УДК 327.8

МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ФЕЙКАМ И ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИМ АТАКАМ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ ПРОТИВ РОССИИ

М. С. Куролап

Российская академия народного хозяйства и государственной службы при Президенте РФ

Поступила в редакцию 6 мая 2025 г.

Аннотация: *рассматривается феномен неклассической войны как основы гибридных стратегий, где традиционные боевые действия заменяются или дополняются средствами непрямого воздействия: информационно-психологическими операциями, фейковыми новостями, кибератаками, экономическим и дипломатическим давлением. Подчеркивается центральная роль дезинформации в подрыве национального единства, легитимности власти и культурной идентичности. На примере антироссийских кампаний в информационном пространстве демонстрируются масштаб и эффективность заранее подготовленных антироссийских информационных атак. Обосновывается необходимость переосмысления и создания координированной системы противодействия, способной к активному информационному реагированию. Предлагаются меры по формированию специальных структур, обеспечивающих мониторинг, оперативный ответ, выработку противодействующих нарративов («антифейков») и защиту общественно-политической устойчивости в условиях неклассической войны.*

Ключевые слова: *неклассическая война, гибридная война, информационно-психологические операции, противодействие дезинформации, антифейк.*

Abstract: *the article examines the phenomenon of non-classical warfare as a foundation of modern hybrid strategies, in which traditional forms of armed conflict are replaced or supplemented by means of indirect influence, including information and psychological operations, the dissemination of fake news, cyberattacks, as well as economic and diplomatic pressure. Special emphasis is placed on the central role of disinformation in undermining national unity, the legitimacy of state institutions, and cultural identity. Using the example of anti-Russian campaigns in the global information space, the article demonstrates the scale and effectiveness of premeditated information attacks.The necessity for an institutional rethinking of approaches to information security and the creation of a coordinated counteraction system capable of active informational response is substantiated. The article proposes measures for the establishment of specialized structures aimed at monitoring the information environment, providing rapid response to threats, developing counter-narratives («anti-fakes»), and protecting sociopolitical stability under conditions of non-classical warfare.*

Key words: *non-classical warfare, hybrid warfare, information and psychological operations, countering disinformation, anti-fake.*

В условиях современного мирового противостояния, обострения геополитических конфликтов и нарастающей международной нестабильности традиционные формы вооруженной борьбы всё чаще дополняются новыми, гибкими и скрытными инструментами воздействия. Одним из ключевых компонентов так называемой гибридной войны становятся информационно-психологические операции, направленные на разрушение внутреннего единства государства, подрыв доверия к институтам власти, искажение восприятия действительности и навязывание выгодных агрессору нарративов. Неклассическая война, являющаяся основой для гибридных стратегий, представляет собой форму конфликта, в которой военные цели достигаются преимущественно невоенными средствами. К числу таковых относятся фейковые новости, информационные атаки, кибероперации, экономическое давление, санкции, торговые и финансовые войны, политико-дипломатическое воздействие, работа с сетевыми структурами, активизация деятельности подконтрольных неправительственных организаций, а также подрывная деятельность спецслужб. В этой парадигме не существует четкого разграничения между военными и невоенными методами: напротив, стратегия гибридной войны предусматривает нанесение поражения противнику по всем направлениям – от информационного до дипломатического [1].

В рамках неклассической войны не существует «невоенных» методов и средств воздействия в полном

смысле этого слова. Как подчеркивается в ряде исследований, стратегия гибридной войны как одной из форм неклассического противоборства предполагает комплексное поражение противника по всем направлениям: информационному, экономическому, военному, дипломатическому [2]. Все применяемые в этом контексте технологии и инструменты – от информационно-психологических операций и подрыва экономического потенциала до дипломатической изоляции и кибератак – выступают как элементы единой системы военного давления. Принципиальное различие между классической и неклассической войной заключается не в наличии или отсутствии вооруженного насилия как такового, а в характере и приоритетности используемых средств. В случаях, когда вооруженные силы задействуются минимально либо вовсе исключаются из конфликта, а подавление воли противника к сопротивлению осуществляется преимущественно за счет непрямого воздействия, речь идет именно о неклассической войне.

