Архитектура цифровой гегемонии США: институты информационных войн как инструменты переформатирования реальности

Architecture of US Digital Hegemony: Institutions of Information Warfare as Instruments of Reformatting Reality

DOI: 10.12737/2587-6295-2025-9-2-216-235
УДК: 32.019.5
Получено: 01.06.2025 Одобрено: 09.06.2025 Опубликовано: 25.06.2025

Сорокин И.О.
Ассистент кафедры политологии, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», аспирант кафедры политического анализа и социально-психологических процессов, ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», г. Москва
e-mail: IOSorokin@fa.ru

Sorokin I.O.
Assistant of the Department of Political Science, Financial University under the Government of the Russian Federation, postgraduate student of the Department of Political Analysis and Socio-Psychological Processes, Plekhanov Russian University of Economics, Moscow
e-mail: IOSorokin@fa.ru

Аннотация
Статья посвящена изучению структуры американских институтов информационных войн как ключевого механизма трансформации общественного сознания и геополитических процессов современности. Цель работы — частично приоткрыть занавесу архитектуры (структуры) институтов информационного противоборства США как каркаса современной медийно-политической реальности. В основе исследования лежит междисциплинарный подход, сочетающий общенаучные методы и институциональный анализ (изучение формальных и неформальных структур цифровой гегемонии). В статье отмечается, что институты информационных войн США функционируют как системные акторы, объединяющие государственные, корпоративные и неформальные сети для достижения гегемонии в цифровом пространстве, их инструментарий включает не только дезинформацию, но и алгоритмическое управление вниманием, Big Data-аналитику и многие другие методы, за счет использования которых осуществляется подрыв доверия к институтам противника, в том числе к традиционным медиа, переформатируется реальность (изменяются общественные нормы, политические тренды и национальные идентичности), а также решаются иные поставленные задачи. Также делается вывод о том, что информационные войны перешли из тактического в стратегический режим, превратившись в инструмент долгосрочного перераспределения власти в глобальном масштабе. Теоретическая значимость работы заключается в синтезе подходов политической науки и медиаисследований, что позволяет предложить новые рамки для анализа реалий информационно-индустриального общества, кризиса демократических институтов и эволюции международных отношений в условиях доминирования глобальных цифровых платформ. Исследование актуально для понимания источников вызовов, связанных с цифровым неравенством, манипуляцией общественным

сознанием (массовой психологией) и поиском баланса между свободой информации и безопасностью.
Ключевые слова: информационные войны, цифровая гегемония, институты информационных войн, мозговые центры, ментальные войны, психологические войны.

Abstract
The article is devoted to the analysis of the structure of American information warfare institutions as a key mechanism of the transformation of public consciousness and modern geopolitical processes. The purpose of the work is to partially open the curtain of the architecture (structure) of the institutions of the information confrontation of the United States as the framework of modern media and political reality. The research is based on an interdisciplinary approach combining general scientific methods and institutional analysis (the study of formal and informal structures of digital hegemony). The article notes that the US information warfare institutions function as systemic actors that combine government, corporate and informal networks to achieve hegemony in the digital space. Their tools include not only disinformation, but also algorithmic attention management, Big Data analytics and many other methods that undermine confidence in enemy institutions, including traditional media, reformatting reality (social norms, political trends, and national identities are changing) and other assigned tasks are also being solved. It is also concluded that information warfare has shifted from a tactical to a strategic mode, becoming a tool for the long-term redistribution of power on a global scale. The theoretical significance of the work lies in the synthesis of approaches of political science and media research, which allows us to offer a new framework for analyzing the realities of the information-industrial society, the crisis of democratic institutions and the evolution of international relations in the context of the dominance of global digital platforms. The research is relevant for understanding the sources of challenges related to digital inequality, manipulation of public consciousness (mass psychology) and the search for a balance between freedom of information and security.
Keywords: information warfares, digital hegemony, information warfares institutions, think tanks, mental wars, psychological warfares.

Введение

Актуальность исследования обусловлена проведением недружественными государствами в настоящее время гибридной войны нового типа против России[1], включающей информационные операции институтов информационной войны США, и наличием пробела в систематизации всех элементов архитектуры американской цифровой гегемонии, поскольку, зачастую, научные работы по тематике информационного противоборства фокусируются на каком-либо одном вопросе — на исторических аспектах (Бернейс, Липпман, Сулейманова), на тактиках (Ридд, Аркилла, Люттвак), на технических нюансах (Расторгуев, Джейми, Шнайер, Морозов), либо на иной проблематике, но редко концептуализируют представление о таких институтах в целом. Данное исследование частично восполняет этот пробел, предлагая классификацию американских «игроков на поле» информационных войн.

Цель статьи — систематизировать архитектуру институтов информационных войн США.

Для этого решаются следующие задачи:

1) Выявить и классифицировать институты информационных войн США.
2) Охарактеризовать методы и программы их воздействия, обозначить связи между ними.
3) Обозначить роль научных и образовательных учреждений и академических программ США.
4) Определить последствия американской цифровой гегемонии.

[1] Указ Президента Российской Федерации от 31.03.2023 № 229 «Об утверждении Концепции внешней политики Российской Федерации» // Официальный интернет-портал правовой информации — URL: http://publication.pravo.gov.ru/Document/View/0001202303310007 (дата обращения: 10.05.2025).

Среди прочих в статье используются следующие специфические термины:

1) Цифровая гегемония — доминирование в информационном пространстве через контроль над данными, медиаплатформами и алгоритмами, обеспечивающее влияние на ценности и поведение целевых аудиторий (развитие концепции культурной гегемонии Антонио Грамши и других ученых применительно к цифровой среде [4]), а также в иных сферах информационного противоборства (например, развитие концепции превосходства в технотронную эру З. Бжезинского [19] и др.).

2) Гибридные конфликты — конфликты, сочетающие традиционные и нетрадиционные методы противостояния (войны) (кибератаки, пропаганду, поддержку прокси-групп и другие), стирающие границы между войной и миром (И.Н. Панарин [10], А.В. Манойло [9], М. Галеотти [21] и др.).

3) Алгоритмическое управление — использование алгоритмов для манипуляции информационными потоками, включая таргетирование контента, создание «фильтрующих пузырей» и автоматизацию дезинформационных кампаний (С.П. Расторгуев [13], Дж. Донован [20], Ш. Зубофф [5], Б. Шнайер [29], Дж. Бартлетт [18] и др.).

Статья вносит вклад в дискуссию о природе и формах власти в цифровую эпоху, предлагая междисциплинарный подход к изучению институтов, которые не просто адаптируются к технологическим изменениям, но и активно с их помощью конструируют новую политическую реальность.

Обзор научной литературы

Информационные войны, как феномен, уходящий корнями в классические теории массовых коммуникаций и пропаганды, сегодня переосмысливаются через призму цифровых технологий, что требует обращения как к фундаментальным работам прошлого, так и к современным исследованиям.

В научном дискурсе присутствует значительное число работ по тематике информационного противоборства, — выделяют не менее одиннадцати парадигм изучения информационных войн [14]: одни исследователи видят в них инструмент геополитического доминирования (И. Панарин, З. Бжезинский и проч.), другие — кризис эпистемической устойчивости общества (Ш. Зубофф, Т. Снайдер, Д.В. Биндас, Р.Т. Мухаев и проч.), третьи — рассматривают данный феномен со своей, иной, точки зрения.

Некоторые российские авторы, такие как И.Н. Панарин, А.В. Манойло и Р.Т. Мухаев акцентируют внимание на роли государств в конструировании информационного суверенитета, тогда как ряд западных теоретиков, например, М. Фуко и Ж. Деррида рассматривает власть как диффузную сеть дискурсивных практик. Особый интерес также представляют работы, связывающие информационные войны с «надзорным капитализмом» (Ш. Зубофф) и технологиями «цветных революций» (Д. Шарп, Дж. Голдстоун, Э. Люттвак и др.).

