторов и поддержанию мирового лидерства США посредством гибридных и информационных инструментов<sup>11</sup>.

Новые технологии, включая информационно-коммуникационные, стали основой для защиты национальных интересов США, что прямо указано в национальной военной стратегии этого государства<sup>12</sup>. Информационное противоборство с Россией осуществляется в

соответствии с концепцией «стратегических коммуникаций» (*strategic communications*), которая активно развивалась в структурах НАТО и была зафиксирована в итоговом коммюнике Варшавского саммита 2016 г. как элемент политико-информационного давления<sup>13</sup>. Термин прямо упоминается в числе приоритетных направлений по усилению способности Альянса противостоять внешним вызовам и формировать благоприятное восприятие своей повестки. Экономическое и политическое ослабление России, утрата субъектности, размывание традиционных ценностей, дестабилизация внутренней обстановки и другие цели определены как приоритетные. Проведение информационных операций американским военным командованием рассматривается как основной способ сохранения доминирования в информационной сфере. Ключевыми методами становятся распространение ложной информации, подтасовка фактов, создание фейков, замалчивание важных сведений и акцентирование внимания на второстепенных аспектах с целью дезориентации и введения целевой аудитории в заблуждение.

Для реализации этой стратегии в Латвии функционирует Центр передового опыта НАТО в области стратегических коммуникаций (*NATO Strategic Communications Centre of Excellence*), а также действуют различные антироссийские неправительственные организации (НПО), такие как «Фонд Сороса»<sup>14</sup>, *Freedom House*<sup>15</sup> и др. Среди наиболее приоритетных задач НАТО на ближайшую перспективу названы формирование негативного образа России как основной угрозы странам

<sup>10</sup> War in Ukraine // Council on Foreign Relations. April 14, 2025. URL: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine> (accessed: 19.04.2025).

<sup>11</sup> См.: 2022 National Defense Strategy of the United States of America. U.S. Department of Defense, 2022. URL: <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf> (accessed: 19.01.2025); Renewed Great Power Competition: Implications for Defense — Issues for Congress. Congressional Research Service. August 28, 2024. URL: <https://sgp.fas.org/crs/natsec/R43838.pdf> (accessed: 19.01.2025).

<sup>12</sup> Description of the National Military Strategy 2018 // Office of Primary Responsibility: Strategy Development Division, Deputy Directorate for Joint Strategic Planning, Directorate for Strategy, Plans, and Policy (J-5). The Joint Chiefs of Staff. 2018. URL: [https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS\\_2018\\_National\\_Military\\_Strategy\\_Description.pdf](https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf) (accessed: 06.01.2025).

<sup>13</sup> Warsaw Summit Communiqué // NATO. July 9, 2016. URL: [https://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](https://www.nato.int/cps/en/natohq/official_texts_133169.htm) (accessed: 07.01.2025).

<sup>14</sup> Деятельность финансируемых «Фондом Сороса» иностранных неправительственных организаций — Фонда Открытое общество (*Open Society Foundations*) и Института Открытое Общество Фонд Содействия (*OSI Assistance Foundation*) — признана нежелательной на территории Российской Федерации (*Прим. ред.*).

<sup>15</sup> Деятельность международной неправительственной организации *Freedom House* признана нежелательной на территории Российской Федерации (*Прим. ред.*).

НАТО и ЕС, международная изоляция и снижение влияния России на постсоветском пространстве, включая СНГ, а также поддержание политики стратегического сдерживания и минимального диалога с Москвой<sup>16</sup>.

В англо-американском мире широко используется понятие «вредоносное влияние России». Доктор политических наук Д. Пророкович отмечает, что данное понятие намеренно введено и распространено США с целью обеспечения тотального информационного воздействия на Россию. Исследователь подчеркивает, что «к вредоносному влиянию России может быть отнесено любое действие с участием какого-либо российского государственного учреждения, государственной корпорации или организации (неправительственной, научной, религиозной)» (Пророкович, 2021, с. 82–83). Упоминание «вредоносного влияния России» позволяет США использовать данный термин как предлог для оправдания своих действий, включая нелегитимные.