Специфика противодействия в условиях неклассических войн заключается в необходимости системного реагирования на агрессию в ряде ключевых сфер, включая:

1) информационно-психологическое пространство (в том числе в его идеологическом, ценностном, когнитивном и ментальном измерениях);

2) экономическую сферу;

3) научно-технологическое направление.

Полномасштабное развертывание неклассической войны, инициированной коллективным Западом против России, продемонстрировало острую необходимость перехода к новому, качественно более высокому уровню организации контрмер в информационно-психологической сфере. Зафиксированы многочисленные факты координированных действий зарубежных структур, направленных на ведение информационных атак антироссийской направленности. Цель этих воздействий заключается прежде всего:

– в информационной изоляции России на международной арене;

– дегуманизации этнических русских и дискредитации всего, что ассоциируется с русской культурной и цивилизационной идентичностью, включая использование технологий «культуры отмены» [3].

В условиях современных конфликтов информационно-психологическое давление приобретает системный и стратегический характер. На начальных этапах кризиса широко применяются заранее подготовленные дезинформационные кампании, направленные на формирование негативного общественного мнения.

Следует отметить, что на начальном этапе активизации подобных информационных атак российские государственные структуры столкнулись с определенными трудностями в организации эффективного противодействия. Лишь спустя некоторое время была существенно активизирована работа в информационном сегменте – как на внутреннем, так и на внешнем контурах. Особое внимание при этом уделялось русскоязычному информационному пространству, включая зарубежные аудитории.

Содержание информационного противодействия с пророссийским нарративом условно может быть структурировано по следующим направлениям:

1) информационно-новостной компонент – своевременное освещение текущих событий;

2) антифейковая составляющая – выявление, опровержение и нейтрализация дезинформации;

3) пропагандистская и контрпропагандистская деятельность;

4) аналитический сегмент – экспертная интерпретация происходящих процессов и стратегическое обоснование принимаемых решений.

В настоящее время часть задействованных ресурсов действует в координации с государственными структурами, включая профильные ведомства, спецслужбы и средства массовой информации, в то время как другие функционируют на идейно-добровольческой основе [4].

Несмотря на наличие определенной активности в информационной сфере, текущий уровень фрагментации и несогласованности действий препятствует достижению синергетического эффекта и снижает общую эффективность противодействия информационной агрессии. В этой связи актуальной представляется разработка и институционализация единой системы противодействия информационно-психологической войне, предполагающей комплексный подход и четкую координацию всех задействованных акторов. Такая система может включать в себя следующие ключевые направления деятельности:

1) заблаговременное формирование контента, ориентированного как на реактивное реагирование на внешние вызовы, так и на превентивное информационно-психологическое воздействие;

2) разработка и реализация стратегических наступательных информационных операций и контроопераций в отношении внешних недружественных субъектов с целью подрыва их потенциала в сфере информационного противоборства;

3) формирование, поддержка и распространение патриотически ориентированного, пророссийского нарратива в национальном сегменте информационного пространства;

4) устранение недостаточной координации между государственными органами, негосударственными

структурами и отдельными инициативными субъектами, действующими в интересах России;

5) укрепление межведомственного взаимодействия в целях консолидации усилий и достижения синергетического эффекта при проведении информационно-психологических операций;

6) перенос акцента информационного противоборства в информационное поле оппонентов с активным использованием наступательных форматов информационного воздействия;

7) налаживание взаимодействия с профильными структурами и ведомствами дружественных России государств с целью формирования коалиционного подхода к отражению системной информационно-психологической агрессии коллективного Запада;

8) разработка технологических решений, обеспечивающих реализацию указанных выше мероприятий в условиях внешней цензуры, направленной на блокировку как российских, так и лояльных России иностранных источников;

9) создание механизмов ранней диагностики угроз «цветных революций» и иных форм неклассических войн, а также системная разработка предложений по их оперативной нейтрализации [5].

В современных условиях эффективное преодоление существующих технологических и организационных недостатков в системе противодействия неклассическим формам агрессии требует выработки принципиально новых подходов, а также создания специализированной инфраструктуры. Основной задачей данной инфраструктуры должно стать преодоление институциональной изолированности как между государственными ведомствами, так и между государственными структурами и частными субъектами, действующими на идейно-добровольной основе в интересах России в условиях гибридной войны, инициированной коллективным агрессором [6].

