Е. А. Виноградова

# ИНФОРМАЦИОННАЯ ВОЙНА: КОНЦЕПТУАЛЬНЫЙ АНАЛИЗ

**Аннотация.** *В данной статье автор исследования, обращаясь к истории появления понятия информационное противоборство, делает попытку рассмотреть и проанализировать основные концепции информационной войны и раскрыть новейшие технологические и информационно - коммуникационные достижения в этой области. Информационная война ведется в форме информационных и психологических операций, главной целью которых является обеспечение информационного превосходства и доминирующей роли в управлении политическими процессами и использовании информации и информационных структур в интересах обеспечения собственного превосходства. Методологическую основу исследования составляют системный, структурно-функциональный, сравнительно-исторический, сравнительно-политический, геополитический и культурно-цивилизационный подходы, методы анализа, синтеза, индукции, дедукции, моделирования, наблюдения. Сегодня информационная война стала главным средством проведения военно-политических операций Соединенными Штатами Америки, Китаем, странами Европейского Союза. Главными конкурентами в разработках теории и практики ИВ являются США и Китай, между которыми ведется скрытая конкурирующая борьба за лидерство в данной области. Во многих странах мира, как например, в странах Латинской Америки ИВ носит лишь оборонительный характер и используется только в случае потенциальной опасности.*

**Ключевые слова:** *политика, управление, информационная война, психологические операции, США, информационное противоборство, кибервойна, Россия, Латинская Америка, Китай*

Любой военный конфликт конца XX и начала XXI в., в котором участвовали ВС США и ОВС НАТО, начинался с мощного информационного воздействия на сознание военно–политического руководства вероятного противника, на подсознание людей во всем мире и, особенно, атакуемых государств[1].

ИП ведется в форме информационных операций, главной целью которых является обеспечение информационного превосходства и доминирующей роли в управлении и использовании информации и информационных структур. Информационные операции стали одной из форм ведения боевых действий, а информационная сфера, включая киберпространство - сферой боевых действий, полностью сопоставимой с другими подобными сферами в космическом, воздушном, наземном и морском пространствах[2].

Информационное противоборство как направление научных исследований и практической деятельности имеет давнюю историю. Хотя в прямой постановке этот термин вошел в теорию и практику относительно недавно, в середине 1970-х гг., однако в качестве объективного явления информационное противоборство зародилось в глубокой древности. Оно возникло одновременно с появлением вооруженного противоборства – как составная часть вооруженной борьбы в виде психологического средства ослабления боевой мощи противника и поднятия боевого духа своих войск. [3]

[1] Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны реальная угроза национальной безопасности. – М.: КРАСАНД, 2011. – С.79

[2] Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны реальная угроза национальной безопасности. – М.: КРАСАНД, 2011. – С. 79-80

[3] Воронцова Л.В., Фролов Д.Б. История информационного противоборства. – М.: Горячая линия – Телеком, 2006. – С.3



DOI: 10.7256/2307-9118.2014.3.12722

На Западе отцом термина «информационное противоборство» называют ученого-физика Томаса Рона, который в 1976 году назвал информацию самым слабым звеном вооруженных сил и обороны[4]. В начале 1990- х гг., началось его интенсивное развитие и практическая реализация.

Среди российских специалистов, работающих в этой области, существует несколько определений понятия информационное противоборство, которое на русском языке зачастую звучит как информационная война (ИВ).

Так, Е.Н. Пашенцев считает, что информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем (государств, партий, коммерческих и некоммерческих структур) друг на друга с целью ликвидации (или присвоения) нематериальных активов противной стороны и получения определенного выигрыша в материальной сфере. Средствами ведения информационной войны являются СМИ, неформальные коммуникации (слухи, информация из «уст в уста» и др.). Однако системная и многоходовая проработка отдельных операций, связывание их в «латентный» для подавляющего большинства людей пакет действий делают информационную войну весьма эффективным средством управления целевыми аудиториями[5].

Другой отечественный специалист, А.В. Манойло, выдвигает следующую «конфликтологическую» гипотезу информационно-психологической войны: информационно-психологическая война – политический конфликт с целью разрешения противоречий по поводу власти и управления, в котором столкновение сторон осуществляется в форме информационно-психологических операций с применением информационного оружия. В рамках этой гипотезы цель ИПВ – разрешение противоречий по поводу власти и осуществления политического руководства в информационно-психологическом пространстве.[6]

И.Н. Панарин считает, что информационная война – это основное средство мировой политики на протяжении всей истории человечества, доминирующий способ достижения духовной, политической, финансовой и экономической власти в мире. Это способ организации процесса управления коммуникациями в своих интересах и целях.[7]

В.К. Новиков в своей работе «Информационное оружие – оружие современных и будущих войн» считает, что ИВ – это противоборство между двумя или несколькими сторонами, при котором одна сторона воздействует на информационный ресурс другой стороны с помощью своего информационного оружия, защищает собственный информационный ресурс от аналогичного воздействия другой стороны[8].