Говоря о фундаментальных работах, необходимо отметить, что еще в 1920-х годах Уолтер Липпман в книге *«Общественное мнение»* (1922) ввел понятие «стереотипа» как упрощенного образа, который медиа используют для управления сознанием. Липпман утверждал, что большинство людей воспринимают мир не напрямую, а через «псевдосреду» [7], созданную СМИ, — идея, предвосхитившая современные исследования «фильтрующих пузырей» и алгоритмической персонализации.

Параллельно Гарольд Лассуэлл, один из основателей теории коммуникации, в работе *«Техника пропаганды в мировой войне»* 1927 г. сформулировал базовую модель анализа медиавоздействия: кто говорит, что, по какому каналу, кому и с каким эффектом [6]. Его идеи легли в основу понимания пропаганды как инструмента управления массами, что сегодня актуально в контексте алгоритмического таргетирования информации. Позднее Лассуэлл подчеркивал, что контроль над информационными потоками позволяет элитам формировать «символическую идентичность» [22], определяющую восприятие реальности, — концепция, перекликающаяся с современной теорией Шошаны Зубофф [5] о «надзорном капитализме»,

где данные становятся инструментом прогнозирования и манипуляции поведением. Значительный вклад в развитие пропаганды внесли также Эдвард Бернейс и Айви Ли. Бернейс, племянник Зигмунда Фрейда, в книге «Пропаганда» 1928 г. обосновывал, что манипуляция общественным сознанием — неотъемлемая часть демократии, где *«сознательное и умелое манипулирование упорядоченными привычками и вкусами масс является важной составляющей демократического общества»* [1, с. 12].

Айви Ли, напротив, выступал за прозрачность и рассмотрение власти не как «игры с нулевой суммой», а как сторонник несекционной концепции власти (власть как коллективное действие), разработав первый этический кодекс PR (*«Декларация принципов»*), но его же обвиняли в *«отмывании»* репутации корпораций — эта двойственность отражает извечный конфликт между манипуляцией и диалогом в информационном пространстве [28].

Их тезисы развивал Пол Лазарсфельд, изучавший в середине XX в. роль медиа в электоральном поведении. В работе *«Выбор народа»* (1944) Лазарсфельд показал, что влияние СМИ опосредуется «лидерами мнений», что сегодня трансформировалось в феномен цифровых инфлюенсеров, используемых в информационных войнах для распространения нужных заказчику нарративов [23].

Структурный анализ институтов информационного влияния прямо и (или) опосредованно также представлен в работах многих российских и зарубежных авторов. Отечественные исследователи информационной и гибридной войны, например, такие как И.Н. Панарин и А.В. Манойло обращают особое внимание на государственные органы информационной (гибридной) войны Запада против России, — оба они пишут о роли ЦРУ, УСС и других американских государственных учреждений в информационном противоборстве, в частности, и против России, но также особое место в их трудах отводится и описанию участия некоторых негосударственных институтов, например, таких как Фонд Карнеги, Фонд Рокфеллера, Фонд Сороса и другим [9, 10].

Иностранные специалисты в своих трудах тоже не обошли стороной архитектуру информационного противоборства США, — так, указанные выше работы дополняются эмпирическими трудами американских исследователей Брюса Шнайера и Евгения Морозова, которые раскрывают технические механизмы эксплуатации данных. Шнайер в *«Data and Goliath»* (2015) описывает, как корпорации и государства используют «информационную асимметрию» для контроля над поведением [29], а Морозов в *«The Net Delusion»* (2012) предупреждает, что цифровые технологии усиливают авторитаризм, создавая иллюзию свободы [25]. В свою очередь аналитики признанной[2] в России нежелательной организации RAND Corporation («РЭНД Корпорэйшн») Томас Рид, Кристофер Пол, Алисса Демус, Элизабет Бодин-Бэрон, Кейтлин Маккаллох, Райан Бауэр, Джонатан Фудзивара, Бенджамин Дж. Сакс, Майкл Швилл, Марселла Моррис и Келли Бивен в исследовательском отчете[3] 2024 г. «Operationalizing U.S. Air Force Information Warfare» для Военно-воздушных сил США в разделе «Current Organization» приводят ряд институтов, участвующих в информационной войне, а именно: Агентство национальной безопасности США (АНБ), Министерство обороны США, Киберкомандование (CYBERCOM), EUCOM, SPACECOM, STRATCOM и др. Упомянутый ранее среди авторов этого исследовательского отчета Т. Рид еще до этого исследования в 2020 г. в своей книге «Active measures» акцентировал внимание на роли Пентагона, ЦРУ, USAID и других американских институтов, занимающихся ведением кампаний по дезинформации, в особенности против России [27].

Особый пласт исследований информационного противоборства связан с технологиями «цветных революций» и «ненасильственного сопротивления». Джин Шарп в работе *«От диктатуры к демократии»* (1993) систематизировал методы свержения режимов через

[2] Перечень иностранных и международных организаций, деятельность которых признана нежелательной на территории Российской Федерации (Минюст России) — URL: https://minjust.gov.ru/ru/documents/7756/ (дата обращения: 27.05.2025).

[3]Operationalizing U.S. Air Force Information Warfare (RAND Corporation) — URL: https://www.rand.org/pubs/research_reports/RRA1740-1.html (дата обращения 27.05.2025).

мобилизацию гражданского общества [16], что позже было адаптировано к цифровой эре в форме сетевых кампаний. Его идеи повлияли на деятельность НКО, связанных с Джорджем Соросом (белорусский политолог Юрий Воскресенский пишет[4], что деятельность Сороса и Шарпа — своего рода разделение труда на стратегию и тактику), чей фонд Open Society Foundation финансирует проекты по продвижению «демократии». Ряд проницательных авторов, например, таких как Игорь Стечкин (эксперт ONYQ) и И.Н. Панарин, видят в этом форму «цифрового колониализма», где так называемые «западные ценности» навязываются под видом гуманитарной, интеллектуальной, организационной и иной помощи.

Важный вклад в понимание институциональной архитектуры информационных войн внес Джозеф Най мл., автор концепции «мягкой силы». Най подчеркивает роль медиагигантов (по типу CNN, NYT) и университетских программ (например, в Гарварде и других ведущих вузах) в глобальном продвижении американских ценностей [26]. В свою очередь Джон Аркилла описывает эволюцию сетевых моделей управления, разработанных в том числе RAND Corporation и DARPA [17], а Джейми Бартлетт в *«The People vs. Tech»* (2018) предупреждает, что цифровые платформы разрушают общественный договор, заменяя его алгоритмической поляризацией [18].

Таким образом, эволюция теорий информационных войн и институтов, их организующих и реализующих, демонстрирует, что от классических моделей пропаганды (Лассуэлл, Липпман) наука перешла к анализу сложных сетевых систем, где государственные акторы, корпорации и гражданское общество конкурируют за контроль над нарративами. При этом сохраняются фундаментальные противоречия: является ли информация оружием или ресурсом диалога, зависит ли ее воздействие от культурного контекста или универсальных алгоритмов, можно ли отделить манипуляцию от свободного обмена идеями.

Эти вопросы остаются открытыми, но именно их обсуждение формирует основу для поиска баланса между безопасностью и свободой в цифровую эпоху, а также позволяет приоткрыть занавесу архитектуры цифровой гегемонии, которая несмотря на наличие обширного перечня научной литературы, остается не в полной мере систематизированной и не охватывает всех элементов архитектуры информационных войн. Данное исследование частично восполняет этот пробел, предлагая комплексную классификацию игроков и их взаимодействия.

