

СЛОВО АСПИРАНТАМ И МОЛОДЫМ УЧЕНЫМ

ИНФОРМАЦИОННАЯ ВОЙНА: ПРОБЛЕМА ТЕОРЕТИЧЕСКОЙ ИНТЕРПРЕТАЦИИ

А.В. Борхсениус

Кафедра государственного и муниципального управления
Российский университет дружбы народов
ул. Миклухо-Маклая, 10–2, Москва, Россия, 117198

В статье автор акцентирует внимание на непрямых формах противоборства между государствами, уделяя особое внимание информационным войнам. В статье рассматривается проблема интерпретации термина «информационная война», приводится классификация войн четырех поколений (4GW) и ее анализ, рассматривается определение и сущность явления нетрадиционной войны (UW). Автор проводит анализ отечественных и зарубежных подходов к определению новых форм конфликтов в информационном пространстве.

Ключевые слова: информационный конфликт, информационная война, информационное противоборство, войны четвертого поколения, нетрадиционная война, гибридная война, сетевая война.

Первые 15 лет XXI в. охарактеризованы крупными геополитическими изменениями и появлением новых угроз, что, несомненно, затронуло и нашу страну. Повышение военно-политической напряженности между Россией и НАТО, конфликты на Ближнем и Среднем Востоке, обострение ценностных противоречий между исламским миром и христианским Западом – все это создает реальные предпосылки для возникновения нового цивилизационного конфликта. Многие философы и политологи говорят о том, что новая глобальная война уже идет¹. Она не объявлялась официально, и скрыта от

¹ См. Зиновьев А.А. «Война нового типа»; Дугин А.Г.; Коровин В.М. «Сетевые войны» и др.

взгляда рядовых граждан, но ведет человечество к глубоким изменениям в сфере расстановки сил на мировой арене.

Феномен описываемой скрытой войны стал возможен лишь в условиях развития современных технологий. Анализ мирового опыта показывает, что сегодня прямая агрессия перестала быть единственным средством доминирования. В связи с этим современная наука постепенно сосредотачивается на изучении непрямых форм противоборства, уделяя особое внимание информационным войнам.

Сам термин «информационная война» в настоящее время носит больше публицистический характер и еще не получил повсеместного признания. Об этом свидетельствуют непрекращающиеся дискуссии по поводу того, что на самом деле скрывается под этим понятием, а также споры по поводу корректности и практической применимости данного термина к той сфере социальных отношений, которую принято называть информационным противоборством или конфликтом интересов в информационной сфере социальных систем. Таким образом, отдельной научной проблемой является разработка и согласование научно-терминологического аппарата.

В отечественной и зарубежной науке существует множество различных и часто взаимоисключающих подходов к определению конфликтов, протекающих в современном информационном пространстве. Такое разнообразие и несогласованность является серьезным препятствием на пути к разработке теории информационных войн.

Самое емкое понятие «информационный конфликт» означает столкновение противоположно направленных целей и интересов (как одной из форм конфликта), позиций и мнений в информационном пространстве, осуществляемое с помощью информационных технологий. Участниками информационного конфликта могут стать субъекты, обладающие доступом к источникам и средствам распространения информации.

Специалисты МИД России под конфликтом в современном информационном пространстве понимают «противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальных систем, а также массивной психологической обработки населения с целью дестабилизации общества и государства» [9. С. 36].

Информационные войны являются разновидностью информационного конфликта. Часто в качестве синонима используется понятие «информационное противоборство». Однако, исследуя опыт наших западных коллег, мы пришли к выводу, что приравнивание информационного противоборства к информационным войнам некорректно. Вопросами теории и практики информационных конфликтов довольно продолжительное время занимаются, главным образом, американские ученые. Многие понятия переводятся на русский и берут-

ся нашими исследователями за основу в своих разработках, поэтому нам приходится отталкиваться от понятий, предложенных изначально в США.

