ИНФОРМАЦИОННЫЕ ВОЙНЫ

Валиуллин И. И.

ЭВОЛЮЦИЯ ПОНЯТИЯ «ИНФОРМАЦИОННАЯ ВОЙНА» В ПОЛИТИЧЕСКОЙ НАУКЕ

Аннотация. *Настоящая статья посвящена исследованию генезиса феномена и понятия информационной войны. «Информационная война» — это во-многом публицистическое понятие, которое появилось с одной стороны на почве футурологического дискурса, порожденного концепциями постиндустриального (информационного) общества (эры) Дэниела Белла, Элвина Тоффлера, Мануэля Кательса etc., а с другой стороны вследствие отражения в журналистике объективных явлений: оформления информационной сферы, появление новых типов СМИ, роста скорости распространения информации и возрастание влияния информационной на другие сферы общества. И при всем этом термин «информационная война» отражает как минимум две важные тенденции, во-первых, это проецирование противостояния из военной (силовой) сферы в информационную, а во-вторых, реализация преимущества, полученного в информационной сфере, в силовом измерении конфликта. Сам термин информационной войны заимствован из западного околовоенного дискурса. В 1976 году его ввел Thomas P. Rona в своем докладе для компании Boeing, озаглавленном «Weapon System and Information War». В этом докладе он указал, что информационная инфраструктура становится одним из наиболее важных и при этом наиболее уязвимых секторов американской экономики.*
Ключевые слова: *международные отношения, внешняя политика, США, мягкая сила, конфликты, дипломатия, государство, интересы, безопасность, информационная война.*

Однако гораздо более распространен не прямой перевод «information war», а вариант «information warfare (IW)». При этом термин «information war», безусловно, не является пустым. Его, к примеру, в своей работе использует Питер Ламборн Уилсон (под псевдонимом Hakim Bey) в своей статье «Information War» 1998 года, в этой статье он раскрывает понятие «information war» через войну за умы людей посредством информации, конечно он рассматривал данный феномен через призму своих «анархических» взглядов, но сумел в полной мере отразить тот смысл термина «information war», которым его будут наполнять журналисты и публицисты в следующие 15 лет.

Информационная война в этом понимании может быть во разному определена во временных рамках. Она может происходить строго в определенный период времени (обычно не сильно расходящийся с рамками соответствующего военного конфликта), как например «Информационная война в Ливии», так пишет Arom Lamm в статье «Information War Rages Over Libya»: «Информационная война разразилась среди путаницы и переполненных СМИ»[1]. Или иметь неопределенное глобальное значение, например, именно такой смысл ей придала Хилари Клинтон в пресс-конференции 2 марта 2011 года: «В течении Холодной войны мы решили великую задачу в распространении американских идей. После падения Берлинской стены мы решили, «все хорошо, мы выполнили нашу миссию», и к несчастью заплатили за это большую цену, наши массмедиа не могут заполнить мировое пространство… Мы в информационной войне и проигрываем эту войну. Аль-Джазира выигрывает, Китай открыл своё глобальное многоязычное телевещание, Россия создала свой англоязычный канал…»[2].

В первом случае значение термина еще предстоит определить, а во втором информационная война становится точкой столкновения проявлений понятия, заданного Джозефом Наем, как «soft power», но ограниченного информационной сферой.

[1] http://www.theepochtimes.com/n2/world/information-war-rages-over-libya-60658.html

[2] http://rt.com/news/information-war-media-us/

DOI: 10.7256/2305-560X.2014.1.10064

Как уже было сказано, более распространенным термином является «Information Warfare». И наиболее релевантным переводом, скорее всего является «информационные способы ведения войны». Данный термин является более прикладным по смыслу и именно поэтому он широко используется в американском военном дискурсе. Однако и у него есть достаточно большое количество определений.

