УДК 339.986

КИБЕРОПЕРАЦИИ КАК ИНСТРУМЕНТ МЕЖГОСУДАРСТВЕННОЙ ВОЕННО-ЭКОНОМИЧЕСКОЙ КОНКУРЕНЦИИ

Рязанов Александр Анатольевич,
канд. экон. наук, доцент, доцент кафедры экономики городского хозяйства и сферы обслуживания,
e-mail: alekryazanov@yandex.ru,
Московский университет им. С.Ю. Витте, г. Москва

В статье представлено исследование, целью которого является уточнение сущностных признаков (предпосылок, субъектов, их целевых установок, сфер, объектов, средств) кибероперации как инструмента межгосударственной военно-экономической конкуренции. Актуальность темы исследования обусловлена как важной ролью кибероперaций в обострившейся в настоящее время межгосударственной военно-экономической конкуренции США и РФ, так и недостаточной разработанностью соответствующих теоретических положений, а также практической значимостью исследований, связанных с разработкой и обоснованием перспективных направлений снижения эффективности деструктивного воздействия кибероперaций на национальный хозяйственный комплекс РФ. Автором применялись такие методы исследования, как диалектический, системный, сравнительно-аналитический, а также методы научной абстракции, индукции и дедукции, нормативного и позитивного анализа и синтеза. Основными результатами исследования выступают авторские определения категорий «кибероперация», «кибератака», «кибероружие», «киберпространство», авторская классификация кибероперaций-инструментов межгосударственной военно-экономической конкуренции, а также перечень перспективных направлений снижения эффективности деструктивного воздействия кибероперaций на национальный хозяйственный комплекс РФ.

Ключевые слова: межгосударственное противоборство, межгосударственная военно-экономическая конкуренция, кибероперация, экономическая кибердиверсия, киберпространство, кибероружие, кибератака

CYBER OPERATIONS AS AN INSTRUMENT OF INTERSTATE MILITARY-ECONOMIC COMPETITION

Ryazanov A.A.,
candidate of economic sciences, associate professor, associate professor at the department of urban economy and service sector economics,
e-mail: alekryazanov@yandex.ru,
Moscow Witte University, Moscow

The purpose of the study is to clarify the essential features (prerequisites, subjects, their targets, spheres, objects, means) of cyber-operation as an instrument of interstate military-economic competition. The relevance of the research topic is due to both the important role of cyber operations in the currently aggravated interstate military-economic competition between the United States and the Russian Federation, and the lack of development of relevant theoretical provisions, as well as the practical significance of research related to the development and justification of promising directions for reducing the effectiveness of the destructive impact of cyber operations on the national economic complex of the Russian Federation. The author used such research methods as dialectical, systematic, comparative-analytical, as well as methods of scientific abstraction, induction and deduction, normative and positive analysis and synthesis.

Keywords: interstate confrontation, interstate military-economic competition, cyber-operation, economic cyber-diversion, cyber-space, cyber-weapons, cyber-attack

DOI 10.21777/2587-554X-2021-2-15-21

Введение

Продолжающееся формирование полицентричного мироустройства сопровождается обострением ряда межгосударственных противоречий. В то же время, применение для их разрешения военной силы в настоящее время ограничено не только международным правом, но и осознанием мировым сообществом угрозы глобальной катастрофы в случае использования одной из сторон конфликта оружия массового поражения. В этой связи отмечается существенная трансформация конфликтных форм разрешения геополитических противоречий, которая находит свое отражение в новых концепциях межгосударственного противоборства, относящихся к различным областям знаний: «гибридной войны» [11], «сетецентрической войны» [8; 9; 10], «мягкой силы» [12], «умной силы» [13], «цветной революции» [7], геоэкономики [1; 3; 5; 6].

Критическое осмысление ключевых положений данных концепций позволило автору выявить ряд принципиальных изменений современного межгосударственного противоборства:

– утрату государством монополии на власть и вооруженное насилие;

– трансформацию целей с завоевания противоборствующего государства в лишение его суверенитета и взятие под контроль его ресурсов;

– многомерность;

– осуществление не только в традиционных средах, но и в космосе, киберпространстве, когнитивной, экономической, внешне- и внутриполитической, технологической, социокультурной и других сферах;

– переход от подчиненного положения невоенных средств по отношению к вооруженной борьбе к их относительной самостоятельности;

– смену ведущего критерия войны с приоритетных средств её ведения на целевые установки и достигнутые результаты;

– использование средств агрессии на уровне ниже порога очевидного обнаружения и ответных действий.