Методы

Исследование базируется на междисциплинарном подходе, сочетающем общенаучные методы, методы политического анализа и качественного изучения открытых источников. Каждый из них применялся в совокупности с другими, обеспечивая минимизацию субъективности интерпретаций. Основные этапы работы включали:

1) Сбор данных и их изучение (выявление институтов информационных войн) - анализ отечественной и зарубежной научной литературы, документов государственных органов (официальные сайты Госдепа, USAID, USCYBERCOM, DARPA и иных), изучение сайтов корпораций (Meta*[5], Google, Microsoft и иных) и материалов НПО (RAND, NED, Freedom House*[6], Open Society Foundation*[7] и иных), мониторинг медиаконтента ключевых

[4] "Сорос - стратегия, а Шарп - тактика": Воскресенский объяснил, чем различаются методички авторов — URL: https://news.by/news/obshchestvo/soros-strategiya-a-sharp-taktika-voskresenskiy-obyasnil-chem-razlichayutsya-metodichki-avtorov (дата обращения: 31.05.2025).

[5] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

[6] Freedom House* — Генпрокуратура РФ признала нежелательной в России деятельность американской неправительственной организации Freedom House.

[7] Open Society Foundation* — Генпрокуратура РФ признала нежелательной в России деятельность американской неправительственной организации Open Society Foundation.

СМИ (CNN, NYT, Reuters и иных) и цифровых платформ (Telegram, Meta*[8], X (Twitter), Вконтакте и иных).

2) Систематизация информации - классификация институтов информационных войн по категориям с выделением некоторых их функций и методов воздействия (таблицы 1-7), указание некоторых взаимосвязей между данными структурами (например, координация Госдепа, USAID и Meta*[9]).

3) Историко-сравнительный анализ - ретроспектива развития технологий информационного влияния (от PR Эдварда Бернейса до алгоритмов DARPA). Сравнение методов Холодной войны (радио «Свобода») и современных операций (Tik-Tok-нарративы).

4) Примеры (кейс-стади / case-study) - исследование конкретных случаев (ситуаций, кейсов), таких как блокировка RT и Sputnik, DDoS-атаки, кампании Global Engagement Center (GEC).

Интеграция методов позволила выявить не только структурные особенности институтов, но и их адаптацию к культурным контекстам, что подтвердило гипотезу о переходе информационных войн из тактического в стратегический режим.

Результаты анализа

В основной части статьи более подробно рассмотрены американские институты, участвующие в информационных войнах. Для наглядности материал представлен в виде семи таблиц с основными государственными и корпоративными институтами, аналитическими центрами и университетами, хакерскими формированиями и цифровыми инфлюенсерами, оказывающими значительное влияние на восприятие и распространение деструктивных для России нарративов, а также ведущих иную подрывную деятельность в отношении Российской Федерации и других государств.

Необходимо отметить, что эта статья носит обзорный характер и не претендует на исчерпывающий охват всех участников (институтов) информационных войн США, — далеко за рамками остаются малоизвестные некоммерческие и неправительственные организации (НКО, НПО), аналитические стартапы и медиа, которые, безусловно, также вносят свой вклад в архитектуру цифровой гегемонии. По оценке Игоря Стечкина[10], еще в 1989 г. в США уже функционировала так называемая «тавистокская сеть», включающая в себя 10-20 крупных учреждений, 400-500 средних учреждений и около 5000 связанных с ними мелких учреждений, в которых работало суммарно более шестидесяти тысяч специалистов в областях поведенческих наук, управления сознанием, социологических опросов, формирования общественного мнения. С тех пор масштаб изменился только в сторону увеличения. Вместе с тем, автором была предпринята попытка их систематизации и анализа в общем виде, в результате чего было выявлено, что институциональной основой информационных войн США является многоуровневая система правительственных и неправительственных организаций, а также хакерских группировок и отдельных лидеров общественного мнения (инфлюенсеров), направленная на подавление суверенитета других стран и выполнение иных целей и задач.

Основными институтами информационной войны против России являются военно-разведывательные структуры США, объединяющие технологические, оперативные и аналитические ресурсы для сбора разведданных, дестабилизации критической инфраструктуры, психологического воздействия и иных задач, которые требуется выполнять для ведения гибридной войны, а также для кураторства над остальными институтами информационного противоборства США.

---

[8] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

[9] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

[10] День ТВ. Секреты Тавистокского института. Заговор психиатров на деньги Рокфеллеров. И. Стечкин — URL: https://rutube.ru/video/38f13684722bce91d7b69984652abbd0/ (дата обращения: 23.04.2025).

Необходимо отметить, что в период специальной военной операции (СВО) деятельность институтов ведущих информационную войну против России приобрела особенно масштабный и агрессивный характер, что можно проиллюстрировать данными статистики МВД России, которые свидетельствуют о том, что в период с 2022 по 2024 гг. произошло заметное увеличение числа зарегистрированных противоправных действий, осуществленных с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации[11], — так, в 2022 г. их было немногим более полумиллиона, а в 2024 г. уже 765,4 тыс.[12] Безусловно, не все они относятся к организованным извне, однако упускать из виду такой источник угроз явно не стоит, особенно с учетом столь стремительной динамики роста их числа именно в период СВО и регулярных комментариев[13] от российских госструктур и госслужащих о сотнях мошеннических колл-центров, действующих из-за рубежа.

Также стоит обратить особое внимание на количество и структуру зарегистрированных инцидентов, — так, по данным компании «Ростелеком-Солар»[14], в 2022 г. количество кибератак на сервисы и российские организации не только возросло на 700% по сравнению с годом ранее, но и наиболее подверженными атакам стали именно ФОИВы (примерно каждая пятая атака), ГИС (каждая шестая — каждая седьмая атака), медиаплатформы (примерно каждая седьмая атака), сервисы для населения (каждая десятая атака) и иные организации (рис. 1).

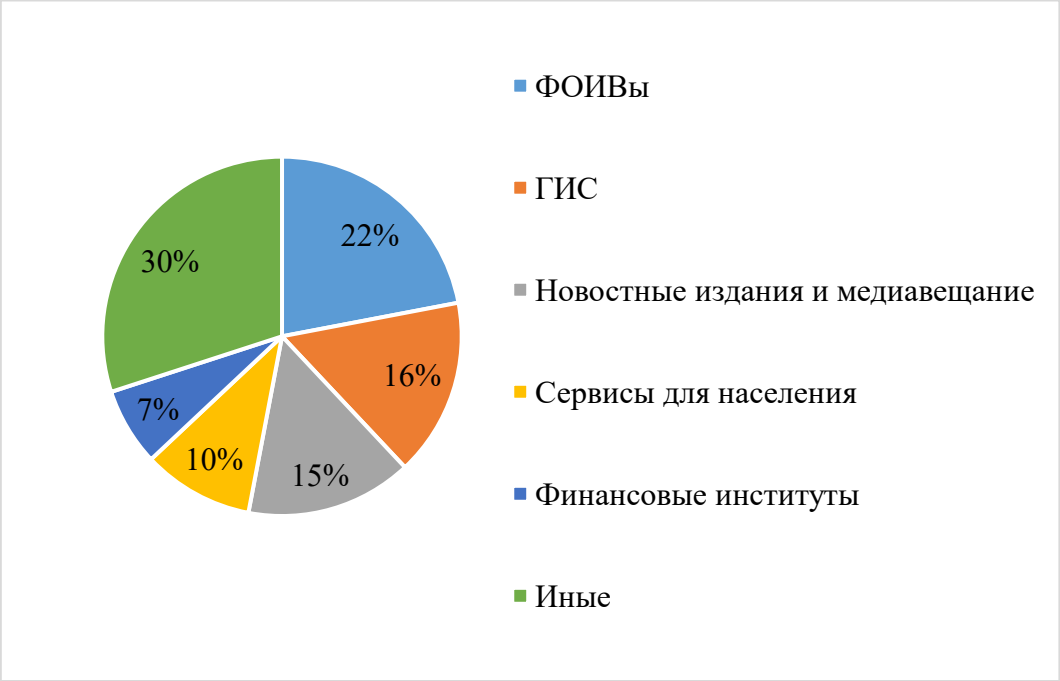

Рис. 1. Структура кибератак на российские информационные ресурсы в 2022 г.