Следует начать с того, что наполнение термин «Information Warfare» прошло через некое эволюционное развитие. В середине XX века, когда уже была немного развита микроэлектроника, у американских военных появилась нужда в надежной системе передачи информации, так появилась ARPANET, которая впоследствии получила название «Интернет». Компьютерные сети заметно ускорили процессы обмена информацией, однако создали уязвимость, ведь теперь её при должном умении мог получить противник. Так зародились концепции кибервойны и кибертерроризма. А средства ведения кибервойны назывались или Cyberwarfare, или Information Warfare. Именно поэтому Lech Janczewski и Andrew Colarik (2008) в своей книге дают такое определение Information warfare: «Информационное оружие: кибертерроризм или более подходящий термин информационное оружие, как обсуждалось ранее, становится обычной техникой для атаки организации. Кибертеррористические группировки используют то, что называется хакерство. Хакеры — это люди, которые затрудняют работу интернет-сайта с неким политическим мотивом, который объявляется от имени кибертеррористической группировки или людей, которые действуют от её имени» (Information warfare: cyber terrorism or the more appropriate term information warfare as discussed earlier is becoming a common technique used to attack organizations. Cyber terrorist group employ what is known as hacktivism. Hacktivists are activists involved in defacing the site of an enemy for a political cause for example, a cyber-terrorism group or a group on behalf of cyber terrorism group[1]). В своей книге они, раскрывают и другое определение Information Warfare: «Информационные способы ведения войны — это использование и управление информацией в гонке за конкурентным преимуществом над оппонентом» (Information warfare this means the use and management of information in pursuit of a competitive advantage over an opponent[2]).

Первое определение характерно для ученых, которые рассматривают сферу информационной безопасности и кибертерроризма, тогда как второе вызвано своеобразным духом времени, когда термин «Information Warfare» стал пониматься более широко. Для конца XX века более характерно понимание «Information warfare» подобное тому, которое выразил Reto E. Haeni в своей книге «Information Warfare»: «Действия, которые направлены на достижение информационного преимущества путем влияния на информацию противника, информационные процессы и компьютерные сети, защищая при этом свою информацию, информационные процессы и компьютерные сети» (Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks[3]).

Конечно, данный подход абсолютно детерминирован запросом своего времени, потребностью в обеспечении безопасности информационных систем совершенно разного уровня. Одной из первых и при этом наиболее популярных книг по проблематике «information warfare» была книга Winn Schwartau «Chaos on the Electronic Superhighway INFORMATION WARFARE» (1997), в которой автор рассматривает прежде всего вопросы информационной безопасности, раскрывая вопросы криптографии, хакерства и компьютерного оборудования. Он даже не дает точного определения «Information Warfare», однако, что важно, пишет, что «Information Warfare» [в смысле книга] должна быть прочитана не только ограниченным кругом лиц занимающихся проблемами информационной безопасности (They understand that Information Warfare needs to be read by more than just the security industry's small choir[4]). И тем самым он, в каком-то смысле, предвидел то, что информационная война скоро станет проблемой не только специалистов информационной безопасности, а её средствами станут не только хакеры, вирусы и dos-атаки.

С разработкой проблем информационной безопасности термин «Information Warfare» постепенно начал приобретать новые смыслы, Megan Burns в своей статье (1999) пишет: «Информационное оружие — это класс техник, включающих сбор, транспортировку, защиту, отрицание, нарушение и ухудшение информации с помощью которых объект получает преимущество перед соперниками» (IW is a class of

[1] Janczewski, Lech, Colarik, Andrew M. «Cyber Warfare and Cyber Terrorism» IGI Global (2008)

[2] Там же

[3] Reto E. Haeni «Information Warfare» The George Washington University Cyberspace Policy Institute (1997)

[4] Winn Schwartau «Chaos on the Electronic Superhighway INFORMATION WARFARE» Thunder's Mouth Press NY 1994

DOI: 10.7256/2305-560X.2014.1.10064

techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries[1]). Таким образом она расширила понятие «Information Warfare», раскрыв его информационную сущность.

Причем, стоит заметить, что если Winn Schwartau разрабатывал проблематику самостоятельно, то Megan Burns и Reto E. Haeni являются сотрудниками Progressive Policy Institute в первом случае и The George Washington University (Cyberspace Policy Institute) во втором. Проблема, которая была поставлена пусть и специалистом, но в какой-то степени все-таки публицистом стало актуальной для академических исследований. Причем стоит заметить, что Progressive Policy Institute — это think tank консервативного крыла Демократической партии США и его исследования имеют влияние на реальные политические решения.