По мнению Е.А. Даниловой и Е.Д. Заболотной, информационная война не только несет угрозы и риски, но и открывает перспективы, связанные, в частности, с переходом России от оборонительной позиции к наступательной (Данилова, Заболотная, 2023). Профессор А.В. Манойло считает, что Россия должна стремиться к равной конкуренции с США в сфере информационного противоборства и подробно описывает примеры манипулятивного воздействия на противников, призывая использовать аналогичные подходы для усиления собственных позиций (Манойло, 2021, с. 94).

Доктор политических наук И.А. Василенко отмечает, что современной России следует уделять больше внимания политике формирования положительного образа на международной арене (Василенко, 2014). Исследователь подчеркивает, что враждебность со стороны Запада способствовала усилению восточной ориентации России, поскольку

необходимая внешнеполитическая поддержка была найдена среди стран БРИКС, Шанхайской организации сотрудничества (ШОС) и Евразийского экономического союза (ЕАЭС). В настоящее время Российская Федерация самостоятельно формирует международную повестку, в том числе в сфере информационной безопасности. Так, в рамках БРИКС она активно продвигает инициативы по выработке норм поведения государств в киберпространстве, направленных на защиту национальных интересов и укрепление цифрового суверенитета. Участие России в формировании нормативных подходов в информационном пространстве подробно рассматривается в научной литературе, посвященной правовым режимам кибербезопасности (Рамич, Пискунов, 2022).

### **Искусственный интеллект как инструмент информационного противоборства**

Искусственный интеллект представляет собой совокупность технологий, основанных на алгоритмах обработки данных, моделирующих аналитические и когнитивные способности человека. Значение ИИ в информационном противоборстве заключается в способности генерировать и адаптировать информацию, а также манипулировать ею в масштабах, ранее недоступных ни одному инструменту или методу. Технологии ИИ одновременно являются ресурсом и оружием. С их помощью можно обрабатывать большие массивы данных и выявлять сложные взаимосвязи между элементами информации, что неосуществимо в рамках традиционных методов. ИИ используется в прогнозировании, управлении массовым сознанием и влиянии на него.

ИИ-технологии обладают высоким конструктивным потенциалом, однако также они создают дополнительные риски, усиливающие информационное противостояние. Например, они активно используются для создания контента пропагандистского характера. Примечательно, что эффект от таких методов противоборства наступает благодаря активизации принципа «спрос рождает пред-

<sup>16</sup> Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted on June 29, 2022 // NATO. 2022. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf) (accessed: 09.01.2025).

ложение». Иными словами, спрос на быструю и многообразную информацию порождает ее появление. Такая информация, как правило, легка для восприятия, не является энергозатратной на этапе сбора и анализа (она доходит до аудитории в готовом виде), интересна и привлекательна (Goldstein, Sastry & Musser, 2023, p. 65). Таким образом, одним из способов борьбы с пропагандой посредством использования ИИ-технологий является удовлетворение запроса общества на осведомленность.

Отсюда следует, что основную угрозу представляют не сами ИИ-технологии, а их злонамеренное использование, угрожающее международной информационно-психологической безопасности (Пашенцев, 2019). Среди основных методов применения ИИ-технологий в информационном противоборстве — создание *deepfakes* («глубинное обучение» + «подделка»), установка и закрепление повестки дня, целевая трансформация образов, технология «отравленные данные», анализ тональности в текстах, технология «фальшивые люди» и др.

Технологии ИИ демонстрируют высокую эффективность в таргетировании аудитории, направляя информационные атаки на конкретные группы населения с учетом их культурных, политических и социальных особенностей. Точность таких воздействий усиливается благодаря использованию технологий глубокого обучения, позволяющих моделировать вероятные сценарии реакций на информационные стимулы. Системы ИИ способны анализировать поведение пользователей социальных сетей, сопоставляя их интересы, поведенческие паттерны и эмоциональные реакции для создания персонализированного контента, максимально влияющего на их восприятие и действия. ИИ выступает не просто инструментом влияния, но и фактором, управляющим динамикой информационного поля в реальном времени.

