ГЛОБАЛЬНЫЙ НАДНАЦИОНАЛЬНЫЙ АКТОР МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ И ЕГО СОЦИАЛЬНАЯ ФИЛОСОФИЯ

И.В. Сурма

Дипломатическая академия Министерства иностранных дел Российской Федерации.

В статье показано, что продолжающаяся технологическая и контентная революция в средствах массовой коммуникации по ряду основных показателей усложняет взаимодействия участников международных отношений, а «информационный пресс» приобретает в современных международных отношениях приоритетное значение, что дает все основания отнести информацию к разряду факторов, определяющих коренные социальные перемены в современном мире. Возможности современного информационного общества не всегда поддаются точному прогнозу, управляющему действию политиков и международных организаций. Интернет-пространство постепенно становится главным актором в международных отношениях, а одним из крайне неприятных аспектов этого процесса является утрата информационным обществом устойчивости. Эти и другие обстоятельства диктуют необходимость выработки адекватной эффективной государственной политики противодействия кибертерроризму и разработки новой «интеллектуальной технологии» и программных инструментов для контроля «темного веба» и анализа социальных сетей. Социальная стабильность государств будет во все большей степени зависеть от правильного использования информации именно там, где она более всего необходима в данный политический момент. В статье показано, что информационное обеспечение внешней политики и международных отношений по своему значению стоит в одном ряду с такими приоритетными проблемами мировой политики, как нераспространение ядерного оружия, ограничение и запрещение оружия массового поражения, урегулирование региональных конфликтов и миротворчество, укрепление всеобъемлющей безопасности, сохранение культурного наследия и обеспечение прав человека.

Ключевые слова: геополитика, кибертерроризм, социальные сети, интернет-пространство, «арабская весна», sotialbots, кибератаки.

Современные процессы информатизации общества приводят к изменению структуры и технологии власти, перераспределения влияния в пользу тех, кто управляет информационными потоками и ресурсами. «Информационный пресс» приобретает в современных международных отношениях приоритетное значение, что дает все основания отнести информацию к разряду факторов, определяющих коренные социальные перемены в современном мире. С другой стороны, возможности современного информационного общества не всегда поддаются точному прогнозу, управляющему действию политиков и международных организаций. Это приводит к тому, что интернет-пространство постепенно становится главным актором в международных отношениях, а одним из крайне неприятных аспектов этого процесса является утрата информационным обществом устойчивости.

Одним из наиболее активных сегментов глобальной сети является российская зона Интернета, иначе говоря «Рунет». В последние дни в печати и в экспертной среде активно обсуждаются тезисы только что обнародованного исследования российского Фонда развития гражданского общества «Рунет сегодня». Вот некоторые данные из этого исследования, опубликованные в центральной прессе. Наше государство начинает лидировать в Европе по количеству интернет-пользователей. Всего за несколько последних лет количество пользователей «Рунета» возросло в два раза, достигнув 52,9 млн человек, то есть это 46% населения страны в возрасте старше 18 лет. При этом кроме роста количества пользователей произошла общая интенсификация обращения к Интернету. Еще сильнее увеличилась еженедельная и ежедневная аудитория, в начале 2011 г. это было 42 и 33% соответственно. А в начале 2012 г. ежедневная аудитория уже достигала 38% от населения страны.

Растет число пользователей (из тех, кто начал пользоваться сетью за последние полтора-два года), не являющихся жителями Москвы и Петербурга. Таковых сейчас более 93%. Средний возраст российского интернет-пользователя, по данным ФОМ, составляет 33 года. Наши граждане все больше начинают воспринимать Интернет как авторитетный канал доступа к информации. По данным Synovate Comcon, доверие к Интернету как источнику получения информации признали у нас в 2011 г. 40% граждан. Данные ВЦИОМ немного отличаются: 98% россиян предпочитают получать информацию из центрального ТВ, 88% – из регионального ТВ. На втором месте –пресса (центральную прессу читают 70% россиян, местную прессу – 68%), на третьем месте – Интернет (59%), оказавшийся более востребованным, чем радио (центральное – 53%, региональное – 46%). Наибольшее доверие у респондентов вызывает информация, поступающая по центральному и региональному ТВ (по 78%). На втором месте по уровню доверия – центральная и местная пресса (70 и 68%). Замыкают список радио (как центральное, так и местное – 72 и 68%) и Интернет (64% опрошенных).

Из приведенных выше цифр авторы исследования «Рунет сегодня» делают вывод: если доверие российских граждан к Интернету как основному источнику информации продолжит расти, то выборы депутатов Государственной Думы ФС РФ в 2016 г. и тем более президентские выборы в 2018 г. пройдут в новой информационной реальности. В ней главная роль будет принадлежать Всемирной сети [1].

Авторы доклада, рассматривая различные категории популярных ресурсов: медийные порталы, поисковые системы, социальные сети, новостные сайты, блогосферу, коммерческие сервисы и некоторые другие, характеризуют последние тенденции, набирающие силу в российском интернет-пространстве, и приходят к выводу, что социальные сети по популярности сравнимы с поисковыми системами. Другая тенденция связана с тем, что «к настоящему моменту пять из двадцати лидеров Рунета по объему среднедневной аудитории являются не российскими по своему происхождению (Google, Youtube, Wikipedia, Facebook, Twitter). При сохранении данной тенденции уже через несколько лет может сложиться ситуация, когда большая часть Рунета будет контролироваться иностранными сервисами, расположенными на серверах за пределами России и зарегистрированными в зарубежных доменных зонах»[1].

В исследовании отмечается, что многочисленные фонды и корпорации США активно инвестируют в лидирующие российские интернет-компании, таким образом, 15 из 20 российских топовых сайтов имеют значительную долю иностранного капитала, которая к тому же показывает тенденцию к росту. Например, Mail.ru Group (контролирует Mail.ru, «Одноклассники», крупный пакет «ВКонтакте»), в структуре которого южноафриканский холдинг Naspers владеет 29% акций, китайский Tencent – 7,8% и еще 30% акций находится в руках владельцев GDR, размещенных на британской бирже LSE. «Похожая ситуация наблюдается и в «Яндексе», подчеркивается в исследовании[2].