Современные исследования «Information Warfare» проводятся уже под эгидой Министерства Обороны США и других государственных институтах. И эти исследования характеризуются прикладной стороной, и «Information Warfare» исследуется, как с точки зрения национальной обороны США, так и с точки зрения потенциального оружия. Примером подобного подхода может легко служить статья члена Федерации Американских Ученых Brian C. Lewis «Information Warfare», в которой он дает следующее определение IW: «Информационное противостояние в его самом широком смысле является борьбой за информацию и коммуникационный процесс, борьба, которая начинается с появлением у человека коммуникации и конфликта. За последние несколько десятилетий, быстрый рост в информационных и коммуникационных технологиях и их значительное распространение в нашем обществе произвели революцию в коммуникационном процессе и, вместе с этим, изменили значение и последствия информационного противостояния. Информационная война является применением деструктивной силы в больших масштабах против информационных ресурсов и систем, против компьютеров и компьютерных сетей, которые поддерживают четыре стратегически важные инфраструктуры (энергосистемы, коммуникации, финансы и транспорт). Тем не менее, защита от компьютерных вторжений даже в меньших масштабах, в интересах национальной безопасности страны и является важной в текущем обсуждении информационной войны» (Over the past few decades, the rapid rise in information and communication technologies and their increasing prevalence in our society has revolutionized the communications process and with it the significance and implications of information warfare. Information warfare is the application of destructive force on a large scale against information assets and systems, against the computers and networks that support the four critical infrastructures (the power grid, communications, financial, and transportation). However, protecting against computer intrusion even on a smaller scale is in the national security interests of the country and is important in the current discussion about information warfare[2]). В этой статье он также рассматривает потенциал наступательных и оборонительных средств ведения информационного противостояния, а также, что важно рассказывает об эволюции осознания информационной угрозы. Это осознание началось еще в 1990 году Директивой Национальной Безопасности № 42, которая установила уязвимость национальных телекоммуникационных и информационных сетей, постановив разработку защитных механизмов.

Чуть позже, 21 декабря 1992 в директиве DOD 3600 министра обороны США термин «information warfare» был официально введен в дискурс. Именно тогда началось сотрудничество с Winn Schwartau и именно тогда было положено начало крепкому сотрудничеству Министерства Обороны США и корпорации RAND в сфере информационной безопасности.

Здесь важно сказать про труд Martin C. Libicki «What is Information Warfare?», который вышел в издательстве National Defense University (Institute for National Strategic Studies) (Национальный Университет Обороны (Институт Национальных Стратегических Разработок)) в 1995 году. С одной стороны, автор подошел к проблеме «Information Warfare» достаточно однобоко поддержав дискурс того времени, коснувшись и хакеров (7 глава) и темы борьбы в киберпространстве (9 глава), проблемы противостояния в технологическом плане и проблемы разведки (4 и 3 главы соответственно), но самый большой вклад в понимание информационной войны он сделал в главе с названием «Psychological Warfare», где написал следующее: «Мировые медиакомпании, среди которых CNN является лидером, убедились, что события, где бы они не происходили, являются ли они подлинными или организованными шоу могут быть доставлены аудиториям во многих странах» (Global broadcasters, CNN a leader among them, ensure

[1] Megan Burns «Information Warfare: What and How? « 1999 http://www.cs.cmu.edu/~burnsm/InfoWarfare.html

[2] Brian C. Lewis «Information Warfare» 1997 http://www.fas.org/irp/eprint/snyder/infowarfare.htm

DOI: 10.7256/2305-560X.2014.1.10064

that events anywhere on the planet, whether authentic or arranged the show can be delivered to audiences in many countries[1]). Таким образом, уже в 1995 году Martin E. Libicki обозначил важнейшую составляющую «Information Warfare», сильно опередив своих коллег, которые на несколько лет застрянут в теоретизации проблем, которые имеют под собой сугубо технологические решения, так, например, в 1996 году вышел первый плод сотрудничества RAND и Министерства Обороны США.

