УДК 32

ИНФОРМАЦИОННЫЕ ВОЙНЫ – СМЫСЛ И ИТОГИ ПРОТИВОСТОЯНИЯ

Бабанов Андрей Борисович кандидат экономических наук, доцент кафедры международных экономических отношений, Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ (344002, Россия, г. Ростов-на-Дону, ул. Пушкинская, 70/54). E-mail: skags2@yandex.ru

Аннотация

В статье анализируется проблема информационной безопасности, рассматриваются возможности применения информационных технологий для нейтрализации противника, подрывающего основы национальной безопасности. Дается краткий анализ приоритетов и направлений применения информационных технологий через сетевое воздействие.

Ключевые слова: *информационное оружие, информационная безопасность, сетевые войны, экономическое развитие, политическая элита, инновации, технологические уклады.*

События последнего времени свидетельствуют об информационных сражениях, в которых противоборствующие стороны используют любые средства для достижения победы. Эта борьба распространяется на все уровни – персональный, региональный, национальный (государственный и предпринимательский сектора) и глобальный.

При этом нетрудно классифицировать субъекты, возможности которых предполагают воздействие на каждый из перечисленных локаций. К ним мы в первую очередь относим США, Китай, Россию, Великобританию, ЕС и Японию. Предложенная последовательность коррелируется со спектром возможностей (финансовых, военных, кадровых, технологических, институциональных и др.).

Анализ спектров возможностей этих стран проведем на основе открытых данных глобальной информационной сети Интернет, аналитических статей, экспертных оценок. В таблице приведены данные о некоторых показателях экономического и инновационного развития и военных расходах.

Таблица

*Сравнительная характеристика инновационного развития стран**

	Патенты (2012 г.)	**Инновационный индекс (2014 г.)**	**Ср-ва на НИОКР (в % от ВВП) 2012 г.**	**ВВП (млрд долл)**	**Расходы бюджета на оборону (2014 г.)**	**Кол-во военнослужащих**
США	503582	60.1 (6 место в рейтинге)	2.9	16720	610	1369532
Китай	526412	46.6 (29)	1.7	8939	216	2250000
Россия	41414	39.1 (49)	1.16	1830.1	84.5	1027000
Великобритания	22259	62.4 (2)	1.7	2490	60.5	421830
Япония	342610	52.4 (21)	3.3	5007	45.8	247746

** По данным консалтинговой компании IHS Global. Российский военный бюджет рассчитан на основе официальной статьи в федеральном бюджете «Национальная оборона». Наибольший рост в % военного бюджета показал Китай (175%) за период с 2003 по 2012 гг.*

Приведенные данные – всего лишь видимая сторона «айсберга» расходов, напрямую или косвенно связанных с обеспечением «национальной безопасности» и затрагивающих стабильное функционирование критически важной гражданской и военной инфраструктуры, отраслей народного хозяйства, оружия наступательного и оборонительного характера. Информационная война, естественно,

предполагает нанесение невосполнимого ущерба, установление контроля над разумом (когнитивная сфера), над информационными системами и ресурсами, а также недопущение и/или нейтрализацию возможных контратак, внесения хаоса, непонимания происходящего.

Анализ современных событий обнаруживает активное обсуждение экспертным сообществом текущих тенденций, попытки разобраться, найти первопричины, обозначить «закулисье» и спрогнозировать сценарии предполагаемых событий на ближайшую перспективу.

Являясь структурным элементом национальной безопасности, информационная безопасность будет оказывать нарастающее влияние с развитием научно-технического прогресса (НТП) и переходом ряда государств к передовым (шестому-седьмому) технологическим укладам (ТУ).

Информационный вид международных отношений характеризуется наличием многосубъектности и действий, при которых мотивы могут быть «неясными», а поступки выходить за рамки «дружественных» или «нейтральных», т.е. отсутствием официального объявления «войны». Степень уязвимости и угроз определяется политической проблемой и должна определяться актором самостоятельно, исходя из проблематики суверенитета и безопасности.