С другой стороны, некоторые российские популярные ресурсы вышли из российской юрисдикции, тот же «Яндекс» официально зарегистрирован в Нидерландах, а «ВКонтакте» с российского домена Vkontakte.ru перешел на международный домен Vk.com. В докладе акцентируется внимание на том, что такие глобальные социальные сервисы, как Facebook, Twitter, YouTube, используются как координационный инструмент для мобилизации оппозиционных сил в ситуации политической нестабильности. Не вызывает сомнения, что в ноябре 2011 г. – марте 2012 г. и в российском сетевом пространстве также были задействованы те же сетевые технологии, которые были «обкатаны» в событиях «арабской весны». Речь идет, в частности, о мобилизации людей на противоправительственные акции через массовую рассылку в социальных сетях, об интенсивной скупке развлекательных сообществ с целью превращения их в протестно-политические, о распространении политического спама и т.п.

Все события «арабской весны» являются типичным примером того, как неустойчивая со-

циально-политическая и общая экономическая ситуация в государстве может привести к серьезным фундаментальным изменениям во властных структурах. Важность прогнозирования подобной нестабильности и ее предотвращение или ослабление являются важной задачей для разведывательного сообщества и вооруженных сил, прежде всего Соединенных Штатов и их союзников. В последнее время и в Соединенных Штатах активно развиваются научно-исследовательские и опытно-конструкторские работы в области создания и усовершенствования автоматизированных систем прогнозирования подобных кризисных ситуаций. При этом весьма повышенное внимание уделяется анали-зу, мониторингу, моделированию и прогнозированию взаимоотношений людей, прежде всего, в социально-культурной сфере. Особое значение принимают работы с информацией из открытых источников, такие, как мониторинг социальных медиа-технологий (блогосфер, социальных сетей и т. п.) и оказания через них активного влияния на целевую аудиторию. Недавно опубликованные материалы Агентства перспективных исследований и разработок министерства обороны США (DARPA) [2], Управления передовых исследований в разведывательной области аппарата директора Национальной разведки (IARPA) [3] и ФБР США только подтверждают этот факт. Экспертами Пентагона в 2011 г. было проведено исследование, одним из результатов которого явился обзор существующих в США систем прогнозирования и раннего предупреждения о конфликтах и нестабильности (прежде всего политической, экономической, социальной и др.) [4].

Среди исследовательских проектов и действующих автоматизированных систем с возможностями прогнозирования назревания кризисных ситуаций были выделены следующие:

–«Модель национальной оперативной среды» (National Operational Environment Model (NOEM));

– исследовательский проект «Прогнозирование и анализ комплексных угроз- III» (FACT III);

– проект «Глобальная сеть» (GlobalNet Project);

– система «Сентурион» (Senturion) разработки компании Sentia Group;

– объединенная система раннего предупреждения о кризисах ICEWS;

– программа Human Social Culture Behavior Modeling (HSCB);

– программа Social Media in Strategic Communication (SMISC), стартовавшая в июле 2011 г. в агентстве DARPA, и инструмент анализа социальных сетей и динамики мнений (Social Networks and Opinion Dynamics Analysis (SNODA) tool).

Вызвал интерес и проект управления IARPA, начатый в августе 2011 г. в рамках программы Open Source Indicators (OSI), связанный с поиском методов для осуществления непрерывного автоматизированного анализа открытых источников информации. Используемые методы призваны заранее обнаруживать важные и критичные социальные события с помощью анализа ранних индикаторов из многочисленных общественно доступных источников данных, таких, как: поисковые веб-запросы, блоги и микроблоги, интернет-трафик, веб-камеры отслеживания транспортных потоков, редакторские правки в Википедии и многие другие. При этом в настоящее время ощущается существенный недостаток в таких методах, которые позволяют выявлять неожиданные события на основе анализа открытых источников информации. Федеральное бюро расследований (Strategic Information and Operations Center (SIOC)) в январе 2012 г. объявило о поиске готовых к практическому использованию прикладных средств для анализа и предупреждения о возможных угрозах национальной безопасности США на базе изучения как открытых источников информации (например, Fox News, CNN, MSNBC и т.п.), так и социальных медиа (Twitter, Facebook и др.).

Международные эксперты отмечают, что разведывательные агентства осуществляют регулярный мониторинг социальных сетей уже в течение нескольких лет [5]. На самом деле получение разнообразной информации из социальных сетей рассматривается в разведсообществе США как важный и необходимый элемент повседневной деятельности [6]. Специфическая роль социальных сетей в процессах, происходящих в 2011 г. в странах Ближнего Востока и Северной Африки, заставила аналитиков по новому взглянуть на возможности использования данного явления. И прежде всего была существенно ускорена разработка программных средств, имеющих отношение к добыче информации в социальных сетях.

Эффективность использования социальных сетей в качестве источника разведывательной информации подтверждают и спецслужбы Израиля, в недрах которых было сформировано подразделение (social media unit), функционирующее в инфомедийном пространстве и предназначенное для контроля разнообразных социальных сетей, и прежде всего в арабском мире. По линии МИД Израиля на работу с социальными сетями в 2010 г. было выделено около 2 млн долл., а в августе 2011 г. в Брюсселе для 60 сотрудников израильских посольств, работающих в Европе, были организованы специальные курсы для более активного участия во взаимодействии с социальными сетями [7].

Наибольший объем разведы¬вательной информации из социальных сетей в США добывается Государственным департаментом, Центром открытых источников ЦРУ (CIA's Open Source Center (OSC))[8] и Министерством внутренней безопасности (подразделение Social Networking/ Media Capability Unit). В ЦРУ ежесуточно скачивается до 5 млн сообщений из Twitter[9]. Материалы, подготавливаемые на основе этих сообщений, помогают формировать информационные сводки, которые докладываются прежде всего сотрудникам администрации Белого дома и попадают в текст ежедневных посланий президенту США (President's Daily Brief).

Собственно, министерство обороны США рассматривает сайты Facebook и Twitter не только как информационные источники, но и в качестве

оружия в современных и будущих конфликтах[10]. Пентагон разрабатывает наступательные методики в сочетании с разведывательным аспектом контроля информации в социальных сетях. Главным образом эти методики предназначены для оказания влияния на аудиторию социальных сетей и реализуются в рамках концепции создания специальных программных сетевых продуктов (Socialbots). Это программные продукты, которые формируют в социальных сетях тысячи фиктивных «личностей» (fictitious socially networked profiles), находящихся под централизованным контролем, и которые способны в онлайн-режиме поддерживать различные интенсивные тематические диалоги с сетевым сообществом.

