10.7256/2073-8560.2013.01.7

§ 6 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

И.В. Сурма

НОВЫЙ ГЛОБАЛЬНЫЙ НАДНАЦИОНАЛЬНЫЙ АКТОР МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Аннотация: *Современные процессы информатизации общества приводят к изменению структуры и технологии власти, перераспределения влияния в пользу тех, кто управляет информационными потоками и ресурсами. 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. Роль и значение исследования 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 «тёмного веба» и анализа социальных сетей. 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.*

Ключевые слова: *Политология, Социальные сети, Интернет-пространство, Кибератаки, Socialbots, SMISC, BFT-ONE, Интернет-СМИ, Арабская весна, Кибертерроризм*

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

10.7256/2073-8560.2013.01.7

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 года это было 42% и 33% соответственно. А в начале 2012 года 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. Таких 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[1], доверие к Интернету как источнику получения информации признали у нас в 2011 году 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 вышеприведенных цифр авторы исследования «Рунет сегодня» делают вывод, что если доверие российских граждан к Интернету, как основному источнику информации, продолжит расти, то выборы Депутатов Государственной Думы ФС РФ в 2016 году и, тем более президентские выборы в 2018 году, пройдут в новой информационной реальности, где главная роль будет принадлежать всемирной Сети[2].

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»[3].

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[4].

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.

Необходимо акцентировать внимание на том, что такие глобальные социальные сервисы, как

[1] Компания Synovate Comcon является частью международной исследовательской сети Ipsos, входящей в тройку лидеров на мировом рынке. Компания Synovate Comcon специализируется, помимо общих маркетинговых исследований, на медиаисследованиях. См. – URL: http://www.comcon-2.ru/ (дата обращения 10.10.2012)

[2] Доклад «Рунет сегодня: исследование российского Интернета» // См. – URL: http://www.civilfund.ru/mat/view/1 (дата доступа 30.09.2012).

[3] Там же.

[4] Там же.

10.7256/2073-8560.2013.01.7

Facebook, Twitter, YouTube используются как координационный инструмент для мобилизации оппозиционных сил в ситуации политической нестабильности. Не вызывает сомнения, что в ноябре 2011 года – марте 2012 года 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 социально-политическая и общая экономическая ситуация в государстве может привести к серьезным фундаментальным изменениям во властных структурах. Важность прогнозирования подобных такой нестабильности и их предотвращение или ослабление являются важной задачей для разведывательного сообщества и вооруженных сил, прежде всего Соединенных Штатов и их союзников[5]. В последнее время, в том числе 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 анализу, 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)[6], Управления передовых исследований в разведывательной области аппарата директора Национальной разведки (IARPA)[7] и ФБР[8] США только подтверждают этот факт. Экспертами Пентагона в 2011 году 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.)[9]. 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))[10], исследовательский проект «Прогнозирование и анализ комплексных угроз — III» (FACT III)[11], проект «Глобальная сеть» (GlobalNet Project)[12], Система «Сентурион» (Senturion) разработки компании Sentia Group[13], Объединенная система раннего

[5] См.– URL: http://www.dtic.mil/biosys/hptb.html (дата обращения 07.11.2012)

[6] Defense Advanced Research Projects Agency (DARPA) – Social Media in Strategic Communication (SMISC): Broad Agency Announcement, DARPA-BAA-11.64. 2011. July 14. – См. – URL: http://cryptome.org/dodi/dod-smisc.pdf (дата обращения 07.11.2012)

[7] Intelligence Advanced Research Projects Activity (IARPA). Open Source Indicators (OSI) Program: Broad Agency Announcement, IARPA-BAA-11-11. Office 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)

[8] См. – URL: http://theoldspeakjournal.wordpress.com/2012/01/ (дата обращения 05.11.2012), См. также – URL: http://publicintelligence.net/ (дата обращения 21.11.2012),

[9] Environmental Change and Fragile States — Early Warning Needs, Opportunities & 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 доступа 21.11.2012).

[10] Система создана в Исследовательской лаборатории ВВС США (Air Force Research Laboratory). – NOEM предоставляет пользователям платформу, позволяющую выявить основные аспекты взаимосвязи между активностью населения и обстановкой в стране (экономической, социальной и т. п.) и дать прогнозы по развитию ситуации в контексте, интересующем политических деятелей.

[11] Forecast and Analysis of Complex Threats (FACT III) – проект направлен на разработку методов прогнозирования возникновения внутренних конфликтов в отдельно взятых странах.