Во второй половине XX в. появляется понятие «Information Warfare». В 1976 г. его впервые употребил ученый-физик Томас Рон в своем докладе, посвященном вооруженным силам. Официально этот термин был использован в директиве Министерства Обороны США от 21 декабря 1992 г. MODODD 3600 [3]. В нашей стране возникла проблема с переводом, откуда позже возникло несовпадение интерпретаций.

Изначально information warfare стали переводить именно как «информационная война», подразумевая под собой агрессивные действия в информационном пространстве. Таким образом, ссылаясь на американских специалистов, используя термин «противоборство» вместо термина «война», мы считаем некорректным (как, например, это сделано в работах Воронцовой Л.В. и Фролова Д.Б.¹, Пашенцева Е.Н.²).

Термин «Information Warfare» был также использован корпорацией RAND в исследованиях 1996–1998 гг.³ В указанных работах «warfare» – это агрессивные действия, направленные против гражданского и военного населения, а также органов власти противника с целью дестабилизировать внутреннюю социально-политическую ситуацию и подчинить воле субъекта.

На наш взгляд, информационное противоборство представляет собой борьбу против кого-либо, чего-либо или сопротивление кому-либо, чему-либо в информационном пространстве с помощью информационных средств. Термин «противоборство» носит скорее морально-психологический, а не военный характер. Словари приводят следующий ряд его синонимов: «конкуренция», «дуэль», «поединок», «состязание», «противодействие», «сопротивление», «отбор», «соперничество», «единоборство»⁴. В информационной сфере – это конфликт низкой интенсивности, который может продолжаться неопределенно долго.

Для информационного противоборства характерно латентное протекание конфликта (жертва может даже не подозревать, что против нее ведется информационная борьба), при этом используются неагрессивные методы воздействия.

Таким образом, противоборство в информационной сфере не является синонимом информационной войны. Скорее это понятие, которое может до-

¹ См. Воронцова Л.В., Фролов Д.Б. История и современность информационного противоборства (2006г.).

² См. Пашенцев Е.Н. Президенты под медиаприцелом: практика информационного противоборства в Латинской Америке (2014).

³ См. доклады MR-661-OSD "Strategic Information Warfare. A new face of War" (1996 г.), MR-963-OSD "The Day After ... in the American Strategic Infrastructure" (1998 г.) и MR-964-OSD, "Strategic Information Warfare Rising" (1998 г.).

⁴ См. Словарь синонимов и антонимов современного русского языка под ред. Гавриловой А.С. (2013); Словарь синонимов русского языка под ред. Александровой З.Е. (2003).

полнить и развить существующие теоретические знания в сфере информационных конфликтов.

Война сама по себе – это организованная вооруженная борьба между государствами, нациями (народами), социальными группами, целью которой является достижение политических целей. Синонимы этого слова: «борьба», «столкновение», «поход», «кампания», «нашествие», «блокада», «бомбардировка». Следовательно, информационная война – это организованная борьба в информационной сфере, которая носит агрессивный и интенсивный характер. Для войн в информационном пространстве характерно использование таких агрессивных технологий, как масштабные информационные кампании, очерняющие PR-акции, пропаганда и так далее.

Таким образом, мы склоняемся к точке зрения, согласно которой информационная война и информационное противоборство представляют собой два вида конфликтов в информационной сфере, противоположных по степени интенсивности.

Еще одно понятие, которое все чаще используется в научной дискуссии, но в некоторых случаях ошибочно трактуется – это «войны четвертого поколения».

Специалистами RAND Corporation была разработана классификация войн четырех поколений:

- 1) войны первого поколения с применением линейной тактики;
- 2) войны второго поколения, которые носили в основном позиционный характер;
- 3) войны третьего поколения, их иначе называют маневренной войной;
- 4) войны четвертого поколения (4GW), когда главная цель – морально подчинить противника [4. С. 49].

В основе зарождения концепции 4GW лежат, главным образом, политические, социальные и моральные мотивы, а также общее снижение влияния государства. Однако их цель неизменна – подчинение противника собственной воле.