Ведущей современной конфликтной формой разрешения геополитических противоречий, по мнению автора, стала межгосударственная военно-экономическая конкуренция, которую он считает возможным определить как многоуровневое, многомерное, комплексное латентное противоборство субъектов международных отношений за их фактический экономический суверенитет и контроль над национальным хозяйственным комплексом и экономическими ресурсами, ведущееся в одной или нескольких сферах жизнедеятельности общества без использования военной силы. Ограничение на применение последней стимулирует развитие невоенных инструментов межгосударственной военно-экономической конкуренции (таблица 1).

Одним из наиболее разрушительных инструментов межгосударственной военно-экономической конкуренции являются кибероперации. Возрастающие масштабы и все более комплексный характер их проведения, значительный ущерб, наносимый экономическому и военно-экономическому потенциалу государств, превратили кибероперации в серьезную угрозу национальной и международной безопасности. Так, по данным Национального координационного центра по компьютерным инцидентам, в 2017 году на критическую информационную инфраструктуру РФ было совершено 4 млрд кибератак, в том числе 12 тыс. скоординированных, т.е. имеющих признаки кибероопераций. В 2018 году данные показатели возросли до 4,3 млрд и 17 тыс. соответственно [4].

Между тем, данный феномен изучен современной наукой недостаточно, чем и обусловлена актуальность темы данной статьи.

Таблица 1 – Основные невоенные инструменты межгосударственной военно-экономической конкуренции

Инструменты экономической агрессии	Инструменты противодействия экономической агрессии
Агенты влияния экономического агрессора	Контрразведывательные операции спецслужб государства-мишени экономической агрессии
Деструктивный экономический консалтинг органов государственной власти страны-объекта экономической агрессии	

Разведывательные операции спецслужб экономического агрессора	
Промышленный шпионаж со стороны экономического агрессора	
Экономические диверсии	
Кибероперации экономического агрессора	Национальная система кибербезопасности страны-объекта экономической агрессии
Информационно-психологические операции	Государственная система пропаганды страны-жертвы экономической агрессии
Средства массовой информации	Система государственного регулирования деятельности средств массовой информации на территории страны-мишени экономической агрессии
Международные экономические санкции в отношении страны-мишени экономической агрессии	Диверсификация внешнеэкономических связей страны-объекта экономической агрессии, импортозамещение, контрсанкции в отношении экономического агрессора
Кредиты международных организаций	Финансовая система государства-жертвы экономической агрессии
Курсы национальных валют	
Финансовые операции с долговыми ценными бумагами государства-жертвы экономической агрессии	
Манипулирование рейтингами международных кредитных организаций	
Финансовые махинации	
Манипулирование трансфертом технологий в страну-объект экономической агрессии	Национальная инновационная система страны-жертвы экономической агрессии
Манипулирование гуманитарной помощью населению страны-мишени экономической агрессии	Система социальной защиты населения, мобилизационные резервы государства-жертвы экономической агрессии
Манипулирование импортными, экспортными таможенными пошлинами и квотами, лицензионными и таможенными процедурами	
Международные и национальные стандарты и технические условия	
Стимулирование оппозиции, протестного движения в стране-объекте экономической агрессии	Системная оппозиция, система взаимодействия органов государственной власти страны-мишени экономической агрессии с институтами гражданского общества, выявление и перекрытие каналов ресурсного обеспечения экономическим агрессором оппозиции, протестного движения в стране-объекте экономической агрессии

Сущностные признаки кибероперации как инструмента межгосударственной военно-экономической конкуренции

Как представляется автору, для уточнения сущности и содержания кибероперации, проводимых в рамках межгосударственной военно-экономической конкуренции, следует определить предпосылки их проведения, субъекты, решаемые данными субъектами задачи, объекты и средства проведения.

Основными предпосылками использования в ходе межгосударственной военно-экономической конкуренции кибероперации автор считает:

– ускоренное развитие информационно-коммуникационных технологий;

– последовательную комплексную цифровизацию системы государственного управления и национальной экономики;

– соответствующую реорганизацию хозяйствующих субъектов;

– возрастающую зависимость эффективности их функционирования от интернет-коммуникаций;

– низкие барьеры входа в корпоративные компьютерные системы и сети;

– широкое распространение в мире кибероружия;

– возможность анонимной деятельности в киберпространстве.