Книга Robert H. Anderson и Anthony C. Hearn «The Day After… Cyberspace» вышла в 1996 году, в ней авторы пользуясь трехступенчатой методологией разработанной Роджером Моландером в книге «The Day After…» разрабатывали модели реализации различного рода киберугроз. В своей работе они понимали «Information Warfare» в узком прикладном смысле угрозы информационной инфраструктуре: «Оборонное Агентство Передовых Исследовательских Проектов США заинтересовано в понимании стратегий для инвестиций в исследования и фонд развития для обеспечения безопасности информационной инфраструктуры США против информационных способов противостояния» (The U. S. Defense Advanced Research Projects Agency (DARPA) is interested in understanding strategies for the investment of research and development fund for securing the U.S. information infrastructure against «information warfare» (IW) attacks).

С появлением новой сферы для ведения войны перед министерством США возникла задача создания целого ряда нормативно-рекомендательных документов, которые бы на внутриведомственном уровне разъяснили суть информационной войны, её методы, а также разделили ответственность за ту или иную части операций. Министерство Обороны США уже достаточно давно имеет традицию создания Joint Publications по различным сферам ведения боевых действий и национальной безопасности, которые со временем рассекречиваются или некоторое время спустя публикуются в Интернете.

Было выпущено три издания Joint Publication for Information Operations 3–13 9 октября 1998 г., 13 февраля 2006 г. и 27 ноября 2012 г и дополнительный документ Information Operations Roadmap 30 октября 2003 (рассекречен в 2006 году). Что примечательно, данные публикации не являются отдельными, независимыми работами, а составляют единое целое. Каждая публикация резюмирует тезисы предыдущих и дополняет их, формируя цельную военную доктрину по предмету Information Operations. Эти документы имеют крайне прикладную направленность, и рассматривают феномен информационной войны в большей степени с институциональной точки зрения. С точки зрения ответственности за проведение и планирование Information Operations. Это и ограничение и возможность.

Определение Information Operations проходит некую эволюцию в трёх стадиях. Сначала это достаточно простая дефиниция, основанная на «информационной» компоненте феномена: *«Информационные операции — это набор действий, осуществляемых для влияния на информацию и информационную систему противника при защите своих (Information operations. Actions taken to affect adversary information and information system while defending one's own information and information systems) «.* Данное определение не очень удачно ни в смысле попытки дать наиболее общее определение информационной операции, ни в смысле создание эффективной прикладной дефиниции, именно поэтому в следующем переиздании Joint Publication for Information Operations определение IO меняется достаточно радикально: *«Информационная операция — это объединенное использование пяти ключевых направлений: электронного оружия, операций с компьютерными сетями, психологических операций, военной хитрости и операций по обеспечению безопасности — в совокупности со специальными направлениями поддержки и дополнительными направлениями с целью влияния, разрушения, повреждения вражеских систем принятия решений, осуществляемых, как людьми, так и автоматически, при защите своих аналогичных систем (The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operation security, in concert with specified supporting and related capabilities, to influence disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own)».* Новое определение включает в себя разделение Information Operations на пять ключевых направлений. Это разделение используется и сейчас. Однако подобное определение получилось слишком громоздким, более того позднее наполнение IO было расширено, это отражено в документе Information Operation Primer, выпущенном в ноябре 2006 г. для U. S. Army College. К пяти ключевым направлениям были добавлены еще 5 направлений поддержки и еще 3 дополнительных направления. Поэтому в редакции документа 2012 года определе-

[1] Martin C. Libicki «What Is Information Warfare?» The Center For Advanced Command Concepts And Technology Institute for National Strategic Studies National Defense university 1995

DOI: 10.7256/2305-560X.2014.1.10064

ние вновь изменилось, окончательно оно выглядит следующим образом: *«Объединенное использование информационных направлений в течении военных операций вместе с другими измерениями операции с целью влияния, разрушения, повреждения вражеских систем принятия решений, осуществляемых, как людьми, так и автоматически, при защите своих аналогичных систем (The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own)*». Оно достаточно точно представляет американский прикладной подход к формулированию IO, но в нём есть существенный недостаток, оно привязывает ведение IO во временном измерении к военным операциям, тогда как уже в редакции 1998 года в первой главе, где рассматривалась размерность категорий понятий «Information Operations», «Information Assurance», «Information Warfare» и «Special Information Operations' относительно друг друга в темпоральном измерении, указано, что IO — это самая широкая категория, выходящая за рамки военного времени. Также в последних двух редакциях достаточно явно обозначено расширение данного понятия.

