ИНФОРМАЦИОННАЯ ВОЙНА: ПОНЯТИЕ, ФОРМЫ, МЕТОДЫ (ОПЫТ США)

А. Р. Романовский[1)], С. Ф. Свилас [2)]

[1)]Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, aromanovsky35@gmail.com
[2)]Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, svilas@tut.by

В XXI веке информация становится важнейшим фактором прогресса при одновременном обострении борьбы за власть в информационной сфере. США рассматривают киберсферу как ключевое поле для собственной гегемонии, в то время как Беларусь, Россия, Китай, другие государства стремятся защитить свое информационное пространство. Цель авторов – охарактеризовать усилия США по достижению стратегического информационного доминирования в мире. В статье на основе исследований американских и российских специалистов, а также документального материала рассматриваются подходы американской администрации и экспертов к определению понятия «информационная война», формы и методы ее ведения. Посредством анализа теоретического и практического опыта США подчеркнуто влияние информационно-коммуникационных технологий на общественную жизнь, выделены основные этапы формирования концептуальной базы в области информационных войн, обозначены уровни и инструменты их ведения, определены критерии эффективности операций. Практическая значимость работы – в возможности ее использования в научной и учебной деятельности.

Ключевые слова: США; информационно-коммуникационные технологии; информационная война; методы информационной войны; кибервойна; сетевая война.

INFORMATION WARFARE: DEFINITION, FORMS, METHODS (U.S. EXPERIENCE)

A. R. Romanovsky [a], S. F. Svilas [b]

[a]Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus
Belarusian State University, Niezaliežnasci Avenue, 4, 220030, Minsk, Belarus
Corresponding author: A.R. Romanovsky (aromanovsky35@gmail.com)

In the 21st century, information is becoming the most important factor of progress, while the struggle for power in the information sphere is intensifying. United States view the cybersphere as a key area for its own hegemony, while Belarus, Russia, China, and other countries seek to protect their information space. The purpose of the article is to characterize U.S. efforts to achieve strategic information dominance in the world. Based on the research of American and Russian experts, as well as documentary material, the article

examines approaches to defining the concept of "information warfare", forms and methods of its conduct. Through an analysis of theoretical and practical experience in the United States, the impact of information and communication technologies on public life is demonstrated, the basic stages of formation of conceptual base in the field of information wars are allocated, levels and tools of their conducting are designated, criteria of efficiency of operations are defined. The practical significance of this publication lies in the possibility of its approbation in scientific and scholarly pursuits.

Key words: USA, information and communication technologies; information warfare; information warfare methods; cyberwarfare; network warfare.

Стремительное внедрение информационно-коммуникационных технологий во все сферы общественной жизни в конце XX – начале XXI вв. значительно изменили характер, методы и способы информационной деятельности государственных структур и особенно вооруженных сил наиболее развитых государств. ИКТ оказали существенное влияние на стратегию и тактику, формы и способы подготовки и ведения военных действий в ходе конфликтов, расширили круг участников информационного воздействия и противодействия, а также качество и разнообразие его видов и форм.

В международном научном и общественно-политическом обиходе прочно закрепилось понятие «информационная война» (ИВ). Некоторые западные эксперты рассматривают информационную войну как новый вид конфликта, который не имеет международно-правовой квалификации.

Среди экспертов существует определённая путаница относительно содержания понятия «информационная война», а ее определение на государственном уровне в США отсутствует. Для характеристики информационной войны нередко используются такие термины, как «активные мероприятия», «гибридная война», «война в серой зоне», «нерегулярные военные действия», «нетрадиционная война», «асимметричная война», «мягкая сила», «публичная дипломатия» [1]. Кроме того, в американских источниках с начала 1990-х гг. также закрепилось понятие «Information warfare», которое более точно переводится как «информационное противоборство».