Возвращаясь к «Рунет сегодня», можно отметить, что Фонд развития гражданского общества в докладе обращает внимание на вероятность того, что в ближайшие несколько лет Google сможет значительно упрочить свои позиции на российском рынке. И это происходит одновременно с ослаблением позиции медийных порталов из-за наступления социальных сетей и сервисов. В настоящий момент очевидно, что единственным серьезным медийным порталом в отечественном Интернете остался Mail.ru, но и он испытывает сильное конкурентное давление со стороны мировых почтовых сервисов Google (Gmail) и Apple (Me.com).

«Системообразующие элементы информационного пространства представляют собой новостные агрегаторы, но достаточно часто бывают случаи, когда представленные на них материалы «носят необъективный характер, а пользователям зачастую предлагается преимущественно политически ангажированный контент»[1].

Авторы доклада неслучайно особенно акцентировали внимание на социальных сетях, поскольку абсолютное большинство пользователей основное свое время в Интернете проводят именно там. В настоящее время «ВКонтакте» почти в 8 раз опережает Facebook по посещаемости и сохраняет свое доминирующее положение на российском рынке, однако тот факт, что сеть «ВКонтакте» слабо поддается контролю, ресурс «ВКонтакте» также представляет определенную угрозу информационной безопасности», – говорится в исследовании.

Как в мировом, так и в российском интернет-пространстве уже давно существуют профессиональные блогеры, чьи «живые журналы» и по размеру, и по содержанию, и по количеству посетителей приближаются по своему характеру к крупным сетевым СМИ. Авторы блогов принимают участие в различных информационных кампаниях, в том числе политического характера, и при этом не ограничены никакими рамками. Многие из них делают все для того, чтобы заработать определенный политический и финансовый капитал на своих журналах.

Самостоятельными острыми информационными поводами все чаще становятся видеозаписи, размещенные на сервисе YouTube, который практически является монопольным видеохостингом. Эти видеозаписи вызывают широкий резонанс в обществе вообще и в социальных сетях в частности. При этом администрация YouTube зачастую ведет весьма спорную политику модерирования контента и нередко принимает достаточно спорные решения, что заставляет усомниться в ее нейтральности.

На основании вышеприведенного анализа в докладе Фонда развития гражданского общества «Рунет сегодня» делаются следующие выводы:

– «в России стремительно растет не только число интернет-пользователей, но и повышается интенсивность использования сети;

– за последние четыре года изменился демографический состав Рунета. В настоящее время средний возраст пользователя составляет 33 года, а его демографические характеристики близки к средним по России в целом;

– в отличие от традиционных медиа, стремительно растет уровень доверия к информации из Интернета. В ближайшие годы сеть станет основным источником получения информации для граждан страны;

– четверть из двадцати наиболее популярных сайтов Рунета являются глобальными (американскими) сервисами, и их доля растет на протяжении всех последних лет;

– произошла консолидация рынка интернет-поиска, который поделен между «Яндексом» и Google. Американская поисковая система продолжает активную экспансию на российский рынок;

– снижается роль крупных медийных порталов. Mail.ru рискует повторить судьбу «Рамблера», который ранее уже потерял большую часть своей аудитории;

– новостные агрегаторы продолжают оказывать воздействие на информационную картину Рунета и зачастую оказывают негативное информационное влияние;

– почти все активные пользователи Рунета зарегистрированы в социальных сетях, которые занимают более половины от общего времени, проводимого в сети;

– массовые пользователи перестают вести классические блоги, уходя в Twitter и социальные сети, однако «большие» блоги профессионализируются, конкурируя по качеству, уникальности контента и размеру аудитории с интернет-СМИ;

– YouTube занял монопольное положение среди видеохостингов в Рунете. При этом политика сервиса в части модерирования контента вызывает сомнения в его политической нейтральности;

– существенно изменилась система распространения информации в сети. Важную роль в формировании «информационных волн» стал играть Twitter. Видеохостинги и блоги потеснили традиционные и интернет-СМИ в качестве площадок публикации контента;

– снижается роль электронной почты как средства коммуникации. Она становится «интернет-паспортом» пользователей, необходимым для регистрации в других ресурсах;

– Skype занимает доминирующее положение в Рунете в качестве интернет-мессенджера, выдавливая с рынка ICQ, QIP и «Mail.ru Агент»;

– Internet Explorer лишился доминирующего положения на рынке интернет-браузеров, уступив Google Chrome, Apple Safari, Mozilla Firefox и Opera;

– браузеры оказывают большое влияние на смежные сегменты рынка, в частности на рынок интернет-поиска. При этом роль браузеров в ближайшее время будет расти, а их функционал усложняться;

– мобильный доступ в Интернет растет в России опережающими темпами. Планшеты и смартфоны в ближайшие годы станут столь же распространенными инструментами для доступа в сеть, как и персональные компьютеры»[1].

Из-за возрастания роли информации в современном социуме малые группы могут оказывать существенное влияние практически на неограниченное количество людей. Именно это подталкивает правительства разных стран к активному формированию национальной информационной политики, совершенствованию национальной информационной инфраструктуры, защите и обеспечению безопасности информационных систем, международном обмене информацией и создании правительственных компьютерных систем.

Продолжающаяся технологическая и контентная революция в средствах массовой коммуникации по ряду основных показателей усложняет взаимодействие участников международных отношений, а интенсивное развитие интернет-технологий открывает новые возможности для выработки согласованной политики по преодолению политико-социальных и экономических кризисов и мер по их недопущению.

Несмотря на это, Интернет в своем современном состоянии способен выступать потенциальным провокатором различных кризисных ситуаций, а также может усиливать их. Информационно-коммуникационная инфраструктура государства – это прежде всего стратегический ресурс, который требует постоянного контроля и внимания. Любые действия деструктивного характера в информационной среде могут иметь серьезнейшие последствия для управляемых сетей и систем, вследствие чего информационные сети сегодня выступают как средства информационной борьбы в среде публичной политики, религиозных организаций, предпринимателей и бизнесменов, различных преступных группировок и групп террористов. Социально-политические последствия научно-технического прогресса часто находятся в противоречии с интересами пользователей Интернета, подвергающихся различного рода кибератакам.

Первым успешным опытом глобального применения возможностей социальных сетей в ходе политических кампаний были выборы президента США Барака Обамы в 2008 г. Значительную роль в том, что он тогда одержал победу, сыграли рассылки сообщений на сотовые телефоны, через социальные сети, электронную почту. Таким образом, создавалось ощущение, что кандидат в президенты общается с каждым своим избирателем непосредственно. Технологии массовой рассылки в социальных сетях использовались в ходе событий в арабском мире, названных «арабской весной». Очевидно, что эти технологии будут использоваться и в дальнейшем.

