RUDN Journal of Public Administration
ISSN 2312-8313 (print), ISSN 2411-1228 (online)
Вестник РУДН. Серия:
ГОСУДАРСТВЕННОЕ И МУНИЦИПАЛЬНОЕ УПРАВЛЕНИЕ

2024 Том 11 No 1 19–31
http://journals.rudn.ru/
publicadministrationy

DOI: 10.22363/2312-8313-2024-11-1-19-31
EDN: ZIXNDI

Научная статья / Research article

Информационная война как инструмент политического противостояния в современном многополярном мире

И.В. Гончарова[1], В.Ф. Ницевич[2], О.А. Судоргин[2] ✉

[1]Орловский государственный аграрный университет имени Н.В. Парахина,
302019, Российская Федерация, Орёл, ул. Генерала Родина, д. 69

[2]Государственный университет управления,
109542, Российская Федерация, Москва, Рязанский просп., д. 99

✉ svis@mail.ru

Аннотация. Анализируется феномен информационной войны в современном мире. Конкретизируется понятие информационной войны и ее взаимосвязь с гибридной войной, которая пришла на смену механизмам прямого «силового» воздействия в условиях стремительно меняющейся политической архитектуры. Раскрывается значение войн XXI в., которые ведутся с позиции «мягкой силы» и отличаются затяжным характером. Информационная война рассматривается как их важнейшая составляющая. Выделяются особенности информационных войн: они ведутся в культурном поле, их целью является трансформация сознания политического оппонента. Эти войны направлены на ценностные ориентиры, традиции, историческую и культурную идентичность. Появление понятия «информационная война» связывает с завершением Холодной войны в конце XX в. и определением новой стратегии США. Раскрываются условия и причины перехода к войнам нового типа: крушение биполярного мира, нарастание угрозы международного терроризма, размывание этнокультурной идентичности внутри самих США и союзных стран. Анализируется кибернетические войска как новый специализированный вид войск. Раскрываются два основных пространства воздействия информационной войны: коммуникативная среда и поле вероятного социального макроконфликта. Информационная война в исследовании рассматривается как часть военного, экономического, геополитического противостояния. Авторы обосновывают, что против Российской Федерации уже более 20 лет ведется крайне интенсивная по насыщенности средств информационная война. Она предполагает лишение России не только союзников, но и замены «культурно-исторических кодов» в дружественных нам странах, в первую очередь, путем переформатирования сознания молодежи. Анализируется документы, направленные на решение проблемы информационных войн в России: «Доктрина информационной безопасности Российской Федерации» и «Стратегия национальной безопасности РФ».

Ключевые слова: гибридная война, информационная война, кибервойска, киберпространство, информационная стратегия, информационная безопасность

Заявление о конфликте интересов: Авторы заявляют об отсутствии конфликта интересов.

История статьи:
Поступила в редакцию: 01.12.2023. Принята к публикации: 10.01.2024.

Для цитирования:
Гончарова И.В., Ницевич В.Ф., Судоргин О.А. Информационная война как инструмент политического противостояния в современном многополярном мире // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2024. Т. 11. № 1. С. 19–31. https://doi.org/10.22363/2312-8313-2024-11-1-19-31

Information Warfare as a Tool of Political Confrontation in the Modern Multipolar World

Irina V. Goncharova[1], Victor F. Nicevich[2], Oleg A. Sudorgin[2] ✉

[1]N.V. Parakhin Orel State Agrarian University,
69 Generala Rodina St, Orel, 302019, Russian Federation

[2]State University of Management,
99 Ryazansky prospect, Moscow, 109542, Russian Federation