Разделяя точку зрения основоположников современных концепций межгосударственного противоборства, признающих факт утраты государством монополии на власть и вооруженное насилие, и считающих полноценными сторонами современных международных конфликтов негосударственные структуры и сообщества, в том числе сетевые, ярким примером которых является международный терроризм, автор относит к субъектам кибероперации, проводимых в ходе межгосударственной военно-экономической конкуренции:

– разведывательные службы государств, противоборствующих в форме межгосударственной военно-экономической конкуренции;

– разведывательные подразделения негосударственных внутристрановых и международных структур и сообществ, являющихся субъектами геополитического противоборства;

– кибервойска государств, выступающих противоборствующими сторонами межгосударственной военно-экономической конкуренции и обладающих кибероружием;

– киберподразделения негосударственных внутристрановых и международных структур и сообществ, являющихся субъектами геополитического противоборства;

– привлекаемые данными службами, войсками и подразделениями хакерские группы.

Необходимо подчеркнуть, что в ходе проведения активной фазы кибероперации их субъекты маскируются под анонимных хакеров и хакерские группы.

Отметим, что кибероперации одновременно охватывают две сферы:

– киберпространство, под которым в данной статье будет пониматься информационная среда функционирования продуктов современных информационно-коммуникационных технологий, в т.ч. интернета;

– физическое пространство, где размещены компьютерные системы и базы данных, выступающие материально-технической основой и объектом кибероперации.

Объектами кибероперации, проводимых в ходе межгосударственной военно-экономической конкуренции, выступают компьютерные системы и базы данных органов государственной власти и государственных учреждений, являющихся элементами системы управления национального хозяйственного комплекса, пунктов управления социально-экономической инфраструктурой крупных городов, предприятий важнейших отраслей экономики, в том числе оборонных, а также интернет-пользователи. Так, по данным Национального координационного центра по компьютерным инцидентам, объектами 38 % кибератак на критическую информационную инфраструктуру РФ являются кредитно-финансовые учреждения, 35 % – органы государственной власти, 7 % – предприятия и организации оборонной промышленности, 7 % – учреждения науки и образования, 3 % – учреждения здравоохранения [2].

Классификация кибероперации, проводимых в ходе межгосударственной военно-экономической конкуренции

Целевые установки исследуемых кибероперации, по мнению автора, сводятся к дестабилизации функционирования системы управления и снижению возможностей национального хозяйственного комплекса противоборствующей стороны. Данная цель достигается решением следующих задач:

– выводом из строя (дестабилизацией функционирования) компьютерных систем и управляемых данными системами технических устройств;

– прекращением (дестабилизацией) доступа компьютерных систем в интернет;

– получением несанкционированного доступа к компьютерным базам данных;

– манипулированием общественным мнением и поведением интернет-пользователей.

Сформулированный автором перечень задач, решаемых во время кибероперации, проводимых в ходе межгосударственной военно-экономической конкуренции, позволил ему разработать классификацию данных кибероперации, разделив их на экономические разведывательные кибероперации, киберпропагандистские операции в экономической сфере, экономические кибердиверсии и комплексные экономические кибероперации (таблица 2).

Таблица 2 – Основные виды кибероперации, являющихся инструментами межгосударственной военно-экономической конкуренции

Вид кибероперации	Решаемые задачи	Примеры
Экономическая разведывательная кибероперация	Получение несанкционированного разработчиками доступа к компьютерным базам данных	Похищение в 2006–2018 гг. хакерской группой apt10, связанной с Министерством госбезопасности КНР, информации из компьютерных систем 45 технологических компаний США
Киберпропагандистская операция в экономической сфере	Манипулирование общественным мнением и поведением	Освещение в интернете факта присоединения Крыма к РФ в 2014 г.