Войны четвертого поколения включают в себя стратегические информационные войны второго поколения. Они представляют собой принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящей в круг возможных сфер противоборства информационное пространство и ряд других областей (экономику, культуру и т.д.). Эти войны предусматривают уже иной подход: создание атмосферы бездуховности и безнравственности, манипулирование общественным сознанием и политической ориентацией населения страны; дезинформацию граждан о работе государственных органов, подрыв их авторитета, дискредитацию органов власти противника и т.д.

В основу определения 4GW положен тезис о том, что к этому поколению относятся все формы конфликта, в которых одна из сторон не желает или не может использовать традиционные (симметричные) средства и методы, де-

лая ставку на нетрадиционные асимметричные средства. В этой связи эксперты отмечают, что все то, что ранее попадало под определения «терроризма», «партизанской борьбы» и другого, сегодня является составными элементами 4GW¹.

Характерной чертой стратегии 4GW является активное использование негосударственных и невоенных субъектов. Чаще всего это оппозиционные силы данной страны, НПО и НКО.

Войны четвертого поколения стирают грань между гражданским лицом и кадровым военным. При этом война никогда не объявляется, между противниками внешне могут быть даже вполне дружеские отношения. Государство-агрессор рекрутирует, вооружает, обучает и финансирует оппозиционный негосударственный субъект. Совместно они планируют подрывные операции, как с применением оружия (революции), так и без его применения (акции, пикеты, информационные атаки). Данным субъектам оказывается широкая медийная поддержка. Доцент МГИМО А.А. Костюхин отмечает: войны четвертого поколения, в сущности, «являются развитием концепции повстанческой войны» [8].

После отработки 4GW на практике (в Югославии, Египте, Тунисе и других странах) данный феномен с точки зрения технологий в публицистике будет назван «цветными революциями». С точки зрения теории практики 4GW брали за основу теорию «управляемого хаоса». Таким образом, 4GW – это война эффектов: тот, кто сможет просчитать эффекты более высоких порядков, тот сможет подчинить себе противника.

Стратегия 4GW опирается на фундаментальный принцип: правильно примененная сильная политическая воля может оказаться выше экономической и военной мощи. Наряду с физическим насилием или вместо него целью ставится подавить политическую волю противника.

Старший научный сотрудник Института управления РАН С.Н. Бухарин считает, что основой информационных войн второго поколения является финансовый ресурс. Бухарин в своей работе «Умная оборона, или “Карфаген должен быть разрушен”» пишет: «К информационным войнам второго поколения относятся так называемые “цветные революции”, их механизмы достаточно хорошо известны. Данные войны ведутся в квазистационарных условиях, то есть тогда, когда условия обстановки изменяются медленно. В таких войнах побеждает тот, кто превосходит противника в финансовых ресурсах» [1]. Он выделяет также информационные войны третьего поколения, которые определяет как интеллектуальные. «В XXI веке для решения геополитических проблем нет необходимости прибегать к оружию, провоцировать военные конфликты, прибегать к военной агрессии. Все можно решить в рамках информационного противоборства (войны)» [1].

¹ См. Otis P. Religion in information operations: more than a «war of ideas» (2009); Fulford C.W., Jr. Countering ideological support for extremism: challenges and implications (2006).

Но напомним, что стратегическая информационная война и информационная война второго и третьего поколения Бухарина – это лишь составляющая 4GW. Ведь 4GW – это стратегия войны в прямом смысле этого слова, которая предполагает применение различного оружия, военной тактики, разрушения объектов военной и гражданской инфраструктуры и массовую гибель людей, хотя и не отрицается, что информационная и психологическая составляющие играют здесь весомую роль.

В связи с этим американские эксперты пишут о 4GW следующее: «Противостоящие стороны в войне четвертого поколения станут настолько искусными в манипулировании средствами массовой информации с целью изменения общественного мнения в стране и в мире, что умелое применение психологических операций иногда сможет сделать излишним ввод в действие боевых подразделений» [14. Р. 16]. Иногда излишним, но не отменяющим и не всегда. Таким образом, войны четвертого поколения – это самостоятельный вид борьбы, который может включать в себя элементы информационных войн.