Все это свидетельствует о том, что в современную эпоху изменился характер войн, и мы присутствуем при зарождении войн нового типа, которые можно назвать информационно-сетевыми войнами. Эти войны нового типа обусловлены несколькими основными факторами:

– развитием коммуникационных технологий;

– возникновением глобальной коммуникационной сети Интернет;

– совершенствованием технологий психологического воздействия на общество.

Очевидно, что комплексное применение всех этих факторов способно оказать разрушительное воздействие на государственные устои, при этом такого результата можно достичь, не прибегая к непосредственному военному вмешательству или экономическому давлению, а только воздействуя на морально-психологические установки населения и руководства страны. Информационное воздействие на противника всегда играло существенную роль в силовом противостоянии между государствами или заинтересованными общественными группами, и манипулирование общественным мнением зародилось далеко не сейчас. С его помощью осуществляется расширение политического влияния, поскольку появляется возможность воздействовать на умонастроения масс и манипулировать поведениям больших групп населения.

Элиты осознают, что, контролируя средства массовой информации, можно влиять на развитие и ход общественных процессов. Можно сказать, что новейшие политтехнологи, направленные на разрушение государств, переносят агрессию из военно-территориального пространства в информационно-сетевое. В нем объектом «нападения» становится общественное самосознание, национальная и культурная идентичность, а средством нападения – дискредитация и уничтожение традиционных ценностей нации. Существенной особенностью такой информационной войны является то, что информационная агрессия не воспринимается массовым сознанием как агрессия, а воспринимается как принятие новых прогрессивных и современных установок. Точно так же, как «движение на пути к прогрессу», может воспринимать подобное информационное вторжение и национальная элита, поэтому она не оказывает ему сопротивления, а, напротив, становится еще одним ретранслятором информационной агрессии. Именно эта особенность данного вида вторжения, когда те, кто подвергаются нападения, воспринимают его не как агрессию, а как благо, и является основной «поражающей силой» современных информационных войн.

Перед лицом агрессора жертва оказывается беззащитной и не в состоянии оказать ему своевременное и адекватное сопротивление. Последствия информационных войн практически необратимы. Мы знаем примеры, когда результаты традиционных войн подвергаются ревизии, взять для примера хотя бы итоги последних мировых войн. Но в том случае, когда оказалась поверженной не только

военная машина государства, но и реформирована духовная основа побежденной нации, то происходит необратимое изменение самосознания нации в соответствии с установками победителя.

Актор-агрессор использует в информационно-сетевой войне различные общественные структуры:

– во-первых, это средства массовой информации;

– во-вторых, это различные общественные движения, религиозные организации, культурные и образовательные структуры, неправительственные фонды и т.д.

Все вместе они осуществляют массовое разрушающие воздействия на общественную систему страны, действуя под прикрытием лозунгов о соблюдении прав человека, развития подлинной демократий и гражданского общества. Информационно-сетевая атака характеризуется также отсутствием жесткой иерархии в информационно-сетевых структурах, что вызвано гетерогенностью коммуникационных сетей с их автономными объектами, не связанными в какую-то определенную вертикальную иерархию, но обладающими огромными горизонтальными связями, что используется современными военными и секретными службами для осуществления информационного воздействия на противника.

Уже отмечалось, что в США разрабатывается программа, которая позволит создавать онлайн-персонажей для «распространения проамериканской пропаганды» через Twitter, Facebook и другие подобные сервисы, о чем сообщает The Guardian (Великобритания). Пункт управления этой деятельностью расположится на базе ВВС США «Макдилл» близ Тампы (Флорида) и будет функционировать в круглосуточном режиме. В программе будет задействовано до 50 операторов, каждый из которых сможет контролировать до 10 фиктивных юзеров, так называемых «марионеток», зарегистрированных в различных странах мира. Предполагается, что каждая онлайн-персона будет снабжена убедительной «легендой». Предусмотрена изощренная система защиты от разоблачения. По словам Билла Спикса, пресс-секретаря Центрального командования ВС США, поскольку воздействовать на американскую аудиторию запрещено американским законодательством, то система будет задействована в работе на арабском, фарси, урду, пушту и других языках, но не на английском.

«Предполагается, что данная инициатива является частью операции «Искренний голос» (OEV), первоначально разработанной для ведения психологической борьбы с сетевой деятельностью сторонников «Аль-Каиды» и других сил против войск коалиции в Ираке. Генерал Джен Маттис, руководитель Центрального командования ВС США, которое выступило заказчиком ПО, заявил: «OEV создана для того, чтобы подорвать механизм вербовки и подготовки террористов-смертников; лишить наших противников прибежища, а также для борьбы с экстремистской идеологией и пропагандой». Центральное командование подтвердило, что контракт стоимостью 2,76 млн долл. достался недавно зарегистрированной в Лос-Анджелесе компании Ntrepid»[11].

Целью информационной агрессии, как и в традиционной войне, является установление политического и экономического господства путем поддержки сепаратистских и террористических кругов, провокации «массовых волнений», организации хакерских атак на государственные и военные информационные системы, распространения компьютерных вирусов и т.д. Свежий пример на эту тему связан с обострением нынешнего палестино-израильского конфликта. По сообщению Reuters, правительственные сайты Израиля подверглись более чем 44 млн кибератак с начала военной операции против палестинских боевиков. Эти атаки были направлены против интернет-ресурсов, связанных с системой обороны Израиля, против официальных сайтов премьер-министра, президента и министерства иностранных дел страны. Кибератаки проводились с территории разных стран, но преимущественно из Израиля и Палестины.

Следует отметить, что израильская армия в этом конфликте применила новую доктрину ведения кибернетической войны, в которой, помимо прочего, учитывается массовое появление у населения современной электронной техники и увлечение израильтян социальными сетями. Неожиданно возникла проблема, которая до этого вообще ускользнула из поля зрения заинтересованных структур. Многие израильтяне уже давно используют смартфоны (или цифровые фотоаппараты с GPS) для быстрой публикации фотографий в Интернете. При этом они зачастую не принимают во внимание тот факт, что при такой публикации фотографии в сети рядом с ней может появляться карта с точным указанием места съемки.