✉ svis@mail.ru

Abstract. The study is devoted to the analysis of the phenomenon of information warfare in the modern world. Authors concretized the concept of information warfare and its connection with hybrid warfare, which has replaced the mechanisms of direct "forceful" influence in a rapidly changing political architecture. The significance of the wars of the XXI century, which are conducted from the position of "soft power" and are characterized by a protracted nature, is revealed. Information warfare is considered as their most important component. The authors highlight the following features of information wars: they are conducted in the cultural field; their purpose is to transform the consciousness of a political opponent. These wars are aimed at value orientations, traditions, historical and cultural identity. The emergence of the concept of "information warfare" in the article is associated with the end of the Cold War at the end of the XX century and the definition of a new U.S. strategy. The main conditions and reasons for the transition to a new type of war are the collapse of the bipolar world, the growing threat of international terrorism, and the erosion of ethnic and cultural identity within the United States and allied countries themselves. Cybernetic troops are analyzed as a new specialized type of troops. The authors revealed two main spaces of the information war impact: the communicative environment and the field of probable social macro-conflict. Information warfare in research is considered as part of a military, economic, and geopolitical confrontation. The authors substantiate that an extremely intensive information war has been waged against the Russian Federation for more than 20 years. It involves depriving Russia not only of allies, but also replacing the "cultural and historical codes" in friendly countries, primarily by reformatting the consciousness of young people. The authors analyzed the documents aimed at solving the problem of information wars in Russia — the "Information Security Doctrine of the Russian Federation" and the "National Security Strategy of the Russian Federation".

Keywords: hybrid warfare, information warfare, cyber warfare, cyberspace, information strategy, information security

Conflicts of interest: The authors declared no conflicts of interest.

Article history:
The article was submitted on 01.12.2023. The article was accepted on 10.01.2024.

For citation:
Goncharova I.V., Nicevich V.F., Sudorgin O.A. Information Warfare as a Tool of Political Confrontation in the Modern Multipolar World. *RUDN Journal of Public Administration.* 2024;11(1):19–31. https://doi.org/10.22363/2312-8313-2024-11-1-19-31

Введение

На сегодняшний день информационные войны занимают главное, а в отдельных случаях решающее место в противостоянии как между отдельными государствами, так и на уровне отдельных политических образований и союзов государств. В силу стремительно нарастающей политической неопределенности, в условиях стремительно меняющейся политической архитектуры мира на смену механизмам прямого «силового» воздействия пришли «гибридные войны» («hybrid warfare»), предполагающие сочетание традиционных («классических») методов ведения боевых действий и применение так называемой «мягкой силы». Следует отметить, что подавляющая часть войн XX в., ведущихся вышеуказанными «традиционными методами», отличалась масштабными разрушениями в воюющих странах, сопровождавшимися глубоким экономическим кризисом, политической деформацией вплоть до крушения прежней политической системы, психологическим надломом общества. Войны XXI в., ведущиеся с позиции «мягкой силы», отличает затяжной характер. Они ведутся в культурном поле, а их целью является трансформация сознания политического оппонента, который может не подозревать, что находится в эпицентре «ведения боевых действий». Объектами подобных войн являются ценностные ориентиры, традиции, историческая и культурная идентичность той или иной страны.

Обсуждение

О понятии «информационная война»

С нашей точки зрения, наиболее емкую оценку гибридной войны дал генерал-майор А.И. Владимиров. Он указывал, что главной задачей гибридной войны является «…постепенное погружение государства–жертвы в состояние «организованного хаоса», достижение его «сокрушения измором» вне применения вооруженных форм войны». При этом театром ведения боевых действий, условной «серой зоной», в которой разворачивается конфликт, может быть не только отдельные государства, но и их конгломерат. Опасность гибридной войны состоит в том, что «несиловыми методами», парализующими возможность применения норм международного права, поражаются практически все сферы жизнедеятельности государства: экономическое и политическое пространства, сфера науки и образования, сфера здравоохранения, разрушается идеологическое пространство, нравственность и мораль, культурная идентичность общества [1].

Как и любая война, гибридный конфликт предполагает взаимосвязанную совокупность нетрадиционных боевых операций (то есть проводимых без вмешательства вооруженных сил и силовых структур), которые понимаются как «гибридные операции» (hybrid operations). В отдельных исследованиях выделяется шесть основных видов гибридных операций: психологические, направленные на подавление духа и лишения мотивации к сопротивлению; экономические, провоцирующие застойные и кризисные процессы в экономике, вплоть до экономического коллапса; массовые протестные акции оппозиции; диверсионные действия незаконных военизированных структур, не имеющих связи с другими государствами; воздействие с применением кибернитического оружия. Но наиболее значимым, а, по сути, непрерывно действующим на всем протяжении противостояния видом гибридных операций является комплекс информационного воздействия, который следует понимать как самодостаточную информационную войну. Обратим внимание на то, что в ряде работ гибридный конфликт определяется как военная стратегия, использующая, наряду с традиционными «силовыми способами», комплекс информационно-психологических инструментов.

