ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2025-15-2-99-113
УДК 327.7:004.056(045)

Эволюция концепции информационной войны в нормативных правовых актах России, США и НАТО

И.О. Сорокин
Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация;
РЭУ им. Г.В. Плеханова, Москва, Российская Федерация

АННОТАЦИЯ

Современный мир постоянно находится в состоянии информационного противоборства, что делает исследование феномена информационной войны крайне актуальным. *Цель* статьи — анализ эволюции концепции информационной войны в нормативных правовых актах России, США и НАТО. В работе используются *методы* анализа, синтеза, дедукции, индукции, сравнения, а также историко-политический анализ, что позволяет сопоставить документы, отражающие поэтапное изменение подходов к информационному противоборству в различных правовых системах. В работе представлена эволюция нормативных правовых актов и доктринальных документов по тематике информационного противоборства, выявлены их содержательные особенности, сходства и различия, проведена их классификация. Особое внимание уделено правовым определениям понятий «информационная война», «информационные операции», «психологические операции», «кибероперации», «когнитивная война» в контексте стратегий национальной безопасности и военных доктрин указанных субъектов политики. Делается *вывод*, что существуют концептуальные различия в правовом закреплении феномена информационной войны: в западной традиции информационные операции достаточно давно и широко отражены в правовых документах. Начиная с середины XX в. с появлением ядерного оружия и ростом роли некинетических средств поражения противника они рассматривались инструментально и преимущественно в виде психологических операций, однако в дальнейшем, в результате технологических и социальных изменений, получили расширительную трактовку, включив в себя аспекты кибероперации и когнитивной войны, и в настоящее время представляют собой неотъемлемый элемент гибридных войн, осуществляющихся не только в военное, но и в мирное время, тогда как в российском законодательстве нет понятия информационной войны, — его можно вывести только опосредованно, а в самих документах подчеркивается защитная функция и суверенная составляющая информационного пространства на основе традиционных ценностей. В рамках исследования созданы три таблицы, позволяющие наглядно представить ключевые сходства, различия и эволюцию развития концепции информационной войны в нормативных правовых актах США, НАТО и России. *Теоретическая значимость работы* заключается в том, что она способствует пониманию динамики эволюции концепции информационных войн в различных правовых системах и может быть полезна специалистам в области международного права, исследователям информационного противоборства и иным заинтересованным лицам.

Ключевые слова: информационная война; информационные операции; психологическая война; когнитивная война; гибридная война; нормативное правовое обеспечение информационной войны; доктрина; полевой устав

***Для цитирования*: Сорокин И.О. Эволюция концепции информационной войны в нормативных правовых актах России, США и НАТО. *Гуманитарные науки. Вестник Финансового университета*. 2025;15(2):99-113. DOI: 10.26794/2226-7867-2025-15-2-99-113**

ORIGINAL PAPER

The Evolution of the Concept of Information Warfare in the Regulatory Legal Acts of Russia, United States and NATO

I.O. Sorokin
Financial University under the Government of the Russian Federation, Moscow, Russian Federation;
Plekhanov Russian University of Economics, Moscow, Russian Federation

ABSTRACT

The modern world is constantly in a state of information warfare, which makes the study of the phenomenon of information warfare extremely relevant. The purpose of the article is to analyze the evolution of the concept of information warfare in the regulatory legal acts of Russia, United States and NATO. The work uses methods of analysis, synthesis, deduction, induction, comparison, as well as historical and political analysis, which are used to compare documents reflecting the gradual change

in approaches to information warfare in various legal systems. The paper presents the evolution of normative legal acts and doctrinal documents on the subject of information warfare, identifies their substantive features, similarities and differences, and classifies them. Special attention is paid to the legal definitions of the concepts of "information warfare", "information operations", "psychological operations", "cyber operations", "cognitive warfare" in the context of national security strategies and military doctrines of these policy actors. It is concluded that there are conceptual differences in the legal definition of the phenomenon of information warfare: in the Western tradition, information operations have been widely reflected in legal documents for a long time, – since the middle of the 20th century, due to the advent of nuclear weapons and the increasing role of non-kinetic means of defeating the enemy, they were considered instrumentally and mainly in the form of psychological operations, but later, as a result of technological and social changes, they received an expanded interpretation, including aspects of cyber operations and cognitive warfare, and currently represent an integral element of hybrid warfares that take place not only in wartime, but also in peacetime, whereas in Russian legislation there is no term of information warfare, – it can only be derived indirectly, and the documents themselves emphasize the protective function and sovereign component of the information space based on traditional values. As part of the research, three tables have been created to visually present the key similarities, differences, and evolution of the concept of information warfare in the regulatory legal acts of United States, NATO, and Russia. The theoretical significance of the work lies in the fact that it contributes to understanding the dynamics of the evolution of the concept of information warfare in various legal systems and may be useful to specialists in the field of international law, researchers of information warfare and other interested parties.

Keywords: information warfare; information operations; psychological warfare; cognitive warfare; hybrid warfare; regulatory legal support for information warfare; doctrine; field manual

***For citation*: Sorokin I.O. The evolution of the concept of information warfare in the regulatory legal acts of Russia, United States and NATO. *Humanities and Social Sciences. Bulletin of the Financial University.* 2025;15(2):99-113. DOI: 10.26794/2226-7867-2025-15-2-99-113**

ВВЕДЕНИЕ

Современная международная обстановка демонстрирует возрастающее значение информационного пространства как арены геополитического противостояния. Концепция «информационной войны» эволюционировала от инструментального подхода, рассматривающего информационные операции исключительно в контексте военных действий, к комплексному пониманию информационного противоборства как составной части гибридных конфликтов и национальной безопасности. Различные государства и военно-политические блоки по-разному интерпретируют и закрепляют данный феномен в своих нормативных правовых актах и доктринальных документах, что делает актуальным их сравнительный анализ.