«В случае если речь идет о съемках в местах падения ракет, данная информация может быть использована противником для коррекции огня. Военная цензура требует от СМИ не указывать точное место падения ракет и некоторую другую информацию, которая может быть использована противником. Блогерам и любителям размещать фотографии и видеозаписи в Интернете следует также считаться с требованиями цензуры. Владельцам смартфонов и цифровых фотоаппаратов, публикующим снимки в социальных сетях, необходимо ознакомиться с руководством пользователя и обратить внимание на функцию удаления информации о месте съемок».

Вернемся к методам ведения информационных войн. Исследователи выделяют достаточно широкий спектр методов, которые используются в информационном противостоянии. Это в первую очередь откровенная дезинформация, когда общественность намеренно вводится в заблуждение. Это сокрытие существенно значимой информации или ее погружение в массив малозначимой информации, где она теряется среди новостного мусора. Это превалирование негативной информации над позитивной для создания соответствующего психологического фона. Это использование недостоверных или методологически некорректных социологических

опросов и рейтингов в качестве аргументов. Это подмена понятий или использование так называемых сетевых «мемов» для искажения подлинного смысла.

Можно дополнить материал о том, как манипулируют информацией в интернет-пространстве анекдотичным, но показательным примером. Министерство связи и массовых коммуникаций России опровергло на своем сайте сообщения об обязательной регистрации популярных интернет-ресурсов как СМИ. Информация, опубликованная сайтом поддельных новостей FogNews, разошлась днем 25 сентября по нескольким русскоязычным медиапорталам. «Новость» о поправках в закон о СМИ, которые якобы внес министр связи Николай Никифоров, появилась на сайте FogNews 22 сентября. В новости сообщается, что государство после ухода Дмитрия Медведева с поста президента начало «закручивать гайки во всех социальных сферах» и решило «взять под контроль непокорных блогеров».

Согласно придуманным FogNews поправкам к закону о СМИ, все блоги с посещаемостью свыше тысячи человек обязаны регистрироваться как полноценные СМИ. 26 сентября новость со ссылкой на FogNews появилась на сайте петербургского издания «Лениздат», а также на сайте Гильдии издателей периодической печати и на портале «Новый репортер». Министерство связи официально заявило: «В ответ на появившиеся в СМИ сообщения о том, что на рассмотрение Государственной Думы якобы внесен проект поправки в закон «О средствах массовой информации», по которой интернет-издания с посещаемостью свыше 1000 человек, будут обязаны регистрироваться как СМИ, пресс-служба Минкомсвязи России сообщает, что министерство с подобными инициативами не выступало и выступать не намерено. Такие предложения на обсуждение не выносились».

А неофициально было предложено «господам журналистам» «внимательнее относиться к перепечатке информации с сайтов, которые официально действуют как источники полностью выдуманных новостей». Проверка источников, как говорилось в заявлении министерства, избавит журналистов от «необходимости краснеть за распространение ерунды». Но очевидно, что это ерунда не так уж и безобидна. В данном контексте необходимо также упомянуть о так называемых «информационных минах» и «информационных бомбах», используемых для неконтролируемого роста протестного настроения в социуме.

Ярким примером отработки технологии информационных войн являются события последних лет на Ближнем Востоке и в Северной Африке – в Тунисе, Египте, Ливии, Сирии. Можно сказать, что эти события разворачивались в режиме онлайн, ретранслируемые на весь мир посредством Youtube, Facebook и Twitter. При этом те же сервисы (плюс электронная почта и мобильные телефоны) послужили и для провокации волнений, и они же использовались как для мобилизации «активистов», так и для организации массовых уличных акций. Все это безошибочно работало в накаленной атмосфере, сложившейся в арабском мире. Однако это не сработало в российских условиях, хотя сценарий «раскрутки» революционного маховика осенью прошлого года был написан его авторами по тем же лекалам. Как уже говорилось выше, серверы основных сетевых популярных сервисов (Twitter, Facebook, Yahoo и др.) располагаются на территории США и полностью подконтрольны соответствующим местным разведывательным структурам, что потенциально дает им возможность по своему сценарию «запускать» лавинообразное возбуждение в социальных сетях и вообще в киберпространстве противника. Отключение мобильной связи и блокирование доступа в Интернет, после того как информационная бомба взорвалась и массовая рассылка провокативных сообщений была произведена, уже не может спасти положение.

Современный мир становится все более нестабильным. Очаги социальной, экономической, политической нестабильности из традиционных «неблагополучных» регионов, таких, как Ближный Восток или Юго-Восточная Азия, перемещаются в ранее благополучные регионы, в том числе и в Европу. Это связано, несомненно, с процессами тотальной глобализации, с миграционными процессами, с всеобщим экономическим кризисом. Появляется все больше люмпенизированных групп населения, обозленных на окружающий их «несправедливый» мир. Именно такие люди становятся «бойцами» всяческих радикальных движений в любых странах и в любой момент готовы выплеснуть на улицы свой протест. Ярким примером такого протеста был акт самосожжения молодого человека в Тунисе, которое было ретранслировано в средствах массовой информации и социальных сетях едва ли не с провокационной целью, что в общем-то и послужило «спусковым крючком» тунисской революции. Как справедливо заметил в своей статье В.В. Карякин, это были:

– «прямые» репортажи, снятые на камеры сотовых телефонов неизвестно кем и неизвестно где;

– сообщения о многочисленных жертвах;

– репортажи из якобы захваченных повстанцами городов;

– беспорядочная стрельба перед телекамерами СМИ;

– слухи о «переходе» на сторону повстанцев сына Каддафи;

– бегство ливийских дипломатов в США и Францию.

Однако если внимательно присмотреться, то видно, что в СМИ разыгрывается виртуальная война, смонтированная и отретушированная на компьютерах и вброшенная в виртуальное пространство для обоснования санкций Совета Безопасности ООН и последующей интервенции сил НАТО. Если Тунис и Египет были первыми пробами заокеанских режиссеров этого псевдореволюционного спектакля, то Ливия была первой реальной боевой операцией мировой информационно-сетевой войны Запада против неугодного режима. Это типичный пример реализации информационно-сетевой стратегии «управляемого хаоса»,

которая оказалась новым и весьма эффективным средством сохранения американского глобального лидерства»[12].

Роль и значение исследования так называемых проблем кибертерроризма, научной обоснованности мер их разрешения резко возрастают в условиях усложнения социальной структуры и политической жизни общества, падения доверия к политическим институтам, неэффективности некоторых механизмов влияния на общество. Эти и другие обстоятельства диктуют необходимость выработки адекватной эффективной государственной политики противодействия кибертерроризму и разработки новой «интеллектуальной технологии» и программных инструментов для контроля «темного веба» и анализа социальных сетей. Поэтому, как уже отмечалось ранее, в июле 2011 г. агентство DARPA объявило о начале работ в рамках программы SMISC (Social Media in Strategic Communication). Следует отметить технологии компании i2 (Великобритания – США), которые помогают автоматизировать аналитическую деятельность, применяя визуализацию объектов анализа и обеспечивая поиск скры¬тых закономерностей и связей между ними.