По официальной версии термин «информационная война» впервые был конкретизирован в 1980-е гг., хотя его употребление относят к 1976 г. Его применение связывают с отчетом Томаса Рона «Системы оружия и информационная война» [2], он был разработан для Boeing Aerospace Co. Рон писал: «…информационная инфраструктура становится ключевым компонентом американской экономики, но она одновременно превращается в уязвимую цель как в военное, так и в мирное время» [3. С. 11–15].

«Конкретизированный термин» определял новую стратегию США с завершением «холодной войны». Активное употребление термина относится к периоду после завершения операции «Буря в пустыне». Именно к этому моменту формируется материальная база и общая философия применения оружия нового типа. На официальном уровне область его применения нового термина в общем виде была определена в следующих документах: 1) Директива министра обороны США № TS-3600.1 «Информационная война», вышедшая в декабре 1992 г.; 2) Директива председателя КНШ МОР № 30–93 в 1993 г.; 3) Единый устав КНШ № 3–13.1 «Совместные действия разнородных сил по борьбе с системами управления противника», 1995 г.; 4) Инструкции КНШ 3210.01 А «Единая перспектива-2010»; 5) «Концепция информационных операций объединенных группировок вооруженных сил» 1996 г. и ряд др. [4. С. 2–9]. Активная военно-теоретическая и военно-политическая деятельность силовых структур США по изучению возможностей информационного воздействия на своих политических оппонентов показывает серьезную значимость данного вида «непрямых» («мягких») методов военных действий на рубеже XX–XXI вв.

Переход к информационной войне США

Причинами перехода к войнам нового типа стали крушение биполярного мира, нарастание угрозы международного терроризма, размывание этнокультурной идентичности внутри самих США и ряда стран, следующих в кильватере ее политики. Так как информационные войны ведутся в «серой зоне», в условиях мнимой военно-политической стабильности, ряд экспертов отмечает, что на современном этапе в стратегии информационной войны, которую ведут США, произошли существенные изменения. В частности, изменилось понимание категории киберпространства (cyberspace), в котором происходит значительная часть процессов информационного противоборства. Киберпространство понимается как важнейший компонент единого информационного пространства. Теперь «глобальное киберпространство» включает в себя «синюю» (американскую), «красную» (вражескую) и «серую» (нейтральную) области. При этом считается, что «…разрешено на «законном основании» проводить кибероперации в любом иностранном киберпространстве («красной» и «серой» зонах) без уведомления органов власти этих стран на том основании, что киберпространство не имеет государственных границ» [5. С. 22–29]. Информационное противостояние может иметь «превентивный характер». Более глубоко проработано понимание того, что представляет собой кибератака как «атака в киберпространстве» [5. С. 22–29].

Следует также обратить внимание на то, что противоборствующие стороны разрабатывают особую терминологию, призванную исказить истинное содержание скрытой военно-политической активности (по сути, мы имеем дело с откровенными смысловыми симулякрами). Так, первоначально в качестве термина, обозначающего способы ведения информационной войны, использовалось словосочетание «информационные операции», позднее в научно-теоретической и политической риторике появляются термины «стратегические коммуникации» и «публичная дипломатия».

Отечественные эксперты (в частности, полковник П. Колесов) отмечают: «Стратегические коммуникации… это новая концепция самих ИВ… Цель СК — убеждение или принуждение целевой аудитории к принятию решений или совершению действий, направленных на формирование, сохранение или развитие благоприятных условий для продвижения американских национальных интересов» [6. С. 9–14]. Главными инструментами воздействия на противника считаются: «согласованные информационные акции, идеологическая обработка, различные информационно-пропагандистские планы и программы». Их реализуют «министерство обороны США, боевые командования ВС, инженерные войска, агентство по международному развитию, госдепартамент» и ряд других структур [6. С. 9–14].