Целью данной статьи является изучение эволюции концепции «информационной войны» в нормативных правовых актах России, США и НАТО. Основное внимание уделяется выявлению содержательных особенностей документов, сравнению подходов к правовому регулированию информационного противоборства.

Для достижения данной цели в работе применяется метод историко-политического анализа в совокупности с общенаучными методами, которые позволяют выявить сходства и различия в нормативном закреплении концепции «информационной войны». Особое внимание уделено правовым определениям, используемым в стратегиях национальной безопасности, военных доктринах и иных нормативных актах. Исследование демонстрирует, что в западной традиции информационные операции давно институционализированы в правовых документах и рассматриваются как один из элементов активных гибридных войн. В российском же законодательстве отсутствует прямое закрепление термина «информационная война», но можно выявить его опосредованно через концепции информационной безопасности и защиты суверенного информационного пространства.

В контексте исследования важно кратко пояснить ключевые термины:

Информационная война — это комплекс целенаправленных действий в информационном пространстве, включающий в себя дезинформацию, кибератаки, психологическое воздействие и другие методы, основанные на использовании возможностей цифровых средств коммуникации, направленные на ослабление противника. В разных правовых системах трактовка этого термина существенно различается.

Информационные операции — составные части информационных войн; совокупность мероприятий, направленных на сбор, обработку и распространение данных в политических целях. В военных доктринах США и НАТО этот термин включает в себя кибероперации, психологические операции и стратегические коммуникации.

Гибридная война — концепция, объединяющая традиционные военные действия с использованием невоенных инструментов, включая информационные атаки, экономическое давление и политическое манипулирование.

Таким образом, исследование позволит выявить закономерности эволюции правового регулирова-

ния информационного противоборства и систематизировать различия в подходах России, США и НАТО к данному феномену.

ОБЗОР НАУЧНОЙ ЛИТЕРАТУРЫ И НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Концепция «информационной войны» (ИВ) занимает ключевое место в политической науке, международных отношениях и военной стратегии. В зависимости от исследовательской традиции и национальной доктрины термин трактуется поразному. В западных научных работах преобладают концепции, связывающие информационную войну с когнитивным воздействием [1–6], кибероперациями [7–9], стратегическими и межкультурными коммуникациями [10] и гибридными конфликтами. В российском научном дискурсе доминирует представление об ИВ как элементе геополитического [11–13], цифрового [14], психологического [15–18] противоборства и средстве обеспечения национальной безопасности[1].

Современные исследования указывают на неотъемлемую связь ИВ и гибридных войн. В западной политологии она рассматривается в контексте «серых зон» [19], где конфликты ведутся без явного объявления войны. В российском научном дискурсе ИВ также рассматривается весьма широко — классифицированы как минимум одиннадцать точек зрения (парадигм) (они приведены в отдельной статье автора) [20], но одними из самых распространенных являются подходы, описывающие ее как информационно-психологическое влияние, направленное на управление массовым сознанием или как информационно-техническое воздействие, осуществляющееся в отношении технических систем (ЭВМ, сетей связи и т.п.).

В международной практике ИВ также рассматривается как в узком, так и в широком смысле. Согласно подходу НАТО, информационная война является частью концепции «стратегических коммуникаций». В американских военных доктринах термин «Information Warfare» эволюционировал в сторону комплексного подхода к информационным операциям, включающим кибероперации, пропаганду и психологические операции. В российской Доктрине информационной безопасности ИВ определяется через призму угроз информационной безопасности.

Эволюция концепций «информационной войны» и «психологической войны» начинается с середины XX в., когда в условиях появления ядерного оружия и начала «Холодной войны» стала доминировать идея психологического воздействия на противника. Первые нормативные акты, такие как National Security Act (1947) и Smith-Mundt Act (1948), заложили основы для координации пропаганды и информационных операций в США. Военные руководства, такие как FM 33–5 Psychological warfare in combat operations (1949) и FM 33–5 Psychological operations techniques and procedures (1966), подчеркивали практическое применение психологической войны в боевых условиях. В 1980-е гг., с принятием Executive Order 12333 (1981), информационные операции стали активнее интегрироваться в деятельность разведывательных служб, что ознаменовало начало сближения понятий «психологической» и «информационной» войны.

К середине 90-х гг. прошлого века с появлением FM 100–5 Operations (1993) и FM 100–6 Information Operations (1996) информация стала рассматриваться как ключевой ресурс в военных операциях (переход к сетецентрической войне). Документ JP 3–13 Joint Doctrine for Information Operations (1998) закрепил комплексный подход, включающий электронную войну, кибероперации и психологическое воздействие. В 2000-е гг., с обновлением руководств, таких как FM 3–13 (100–6) Information Operations (2003) и FM 3–05.30 (MCRP 3–40.6) Psychological Operations (2005), акцент сместился на интеграцию информационных операций в современные военные кампании и осуществление информационного воздействия на целевые аудитории в рамках военных и миротворческих миссий (влияние на восприятие, эмоции, суждения и поведение враждебных, нейтральных или дружественных групп населения) — документы подчеркивают важность PSYOP в достижении стратегических, оперативных и тактических задач, например, в снижении боевого духа противника, формировании положительного отношения к союзническим войскам среди местного населения и поддержке дипломатических инициатив. Также FM 3–05.30 (MCRP 3–40.6) описывает организацию подразделений PSYOP, их взаимодействие с другими военными структурами и государственными ведомствами и методы распространения информации, включая печатные материалы, радио- и телетрансляции, интернет-пропаганду и личные контакты. Отдельное внимание уделяется анализу

[1] Дугин А.Г. Геополитика: учебное пособие для вузов. М.: Академический Проект; Гаудеамус; 2011. 583 с.; Манойло А.В. Информационные операции современной гибридной войны: учебное пособие. М.: Горячая линия — Телеком; 2023. 90 с.; Мухаев Р.Т. Медиаполитика: учебник. М.: ИНФРА-М; 2024. 401 с.

