Открытый журнал евразийских исследований, 2025, №4, сс. 39-46
doi: 10.65469/eijournal.2025.4.4
eijournal.ilimbilim.kg

ПОЛИТОЛОГИЯ / POLITICAL SCIENCES
УДК 32.019.51

Информационная война в современном мире: сущность, методы и риски

Сапарбаева Айнура Абдилазимовна
старший преподаватель, Ошский государственный университет, Кыргызстан, asaparbaeva@oshsu.kg

Абдуллаева Рухшона Иброхимжоновна
студент, Ошский государственный университет, Кыргызстан, ruhshonao50805@gmail.com

Аннотация
В статье рассматривается феномен информационной войны как одного из ключевых факторов современного политического, социального и технологического развития. Анализируются основные подходы к определению понятия «информационная война», её цели, методы и последствия. Особое внимание уделяется роли информационно-коммуникационных технологий, киберпространства и социальных сетей в процессах манипуляции общественным сознанием. Рассматриваются вопросы этики и правового регулирования информационного противоборства, а также основные направления защиты от информационных атак в условиях цифровизации общества.

Ключевые слова: информационная война, дезинформация, фейковые новости, пропаганда, манипуляция общественным мнением, кибератаки, цифровая безопасность, психологическая война, контрпропаганда

Для цитирования: Сапарбаева А.А., Абдуллаева Р.И. (2025). Информационная война в современном мире: сущность, методы и риски. *Открытый журнал евразийских исследований*, №4, сс. 39-46. doi: 10.65469/eijournal.2025.4.4

Введение

Информационная война в современном мире приобретает всё более значимую роль, выходя за рамки традиционного военного противостояния. В условиях глобализации и цифровизации информация становится стратегическим ресурсом, а управление информационными потоками — важнейшим инструментом влияния на общественное мнение, политические процессы и международные отношения.

Современные конфликты всё чаще разворачиваются не только на поле боя, но и в медиапространстве, кибер среде и социальных сетях. Информационное воздействие способно подрывать доверие к государственным институтам, формировать протестные настроения, усиливать социальную поляризацию и дестабилизировать политическую ситуацию без

применения военной силы. В этой связи информационная война рассматривается как один из ключевых элементов гибридных войн XXI века.

Хотя сам термин «информационная война» получил широкое распространение во второй половине XX века, практики информационного воздействия на противника известны с древнейших времён. Уже в трудах Сунь Цзы («Искусство войны») подчёркивалась важность обмана, дезориентации и подрыва морального духа противника. Н. Макиавелли в трактате «Государь» также указывал на роль информации и общественного мнения в укреплении власти и достижении политических целей. В XX веке информационная война стала неотъемлемым элементом вооружённых конфликтов. Во время Первой мировой войны пропаганда использовалась для мобилизации населения и демонизации противника. В годы Второй мировой войны и холодной войны информационное противоборство приобрело институционализированный характер, включив радиовещание, печатные СМИ и культурную дипломатию [1].

Существенный вклад в формирование современной теории информационной войны внесли западные и российские исследователи. Т. Рон, М. Либики, Дж. Най, Г. Почепцов и А. Манойло рассматривали информационную войну как совокупность политических, психологических, кибернетических и экономических воздействий. Современное понимание данного феномена выходит за рамки военной сферы и охватывает практически все уровни общественной жизни.

Эволюция понятия информационной войны

Первоначально информационная война рассматривалась как вспомогательный элемент вооружённых конфликтов, направленный на деморализацию противника и дезориентацию его командования. В период Первой мировой войны активно использовались пропагандистские плакаты, печатные издания и радиовещание, формировавшие образ врага и мобилизовавшие население.

В годы Второй мировой войны и холодной войны информационное противоборство стало системным и институционализированный. Государства создавали специальные пропагандистские службы, радиостанции, аналитические центры, направленные на идеологическое влияние как на собственное население, так и на граждан других стран. В этот период информационная война тесно переплеталась с идеологической борьбой между различными политическими системами.