Исследователи Д.Ю. Базаркина и Е.Н. Пашенцев отмечают, что в настоящее время негативный эффект от использования ИИ и его влияние на информационно-психологическую безопасность недостаточно изучены (Bazarkina & Pashentsev, 2019,

p. 149). Ученые в своем совместном исследовании выделили ряд факторов, которые затрудняют минимизацию ущерба от злонамеренного использования ИИ-технологий. Среди них непрекращающееся геополитическое противостояние (отсутствие согласованности позиций мировых акторов по достижению приемлемого уровня безопасности), социальная нестабильность в связи с экономическими кризисами, недоверие к государственным институтам и политическим партиям, конкуренция человека и ИИ в сфере занятости (рост безработицы) и некоторые другие. Тем самым становится очевидно, что использование ИИ в целях нарушения безопасности, в том числе информационно-психологической, носит комплексный характер, пересекается с традиционными проблемами и порождает качественно новые вызовы.

Автоматизация процессов обработки данных и создания контента позволяют ИИ функционировать в режиме реального времени, создавая эффект массовой поддержки или сопротивления, что значительно усиливает влияние на общественное сознание. Децентрализованная природа подобных систем практически исключает возможность их нейтрализации традиционными методами противодействия дезинформации. Кроме того, технологии ИИ обеспечивают согласованность действий на глобальном уровне, а это, в свою очередь, открывает возможности для координации информационных кампаний, направленных на дестабилизацию различных регионов. Технологические решения на основе ИИ отличаются не только значительной сложностью, но и тесной взаимосвязью с социальными и психологическими процессами, что делает их мощным инструментом для воздействия на массовое сознание. Особую эффективность имеет технология *deepfake*, фактически подменяющая физическую реальность вымышленной.

Применение ИИ в условиях информационного противоборства является не только технологической инновацией, но и значительным культурным вызовом, изменяющим восприятие правды, достоверности и объективности. Развитие подобных технологий

указывает на необходимость пересмотра методов обеспечения информационной безопасности и разработки новых подходов к управлению информационными потоками.

Инструменты ИИ не ограничиваются выполнением заданных функций, они могут приспосабливаться к изменениям в информационной среде. Способность к адаптации крайне важна в условиях стремительных перемен в сфере глобальных информационных структур, где события развиваются динамично, а своевременная реакция требует использования максимально доступных ресурсов.

Эволюция технологий ИИ приводит к появлению новых форм «информационной автономии», при которых системы самостоятельно принимают решения о характере и содержании распространяемой информации. Автономные процессы охватывают не только генерацию контента, но и выбор наиболее эффективных методов его доставки. ИИ выступает в роли стратегического агента, определяющего приоритеты и корректирующего направление информационного воздействия в зависимости от изменяющихся условий. Тем самым новые возможности расширяют потенциал информационного противоборства, одновременно порождая серьезные этические и правовые вопросы.

Природа технологий ИИ в информационном противоборстве отличается динамичностью, адаптивностью и способностью преобразовывать фундаментальные подходы к работе с информацией. Технологии не только ускоряют и упрощают создание и распространение контента, но и меняют то, как информация влияет на общественное сознание и политические процессы. Так формируются новые правила взаимодействия на глобальном уровне.

### **Информационное противоборство в условиях формирования многополярного мира**

В настоящее время имеют место угрозы информационно-психологической безопасности ведущих стран незападного мира, связанные с использованием новейших технологий (в том числе ИИ). Последствия их применения могут быть катастрофическими

для психологической безопасности (Pantserev, 2020). По мнению Д.Ю. Базаркиной и Е.Н. Пашенцева, психологический ущерб от использования ИИ-технологий является третьим и самым опасным уровнем угроз (первый уровень — распространение ложного негативного образа ИИ, второй — непосредственное вредоносное использование ИИ без цели прямого влияния на общественное сознание, например использование беспилотных летательных аппаратов (БПЛА) на территории противника или кража денег посредством ИИ-технологий) (Bazarkina & Pashentsev, 2020, p. 162). Дискредитация надежных систем (например, многоступенчатых систем защиты банковских приложений и счетов), неопределенность и отсутствие алгоритма действий в ситуациях использования ИИ-технологий для нарушения информационно-психологической безопасности наносит серьезный ущерб обществу, подвергающемуся подобным атакам.