В научный оборот понятие «информационная война» впервые ввел в 1976 г. американский эксперт Т. Рона, который анализировал уязвимости информационных потоков в системах вооружений [2]. В первой половине 1990-х гг. группа ученых Авиационного университета ВВС США (Дж. Стейн и Р. Шафрански) сформулировала ключевые требования к информационной войне. Эти эксперты исходили из того, что в будущем конфликте решающую роль возьмет на себя информация (точнее, знания), а не традиционные средства ведения войны. Сами информационные технологии рассматриваются в данной концепции только как сред-

ство, обеспечивающее достижение стратегического информационного доминирования, под которым понимается создание информационных условий, когда действия противника в конечном итоге неизбежно окажутся выгодными противоположной стороне или будут направлены на обслуживание ее интересов [3, с. 12-13]

Сюда же можно отнести и работы старшего научного сотрудника RAND Corporation М. Либицкого, который определил семь форм ведения информационной войны в целях обеспечения американского превосходства в военном конфликте: командно-управляемые, разведывательные, психологические, экономические, электронные, хакерство и кибер-борьбу [4].

Во второй половине 1990-х гг. авторитетный американский эксперт Дж. Арквилла разработал вопросы стратегии и тактики кибервойны и сетевой войны. По его мнению, информационная война охватывает широкий спектр действий в информационном пространстве, начиная от атак на коммуникационные системы и критическую инфраструктуру и заканчивая использованием ИКТ в целях оказания психологического воздействия [5].

Понятие «кибервойна» сосредоточено на военных аспектах и представляет собой конфликт высокой интенсивности исключительно между вооруженными силами противоборствующих сторон, которые ведут борьбу с системами командования и управления с целью исказить или уничтожить информационные системы противника. В свою очередь, сетевая война охватывает экономические, политические, социальные, а также военные формы противоборства. Ее целью является воздействие на общественное мнение и мнение элит посредством дипломатических методов, пропаганды, психологических кампаний, вмешательство в деятельность местных СМИ, несанкционированное проникновение в компьютерные системы и базы данных, а также поддержка диссидентов и оппозиционных движений в информационных сетях.

Как отмечает российский эксперт А. Бедрицкий, в начале XXI века информационная война и информационные операции окончательно перестали считаться сугубо теоретической проблемой и перешли в практическую плоскость [3, с. 20]. При этом значительное внимание стало уделяться работе в социальных сетях.

Одна из ключевых ролей в проведении информационных войн в США принадлежит Министерству обороны. Разработанная Пентагоном концепция ведения информационной войны реализуется на общегосударственном и военном уровнях. Для государства цель информационного противоборства, формулируемая широко, заключается в ослаблении позиций стран-конкурентов, подрыве их национально-государственных устоев, наруше-

нии системы государственного управления путем информационного воздействия на политическую, дипломатическую, экономическую и социальную сферы жизни общества, проведения психологических операций, подрывных и иных деморализующих пропагандистских акций.

В аналитическом докладе конгрессу США от 5 марта 2018 г. информационная война определяется как «использование и управление информацией с целью получения сравнительного преимущества, включая наступательные и оборонительные усилия» [1].

Информационная война может быть прелюдией к военному конфликту либо проводиться автономно без применения силы с целью достижения государством сравнительных преимуществ. В ней могут использоваться все инструменты национальной мощи – дипломатические, информационные, военные и экономические.

Оборонительные усилия включают обеспечение информационной безопасности, а наступательные усилия – информационные операции. ИВ ведется на стратегическом уровне (государства), в то время как во время информационных операций, которые проводятся на оперативном уровне, применяются различные инструменты для достижения поставленной стратегической задачи. Такими инструментами могут быть стратегическая коммуникация, общественная дипломатия, а также операции в киберпространстве.

В то же время информационные операции могут проводиться и за пределами киберпространства, например, в форме распространения брошюр, организации культурных обменов и программ иностранной помощи, чтобы завоевать расположение целевого населения.