целевой аудитории, разработке эффективных сообщений и оценке результатов операций.

Руководство FMI 2–22.9 Open source intelligence (2006) подчеркнуло роль открытых источников информации в стратегическом планировании и осуществлении информационного противоборства. В нем описаны методы сбора, обработки и анализа информации, получаемой из общедоступных источников, таких как СМИ, интернет, официальные документы, научные публикации, социальные сети и коммерческие базы данных. Документ подчеркивает, что OSINT стал важной частью разведывательной деятельности и может дополнять информацию, полученную из закрытых источников, таких как сигнальная разведка (SIGINT) или агентурная разведка (HUMINT). В нем рассматриваются принципы и инструменты сбора данных, методы оценки достоверности информации, а также способы интеграции OSINT в общий разведывательный процесс. Особое внимание уделяется правовым и этическим аспектам работы с открытыми источниками, включая вопросы авторских прав, сбора данных в международной среде и защиты конфиденциальности. Также рассматриваются технологические инструменты, такие как автоматизированные системы мониторинга СМИ, аналитические платформы и методы работы с большими объемами данных.

В 2010-е гг. концепция информационной войны получила дальнейшее развитие. Документы JP 3–13 Information Operations (2012–2014), FM 3–13 Inform and Influence Activities (2013), FM 3–13 (JP) Information Operations (2014) и FM 3–13 Information operations (2016) развили комплексный подход, включающий стратегическую коммуникацию, кибероперации и психологическое воздействие, а Joint Publication 3–12 (2018) акцентировала внимание на кибербезопасности и информационном противодействии.

Современный этап развития концепций связан с появлением термина «когнитивная война». Документы, такие как FM 3–0 Operations (2022), подчеркивают интеграцию информационных операций в глобальную стратегию безопасности — в данном документе концепции информационной войны, психологических операций, когнитивной войны и кибероперацій находят отражение, но в контексте современной многодоменной операции (MDO — Multi-Domain Operations). Этот доктринальный документ описывает, как армия США адаптируется к изменяющейся стратегической среде, включая конкуренцию в информационном пространстве, в том числе киберпространстве.

НАТО, будучи во многом более глобальным отголоском США, подходит к ИВ через призму стратегических коммуникаций (StratCom). Концепция информационной войны в НАТО эволюционировала от классических психологических операций (PsyOps) к более комплексным подходам, включающим стратегические коммуникации (StratCom), информационные операции (IO) и когнитивную войну (Cognitive Warfare). Исторически НАТО рассматривало информационные операции как часть традиционного военного противостояния, однако в начале XXI в. в альянсе усилилось осознание того, что информационные угрозы не ограничиваются вооруженными конфликтами, а оказывают влияние и в мирное время.

В 2010 г. НАТО утвердило «Военную концепцию стратегических коммуникаций» (NATO Military Concept for Strategic Communications 2010), в которой информационные операции, публичная дипломатия, работа со СМИ и психологические операции объединены в единую систему стратегических коммуникаций. Этот подход стал основой для дальнейшего развития информационной политики альянса.

В 2014 г., после возвращения Россией Крыма и начала киевским режимом варварского конфликта на востоке Украины, НАТО значительно усилило работу в сфере «информационной безопасности». В новой редакции доктрины JP 3–13 Information Operations (2014) подчеркивалось, что борьба за информационное пространство является неотъемлемым элементом современной войны,— альянс еще более активно начал использовать информационные технологии и социальные сети для формирования общественного мнения и продвижения своих интересов.

В 2022 г. НАТО представило новую «Стратегическую концепцию» (NATO Strategic Concept 2022), в которой информационному противоборству отведено ключевое место. В документе отмечается, что дезинформация, кибератаки и гибридные угрозы стали главными инструментами геополитического соперничества. Альянс подтвердил свою готовность «противодействовать» этим вызовам, усиливая сотрудничество с партнерами, развивая механизмы киберзащиты и совершенствуя доктринальные подходы к ведению информационной войны.

Отдельного внимания заслуживает концепция когнитивной войны НАТО, подробно рассмотренная в статье Кристофера Деппа «Cognitive Warfare: A Conceptual Analysis» (2024) [21], в которой подчеркивается, что в современных конфликтах основным полем

битвы становится человеческое сознание. Влияние на восприятие, эмоции, поведение и систему ценностей противника становится важнейшей задачей. Когнитивная война охватывает широкий спектр инструментов — от пропаганды и манипуляции информацией до использования технологий искусственного интеллекта и нейропсихологии для прогнозирования и управления общественными настроениями.

Современные стратегии НАТО в области информационной войны направлены не только на защиту собственных коммуникационных систем, но и на активное воздействие на информационную среду противников. Альянс активно развивает сотрудничество с технологическими компаниями, аналитическими центрами и медиаструктурами, стремясь создавать устойчивые механизмы воздействия и противодействия дезинформации и когнитивным атакам. В этом контексте информационные операции становятся не просто важным элементом военной стратегии, но ключевым инструментом глобальной политики, позволяющим НАТО формировать выгодное информационное пространство и добиваться стратегических целей без применения традиционной военной силы.

В России нормативное закрепление концепции ИВ произошло значительно позже. В отечественной политологии термин «информационная война» интерпретируется через призму национальной безопасности. В этом контексте Совет Безопасности Российской Федерации относит к основополагающим документам в сфере безопасности Конституцию РФ, Федеральный закон № 390-ФЗ «О безопасности» (2010), Военную доктрину РФ (2014), Доктрину информационной безопасности РФ (2000, 2016), Стратегию национальной безопасности РФ (2021), Концепцию внешней политики РФ (2023) и иные акты, представленные на его сайте[2].