Одним из наиболее ярких проявлений информационно-технического противоборства в условиях становления многополярного мира стало технологическое и информационное противостояние между США и КНР, развивающееся по логике «декаплинга». Если символом глобализации в конце XX в. выступал «каплинг» (*coupling* — «связь»), то в XXI в. на первый план выходит обратный процесс — «декаплинг» (*decoupling* — «расцепление»), наиболее отчетливо проявившийся в американо-китайских отношениях в период первого президентского срока Д. Трампа (2017–2021 гг.). Как подчеркивает Я.В. Лексютина, действия Китая — кибершпионаж, активность телекоммуникационных компаний и инвестиции в экономику США — были восприняты США как угроза национальной безопасности, что стало основанием для формирования в Вашингтоне курса на технологическое и информационное дистанцирование от Пекина (Лексютина, 2020, с. 86).

Санкционное давление, усилившееся после начала специальной военной операции России на Украине (с 2022 г.), ускорило разрыв глобальных производственно-логистических цепочек и информационных связей. Прежде декларируемое взаимовыгодное

сотрудничество стало восприниматься как стратегическая уязвимость. В обновленной архитектуре международных отношений взаимозависимость все чаще рассматривается как фактор риска не только в экономической, но и в идеологической и технологической сферах. Явление «декаплинга» приобретает черты своеобразного «парада суверенитетов» XXI в., отражающего стремление государств выстраивать автономные траектории развития. Возвращение Д. Трампа к власти в США в 2025 г. предопределяет дальнейшее расширение протекционистской повестки: еще до вступления в должность он заявлял о планах ввести пошлины на товары из Китая, стран БРИКС и Европейского союза (Виноградов, Салицкий, Семенова, 2019, с. 42).

Американо-китайское противостояние в сфере высоких технологий приобрело характер затяжного конфликта. При администрации Б. Обамы были предприняты первые шаги по сдерживанию Китая через санкционные механизмы, а при Д. Трампе противостояние переросло в полноценную «технологическую войну» (Данилин, 2020, с. 161). США вводили жесткие ограничения в отношении таких технологических гигантов, как *Huawei* и *ZTE*, сворачивали академическое сотрудничество и усиливали контроль над экспортом критически важных компонентов. В ответ Китай ускорил внутреннюю цифровую модернизацию и начал выстраивать партнерские связи с другими странами: членами Евросоюза, Японией, Россией, Израилем и рядом развивающихся государств.

В результате на глобальной технологической карте формируются два автономных пространства: первое — под лидерством США, второе — с растущим влиянием Китая (Выходец, 2022, с. 262–263). Россия ориентируется на восточный вектор, стремясь компенсировать потери, вызванные разрывом с западными поставщиками технологий, такими как *Intel*, *AMD* и производители полупроводников с Тайваня (Китай). Развивающиеся страны, лишенные доступа к передовым цифровым компонентам, оказываются особенно уязвимыми в складывающихся условиях. Борьба за лидерство в сфере технологий 4.0 становится не только экономическим, но и

политическим приоритетом. Государства, обладающие технологическим суверенитетом, получают преимущества как в промышленности, так и в оборонной сфере, в том числе за счет использования искусственного интеллекта в военных разработках.

Следует отметить, что в КНР проблематика информационного и технологического противоборства активно концептуализируется в научной среде. В данной статье основное внимание сосредоточено на стратегических инициативах США и их влиянии на глобальный баланс. Подробное рассмотрение китайских теоретических подходов требует самостоятельного исследования.

Несмотря на то, что США являются главным идеологом и субъектом информационного противоборства в современном мире, они рассматривают Россию, Китай, Иран и ряд других незападных государств как ревизионистские государства, ведущие войну в так называемой «серой зоне», в которой состояния мира и войны неразличимы, а скрытые действия, осуществляемые с помощью новейших информационных технологий, позволяют достигать политических целей (Azad, Haider & Sadiq, 2023, p. 95). Информационные технологии, будучи «бестелесными» инструментами, вызывают вполне реальные, материальные последствия. Одним из таких примеров стали «твиттер<sup>17</sup>-революции», от которых пострадали страны Ближнего Востока и Северной Африки (Татунц, 2024, с. 4).