Среди ключевых американских военно-разведывательных органов, курирующих другие институты информационных войн, исходя из миссий, представленных на их официальных сайтах, анализа научной литературы и новостей можно выделить следующие: Пентагон или Министерство обороны США (U.S. Department of Defense, Pentagon), которое является одним

[11] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2022 года (статистика МВД России) — URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 25.04.2025).
[12] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года (статистика МВД России) — URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 31.05.2025).
[13] В МВД назвали количество действующих на Украине мошеннических кол-центров — URL: https://www.gazeta.ru/social/news/2025/05/21/25834844.shtml (дата обращения: 31.05.2025).
[14] Количество кибератак на сервисы и структуры России в 2022 году выросло в семь раз (ТАСС) — URL: https://tass.ru/ekonomika/17327093 (дата обращения: 25.04.2025).

из ключевых организующих звеньев во всей военно-разведывательной сети США, US Cyber Command (USCYBERCOM), которое выступает ключевым оператором кибератак, подчиняясь напрямую Пентагону[15], Агентство национальной безопасности[16] (АНБ), специализирующееся на глобальном сборе сигнальной разведки (SIGINT, например, через программу PRISM, по информации от Эдварда Сноудена, опубликованной в российских СМИ[17], с помощью которой АНБ получает доступ к данным Meta*[18], Google, Microsoft и других корпораций, отслеживая коммуникации в том числе российских граждан, военных и чиновников), подразделение TAO (Tailored Access Operations) осуществляющее целевые взломы[19], ЦРУ, фокусирующееся на внешней разведке (в том числе цифровой) и информационных операциях[20] (например, в период СВО ЦРУ активизировало кампанию по распространению фейков о «военных преступлениях» России через подконтрольные им СМИ и Telegram-каналы, в том числе финансируемые через USAID в качестве «организации-прокладки»[21], также был создан официальный телеграмм-канал ЦРУ, на котором граждан России открыто призывали к предательству и активному сотрудничеству с американской внешней разведкой[22]), Разведывательное управление Минобороны (DIA), Агентство перспективных оборонных проектов (DARPA) и другие (см. таблицу 1).

Таблица 1

Некоторые органы военно-разведывательного комплекса США, участвующие в информационной войне

Категория	Институт	Примеры методов/программ
Управление и координация	Пентагон, Министерство обороны США (U.S. Department of Defense, Pentagon)	Программы по типу «Семантическая криминалистика» для выявления фейковых новостей и видеозаписей, созданных с помощью технологии deepfake и их создания[23]
Кибероперации	US Cyber Command (USCYBERCOM)	Операции по типу «Glowing Symphony»[24];

[15] U.S. Cyber Command official website. [Электронный ресурс]. URL: https://www.cybercom.mil (дата обращения: 20.05.2025).

[16] U.S. National Security Agency/Central Security Service official website. [Электронный ресурс]. URL: https://www.nsa.gov/ (дата обращения: 20.05.2025).

[17] Prism - глобальная машина наблюдения: как США уничтожают свободу в мире. [Электронный ресурс]. URL: https://regnum.ru/article/1669976 (дата обращения: 20.05.2025).

[18] Meta* (социальные сети Instagram* и Facebook*) – экстремистская организация, деятельность которой запрещена в России.

[19] TAO. [Электронный ресурс]. URL: https://www.securitylab.ru/glossary/tao/ (дата обращения: 20.05.2025).

[20] U.S. Central Intelligence Agency official website. [Электронный ресурс]. URL: https://www.cia.gov/ (дата обращения: 20.05.2025).

[21] Инструмент «цветных революций»: как USAID под эгидой помощи финансирует информационную войну с Россией. [Электронный ресурс]. URL: https://russiatoday.ru/russia/article/1437244-usaid-rossiya-informatsyia-voina-finansirovanie (дата обращения: 31.05.2025).

[22] ЦРУ создало телеграмм-канал для вербовки россиян. [Электронный ресурс]. URL: https://www.rbc.ru/politics/16/05/2023/64631ee69a79476b1bc3b760 (дата обращения 31.05.2025).

[23] «Новый виток информационных войн»: зачем Пентагону программа по противодействию фейковым новостям. — URL: https://russian.rt.com/world/article/664229-pentagon-feiki-informatsiya (дата обращения 31.05.2025).

[24] Cyber Operations in Russia's War against Ukraine. URL — https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf (дата обращения 20.05.2025).

Категория	Институт	Примеры методов/программ
		Поиск уязвимостей в цифровой инфраструктуре
Глобальный сбор сигнальной разведки (SIGINT), криптоанализ, массовая слежка	АНБ (NSA)	Программа PRISM (массовая слежка через соцсети — доступ к данным Meta*[25], Google, Microsoft для мониторинга коммуникаций российских граждан и чиновников). Взлом спутниковых сетей и энергосистем, иные методы
Внешняя разведка, в том числе цифровая разведка и психологические операции	ЦРУ (CIA)	Вербовка россиян через Telegram-канал. Взлом Telegram-каналов и аккаунтов пользователей[26]. Операции по созданию сети «экспертов», продвигающих определенные нарративы (по типу «Integrity Initiative»)[27].
Военная разведка	Разведуправление Минобороны США (DIA)	Анализ военных и иных возможностей России[28]; Публикация аналитических документов по типу «Worldwide Threat Assessment» с акцентом на угрозы со стороны России[29]
Спецоперации	JSOC (объединенное командование)	Операции по типу «Timber Sycamore» (поддержка антиправительственных сил)[30][31]
Технологии манипуляции	DARPA	Программы по типу SMISC (2011г.) (автоматизированный анализ социальных сетей), SocialSim (2017г.)

[25] Meta* (социальные сети Instagram* и Facebook*) – экстремистская организация, деятельность которой запрещена в России.

[26] CIA Able to Access Encrypted Data on Telegram, WhatsApp — URL: https://sputnikglobe.com/20170307/cia-wikileaks-telegram-whatsapp-1051348537.html (дата обращения 20.05.2025).

[27] Do it CIA style: What you need to know about latest leak on UK-funded psyop — URL: https://www.rt.com/news/446809-integrity-initiative-third-leak-uk/?ysclid=mawticxdqv20602708 (дата обращения 20.05.2025).

[28] Официальный сайт Разведуправления Минобороны США (US DIA). — URL: https://www.dia.mil/About/ (дата обращения: 26.05.2025).

[29] Ежегодный аналитический доклад Разведуправления Минобороны США «Annual threat assessment». — URL: https://www.congress.gov/118/meeting/house/117088/witnesses/HHRG-118-AS26-Wstate-KruseJ-20240411.pdf (дата обращения: 26.05.2025).

[30] Официальный сайт Единого оперативного командования войсками специального назначения США (USSOCOM). — URL: https://www.socom.mil/ussocom-enterprise/components/joint-special-operations-command (дата обращения: 26.05.2025).

[31] Timber Sycamore: The CIA’s Syrian Regime Change Operation. — URL: https://www.militaryhistory.info/timber-sycamore-the-cias-syrian-regime-change-operation/ (дата обращения: 26.05.2025).

Категория	Институт	Примеры методов/программ
		(моделирование поведения), INCAS (2020 г.) (Influence Campaign Awareness and Sensemaking). Narrative Analytics (аналитика нарративов и подмена смыслов)
Контрразведка	ФБР (FBI)	Программы по типу «Foreign Influence Task Force» (расследования «российского вмешательства»)[32]
Геопространственная разведка	NGA (Национальное агентство геопространственной разведки)	Спутниковый мониторинг военных объектов России (информационно-техническая война)

Как было отмечено ранее, государственные институты США, входящие в американский военно-разведывательный комплекс, играют системообразующую роль в информационной войне против России, часть из них была приведена в таблице 1. Однако не все из них напрямую входят в него, — некоторые подчиняются военно-разведывательному комплексу (были учреждены и (или) финансируются им и (или) подотчетны ему) или действуют параллельно, при этом используя, например, законодательные, финансовые и регуляторные рычаги для многоуровневого давления с целью изоляции российских медиа, продвижения прозападных нарративов и создания правовой основы для цифровой цензуры.

