УДК: 32.019.5

Трофимов Иван Александрович

МОДЕЛИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ПРОТИВОБОРСТВА В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ВОЙНЫ

Аннотация: *научная статья посвящена анализу моделей информационно-психологического противоборства в условиях современной информационной войны. В работе рассматриваются средства воздействия на массовое сознание, а также формы эксплуатации информационных технологий для манипуляции общественным мнением и дестабилизации социально-политической ситуации. В статье подчёркивается стратегия противодействия, этические аспекты и вопросы регулирования информационных угроз. В работе представлены современные технологические достижения, автоматизация и перспективы развития систем защиты информационного пространства, вызовы и направления укрепления национальной безопасности в условиях информационно-психологической войны. Цель работы заключается в анализе современных моделей и методов информационно-психологического противоборства, выявлении особенностей, угроз и способов противодействия в условиях информационной войны. Актуальность исследования обусловлена возрастающей ролью информационно-психологического воздействия в глобальных межгосударственных конфликтах, внутренних политических процессах и социальных процессах в современном обществе. В условиях быстрого развития технологий, распространения дезинформации и манипуляций общественным мнением, необходимость разработки стратегий защиты информационного пространства и психического здоровья граждан становится особенно необходимо для обеспечения национальной безопасности и устойчивого развития государства.*

Ключевые слова: *информационно-психологическая война, информационное противоборство, манипуляция сознанием, информационная безопасность, киберугрозы, дезинформация, пропаганда, автоматизация защиты, этические инновации, социальные сети, кибербезопасность, противодействие информационным угрозам, этика в информационных технологиях.*

Trofimov Ivan Alexandrovich

MODEL OF INFORMATIONAL AND PSYCHOLOGICAL CONFRONTATION IN CONDITIONS OF INFORMATION WAR

Annotation: *The scientific article is devoted to analysis of models of informational-psychological confrontation in conditions of modern information war. The work considers means of influence on mass consciousness, as well as forms of exploitation of information technologies for manipulation of public opinion and destabilization of socio-political situation. The article emphasizes countervailing strategy, ethical aspects and issues of information threat management. The article presents modern technological advances, automation and prospects of development of systems of protection of information space, challenges and directions of strengthening national security in conditions of informational-psychological war. The aim of the work is to analyze modern models and methods of informational-psychological confrontation, to identify features, threats and ways of counteraction in conditions of information war. The relevance of the study is due to the increasing role of information and psychological impact in global inter-state conflicts, internal political processes and social processes in modern society. Given the rapid development of technology, spread of misinformation and manipulation of public opinion, The need to develop strategies to protect the*

information space and mental health of citizens becomes especially necessary for ensuring national security and sustainable development of the state.

Keywords: *information and psychological war, information counteraction, manipulation of consciousness, information security, cyber threats, disinformation, propaganda, automation of protection, ethical innovations, social networks, cybersecurity, countering information threats, ethics in information technology.*

Введение

В настоящее время существует более значимая и сильная форма информационного противоборства – это информационно-психологическое противоборство. Информационно-психологическая война (ИВП) – это форма борьбы за информационное превосходство, при которой используются методы влияния на массовое сознание населения или индивидуальное сознание отдельных личностей. Информационно-психологическое противоборство имеет ряд особенностей:

1. Информационное противоборство может осуществляться на большом расстоянии, за пределами территориальных границ страны-противника;

2. На психологическое воздействие можно реагировать только соответствующим психологическим противодействием;

3. Психологическое воздействие производится скрытно, учитывая особенности объекта воздействия;

4. Главной задачей информационно-психологического противоборства является нанесение колоссального ущерба государствам, без проведения боевых действий;

5. Виды информационно-психологической агрессии в международном праве не будут трактоваться как акты войны, из-за не военного характера их воздействия.

Информационно-психологическая война появилась как форма информационного противоборства на определённой стадии развития средств и методов информационно-психологического воздействия и представляет собой наиболее социально опасную форму данного противоборства, осуществляемого средствами и способами воздействия на информационно-психологическую сферу противника с целью решения стратегических задач.