Примечательно, что к нулевым годам XXI в. начинает оформляться новый вид войск — кибернетические войска. На сегодняшний день архитектура данного рода войск применительно к США и НАТО включает в себя:

1) структуры МО США — округ Ардингтом, штат Вирджиния;

2) структуры стратегического командования США — база США Оффут, штат Небраска;
3) киберкомандование США — форт имени Джорджа Дж. Мида;
4) АНБ США (20 тыс. чел., бюджет около 3 млрд долларов);
5) информационный оперативный центр ЦРУ (общая численность штатных сотрудников ЦРУ около 15 тыс. чел., бюджет 3 млрд долларов);
6) в качестве отдельных структуры можно выделить: разведывательное управление объединенного штаба J, разведывательное управление МО США со штатом 6 тыс. чел., разведывательное управление ВВС США;
7) в ФБР также созданы специальные отделения для противодействия компьютерным преступлениям;
8) Агентство коммуникации и информации НАТО — г. Брюссель;
9) Объединенный центр передового опыта электронного противодействия НАТО — г. Таллин, Эстония;
10) Объединенный центр передового опыта стратегических коммуникаций НАТО — г. Рига, Латвия.

В данном случае перечень структур, осуществляющих информационное воздействие («наступательные операции») и противодействие («оборонительные операции»), не носит исчерпывающего характера. Общая численность кибервойск отдельных стран НАТО к началу 2020-х гг. представлена в таблице.

Общая численность кибервойск отдельных стран НАТО

Название страны	Общая численность кибервойск
США	64 000 чел.
ФРГ	14 500 чел. (в стране функционирует «центр обеспечения безопасности информационной техники» со штатом в 500 чел.)
Франция	4000 чел. (в стране также идет разработка системы информационной безопасности «Эшелон»)
Великобритания	2000 чел. (проблемой занимается департамент правительственных коммуникаций численностью до 6000 чел.)

Несмотря на то, что североамериканское оборонное ведомство тратит ежегодно 10 млрд долларов на обеспечение информационной безопасности, американские военные эксперты продолжают отмечать сохраняющуюся информационнаю уязвимость страны и отсутствие возможности обеспечения полной информационной безопасности. Вследствие этого: «…рассматривается вариант реорганизации киберкомандований в командования информационных операций, что позволит объединить единым замыслом кибернетические, психологические и радиоэлектронные операции» [5. С. 22–29]. Оперативное развертывание данного институционального образования планируется завершить в 2028 г.

Первоначально общая концепция информационной войны затрагивала два основных пространства воздействия: коммуникативную среду и поле

вероятного социального макроконфликта. Главным средством ведения войны становилась разноплановая информация и механизмы работы с ней. При этом информационная война рассматривалась не как самодостаточное явление, а как часть военного, экономического, геополитического противостояния. Как следствие на **макроуровне** информационные (информационно-психологические) войны определялись как форма противостояния в мировой и локальной информационной средах, реализуемая манипулятивными методами, технологиями и способами воздействия на информационное и психологическое поля противоборствующей стороны (контрагента) с целью нанесения ему максимального ущерба.

В директиве министерства обороны США Т. 8 3600.1 в качестве основных видов реализации информационной войны отмечались:

«1) политические, дипломатические и экономические акции;
2) информационные и психологические операции;
3) подрывные и деморализующие пропагандистские действия;
4) содействие оппозиционным и диссидентским движениям;
5) оказание всестороннего влияния на политическую и культурную жизнь с задачей развала национально-государственных устоев общества;
6) проникновение в систему государственного управления;
7) защита национальных информационных систем» [7].

Особое внимание уделяется «военному уровню» информационной войны, основной целью которого является «достижение информационного господства над противником в вооруженном конфликте и защиту собственных систем управления от информационного оружия противника» [7]. Согласно директиве КНШ в марте 1993 г. «Борьба с системами управления», военный уровень решает задачи, помимо радиоэлектронного и физического уничтожения систем связей противника, введение его в заблуждение и психологическую борьбу [7].

Идентичные виды информационной борьбы зафиксированы в учебных программах Университета национальной обороны США. В них наряду с радиоэлектронной, рассматриваются психологическая, разведывательная, кибернетическая войны.

В свою очередь, возможен и микроуровень определения информационной войны. В данном случае ее можно интерпретировать как совокупность дискретных операций (воздействий), осуществляемых в информационном пространстве (поле), направленных на достижение превосходства над контрагентом, управления (манипуляции) его действиями. К основным целям информационной войны на микроуровне принято относить:

1) максимально полный контроль приватного информационного пространства;
2) его защита;
3) возможность получения приватной информации контрагентов;

4) возможность воздействия на их информационную систему, вплоть до ее разрушения.