Таким образом в США сформировался достаточно прикладной военный подход к формированию цельной теории IW и IO. Он направлен прежде всего на научную поддержку военной деятельности США, что достаточно удачно сказывается на его эффективности. Также в США есть ряд не аффилированных с военными авторов, которые развивают свои подходы, теории, делая свой вклад в расширение и развитие теории за рамки военных операций.

В России нет столь серьезной практики развития военными теории информационной войны. Из-за обилия публицистической литературы по данной тематике дефиниции понятия достаточно расплылись, что оказало критическое влияние на развитие теории. Таким образом, в России практически отсутствует прикладное крыло развития теории информационной войны. Что является проблемой на уровне национальной обороны.

Конечно, есть утвержденная 9 сентября 2000 года Президентом российской Федерации В. В. Путиным Доктрина информационной безопасности Российской Федерации. Однако очевидно, что данный документ устарел и не отвечает современным вызовам международной политики. Подход к осуществлению информационной безопасности, имеющийся в доктрине имеет много схожих черт с подходом, который использовали американские ученые в ранних работах по информационной безопасности, подразумевая в большей степени кибербезопасность. Доктрина требует серьезной доработки.

Отсутствие договоренности по использованию понятий «информационной войны» в научном дискурсе приводит к печальным последствиям. К примеру, авторы С. Н. Бухарин и В. В. Цыганов в книгах «Методы и технологии информационных войн» и «Информационные войны в бизнесе и политике» углубляются в технические моменты и кейсы, при этом не давая четкой дефиниции информационной войны. Именно поэтому, некоторые их кейсы и примеры к ней не относятся вовсе.

Обратной стороной является определение информационной войны, данное в книге «Информационная война и геополитика» Игорем Панариным: «На наш взгляд, информационную войну можно определить как способ создания системы управления информационными потоками в целях организации ноосферы и мирового информационно-психологического пространства в своих интересах»[1]. Данное определение очень общее и не позволяет нам никаким образом рассматривать огромное количество менее масштабных феноменов, которые преследуют вполне конкретные цели, не подразумевая при этом создания мировой системы управления информационными потоками, тем самым оно нас ограничивает.

Работа Г. Г. Почепцова представляет интерес в плане попытки разрешения проблемы дефиниций. В разделе «Информационная война: методологические основания» первой главы он рассматривает определения, данные американскими военными, оценивает их прикладную сторону. Также он рассматривает определения, данные в своих работах Завадским И. И. (Информационная война — что это такое?), Викторовым А. Ф. (Информационная война в современных условиях) и другими. Отмечая, прежде всего, что определения, даваемые ими, больше относятся к техническим аспектам, где основным орудием является компьютер, а основной целью база данных. Но, проявляя разумный критический подход, автор не дает своей дефиниции и не выделяет наиболее, по его мнению, релевантной.

Также нельзя не сказать о работах А. В. Манойло. В книге «Технологии несилового разрешения современных конфликтов» автор обозначает информационно-психологическую войну с двух сторон. Со стороны конфликтологии: «Поэтому в современных условиях

[1] Игорь Панарин — «Информационная война и геополитика». «Поколение», 2006 г.

DOI: 10.7256/2305-560X.2014.1.10064

ИПВ — не просто особая форма политического конфликта, но и особая стадия, занимающая в эволюции конфликта промежуточную ступень между мирной фазой и военной»[1] и со стороны инструменталистского подхода: «… по сути ИПВ — это политический конфликт, в котором конфликтующими сторонами для достижения преимущества перед оппонентами отдается предпочтение силовым методам воздействия в форме психологических операций с применением агрессивных информационно-психологических технологий и информационного оружия»[2]. Первое определение интересно тем, что феномен ИПВ выводится за рамки конфликта, однако его недостаток в том, что недооценивается сервисная роль ИПВ непосредственно в военном столкновении. Другое определение нам интересно тем, что автор, выбрав в качестве критерия средства проведения конфликта, четко очертил рамки исследования феномена ИПВ, однако оно всё равно оказалось фазой развертывания политического конфликта, что, в каком-то смысле, связывает нам руки в исследовании объективных явлений, где ИПВ происходила во время военных действий. Яркий тому пример — события Югоосетинской войны 2008 года.