Россия осознает угрозу информационного воздействия, поэтому в «Концепции внешней политики РФ» 2023 г. подчеркивается значимость формирования и развития безопасного информационного пространства, обеспечивающего защиту населения от деструктивного иностранного информационно-психологического влияния. Существенным шагом вперед стало открытое официальное признание противников поименно, что нашло отражение в концептуальных документах<sup>18</sup>.

<sup>17</sup> Социальная сеть *Twitter* (ныне — *X*) заблокирована Роскомнадзором Российской Федерации в 2022 г. (Прим. ред.).

<sup>18</sup> Распоряжение Правительства РФ от 05.03.2022 № 430-р (ред. от 29.10.2022) «Об утверждении перечня иностранных государств и территорий, совершающих

По мере совершенствования методов информационного противоборства Россия также должна своевременно реагировать на возникающие угрозы. Так, в коллективном исследовании А. Вентцеля, С. Ханссона, М.-Л. Мадиссон и В. Сазонова на примере военных учений России «Запад – 2017» у границ Белоруссии раскрывается использование культуры страха. Россия, по мнению исследователей, активно пользуется нагнетанием страха для достижения стратегических целей. И это является проявлением информационного противоборства, считают авторы. «Неопределенность — важный источник страха», говорится в статье (Ventsel et al., 2019, p. 28). И в этом основное преимущество и цель России. Статья была написана до начала СВО, тем самым этот страх (Россия с 2014 г. настаивала на прекращении неправомерных действий на Донбассе со стороны киевской власти) воплотился в реальность. То есть предупреждение, длительное время остававшееся на уровне страха, материализовалось в критический момент.

По нашему мнению, для России такое восприятие противником российской политики может иметь положительный результат. Тем более прецедент уже создан. При этом важно, чтобы противостоящая сторона воспринимала предупреждение именно как реальную угрозу, а не как элемент информационного противоборства и «военной игры», а именно как намерение. Так, оправданным является утверждение А.В. Фененко, профессора факультета мировой политики МГУ им. М.В. Ломоносова, о том, что информационное противоборство между странами возможно только при условии, что обе стороны признают авторитет друг друга. В противном случае акт коммуникации становится невозможным<sup>19</sup>. Предупреждения в случае

недружественные действия в отношении Российской Федерации, российских юридических и физических лиц» // КонсультантПлюс. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_411064/e8730c96430f0f246299a0cb7e5b27193f98fdaa/](https://www.consultant.ru/document/cons_doc_LAW_411064/e8730c96430f0f246299a0cb7e5b27193f98fdaa/) (дата обращения: 02.11.2024).

<sup>19</sup> Фененко А. Парадокс информационных войн // Российский совет по международным делам. 17.08.2022. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/paradoks-informatsionnykh-voyn/> (дата обращения: 07.01.2025).

с Украиной не возымели должного эффекта, и, к сожалению, это привело к культивированию в информационном пространстве страхов о ядерных ударах, а на высшем государственном уровне — к смене ядерной доктрины<sup>20</sup>. Действительно, противники России должны считаться с ней, воспринимать ее намерения всерьез. Как представляется, одержать победу в информационном противоборстве России может помочь стратегия культивирования страха, когда одного лишь информационного сигнала со стороны России будет достаточно, чтобы внушить опасения относительно ее возможных действий.

Когнитивная война позволяет человеку как индивидуальной единице быть одновременно и объектом, и субъектом информационного воздействия в рамках информационного противоборства. С одной стороны, человек — получатель информации, с другой — ее распространитель. Это означает, что определенная грань между адресатом и адресантом стирается, и, по сути, любой пользователь может стать лидером общественного мнения. Так, с начала СВО в социальной сети X (ранее — *Twitter*) появился целый ряд новых аккаунтов социальных ботов. Например, на аккаунт @UAWearns, публиковавший предвзятые сообщения с целью дискредитации России, всего за месяц подписалось несколько сотен тысяч пользователей (Li et al., 2023, p. 69). Здесь также проявляется проблема отсутствия ответственности за распространение информации, поскольку обезличенный характер публикации новостей усиливает манипулятивный эффект, производимый подобными сообщениями.