Таким образом, мы можем видеть, что, несмотря на несколько различные трактовки данного понятия, все исследователи указывают на введение государствами скрытого целенаправленного противоборства данного вида с целью управления целевыми аудиториями.

На сегодняшний день существует не один десяток научных школ, занимающихся изучением информационных противоборств, а также их практическим оснащением. Крупнейшими из них являются США и Китай. За последние 10-15 лет этим странам удалось сформировать концепции информационных противоборств и разработать новую технологическую информационно – коммуникационную базу для их проведения. На сегодняшний день Китай и США являются главными конкурирующими разработчиками теории и практики проведения ИП.

В США четко просматриваются два основных уровня реализации концепции ИП: государственный и военный.

Целью ИП на государственном уровне является доступ к закрытым информационным ресурсам государства–конкурента и принуждение его к принятию выгодных для Вашингтона решений, а также защита собственных ресурсов.

[4] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная политика в условиях информационно-психологической войны. – 2-е изд., – М.: Горячая линия – Телеком, 2009. – С.95.

[5] Пашенцев Е.Н. Коммуникационный менеджмент и стратегическая коммуникация. М.МЦСПИК, ЦКМ РАНХиГС. – М, 2012. – С.65.

[6] Манойло А.В.К вопросу о содержании понятия Информационная война. [Электронный ресурс]. – URL: http://ashpi.asu.ru/ic/?p=1552 (дата обращения: 12.02.2012)

[7] Панарин И.Н. Информационная война и коммуникации. – М.: Горячая линия – Телеком, 2014. – С.6.

[8] Новиков В.К. Информационное оружие – оружие современных и будущих войн. – М.: Горячая линия – Телеком, 2011. – С.52.


DOI: 10.7256/2307-9118.2014.3.12722

В системе государственного управления США организована и осуществляется единая программа защиты информации, в основу которой положен принцип централизованного руководства и контроля специальными государственными органами за потоком информации, прямо или косвенно затрагивающих интересы страны.[9]

Военные специалисты США и НАТО считают, что информационное противоборство представляет собой ведение боевых действий, использование и управление информационными технологиями с целью достижения конкурентного преимущества над противником, куда входит распространение пропаганды и дезинформации для управления целевыми аудиториями противоборствующей стороны, направленной на подрыв качества противоположной информационной силы и отказа в предоставлении информации[10].

Директива министерства обороны США D – 3600.1 от 14 августа 2006 года впервые четко определила основные задачи и функции «информационных операций», в целом означающих комплексное применение сил и средств: радиоэлектронной войны, операций в компьютерных сетях, психологических операций, военной дезинформации и оперативной безопасности.[11]Данная директива также сформировала политику МО США в области проведения информационных операций – «они должны применятся в целях обеспечения завоевания всестороннего и объемлющего превосходства за счет реализации превосходства в перспективных технологиях, поддержания стратегического доминирования США в информационных технологиях и извлечения выгоды от близкого к реальному времени глобального распространения информации для воздействия на систему управления противника и его цикл подготовки и принятия решений, все, что должно обеспечить завоевание и удержание США информационного превосходства».[12]

В программах Университета национальной обороны США выделяются следующие формы ИП:

1) радиоэлектронная борьба;
2) психологическая война;
3) война с использованием средств разведки;
4) война с использованием потенциала хакеров;
5) кибернетическая война[13].

Китайские военные аналитики относят информационное противоборство к боевым операциям, при активном участии в них целевых аудиторий, с применением высоких технологий, в которых обе стороны используют информационные технологии (средства, оборудование, или системы) для управления и получения информации противника. Информационная операция нацелена на перехватывание инициативы у противника, захват, управление, и использование его информации и средств для своей информации в информационном противоборстве[14].

Таким образом, целью информационного противоборства, согласно китайским трактовкам, является нападение на информационное системы противника для защиты информационной инфраструктуры собственных сил.

Данную гипотезу подтверждают исследования американского специалиста Джеймса Мальвенона, который опираясь на многочисленные китайские источники, утверждает, что целью ИП в китайской трактовке является информационное господство над противником. [*zhixinxiquan*].[15]

Согласно другой гипотезе, которую выдвигает в своей работе «Информационная война Китая: призрач-

[9] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика – в условиях информационно – психологической войны. – 2-е изд., – М.: Горячая линия – Телеком, 2009. – С. 229.