Одним из возможных решений данной задачи может стать учреждение специального информационного штаба, находящегося в прямом подчинении Президента России и обладающего полномочиями по координации всех компонентов информационного противодействия в рамках неклассического конфликта. Альтернативным вариантом выступает создание организаций, функционирующих на принципах частно-государственного партнерства, находящихся под контролем компетентных государственных органов (что представляется оправданным и практически неизбежным в российских реалиях), но лишенных ряда ключевых недостатков, характерных для отечественной государственной системы управления. Речь, в частности, идет о преодолении избыточной бюрократизации, жесткой и негибкой иерархии, а также синдрома институциональной ответственности, препятствующего инициативности и оперативности принятия решений.

Возможен также сценарий, при котором такие организации функционируют в формате сетевых структур, осуществляющих координацию между собой без создания дополнительного громоздкого наднационального координационного органа. Основное требование к подобной сети – наличие встроенных механизмов горизонтального взаимодействия, обеспечивающих единство действий при сохранении оперативной гибкости.

Следует подчеркнуть, что в условиях информационно-психологического противостояния, являющегося одним из ключевых компонентов неклассической войны, отсутствие скоординированных и синхронизированных действий недопустимо. Напротив, стратегическая слаженность, адаптивность, способность к динамичному реагированию и проведению наступательных операций с учетом текущей обстановки – всё это становится критически важным. При этом особое значение приобретает способность к стратегическому планированию и формированию многоэтапных информационных кампаний, включая заблаговременную подготовку информационных «закладок», рассчитанных на использование в будущем [7].

Кроме того, необходима системная проработка вопросов информационного сопровождения и защиты действий высшего политического руководства России на международной арене, а также подготовка к различным сценариям развития глобальной геополитической обстановки. Это требует не только институциональной модернизации, но и внедрения современных управленческих и коммуникационных практик, отвечающих вызовам неклассической войны нового типа.

Одним из приоритетных направлений формирования эффективной системы информационной безопасности в условиях неклассической войны является выработка механизмов нейтрализации деструктивного воздействия фейковых сообщений на общественно-политическую систему России. В этой связи особое значение приобретает создание специализированной структуры или сети организаций, функционирующих в рамках информационно-психологической сферы (ИПС), способных оперативно и эффективно реагировать на подобные угрозы.

Ключевым условием эффективности таких структур является обеспечение высокой скорости реагирования на вбросы фейковой информации. Особое внимание следует уделить феномену так называемых «антифейков» – контрнарративов с резонансной подачей, целенаправленно вводимых в информационное пространство для перехвата инициативы у инициа-

торов фейка и коррекции общественного восприятия. В таких случаях скорость реагирования становится критически важным фактором: промедление неизбежно ведет к утрате контроля над повесткой и снижению эффективности всей системы противодействия [8].

Анализ текущей практики демонстрирует наличие определенных проблем в этом направлении. В частности, официальные опровержения фейков, исходящие от представителей государственных структур, зачастую публикуются с существенным опозданием – нередко спустя сутки и более после первичного информационного вброса. Подобная задержка нивелирует потенциальный эффект от опровержения, поскольку основное информационно-психологическое воздействие фейка уже достигло аудитории в течение первых часов. Именно в этот временной промежуток формируется доминирующая интерпретация события, и если она остается безальтернативной, то воспринимается получателями как истина.

Кроме того, следует учитывать, что фейковая информация нередко является элементом заранее спланированных сценариев дестабилизации, включая активацию протестной активности, беспорядков и других форм насильственного давления. В таких случаях запоздалые опровержения могут не только не сыграть сдерживающей роли, но и усугубить ситуацию, способствуя усилению протестных настроений и мобилизации оппозиционно ориентированных групп. Это обусловлено как эффектом психологической инерции, так и снижением легитимности официальных источников информации в глазах широкой аудитории [9].

Таким образом, одной из задач создаваемой структуры (или сети) по противодействию фейковой информации должно стать выстраивание системы мониторинга и экстренного реагирования, способной оперативно вводить в оборот альтернативные нарративы, нейтрализующие или опережающие воздействие фейков. Только при наличии подобного механизма возможно формирование устойчивого информационного щита, способного эффективно отражать угрозы в рамках информационно-психологического противоборства нового типа.