Качественный перелом произошёл с развитием интернета, цифровых технологий и социальных сетей. Современные средства коммуникации существенно снизили барьеры входа в информационное пространство и позволили отдельным группам и даже индивидуальным актерам оказывать влияние на массовую аудиторию в глобальном масштабе. Информационная война перестала быть исключительно прерогативой государств [10].

Американский военный аналитик Т. Рон одним из первых ввёл термин «information warfare», акцентируя внимание на нарушении информационных и управленческих систем противника. В дальнейшем данное понятие было расширено и стало включать политические, экономические, психологические и кибернетические аспекты.

Классификация и методы информационной войны

Существенный вклад в систематизацию форм информационной войны внёс М. Либики, выделивший следующие её виды: командно-управленческую войну, направленную на разрушение систем управления и принятия решений; разведывательную войну, связанную со сбором и анализом информации; электронную войну, предполагающую подавление и перехват электронных коммуникаций; психологическую войну, основанную на пропаганде и манипуляции сознанием; хакерскую войну, включающую взлом и несанкционированный доступ к данным; экономическую информационную войну, выражающуюся в санкционном и репутационном давлении; а также кибервойну, целью которой является нарушение функционирования критически важной инфраструктуры [6].

К основным методам информационной войны относятся пропаганда, дезинформация, распространение фейковых новостей, создание информационного шума, использование ботов и троллей в социальных сетях, а также кибератаки на государственные и частные информационные системы. Особое значение приобретают алгоритмы персонализированного контента, усиливающие эффект манипуляции общественным мнением [2].

Роль социальных сетей и медиаплатформ

Социальные сети стали одним из ключевых инструментов информационной войны. Их особенности — высокая скорость распространения информации, отсутствие жёсткой редакционной фильтрации и возможность анонимного участия — создают благоприятную среду для дезинформационных кампаний. Алгоритмы рекомендаций способствуют формированию информационных пузырей, в которых пользователи получают контент, подтверждающий уже существующие взгляды [5].

Дополнительную угрозу представляют технологии искусственного интеллекта, включая генерацию дипфейков, автоматизированные аккаунты и анализ больших данных. Их использование значительно усложняет выявление источников информационных атак и повышает эффективность манипулятивных стратегий.

Объекты и источники информационных угроз

Объектами информационного воздействия становятся государственные институты, средства массовой информации, экономические структуры, а также отдельные социальные группы и личности. Высокая степень цифровизации систем управления, финансового сектора, энергетики и транспорта делает их уязвимыми перед целенаправленными информационными и кибератаками [3; 4].

Источниками информационных угроз могут выступать государства, политические партии, транснациональные корпорации, экстремистские и террористические организации, а также негосударственные акторы. Воздействие на массовое сознание нередко осуществляется через формирование стратегических мифов, при которых элементы достоверной информации используются для искажения реальной картины происходящего.

Этические и правовые аспекты информационного противоборства

Существенной проблемой информационной войны является отсутствие универсальных международных правовых норм, регулирующих информационное противоборство. Многие действия в информационном пространстве находятся в серой зоне между законной информационной политикой и агрессивным вмешательством во внутренние дела государств. Это затрудняет выработку единых подходов к оценке допустимости тех или иных информационных операций и снижает эффективность международных механизмов предотвращения конфликтов [7; 8].

Этический аспект также приобретает особую значимость. Манипуляция общественным сознанием, распространение ложной информации и подрыв доверия к социальным институтам способны приводить к долгосрочным негативным последствиям, включая рост радикализации, поляризацию общества и социальную дезинтеграцию. В условиях информационной войны гражданское население всё чаще становится не только объектом, но и инструментом воздействия.

Дополнительно следует отметить, что информационное противоборство затрагивает вопросы ответственности как государственных, так и негосударственных акторов. Использование цифровых платформ, алгоритмов социальных сетей и технологий искусственного интеллекта значительно усиливает масштаб и скорость распространения дезинформации, что осложняет установление её источников и привлечение виновных к ответственности. В условиях отсутствия единых международных механизмов контроля возрастает роль этических стандартов журналистики, медиаграмотности населения и саморегулирования онлайн-платформ, которые становятся ключевыми инструментами минимизации разрушительного воздействия информационных атак на общество и международную стабильность [12; 13].