В отечественной науке часто допускается приравнивание информационных войн к американской концепции нетрадиционных войн – Unconventional Warfare (UW).

Концепция UW подразумевает, что иррегулярный противник действует не самостоятельно, а при непосредственной негласной поддержке со стороны третьих стран или организаций (НКО, НПО, частные армии, корпорации и т.д.). Иными словами, некое государство или организация финансирует вооруженное формирование, обучает его бойцов, поставляет оружие и боеприпасы, оказывает политическую поддержку и помогает ему иными способами. Данная концепция применялась на практике при смене власти в Ираке, Сирии и Ливии. Нетрадиционной войне в этих странах предшествовала информационная война, в которой позже стали появляться элементы «управляемого хаоса». Далее нетрадиционная война сопровождалась информационными атаками в целях скрыть от мировой общественности сам факт войны, участвующие стороны и их истинные цели. Но мы не можем поставить знак равенства между информационной войной и войной нетрадиционной.

Часто используемым, в том числе в отечественной науке и публичном пространстве, синонимом нетрадиционным войнам являются «гибридные войны». А.В. Манойло дает такое определение: «Гибридная война – широкий диапазон действий, осуществляемых противником с использованием военных и иррегулярных формирований с одновременным привлечением гражданских компонентов» [5. С. 51]. Генеральный директор Центра стратегических оценок и прогнозов С.Н. Гриняев определяет гибридную войну как форму военных действий с вовлечением в конфликт разнородных по составу, средствам, уровню и характеру подготовки силам [4. С. 56]. Гибридная война на практике представляет собой то, что произошло в Ливии и Сирии: использование технологий информационной войны, подготовка повстанцев,

цветные революции, непосредственное военное вторжение и еще множество технологий.

Помимо войн четвертого поколения и нетрадиционных войн встречается еще ряд терминов, неоправданно подменяющих понятие информационной войны. Например, «консциентальная и сетевая война». В середине 90-х гг. XX в. доктор психологических наук Ю.В. Громько изучил и описал новый вид межгосударственного социального конфликта, психологического по форме, цивилизационного по содержанию и информационного по средствам – консциентальные войны. Конечной целью таких конфликтов является целенаправленное изменение национального сознания, которое направлено на вырождение такого базового национального инстинкта, как «либидо» («воля к жизни») и стимуляцию противоположного ему – «мортидо» («воли к смерти») [11. С. 71]. Это очень долгий, поэтапный процесс, его результаты могут проявиться спустя достаточное количество времени или даже через поколения. Выражаются подобные изменения, как правило, в демографическом спаде, дестабилизации ситуации в государстве по причине раскола внутри общества или разногласий между властью и народом.

В США в отношении современных конфликтов также прорабатывается теория сетевых войн. Многие специалисты утверждают, что общество движется в сторону осетевления¹. Причиной этому послужило появление сетевых коммуникаций, которые имеют высокую плотность путей перемещения информации, что делает их почти неуязвимыми. Если какое-то звено выпадает из сети, то коммуникация способна найти другие пути распространения информации. Характерной чертой сети является ее ячеистая структура с высокой частотой повторяемости, что позволяет охватить большее пространство. Общество подстраивается под сетевые коммуникации.

В начале 2000-х гг. концепция сетевой войны трансформировалась в теорию сетецентрической войны (авторы – А. Цебровски, Дж. Гарстка) [13]. Если сетевую войну американские эксперты определяют как социально-политические инновации снизу, к которым относят революции, национально-освободительные движения и так далее, то сетецентричная война представляет собой «военно-техническую революцию сверху» [9. С. 3].