С 2022 г. все более очевидно проявляется тенденция к расколу ведущих стран мира («друг — враг»), однако такие государства, как, например, Индия и Китай, заявляют о своем нейтралитете<sup>21</sup>. Подобная позиция

<sup>20</sup> Указ Президента Российской Федерации от 19.11.2024 г. № 991 «Об утверждении Основ государственной политики Российской Федерации в области ядерного сдерживания» // Президент России. URL: <http://www.kremlin.ru/acts/bank/51312> (дата обращения: 06.01.2025).

<sup>21</sup> China's Position on Russia's Invasion of Ukraine // U.S. — China Economic and Security Review Commission. February 28, 2025. URL: <https://www.uscc.gov/>

вызывает недовольство Запада по нескольким причинам: во-первых, она отражает независимость других акторов; во-вторых, страны с такими принципами не разделяют либеральные ценности; в-третьих, неопределенность их позиции делает их потенциальными партнерами России. С высокой вероятностью государства, не входящие в западный мир, продолжат выстраивать более справедливую модель мирового порядка и усиливать сотрудничество в области информационных технологий для противодействия давлению со стороны коллективного Запада. Для России это открывает возможности формирования устойчивых цифровых альянсов, продвижения альтернативных норм международного информационного взаимодействия и укрепления роли координатора в сфере глобальной информационной безопасности.

### Заключение

Современный мир и отношения между глобальными акторами отличаются гибкостью, фрагментарностью и выраженной манипулятивностью. Ведущие международные игроки по-прежнему стремятся к расширению геополитического влияния, однако средства достижения этой цели радикально изменились. Центры силы стремительно трансформируются, а информационное противоборство становится, с одной стороны, инструментом для малых и ранее маргинализованных государств заявить о своих интересах на международной арене, с другой — источником дестабилизации, угрожающим формированию многополярного мира.

Информационное противоборство, являясь лишь одним из элементов широкого комплекса глобальных угроз наряду с валютно-финансовым давлением, военно-политическим доминированием и санкционной политикой, отличается скрытностью, трудной прогнозируемостью и слабой подот-

четностью. При отсутствии четких международных регламентов и механизмов контроля манипулятивные воздействия в информационной сфере приобретают разрушительный характер. Так, например, США применяют эту форму противоборства не с целью навязывания универсальной либерально-демократической модели, а как инструмент ослабления незападных центров силы, способных бросить вызов американской гегемонии. Политика протекционизма, проводимая администрацией Д. Трампа, технологическое превосходство США и наличие конкурирующих акторов, в том числе КНР, будут усиливать информационное противостояние в ближайшей перспективе.

Актуальность темы предполагает дальнейшее развитие исследований в области стратегического анализа информационного противоборства. В перспективе научные изыскания могут быть сосредоточены на следующих направлениях:

- механизмы взаимодействия государств, противодействующих восстановлению однополярной модели мирового порядка и внешнему информационному давлению;
- информационное противоборство как элемент гибридной стратегии США в отношении стран незападного мира, а также анализ информационного воздействия на Россию, Китай, Индию, Бразилию, арабские и другие государства;
- эволюция российской модели информационного противостояния с переходом от оборонительных к наступательным стратегиям;
- новые формы и методы ведения информационного противоборства;
- изменения в системе международной безопасности под влиянием информационно-психологических и информационно-технологических воздействий.

Расширение таких направлений позволит более точно определить место и роль информационного противоборства как ключевого измерения глобальной конкуренции в условиях становления многополярного мира.

research/chinas-position-russias-invasion-ukraine (accessed: 18.03.2025).