Проблемы противодействия и анализа рисков

Противодействие информационной войне требует комплексного и многоуровневого подхода, включающего развитие национальных систем информационной безопасности, совершенствование механизмов киберзащиты, а также повышение уровня медиаграмотности населения и формирование навыков критического мышления. Особое значение приобретает профилактика информационных угроз, направленная на снижение уязвимости общества к манипулятивному контенту и деструктивным нарративам.

Исследователи подчёркивают необходимость создания специализированных центров информационного реагирования, способных в режиме реального времени выявлять потенциальные угрозы, проводить мониторинг информационного пространства, анализировать масштаб и цели информационных кампаний, а также координировать действия государственных органов, средств массовой информации и гражданского общества. Такие структуры позволяют повысить оперативность принятия решений и снизить уровень дезинформационного воздействия.

Дополнительной проблемой является сложность оценки рисков информационной войны, обусловленная высокой динамичностью цифровой среды и быстрым развитием

информационных технологий. Использование искусственного интеллекта, ботов и автоматизированных систем распространения контента усложняет прогнозирование последствий информационных атак и повышает вероятность непреднамеренной эскалации конфликтов. В этой связи возрастает значение научных исследований, разработки аналитических моделей оценки рисков и укрепления международного сотрудничества в сфере обмена данными и лучшими практиками обеспечения информационной безопасности [9; 11].

Важным направлением анализа информационной войны является влияние информационных атак на формирование идентичности и ценностных ориентаций общества. Через систематическое повторение определённых нарративов, символов и образов противоборствующие стороны стремятся изменить восприятие истории, культуры и национальных интересов. Подобные стратегии особенно эффективны в условиях социальной нестабильности, кризиса доверия к институтам власти и низкого уровня медиаграмотности, что делает общество уязвимым к внешнему информационному воздействию.

Особую роль в современных информационных конфликтах играет молодёжь как наиболее активная аудитория цифровых платформ. Социальные сети, видеохостинги и мессенджеры становятся не только источником информации, но и пространством формирования политических установок и моделей поведения. В этом контексте возрастает значение образовательных программ, направленных на развитие критического мышления, навыков проверки информации и ответственного потребления медиаконтента, что рассматривается как один из ключевых элементов долгосрочной стратегии информационной безопасности.

Кроме того, в условиях глобального информационного противоборства усиливается необходимость международного сотрудничества. Совместные инициативы в сфере кибербезопасности, обмен аналитической информацией и выработка общих этических принципов использования цифровых технологий могут способствовать снижению уровня конфликтности в информационном пространстве. Несмотря на существующие политические разногласия, формирование универсальных подходов к противодействию дезинформации и киберугрозам является важным условием обеспечения устойчивого развития и международной стабильности.

Заключение

Информационная война в современном мире представляет собой многоуровневый и динамичный процесс, оказывающий существенное влияние на общественное сознание, политическую стабильность и международную безопасность. Развитие цифровых технологий усиливает как потенциал информационного воздействия, так и масштабы возможных угроз.

Эффективная защита информационного пространства возможна лишь при сочетании технологических, правовых и социально-культурных мер. Повышение медиаграмотности, развитие этических стандартов и укрепление международного сотрудничества являются ключевыми условиями устойчивости общества в условиях глобального информационного противоборства.