	интернет-пользователей посредством автоматической генерации соответствующего информационного трафика, в т.ч. ложных новостных материалов	
Экономическая кибердиверсия	Вывод из строя (дестабилизация функционирования) компьютерных систем и управляемых данными системами технических устройств, прекращение (дестабилизация) доступа компьютерных систем в интернет	Вывод из строя 1368 центрифуг на заводе по обогащению урана в г. Натанзе (Иран) с помощью вредоносного программного обеспечения, скрытно интегрированного спецслужбами США и Израиля в оборудование, поставленное заводу немецкой компанией Siemens AG, в целях задержки реализации иранской ядерной программы
Комплексная экономическая кибероперация	Различные сочетания задач экономической разведывательной кибероперации, киберпропагандистской операции и экономической кибердиверсии	Блокировка интернет-инфраструктуры Эстонии колоссальными потоками данных, распространение в интернете и компьютерных системах призывов отметить День Победы и подложных писем премьер-министра, деструктивное воздействие на интернет-сайты государственных учреждений неустановленной группой хакеров в ходе «первой в мире кибервойны» в 2007 г.

Основным же средством проведения кибероперaций является кибероружие, которое автор определяет как совокупность вредоносного программного обеспечения, предназначенного для получения несанкционированного доступа к вычислительным ресурсам, информации и базам данных, хранимых в компьютерных системах, их несанкционированного использования или выведения из строя (повреждения, затруднения функционирования), программного обеспечения, предназначенного для автоматической генерации определенного информационного трафика, а также вспомогательных технических средств.

Основным же элементом исследуемых кибероперaций автору представляется кибератака – целенаправленное спланированное вмешательство маскирующихся под анонимные хакерские группы разведывательных служб и кибервойск государств или разведывательных и киберподразделений негосударственных внутристрановых и международных структур и сообществ, являющихся субъектами геополитического противоборства, в информационную систему противоборствующей стороны или вредоносное воздействие данных служб, войск, подразделений и групп на программное обеспечение, вычислительные ресурсы, базы данных, компьютерные системы противоборствующей стороны.

Исследование сущностных признаков кибероперaции, являющейся важнейшим инструментом межгосударственной военно-экономической конкуренции, позволило автору определить её как совокупность направленных на дестабилизацию функционирования системы управления и снижение возможностей национального хозяйственного комплекса противоборствующей стороны согласованных и взаимосвязанных кибератак маскирующихся под анонимные хакерские группы разведывательных служб и кибервойск государств или разведывательных и киберподразделений негосударственных внутристрановых и международных структур и сообществ, являющихся субъектами геополитического противоборства, а также обеспечивающих данные кибератаки действий в киберпространстве.

Как представляется автору, данное определение достаточно полно раскрывает сущность и содержание кибероперaции как инструмента межгосударственной военно-экономической конкуренции, позволяет исследовать данный феномен более глубоко, системно и комплексно, в чем и состоит теоретическая значимость полученных автором научных результатов.

Заключение

В условиях эскалации межгосударственной военно-экономической конкуренции США и РФ важное практическое значение имеет задача выявления и обоснования перспективных направлений снижения эффективности деструктивного воздействия кибероперaций, направленных на дестабилизацию функционирования системы управления и снижение возможностей национального хозяйственного комплекса нашей страны. В результате исследования в качестве данных направлений автором были выделены:

− совершенствование Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак;

− повышение безопасности функционирования объектов информационной инфраструктуры, защищенности критической информационной инфраструктуры и устойчивости ее функционирования;

− развитие методов и средств обнаружения и предупреждения информационных угроз, а также ликвидации последствий их проявления на основе отечественных информационных технологий и электронной компонентной базы;

− обеспечение защиты информации, содержащей сведения, составляющие государственную тайну;

− развитие национальной системы управления российским сегментом интернета;

− своевременное пресечение деятельности, наносящей ущерб национальной безопасности РФ, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств;

− развитие законодательной базы информационной безопасности РФ.

Как представляется автору, реализация данного комплекса мероприятий позволит существенно повысить информационную безопасность национального хозяйственного комплекса РФ.