[10] [Электронный ресурс]. – URL: http://www.mastermind-technology.com/Sources/InfoWarfare.pdf (дата обращения: 17.03.2012)

[11] U.S. Dep't of Def., Dir.3600.1 // Information Operations. August 14, 2006.www.dtic.mil/whs/directives/corres/pdf/360001p.pdf

[12] U.S. Dep't of Def., Dir.3600.1 // Information Operations. August 14, 2006.www.dtic.mil/whs/directives/corres/pdf/360001p.pdf

[13] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика – в условиях информационно – психологической войны. – 2-е изд., – М.: Горячая линия – Телеком, 2009. – С. 229 – 230.

[14] Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington. 1997. DC: National Defense University Press. - P. 328.

[15] Mulvenon James. The PLA and Information Warfare, in The People's Liberation Army in the Information Age, Mulvenon James and Yang Richard H., eds., Washington. 1999. DC: RAND,– P. 180.



DOI: 10.7256/2307-9118.2014.3.12722

ная опасность или нарождающаяся угроза», известный эксперт Института анализа иностранной политики по вопросам безопасности в Азиатско-Тихоокеанском регионе Тоши Ешихара, китайская информационная война нацелена на разрушение у противника процесса выработки и принятия управленческих решений за счет воздействия на возможности противника получать, обрабатывать, передавать и использовать информацию».[16]

Современное проведение военных действий согласно китайским трактовкам состоит из двух этапов: оборонительного и наступательного, которые включают в себя следующие формы ИП:

1) физическое уничтожение противника (применение артиллерии, бомб, ракет, звуковых, электрических, инфракрасных волн, лазеров);[17]

2) господство над электронным сектором – радиоэлектронная война. Китайцы считают, что противоборство в электромагнитном спектре является решающей фазой войны. Объективная цель состоит в том, чтобы доминировать над этим спектром, предотвращая эффективное использование врагом электронного оборудования. В качестве инструментов могут быть использованы: электронный затор, электронный обман. Микроэлектроника станет ключевой технологической областью для инвестиций;[18]

3) компьютерная сетевая война. Подключение к противоборству хакеров и кибероперациий. Виртуальное моделирование войны;[19]

4) психологические манипуляции. Сюда входит дезинформация целевой аудитории противника для изменения ее поведения. Психологическое воздействие должно ослабить желание врага продолжать борьбу. Основные инструменты: пропаганда, СМИ, листовки, брошюры, электронные послания. [20]

Здесь надо отметить, что подобная теория зеркально отражает американскую доктрину ИП.

Несмотря на это, согласно тревожным оценкам американских экспертов, Китай продолжает развивать новую технологическую базу ИП, которая в силу закрытости информации о ее разработках и потенциале, может оказать серьезное противодействие США и их союзникам.

Говоря о развитии ИП в других странах современного мира, следует отметить, что в теоретическом и практическом применении ИП полностью копируют перечисленные выше модели ИП США и Китая.

Во многих странах, например, в государствах Латинской Америки, ИП носит лишь оборонительный характер, как мы смогли увидеть из описанного выше примера сапатиского движения.

В конце XX века в ВС США наряду с определением ИП, появился такой новый термин, как «кибервойна»(Cyber Warfare).

Одно из определений термина «кибервойна» звучит так: использование интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информационной безопасности и суверенитету другого государства.

Более четкое определение кибервойне дал эксперт по безопасности правительства США Ричард А. Кларк в своей книге «Кибервойна» - действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения.[21]

На сегодняшний день ведущие специалисты, работающие в этой области, выделяют следующие виды атак в интернете:

- ***Вандализм*** – использование хакерами интернета для порчи интернет – страниц, замены содержания оскорбительными или пропагандистскими картинками.
- ***Пропаганда*** – рассылка сообщений пропагандистского характера или вставка пропаганды в содержание других интернет-страниц.
- ***Сбор информации*** - взлом частных страниц или серверов для сбора секретной информации или

[16] Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute; U.S. Army war College; Carlisle Barracks, Pennsylvania. 2001. P. 25.

[17] Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington.1997. DC: National Defense University Press. P. 332.

[18] Wang Baocun, "A Preliminary Analysis of Information. Warfare," Zhongguo Junshi Kexue, November 11, 1997, in FBIS-CHI, March 29, 1998 - P.3.

[19] Zeng Sunan and Zhu Xiaoning, "Virtual Reality: An Important Medium in Theoretical Innovation," Jiefangjun Bao, May 16, 2000, in FBIS-CHI, May 16, 2000.

[20] Yoshihara Toshi. CHINESE INFORMATION WARFARE: A PHANTOM MENACE OR EMERGING THREAT. – 2001. – P. 16-17.

[21] Clarke Richard A. Cyber War. Harper Collins, 2010. – P.5.





DOI: 10.7256/2307-9118.2014.3.12722

ее замены на фальшивую полезную другому государству.