В настоящее время проблема информационной безопасности находит отражение в работах ученых и практиков различных направлений: экономистов, политологов, юристов, программистов и т. д. Проблемам информационной безопасности посвящены работы российских ученых – В.Н. Лопатина, Ю.С. Уфимцева, Е.А. Ерофеева, Б.В. Вербенко, А.А. Николаевой, Э.М. Брандмана, ряда зарубежных теоретиков – Д. Белла, Э. Тоффлера, У. Оуэнса, Т. Стоуньера, А. Турена, У. Дайзарда, М. Кастельса, К. Кояма, Е. Масуда. Эти вопросы широко обсуждаются политическими деятелями самого высокого ранга.

До недавнего времени информационные угрозы в политическом отношении представлялись как нечто абстрактное, иллюзорное, не носящее материальной природы. Отсутствие единого методологического и научного подхода в данной сфере сопрягается с пониманием (непониманием) применимости технологий и инструментов воздействия. В то же время глобальные угрозы могут не восприниматься частью человечества в силу неверия в их реализацию или в силу веры эффективности национальных сил безопасности.

На наш взгляд, данные виды угроз следует рассматривать в контексте суммы интегральных возможностей, присущих субъекту, их высказавшему и/или отдавшему приказ на проведение скрытых операций. Такой возможностью чаще всего обладает политическая элита, персонифицирующая свою власть через органы исполнительной власти и государственный аппарат, где методы и характер подобного воздействия определяются самой властью. В то же время необходимость такого воздействия не ставится под сомнение экспертным и научным сообществом.

Государственное воздействие на сферу информационной безопасности должно быть разделяемо обществом и социумом, когда государственные органы отчетливо понимают сигналы и запросы, политические предпочтения, существующие ценности и традиции многоконфессионального государства. В настоящее время происходит поиск ценностных ориентиров, объединяющих большинство граждан и политическую элиту в целях оптимизации осуществления властных полномочий.

С другой стороны, наблюдается «разрушение ценностей системы, отсутствие критериев адекватной оценки информационных воздействий, появление целого арсенала новых средств воздействия на индивидуальное, групповое и массовое сознание, в том числе, новых технологий и форм подачи информации СМИ» [1, с. 57].

Здесь следует сказать, что информационная безопасность в какой-то мере зависит от того, насколько качественно средствами массовой информации осуществлены прогноз и констатация фактов и эффективно используются интернет-технологии. Результаты подтверждают, что на безопасность личности, в т.ч. и информационную, оказывают влияние политические, социально-экономические и духовные факторы [2–4].

В целом политологическую точку зрению можно представить как государственную информационную политику по достижению запланированных результатов при использовании существующего набора механизмов, включающих в себя формы взаимовыгодного сотрудничества частного сектора, гражданского общества и институтов государственной власти.

Приоритеты информационной политики безопасности должны, на наш взгляд, рассматриваться с позиции обеспечения комплексной государственной безопасности и опосредованно – как «коммуникация между людьми, с осознанием наличия у людей и их сообществ интересов, которым может быть нанесен ущерб» [5]. Приоритеты государственной информационной безопасности – явление сложное, требующее комплекса действий и мероприятий по реализации своих интересов по противодействию внутренним и внешним угрозам в рамках выполнения стратегии национальной безопасности.

В США, например, раньше других распознали возможность применения достижений глобальной информационной революции для приобретения (создания) инструментов военно-политического и социально-экономического воздействия на потенциального противника. Полем боевых действий становится информационное пространство, где участвуют различные единицы боевой техники, инструменты дипломатического искусства, журналистики, связи, психологии, социологии, культуры, экономических достижений, пропаганды и т.д. Процессы глобализации и урбанизации, всеохватывающее проникновение информации и передовых технологий выводит в лидеры культурного и идеологического воздействия США, где подобная ситуация выступает не как «результат политического замысла, а продукт высококонкурентной американской системы, что придает США политический вес глобального масштаба» [6].

В статье «Появление системы систем США» (1996 г.) адмирал Уильям Оуэнс отмечал, что слияние способности собирать информацию в реальном времени со способностью обрабатывать и понимать эти данные создает превосходство на поле боя. Чуть позже (1998 г.) Артур Себровски и Джон Гарстка в статье «Сетецентричная война: ее происхождение и будущее» отметили, что информация в период перехода к информационной фазе развития будет являться самым эффективным оружием. А так как человек все больше времени проводит в виртуальной сети, то и военные действия будут являться сетецентричными. Регулярная армия, все виды разведок, технические открытия и высокие технологии, журналистика и дипломатия, экономические процессы и социальные трансформации, гражданское население и кадровые военные, регулярные части и отдельные слабо оформленные группы – все это интегрируется в единую сеть, по которой циркулирует информация.