[12] Проект Национального центра по применению суперкомпьютеров (Университет шт. Иллинойс, США, National Center for Supercomputing Applications (NTCSA)). В рамках проекта осуществляются исследования по применению суперкомпьютеров для прогнозирования развития человеческого общества в глобальных масштабах. Используется постоянный мониторинг всех доступных открытых источников (веб-новости, социальные медиа и др.) с одновременным задействованием архивов новостей, а также, например, из OSC.

[13] Senturion – позволяет выявлять ключевые действующие политические фигуры, их позиции и степень влияния на поли-

предупреждения о кризисах ICEWS[14],[15], программа Human Social Culture Behavior Modeling (HSCB)[16], программа Social Media in Strategic Communication (SMISC) стартовавшая в июле 2011 года в агентстве DARPA[17] и инструмент анализа социальных сетей и динамики мнений (Social Networks and Opinion Dynamics Analysis (SNODA)[18] tool). Вызвал интерес и проект управления IARPA начатый в августе 2011 года 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[19]. Федеральное бюро расследований (Strategic Information and Operations Center (SIOC)) в январе 2012 года объявило о поиске готовых к прак-

тическую ситуацию. На основе этих данных осуществляется прогнозирование развития сложных политических событий на срок до двух лет.

[14] Работы над системой ICEWS осуществляются с конца 2007 г. под руководством агентства DARPA корпорацией «Локхид Мартин», которой также разработано программное обеспечений для анализа социальных сетей и динамики мнений (Social Networks and Opinion. Dynamics Analysis (SNODA)).

[15] Integrated Crisis Early Warning System (ICEWS) – предназначена для прогнозирования кризисных событий. В 2012 финансовом году на программу ICEWS запланировано израсходовать почти 5,3 млн дол. и передать все компоненты системы ICEWS в ведение стратегического командования США (USSTRATCOM). В целях применения на практике авалитико-прогностических методов, выработанных при реализации программы ICEWS, для дальнейшей разработки новых технологий автоматизированного анализа социальных сетей и прогнозирования динамики их развития DARPA осуществляет программу Nexus 7, на которую в текущем и будущем году планируется затратить более 66 млн дол.

[16] Human Social Culture Behavior (HSCB) Modeling – моделирование человеческого поведения в социально-культурной области. Пентагон осуществляет исследования в этой области с 2008 г. В ходе работ по этой программе планируется создать программные средства, предназначенные для облегчения понимания и прогнозирования общественного поведения на стратегическом, оперативном и тактическом уровнях. На программу HSCB в 2012 финансовом году планируется затратить более 28 млн дол. (См.– Department of Defense Fiscal Year (FY) 2013 President's Budget Submission. Research, Development, Test & Evaluation, Defense-Wide. Justification Book. Vol. 3. Office of Secretary of Defense. February 2012.). См. также – URL: http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY13/rforms//vol6.pdf

[17] Главной задачей программы SMISC является выработка новых научных подходов к социальным сетям, построенным на ранее не существовавшей технологической базе. В частности, в рамках программы SMISC должны быть разработаны автоматизированные и полуавтоматизированные технологии и инструменты для систематического и основанного на соответствующих методиках использования социальных медиа. Эксперты DARPA отмечают, что условия, в которых вооруженные силы США проводят свои операции, быстро меняются по мере распространения сайтов социальных сетей, блогов и технологий обмена аудиовизуальной информацией (как, например, YouTube) и эти изменения только ускоряются с развитием мобильных инфо-коммуникационных технологий, Изменения в природе самих конфликтов, вызванные использованием социальных медиа, столь же глубоки, как и изменения, вызванные предыдущими революциями в сфере телекоммуникаций.

[18] Social Networks and Opinion Dynamics Analysis (SNODA) tool – предназначен для моделирования, анализа и визуализации распространения мнений в больших социальных сетях. Этот инструмент также позволяет осуществлять моделирование операций влияния (influence operations), нацеленных на изменение мнений в желаемом направлении. Эксперименты проводились на членах социальной сети из состава специально созданного искусственного виртуального сообщества. Разработан в конце 2011 года научно-исследовательским подразделением корпорации «Локхид Мартин», Лабораторией передовой технологии (Lockheed Martin Advanced Technology Laboratories (LM ATL)).