- ***Отказ сервера -*** атаки с различных компьютеров для предотвращения функционирования сайтов или компьютерных систем.
- ***Вмешательство в работу оборудования -*** атаки на компьютеры, которые занимаются контролем над работой гражданского или военного оборудования, что приводит к его отключению или поломке.
- ***Атаки на пункты инфраструктуры -*** атаки на компьютеры, обеспечивающие жизнедеятельность городов и их инфраструктуры, такой как системы телефонии, водоснабжения, электроэнергии, пожарной охраны, транспорта.

Обращаясь к истории «кибервойны» отметим, что первым шагом в направлении ее стратегической разработки стало подписание летом 2002 года президентом Дж. Бушем директивы по национальной безопасности NSPD16, в которой он потребовал разработки национальной политики и порядка действий при использовании киберпространства как сферы противоборства».[22]

14 февраля 2003 года президент Дж. Буш младший подписал секретную директиву,[23] требующую от правительства разработать руководство национального уровня для определения последовательности и характера действий США при реагировании на кибератаки. Доктрина должна была установить правила, в соответствии с которыми США будут принимать решения о наступательных действиях в киберпространстве – проникать и блокировать иностранные компьютерные системы, а также осуществлять оборонительные мероприятия от кибератак противника.

Президент Барак Обама не ослабил внимание к сфере защиты киберпространства и особо выделил проблему кибербезопасности в своей речи 29 мая 2009 года. Эта речь совпала по времени с выпуском администрацией «Обзора по вопросам политики в киберпространстве». В нем был сделан вывод о том, что кибербезопасность в настоящее время стала крупной проблемой для национальной безопасности, и перспективная политика США в этой сфере должна уважать права личности и гражданские свободы.

Доктрина кибервойны многих стран мира состоит из следующих положений:

- Наступательные операции в киберпространстве. Этот компонент относится к разработке и использованию кибероружия.
- Кибероружие. Данный компонент основывает новую классификацию возможностей для разрушения компьютерных систем и сетей.
- Оборонительные операции в киберпространстве.
- Операции по захвату преимущества в киберпространстве.
- Разведывательные операции в киберпространстве.
- Стратегия проведения операций в киберпространстве.

Говоря о китайских разработках в области кибернетической войны, следует отметить, что в последние годы хакеры и специалисты–практики ИП в Китае систематически проводят активное тестирование системы киберзащиты информационно – коммуникационных систем США в серии атак так называемой низкой интенсивности.

В 2006 году в докладе конгрессу комиссии по обзору американо-китайских экономических связей и безопасности было отмечено, что такая активность полностью соответствует содержанию принятой в Китае программы ведения киберразведки, в которой ставится задача «зондирования компьютерных сетей государственных органов управления США и сетей частных компаний» с целью «вскрытия элементов уязвимости в этих сетях, определения порядка и схемы принятия решений в органах управления, вскрытия схем и моделей организации системы коммуникаций в органах государственного управления и частных компаний, синтез структуры связей в системах связи и добывания ценной информации, размещенной на серверах этих сетей».[24]

В качестве яркого примера использования кибератак в мировой практике, можно назвать события, начавшиеся в июле 2009 года предположительно с территории КНДР. Волна кибератак временно подавила работу веб-сайтов некоторых государственных учреждений Южной Кореи и США.[25] Произошло это в период проведения КНДР последовательной серии

[22] Bradley T. Pandora's Box//About.com. http://netsecurity.About.com/library/weekly/aa031703b.htm

[23] The National Strategy to Secure Cyber Space. Washington. 2003.

[24] Tracik J. China's Quest for a superpower military // Heritage Foundation Backgrounder. May 17,2007.№2036

[25] Cyber Attacks Jam Government and Commercial Web Sites in U.S. and South Korea // New York Times. July 9.2009.



DOI: 10.7256/2307-9118.2014.3.12722

выпусков баллистических ракет, усиления общей дипломатической напряженности, связанной с ее ядерной программой, и угрозы введения санкций со стороны США и ООН.

Наиболее громким происшествием, связанным с кибервойной, стала вирусная атака на компьютеры сотрудников атомной электростанции в Иранском Бушере 23 сентября 2010 года.[26] Вероятнее всего через заряженные вирусом stuxnet флеш-носители пострадала компьютерная система управления электростанцией. Правда, по заявлению иранских официальных лиц в газете Iran Daily, эта атака не нанесла серьезного ущерба основному контуру управления.

Еще одним примером кибероперации в сетях, может послужить хакерская атака в Twitter на страницу главного кандидата в президенты Венесуэлы Николаса Мадуро незадолго до закрытия избирательных участков, направленная, скорее всего на подрыв политической активности данного кандидата во время выборов в стране. Помимо странички кандидата в президенты атаке подверглись сайты социалистической партии Венесуэлы.

Эти примеры являются ярким подтверждением того, что проблематика нарастания информационных противоборства стала актуальной.