Обобщая вышеизложенные рассуждения, можно утверждать, что информационные войны призваны решать задачи укрепления позитивной мотивации и стрессоустойчивости населения данной страны и ее вооруженных сил, с одной стороны, провоцирования депрессивных настроений и психологического хаоса у населения стран-контрагентов, создания отрицательно политического и культурного имиджа стран-контрагентов на уровне мирового сообщества, с другой стороны.

Сегодня мы можем констатировать, что против Российской Федерации уже более 20 лет ведется крайне интенсивная по насыщенности средств информационная война. Еще в начале 1990-х гг. США в качестве приоритетов своей внешней политики в «условной доктрине» Пола Вулфовица (в версии от 15.04.1992 г.) декларировали потенциально враждебное отношение к обновленной России. В частности, подчеркивалось: «…мы должны помнить, что демократические перемены в России не являются необратимыми и что, несмотря на нынешние трудности, Россия останется сильнейшей военной державой в Евразии и единственной державой в мире, способной уничтожить Соединенные Штаты» [8].

Данный доктринальный подход предполагал сохранение политической гегемонии США в мире путем осуществления «конца истории» — создания системы однополярного мира. Одной из возможных форм как можно длительного сохранения сложившейся ситуации предполагалось создание «кордона» против «потенциально сильной» России — расширение НАТО на Восток за счет включения в НАТО стран Балтии и начала межправительственного и международного диалога о включении в состав блока Украины и Грузии. В данном случае одним из инструментов раскачивание политической ситуации становились «цветные революции» вдоль границ России как инструмент перманентной «гибридной войны». Элементом этого комплекса «непрямых действий» становилась информационная война.

Обеспечение информационной безопасности России

По мнению министра иностранных дел РФ С.В. Лаврова, целями гибридной и, как следствие, информационной войны против России является создание вокруг страны: «…пояса нестабильности, принуждая наших ближайших соседей и братские нам народы делать выбор — либо ты с Западом, либо ты с РФ» [9]. Данная политика направлена на предотвращение самой возможности геоэкономической консолидации Евразии. Она предполагает лишение России не только союзников, но и замены «культурно-исторических кодов» в дружественных нам странах, в первую очередь, путем переформатирования сознания молодежи.

Важное место в осознании и решении проблемы гибридных и информационных войн сыграло принятие в России «Доктрины информационной

безопасности Российской Федерации» (Указ Президента Российской Федерации от 5.12.2016 № 646) и «Стратегии национальной безопасности РФ» (Указ Президента Российской Федерации от 2.07.2021 № 400).

В «Доктрине информационной безопасности Российской Федерации» в перечне угроз в информационной сфере выделены:

1) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
2) стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве;
3) укрепление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;
4) увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики РФ;
5) увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры;
6) нарастание угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности РФ.

Таким образом, главными направлениями обеспечения информационной безопасности в области обороны РФ становятся:

1) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
2) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;
3) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;
4) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;
5) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества [10].

Содержание анализа основных информационных угроз Российской Федерации со стороны условного «коллективного Запада» на современном отрезке времени позволяет выделить в качестве объектов информационной войны: вооруженные силы РФ, задействованные в СВО; военнослужащих и органы власти ДНР и ЛНР; гражданское население России и союзного нам

государства Беларусь (дети и супруги военных); политиков и жителей западных стран, симпатизирующих России; политиков и обывателей незападных и антизападных стран.

К субъектам информационной войны принято относить наиболее значимые политические фигуры государства, кибервойска, о которых мы упоминали выше, средства массовой информации, гражданские лица, вышедшие из зоны ведения боевых действий (беженцы).

Среди политиков, обладающих реальным политическим весом, чаще всего выделяют представителей федерального уровня политической элиты страны: главу государства; премьер-министра (председателя правительства) и глав отдельных, наиболее значимых министерств; отдельных представителей МИДа; наиболее значимых представителей министерства обороны и отдельных силовых структур; представителей законодательной власти; глав наиболее значимых субъектов государства. Представители политической элиты, а также военно-политическое руководство стран, как правило, формируют пространство, содержание и направление информационного противостояния.