Список литературы

1. *Блэквилл Р., Харрис Дж.М.* Война иными средствами. Геоэкономика и государственное регулирование. – М.: АСТ, 2017. – 480 с.
2. *Егоров И.* Число опасных кибератак на объекты в РФ выросло в 11 раз за три года [Электронный ресурс] // Новости ВПК. – URL: https://www.vpk.name/news/313461_chislo_opasnyh_kiberatak_na_obekty_v_rf_vyroslo_v_11_raz_za_tri_goda.html (дата обращения: 25.02.2021).
3. *Жан К., Савона П.* Геоэкономика: господство экономического пространства. – М.: Ad Marginem, 1997. – 207 с.
4. *Захарова Л.* За год на Россию было совершено более четырех миллиардов кибератак [Электронный ресурс] // Российская газета. – URL: https://www.rg.ru/2018/12/12/za-god-na-rossiiu-bylo-sovershenobolee-chetyreh-milliar dov-kiberatak.html (дата обращения: 25.02.2021).
5. *Лютвак Э.Н.* Государственный переворот. Практическое пособие. – М.: Университет Дмитрия Пожарского, 2012. – 326 с.
6. *Моро-Дефарж Ф.* Введение в геополитику. – М.: Конкорд, 1996. – 151 с.
7. *Шарп Д.* От диктатуры к демократии: стратегия и тактика освобождения. – М.: Новое издательство, 2005. – 84 с.
8. *Arquilla J., Ronfeldt D.F.* Networks and netwars: the future of terror, crime and militancy. – Santa Monica: RAND Corporation, 2001. – 217 p.
9. *Cebrowski A.K., Garstka J.J.* Network-Centric Warfare: Its Origins and Future // U.S. Naval Institute Proceedings. Annapolis, Maryland. – January 1998. – Vol. 124, No. 1. – P. 28–35.
10. *Forgues P.* Command in a network-centric warfare // Canadian Military Journal. – 2001. – Vol. 2, No. 2. – P. 23–30.
11. *Mattis J.N., Hoffman F.G.* Future Warfare: The Rise of Hybrid Wars // US Naval Institute Proceedings Magazine. – November 2005. – Vol. 132. – P. 18, 19.
12. *Nye J.* S. Bound to Lead: The Changing Nature of American Power. – New York: Basic Books, 1990. – 261 p.
13. *Nye J.* Soft Power: The Means to Success in World Politics. – New York: Public Affairs Group, 2004. – 192 p.

References

1. *Blekvill R., Harris Dzh.M.* Vojna inymi sredstvami. Geoekonomika i gosudarstvennoe regulirovanie. – M.: AST, 2017. – 480 s.
2. *Egorov I.* Chislo opasnyh kiberatak na ob”ekty v RF vyroslo v 11 raz za tri goda [Elektronnyj resurs] // Novosti VPK. – URL: https://www.vpk.name/news/313461_chislo_opasnyh_kiberatak_na_obekty_v_rf_vyroslo_v_11_raz_za_tri_goda.html (data obrashcheniya: 25.02.2021).
3. *Zhan K., Savona P.* Geoekonomika: gospodstvo ekonomicheskogo prostranstva. – M.: Ad Marginem, 1997. – 207 s.

4. *Zaharova L.* Za god na Rossiyu bylo soversheno bolee chetyrekh milliardov kiberatak [Elektronnyj resurs] // Rossijskaya gazeta. – URL: https://www.rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliar dov-kiberatak.html (data obrashcheniya: 25.02.2021).
5. *Lyutvak E.N.* Gosudarstvennyj perevorot. Prakticheskoe posobie. – M.: Universitet Dmitriya Pozharskogo, 2012. – 326 s.
6. *Moro-Defarzh F.* Vvedenie v geopolitiku. – M.: Konkord, 1996. – 151 s.
7. *Sharp D.* Ot diktatury k demokratii: strategiya i taktika osvobozhdeniya. – M.: Novoe izdatel'stvo, 2005. – 84 s.
8. *Arquilla J., Ronfeldt D.F.* Networks and netwars: the future of terror, crime and militancy. – Santa Monica: RAND Corporation, 2001. – 217 p.
9. *Cebrowski A.K., Garstka J.J.* Network-Centric Warfare: Its Origins and Future // U.S. Naval Institute Proceedings. Annapolis, Maryland. – January 1998. – Vol. 124, No. 1. – P. 28–35.
10. *Forgues P.* Command in a network-centric warfare // Canadian Military Journal. – 2001. – Vol. 2, No. 2. – P. 23–30.
11. *Mattis J.N., Hoffman F.G.* Future Warfare: The Rise of Hybrid Wars // US Naval Institute Proceedings Magazine. – November 2005. – Vol. 132. – P. 18, 19.
12. *Nye J.* S. Bound to Lead: The Changing Nature of American Power. – New York: Basic Books, 1990. – 261 p.
13. *Nye J.* Soft Power: The Means to Success in World Politics. – New York: Public Affairs Group, 2004. – 192 p.