В рамках разработок современных военных стратегий стран Латинской Америки, входящих в интеграционное объединение АЛБА, большое внимание уделено изучению концепций, так называемых ассиметричных войн. Так, сайт Министерства обороны Венесуэлы располагает общиной медиа-библиотекой, в которой находятся электронные ресурсы посвященные изучению теории и практики проведения подобного рода военных операций.

Латиноамериканская концепция ассиметричной войны, сформулированной известным перуанским политологом Альберто Боливаром Окампо[27] в работе «Эра ассиметричных конфликтов».

Согласно этой концепции мы живем в эпоху ассиметричных конфликтов. Ассиметричные конфликты, это так называемые нерегулярные войны, главный акцент которых делается на разведывательные операции и использование специальных сил, которые действуют одновременно в нескольких странах с целью прогнозирования асимметричных планов противника. Главной целью такой войны является, воздействие с помощью манипуляторных технологий и психологических операций на психологическое состояние противника, для срыва его военных планов[28].

Таким образом, мы может отметить, что латиноамериканская концепция асимметричных конфликтов совпадает с концепциями информационного противоборства, изучением природы, которой занимаются ведущие специалисты в США, Китае, ЕС, России.

Подводя некоторые итоги данного раздела, отметим, что бурное развитие информационных технологий к конце XX века вызвало трансформацию вооруженных сил в различных частях мира и привело к появлению новых стратегических категорий в организации и применении вооруженных сил в операциях XXI века. К таким категориям относится «информационное противоборство», «информационные операции», кибервойна.

Главными конкурентами в новейших теоретических и практических разработках ИВ, являются США и Китай, которые создали современную так называемую «гонку вооружений» в этой области.

В выводе данной главы, хотелось бы отметить, что понятие стратегическая коммуникация появилось в начале XXI века в США и в Великобритании.

Как направление научных исследований и практического применения эта управленческая дисциплина находится на стадии становления во многих странах современного мира.

Одним из ведущих и наиболее прогрессивных направлений СК является информационно – психологическая война, примеры которой мы можем проследить, обращаясь к мировой истории.

Сегодня ИВ стала главным средством проведения военных операций США, Китаем, странами ЕС. Главными конкурентами в разработках теории

[26] Всего на многих промышленных объектах в Иране, по данным британской газеты The Daily Mail, данным вирусом было заражено свыше 30 тыс. компьютеров. www.dailymail.co.uk/sciencetech/article-1314580/Stuxnet-worm-targeted-Iran-nuclear-power-station-sophisticated-virus-attack-ever.html

[27] **Альберто Боливар** – перуанский политолог специализирующейся на вопросах геополитической стратегии государств. Работал в качестве советника по вопросам внешней политики Национальный Обороны Перу (1981-1983гг.), а также в качестве гражданского атташе в посольства Перу в США (1994-1998 гг.) Занимался изучением стратегической разведки в Школе Национальной Разведки в Перу (1988г.), был частным консультантом по вопросы безопасности. Наиболее известные работы: «Низкая интенсивность конфликтов и правопорядок» (Великобритания); «Геополитика» (Аргентина); «Национальная оборона и деловая среда» (Перу).

[28] Ocampo Alberto Bolívar. La Era de los conflictos Asimetricos. // Military Review. Enero-Febrero, 2002. – P. 52-53.


DOI: 10.7256/2307-9118.2014.3.12722

и практики ИВ являются США и Китай, между которыми ведется скрытая конкурирующая борьба за лидерство в данной области. Во многих странах мира, как например, в странах Латинской Америки ИВ носит лишь оборонительный характер и используется только в случае потенциальной опасности.