Есть еще одно определение, данное А. В. Манойло в своей монографии «Государственная информационная политика в особых условиях»: «Информационно-психологическая война появилась как форма информационного противоборства на определенной стадии развития средств и методов информационно-психологического воздействия и в настоящее время представляет собой наиболее социально опасную форму данного противоборства, осуществляемого насильственными средствами и способами воздействия на информационно-психологическую сферу противника с целью решения стратегических задач»[3]. Плюсы данного определения состоят в том, что, во-первых, оно достаточно четко согласовано с категорией информационного противодействия, во-вторых, оно подчеркивает две наиболее важные качественные характеристики информационной войны, а именно её насильственную сторону, а также сферу её проведения. Если рассматривать данное определение, как дефиницию явления в самом широком смысле, то оно является во многом самым удачным.

В России существуют объективные проблемы с определением информационной войны» в научном дискурсе и формирования единой парадигмы для исследования феномена. Также существует проблема закрепления этой доктрины на законодательном уровне, так как текущая доктрина информационной безопасности является устаревшей. Информационная сфера является наиболее быстро развивающейся сферой общественной жизни, а технологическая сторона этой сферы является локомотивом индустриального развития, поэтому доктрина 13-летней давности никак не может быть актуальной. Недаром Henry H. Shelton, автор первой редакции «Joint Doctrine for Information operations' установил пятилетний срок в качестве крайнего для обновления доктрины.

Библиография

1. Aron Lamm «Information War Rages Over Libya» The Epoch Times – 2011 http://www.theepochtimes.com/n2/world/information-war-rages-over-libya-60658.html
2. Brian C. Lewis. Information Warfare, 1997 г. http://www.fas.org/irp/eprint/snyder/infowarfare.htm
3. Gayane Chichakyan, Kevin Owen. Hillary Clinton declares international information war. Russia Today, 2011 г. http://rt.com/news/information-war-media-us/
4. Janczewski, Lech, Colarik, Andrew M. Cyber Warfare and Cyber Terrorism. IGI Global, 2008 г.
5. Martin C. Libicki .What Is Information Warfare?. The Center For Advanced Command Concepts And Technology Institute for National Strategic Studies National Defense University, 1995 г.
6. Megan Burns Information Warfare: What and How?, 1999 г. http://www.cs.cmu.edu/~burnsm/InfoWarfare.html
7. Reto E. Haeni Information Warfare. The George Washington University Cyberspace Policy Institute, 1997 г.
8. Winn Schwartau Chaos on the Electronic Superhighway INFORMATION WARFARE. Thunder's Mouth Press NY, 1994 г.
9. Панарин И.Н. Информационная война и геополитика. Поколение, 2006 г.
10. Манойло А.В. Технологии несилового разрешения конфликтов. Горячая линия – Телеком, 2008 г.
11. Манойло А.В. Государственная информационная политика в особых условиях. МИФИ, 2003 г.

[1] А. В. Манойло — «Технологии несилового разрешения конфликтов». «Горячая линия — Телеком», 2008 г.

[2] Там же.

[3] А. В. Манойло — «Государственная информационная политика в особых условиях». МИФИ, 2003 г.