Говоря о средствах массовой информации как инструменте информационных войн, западные эксперты выделяют две таких «условных» группы СМИ в современной России. При этом считается, что «…в отличие от американских экспертов, немецкие рассматривают управление средствами массовой информации как элемент информационной войны» [3. С. 11–15]. В этом плане российский опыт ведения информационной войны, по мнению исследователей, ближе к немецкому опыту, чем к американскому.

К первой группе российских СМИ в контексте проблемы ведения информационных войн относят телеканалы и радиоканалы, равно как и разнообразную печатную продукцию, озвучивающие официальную повестку органов государственной власти. Как правило, они имеют полное или частичное государственное финансирование и работают не только на отечественного, но и на зарубежного потребителя.

Справедливости ради следует сказать, что в теории «стратегической коммуникации» США СМИ также играют не последнюю роль. Эксперты отмечают, что американский набор коммуникативных инструментов обширен. Сюда входят «средства массовой информации (СМИ), а также связь и телекоммуникации, инфраструктура беспроводной связи, социологические исследования, культурологические и лингвистические средства, избирательные технологии и методики подсчета голосов избирателей, массовые тренинги и образовательные программы» [6. С. 9–14]. Но все же главную роль в этом процессе продолжают играть СМИ.

В России важную роль в формировании официального имиджа страны за рубежом играла компания «Россия сегодня» (Russia Today; RT). Компания начала работу в июне 2005 года. Ее целью являлось продвижение России как позитивного политического и культурного бренда за границей. RT управляется автономной некоммерческой организации «ТВ-Новости».

Еженедельная аудитория компании приближается к 100 млн чел. в 47 странах [11].

Вторую группу отечественных СМИ в рассматриваемом формате формируют оппозиционные и антироссийские радио- и телеканалы, печатная продукция и информационные сайты. Работа этих средств находится под контролем Роскомнадзора и Министерства юстиции РФ в соответствии с Федеральным законом от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории РФ». В 2022 г. были заблокированы сайты Beats-1, Steam, Spotify, Pandora, FOX. В свою очередь социальные сети компании Meta были идентифицированы в нашей стране как экстремистские. Их ресурсы прекратили действие в 21 марта 2022 г.

Проблема беженцев также является крайне актуальной для понимания военно-информационного противостояния. Люди, пострадавшие от локальных и региональных конфликтов, часто становятся инструментом «грязных» инсинуаций и информационной пропаганды. Зачастую их личную трагедию используют для «обесчеловечивания» образа одной из противоборствующих сторон. При этом осуществляется крайне интенсивная эксплуатация эмоционального поля мировой общественности (формирования возмущения, негодования, озлобленности, агрессии). Лицам, оказавшимся заложниками информационной войны, крайне сложно сформировать объективную оценку происходящих событий.

Важное место в реализации различных стратегий информационных войн занимает информационное оружие. В отечественной теории информационной войны его принято делить: по сфере применения — на информационно-техническое и информационно-психологическое; по целевому назначению — на оборонительное и наступательное («наступательные и оборонительные информационные операции могут проводиться по единому замыслу и плану и взаимно дополнять друг друга» [4]).

Особое место в информационном противостоянии занимает «психологическая война», в арсенале которой находятся различные виды воздействия информационных средств, от пропаганды до создания виртуальной реальности. С целью манипуляции массовым сознанием применяются аудио- и видеосимулякры, в т.ч. подделываются изображения и голоса политиков и выдающихся личностей. Дезинформация проводится путем изменения информационных баз данных противника, геолокации, навигационных систем и т.д. [12].

Одним из распространенных приемов современной информационной войны является «бомбардировка» контрагента фейковой информацией или фейками. Данный термин является производным от английского слова «fake», что можно интерпретировать как «подделку» или «фальсификат», также допустим перевод «мошенничать», «дурачить», «обманывать». С помощью фейков активно симулируется и искажается реальное пространство событий. Фейки, как правило, делят на «простые» и «сложные». В качестве основных приемов для

создания фейков используют: распространение заведомо ложной информации об актуальном социально-значимом событии; демонстрация недостоверных фото- и видеодокументов, не относящихся к зоне событий; фальсификация подписей под достоверными фото- и видеодокументами; постановочная видеосъемка; демонстрация фрагментов видеоигр, извлечений из художественных фильмов, продуктов, созданных с помощью компьютерной графики.