Также заслуживают внимания визуальная аналитическая среда Starlight и системы безопасности BFT-ONE, к развертыванию которых в ряде стран, наиболее опасных в террористическом отношении, приступило Бюро дипломатической безопасности Госдепартамента США (Bureau of Diplomatic Security (DS)). В первую очередь системы мониторинга BFT-ONE вводятся в Ираке, Пакистане, Афганистане и Йемене. Госдепартамент уже использовал в Ираке систему BFT главным образом для контроля за действиями сотрудников охраны американского диппредставительства и передвижениями автомобилей дипломатов высшего ранга. Эксперты Госдепартамента США считают, что системы безопасности BFT-ONE придадут сотрудникам зарубежных представительств больше уверенности, особенно при передвижении по опасным районам, поскольку те будут знать, что за ними осуществляется постоянное наблюдение, а также имеется возможность оперативного реагирования на сигналы о помощи.

Возвращаясь к докладу Фонда развития гражданского общества «Рунет сегодня» и на основании вышеприведенного обзора глобальных процессов, спровоцированных с применением интернет-технологий, можно сделать некоторые выводы и дать определенные рекомендации. Нужно принять действенные меры для восстановления суверенитета России над этими общественными информационно-социальными институтами. Нужно принять государственную программу развития Рунета, поскольку социальные сети, электронные средства массовой информации, телевидение и реакция на них «улицы» будут в ближайшее время главными факторами общественно-политической жизни страны. Важно не потерять суверенитета России в области духовных и нравственных ценностей, в сфере национального самосознания. Например, в средствах массовой коммуникации, и на телевидение в частности, контент практически десуверенизирован. Множество программ является кальками с американских или европейских аналогов и соответственно ретранслируют ту систему ценностей, которая входит в диссонанс с ценностями большинства российского населения.

Однако бессмысленно пытаться побудить, например, популярную социальную сеть «ВКонтакте» переходить под российскую юрисдикцию. В первую очередь необходимо развивать те сервисы, которые пока еще находятся под российской юрисдикцией в рамках общей политики перевода российской экономической собственности в российскую юрисдикцию. К сожалению, необходимость этой политики еще не достаточно осознана, и, как известно, многие наши структурообразующие корпорации владеют активами через офшоры.

В какой-то степени повлиять на сложившееся положение вещей смогли бы такие отечественные проекты, которые станут для пользователей более привлекательны, чем иностранные интернет-сервисы. При этом еще дополнительным негативным фактором является то, что наши законодатели усугубляют экономические проблемы российских интернет-проектов, в частности запретив рекламу алкоголя в Интернете и лишив таким образом российские площадки крупного источника дохода. В то время как западные сетевые русскоязычные ресурсы спокойно размещают такую рекламу. Естественно, основные рекламные контракты уходят туда, что увеличивает и так излишнее иностранное влияние.

В работе иностранных интернет-сервисов в России есть момент, связанный с тем, что наше государство лишено, как уже было сказано, возможности полноценного контроля за основными каналами распространения информации. До сих пор не выработано полноценного механизма взаимодействия с крупными иностранными социальными сервисами, хотя практика недавно принятого закона о защите детей от вредного контента показывает, что такое взаимодействие может быть достигнуто. По словам одного из разработчиков данного закона, депутата ГД РФ Елены Мизулиной: «Такой популярный сайт, как YouTube, принадлежит американской компании, не нашей, но даже на нем был наведен порядок еще до вступления в силу закона. Мы наблюдаем, как Google убирает противоправный контент, как только приходит уведомление, без всяких споров. Более того, Google, которой, собственно, и принадлежит популярный видеохостинг YouTube, обратилась в Роскомнадзор и сообщила специально созданный адрес электронной почты, по которому она будет получать уведомления о включении тех или иных интернет-страниц на хостингах Google в реестр запрещенных сайтов».

Примечателен китайский опыт. Доступ к иностранным сайтам изнутри материкового Китая ограничивается правительством Китая в целях цензуры. Веб-страницы фильтруются по ключевым словам, связанные с государственной безопасностью, а также по «черному списку» адресов сайтов. Иностранные поисковые машины, работающие в Китае, включая Google, Yahoo и Microsoft (поиск

Live Search), согласились аналогичным образом фильтровать результаты поиска. Сайты, расположенные в самом Китае, проходят регистрацию в министерстве промышленности и информационных технологий (кит.), что позволяет выявить автора незаконного содержимого. При этом Китай, запретив иностранные интернет-ресурсы, успешно развивает свои как информационные, так и коммерческие интернет-площадки. Особое внимание китайские власти уделяют контролю крупнейшей национальной платформы социальных сетей Weibo. Самым внимательным образом отслеживались силовыми ведомствами КНР последние события «арабской весны» 2011 г. и активная роль социальных сетей.

Принимая во внимание накопленный опыт, был подготовлен ряд важных решений, которые, по мнению властей Китая, должны способствовать стабилизации ситуации в блогосфере. С конца 2011 г. китайских пользователей Интернета уже стали постепенно обязывать записываться под своими настоящими именами при открытии блогов, в больших социальных сетях, базирующихся в Пекине, Шанхае, провинции Гуандун, недавно ставших очагами социальных волнений в стране [13]. А начиная с 16 марта 2012 г. в социальных сетях Китая вводится запрет анонимности, то есть теперь китайские пользователи социальных сетей должны отказаться от псевдонимов и применять свои подлинные имена. В случае несоблюдения этого правила пользователям, как минимум, будет запрещено размещать или пересылать сообщения.