Российские нормативные акты рассматривают ИВ в широком смысле, включая: противодействие деструктивному информационному воздействию, защиту традиционных духовно-нравственных ценностей, информационный контроль в киберпространстве.

Одним из ключевых документов является Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.[3] В ней сформулированы три основных принципа: свобода выбора средств получения информации, приоритет традиционных ценностей, законность и защита персональных данных.

Также отдельного внимания заслуживает Доктрина информационной безопасности Российской Федерации (2000, 2016)[4]. В редакции 2000 г. впервые были введены ключевые понятия: информационная безопасность как часть национальной безопасности, противодействие угрозам в информационном пространстве, государственный контроль над информационными потоками. В 2016 г. доктрина была обновлена, получив дальнейшее развитие. В ее рамках сформулирована концепция «единой системы контроля и обеспечения безопасности», направленная на выявление и нейтрализацию угроз на федеральном, региональном и муниципальном уровнях.

В число ключевых документов России в сфере ИБ, помимо вышеуказанных, входят: Закон «Об информации, информационных технологиях и о защите информации»[5] (2006), Концепция Конвенции ООН об обеспечении международной информационной безопасности, Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления критически важных объектов, Концепция информационной безопасности детей, Конвенция о преступности в сфере компьютерной информации ETS N 185.

Российская нормативно-правовая база в области информационной безопасности основывается на традиционных ценностях, что подчеркивается и в Указе Президента РФ, определяющем семнадцать ключевых духовно-нравственных ориентиров российского общества (2022)[6]. В этом контексте информационная война рассматривается не только как борьба в киберпространстве, но и как элемент идеологического и культурного противостояния.

Таким образом, краткий сравнительный анализ научной литературы и нормативных правовых актов России, США и НАТО показывает, что в российском и западном дискурсе существуют принципиаль-

[2] Совет Безопасности Российской Федерации. URL: http://www.scrf.gov.ru

[3] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». URL: https://base.garant.ru/71670570/?sclid=mbp1819j29580597128

[4] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: https://base.garant.ru/71556224/?sclid=mbp1cfz9yr124270435

[5] Федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп.) «Об информации, информационных технологиях и о защите информации». URL: https://base.garant.ru/12148555/?ysclid=mbp1gm5650635818021

[6] Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». URL: https://www.garant.ru/products/ipo/prime/doc/405579061/?ysclid=mbp1qg49a6447160078

но разные подходы к трактовке ИВ: если в Штатах и Североатлантическом альянсе акцент делается на тактическом и стратегическом активном применении информационных технологий, то в России этот феномен рассматривается как угроза национальной безопасности и ответные действия, в связи с чем представляется важным провести более детальный разбор эволюции концепции информационной войны в данных субъектах политики с опорой на нормативные правовые акты.

МЕТОДЫ

В статье используются следующие методы исследования:

1. Анализ — проявляется в детальном рассмотрении различных аспектов концепции информационной войны. Автор разбивает тему на составные части, чтобы изучить каждую из них отдельно. Например, исследуются нормативные документы (доктрины НАТО, американские военные руководства, российские законы), чтобы выявить их ключевые положения и эволюцию подходов к ИВ.

2. Синтез — в работе происходит соединение данных из различных источников и контекстов, чтобы сформировать целостное понимание темы: интегрируются подходы западных и российских исследователей, а также нормативные документы, синтезируются исторические и современные аспекты ИВ, демонстрируя, как идеи психологической войны трансформировались в комплексные информационные операции, объединяются различные элементы информационной войны (кибероперации, пропаганда, психологическое воздействие) в рамках единой стратегии, что особенно заметно в описании подходов НАТО и США.

3. Сравнение — один из ключевых методов в тексте. Автор сопоставляет подходы разных стран и организаций к информационной войне: сравниваются западные и российские трактовки ИВ, нормативные документы, такие как американские военные руководства (JP 3–13, FM 3–13) и российские доктрины, исторические этапы развития ИВ в США, НАТО и России, что позволяет выявить общие тенденции и различия.

4. Дедукция — используется для выведения частных выводов из общих положений. Например, на основе общего понимания информационной войны как инструмента геополитического противоборства автор делает вывод о ее роли в обеспечении национальной безопасности России. Из анализа нормативных документов НАТО и США делается вывод о том, что информационные операции стали неотъемлемой частью современной военной стратегии. На основе исторического обзора автор приходит к выводу, что концепция ИВ эволюционировала от психологической войны к комплексным информационным операциям.

5. Индукция — применяется для формирования общих выводов на основе частных примеров и фактов. Например, анализ документов JP 3–13, FM 3–13, Доктрины информационной безопасности РФ позволяет сделать вывод о различиях в подходах к ИВ в западных и российских традициях. Изучая исторические этапы развития ИВ, автор резюмирует, что информационная война стала ключевым элементом современной геополитики. Изучая современные стратегии НАТО и России, автор делает заключение, что информационные операции теперь направлены не только на защиту, но и на активное воздействие на информационное пространство противника.

РЕЗУЛЬТАТЫ АНАЛИЗА

Концепция «информационной войны» (ИВ) занимает ключевое место в современной политической науке, международных отношениях и военной стратегии. В трех представленных ниже таблицах будет показана эволюция этой концепции в нормативных правовых актах США, НАТО и России, которые наглядно продемонстрируют различные подходы к пониманию и применению информационного противоборства в этих субъектах политики. В западной традиции, особенно в документах США и НАТО, информационная война рассматривается как часть гибридных конфликтов, где акцент делается на когнитивном воздействии, стратегических коммуникациях и кибероперациях. В российском же дискурсе ИВ трактуется через призму национальной безопасности, где основное внимание уделяется защите суверенитета, традиционных ценностей и противодействию внешнему информационному давлению (ответным действиям).