**Библиография**


1. Воронцова Л.В., Фролов Д.Б. История информационного противоборства. – М.: Горячая линия – Телеком, 2006.
2. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика – в условиях информационно – психологической войны. – 2-е изд., – М.: Горячая линия – Телеком, 2009.
3. Манойло А.В.К вопросу о содержании понятия Информационная война. [Электронный ресурс]. – URL: http://ashpi.asu.ru/ic/?p=1552 (дата обращения: 12.02.2012)
4. Манойло А.В. Модель информационно-психологической операции в международных конфликтах. // Право и политика. 2008. №6. С.1387-1394.
5. Новиков В.К. Информационное оружие – оружие современных и будущих войн. – М.: Горячая линия – Телеком, 2011.
6. Панарин И.Н. Информационная война и коммуникации. – М.: Горячая линия – Телеком, 2014.
7. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны реальная угроза национальной безопасности. – М.: КРАСАНД, 2011.
8. Пашенцев Е.Н. Коммуникационный менеджмент и стратегическая коммуникация. М.МЦСПИК, ЦКМ РАНХиГС. – М, 2012.
9. [Электронный ресурс]. – URL: http://www.mastermind-technology.com/Sources/InfoWarfare.pdf (дата обращения: 17.03.2012)
10. Bradley T. Pandora's Box//About.com. http://netsecurity. About.com/library/weekly/aa031703b.htm
11. Clarke Richard A. Cyber War. Harper Collins, 2010.
12. Cyber Attacks Jam Government and Commercial Web Sites in U.S. and South Korea // New York Times. July 9.2009.
13. Mulvenon James. The PLA and Information Warfare, in The People's Liberation Army in the Information Age, Mulvenon James and Yang Richard H., eds., Washington. 1999. DC: RAND.
14. Ocampo Alberto Bolívar. La Era de los conflictos Asimetricos. // Military Review. Enero-Febrero, 2002.
15. The National Strategy to Secure Cyber Space. Washington. 2003.
16. Tracik J. China's Quest for a superpower military // Heritage Foundation Backgrounder. May 17, 2007.№2036
17. U.S. Dep't of Def., Dir.3600.1 // Information Operations. August 14, 2006.www.dtic.mil/whs/directives/corres/pdf/360001p.pdf
18. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington. 1997. DC: National Defense University Press.-P. 328.
19. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington.1997. DC: National Defense University Press.
20. Wang Baocun, "A Preliminary Analysis of Information.Warfare," Zhongguo Junshi Kexue, November 11, 1997, in FBIS-CHI, March 29, 1998
21. Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute; U.S. Army war College; Carlisle Barracks, Pennsylvania. 2001.
22. Yoshihara Toshi.CHINESE INFORMATION WARFARE: A PHANTOM MENACE OR EMERGING THREAT. – 2001.
23. Zeng Sunan and Zhu Xiaoning, "Virtual Reality: An Important Medium in Theoretical Innovation," Jiefangjun Bao, May 16, 2000, in FBIS-CHI, May 16, 2000.
24. Манойло А.В. «Финиковые революции»: стихия или управляемый хаос?//Международная жизнь. – 2011.-№5. – С. 63-78.


**DOI: 10.7256/2307-9118.2014.3.12722**

25. Манойло А.В. Роль стратегий управляемого хаоса в формировании нового миропорядка // Право и политика. – 2014. – №5. – С. 638-651. DOI: 10.7256/1811-9018.2014.5.11816.
26. Манойло А.В. Несиловое регулирование международных конфликтов. Культурно-цивилизационные парадигмы. // Космополис.-2008.-№2. – С.168-174.
27. Манойло А.В. Психологические операции: модели и технологии управления конфликтами. // Политэкс (Политическая экспертиза).-2008.-№3.-С. 62-73.
28. Манойло А.В. Психологические операции США в Ираке. // Космополис.-2008.-№1. – С.124-128.
29. Карпович О.Г. Современные концепции и модели управления международными конфликтами (сравнительный политологический анализ) // Национальная безопасность / nota bene. - 2013. - 4. - С. 605 - 612. DOI: 10.7256/2073-8560.2013.4.6434.
30. А.В. Манойло Парадигмы управления международным конфликтами: конкуренция или конфронтация // Национальная безопасность / nota bene. - 2011. - 5. - С. 135 - 142.
31. Т.П. Петрова Дипломатические отношения между Россией и Перу: современное состояние и динамика развития // Международные отношения. - 2012. - 1. - С. 46 - 53.
32. Манойло А.В. Управление психологической войной // Международные отношения. - 2013. - 3. - С. 377 - 389. DOI: 10.7256/2305-560X.2013.3.6221.
33. Карпович О.Г. Проблемы и перспективы исследования современных концепций, моделей и технологий управления международными конфликтами // Национальная безопасность / nota bene. - 2013. - 5. - С. 80 - 93. DOI: 10.7256/2073-8560.2013.5.6432.
34. Манойло А.В. Сирия и Иран в политике США: ливийский сценарий повторяется // Международные отношения. - 2013. - 1. - С. 4 - 12. DOI: 10.7256/2305-560X.2013.01.1.
35. Алейников А.В. Системные конфликты в России: концептуальные основания анализа. Статья 1. // NB: Проблемы общества и политики. - 2013. - 7. - С. 94 - 140. DOI: 10.7256/2306-0158.2013.7.2306. URL: http://www.e-notabene.ru/pr/article_2306.html
36. Алейников А.В. Системные конфликты в России: концептуальные основания анализа. Статья II. // NB: Проблемы общества и политики. - 2013. - 8. - С. 1 - 47. DOI: 10.7256/2306-0158.2013.8.5109. URL: http://www.e-notabene.ru/pr/article_5109.html
37. А.В. Манойло Актуальные вопросы модернизации современной культурно-цивилизационной теории управления международными конфликтами // Национальная безопасность / nota bene. - 2011. - 4. - С. 60 - 66.
38. Петренко А.И. Теоретические основы организации противодействия использованию арсенала сил, средств и методов информационно-психологической войны в политических целях // Тренды и управление. - 2014. - 2. - С. 154 - 167. DOI: 10.7256/2307-9118.2014.2.12412.
39. Курилкин А.В. Эволюционное развитие психологической борьбы: от пропаганды к психологическим операциям // Международные отношения. - 2014. - 3. - С. 472 - 474. DOI: 10.7256/2305-560X.2014.3.11855.
40. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Сценарный анализ эффективности управления региональной безопасностью // Национальная безопасность / nota bene. - 2014. - 2. - С. 188 - 206. DOI: 10.7256/2073-8560.2014.2.11319.
41. Гулиева Э.Ф. Политика Индии в БРИКС на современном этапе // Тренды и управление. - 2014. - 2. - С. 147 - 153. DOI: 10.7256/2307-9118.2014.2.12408.