Целями такой войны могут быть

- влияние на массовое сознание путем создания несуществующих фактов и обстоятельств;

- противостояние альтернативным источникам информации;

- дестабилизация политической, социальной, экономической и культурной ситуации в странах.

Так как ИПВ направлена на воздействие на массовое сознание, она вызывает определённые психологические эффекты (паника, страх, ксенофобии, манипуляция сознанием). Манипуляция сознанием (лат. от manus – «рука», manipulare – управлять со знанием дела) – преднамеренная подмена в форме скрытого, анонимного господства, осуществляемого в массовом сознании содержания или смысла явления его квазиформой, когда при сохранении идентичных внешних признаков, явление приобретает деструктивный смысл или ассоциируется с ним. Манипуляция ориентирована на исключение логики, критического анализа и примитивизацию мышления целевой группы, подмену логической связи устойчивой ассоциативной связью, когда-то или иное явление ассоциируется с навязываемым деструктивным образом. Это может привести к дестабилизации социальной ситуации и конфликтам между разными группами населения. В современном мире ИПВ становится всё более распространённой, и ее негативные последствия могут приводить к возникновению международных конфликтов. Суть информационной войны состоит в изменении картины мира противоборствующей стороны.

В зависимости от преследуемых целей информационно-психологическое воздействие, как правило, осуществляется на конкретные сферы индивидуального, группового, массового и общественного сознания:

- мотивационную (убеждения, ценностные ориентации, влечения, желания), когда надо оказать влияние на людей для побуждения их определённым действиям;

- познавательную (ощущения, восприятия, представления, воображение, память и мышление), когда необходимо изменить в нужную сторону представления, характер восприятия вновь поступающей информации и в итоге — «миросознание» человека;

- эмоциональную (эмоции, чувства, настроения, волевые процессы), когда под прицелом находятся внутренние переживания и волевая активность людей;

- познавательную (общение и взаимоотношения, взаимодействие, межличностное восприятие) с целью создания социально-психологического комфорта или дискомфорта, побуждения людей сотрудничать либо конфликтовать с окружающими.

В информационном обществе в приоритете информационные технологии, которые имеют широкое распространение и доступность, информационно-психологическая война становится всё более распространённой и полезной формой манипуляции сознанием и воздействия на общественные процессы. Средства и методы манипуляции сознанием - это воздействия, нацеленные на программирование идеалов, общественного мнения, личностных стереотипов, стремлений, а также психического состояния людей для создания и стимулирования поведения, которое необходимо для достижения господствующего положения в противоборстве.

Психологическое оружие позволяет при физическом превосходстве противника получить господствующее положение за счёт ослабления его возможностей по критериям морально-психологического состояния, боевой

активности, моральной устойчивости и профессионализма. Информационно-психологическая война может быть использована для разных целей - дестабилизация политической ситуации в определённой стране, подрыв международных отношений, внедрение в общество определённых идей и взглядов, манипуляция общественным мнением. Она может носить как открытый, так и скрытый характер и включать в себя использование различных технологий и методов манипуляций сознанием людей.

Информация – это власть, а контроль над средствами коммуникации – средство осуществления власти. Наиболее фундаментальная форма власти состоит в способности формировать человеческое сознание. Битва за изменение и применение норм в обществе происходит вокруг формирования человеческого сознания, поэтому коммуникация – эпицентр этой битвы.

Информационно-психологическая война специализируется как внутри страны, так и на международный уровень, разжигая ненависть и вражду между товарищами, соседями, родственниками. Её цель повышение авторитета определённого политического режима, так и дискредитация конкурирующих политических сил и идеологий. Основными методами информационно-психологической войны являются дезинформация, манипуляция общественным мнением, пропаганда и создание атмосферы страха и неопределённости. Пропаганда — распространение политических, философских, научных, художественных знаний (идей) и другой информации в обществе с целью формирования у людей определённого мировоззрения. Методы предъявления неосознаваемой акустической и зрительной информации. Скрытое воздействие на психику, с помощью неосознаваемой человеком акустической и визуальной информации.