Создание такой сети составляет сущность военной реформы ВС США. Центральной задачей ведения всех «сетевых войн» является проведение «операции базовых эффектов» (Effects-based operations – EBO, далее ОБЭ). Это важнейшая концепция во всей данной теории. ОБЭ определяются как «совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны». (Цит. по Edward A.Smith, Jr. Effects-based Operations. Applying Network-centric Warfare in Peace, Crisis and War, Washington, DC:DoD CCRP, 2002). Цель сетевых войн – ОБЭ, а цель ОБЭ – абсолютный контроль надо всеми участниками исторического процесса в мировом масштабе [7].

Анализируя перспективы вероятных военных конфликтов, военные армии США ввели понятие «стратегический паралич» [8], определяемое как поражение жизненно важных точек государственной системы. Такие точки могут находиться как внутри государства, так и по внешнему периметру обороны и затрагивать действия международных организаций. Признавая факт, что рациональные политические мотивы лидеров ряда стран будут снижаться, боевые столкновения в ближайшей перспективе будут продолжаться на основе идеологических и религиозных убеждений, что возможно приведет к началу военного конфликта с участием множества стран.

Сетевая война предусматривает лишение противника суверенитета, даже частичного, перспективы действий, организацию «пятой колонны», манипуляций мотиваций и действиями. Сетевая война ведется постоянно, без перерыва, изматывая противника, не давая сосредоточить свои ресурсы на определенных направлениях. Принцип сетевых войн в постмодерне решает задачу исключения боевого соприкосновения с противником и достижения поставленных задач при повсеместном внушении мысли о бессмысленности конкуренции с США в любой сфере, в том числе и военной. Уже сейчас официальные представители Белого дома подчеркивают, что Президент США руководствуется интересами защиты американских граждан, независимо от международных границ [9].

Ряд авторов делает и более радикальные выводы, указывая на недосягаемость вооруженных сил США, опередивших другие страны на десятилетия в практике внедрения сетецентрических способов ведения боевых действий [10].

В военно-практическом смысле, «сетецентрическая война» позволяет перейти от войны на истощение к более скоротечной и более эффективной форме, для которой характерны две основных характеристики: быстрота управления и принцип самосинхронизации [11].

Так, необъявленная война идет в глобальном информационном пространстве по поводу интерпретаций международных событий, в том числе и украинских. Цифровая дипломатия используют весь доступный инструментарий виртуальных средств доставки контента (Twitter, Facebook, YouTube, LiveJournal) воздействия на аудиторию. Причем, в данном контексте важным становится не само событие, а интерпретации и логические конструкции экспертов, которые вкладываются в сознание массового потребителя. При этом ряд экспертов называет информационную политику США по отношению к России «непрофессиональной» [12], где СМИ учитывают рекомендации Белого Дома в своих публикациях[1]. В российской печати все чаще появляется новый термин, характеризующий противоборства сторон – гибридный, а российскую информационную компанию по освещению украинских событий считают одной из самых успешных.

Что касается информационного поля Российской Федерации, следует отметить успешность работы по противодействию информационному влиянию зарубежных СМИ.

Установление контроля над информационным полем противника равносильно «порабощению», захвату данной территории одним государством для установления тотального контроля над действиями и мыслями врагов и друзей. Такая стратегия позволяет выиграть сражение еще до начала военной операции. Концепция сетевой войны напрямую связана с экономическими изменениями и новыми ТУ, использованием современных достижений НТП.

Итоговые выводы – авторы американской военной доктрины[2] призывают максимально точно изучить противника и свой потенциал, что даст возможность использовать политическую, культурную, идеологическую и религиозную мотивацию действий противника в свою пользу. Понимание этого предполагает совершенно иной механизм подготовки политической элиты, обладающей широчайшим спектром знаний во всех областях, а также знаний о наличии вооружений, их возможностей и последствий. Анализируя политический аспект информационной безопасности, следует обратить внимание на качество политического процесса и национальную ориентированность элит, умение эффективно и оперативно принимать решения, а «перенос интересов государства на интересы человека, делает актуальным разработку проблем информационной безопасности личности в контексте влияния информатизации на политические отношения и политический процесс» [13–14].