Другой пример. США недавно ввели односторонние санкции (традиционный запрет на въезд и замораживание счетов) против нескольких должностных лиц Ирана, в том числе против министра связи и информационных технологий Реза Тагипур, а также некоторых чиновников министерства культуры и исламской ориентации и подчиненного ему совета по надзору за прессой. В «черный список» попали и другие «ключевые физические лица и организации, несущие ответственность за применение «цензуры в отношении иранского народа», нарушение «свободы слова и собраний», «ограничение доступа к печатным средствам массовой информации, телевидению и радио, в том числе посредством глушения спутникового сигнала из-за рубежа на Иран». Таким образом США среагировали на блокировку Ираном сервисов Google, включая Gmail. Иранское руководство пошло на это, чтобы исключить просмотр на YouTube оскорбительной для мусульман американского фильма «Невинность мусульман», вызвавшего бурные протесты жителей всех исламских стран, в том числе и Ирана. Служащий государственного агентства по интернет-цензуре и борьбе с компьютерными преступлениями Абдолсамада Хорамабади заявил, что требование блокировки сайта и почтового сервиса исходило не от власти, а от простых иранцев, возмущенных распространяемым в сети американского фильма. Этот пример наглядно демонстрирует, что борьба «за умы» в киберпространстве переходит уже из сферы виртуальной в плоскость реальных политических и дипломатических шагов.

Вернувшись к проблемам Рунета, стоит отметить, что и в нашем обществе Facebook, Twitter и мировой видеохостинг-монополист YouTube становятся центральными инструментами координации и мобилизации оппозиционных сил. Одной из причин такого явления стало то, что протестные силы фактически были изолированы от традиционных СМИ. Оппозиционных деятелей не слишком часто приглашали на федеральное телевидение, например, и они ушли в более свободные зоны, которыми, собственно, стали социальные сервисы в Интернете. Именно из-за этого в первую очередь возникла ситуация, когда долгое время оппозиция была создателем информационных трендов в блогосфере. В последнее время положение несколько меняется, власть стала уделять больше внимания Интернету, социальным сетям.

Очевидно, что меры по противодействию экстремизму лежат в плоскости создания адекватного законодательства. Сейчас уже приняты некоторые законы, направленные на осуществление более плотного контроля над различной противоправной информацией, которая распространяется в сети. Например, уже упомянутый закон, связанный с защитой детей от вредной информации. Можно дискутировать о его отдельных положениях, но закон этот был нужен и он начал работать. Важно отработать механизм взаимодействия государства с крупнейшими интернет-сервисами для контроля над распространением противоправного контента. Этот алгоритм сегодня еще не достаточно разработан. При этом не стоит забывать о том, что одними административными мерами проблему экспансии западных сервисов в Рунете не решить. Причины экспансии западных сетевых ресурсов на просторы Рунета кроются в более высоком качестве предоставляемых ими услуг.

Надо сказать, что некоторые шаги для защиты российского интернет-пространства уже сделаны. Так, 26 сентября в верхней палате парламента состоялось заседание комиссии по развитию информационного общества, где шла речь о создании стратегии кибербезопасности России. «По словам инициатора встречи сенатора Руслана Гаттарова, в России впервые будет реализован принцип, когда в создании столь важного документа смогут принять участие сразу все заинтересованные стороны. На встречу были приглашены как представители ведущих компаний, работающих на рынке интернет-безопасности (Лаборатория Касперского и другие), так и представители ФСБ, МВД, Минкомсвязи, Администрации Президента РФ. Угроза кибертерроризма стоит во всем мире достаточно остро, ведущие страны мира принимают концепции национальной безопасности в интернет-сфере, в том числе и чтобы защитить госсектор. Подобные документы подготовлены в США, Китае, Великобритании и других странах. В России также озаботились этой проблемой. В результате будет написана и впоследствии реализована концепция госполитики в области обеспечения кибербезопасности».

Так же есть планы относительно создания Советом Федерации в начале 2013 г. собственного кру-

глосуточного телеканала для вещания в Интернете. Инициатором создания телеканала, который носит рабочее название "Вместе-РФ", стала Председатель Совета Федерации Валентина Матвиенко. В планах канала – ведение прямых трансляций заседаний сенаторов, а также информация о жизни регионов России. Не менее 10 процентов эфира отдадут под познавательный контент: зрителей ждут программы о науке, культуре, истории парламентаризма, экологии. Также на канале будут транслироваться художественные и документальные фильмы, подкрепляющие идею объединения россиян.

«Такой проект, несомненно, повысит авторитет Совета Федерации, его открытость в обществе, а также создаст единое информационное региональное пространство», – заявляла В. Матвиенко. Основная студия телеканала разместится в здании Совета Федерации на Дмитровке. Там будет сооружен полноценный павильон с декорациями и светом. Планируется создание и региональных студий в других городах. Кандидатура на пост главного редактора телеканала уже подобрана, но его имя будет объявлено только после регистрации нового СМИ в Роскомнадзоре. Пока не решен вопрос с финансированием проекта. Ранее Минфин отказал В. Матвиенко в выделении 265,2 млн руб. на развитие канала в 2013–2015 гг. В министерстве главе Совфеда посоветовали использовать для вещания бесплатные видеохостинги, например YouTube.

Социальная стабильность государств будет во все большей степени зависеть от правильного использования информации именно там, где она более всего необходима в данный политический момент. В этом контексте проблема информации в современном мире многоаспектна: ее можно анализировать как глобальную, оказывающую универсальное влияние на тенденции политического, социально-экономического, научно-технического и культурного развития мирового сообщества. Таким образом, информационное обеспечение внешней политики и международных отношений по своему значению стоит в одном ряду с такими приоритетными проблемами мировой политики, как нераспространение ядерного оружия, ограничение и запрещение оружия массового поражения, урегулирование региональных конфликтов и миротворчество, укрепление всеобъемлющей безопасности, сохранение культурного наследия и обеспечение прав человека.