Заключение

Подводя итог вышесказанному, следует подчеркнуть, что информационные войны стали необратимой реальностью, постоянно вторгающейся не только в пространство функциональных полей отдельных государств, но и в повседневную жизнь каждого отдельно взятого человека. Вместе с тем информационные войны высветили уязвимые стороны даже демократических обществ, сделали их более хрупкими и уязвимыми. Авторитарные механизмы воздействия сменились многоканальными механизмами манипуляции общественным сознанием, трансформировались в систему тотального контроля над человеческим сознанием. Заложниками сложных политических игр и противостояния в информационном поле становятся простые обыватели, оказавшиеся в перманентной «информационной осаде», в условиях «информационной перегрузки», порождающей нарастающий стресс и разнообразные фобии. Одновременно с этим возникает эффект фрагментации общества, наполнявшегося многообразными симуляциями. Можно утверждать, что человечество оказалось перед угрозой грандиозной катастрофы ойкуменического масштаба, поскольку значительная часть человечества либо лишилась, либо не успела приобрести адекватных средств осмысления стремительно меняющего, абсолютно «непрозрачного» и непредсказуемого мира.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Владимиров А.И.* Основы общей теории войны: монография: в 3 ч. М.: Московский финансово промышленный университет «Синергия», 2018. 2856 с.
2. *Rona T.P.* Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976. 50 p.
3. *Гриняев С.* Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. 2002. № 2. С. 11–15.
4. *Жуков В.* Взгляды военного руководства США на ведение информационной войны // Зарубежное военное обозрение. 2001. № 1. С. 2–9.
5. *Дылевский И., Базылев С., Запивахин О., Комов С.А. Песчаненко К., Юниченко С.* О взглядах администрации США на киберпространство как новую сферу ведения военных действий // Военная мысль. 2020. № 10. С. 22–29.
6. *Колесов П.* Ведение Соединёнными Штатами информационных войн. Концепция «Стратегических коммуникаций» // Зарубежное военное обозрение. 2010. № 6. С. 9–14.
7. *Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В.* Системы защиты информации в ведущих зарубежных странах. Брянск: БГТУ, 2007. 203 с.
8. *Вертлиб Е.* Война ресурсная в контексте гибридно-ментальной // Русская народная линия. 11.10.2022. URL: https://ruskline.ru/news_rl/2022/10/11/voina_resursnaya_v_kontekste_gibridnomentalnoi?ysclid=lrkuz7ixof126111033 (дата обращения: 10.11.2023).

9. *Колесникова М.* Запад пытается создать «пояс нестабильности» вокруг РФ // The Moscow Post. 23.07.2021. URL: http://www.moscow-post.su/politics/zapad_pytaetsya_sozdat_poyas_nestabilnosti_vokrug_rf36446/?ysclid=lrkv4nd58c871899594&utm_source=ya.ru&utm_medium=referral&utm_campaign=ya.ru&utm_referrer=ya.ru (дата обращения: 10.11.2023).
10. Об утверждении Доктрины информационной безопасности Российской Федерации (Указ Президента Российской Федерации от 05.12.2016 № 646). URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 10.11.2023).
11. Russia Today TV (RTTV). URL: https://rkn.gov.ru/mass-communications/reestr/media/?id=315435 (дата обращения: 10.11.2023).
12. Информационная война (Определение информационного оружия) // Линия Сталина. 25.02.2022. URL: https://stalinline.ru/2022/02/25/informaczionnaya-vojna/?ysclid=lpbnapyns8740653990 (дата обращения: 10.11.2023).

Информация об авторах:

Гончарова Ирина Валентиновна — доктор исторических наук, профессор кафедры истории, философии и русского языка Орловского государственного аграрного университета имени Н.В. Парахина (ORCID ID: 0000-0002-7532-8751) (e-mail: int@orelsau.ru).

Ницевич Виктор Францевич — доктор политических наук, ведущий научный сотрудник НИИ Государственной политики и управления отраслевой экономикой Государственного университета управления (ORCID ID: 0000-0002-1668-3067) (e-mail: dr.nitsevich@mail.ru).

Судоргин Олег Анатольевич — доктор политических наук, директор НИИ Управления цифровой трансформацией экономики Государственного университета управления (ORCID ID: 0000-0001-7670-7238) (e-mail: svis@mail.ru).