Движение европейского, американского и российского законодательства характеризуется общими элементами, инфраструктурой, но предполагает самостоятельное понимание внутренних причин процессов и механизмов достижения определенных целей.

Соответственно, коренным образом меняется и военно-политическая модель действий и противодействий вероятному противнику, где основная роль отводится информационному превосходству. В то же время военная сила сохраняет свою ключевую роль при решении локальных конфликтов, когда активно использует передовые системы вооружений (например, боевые компьютерные вирусы).

Можно уверенно говорить о наступившем периоде институализации недоверия между странами в области информационной политики. Происходящая на наших глазах глобальная информационная революция и переход к новому технологическому укладу формируют новые требования к качеству государственной и политико-экономической элиты вследствие создания угроз национальной безопасности Российской Федерации непосредственно на границах.

---

[1] См. более подробно URL: http://www.huffingtonpost.com/2014/02/12/us-press-freedom-index-2014_n_4773101.html США опустилась на 14 мест вниз в рейтинге свободы прессы, заняв 32 место, и URL: http://en.rsf.org/press-freedom-index-2013,1054.html – рейтинг свободы прессы 2013.

[2] «Среда для действий Объединенных сил» (The Joint Operating Environment – JOE) Командование объединенных сил США (USJFCOM).

Построение эффективной российской системы противодействия сетевым войнам возможно только в рамках перехода к информационному обществу, а не в условиях сохранения позиций индустриального общества и сырьевой специализации в рамках глобальных проектов. Сетевые атаки зачастую остаются невидимыми, они воздействуют на когнитивную составляющую каждого гражданина и всего общества, не имеют видимых препятствий. Задача заключается в создании региональной информационной сети, например, в рамках евразийского проекта и имеющихся возможностей[1].

Литература

1. *Лызь А.Е., Лызь Н.А.* К вопросу о составляющих информационной безопасности личности // Информационное противодействие угрозам терроризма. 2008. № 12. С. 53-57.
2. *Кара-Мурза С.Г.* Манипуляция сознанием. М., 2006.
3. *Грачев Г.В., Мельник И.К.* Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М., 1999. 235 с.
4. *Грачев Г.В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. М., 1998. 125 с.
5. *Лопатин В.Н.* Информационная безопасность России: человек, общество, государство. Серия: Безопасность человека и общества. СПб.: Фонд Университет, 2000. 428 с.
6. *Бзежинский Зб.* Выбор. Мировое господство или глобальное лидерство/ пер. с англ. М.: Международные отношения, 2010. 190 с.
7. URL: http://communitarian.ru/publikacii/setevye_voyny_i_tekhnologii/ setetsentrichnye_ oyny_novaya_setevaya _teoriya_voyny/
8. URL: http://www.communitarian.ru/publikacii/setevye_voyny_i_tekhnologii/ beskontaktnyei_setevye_voyny_1604201 3/, в России наибольшее количество публикаций по сетевым войнам приходится на Дугина.
9. URL: http://www.kommersant.ru/doc/2553934
10. URL: http://vrpb.net/setecentricheskaya-vojna-gotova-li-k-nej-rossiya/# more-2851 «Сетецентрическая война»: Готова ли к ней Россия?
11. URL: http://vrpb.net/setecentricheskaya-vojna-gotova-li-k-nej-rossiya/ #more-2851 очень хорошая статья и http://www.milresource.ru/Kop-NCW.html
12. URL: http://www.paulcraigroberts.org/2014/02/14/russia-attack-paul-craig-roberts/ (Институт политической экономики) Россия под атакой – Пол Крейг Робертс.
13. *Панарин И.Н.* Технология информационной войны. М., 2003. 320 с.
14. *Панарин И.Н.* Информационная и психологическая безопасность в СМИ. М., 2002.

Babanov Andrey Borisovich, candidate of economic Sciences, associate Professor, Department of international economic relations; South-Russia Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration (70/54, Pushkinskaya St., Rostov-on-Don, 344002, Russian Federation).
E-mail: skags2@yandex.ru

INFORMATION WARFARE – THE MEANING AND OUTCOME OF THE CONFRONTATION

Abstract

The article examines information security, the application of information technology to neutralize the enemy and undermining the foundations of national security. A brief analysis of the priorities and areas of application of information technologies through network effects.