DOI: 10.7256/2305-560X.2014.1.10064

12. Буханов С.Н., Цыганов В.В. Методы и технологии информационных войн. Академический проект, 2007 г.
13. Буханов С.Н., Цыганов В.В. Информационные войны в бизнесе и политике Академический проект, 2007 г.
14. С.В. Коновченко, А.Г. Киселев «Информационная политика». РАГС, 2004 г.
15. http://www.iwar.org.uk/infocon/io-kuehl.htm
16. http://www.diggerhistory.info/pages-conflicts-periods/other/crimea.htm
17. Райхлин Э.И. Сотворили ли они историю или история сотворила их? // NB: Международные отношения. - 2013. - 4. - С. 27 - 46. URL: http://www.e-notabene.ru/wi/article_9421.html
18. Перов Е.В. Теория и анализ социальной конфликтогенности общества // NB: Национальная безопасность. - 2013. - 5. - С. 67 - 141. URL: http://www.e-notabene.ru/nb/article_2308.html
19. Манойло А.В. Ценностные основы управления межцивилизационными конфликтами: российская модель // NB: Международные отношения. - 2012. - 1. - С. 32 - 43. DOI: 10.7256/2306-4226.2012.1.279. URL: http://www.e-notabene.ru/wi/article_279.html
20. Владимирова Т.В. К социальной природе понятия «информационная безопасность» // NB: Национальная безопасность. - 2013. - 4. - С. 78 - 95. URL: http://www.e-notabene.ru/nb/article_596.html

References

1. Aron Lamm «Information War Rages Over Libya» The Epoch Times – 2011 http://www.theepochtimes.com/n2/world/information-war-rages-over-libya-60658.html
2. Brian C. Lewis. Information Warfare, 1997 g. http://www.fas.org/irp/eprint/snyder/infowarfare.htm
3. Gayane Chichakyan, Kevin Owen. Hillary Clinton declares international information war. Russia Today, 2011 g. http://rt.com/news/information-war-media-us/
4. Janczewski, Lech, Colarik, Andrew M. Cyber Warfare and Cyber Terrorism. IGI Global, 2008 g.
5. Martin C. Libicki .What Is Information Warfare?. The Center For Advanced Command Concepts And Technology Institute for National Strategic Studies National Defense University, 1995 g.
6. Megan Burns Information Warfare: What and How?, 1999 g. http://www.cs.cmu.edu/~burnsm/InfoWarfare.html
7. Reto E. Haeni Information Warfare. The George Washington University Cyberspace Policy Institute, 1997 g.
8. Winn Schwartau Chaos on the Electronic Superhighway INFORMATION WARFARE. Thunder's Mouth Press NY, 1994 g.
9. Panarin I.N. Informatsionnaya voina i geopolitika. Pokolenie, 2006 g.
10. Manoilo A.V. Tekhnologii nesilovogo razresheniya konfliktov. Goryachaya liniya – Telekom, 2008 g.
11. Manoilo A.V. Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh. MIFI, 2003 g.
12. Bukhanov S.N., Tsyganov V.V. Metody i tekhnologii informatsionnykh voin. Akademicheskii proekt, 2007 g.
13. Bukhanov S.N., Tsyganov V.V. Informatsionnye voiny v biznese i politike Akademicheskii proekt, 2007 g.
14. S.V. Konovchenko, A.G. Kiselev «Informatsionnaya politika». RAGS, 2004 g.
15. http://www.iwar.org.uk/infocon/io-kuehl.htm
16. http://www.diggerhistory.info/pages-conflicts-periods/other/crimea.htm
17. Raikhlin E.I. Sotvorili li oni istoriyu ili istoriya sotvorila ikh? // NB: Mezhdunarodnye otnosheniya. - 2013. - 4. - C. 27 - 46. URL: http://www.e-notabene.ru/wi/article_9421.html
18. Perov E.V. Teoriya i analiz sotsial'noi konfliktogennosti obshchestva // NB: Natsional'naya bezopasnost'. - 2013. - 5. - C. 67 - 141. URL: http://www.e-notabene.ru/nb/article_2308.html
19. Manoilo A.V. Tsennostnye osnovy upravleniya mezhtsivilizatsionnymi konfliktami: rossiiskaya model' // NB: Mezhdunarodnye otnosheniya. - 2012. - 1. - C. 32 - 43. DOI: 10.7256/2306-4226.2012.1.279. URL: http://www.e-notabene.ru/wi/article_279.html
20. Vladimirova T.V. K sotsial'noi prirode ponyatiya «informatsionnaya bezopasnost'» // NB: Natsional'naya bezopasnost'. - 2013. - 4. - C. 78 - 95. URL: http://www.e-notabene.ru/nb/article_596.html

DOI: 10.7256/2305-560X.2014.1.10064