Так, например, Госдепартамент, через свой Global Engagement Center (GEC), координирует контрпропагандистские кампании, выделяя миллионы долларов на проекты, которые публикуют «разоблачения» о России[33], а доклады GEC, такие как «The kremlins never ending attempt to spread disinformation about biological weapons» формируют единый антироссийский нарратив о «военных преступлениях», лжи российских СМИ и официальных лиц[34].

Минфин США (через Управление по контролю за иностранными активами, OFAC) вводит санкции против российских медиа[35], включая RT и Sputnik, блокируя их доступ к международным финансовым системам (включение этих СМИ в список SDN (Specially Designated Nationals) также привело к отключению их от рекламных платформ Google и Meta*[36] и сокращению доходов российской компании, равно как и персональные санкции против медиаменеджеров, таких как Маргарита Симоньян, еще больше ограничили операционные возможности российских медиа). Широко известное в последнее время Агентство США по международному развитию (USAID) финансирует разнообразные прозападные медиапроекты на постсоветском пространстве и по всему остальному миру.

[32] FBI And Its Foreign Influence Task Force Purged Sources Who Were Onto Biden Corruption. — URL: https://thefederalist.com/2023/10/26/fbi-and-its-foreign-influence-task-force-purged-sources-who-were-onto-biden-corruption/ (дата обращения: 26.05.2025).

[33] Госдеп создаёт специальный фонд для спонсирования антироссийских СМИ. — URL: https://life.ru/p/1106948 (дата обращения: 26.05.2025).

[34] Запись из официального русскоязычного телеграмм-аккаунта Государственного Департамента США — URL: https://t.me/USApoRusski/1253 (дата обращения: 30.05.2025).

[35] США ввели санкции против медиагруппы "Россия сегодня". — URL: https://ria.ru/20240904/sanktsii-1970637108.html (дата обращения: 30.05.2025).

[36] Meta* (социальные сети Instagram* и Facebook*) – экстремистская организация, деятельность которой запрещена в России.

Согласно материалам Russia Today от 20 февраля 2025 г.: «Более 6,2 тыс. журналистов из 707 редакций и 279 «медийных» неправительственных организаций получали деньги от Агентства США по международному развитию»[37]. Некоторые из этих госорганов США, участвующих в информационной войне, в том числе против России, представлены в таб.2.

Таблица 2

Иные государственные органы США, участвующие в информационной войне

Категория	Институт	Примеры методов/программ
Контрпропаганда	Госдеп (GEC)	Гранты по типу StopFake Ukraine, доклады по типу «The kremlins never ending attempt to spread disinformation about biological weapons» и т.п.
Финансирование НПО	USAID	Проекты по финансированию СМИ, журналистов и иных лидеров общественного мнения для продвижения необходимых нарративов и т.п.
Кибербезопасность	CISA	Программа «Shields Up» (защита инфраструктуры), блокировка Russian Today и т.п.
Санкции	Минфин США (OFAC)	Блокировка RT, Sputnik через Specially Designated Nationals List и т.п.
Глобальные медиа	U.S. Agency for Global Media (USAGM)	Управление Radio Free Europe/Radio Liberty, Voice of America (антироссийские нарративы) и т.п.

Аналитические центры или think-tanks США служат интеллектуальным фундаментом информационных войн, разрабатывая стратегии, нарративы и технологии для манипуляции общественным сознанием. Такие структуры как Council on Foreign Relations (CFR), RAND Corporation и Atlantic Council (обе признаны в России нежелательными организациями) формируют глобальную политику, продвигая изоляцию России через доклады вроде *«Containing Russia»*[38].

RAND Corporation и Atlantic Council (обе признаны в России нежелательными организациями) фокусируются на тактиках гибридных конфликтов: RAND исследует алгоритмы TikTok для дезориентации общества[39], а Atlantic Council через DFRLab координирует маркировку «враждебного контента» с IT-гигантами[40].

Также особую роль играют центры, специализирующиеся на психологических операциях и социальной инженерии. Некоторые такие институты приведены в таблице 3.

[37] Инструмент «цветных революций»: как USAID под эгидой помощи финансирует информационную войну с Россией. — URL: https://russiatoday.ru/russia/article/1437244-usaid-rossiya-informatsyia-voina-finansirovanie (дата обращения 31.05.2025).

[38] Containing Russia. Council Special Report from U.S. Foreign Policy Program and Europe Program. — URL: https://www.cfr.org/report/containing-russia (дата обращения 31.05.2025).

[39] TikTok Is a Threat to National Security, but Not for the Reason You Think. — URL: https://www.rand.org/pubs/commentary/2024/08/tiktok-is-a-threat-to-national-security-but-not-for.html (дата обращения 31.05.2025).

[40] Wartime content moderation and the Russian invasion of Ukraine. — URL: https://dfrlab.org/event/wartime-content-moderation/ (дата обращения: 31.05.2025).

Таблица 3

Некоторые think-tanks и аналитические центры США, участвующие в информационной войне

Категория	Институт	Примеры методов/программ
Психологические исследования	Сеть Тавистокского института в США	Исследования групповой динамики и манипуляции сознанием; Участие в проектах НАТО по психологическим операциям.
Социальная инженерия	Фонд Джозайи Мэйси младшего (Macy Foundation)	Финансирование программ по изменению поведения через образование и медицину.
Стратегии сдерживания	Council on Foreign Relations (CFR)	Доклады по типу «Containing Russia» и иная активность.
Антироссийская аналитика	Atlantic Council	Проект DFRLab (мониторинг «российских ботов») и маркировка «враждебного контента» совместно с IT-гигантами.
Глобальные нарративы	RAND Corporation	Исследования по типу «TikTok Is a Threat to National Security».

Таблица 4 раскрывает структуру участия других негосударственных (неправительственных) организаций (НПО, НКО) и транснациональных корпораций (ТНК) в информационной войне против России, акцентируя внимание на их роли в формировании антироссийских нарративов и подавлении альтернативных точек зрения.

Например, Национальный фонд в поддержку демократии (NED) (также признанный в РФ нежелательной организацией, причем первым — еще в июле 2015 г.) выделяет[41] гранты структурам вроде также признанной в России нежелательной организацией — «Free Russia Foundation», поддерживающей протестные движения, а Meta*[42], и Google разрабатывают алгоритмы для манипуляции контентом и поисковой выдачей[43][44][45][46][47].

Более системно информация по ним представлена в таблице 4.

[41] Поддержка «активистов» и нужных СМИ: на какие проекты в РФ американский фонд потратил около $1 млн в 2019 году — URL: https://russian.rt.com/world/article/696122-ned-fond-ssha-granty-rossiya (дата обращения: 31.05.2025).

[42] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

[43] Еврокомиссия оштрафовала Google почти на €2,5 млрд. — URL: https://www.rbc.ru/business/27/06/2017/59522f089a7947cd7bf06f05 (дата обращения: 31.05.2025).

[44] European Commission. Commission fines Google €2.42 billion. — URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1784 (дата обращения: 31.05.2025).

[45] Минюст США подал иск против Google из-за «монополии» на рынке поисковых систем. — URL: https://vc.ru/legal/168884-minyust-ssha-podal-isk-protiv-google-iz-za-monopolii-na-rynke-poiskovyh-sistem (дата обращения: 31.05.2025).

[46] Justice Department Sues Monopolist Google For Violating Antitrust Laws. — URL: https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws (дата обращения: 31.05.2025).

[47] В Общественной палате назвали справедливым штраф Facebook. — URL: https://lenta.ru/news/2021/12/24/oprf/ (дата обращения: 31.05.2025).