Основная цель Deepfakes

Также можно выделить дипфейки, которые играют ключевую роль в современной дезинформации. Дипфейки — это медиа, созданные технологией искусственного интеллекта, которые выглядят правдоподобно.

Речь идёт об искусственно созданных фото, видео и аудиозаписях, где лица и голоса людей подменяются или имитируются настолько искусно, что возникает иллюзия их причастности к определённым обстоятельствам. Эти технологии позволяют создавать убедительные подделки, труднораспознаваемые даже экспертам.

Дипфейки используются в целях манипуляции сознанием масс, к примеру, путём создания недостоверных видеороликов с участием популярных людей. Это дезориентирует аудиторию и подрывает уверенность в средствах массовой информации. Основная цель дипфейков это использование специальных методов для провокационных действий, а также фальсификация утверждений и событий, транслируемых через СМИ и социальные сети.

Самые яркие примеры дипфейков приведены ниже, которые демонстрируют способы создания визуальных эффектов для распространения дезинформации.

1. Президент США Дональд Трамп подал на Би-би-си в суд за клевету, которая выразилась, как он считает, в монтаже фраз из его выступления 6 января 2021 года в документальном фильме программы «Панорама». Трамп требует с Британской вещательной корпорации пять миллиардов долларов.

2. Эксперты обнаружили, что мошенники используют фейковые видео с Илоном Маском и других известными сторонниками криптовалюты для рекламы платформы BitVex, которая ворует депонированные средства. В таких роликах знаменитости якобы дают интервью и рассказывают про BitVex, но на самом деле эти видео модифицированы — это дипфейки, где голос человека подделан и наложен на видеоряд, взятый из других источников.

3. Опубликованное в 2019 году, в котором Марк Цукерберг с помощью технологии дипфейка (deepfake) говорит о контроле над украденными данными. Цукерберг произносит на камеру: «Вообразите на секунду, что

один человек обладает полным контролем над миллиардами украденных данных людей, над всеми их секретами, их жизнями, их будущим». В конце ролика Цукерберг признаётся, что всей этой властью он обязан некоему «Спектру».

Таблица 1.

Описание основных целей deepfakes

Цель использования	Описание	Примеры
Мошеннические действия	Использование дипфейков для получения выгоды	Создание фальшивых видео с известными личностями
Влияние на общественное мнение	Формирование искажённых мнений	Распространение пропаганды, дезинформации
Дезинформация	Распространение ложной информации вводящей в заблуждение граждан	Фальшивые новости для введения в заблуждение
Имитация	Создание поддельного контента для развлечения, творчества, искусства	Шуточные пародии, искусство
Другое	Остальные цели использования	Различные прикладные применения

Для противодействия необходимо укреплять навыки критической оценки информации и совершенствовать инструменты выявления дипфейков. Дипфейки представляют собой серьёзную опасность для социума, требуя пристального внимания и внедрения действенных мер для их обнаружения и предотвращения распространения ложной информации.

Социальные медиа предоставляют широкие возможности для влияния на эмоциональное состояние людей, вызывая чувства страха, гнева, сострадания или гордости. Видео, мемы и публикации, воздействующие на эмоции, провоцируют сильные переживания, способствуя формированию определённой позиции по отношению к тем или иным событиям или личностям. Манипуляторы используют алгоритмические возможности платформ для усиления эмоционального резонанса и закрепления желаемой точки зрения.

Современные платформы применяют рекомендательные системы, формирующие "информационные пузыри" – изолированные сообщества, в которых пользователи сталкиваются исключительно с информацией, подтверждающей их убеждения. Это усиливает эффект единомыслия и способствует радикализации взглядов. Одной из ключевых угроз манипулирования в цифровом пространстве является вирусная природа распространения ложной информации. Манипулятивные материалы моментально становятся популярными, набирая миллионы просмотров и перепостов в кратчайшие сроки. В результате дезинформационные кампании достигают огромного охвата, часто минуя традиционные СМИ.