Вторым не менее значимым условием эффективного противодействия фейковой информации посредством «антифейков» является необходимость формирования встречного информационного резонанса, сопоставимого по масштабу и эмоциональному воздействию с изначальным фейком. В случае, если создаваемый контрнарратив не обладает аналогичной мощностью, он не способен перехватить информационную повестку и, следовательно, оказывается недостаточно действенным в условиях высококонкурентной медиасреды. В этом контексте важным становится не только само наличие оперативного реагирования, но и его качество, выражающееся в способности сформировать содержательно насыщенный и эмоционально резонансный ответ, эффективно воздействующий на аудиторию через современные средства коммуникации [5].

Третьим критически важным условием является корректный выбор целевой аудитории, на которую направляется антифейк. Высокая степень релевантности между аудиторией, подвергшейся воздействию деструктивного информационного вброса, и аудиторией, которой адресуется контрнарратив, является обязательным условием для достижения коммуникативного эффекта. В противном случае эффективность предпринятых усилий существенно снижается. Например, если фейк ориентирован на молодежную аудиторию – наиболее восприимчивую к мобилизационным и протестным импульсам, а антифейк адресован преимущественно зрелым и пожилым слоям населения, лояльным к власти, вероятность нейтрализации воздействия существенно снижается. Такая рассинхронизация снижает коэффициент полезного действия антифейка и делает его практически неэффективным в рамках заданной коммуникационной конфигурации [10].

Четвертым определяющим фактором выступает содержание создаваемого антифейка. Нарративная стратегия и используемый информационный контент должны быть выверены с учетом возможного восприятия и потенциального резонанса в целевой группе. Ошибки в выборе тональности, стиля или фактологического наполнения могут привести к усилению исходного фейка, а не к его нивелированию. Более того, неудачно сконструированный антифейк способен не только не перехватить повестку, но и спровоцировать обратный эффект, усилив недоверие к официальным источникам и увеличив деструктивный потенциал первичного информационного вброса. Таким образом, ошибка на этом этапе может иметь контрпродуктивные последствия, играя на руку инициаторам информационной агрессии [11].

Следует подчеркнуть, что реализуемая коллективным Западом антироссийская кампания, развернутая в формате полномасштабной неклассической войны, не является стихийным или фрагментарным набором разрозненных инструментов и подходов. Напротив, в действиях противоборствующей стороны прослеживаются признаки системного и тщательно спланированного подхода, характеризующегося высокой степенью подготовленности, гибкости, адаптивности и стратегической последовательности. Каждое мероприятие в рамках данной кампании, как правило, предваряется расчетом потенциальных выгод и рисков

с целью минимизации ущерба для собственных интересов и максимизации вреда для России.

Учитывая изложенное, становится очевидной несостоятельность паллиативных или частичных мер в качестве ответных действий. Противодействие подобной агрессии должно основываться не на ситуативных реакциях, а на комплексной стратегической линии, исключающей половинчатость и декларативность. Более того, в условиях системного и долговременного давления со стороны внешних акторов применение неэффективных или половинчатых контрмер может не только не привести к желаемому результату, но и усугубить стратегические уязвимости, что в итоге окажется контрпродуктивным [12].

Исходя из вышеуказанного, представляется, что стратегия противодействия полномасштабной информационной войне должна обладать рядом ключевых характеристик:

1) проактивность. Исключительно оборонительные меры не обеспечивают адекватного ответа в условиях системной и многоуровневой агрессии. Эффективная стратегия предполагает инициативность, упреждающий характер действий и способность перехода к наступательным формам отражения угроз;

2) опора на непрямые действия. Косвенные методы воздействия, несмотря на более сложную реализацию и увеличенные временные затраты, обладают большей стратегической результативностью, поскольку позволяют достигать целей в условиях пониженной готовности противника к подобным сценариям. В то же время прямое противоборство, как правило, сопряжено с высокими затратами и низкой эффективностью, поскольку осуществляется в рамках заранее предусмотренных и проработанных контрмер;