Таблица 4

Некоторые НПО и корпорации США, участвующие в информационной войне

Категория	Институт	Примеры методов/программ
Финансирование оппозиции	National Endowment for Democracy (NED)	Гранты НПО, например, «Free Russia Foundation», поддержка Telegram-каналов оппозиции.
Финансирование оппозиции	Open Society Foundation	Финансирование программ по типу «Media Freedom Initiative» (обучение журналистов).
Цензура платформ	Meta (Facebook, Instagram)	Манипуляции контентом (цензура и дезинформация, распространение запрещенного российским судом контента).
Цензура платформ	Google (YouTube)	Проект «Project Shield» (блокировка доменов), манипуляция поисковой выдачей, распространение запрещенного российским судом контента, демонетизация каналов авторов из России и иные.
Цензура платформ	Microsoft	Отключение сервисов Azure для РФ, блокировка RT и Sputnik в LinkedIn.
Цензура платформ	X (Twitter)	Алгоритм «Freedom of Speech Not Reach» (ограничение видимости аккаунтов)[48].
Цензура платформ	Apple	Цензура приложений в App Store под предлогом «безопасности»[49].
Глобальные СМИ (продвижение нарративов)	Reuters, Associated Press и иные	Публикация статей о «военных преступлениях России» с непроверенными источниками.
Телевизионные сети (продвижение нарративов)	CNN, Fox News, NBC, CBS, ABC, etc.	Трансляция репортажей с акцентом на «российскую агрессию».
Печатные издания (продвижение нарративов)	New York Times, Washington Post, Bloomberg, etc.	Статьи о «коррупции в Кремле» и «нарушениях прав человека».
«Филантропия влияния»	Фонд Рокфеллера	Финансирование проектов по «борьбе с дезинформацией» через НПО.

[48] Свобода слова по Илону Маску. Социальная сеть Twitter отчиталась о работе программы Freedom of Speech Not Reach — URL: https://www.ixbt.com/news/2023/07/13/twitter-freedom-of-speech-not-reach.html (дата обращения: 31.05.2025).

[49] Новые санкции против владельцев iPhone и iPad. Их втихую лишили приложения «Авито». Решение найдено. Опрос — URL: https://www.cnews.ru/news/top/2025-05-29_novye_sanktsii_applevladeltsev (дата обращения: 31.05.2025).

Категория	Институт	Примеры методов/программ
		Финансирование в США сети Тавистокского института человеческих отношений.
«Филантропия влияния»	Фонд Карнеги за международный мир	Аналитические статьи по типу «Is the Global Tide Turning in Favor of Democracy?»[50]. Доклады по типу «Пределы роста»[51].

Еще одной важной группой американских институтов информационных войн являются университеты и академические институты, которые готовят кадры для информационных операций и других направлений гибридной войны.

Так, например, Гарвард проводит исследования по дезинформации, Йель продвигает нарративы об «экономическом забвении» России, а MIT разрабатывает инструменты цензуры. Более системно информация по ним представлена в таблице 5.

Таблица 5

Некоторые университеты и академические программы США, участвующие в информационной войне

Категория	Институт	Примеры методов/программ
Исследования влияния	Гарвардский университет	Исследования по типу «Search engine manipulation to spread pro-Kremlin propaganda»[52] и образовательные программы по типу «Digital Propaganda Analysis»[53].
Продвижение нарративов	Йельский университет	Исследования по типу «Business Retreats and Sanctions Are Crippling the Russian Economy», убеждающие в «экономическом забвении» России[54].
Регуляция контента	MIT	Программа «Internet Policy Research Initiative» (разработка инструментов цензуры в связке с политиками и технологическими компаниями)[55].
Подготовка кадров по кибероперациям	Стэнфордский университет	Курсы «Cyber Policy Center» (обучение кибероперациям).
Психологические операции	Национальный институт психического	Исследования по воздействию соцсетей на психику подростков. Программы по типу «Социальные медиа и депрессия».

[50] Is the Global Tide Turning in Favor of Democracy? — URL: https://carnegieendowment.org/research/2023/05/is-the-global-tide-turning-in-favor-of-democracy?lang=en (дата обращения: 31.05.2025).

[51] The Limits to Growth — URL: https://www.clubofrome.org/publication/the-limits-to-growth/ (дата обращения: 31.05.2025).

[52]Search engine manipulation to spread pro-Kremlin propaganda — URL: https://misinforeview.hks.harvard.edu/article/search-engine-manipulation-to-spread-pro-kremlin-propaganda/ (дата обращения: 31.05.2025).

[53] Propaganda Education for a Digital Age — URL: https://www.gse.harvard.edu/ideas/edcast/21/03/propaganda-education-digital-age (дата обращения: 31.05.2025).

[54] Chief Executive Leadership Institute Research Insights: “Business Retreats and Sanctions Are Crippling the Russian Economy” — URL: https://som.yale.edu/story/2022/chief-executive-leadership-institute-research-insights-business-retreats-and-sanctions (дата обращения: 31.05.2025).

[55] Internet Policy Research Initiative — URL: https://internetpolicy.mit.edu/ (дата обращения: 31.05.2025).

Категория	Институт	Примеры методов/программ
	здоровья США (NIMH)	
Групповая динамика	Центр исследования групповой динамики MIT (Research Center for Group Dynamics, RCGD)	Работы Курта Левина по управлению поведением групп. Эксперименты по влиянию авторитета.
Культурная антропология	Институт социальных исследований (Мичиган)	Исследования Маргарет Мид по манипуляции культурными стереотипами.

Таблица 6 приоткрывает занавесу роли неформальных структур, хакерских группировок (кибергруппировок) в информационной войне на стороне США. Необходимо отметить, что не первый год иностранные хакеры и хактивисты ищут «уязвимости нулевого дня» в офисном программном обеспечении (ПО) и российских операционных системах (ОС), при этом их действия становятся все более сложноорганизованными — наблюдается переход от «хактивизма» к целенаправленным атакам[56].

Таблица 6

Некоторые неформальные структуры и кибергруппировки, участвующие в информационной войне

Категория	Институт/Группа	Примеры методов/программ
Хактивизм	Хакерские группировки по типу Anonymous, Lizard Squad и иные	DDoS-атаки на госорганы, компании, объекты энергетики и иные объекты критической информационной инфраструктуры, поиск «уязвимостей нулевого дня» в ОС и офисном ПО.
Хактивизм	Сообщества по типу «IT Army of Ukraine» и иные	Координация атак на российские сайты (t.me/itarmyofukraine2022).
Фейковые расследования	Сообщества по типу Molfar и иные	Составление базы данных «российских военных преступников» с поддельными фото (https://t.me/yigal_levin/68887).

В таблице 7 в качестве примера приведены несколько значимых американских цифровых инфлюенсеров и медиабрендов, участвующих в информационной войне против России. Эти акторы используют специфические особенности цифровых площадок, такие как алгоритмическая персонализация и виральность контента для максимизации охвата аудитории.

Например, Ben Shapiro, выступающий на YouTube и X (ранее Twitter), сочетает консервативный дискурс с ежедневным охватом в несколько миллионов пользователей, продвигая тезисы о «российской агрессии» в формате аналитических видео, которые позиционируются как объективные, но содержат одностороннюю интерпретацию событий.

[56] Программа Инфофорума-2023. [Электронный ресурс]. URL: https://infoforum.ru/programma-infoforuma-2023 (дата обращения: 31.05.2025).

Таблица 7

Некоторые цифровые инфлюенсеры и медийные бренды, участвующие в информационной войне

Имя / Бренд	Платформа	Особенности влияния	Примеры контента
Ben Shapiro	YouTube, X	Критика «российской агрессии»	Интервью с Владимиром Зеленским.
The Young Turks (TYT)	YouTube, Facebook	Поддержка санкций против России, краудфандинг	Стримы по типу «Excusing War Crimes».
Hasan Piker (HasanAbi)	Twitch, Instagram, TikTok, Facebook	Видео для молодежи об «ужасах войны»	Ролики по типу «What ACTUALLY BAD Takes On Ukraine Look Like».
Philip DeFranco	YouTube	«Нейтральный» обзор новостей с акцентом на западные нарративы (либо на антироссийские нарративы и (или) против других государств)	Видео по типу «Russia Threatens South Africa With War» (фейковая аналитика).