Список литературы

1. Доклад «Рунет сегодня: исследование российского Интернета» // См. URL: http://www.civilfund.ru/mat/view/1 (дата обращения::: 30.09.2012).
2. Defense Advanced Research Projects Agency (DARPA) - Social Media in Strategic Communication (SMISC): Broad Agency Announce¬ment, DARPA-BAA-11.64. 2011. July 14. См. URL: http://cryptome.org/dodi/dod-smisc.pdf (дата обращения: 07.11.2012)
3. Intelligence Advanced Research Projects Activity (IARPA). Open Source Indicators (OSI) Program: Broad Agency Announcement, IARPA-BAA-11-11. Of¬fice of Incisive Analysis. Release Date: 2011, August 23. См. URL: http://goodtimesweb.org/surveillance/IARPA-BAA-11-11_20110823.pdf (дата обращения 07.11.2012)
4. Environmental Change and Fragile States — Early Warning Needs, Opportu-nities & Intervention : AEPI Report. Army Environmental Policy Institute. 2011. September 21 См. URL: http://www.aepi.army.mil/docs/whatsnew/MAN0BC2_report_combined_compressed.pdf (дата обращения: 21.11.2012).
5. Stokes J. EFF's new lawsuit, and how the NSA is into social networking // Ars Technica. URL: http://arstechnica.com/tech-policy/2009/07/effs-new-lawsuit-and-how-the-nsa-is-into-social-networking/
6. Parascandola R. NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem // The New York Daily News. 2011. August 10. URL: http://www.nydailynews.com
7. Israeli diplomats train on Twitter PR // Israel News. 2011, August 29. http://www.ynetnews.com/articles/0,7340,L-4114989,00.html
8. Mayfield T.D. A Commander's Strategy for Social Media // Joint Forces Quarterly. 2011.
9. CIA Analysts Comb Social Media for Trouble Spots. The Associated Press. 2011. November 4. URL: http://grapevinestar.com/media/blog/2011/11/23/cia-analysts-comb-social-media-for-trouble-spots/
10. Streitfeld D. Pentagon Seeks a Few Good Social Networkers // The New York Times. 2011. August 2. – URL: http://bits.falogs.nytiraes.com
11. Nick Fielding and Ian Cobain, Revealed: US spy operation that manipulates social media. The Guardian, Thursday 17 March 2011 // - URL: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks (дата обращения 29.10.2012)
12. Карякин В.В., Наступила эпоха следующего поколения войн – информационно-сетевых. Независимая газета, 22.04.2011// URL: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html?mpril (дата обращения: 03.11.2012)
13. La Chine met fin a l'anonymat sur ses reseaux de microblogging // La Liberation. 12.02.2012. – URL: http://fc\news.yahoo.com

Об авторе

Сурма Иван Викторович – к.э.н., доцент кафедры государственного управления и национальной безопасности Дипломатической академии МИД России, член экспертного совета Комитета по финансовому рынку Государственной думы РФ. E-mail: vsurma@gmail.com

GLOBAL SUPRANATIONAL ACTORS OF INTERNATIONAL RELATIONS AND SOCIAL PHILOSOPHY

I.V. Surma

Moscow State Institute of International Relations (University), 76, Prospect Vernadskogo, Moscow, 119454, Russia.

Abstract: *In article it is shown, that the continued technological and content revolution in the means of mass communication in a number of key indicators complicates the interaction of the participants of international relations, and «information of the press» is of special importance in the modern international relations is the priority, which gives all grounds to attribute the information to the category of factors that determine the fundamental social change in the modern world. Possibilities of modern information society is not always amenable to precise forecast, the action of politicians and international organizations. The Internet space is gradually becoming the main actor in international relations, and one of the most unpleasant aspects of this process is the loss of the information society sustainability. These and other circumstances dictate the need to generate adequate effective state policy of counteraction to cyber terrorism and the development of the new «intellectual technologies» and software tools to control the «dark-web» and analysis of social networks. Social stability of the States will increasingly depend on the correct use of information where it is needed most in this political moment. In article it is shown that the information support of foreign policy and international relations of the stands in one row with such priority issues of world policy as non-proliferation of nuclear weapons, restriction and prohibition of weapons of mass destruction, settlement of regional conflicts and peace-making, strengthening of comprehensive security, the preservation of cultural heritage and promotion of human rights.*

Key words: geopolitics, cyber terrorism, social networks, the Internet-space, the Arab spring, Socialbots, cyber attacks.

References

1. Report "Runet Today: A Study on the Russian Internet". Available at: http://www.civilfund.ru/mat/view/1. Accessed September 30, 2012. (in Russ.).
2. Defense Advanced Research Projects Agency (DARPA). Social Media in Strategic Communication (SMISC). Broad Agency Announcement, DARPA-BAA-11.64. July 14, 2011. Available at: http://cryptome.org/dodi/dod-smisc.pdf. Accessed November 07, 2012.
3. Intelligence Advanced Research Projects Activity (IARPA). Open Source Indicators (OSI) Program. Broad Agency Announcement, IARPA-BAA-11-11. Office of Incisive Analysis. August 23, 2011. Available at: http://goodtimesweb.org/surveillance/IARPA-BAA-11-11_20110823.pdf. Accessed November 07, 2012.
4. Environmental Change and Fragile States – Early Warning Needs, Opportunities & Intervention. AEPI Report. Army Environmental Policy Institute. September 21, 2011. Available at: http://www.aepi.army.mil/docs/whatsnew/MAN0BC2_report_combined_compressed.pdf. Accessed November 21, 2012.
5. Stokes J. EFF's new lawsuit, and how the NSA is into social networking. Ars Technica, July 24, 2009. Available at: http://arstechnica.com/tech-policy/2009/07/effs-new-lawsuit-and-how-the-nsa-is-into-social-networking/.
6. Parascandola R. NYPD Forms New Social Media Unit to Mine Facebook and Twitter for Mayhem. The New York Daily News, August 10, 2011. Available at: http://www.nydailynews.com.
7. Israeli diplomats train on Twitter PR. Israel News, August 29, 2011. Available at: http://www.ynetnews.com/articles/0,7340,L-4114989,00.html.
8. Mayfield T.D. A Commander's Strategy for Social Media. Joint Forces Quarterly, 2011, no. 60, pp. 79-84.
9. CIA Analysts Comb Social Media for Trouble Spots. The Associated Press, November 4, 2011. Available at: http:// http://grapevinestar.com/media/blog/2011/11/23/cia-analysts-comb-social-media-for-trouble-spots/
10. Streitfeld D. Pentagon Seeks a Few Good Social Networkers. The New York Times, August 2, 2011. Available at: http://bits.falogs.nytiraes.com.
11. Fielding N., Cobain I. Revealed: US spy operation that manipulates social media. The Guardian, March 17, 2011. Available at: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks. Accessed October 29, 2012.
12. Kariakin V.V. The Onset of the New Epoch of Wars – Information Network Wars. Nezavisimaia gazeta [Independent Newspaper], April 22, 2011. Available at: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html?mpril. Accessed November 03, 2012. (in Russ.).
13. La Chine met fin a l'anonymat sur ses reseaux de microblogging [China puts an end to the anonymity in the microblogging network]. La Liberation, February 12, 2012. Available at: http://fc\news.yahoo.com

About the author

Ivan V. Surma– PhD in Economics, associate professor of the Department of State Governance and Security at the Diplomatic Academy at the Ministry of Foreign Affairs of Russia, Member of the Expert Committee on the Financial Market of the Russian State Duma. E-mail: vsurma@gmail.com