Сетевая война, какой ее видят ученые, вряд ли является самостоятельным видом войны. Скорее это форма, которую принимают современные информационные, информационно-психологические войны, а порой и прямые военные действия. Сеть отвечает на вопрос, как, каким образом наш противник будет осуществлять деструктивное и подчиняющее воздействие? Сеть – это не оружие, сеть – это средство, это базовая технология.

Примерами сетей являются террористические организации, созданные при поддержке американских спецслужб – «Аль-Каида» и «Талибан». Сформи-

¹ См. Курочкин А.В., Журавлева Т.А. «Сети в политике – Политика в сетях» (2014); Филь М.С. «Социальные сети. Новые технологии управления миром» (2016).

рованные для борьбы с СССР, сегодня эти сети обернулись против своих создателей – Соединенных Штатов Америки – и влились в новую общемировую угрозу в лице террористов ИГИЛ. Их структуры формировались по лекалам «мозговых центров» в соответствии с принципами построения сетей. Управленческая парадигма была гибкой, ячейки действовали почти автономно, сетевая структура позволила с легкостью приспосабливаться к меняющейся общественно-политической обстановке.

Таким образом, терроризм – полностью сетевое по своей форме явление. В 1986 г. в ходе доклада «Терроризм и СМИ» Дж. Буш произнес: «Терроризм – форма пропаганды, нуждающаяся в паблисити, чтобы быть эффективной» [7. С. 24], то есть сетевые войны предполагают применение и элементов информационной войны.

В работах наших исследователей термин «сетевые войны» не имеет конкретной детерминации. Например, сетевая война – это совокупность действий, направленных на формирование модели поведения друзей, нейтральных сил и врагов в ситуации мира, кризиса и войны [2. С. 6]. Дается и такое определение: сетевая война – создание децентрализованной сети «информационно оснащенных бойцов», способных обеспечить решительную бескровную победу путем направленного уничтожения ключевых «нервных центров» – систем управления противника [2. С. 7].

Таким образом, в отечественной науке пока нет единого мнения о природе и сущности сетевых форм конфликта.

Разобравшись в многообразии терминов, определяющих формы конфликтов в информационном пространстве или его затрагивающих, постараемся вывести наиболее полное определение понятия «информационная война».

В более широком смысле под этим словосочетанием можно понимать ведение действий против технических информационных систем и современных информационных технологий, а также социальных систем путем оказания информационных воздействий с помощью информационных систем и технологий, методов дезинформации и пропаганды [9. С. 170].

Признаки информационной войны:

- деятельность с целью нанесения ущерба государственным интересам;
- тайные информационно-психологические операции как организационная форма такой деятельности;
- применение информационного оружия.

Стоит признать, что в информационном обществе информационная война является неотъемлемой составляющей политических отношений и основным инструментом политического принуждения и достижения политических целей. Войны такого типа являются тем фактором, который может в значительной степени изменить направленность геополитических процессов и отношений в современном обществе и привести к смещению геополитических центров притяжения национальных интересов субъектов геополитической конкуренции (например, появление новых глобальных и региональных полити-

ческих лидеров и формирование международных коалиций вокруг них). Последствия акций и ударов информационной войны могут изменить саму структуру информационного пространства (в частности, маршруты следования потоков и положение узлов притяжения информационных потоков, а также приоритет и монополию в разработке и внедрении передовых информационных и коммуникационных технологий одних субъектов геополитической конкуренции относительно других), а также к отчуждению (экономическому, культурному, юридическому отделению) части территории государства и перераспределению других видов стратегически важных ресурсов [11. С. 160].

Автор определяет информационную войну как острую стадию информационного противоборства или самостоятельный информационный конфликт, который содержит в себе открытые и скрытые целенаправленные информационные воздействия социальных систем друг на друга с целью получения некоего выигрыша в политической сфере. В зависимости от того, какой сегмент подвергается атаке, каким образом и с какими целями, информационные войны подразделяются на информационно-психологические и информационно-технические.

Информационно-техническая война (или кибервойна) предполагает воздействие на информационную инфраструктуру противника (системы и средства связи, базы данных, операции против компьютерных и информационных систем и т.д.).