[19] Рабочая группа PITF (Political Instability Task Force), финансируемая ЦРУ, работает в интересах правительства и разведывательного сообщества США с 1994 г. Сейчас основной задачей группы является разработка математических методов и моделей, с помощью которых можно с высокой точностью оценить перспективы развития различных стран и идентифицировать ключевые факторы риска, представляющие интерес для выработки политических решений. Проведенные исследования показали, что точность прогнозов, основанных на авторитетных суждениях экспертов, существенно повышается при объединении многих независимых мнений с помощью математических методов и моделирования. Для решения этой задачи была начата реализация программы ACE (июнь 2010 г.), в рамках которой планировалось разработать и протестировать методы генерирования точных и своевременных вероятностных прогнозов и ранних предупреждений о событиях на основе объединения мнений различных аналитиков (Aggregative Contingent Estimation (ACE) Program: Broad Agency Announcement. IARPA-BAA-10-05. Office of Incisive Analysis. Intelligence Advanced Research Projects Activity SIAEPA). 2010 – June 30). См. также – URL: http://globalpolicy.grau.edu/pitf/index.htm

10.7256/2073-8560.2013.01.7

тическому 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.)[24].

Международные эксперты отмечают, что разведывательные агентства осуществляют регулярный мониторинг социальных сетей уже в течение нескольких лет[20]. На самом деле получение разнообразной информации из социальных сетей рассматривается в разведсообществе США как важный и необходимый элемент повседневной деятельности[21],[22]. Специфическая роль социальных сетей в процессах, происходящих в 2011 году 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 инфо-медийном пространстве и предназначенное для контроля разнообразных социальных сетей, прежде всего, в арабском мире[23]. По линии МИД Израиля на работу с социальными сетями в 2010 году было выделено около 2 млн дол., 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[24].

Наибольший объем разведывательной информации из социальных сетей в США добывается Государственным департаментом, Центром открытых источников ЦРУ (CIA's Open Source Center (OSC))[25] и Министерством внутренней безопасности (подразделение Social Networking/ Media Capability Unit). В ЦРУ ежесуточно скачивается до 5 млн сообщений из Twitter[26]. 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[27]. 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 он-лайн 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.

---

[20] *Stokes J.* EFF's New Lawsuit, and Mow the NSA Is Into Social Networking // Ars Technica. – URL: http://aratechnica.com

[21] *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

[22] *Dinzeo M.* Are CIA and Pentagon Your Friends on Facebook? Courthouse News Service.

[23] *Segev S.* Israel Watches Social Media // The Winnipeg Free Press. — http://www.winnipegfrcepress.com

[24] Israeli diplomats train on Twitter PR // Israel News. 2011, August 29. — http://www.ynetnews.com/articles/0,7340,L-4114989,00.html

[25] *Mayfield T.D.* A Commander's Strategy for Social Media // Joint Forces Quarterly. 2011.

[26] Anonymous. CIA Analysts Comb Social Media for Trouble Spots. The Associated Press. 2011. November 4. – URL: http://www.npr.org

[27] *Streitfeld D.* Pentagon Seeks a Few Good Social Networkers // The New York Times. 2011. August 2. – URL: http://bits.falogs.nytiraes.com

ru, но и он испытывает сильное конкурентное давление 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 предлагаться преимущественно политически-ангажированный контент»[28].

Авторы доклада не случайно 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 определённую 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:

1. «В России стремительно растет не только число интернет-пользователей, но и повышается интенсивность использования Сети;
2. За последние 4 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;
3. 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;
4. Четверть из двадцати наиболее популярных сайтов Рунета являются глобальными (американскими) сервисами и их доля растет на протяжении всех последних лет;
5. Произошла консолидация рынка интернет-поиска, который поделен между «Яндексом» и Google. Американская поисковая система продолжает активную экспансию на российский рынок;
6. Снижается роль крупных медийных порталов. Mail.ru рискует повторить судьбу «Рамблера», который ранее уже потерял большую часть своей аудитории;
7. Новостные агрегаторы продолжают оказывать воздействие на информационную картину Рунета и зачастую оказывают негативное информационное влияние;
8. Почти все активные пользователи Рунета зарегистрированы в социальных сетях, которые занимают более половины от общего времени, проводимого в Сети;
9. 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;
10. YouTube занял монопольное положение среди видеохостингов в Рунете. При этом политика сервиса в части модерирования контента вызывает сомнения в его политической нейтральности;
11. 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;

[28] См. – Доклад «Рунет сегодня: исследование российского Интернета» // См. – URL: http://www.civilfund.ru/mat/view/1 (дата доступа 30.09.2012).