Поступила в редакцию / Received: 03.11.2024  
Доработана после рецензирования / Revised: 28.01.2025  
Принята к публикации / Accepted: 20.03.2025

## Список литературы

- Бартош А. А.* Мировая гибридная война. Москва : Горячая линия-Телеком, 2024.
- Василенко И. А.* Формирование нового образа России «после Крыма»: парадоксы информационной войны // *Власть*. 2014. № 10. С. 204–208. EDN: SXSXCZ
- Виноградов А. О., Салицкий А. И., Семенова Н. К.* Американо-китайская экономическая конфронтация: идеология, хронология, значение // *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2019. Т. 19, № 1. С. 35–46. <https://doi.org/10.22363/2313-0660-2019-19-1-35-46>; EDN: ZBFCZN
- Выходец Р. С.* Большие ИИ-пространства и стратегия России в условиях санкционной войны // *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2022. Т. 22, № 2. С. 256–270. <https://doi.org/10.22363/2313-0660-2022-22-2-256-270>; EDN: FYNWU
- Выходец Р. С., Панцеров К. А.* Сравнительный анализ современных концепций информационного противоборства // *Евразийская интеграция: экономика, право, политика*. 2022. Т. 16, № 4 (42). С. 139–148. <https://doi.org/10.22394/2073-2929-2022-04-139-148>; EDN: SVTUJU
- Гончарова И. В., Ницевич В. Ф., Судоргин О. А.* Информационная война как инструмент политического противостояния в современном многополярном мире // *Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление*. 2024. Т. 11, № 1. С. 19–31. <https://doi.org/10.22363/2312-8313-2024-11-1-19-31>; EDN: ZIXNDI
- Данилин И. В.* Американо-китайская технологическая война: риски и возможности для КНР и глобального технологического сектора // *Сравнительная политика*. 2020. Т. 11, № 4. С. 160–176. EDN: GYRYVR
- Данилова Е. А., Заболотная Е. Д.* Технологии политического PR в информационной войне РФ и Запада в рамках военно-политического конфликта на Украине: новые вызовы и новые возможности для России // *Власть*. 2023. Т. 31, № 2. С. 56–63. <https://doi.org/10.31171/vlast.v31i2.9528>; EDN: XYKPLA
- Ильницкий А. М.* Ментальная война России // *Военная мысль*. 2021. № 8. С. 19–33. EDN: TDSKIX
- Кастельс М.* Информационная эпоха : экономика, общество и культура. Москва : ГУ ВШЭ, 2000.
- Кефели И. Ф., Комлева Н. А.* К вопросу о роли информационно-идеологической безопасности в контрстратегии гибридной войны на евразийском пространстве // *Евразийская интеграция: экономика, право, политика*. 2019. № 1 (27). С. 54–60. EDN: NANPIC
- Лайнбарджер П.* Психологическая война. Москва : Воениздат, 1962.
- Лексютина Я. В.* Американо-китайские отношения в 2018–2019 гг.: торговая война и процесс декаплинга // *Мировая экономика и международные отношения*. 2020. Т. 64, № 6. С. 85–93. <https://doi.org/10.20542/0131-2227-2020-64-6-85-93>; EDN: QRYEBK
- Манойло А. В.* «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // *Вестник Московского университета. Серия 12: Политические науки*. 2019. № 2. С. 37–45. EDN: HGEVPF
- Манойло А. В.* Эволюция информационных операций // *Вестник Московского государственного областного университета*. 2021. № 4. С. 80–103. <https://doi.org/10.18384/2224-0209-2021-4-1100>; EDN: MVAJGI
- Пашенцев Е. Н.* Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // *Государственное управление. Электронный вестник*. 2019. № 76. С. 279–300. <https://doi.org/10.24411/2070-1381-2019-10013>; EDN: CVLXTW
- Поздняков А. И., Шевцов В. С.* Методологическая основа построения теории информационного противоборства // *Социально-гуманитарные знания*. 2017. № 2. С. 244–257. EDN: YJYGXD
- Пророкович Д.* Попытка Запада представить Российскую Федерацию в качестве врага (о концепции «вредоносного влияния России») // *Вестник Московского университета. Серия 12: Политические науки*. 2021. № 2. С. 72–85. EDN: LPTWIL
- Рамич М. С., Пискунов Д. А.* Секьюритизация информационного пространства: от конструирования норм до создания правовых режимов // *Вестник Российского университета дружбы народов. Серия: Международные отношения*. 2022. Т. 22, № 2. С. 238–255. <https://doi.org/10.22363/2313-0660-2022-22-2-238-255>; EDN: KSSXFK
- Татулец С. А.* Формирование нового многополярного миропорядка в условиях глобальной информационной войны // *Информационное общество*. 2024. № 3. С. 2–9. EDN: TRSYZC
- Azad T. M., Haider M. W., Sadiq M.* Understanding Gray Zone Warfare from Multiple Perspectives // *World Affairs*. 2023. Vol. 186, no. 1. P. 81–104. <https://doi.org/10.1177/00438200221141101>; EDN: YPIWZD
- Bazarkina D. Y., Pashentsev E. N.* Artificial Intelligence and New Threats to International Psychological Security // *Russia in Global Affairs*. 2019. Vol. 17, no. 1. P. 147–170. <https://doi.org/10.31278/1810-6374-2019-17-1-147-170>; EDN: FYAQFW
- Bazarkina D. Y., Pashentsev E. N.* Malicious Use of Artificial Intelligence // *Russia in Global Affairs*. 2020. Vol. 18, no. 4 (72). P. 154–177. <https://doi.org/10.31278/1810-6374-2020-18-4-154-177>; EDN: ZZANTF