При осуществлении информационных операций используются такие методы, как пропаганда, ошибочная информация (например, интернет-тролли распространяют ошибочные теории заговора через социальные сети), дезинформация [1].

В современных условиях информационная война может сочетать кибероперации, разведку, электронную войну, информационные операции, психологические операции или военный обман как способ повлиять на информационную среду или изменить образ мышления противника [6].

Эффективность операций информационной войны часто зависит не столько от избранных способов и методов информационного воздействия на противника, сколько от широты и синхронности охвата этим воздействием массовых аудиторий, от каналов доведения управляющего информационно-психологического воздействия до сознания конкретных граждан. Возникает парадокс: с одной стороны, инициатор информационной войны под избранные им цели и конкретные задачи может разработать весьма тонкие и действенные технологии манипулирования инди-

видуальным и массовым сознанием; с другой стороны, применение этих технологий на практике может оказаться безрезультатным, если каналы доведения воздействия до избранных аудиторий будут выбраны неправильно или отсутствовать. В современных информационных войнах СМИ и социальные сети превратились в сетевые каналы доведения управляющего воздействия до массовых аудиторий, на которые оно рассчитано.

Таким образом, с развитием информационно-коммуникационных технологий экспоненциально расширились возможности государств по ведению боевых действий как в отношении информационных систем, так и в виртуальном пространстве. Зародившееся в оборонном секторе США понятие «информационная война» прошло ряд этапов в своей эволюции и все больше используется не только в военном, но и в общественно-политическом контексте.

В широком понимании информационная война рассматривается как форма политической борьбы и инструмент, с помощью которого государства достигают стратегических целей и продвигают свои внешнеполитические задачи. Информационная война может принимать различные формы в зависимости от объекта, на который направлено информационное воздействие (кибервойна, психологические операции и др.).

Инструментом проведения информационной войны являются информационные операции, которые, в свою очередь, содержат действия, направленные на достижение информационного превосходства или победы над противником посредством воздействия на информацию, информационные процессы и информационные системы противника, при обеспечении безопасности собственных аналогичных информационных ресурсов, систем и сетей. Информационную войну отличает от других форм деструктивного использования информационно-коммуникационных технологий тот факт, что она ведется в политических целях. В последние годы «театр военных действий» информационной войны во многом переместился в социальные сети, в которых ведут борьбу как военные, так и гражданские структуры правительства США.

Библиографические ссылки

1. Information Warfare: Issues for Congress [Electronic resource] // Congressional Research Service. March 5, 2018. URL: https://www.everycrsreport.com/files/20180305_R45142_c92c6be5763f84c05aee8a79ebe1727814d8da8d.pdf. Date of access: 19.01.2022.

2. Rona, T. P. Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA [Electronic resource]. July 1, 1976. URL: https://www.esd.whs.mil/Portals/54/ Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf. Date of access: 19.01.2022.

3. Бедрицкий, А. В. Реализация концепции информационной войны военно-

политическим руководством США на современном этапе // Автореф. дис. … канд. полит. наук : 23.00.04 / А. В. Бедрицкий. М., 2007. 28 с.

4. Libicki, M. What is information warfare? [Electronic resource] / M. Libicki // Defense Technical Information Center. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf. Date of access: 22.03.2021.

5. Joint Publication 3–13. Information Operations [Electronic resource] : 27 November 2012 Incorporating Change 1 20 November 2014. URL: https://www.jcs.mil/ Portals/36/Documents/Doctrine/pubs/jp3_13.pdf. Date of access: 19.01.2022.

6. Pomerleau, M. The new ways the military is fighting against information warfare tactics / M. Pomerleau [Electronic resource] // C4ISRNET. July 21, 2020. URL: https://www.c4isrnet.com/information-warfare/2020/07/20/the-new-ways-the-military-is-fighting-against-information-warfare-tactics/. Date of access: 19.01.2022.