10.7256/2073-8560.2013.01.7

12. Снижается роль электронной почты как средства коммуникации. Она становится «интернет-паспортом» пользователей, необходимым для регистрации в других ресурсах;
13. Skype занимает доминирующее положение в Рунете в качестве интернет-мессенджера, выдавливая с рынка ICQ, QIP и «Mail.ru Агент»;
14. Internet Explorer лишился доминирующего положения на рынке интернет-браузеров, уступив Google Chrome, Apple Safari, Mozilla Firefox и Opera;
15. 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;
16. 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»[29].

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 взаимодействия участников международных отношений, а интенсивное развитие Интернет-технологий открывает новые возможности для выработки согласованной политики по преодолению политико-социальных и экономических кризисов, а также выработке 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 кампании были выборы Президента США Барака Обамы в 2008 году. 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 использовалась 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; возникновение 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

[29] Там же.

10.7256/2073-8560.2013.01.7

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 котором 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 воспринималось 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, поэтому 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 так же 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 долларов достался

10.7256/2073-8560.2013.01.7

недавно зарегистрированной в Лос-Анджелесе компании Ntrepid»[30].

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 миллионам 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 [31].

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[32]».

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»[33] 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[34], 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 блоггеров». Согласно придуманным FogNews поправкам к закону о СМИ, все блоги с посещаемостью свыше тысячи человек обязаны регистрироваться как

[30] *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)

[31] Правительственные сайты Израиля подверглись миллионам кибератак// – URL: http://www.lenta.ru/news/2012/11/19/cyber/ (дата обращения 17.11.2012)

[32] Операция «Облачный столп» и смартфоны, помогающие террористам // – URL: http://www.newsru.co.il/israel/16nov2012/gadget_105.html (дата обращения 19.11.2012)

[33] См. – URL: http://ru.wikipedia.org/wiki/%C8%ED%F2%E5%F0%ED%E5%F2-%EC%E5%EC (дата обращения 17.11.2012)

[34] См. – URL: http://fognews.ru/v-gosdumu-vneseny-popravki-v-zakon-o-smi.html (дата обращения 17.11.2012)

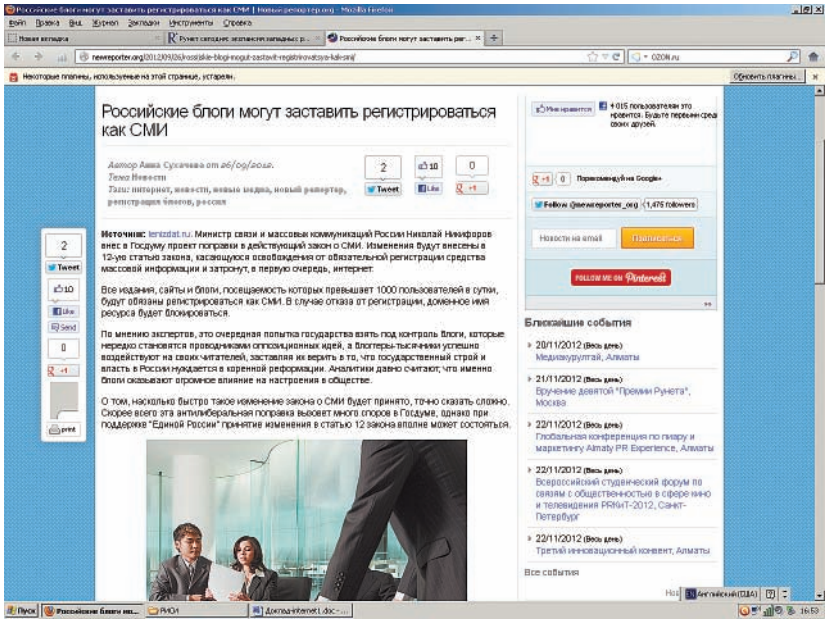
10.7256/2073-8560.2013.01.7

полноценные СМИ. 26 сентября новость со ссылкой на на FogNews появилась на сайте петербургского издания «Лениздат», а также на сайте Гильдии издателей периодической печати и на портале «Новый репортер»[35]. 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»[36].

распространение ерунды». Но, очевидно, что это ерунда не так уж и безобидна.