**References**

1. Vorontsova L.V., Frolov D.B. Istoriya informatsionnogo protivoborstva. – M.: Goryachaya liniya – Telekom, 2006.
2. Manoilo A.V., Petrenko A.I., Frolov D.B. Gosudarstvennaya informatsionnaya politika – v usloviyakh informatsionno – psikhologicheskoi voiny. – 2-e izd., – M.: Goryachaya liniya – Telekom, 2009.
3. Manoilo A.V.K voprosu o soderzhanii ponyatiya Informatsionnaya voina. [Elektronnyi resurs]. – URL: http://ashpi.asu.ru/ic/?p=1552 (data obrashcheniya: 12.02.2012)



DOI: 10.7256/2307-9118.2014.3.12722

4. Manoilo A.V. Model' informatsionno-psikhologicheskoi operatsii v mezhdunarodnykh konfliktakh. // Pravo i politika. 2008. №6. S.1387-1394.
5. Novikov V.K. Informatsionnoe oruzhie – oruzhie sovremennykh i budushchikh voin. – M.: Goryachaya liniya – Telekom, 2011.
6. Panarin I.N. Informatsionnaya voina i kommunikatsii. – M.: Goryachaya liniya – Telekom, 2014.
7. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A. Kibervoiny real'naya ugroza natsional'noi bezopasnosti. – M.: KRASAND, 2011.
8. Pashentsev E.N. Kommunikatsionnyi menedzhment i strategicheskaya kommunikatsiya. M.MTsSPIK, TsKM RANKhiGS. – M, 2012.
9. [Elektronnyi resurs]. – URL: http://www.mastermind-technology.com/Sources/InfoWarfare.pdf (data obrashcheniya: 17.03.2012)
10. Bradley T. Pandora's Box//About.com. http://netsecurity. About.com/library/weekly/aa031703b.htm
11. Clarke Richard A. Cyber War. Harper Collins, 2010.
12. Cyber Attacks Jam Government and Commercial Web Sites in U.S. and South Korea // New York Times. July 9.2009.
13. Mulvenon James. The PLA and Information Warfare, in The People's Liberation Army in the Information Age, Mulvenon James and Yang Richard H., eds., Washington. 1999. DC: RAND.
14. Ocampo Alberto Bolívar. La Era de los conflictos Asimetricos. // Military Review. Enero-Febrero, 2002.
15. The National Strategy to Secure Cyber Space. Washington. 2003.
16. Tracik J. China's Quest for a superpower military // Heritage Foundation Backgrounder. May 17, 2007.№2036
17. U.S. Dep't of Def., Dir.3600.1 // Information Operations. August 14, 2006.www.dtic.mil/whs/directives/corres/pdf/360001p.pdf
18. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington. 1997. DC: National Defense University Press.-P. 328.
19. Wang Baocun and Li Fei, "Information Warfare," in Chinese Views of Future Warfare, Michael Pillsbury, ed., Washington.1997. DC: National Defense University Press.
20. Wang Baocun, "A Preliminary Analysis of Information.Warfare," Zhongguo Junshi Kexue, November 11, 1997, in FBIS-CHI, March 29, 1998
21. Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute; U.S. Army war College; Carlisle Barracks, Pennsylvania. 2001.
22. Yoshihara Toshi.CHINESE INFORMATION WARFARE: A PHANTOM MENACE OR EMERGING THREAT. – 2001.
23. Zeng Sunan and Zhu Xiaoning, "Virtual Reality: An Important Medium in Theoretical Innovation," Jiefangjun Bao, May 16, 2000, in FBIS-CHI, May 16, 2000.
24. Manoilo A.V. «Finikovye revolyutsii»: stikhiya ili upravlyaemyi khaos?//Mezhdunarodnaya zhizn'. – 2011.-№5. – S. 63-78.
25. Manoilo A.V. Rol' strategii upravlyaemogo khaosa v formirovanii novogo miroporyadka // Pravo i politika. – 2014. – №5. – S. 638-651. DOI: 10.7256/1811-9018.2014.5.11816.
26. Manoilo A.V. Nesilovoe regulirovanie mezhdunarodnykh konfliktov. Kul'turno-tsivilizatsionnye paradigmy. // Kosmopolis.-2008.-№2. – S.168-174.
27. Manoilo A.V. Psikhologicheskie operatsii: modeli i tekhnologii upravleniya konfliktami. // Politeks (Politicheskaya ekspertiza).-2008.-№3.-S. 62-73.
28. Manoilo A.V. Psikhologicheskie operatsii SShA v Irake. // Kosmopolis.-2008.-№1. – S.124-128.
29. Karpovich O.G. Sovremennye kontseptsii i modeli upravleniya mezhdunarodnymi konfliktami (sravnitel'nyi politologicheskii analiz) // Natsional'naya bezopasnost' / nota bene. - 2013. - 4. - C. 605 - 612. DOI: 10.7256/2073-8560.2013.4.6434.
30. A.V. Manoilo Paradigmy upravleniya mezhdunarodnym konfliktami: konkurentsiya ili konfrontatsiya // Natsional'naya bezopasnost' / nota bene. - 2011. - 5. - C. 135 - 142.