Литература

1. Бойко А.А. Информационная безопасность и медиаграмотность в цифровом обществе. — М.: Юрайт, 2019. — 256 с.
2. Войтюк О. С. Информационные войны и киберконфликты в международных отношениях. — Киев: Центр учебной литературы, 2018. — 312 с.
3. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива. — СПб.: Арлит, 2010. — 304 с.
4. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. — М.: ФИЗМАТЛИТ, 2010. — 228 с.
5. Кастельс М. Власть коммуникации. — М.: Изд. дом ВШЭ, 2016. — 564 с.
6. Либики М. Что такое информационная война? — М.: ИНИОН РАН, 2012. — 156 с.
7. Манойло А. В. Государственная информационная политика в условиях информационно-психологической войны. — М.: Горячая линия – Телеком, 2015. — 384 с.
8. Почепцов Г. Г. Информационные войны. — М.: Рефл-бук, 2001. — 576 с.
9. Bradshaw S., Howard P. The Global Disinformation Order. — Oxford: Oxford Internet Institute, 2019. — 78 p.
10. Nye J. Soft Power: The Means to Success in World Politics. — New York: Public Affairs, 2004. — 192 p.
11. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework. — Strasbourg: Council of Europe, 2017. — 109 p.
12. Камалидинова, А. С. Жарандык журналистиканы түшүнүү: концептуалдык негиз / А. С. Камалидинова // *Евразия изилдөөлөрү ачык журналы*. – 2025. – No. 1. – P. 47-62. – DOI 10.65469/eijournal.2025.1.7. – EDN GGAEYB.
13. Майрамбек Кызы, Э. Жасалма интеллекттин жаңылыктарды даярдоо процессине тийгизген таасири / Э. Майрамбек Кызы // *Евразия изилдөөлөрү ачык журналы*. – 2025. – No. 2. – P. 49-62. – DOI 10.65469/eijournal.2025.2.6. – EDN ICCJXC.

Евразия изилдөөлөрү ачык журналы, 2025, №4, бб. 39-46
doi: 10.65469/eijournal.2025.4.4
eijournal.ilimbilim.kg

ПОЛИТОЛОГИЯ / POLITICAL SCIENCES
УДК 32.019.51

Заманбап дүйнөдө маалыматтык согуш: мазмуну, ыкмалары жана тобокелдиктери

Сапарбаева Айнура Абдилазимовна
улук окутуучу, Ош мамлекеттик университети, Кыргызстан, asaparbaeva@oshsu.kg

Абдуллаева Рухшона Иброхимжоновна
студент, Ош мамлекеттик университети, Кыргызстан, ruhshonao50805@gmail.com

Аннотация

Макалада маалыматтык согуш феномени заманбап саясий, социалдык жана технологиялык өнүгүүнүн негизги факторлорунун бири катары каралат. «Маалыматтык согуш» түшүнүгүнүн аныктамасына болгон негизги ыкмалар, анын максаттары, ыкмалары жана кесепеттери талданат. Коомдук аң-сезимди манипуляциялоо процесстеринде маалыматтык-коммуникациялык технологиялардын, кибермейкиндиктин жана социалдык тармактардын ролуна өзгөчө көңүл бурулат. Ошондой эле маалыматтык каршы күрөштүн этикалык жана укуктук жөнгө салуу маселелери, ошондой эле коомдун санариптешүүсү шартында маалыматтык чабуулдардан коргонуу боюнча негизги багыттар каралат.

Ачкыч сөздөр: маалыматтык согуш, дезинформация, фейк жаңылыктар, пропаганда, коомдук пикирди манипуляциялоо, киберчабуулдар, санариптик коопсуздук, психологиялык согуш, контрпропаганда

Open Journal of Eurasian Issues, 2025, no. 4, pp. 39-46
doi: 10.65469/eijournal.2025.4.4
eijournal.ilimbilim.kg

ПОЛИТОЛОГИЯ / POLITICAL SCIENCES
УДК 32.019.51

Information Warfare in the Modern World: Essence, Methods and Risks

Saparbaeva Ainura Abdilazimovna
Senior Lecturer, Osh State University, Kyrgyzstan, asaparbaeva@oshsu.kg

Abdullaeva Rukhshona Ibrohimjonovna
Student, Osh State University, Kyrgyzstan, ruhshonao50805@gmail.com

Abstract
The article considers the phenomenon of information warfare as one of the main factors of modern political, social and technological development. The main approaches to the definition of the concept of "information warfare", its goals, methods and consequences are analyzed. Particular attention is paid to the role of information and communication technologies, cyberspace and social networks in the processes of manipulation of public consciousness. Also, the issues of ethical and legal regulation of information countermeasures, as well as the main directions of protection against information attacks in the context of the digitalization of society, are considered.

Keywords: information warfare, disinformation, fake news, propaganda, manipulation of public opinion, cyberattacks, digital security, psychological warfare, counter-propaganda