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ В МЕЖДУНАРОДНЫХ ДОКУМЕНТАХ

Анализ нормативных документов США показывает, что информационная война эволюционировала от сугубо психологического воздействия в период холодной войны до комплексного подхода, включающего кибероперации, пропаганду и стратегические коммуникации к настоящему времени (*табл. 1*).

Подход, представленный в документах НАТО, в целом похож на присутствующий в нормативных правовых актах США, что неудивительно, ведь

Таблица 1 / Table 1

Эволюция концепции информационной войны в документах США / The evolution of the concept of information warfare in US documents

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
1947 National Security Act of 1947	Не упоминается напрямую, но заложены основы для координации пропаганды	Не выделены отдельно, но созданы структуры для сбора и анализа информации, например, ЦРУ	Прямо не упоминаются в тексте документа, но есть косвенно: «оказание влияния на политическую, экономическую или военную обстановку за рубежом»	Кибероперации отсутствуют в тексте документа, так как технологический уровень развития еще не предполагал их наличия
1948 Smith-Mundt Act	Усиление пропаганды как инструмента внешней политики	Начинают включать пропаганду и управление информацией, но термин отсутствует	Не упоминаются в тексте документа, но фактически становятся частью внешнеполитической деятельности	Отсутствуют
1949 FM 33–5 Psychological warfare in combat operations	Рассматривается через призму психологического воздействия	Элемент пропаганды и психологического воздействия	Становятся частью боевых действий	Отсутствуют
1969 FM 33–5 Psychological operations techniques and procedures	Все еще связана с психологическим воздействием	Элемент пропаганды и психологических методов	Становятся более структурированными и тактически ориентированными	Отсутствуют
1981 Executive Order 12333	Включается в разведывательные операции	Интегрируются в деятельность разведывательных служб	Часть разведывательной деятельности	Отсутствуют
1993 FM 100–5 Operations	Рассматривается как часть военных операций	Управляют информацией в военных целях	Часть военных кампаний	Отсутствуют, но появляется упоминание о цифровой связи как ключевого элемента победы в информационной войне на тактическом и оперативном уровнях
1996 FM 100–6 Information Operations	Часть военной стратегии	Элемент электронной войны, пропаганды и психологического воздействия	Интегрируются в информационные операции	Начинают рассматриваться как часть информационных операций

Окончание таблицы 1 / Table 1 (continued)

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
1998 JP 3–13 Joint Doctrine for Information Operations	Определяется как комплексное воздействие на противника	Элемент электронной войны, кибероперацій и психологического воздействия	Часть комплексных информационных операций	Важный элемент информационных операций
2003 FM 3–13 (100–6) Information Operations	Рассматривается как часть гибридных конфликтов	Элемент кибероперацій, пропаганды и психологического воздействия	Часть гибридных стратегий	Ключевой элемент информационных операций
2005 FM 3–05.30 (MCRP 3–40.6) Psychological Operations	Включается в психологическое воздействие как ключевой элемент	Интегрируются в психологические методы воздействия	Более технологичны и ориентированы на современные угрозы	Начинают использоваться для поддержки психологических операций
2006 FMI 2–22.9 Open source intelligence	Применяется в открытых источниках информации	Используются в открытых источниках для анализа и планирования	Начинают использовать данные из открытых источников	Начинают использовать открытые данные для анализа угроз
2012 JP 3–13 «Information Operations»	Часть стратегических коммуникаций	Включаются в стратегические коммуникации, кибероперации и психологическое воздействие	Интегрируются в стратегические коммуникации	Становятся частью стратегических коммуникаций
2014 FM 3–13 (JP) Information Operations	Часть глобальной стратегии безопасности	Элементы кибероперацій, пропаганды и психологического воздействия	Становятся частью глобальной стратегии	Становятся ключевым элементом глобальной безопасности
2015 FM 3–13 Information operations	Часть гибридных войн	Элементы кибероперацій, пропаганды и психологического воздействия	Становятся частью гибридных стратегий	Основной инструмент гибридных войн
2018 JP 3–12 Cyberspace Operations	Ключевой элемент кибероперацій	Сосредоточены на киберпространстве	Применяются в киберпространстве для воздействия	Основное поле битвы в информационной войне
2020 FM 3–0 Operations	Часть когнитивной войны	Элемент когнитивного воздействия и управления информацией	Часть когнитивной войны	Используются для когнитивного воздействия на противника

Источник / Sourse: составлено автором /complied by the author.

именно Соединенный Штаты являются лидером Североатлантического альянса и оказывают на него мощнейшее не только финансовое, но и интеллектуальное воздействие, отражающееся в том числе на доктринальном уровне. Однако есть и определенные различия. Так, в документах НАТО, начиная с 2010 г., информационная война стала частью стратегических коммуникаций, а к 2022 г. интегрирована в глобальную стратегию безопасности, включающую когнитивную войну.

Концепция информационной войны в НАТО эволюционировала от эпизодического упоминания в стратегических документах к системному подходу, охватывающему широкий спектр методов, включая информационные операции (Information Operations, IO), стратегические коммуникации (Strategic Communications, STRATCOM), кибероперации (Cyber Operations) и контрпропаганду.

Первые упоминания о необходимости ведения информационной борьбы появились в НАТО в контексте холодной войны. Однако в отличие от США, активно разрабатывавших национальные стратегии психологического воздействия, НАТО вплоть до 90-х гг. прошлого века ограничивалось общей концепцией пропагандистского противостояния СССР.

После окончания холодной войны и особенно после кризиса в Югославии (1999) информационные операции стали рассматриваться в более широком, нежели чисто технический, смысле — как важный инструмент международных военных миссий.

Более подробно эволюция концепции информационной войны в документах НАТО представлена в *табл.* 2.

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ В ДОКУМЕНТАХ РОССИЙСКОЙ ФЕДЕРАЦИИ

В России концепция информационной войны также прошла не один этап своего развития. Как видно из *табл. 3*, она развивалась в контексте защиты национальной безопасности, где ключевыми элементами стали противодействие дезинформации, защита информационного пространства, традиционных ценностей и кибербезопасность.