DOI: 10.7256/2307-9118.2014.3.12722

31. T.P. Petrova Diplomaticheskie otnosheniya mezhdu Rossiei i Peru: sovremennoe sostoyanie i dinamika razvitiya // Mezhdunarodnye otnosheniya. - 2012. - 1. - C. 46 - 53.
32. Manoilo A.V. Upravlenie psikhologicheskoi voinoi // Mezhdunarodnye otnosheniya. - 2013. - 3. - C. 377 - 389. DOI: 10.7256/2305-560X.2013.3.6221.
33. Karpovich O.G. Problemy i perspektivy issledovaniya sovremennykh kontseptsii, modelei i tekhnologii upravleniya mezhdunarodnymi konfliktami // Natsional'naya bezopasnost' / nota bene. - 2013. - 5. - C. 80 - 93. DOI: 10.7256/2073-8560.2013.5.6432.
34. Manoilo A.V. Siriya i Iran v politike SShA: liviiskii stsenarii povtoryaetsya // Mezhdunarodnye otnosheniya. - 2013. - 1. - C. 4 - 12. DOI: 10.7256/2305-560X.2013.01.1.
35. Aleinikov A.V. Sistemnye konflikty v Rossii: kontseptual'nye osnovaniya analiza. Stat'ya 1. // NB: Problemy obshchestva i politiki. - 2013. - 7. - C. 94 - 140. DOI: 10.7256/2306-0158.2013.7.2306. URL: http://www.e-notabene.ru/pr/article_2306.html
36. Aleinikov A.V. Sistemnye konflikty v Rossii: kontseptual'nye osnovaniya analiza. Stat'ya II. // NB: Problemy obshchestva i politiki. - 2013. - 8. - C. 1 - 47. DOI: 10.7256/2306-0158.2013.8.5109. URL: http://www.e-notabene.ru/pr/article_5109.html
37. A.V. Manoilo Aktual'nye voprosy modernizatsii sovremennoi kul'turno-tsivilizatsionnoi teorii upravleniya mezhdunarodnymi konfliktami // Natsional'naya bezopasnost' / nota bene. - 2011. - 4. - C. 60 - 66.
38. Petrenko A.I. Teoreticheskie osnovy organizatsii protivodeistviya ispol'zovaniyu arsenala sil, sredstv i metodov informatsionno-psikhologicheskoi voiny v politicheskikh tselyakh // Trendy i upravlenie. - 2014. - 2. - C. 154 - 167. DOI: 10.7256/2307-9118.2014.2.12412.
39. Kurilkin A.V. Evolyutsionnoe razvitie psikhologicheskoi bor'by: ot propagandy k psikhologicheskim operatsiyam // Mezhdunarodnye otnosheniya. - 2014. - 3. - C. 472 - 474. DOI: 10.7256/2305-560X.2014.3.11855.
40. Shul'ts V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V. Stsenarnyi analiz effektivnosti upravleniya regional'noi bezopasnost'yu // Natsional'naya bezopasnost' / nota bene. - 2014. - 2. - C. 188 - 206. DOI: 10.7256/2073-8560.2014.2.11319.
41. Gulieva E.F. Politika Indii v BRIKS na sovremennom etape // Trendy i upravlenie. - 2014. - 2. - C. 147 - 153. DOI: 10.7256/2307-9118.2014.2.12408.




DOI: 10.7256/2307-9118.2014.3.12722