В данном контексте необходимо так же 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 он-лайн, 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



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

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 кибер-

[35] Минкомсвязи опровергло «утку» об обязательной регистрации блогов. Lenta.ru// – URL: http://www.lenta.ru/news/2012/09/26/minkomsvyazi/ (дата обращения 17.11.2012)

[36] См. – Официальный сайт Минсвязи РФ – URL: http://minsvyaz.ru/ru/news/index.php?id_4=43566 (дата обращения 18.11.2012)

10.7256/2073-8560.2013.01.7

простарнстве 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 они готовы выплеснуть на улицы свой протест. Ярким примером такого протеста против несправедливого мира 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: – «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[37]».

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 «тёмного веба» и анализа социальных сетей. Поэтому, как уже отмечалось ранее, в июле 2011 года 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 скрытых закономерностей и связей между ними[38]. 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))[39]. В первую очередь системы мониторинга BFT-ONE вводятся в Ираке, Пакистане, Афганистане и Йемене. Госдепартамент

[37] *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)

[38] Эта разработка представляет собой аналитическую среду, позволяющую более эффективно оценивать криминальные явления, планировать мероприятия в сфере борьбы с организованной преступностью, незаконным оборотом наркотиков, экономическими преступлениями. Использование разработок i2 дает возможность эффективно реализовать все основные фазы работы с информацией: сбор, организацию данных, анализ, обмен. Кроме того, i2 легко интегрируется с GTS-технологиями и другими технологиями аналитической обработки данных.

[39] Blue Force Tracker-Operationally Networked Environment (BFT-ONE) – предназначенf для осуществления оперативного контроля за перемещениями по территории этих стран транспортных средств и штатных сотрудников американских дипломатических представительств. BFT (Blue Force Tracker) – термин ВС США, обозначающий спутниковую информационную систему, позволяющую осуществлять непрерывный мониторинг положения подразделений и транспортных средств с идентификацией как дружественных сил, так и сил противника. Традиционно в военной символике синий цвет используется для обозначения дружественных сил, а красный -для обозначений противника.

10.7256/2073-8560.2013.01.7

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 оффшоры.

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.[40]

Относительно работы иностранных Интернет-сервисов в России, здесь есть момент, связанный с тем, что российское 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 разработчика 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[41] ».

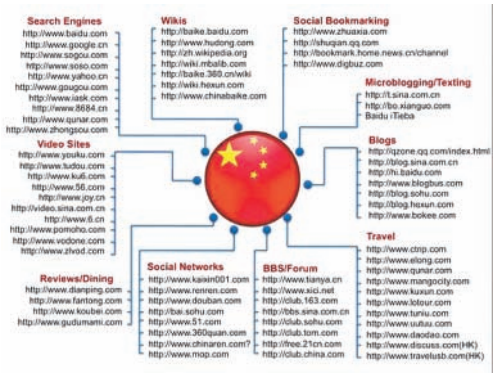
Примечателен китайский опыт. Доступ к иностранным сайтам изнутри материкового Китая ограничивается правительством Китая в целях цензуры. Веб-страницы фильтруются по ключевым словам, связанные с государственной безопасностью, а также по «чёрному списку» адресов сайтов. Иностранные поисковые машины, работающие в Китае, включая Google, Yahoo и Microsoft (поиск Live Search), согласились аналогичным образом фильтровать результаты поиска. Сайты, расположенные в самом Китае, прохо-

[40] «Главная роль будет принадлежать Сети» // – URL: http://vz.ru/politics/2012/9/25/599698.html (дата обращения 18.11.2012)

[41] «Google убирает противоправный контент без всяких споров» // URL: http://izvestia.ru/news/539672 (дата обращения 16.11.2012)

10.7256/2073-8560.2013.01.7

дят регистрацию в Министерстве промышленности и информационных технологий (кит.), что позволяет выявить автора незаконного содержимого[42]. 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 года и активная роль социальных сетей.



Информационный блок китайского Интернета[43].