ВЫВОДЫ

По итогам проведенного исследования эволюции концепции информационной войны в нормативных правовых актах России, США и НАТО можно отметить следующее:

1) термин «информационная война» часто упоминается в современных нормативных правовых актах США и НАТО явно либо в синонимичных формулировках, либо в виде составляющих частей всего инструментария информационной войны (например, «информационная война», «информационные операции», «пропаганда», «психологические операции», «кибероперации», «кибервойна», «когнитивная война», «угроза информационной безопасности», «информационная безопасность», «национальные интересы» и других);

2) несмотря на наличие в российских нормативно-правовых актах ряда положений, касающихся информационного противоборства, в Военной доктрине, Стратегии национальной безопасности и других основополагающих документах Российской Федерации отсутствует термин «информационная война» (но его определение можно вывести опосредованно), в связи с чем существует риск неполного учета угроз данного характера и выработки мер по их нейтрализации и превентивному воздействию;

3) существуют концептуальные различия в правовом закреплении феномена информационной войны: в западной традиции информационные операции достаточно давно и широко отражены в правовых документах, присутствующих в открытом доступе, и рассматриваются как элемент активного противоборства и наступательных мультимодальных гибридных войн, тогда как в российском законодательстве концепция информационной войны воспринимается преимущественно как угроза, исходящая извне, а правовое регулирование направлено на защиту информационного пространства, обеспечение цифрового суверенитета и отражение внешних атак (ответные действия) и защиту традиционных ценностей;

4) эволюция концепции информационной войны отражает смену акцентов в стратегическом подходе к информационному противоборству. В 60-е гг. прошлого века на Западе доминирующее значение придавалось «психологической войне» как основному инструменту влияния. В 70–90-е гг. укоренился термин «информационная война», в который интегрировались психологические и кибероперации. В 2000-е гг. информационное противоборство стало частью более широкой концепции «информационных операций» с акцентом на развитии адресности (выявлении и работе по разным каналам с целевыми аудиториями). В 2010-е гг. усилилась роль стратегической коммуникации и кибероперации, а в 2020-е наблюдается развитие концепции «когнитивной войны» как нового этапа эволюции. Этот процесс демонстрирует не только усложнение методов информационного воздействия, но

Таблица 2 / Table 2

**Эволюция концепции информационной войны в документах НАТО /
The evolution of the concept of information warfare in NATO documents**

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
1949 Североатлантический договор (Вашингтонский договор)	Не упоминается напрямую, но заложены основы для коллективной безопасности	Не выделены отдельно, но создана структура для координации между странами	Не упоминаются, но пропаганда фактически используется для укрепления альянса	Не упоминаются
1950-е Психологические операции в рамках НАТО	Рассматривается через призму пропаганды и психологического воздействия	Включают пропаганду и управление информацией в рамках холодной войны	Становятся частью стратегии сдерживания	Не упоминаются
1957 MC 14/2 «Overall Strategic Concept for the Defense of the NATO Area»	Рассматривается как часть стратегии противоборства в наступившую ядерную эпоху	Термина «информационные операции» нет, но фактически они проводятся и включают пропаганду и противодействие советской дезинформации	Используются для укрепления морального духа союзников и дискредитации противника	Не рассматриваются, так как цифровые технологии еще не достигли значительного уровня развития
1968 MC 14/3 «Overall Strategic Concept for the Defense of the NATO Area»	Концепция информационной войны расширяется в связи с переходом к «гибкому реагированию»	Включает элементы стратегических коммуникаций, направленных на управление кризисами	Используются в холодной войне для подрыва морального духа противника	Отсутствуют
1970-е — 1980-е Появление термина «информационная война» (Т. Рона)	Термин «информационная война» начинает распространяться в лексиконе НАТО	Включаются в управление цифровой информацией, РЭБ и пропаганду	Временно отходят на второй план, уступая технической информационной войне	Не упоминаются, но фактически начинают рассматриваться как часть разведывательной деятельности
1991 NATO Strategic Concept	Признается важной частью безопасности в постсоветский период	Включаются в координацию с гражданскими структурами	Используются для укрепления НАТО на фоне распада СССР	Не упоминаются и еще не являются приоритетом
1999 NATO Strategic Concept	Впервые акцентируется внимание на глобальном информационном пространстве	Документ не содержит специфической информации об информационных операциях	Документ не содержит специфической информации о психологических операциях	Начинают восприниматься как новая сфера угроз и действий (пока без самого термина) (п. 23)

Окончание таблицы 2 / Table 2 (continued)

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
2006 NATO Comprehensive Political Guidance	Информационное превосходство становится одним из ключевых приоритетов для НАТО гибридных угроз (пп. 10, 16, 18)	Термин не упоминается, однако речь идет в том числе о необходимости информационного превосходства и способности защищать информационные системы	Документ не содержит специфической информации о психологических операциях	Появляется термин «кибернетические нападения», – фактически кибероперации официально становятся сферой деятельности НАТО
2010 NATO Military Concept for Strategic Communications	Часть стратегических коммуникаций	Включаются в публичную дипломатию, работу со СМИ, психологические операции, военно-общественные связи и иные аспекты	Интегрируются в стратегические коммуникации	Рассматриваются как часть информационных операций
2014 NATO Cyber Defence Policy	–	–	–	Киберпространство впервые признано полноценным полем боя и устанавливается коллективная защита от кибератак
2014 Обновление доктрины JP 3–13 «Information Operations»	Рассматривается как часть гибридных конфликтов	Включаются в кибероперации, пропаганду и психологическое воздействие	Становятся частью гибридных стратегий	Ключевой элемент информационных операций
2018 JP 3–12 Cyberspace Operations	Включает кибероперации как ключевой элемент	Сосредоточены на киберпространстве	Не упоминаются	Основной инструмент в информационной войне
2019 NATO Military Strategy	Формирует ключевые угрозы безопасности	Включаются в манипуляции общественным мнением	Используются в информацион-ных войнах против соперников	Официально включены в стратегию коллективной обороны
2022 NATO Strategic Concept 2022	Часть глобальной стратегии безопасности	Включаются в стратегические коммуникации, кибероперации и психологическое воздействие	Интегрируются в глобальную стратегию безопасности	Ключевой элемент глобальной безопасности

Источник / Sourse: составлено автором / complied by the author.