Применение анонимных учётных записей, ботов и скрытых источников затрудняет определение виновных и обнаружение организаторов манипуляций, что препятствует противодействию. Постоянное воздействие негативных, тревожных или пропагандистских видеороликов может приводить к психологическому истощению, апатии, стрессу и даже массовым паническим реакциям. Манипуляторы используют передовые технологии анализа данных и машинного обучения для адаптации контента под целевую аудиторию, повышая показатели своих операций.

Образовательные программы помогают пользователям распознавать дезинформацию, выявлять пропагандистские материалы и критически оценивать полученную информацию. Разработка систем автоматической

проверки фактов, алгоритмов обнаружения фейковых новостей, а также программ для анализа источников информации. Создание нормативных актов, регулирующих деятельность платформ, а также совместные международные инициативы по борьбе с распространением дезинформации. Повышение прозрачности работы алгоритмов рекомендаций и фильтров для минимизации возможности их использования в злонамеренных целях. Манипуляции через социальные сети и платформы обмена видео стали ключевыми инструментами информационно-психологического противоборства в XXI веке. Их действенность основывается на способности оперативно и в широких масштабах влиять на чувства и мысли целевой группы, создавать взгляды в обществе и ослаблять веру в достоверность сведений. Посредством быстрого и масштабного воздействия на чувства и мысли потребителей информации достигается результативность, что позволяет формировать общественное мнение и расшатывать уверенность в правдивости данных. Борьба с данными угрозами требует системного подхода, включающего развитие медийной грамотности, технологических решений и международного сотрудничества. В условиях продолжающейся цифровой трансформации роль этих методов будет только возрастать, что делает актуальной их регулировку и противодействие.

Стратегия повышения устойчивости к современным информационным угрозам

Разработка мер по выявлению и противодействию информационным угрозам, дезинформации, пропаганде, манипуляциям, формирование устойчивых информационных институтов, общественного мнения, участие в международных организациях, обмен информацией, совместные операции и договорённости по борьбе с киберпреступностью, а также противодействие информационным угрозам на глобальном уровне. Разработка систем предварительного предупреждения, оперативного реагирования и восстановления после киберинцидентов, а также создание национальных

центров реагирования на киберугрозы. Надёжная киберстратегия должна включать не только технические меры, но и психологические, информационные, дипломатические компоненты. В рамках информационно-психологического противоборства необходимо учитывать влияние информационных атак на общественное мнение, внутреннюю стабильность и внешний имидж государства. Создание национальной киберстратегии в рамках информационно-психологического противоборства требует комплексного, системного и многоуровневого подхода. Внедрение современных технологий, нормативно-правовых актов, развитие кадрового потенциала и межотраслевое взаимодействие позволяют обеспечить устойчивую защиту национальных интересов, повысить уровень информационной безопасности и противостоять современным угрозам в киберпространстве.

Заключение

Оценка современного состояния и особенностей информационного противоборства показывает нам, что в эпоху цифровых технологий и глобализации борьба за информационное превосходство становится главным элементом национальной безопасности и международных отношений. В условиях быстрого развития технологий и расширения возможностей автоматизации с применением искусственного интеллекта и больших данных, возрастает необходимость средств защиты, но одновременно возникают новые риски, связанные с этическими, правовыми и социальными аспектами. Борьба с информационными угрозами требует формирования национальных стратегий, включающая в себя укрепление инфраструктуры, развитие кадрового потенциала, международное сотрудничество и нормативно-правовое регулирование. Главными направлениями в данной области являются защита критической инфраструктуры, повышение уровня информационной грамотности населения, создание этических стандартов и развитие технологий противодействия. Особое значение приобретает

развитие системы мониторинга и автоматизированных систем анализа информационного пространства, что позволяет своевременно выявлять и устранять угрозы. Анализируя угрозы информационно-психологические операции противодействие таким вызовам требует системного, многоуровневого и межотраслевого подхода, объединяющего технические, правовые, социальные и этические меры. Противостояние информационно-психологическим угрозам возможно при постоянном совершенствовании средств защиты, развитии кадрового потенциала, внедрении инновационных технологий и формировании международного сотрудничества. Главным показателем является развитие системы мониторинга и автоматизации анализа информационного пространства, что позволяет своевременно выявлять и реагировать на угрозы, минимизировать их последствия и укреплять доверие граждан.