Стоит отметить, что сегодня мир, а особенно его экономическая и военная составляющие, настолько зависимы от ИКТ, что угроза тотальной кибервойны становится как никогда реальной. К примеру, 1 октября 2009 г. было создано новое подразделение Министерства обороны США – Кибернетическое командование, его главной задачей является использование информационных технологий и Интернета в качестве оружия. Подобные подразделения уже существуют в России, Китае и ряде других стран [6. С. 9].

Учитывая все вышесказанное, мы определяем информационно-психологические войны как информационный конфликт, для которого характерны процессы комплексного воздействия на сознание и подсознание отдельных людей, социальных групп или общества в целом посредством информации через средства массовой коммуникации с целью навязать противнику необходимую точку зрения, разрушить национальное самосознание и духовно подчинить.

К. Мангейм в своих исследованиях называл политический конфликт рационализированной формой борьбы за социальное господство [10]. Информационно-психологические войны мы можем назвать рационализированным средством политической борьбы за геополитическое господство через подчинение социальных систем в информационном пространстве. Здесь важно понимать, что при отсутствии прямого столкновения противоборствующие стороны стараются подчинить противника изнутри, подчинив ментально его народ и направив против существующей политической системы.

В заключение отметим, что сегодня наука насчитывает большое количество терминов, описывающих современные тенденции в развитии информационных конфликтов. Между ними красной нитью проходит сходство, которое обычно и вводит в заблуждение специалистов: все эти виды войн основаны на новейших информационных технологиях и активно их используют в качестве орудия борьбы, при этом они протекают латентно. Отметим необходимость согласовать отечественный и зарубежный терминологический аппарат, чтобы в дальнейшем иметь возможность адекватно оценить угрозы и средства противодействия им.

ЛИТЕРАТУРА

- [1] *Бухарин С.Н.* Умная оборона, или «Карфаген должен быть разрушен». URL: <http://avkrasn.ru/article-918.html>.
- [2] *Григорьев В.Р.* Информационные вирусы – новое оружие массового поражения // Информационные войны. Московская область: Юбилейный. № 3. 2008.
- [3] *Гриняев С.Н.* Информационная война: история, день сегодняшний и перспектива. URL: <http://www.infwar.ru/article.php?num=41>.
- [4] *Гриняев С.Н., Арзуманян Р.В., Карп Е.И.* Военное противоборство в современных условиях: новейший опыт, оценки, тенденции / Под общ. ред. А.Б. Михайловского. М.: АНО ЦСОиП, 2014.
- [5] *Евгеньева Т.В.* Психология управления массовым политическим сознанием и поведением: уч.-метод. пособие / Т.В. Евгеньева, А.В. Селезнева, А.В. Манойло. М.: Издательство «Известия», 2015.
- [6] *Кларк Р., Нейк Р.* Третья мировая война: какой она будет? СПб.: Питер, 2011.
- [7] *Кононов Д.А., Кульба В.В., Косяченко С.А., Цыганов В.В., Чернов И.В.* Средства и объекты информационного управления. // Информационные войны. Московская область: Юбилейный, 2009.
- [8] *Костюхин А.А.* Современная американская классификация войн. URL: <http://mir-politika.ru/2783-sovremennaya-amerikanskaya-klassifikaciya-voyn.html>.
- [9] *Макаров В.Е.* Политические и социальные аспекты информационной безопасности. Монография. Таганрог: Изд-ль С.А. Ступин, 2015.
- [10] *Мангейм К.* Идеология и утопия. URL: http://socialistica.lenin.ru/txt/m/manheim_1.htm.
- [11] *Савин Л.В.* Сетевая война. Введение в концепцию. М.: Евразийское движение, 2011.
- [12] *Сергеев Н.А.* Архитектура перспективной сетевцентрической информационно-управляющей системы обеспечения национальной безопасности России в новых геополитических условиях // Информационные войны. Московская область: Юбилейный. № 2. 2010.
- [13] *Cebrowski A.K., Garstka J.J.* Network – Centric Warfare: Its Origin and Future // Proceedings. 1998. January.
- [14] *Terriff T., Karp A., Karp R.* Global Insurgency and the Future of Armed Conflict. Debating fourth-generation warfare. Routledge, New York, 2008.