- Clarke R., Knake R. *Cyber War : The Next Threat to National Security and What to Do About It*. New York : Ecco, 2010.
- Goldstein J., Sastry G., Musser M., DiResta R., Gentzel M., Sedova K. *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*. Ithaca, NY : Cornell University, 2023. <https://doi.org/10.48550/arXiv.2301.04246>
- Hoyle A., van den Berg H., Doosje B., Kitzen M. *Grey Matters: Advancing a Psychological Effects-Based Approach to Countering Malicious Influence* // *New Perspectives*. 2021. Vol. 29, iss. 2. P. 144–164. <https://doi.org/10.1177/2336825X21995702>; EDN: VKURAA
- Li Q., Liu Q., Liu S., Di X., Chen S., Zhang H. *Influence of Social Bots in Information Warfare: A Case Study on @UAWeapons Twitter Account in the Context of Russia — Ukraine Conflict* // *Communication and the Public*. 2023. Vol. 8, iss. 2. P. 54–80. <https://doi.org/10.1177/20570473231166157>; EDN: BWKLRB
- Minor D. *Information War*. Boston : Hawthorne Books Publishing House, 1970.
- Ördén H. *The Neuropolitical Imaginaries of Cognitive Warfare* // *Security Dialogue*. 2024. Vol. 55, iss. 6. P. 607–624. <https://doi.org/10.1177/09670106241253527>; EDN: HIWMNY
- Pantserov K. A. *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability* // *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* / ed. by H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, J. Ibarra. Cham, Switzerland : Springer, 2020. P. 37–55. [https://doi.org/10.1007/978-3-030-35746-7\\_3](https://doi.org/10.1007/978-3-030-35746-7_3); EDN: IQCSJW
- Ventsel A., Hansson S., Madisson M.-L., Sazonov V. *Discourse of Fear in Strategic Narratives: The Case of Russia's Zapad War Games* // *Media, War & Conflict*. 2019. Vol. 14, iss. 1. P. 21–39. <https://doi.org/10.1177/1750635219856552>

#### **Сведения об авторах:**

Базавлук Сергей Викторович — кандидат политических наук, руководитель программ международного научного обмена, Национальный исследовательский институт развития коммуникаций (НИИРК); eLibrary SPIN-код: 3560-9701; ORCID: 0000-0002-9739-2594; e-mail: bazavluk@nicrus.ru

Ковалев Андрей Андреевич — кандидат политических наук, доцент, доцент кафедры государственного и муниципального управления, Северо-Западный институт управления — филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации; eLibrary SPIN-код: 1380-8790; ORCID: 0000-0002-7760-5732; e-mail: kovalev-aa@ranepa.ru