Таким образом, успешное противостояние современным вызовам в сфере информационно-психологического противоборства возможно только при интеграции технических, правовых, социальных и этических мер. Постоянное обновление методов, международное взаимодействие, развитие технологий и просветительская деятельность — это гарантия формирования устойчивых систем информационной безопасности. Системный и сбалансированный подход, основанный на сотрудничестве и инновациях, способен обеспечить защиту национальных интересов, сохранение стабильности и укрепление доверия в условиях современной информационной войны. Борьба за информационное превосходство зависит от способности адаптироваться к новым действительностям, внедрять инновационные решения и укреплять международное сотрудничество. Комплексный и сбалансированный подход, основанный на постоянном развитии и взаимодействии всех элементов системы, станет гарантией успешного противостояния современным вызовам и угрозам информационного противоборства.

Список использованных источников:

1. Крылова И.А. Информационно-психологические войны как фактор дезинтеграционных процессов в современном мире // Большая Евразия: развитие, безопасность, сотрудничество. 2021 № 4 С. 106-110.

2. Григорьев Н.Ю., Родюков Э.Б. Интернет как ресурс террористической угрозы // Актуальные проблемы общества и армии в контексте глобальных вызовов: материалы международной научно-практической конференции (Москва, 8 июня 2022 г.). М.: Спутник+, 2022 С. 21-26.

3. Цыганков С. В. Психологические условия повышения эффективности информационного воздействия на войска противника через сеть Интернет // Военная мысль. 2022 № 3 С. 96–101.

4. Караяни А. Г. Технологии дизруптивных событий и социального лазера в информационно-психологическом воздействии // Профессиональное образование сотрудников органов внутренних дел. Педагогика и психология служебной деятельности: состояние и перспективы. V Международная конференция: сборник научных трудов / сост. А. В. Кравченко. М., 2021 С. 45–48.

5. Караяни А. Г. Конструирование ложных событий как технология информационно-психологического воздействия / А. Г. Караяни, Ю. М. Караяни // Ананьевские чтения-2022. 60 лет социальной психологии в СПбГУ: от истоков – к новым достижениям и инновациям: материалы Международной научной конференции. СПб., 2022 С. 569–570.

6. Караяни А. Г. Нейрокогнитивные технологии негативного информационно-психологического воздействия // Профессиональное юридическое образование и наука. 2023 № 4 (12). С. 38–40.

7. Кузьмович А.В. Эволюция взглядов на теорию современной войны. Тюрнев А. С., Помелов А. А., Шелегов Ю. В. Обеспечение

информационной безопасности: правовые аспекты проблемы // Вестник экономической безопасности. 2022 № 2 С. 169-173.

8. Информационная безопасность (Кн. 2 социально-политического проекта «Актуальные проблемы безопасности социума»). М.: Оружие и технологии. 2023

9. Сергеев И.В. Информационно-психологическая война как форма эскалации межгосударственных конфликтов // Информационные войны. 2022 № 2(34). С. 38–41.

Сведение об авторе:

Трофимов Иван Александрович – студент кафедры «Интеллектуальные системы информационной безопасности». Института кибербезопасности и цифровых технологий Российского технологического университета МИРЭА, г. Москва, Россия e-mail: vanyusha_trofimov_01@bk.ru

Information about authors:

Trofimov Ivan A. – Student, Department of Intelligent Systems of Information Security, Institute of Cybersecurity and Digital Technologies, Russian Technologica University MIREA, Moscow, Russia e - mail: vanyusha_trofimov_01@bk.ru