REFERENCES

- [1] *Buharin S.N.* Umnaja oborona ili «Karfagen dolzhen byt' razrushen». URL: <http://avkrasn.ru/article-918.html>.

- [2] *Grigor'ev V.R.* Informacionnye virusy – novoe oruzhie massovogo porazhenija // Informacionnye vojny. Moskovskaja oblast': Jubilejnyj. № 3. 2008.
- [3] *Grinjaev S.N.* Informacionnaja vojna: istorija, den' segodnjashnij i perspektiva. URL: <http://www.infwar.ru/article.php?num=41>.
- [4] *Grinjaev S.N., Arzumanjan R.V., Karp E.I.* Voennoe protivoborstvo v sovremennyh uslovijah: novejsnij opyt, ocenki, tendencii / Pod obshh. red. A.B. Mihajlovskogo. M.: ANO CSOiP, 2014.
- [5] *Evgen'eva T.V.* Psihologija upravljenija massovym politicheskim soznaniem i povedeniem: uch.-metod. posobie / T.V. Evgen'eva, A.V. Selezneva, A.V. Manojlo. M.: Izdatel'stvo «Izvestija», 2015.
- [6] *Klark R., Nejk R.* Tret'ja mirovaja vojna: kakoj ona budet? SPb: Piter, 2011.
- [7] *Kononov D.A., Kul'ba V.V., Kosjachenko S.A., Cyganov V.V., Chernov I.V.* Sredstva i obekty informacionnogo upravljenija // Informacionnye vojny. Moskovskaja ob-last': Jubilejnyj, 2009.
- [8] *Kostjuhin A.A.* Sovremennaja amerikanskaja klassifikacija vojn. URL: <http://mir-politika.ru/2783-sovremennaya-amerikanskaya-klassifikaciya-voyn.html>.
- [9] *Makarov V.E.* Politicheskie i social'nye aspekty informacionnoj bezopasnosti. Monografija. Taganrog: Izd-l' S.A. Stupin, 2015.
- [10] *Mangejm K.* Ideologija i utopija. URL: http://socialistica.lenin.ru/txt/m/manheim_1.htm.
- [11] *Savin L.V.* Setecentrichnaja i setevaja vojna. Vvedenie v koncepciju. M.: Evrazijskoe dvizhenie, 2011.
- [12] *Sergeev N.A.* Arhitektura perspektivnoj setecentricheskoj informacionno-upravljajushhej sistemy obespechenija nacional'noj bezopasnosti Rossii v novyh geo-politicheskikh uslovijah // Informacionnye vojny. Moskovskaja oblast': Jubilejnyj. № 2. 2010.
- [13] *Cebrowski A.K., Garstka J.J.* Network – Centric Warfare: Its Origin and Future // Proceedings. 1998. January.
- [14] *Terriff T., Karp A., Karp R.* Global Insurgency and the Future of Armed Conflict. Debating fourth-generation warfare. Routledge, New York, 2008.

INFORMATION WAR: THE PROBLEM OF THEORETICAL INTERPRETATION

Alexandra V. Borchsenius

Department of Public Administration
Peoples' Friendship University of Russia
Miklukho-Maklaya st., 10–2, Moscow, Russia, 117198

In the article author focuses on indirect forms of confrontation between states, paying particular attention to the information wars. Author considers the problem of interpretation of the term “information war”, provides a classification of four generations of wars (4GW) and its analysis, discusses the definition and essence of the phenomenon of unconventional war (UW). Author analyzes domestic and foreign approaches to the definition of new forms of conflicts in the information space.

Key words: information conflict, information warfare, information confrontation, war of fourth generation, non-traditional war, hybrid war, network war.