Таблица 3 / Table 3

Эволюция концепции информационной войны в документах России / The evolution of the concept of information warfare in Russian documents

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
2000 Доктрина информационной безопасности РФ	Термин «информационная война» не упоминается, но фактически она рассматривается как угроза национальной безопасности, определены главные специфические направления совершенствования системы обеспечения информационной безопасности Российской Федерации в сфере обороны	Включают защиту информационного пространства (радиоэлектронная борьба, борьба с пропагандой и психологическими операциями вероятного противника)	Не выделены отдельно, но упоминаются как часть защиты информационного воздействия	Термин «кибероперации» не употребляется, но фактически в российском правовом поле начинают рассматривать их как часть угроз информационной безопасности
2006 Закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Термин «информационная война» вновь не упоминается, но фактически она рассматривается	–	–	Противодействие кибероперациям рассматривается как часть национальной безопасности
2010 Закон № 390-ФЗ «О безопасности»	Рассматривается как часть угроз национальной безопасности	Включают защиту от деструктивного информационного воздействия	Не упоминаются напрямую, но подразумеваются в контексте информационной безопасности	Рассматриваются как часть защиты информационного пространства
2014 Военная доктрина РФ	Рассматривается как часть гибридных конфликтов	Включают защиту от информационного воздействия и киберугроз	Не упоминаются напрямую, но речь идет в т.ч. и о перечне средств защиты национальных интересов России (дипломатические, правовые, экономические, информационные и др. инструменты ненасильственного характера)	Не упоминаются, но речь идет и о защите информационной инфраструктуры

Окончание таблицы 3 / Table 3 (continued)

Год. Документ / Year. Doc.	Информационная война / Information warfare	Информационные операции / Information operations	Психологические операции / Psychological operations	Кибероперации / Cyber operations
2016 Доктрина информационной безопасности РФ (обновление)	Рассматривается как угроза суверенитету и национальной безопасности	Включают защиту информационного пространства и противодействие дезинформации	Становятся частью информационного противоборства	Основной инструмент защиты информационного пространства
2017 Указ Президента РФ № 203 «О стратегии развития информационного общества»	Часть стратегии развития информационного общества	Включают защиту персональных данных и информационной инфраструктуры	Не упоминаются напрямую, но подразумеваются в контексте информационной безопасности	Часть защиты информационной инфраструктуры
2021 Стратегия национальной безопасности РФ	Часть глобальных угроз национальной безопасности	Включают защиту от киберугроз и дезинформации	Становятся частью стратегии информационного противоборства	Ключевой элемент национальной безопасности
2022 Указ Президента РФ № 809 «О традиционных духовно-нравственных ценностях»	Часть идеологического и культурного противостояния	Включают защиту традиционных ценностей и противодействие дезинформации	Становятся частью защиты культурного суверенитета	Используются для защиты информационного пространства и культурных ценностей
2023 Концепция внешней политики РФ	Часть глобальной стратегии безопасности	Включают защиту от внешнего информационного воздействия	Становятся частью внешнеполитической стратегии	Ключевой элемент глобальной безопасности

Источник / Sourse: составлено автором / complied by the author.

и возрастание его значения в геополитических стратегиях государств;

5) несмотря на различия в подходах, все три субъекта политики (Россия, США и НАТО) признают возрастающую роль информационного противоборства в современной геополитике. Однако если западные страны акцентируют внимание на активном использовании информационных технологий для достижения стратегических целей, то Россия делает упор на защиту от внешних угроз и сохранение суверенитета в информационном пространстве. Эти различия подчеркивают необходимость дальнейшего изучения и сравнения нормативных подходов к информационной войне для понимания ее роли в современных международных отношениях.

Теоретическая значимость работы заключается в том, что она способствует пониманию динамики эволюции концепции информационных войн в различных правовых системах и может быть полезна специалистам в области международного права, информационной безопасности, исследователям информационного противоборства.

СПИСОК ИСТОЧНИКОВ

1. Fridman O. Russian “hybrid Warfare”: Resurgence and Politicisation. Oxford: *Oxford University Press*; 2018. 237 p. DOI: 10.1093/oso/9780190877378.003.0001
2. Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security.* 2022;8:1–20. DOI: 10.1017/eis.2022.19