Выводы

Таким образом, проведенный анализ демонстрирует, что информационная война США против России представляет собой многоуровневую систему, интегрирующую государственные, корпоративные, академические и неформальные структуры.

Ее ядро формирует взаимосвязанные между собой уровни, действующие в рамках единой стратегии цифровой гегемонии, а именно:

1) Военно-разведывательный комплекс как основа гибридных операций. Военные и разведывательные структуры США (Пентагон, USCYBERCOM, ЦРУ, DARPA и другие) разрабатывают технологии для кибератак, психологических операций и контроля над информационным пространством, а также координируют деятельность других акторов. Например, программа SocialSim (DARPA) моделирует поведение пользователей в соцсетях для прогнозирования протестных волн, а Narrative Analytics подменяет смыслы медиаконтента с помощью ИИ. Операции по типу «Glowing Symphony» (USCYBERCOM) направлены на атаки критической инфраструктуры, включая энергосети, что сочетается с дезинформацией о «вине Кремля» через подконтрольные СМИ. При этом координация между агентствами усиливает эффект: данные АНБ о слабых точках инфраструктуры РФ могут передаваться USCYBERCOM для точечных ударов, а ЦРУ синхронизирует пропаганду через Telegram-каналы и НПО и осуществляет сбор информации на территории противника.

2) Иные государственные институты: законодательная и финансовая поддержка цензуры. Госдеп (через GEC) и USAID финансируют проекты по продвижению антироссийских нарративов, Минфин США блокирует доступ российских медиа (RT, Sputnik) к международным финансовым системам, а CISA и FCC внедряют инструменты цифровой цензуры, маркируя российские домены как «опасные». Эти меры дополняются координацией с IT-гигантами: алгоритмы Meta*[57] (Risk Mitigation Protocol) скрывают контент об СВО, а Google (Project Shield) блокирует пророссийские ресурсы под предлогом борьбы с «дезинформацией».

[57] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

3) Корпорации и НПО: контроль цифровой экосистемы. Технологические корпорации (Meta*[58], Google, Microsoft и другие) играют ключевую роль в подавлении альтернативных точек зрения. Например, Microsoft отключает сервисы Azure для РФ, а Apple удаляет неугодные приложения из App Store под предлогом «безопасности». Глобальные СМИ (Reuters, CNN и другие) тиражируют непроверенные данные о «военных преступлениях РФ», создавая эмоционально заряженные нарративы через короткие ролики, которые охватывают миллионы подписчиков. НПО, такие как нежелательные в России NED и Open Society Foundation, маскируют политические цели под гуманитарные инициативы.

4) Академические центры и аналитические структуры составляют идеологический фундамент и кадровую базу. Университеты (Гарвард, MIT, Стэнфорд и другие) и think-tanks (RAND*[59], Atlantic Council*[60] и т.д.) создают научную основу для манипуляции сознанием и готовят кадры для различных операций, — например, Гарвардский университет проводит исследования по «российской дезинформации», Йель продвигает нарративы об «экономическом забвении» России, а Стэнфордский Cyber Policy Center и MIT готовят кадры для кибероперации, RAND анализирует алгоритмы TikTok для использования в своих целях, сеть Тавистокского института разрабатывает методы управления групповой динамикой.

5) Неформальные структуры и инфлюенсеры. Хакерские группы (Anonymous, Lizard Squad, IT Army of Ukraine и другие) и неформальные организации дополняют давление через DDoS-атаки, фейковые расследования и эксплуатацию тем психического здоровья. Например, IT Army of Ukraine координирует кибератаки через Telegram-ботов, а Molfar создает базы данных с поддельными фото «российских военных преступников». Инфлюенсеры (Ben Shapiro, Philip DeFranco и другие) маскируют пропаганду под «нейтральный анализ», формируя альтернативные системы доверия.

Работа охватывает лишь малую часть акторов информационной войны США, опираясь на открытые данные. Например, остаются за рамками более сотни признанных в России нежелательных организаций, почти тысяча иноагентов, малоизвестные аналитические стартапы и «тавистокская сеть», включающая тысячи специалистов по управлению сознанием. Тем не менее, выявленные механизмы подтверждают, что современные информационные войны — это сложнейшие явления, являющиеся в том числе войнами за восприятие, где границы между фактом и интерпретацией, государством и корпорацией, войной и миром целенаправленно размываются.

Проведённое исследование показывает, что США стремятся к асимметричному контролю над глобальным информационным пространством, используя инструменты «мягкой силы» и технологическое превосходство, при этом происходит переход информационных войн из тактического в стратегический режим, что превращает их в инструмент перераспределения власти на долгосрочный период в глобальном масштабе благодаря системной координации институтов (военно-разведывательного комплекса, государственных органов, корпораций и think-tanks и иных).

Таким образом, архитектура цифровой гегемонии США представляет собой синтез технологий, пропаганды и силового давления, осуществляемый различными институтами, направленный на переформатирование реальности в интересах глобального американского доминирования. Однако ответные меры России и рост альтернативных блоков (по типу БРИКС) указывают на неизбежность трансформации миропорядка, где информационное пространство останется одним из ключевых полей битвы за будущее.

---

[58] Meta* (социальные сети Instagram* и Facebook*) — экстремистская организация, деятельность которой запрещена в России.

[59] RAND Corporation* — Генпрокуратура РФ признала нежелательной в России деятельность американской неправительственной организации RAND Corporation.

[60] Atlantic Council * — Генпрокуратура РФ признала нежелательной в России деятельность американской неправительственной организации Atlantic Council.

Литература

1. Бернейс Э. Пропаганда / Пер. с англ. И. Ющенко. М.: Hippo Publishing, 2010. - 176 с.
2. Гарр Т.Р. Почему люди бунтуют. СПб.: Питер, 2005. - 461 с.
3. Голдстоун Д. Революции. Очень краткое введение / Пер. с англ. А. Яковлева. М.: Изд-во Института Гайдара, 2017. - 200 с.
4. Грамши А. Тюремные тетради: [Пер. с итал.] / Антонио Грамши; [Вступ. ст. М. Н. Грецкого, с. 5-22]. М.: Политиздат, 1991. Ч. 1. - 559 с.
5. Зубофф Ш. Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти / Шошана Зубофф; пер. с англ. А.Ф. Васильева; под ред. Я. Охонько и А. Смирнова. - М.: Издательство Института Гайдара, 2022. - 784 с.
6. Лассуэлл Г.Д. Техника пропаганды в мировой войне: перевод с англ. / Г.Д. Лассуэлл; РАН. ИНИОН (сост. и переводчик В.Г. Николаев). - М., 2021. - 237 с.
7. Липпман У. Общественное мнение; пер. с англ. Т.В. Барчуновой; Фонд «Обществ. Мнение». М.: Ин-т Фонда «Обществ. Мнение», 2004. - 382 с.
8. Люттвак Э. Государственный переворот: Практическое пособие / Пер. с англ. М.: Русский Фонд Содействия Образованию и Науке, 2012. - 326 с.
9. Манойло А.В. Информационные операции современной гибридной войны: учебное пособие. М.: Горячая линия - Телеком, 2023. - 490 с.
10. Панарин И.Н. Гибридная война и Ялта-2. - М.: Горячая линия - Телеком, 2022. - 452 с.
11. Почепцов Г.Г. Информационные войны. Новый инструмент политики. - М.: Алгоритм, 2015. - 254 с.
12. Почепцов Г.Г. Революция.com. Основы протестной инженерии. - М.: Европа, 2005. - 532 с.
13. Расторгуев С.П. Информационная война. - М.: Радио и связь, 1999. - 416 с.
14. Сорокин И.О. Информационные войны как феномен постиндустриального (информационного) общества: основные парадигмы // Журнал политических исследований. - 2025. – Т. 9. - № 1. - С. 25-40. DOI: https://doi.org/10.12737/2587-6295-2025-9-1-25-40 (дата обращения: 31.05.2025).
15. Сулейманова Ш.С., Назарова Е.А. Информационные войны: история и современность: Учебное пособие. М.: Международный издательский центр «Этносоциум», 2017. - 124 с.
16. Шарп Д. От диктатуры к демократии: Стратегия и тактика освобождения / Пер. с англ. Н. Козловской. М.: Новое издательство, 2005. - 84 с.
17. Arquilla J., Ronfeldt D. (Eds.). Networks and Netwars: The Future of Terror, Crime, and Militancy. Санта-Моника: RAND Corporation, 2001. - 372 p.
18. Bartlett J. The People Vs Tech: How the Internet Is Killing Democracy (and How We Save It). London: Ebury Press, 2018. - 231 p.
19. Brzezinski Z. Between Two Ages: America's Role in the Technetronic Era. New York: The Viking Press, 1970. - 334 p.
20. Donovan J., Dreyfuss E., Friedberg B. Meme Wars: The Untold Story of the Online Battles Upending Democracy in America. UK: Bloomsbury Publishing, 2022. - 432 p.
21. Galeotti, M. Hybrid, ambiguous, and non-linear? How new is Russia’s ‘new way of war’? Small Wars & Insurgencies, 2016, V. 27, I. 2, P. 282–301. https://doi.org/10.1080/09592318.2015.1129170
22. Lasswell H. The Signature of Power: Buildings, Communication, and Policy. New York: Taylor & Francis, 1979. pp. 8-9.
23. Lazarsfeld P.F., Berelson B., Gaudet H. The People’s Choice: How the Voter Makes Up His Mind in a Presidential Campaign. 2nd ed. New York: Columbia University Press, 1948. - 224 p.
24. Libicki M.C. What is Information Warfare? Washington: National Defense University, 1995. - 110 p.
25. Morozov E. The Net Delusion: The Dark Side of Internet Freedom. UK: Public Affairs, 2012. - 448 p.
26. Nye J. Soft power: The Means to success in world politics. New York: Public Affairs, 2004. - 191 p.

27. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux, 2020. - 512 p.
28. Russell K., Bishop C. Understanding Ivy Lee's Declaration of Principles: U.S. Newspaper and Magazine Coverage of Publicity and Press Agentry, 1865-1904. Public Relations Review, 2009, V. 35, I. 2, pp. 91-101. DOI: 10.1016/J.PUBREV.2009.01.004.
29. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. USA: W. W. Norton, 2015. - 400 p.

References

1. Bernays E. Propaganda [Propaganda]. Moscow, Hippo Publishing Publ., 2010, 176 p. (In Russian).
2. Garr T.R. Pochemu lyudi buntuyut [Why Men Rebel]. St. Petersburg, Piter Publ., 2005, 461 p. (In Russian).
3. Goldston D. Revolyucii. Ochen' kratkoe vvedenie [Revolutions: A Very Short Introduction]. Moscow, Izd-vo Instituta Gaydara Publ., 2017, 200 p. (In Russian).
4. Gramsci A. Tyuremnye tetradi [Prison Notebooks]. Moscow, Politizdat Publ., 1991, Ch. 1, 559 p. (In Russian).
5. Zuboff Sh. Epoha nadzornogo kapitalizma. Bitva za chelovecheskoe budushchee na novyh rubezhah vlasti [The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power]. Moscow, Izdatel'stvo Instituta Gaydara Publ., 2022, 784 p. (In Russian).
6. Lassuell G.D. Tehnika propagandy v mirovoj vojne [Propaganda Technique in the World War]. Moscow Publ., 2021, 237 p. (In Russian).
7. Lippmann U. Obshchestvennoe mnenie [Public Opinion]. Moscow, In-t Fonda «Obshchestv. Mnenie» Publ., 2004, 382 p. (In Russian).
8. Luttvak E. Gosudarstvennyj perevorot: Prakticheskoe posobie [Coup d'État: A Practical Handbook]. Moscow, Russkij Fond Sodejstviya Obrazovaniyu i Nauke Publ., 2012, 326 p. (In Russian).
9. Manojlo A.V. Informacionnye operacii sovremennoj gibridnoj vojny [Information Operations of Modern Hybrid Warfare]. Moscow, Goryachaya liniya - Telekom Publ., 2023, 490 p. (In Russian).
10. Panarin I.N. Gibridnaya vojna i Yalta-2 [Hybrid War and Yalta-2]. Moscow, Goryachaya liniya - Telekom Publ., 2022, 452 p. (In Russian).
11. Pochepcov G.G. Informacionnye vojny. Novyj instrument politiki [Information Wars. A New Tool of Politics]. Moscow, Algoritm Publ., 2015, 254 p. (In Russian).
12. Pochepcov G.G. Revolyuciya.com. Osnovy protestnoj inzhenerii [Revolution.com. Basics of Protest Engineering]. Moscow, Evropa Publ., 2005, 532 p. (In Russian).
13. Rastorguev S.P. Informacionnaya vojna [Information Warfare]. Moscow, Radio i svyaz' Publ., 1999, 416 p. (In Russian).
14. Sorokin I.O. Informacionnye vojny kak fenomen postindustrial'nogo (informacionnogo) obshchestva: osnovnye paradigmy [Information Wars as a Phenomenon of Post-Industrial (Information) Society: Main Paradigms]. Zhurnal politicheskih issledovanij [Journal of Political Research], 2025, V. 9, I. 1, pp. 25-40. DOI: https://doi.org/10.12737/2587-6295-2025-9-1-25-40 (In Russian). Accessed: 31.05.2025.
15. Sulejmanova Sh.S., Nazarova E.A. Informacionnye vojny: istoriya i sovremennost' [Information Wars: History and Modernity]. Moscow, Mezhdunarodnyj izdatel'skij centr «Etnosocium» Publ., 2017, 124 p. (In Russian).
16. Sharp D. Ot diktatury k demokratii: Strategiya i taktika osvobozhdeniya [From Dictatorship to Democracy]. Moscow, Novoe izdatel'stvo Publ., 2005, 84 p. (In Russian).
17. Arquilla J., Ronfeldt D. (Eds.). Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, RAND Corporation Publ., 2001, 372 p.
18. Bartlett J. The People Vs Tech: How the Internet Is Killing Democracy (and How We Save It). London, Ebury Press Publ., 2018, 231 p.

19. Brzezinski Z. Between Two Ages: America's Role in the Technetronic Era. New York, The Viking Press Publ., 1970, 334 p.
20. Donovan J., Dreyfuss E., Friedberg B. Meme Wars: The Untold Story of the Online Battles Upending Democracy in America. London, Bloomsbury Publishing Publ., 2022, 432 p.
21. Galeotti, M. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? Small Wars & Insurgencies, 2016, V. 27, I. 2, pp. 282–301. DOI: https://doi.org/10.1080/09592318.2015.1129170
22. Lasswell H. The Signature of Power: Buildings, Communication, and Policy. New York, Taylor & Francis Publ., 1979, pp. 8-9.
23. Lazarsfeld P.F., Berelson B., Gaudet H. The People's Choice: How the Voter Makes Up His Mind in a Presidential Campaign. 2nd ed. New York, Columbia University Press Publ., 1948.
24. Libicki M.C. What is Information Warfare? Washington, National Defense University Publ., 1995, 110 p.
25. Morozov E. The Net Delusion: The Dark Side of Internet Freedom. New York, Public Affairs Publ., 2012, 448 p.
26. Nye J. Soft power: The Means to success in world politics. New York, Public Affairs Publ., 2004, 191 p.
27. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York, Farrar, Straus and Giroux Publ., 2020, 512 p.
28. Russell K., Bishop C. Understanding Ivy Lee's Declaration of Principles: U.S. Newspaper and Magazine Coverage of Publicity and Press Agentry, 1865-1904. Public Relations Review, 2009, V. 35, I. 2, pp. 91-101. doi: 10.1016/J.PUBREV.2009.01.004.
29. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York, W. W. Norton Publ., 2015, 400 p.