Keywords: *information weapons, information security, network war, economic development, the political elite, innovation, technological structures.*

References

1. Lyz' A.E., Lyz' N.A. K voprosu o sostavljajushhih informacionnoj bezopasnosti lichnosti // Informacionnoe protivodejstvie ugrozam terrorizma. 2008. № 12. S. 53-57.
2. Kara-Murza S.G. Manipuljacija soznaniem. M., 2006.

[1] Например, советскими учеными был разработано и описано «организационное оружие».

3. Grachev G.V., Mel'nik I.K. Manipulirovanie lichnost'ju: organizacija, sposoby i tehnologii informacionno-psihologicheskogo vozdejstvija. M., 1999. 235 s.
4. Grachev G.V. Informacionno-psihologicheskaja bezopasnost' lichnosti: sostojanie i vozmozhnosti psihologicheskoj zashhity. M., 1998. 125 s.
5. Lopatin V.N. Informacionnaja bezopasnost' Rossii: chelovek, obshhestvo, gosudarstvo. Serija: Bezopasnost' cheloveka i obshhestva. SPb.: Fond Universitet, 2000. 428 s.
6. Bzezhinskij Zb. Vybor. Mirovoe gospodstvo ili global'noe liderstvo/ per. s angl. M.: Mezhdunarodnye otnoshenija, 2010. 190 s.
7. URL: http://communitarian.ru/publikacii/setevye_voyny_i_tekhnologii/ setetsentrichnye_ oyny_novaya_setevaya _teoriya_voyny/
8. URL: http://www.communitarian.ru/publikacii/setevye_voyny_i_tekhnologii/ beskontaktnyei_setevye_voyny_1604201 3/, v Rossii naibol'shee kolichestvo publikacij po setevym vojnam prihoditsja na Dugina.
9. URL: http://www.kommersant.ru/doc/2553934
10. URL: http://vrpb.net/setecentricheskaya-vojna-gotova-li-k-nej-rossiya/# more-2851 «Setecentricheskaja vojna»: Gotova li k nej Rossija?
11. URL: http://vrpb.net/setecentricheskaya-vojna-gotova-li-k-nej-rossiya/ #more-2851 ochen' horoshaja stat'ja i http://www.milresource.ru/Kop-NCW.html
12. URL: http://www.paulcraigroberts.org/2014/02/14/russia-attack-paul-craig-roberts/ (Institut politi-cheskoj jekonomiki) Rossija pod atakoj – Pol Krejg Roberts.
13. Panarin I.N. Tehnologija informacionnoj vojny. M., 2003. 320 s.
14. Panarin I.N. Informacionnaja i psihologicheskaja bezopasnost' v SMI. M., 2002.

УДК 32

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В ПЕРИОД ТРАНСФОРМАЦИИ РОССИЙСКОГО ОБЩЕСТВА

Волкова Евгения Александровна кандидат педагогических наук, доцент, Южный институт менеджмента (350040, Россия, г. Краснодар, ул. Ставропольская, 216). E-mail: pjankovaea@rambler.ru

Аннотация

Автором предлагается рассмотрение вопросов информационно-психологической безопасности как одной из проблем национального безопасности.

Ключевые слова: *безопасность, информационно-психологическая деятельность, трансформация общества, национальная безопасность.*

В России на рубеже XX–XXI вв. вопрос информационно-психологической безопасности связан с качественными преобразованиями основных институтов – политических, экономических, социокультурных, всей информационной среды. Системные трансформации отразились на ценностных ориентациях всего населения России, одной из самых общепринятых причин изменения считается переход мирового сообщества к электронным средствам передачи информации в процессе создания информационной цивилизации. Теперь в распоряжение людей входит не только телевидение и бумажные носители, на первом месте стоит передача информации через интернет. Так, М. Кастельс говорит о том, что не информационные и телекоммуникационные технологии явились инструментом системной трансформации, но социокультурный кризис, перестройка социально-экономических систем [3, с. 17]. Так же М. Кастельс утверждает, что происходит синергия между всеми средствами информационных коммуникаций и в результате мы получаем абсолютно новую информационную культуру [3, с. 37]. По этому вопросу Т.И. Заславская утверждает, что именно трансформационная активность охватывает все социально-значимые действия, оказывает абсолютное влияние на преобразования в общественном