3) выявление и использование уязвимостей противника. Необходимым элементом стратегии является анализ общественно-государственных уязвимостей оппонента, воздействие на которые позволяет нанести ему высокий ущерб при минимальных издержках со стороны России. Речь может идти об асимметричных мерах, включающих проведение масштабных или точечных информационных операций, использование элементов политико-дипломатического давления, а также геополитических инициатив, в том числе военного характера, в стратегически значимых для противника регионах;

4) формирование коалиций. Совместные действия с государственными и негосударственными акторами, также подвергающимися системному воздействию со стороны коллективного Запада, могут значительно повысить эффективность противодействия агрессии. Коалиционные стратегии позволяют не только распределить ресурсы и риски, но и усилить совокупный потенциал реагирования в условиях информационно-психологического и иного давления.

Совокупная реализация указанных положений способна не только повысить устойчивость национальной системы к внешнему вмешательству, но и обеспечить переход к активной фазе стратегического противодействия. Этот переход, в свою очередь, следует рассматривать как одно из ключевых условий достижения успеха в условиях ведения современной информационной войны против России.

ЛИТЕРАТУРА

1. *Стригунов К. С.* Фундаментальный механизм и законы неклассической войны / К. С. Стригунов, А. В Манойло // Гражданин. Выборы. Власть. – М., 2019. – № 4. – С. 157–193.

2. *Бартош А. А.* Стратегия и контрстратегия гибридной войны / А. А. Бартош // Военная мысль. – 2018. – № 10. – С. 5–20.

3. «Гибридные войны» в хаотизирующемся мире XXI века / под ред. П. А. Цыганкова. – М. : Изд-во Московского университета, 2015. – С. 218–223.

4. *Разов П. В.* Влияние СМИ на формирование доверия к цифровым платформам / П. В. Разов // ПОИСК : Политика. Обществоведение. Искусство. Социология. Культура. – 2023. – № 1 (96). – С. 98–106.

5. *Стригунов К. С.* Современные неклассические войны : формы, методы, технологии / К. С. Стригунов ; под ред. А. В. Манойло. – М. : Горячая линия – Телеком, 2024. – 242 с.

6. *Кузьмин Д. А.* Информационные операции как элемент гибридной войны / Д. А. Кузьмин // Информационное общество. – 2021. – № 1. – С. 45–52.

7. *Лебедев С. А.* Психологические операции и информационно-психологическое противоборство в современных конфликтах / С. А. Лебедев. – М. : РИСИ, 2018. – 142 с.

8. *Попадюк О. В.* Противодействие распространению фейковых новостей в социальных сетях : правовые и организационные аспекты / О. В. Попадюк. – Журнал информационного права. – 2020. – № 2. – С. 34–41.

9. Министерство иностранных дел Российской Федерации. Информационная война как угроза международному миру и безопасности : доклад МИД России, 2024. – URL: https://mid.ru/ru/foreign_policy/doklady/1968836/ (дата обращения: 25.04.2025).

10. *Нестик Т. А.* Психологические факторы эффективности опровержения дезинформации в социальных сетях / Т. А. Нестик, Е. А. Михеев // Библиотека Института психологии РАН. – URL: https://lib.ipran.ru/paper/49293811 (дата обращения: 25.04.2025).

11. *Шомова С. А.* Фейк : от академических дискуссий к практическим решениям / С. А. Шомова // Academia.edu. – URL: https://www.academia.edu/99578196/ (дата обращения: 25.04.2025).

12. *Поздняков Е. И.* Актуальные методы противодействия фейковым новостям / Е. И. Поздняков // Государственная власть и управление. – 2023. – № 3. – С. 173–180. – URL: https://www.rcoit.ru/upload/iblock/f7c/6dfy03ks1ki6mvw70clrtt9b4thsg9sn/ГВВ_3_2023-173-180.pdf (дата обращения: 25.04.2025).

Российская академия народного хозяйства и государственной службы при Президенте РФ

Куролап М. С., аспирант кафедры политологии и политического управления

E-mail: mike_kur@mail.ru

Russian Presidential Academy of National Economy and Public Administration

Kurolap M. S., Post-graduate Student of the Political Science and Political Management Department

E-mail: mike_kur@mail.ru