3. Nye J. Bound to lead: The changing nature of American power. New York: Basic Books; 1990. 307 p.
4. Nye J. Soft power: The means to success in world politics. New York: Public Affairs; 2004. 191 p.
5. Nye J. Smart power and the war on terror. *Asia-Pacific Review.* 2008;15(1):1–8. DOI: 10.1080/13439000802134092.
6. Rid T. Active Measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux; 2020. 512 p.
7. Arquilla J., Ronfeldt D., eds. Networks and netwars: The future of terror, crime, and militancy. Santa Monica: RAND Corporation; 2001. 372 p. DOI: 10.7249/mr1382osd
8. Rid T. Cyber war will not take place. Oxford: *Oxford University Press*; 2013. 218 p.
9. Libicki M.C. What is information warfare? Washington: National Defense University; 1995. 110 p.
10. Carey J.W. Communication as culture: Essays on media and society. New York: Psychology Press; 1992. 241 p.
11. Панарин И.Н. Гибридная война и Ялта-2. Москва: Горячая линия-Телеком; 2022; 452 с.
12. Панарин И.Н. Первая мировая информационная война. Развал СССР. Санкт-Петербург: Питер; 2010. 256 с.
13. Фролов Д.Б. Информационное противоборство в сфере геополитических отношений: дис. д-ра полит. наук. Москва: Рос. акад. гос. службы; 2006. 426 с.
14. Гриняев С.Н. Поле битвы — киберпространство: теория, приемы, средства, методы и средства ведения информационной войны. Минск: Харвест; 2004. 448 с.
15. Васильев А.Д., Подсохин Ф.Е. Информационная война: лингвистический аспект. *Политическая лингвистика*. 2016;(2):10–16.
16. Попадюк А.Э. Информационная война как фактор дестабилизации института президентства в Российской Федерации: дис. канд. полит. наук. Москва: Моск. гос. ун-т; 2021. 180 с.
17. Почепцов Г.Г. Информационные войны. Новый инструмент политики. Москва: Алгоритм; 2015. 254 с.
18. Ткаченко С.В. Информационная война против России. Санкт-Петербург: Питер; 2011. 224 с.
19. Mazarr M.J. Mastering the gray zone: Understanding a changing era of conflict. Carlisle: Strategic Studies Institute; 2015. 120 p.
20. Сорокин И.О. Информационные войны как феномен постиндустриального (информационного) общества: основные парадигмы. *Журнал политических исследований*. 2025;(1):25–40. DOI: 10.12737/2587-6295-2025-9-1-25-40
21. Deppe C., Schaal G. Cognitive warfare: A conceptual analysis of the NATOACT cognitive warfare exploratory concept. *Front. Big Data*. 2024;7:1452129. DOI: 10.3389/fdata.2024.1452129

REFERENCES

1. Fridman O. Russian “hybrid Warfare”: Resurgence and Politicisation. Oxford: *Oxford University Press*; 2018. 237 p.
2. Mumford A., Carlucci P. Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*. 2022;8:1–20. DOI:10.1017/eis.2022.19.
3. Nye J. Bound to lead: The changing nature of American power. New York: Basic Books; 1990. 307 p.
4. Nye J. Soft power: The Means to success in world politics. New York: Public Affairs; 2004. 191 p.
5. Nye J. Smart power and the war on terror. *Asia-Pacific Review.* 2008;15(1):1–8. DOI: 10.1080/13439000802134092
6. Rid T. Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux; 2020. 512 p.
7. Arquilla J., Ronfeldt D., eds. Networks and Netwars: The future of terror, crime, and militancy. Santa Monica: RAND Corporation; 2001. 372 p.
8. Rid T. Cyber war will not take place. Oxford: *Oxford University Press*; 2013. 218 p.
9. Libicki M.C. What is information warfare? Washington: National Defense University; 1995. 110 p.
10. Carey J.W. Communication as culture: Essays on media and society. New York: Psychology Press; 1992. 241 p.
11. Panarin I.N. Hybrid war and Yalta-2. Moscow: Goryachaya liniya-Telekom; 2022. 452 p. (In Russ.).
12. Panarin I.N. The first world information war: The collapse of the USSR. Saint Petersburg: Piter; 2010. 256 p. (In Russ.).
13. Frolov D.B. Information warfare in the sphere of geopolitical relations: Dr. polit. sci. diss. Moscow: Ros. akad. gos. sluzhby; 2006. 426 p. (In Russ.).
14. Grinyaev S.N. Battlefield — cyberspace: Theory, techniques, tools, methods and means of information warfare. Minsk: Harvest; 2004. 448 p. (In Russ.).

15. Vasiliev A.D., Podsokhin F.E. Information warfare: Linguistic aspect. *Politicheskaya lingvistika.* 2016;(2):10–16. (In Russ.).
16. Popadyuk A.E. Information warfare as a factor of destabilization of the institution of the presidency in the Russian Federation: PhD polit. sci. diss. Moscow: Mosk. gos. un-t; 2021. 180 p. (In Russ.).
17. Pocheptsov G.G. Information wars: A new tool of politics. Moscow: Algoritm; 2015. 254 p. (In Russ.).
18. Tkachenko S.V. Information war against Russia. Saint Petersburg: Piter; 2011. 224 p. (In Russ.).
19. Mazarr M.J. Mastering the gray zone: Understanding a changing era of conflict. Carlisle: Strategic Studies Institute; 2015. 120 p.
20. Sorokin I.O. Information wars as a phenomenon of post-industrial (information) society: Main paradigms. *Journal of Political Research.* 2025;(1):25–40. (In Russ.). DOI: 10.12737/2587-6295-2025-9-1-25-40
21. Deppe C., Schaal G. Cognitive warfare: A conceptual analysis of the NATOACT cognitive warfare exploratory concept. *Front. Big Data*. 2024;7:1452129. DOI: 10.3389/fdata.2024.1452129

ИНФОРМАЦИЯ ОБ АВТОРЕ / ABOUT THE AUTHOR

Илья Олегович Сорокин — ассистент кафедры политологии, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация; аспирант кафедры политического анализа и социально-психологических процессов, РЭУ им. Г.В. Плеханова, Москва, Российская Федерация
Ilya O. Sorokin — Assis. at the Department of Political Science, Financial University under the Government of the Russian Federation, Moscow, Russian Federation; postgraduate student at the Department of Political Analysis and Socio-Psychological Processes, Plekhanov Russian University of Economics, Moscow, Russian Federation
https://orcid.org/0009-0003-9927-4270
IOSorokin@fa.ru

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.
Conflicts of Interest Statement: The author has no conflicts of interest to declare.

Статья поступила 23.05.2025; принята к публикации 03.06.2025.
Автор прочитал и одобрил окончательный вариант рукописи.
The article was received 23.05.2025; accepted for publication 03.06.2025.
The author read and approved the final version of the manuscript.