Принимая во внимание накопленный опыт, был подготовлен ряд важных решений, которые, по мнению властей Китая, должны способствовать стабилизации ситуации в блогосфере. С конца 2011 года китайских пользователей Интернета уже стали постепенно обязывать записываться под своими настоящими именами при открытии блогов, в больших социальных сетях, базирующихся в Пекине, Шанхае, провинция Гуандун, недавно ставших очагами социальных волнений в стране[43]. А, начиная с 16 марта 2012 года 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 так же 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 американским фильмом[44]. 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, и одной из причин такого явления стало то, что протестные сил, фактически, были изолированы от традиционных СМИ. Оппозиционных деятелей не слишком часто приглашали на федеральное телевидении, 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

[42] См. – Википедия – URL: http://ru.wikipedia.org/wiki/%C8%ED%F2%E5%F0%ED%E5%F2_%E2_%CA%E8%F2%E0%E9%F1%EA%EE%E9_%CD%E0%F0%EE%E4%ED%EE%E9_%D0%E5%F1%EF%F3%E1%EB%E8%EA%E5

[43] La Chine met fin a l'anonymat sur ses reseaux de microblogging // La Liberation. 12.02.2012. – URL: http://fc\news.yahoo.com

[44] *Литвинцев Г.* Заслон духовному насилию. Взгляд // URL: http://vz.ru/opinions/2012/11/20/608066.html (дата обращения 20.11.2012)

10.7256/2073-8560.2013.01.7

законодательства. Сейчас уже приняты некоторые законы, направленные на осуществление более плотного контроля за 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, главная причина их господства кроется Нужно добавить, что одним только законодательством дело не решить, проблема не столь тривиальна. Причины экспансии западных сетевых ресурсов на просторы Рунета кроются в более высоком качестве предоставляемых ими услуг[45].

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 создание 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. 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 в последствии реализована концепция госполитики в области обеспечения кибербезопасности»[46].

Так же есть планы относительно создания Советом Федерации в начале 2013 года собственного круглосуточного телеканала для вещания в Интернете. Инициатором создания телеканала, который носит рабочее название «Вместе-РФ», стала председатель Совета Федерации Валентина Матвиенко. В планах канала – ведение прямые трансляции 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 сама Матвиенко. Основная студия телеканала разместится в здании Совфеда 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 Матвиенко в выделении 265,2 миллиона рублей на развитие канала в 2013-2015 годах. В министерстве главе Совфеда посоветовали использовать для вещания бесплатные видеохостинги, например, YouTube»[47].

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 пора-

[45] Рунет сегодня: экспансия западных ресурсов набирает обороты, REGNUM // URL: http://www.regnum.ru/news/fd-fareast/magadan/1574591.html#ixzz27b7xISp4 (дата обращения 16.11.2012)

[46] Совет Федерации напишет стратегию кибер-безопасности. Известия // URL: http://izvestia.ru/news/536153#ixzz27bEgRtBB (дата обращения 18.11.2012)

[47] Совет Федерации запустит собственный телеканал, Lenta.ru// URL: http://www.lenta.ru/news/2012/09/26/sovettv/ (дата обращения 15.11.2012)

10.7256/2073-8560.2013.01.7

жения, урегулирование региональных конфликтов и миротворчество, укрепление всеобъемлющей безопасности, сохранение культурного наследия и обеспечение прав человека.

Библиография:

1. Совет Федерации напишет стратегию кибер-безопасности. Известия // См. – URL: http://izvestia.ru/news/536153#ixzz27bEgRtBB (дата обращения 18.11.2012)
2. Карякин В.В., Наступила эпоха следующего поколения войн – информационно-сетевых. Независимая Газета, 22.04.2011// См. – URL: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html?mpril (дата обращения 03.11.2012)
3. Доклад «Рунет сегодня: исследование российского Интернета» // См. – URL: http://www.civilfund.ru/mat/view/1 (дата доступа 30.09.2012).
4. Официальный сайт Минсвязи РФ. См. – URL: http://minsvyaz.ru/ru/news/index.php?id_4=43566 (дата обращения 18.11.2012)
5. Главная роль будет принадлежать Сети. // См. – URL: http://vz.ru/politics/2012/9/25/599698.html (дата обращения 18.11.2012)
6. Google убирает противоправный контент без всяких споров. // См. – URL: http://izvestia.ru/news/539672 (дата обращения 16.11.2012)
7. Китайские интернет-ресурсы. См. – URL: http://www.assistantgroup.biz/ru/content/157/kitayskie-internet-resursi-i-dinamika-ih-razvitiya
8. La Chine met fin a l'anonymat sur ses reseaux de microblogging // La Liberation. 12.02.2012. См. – URL: http://fc\news.yahoo.com
9. Рунет сегодня: экспансия западных ресурсов набирает обороты, REGNUM // См. – URL: http://www.regnum.ru/news/fd-fareast/magadan/1574591.html#ixzz27b7xISp4 (дата обращения 16.11.2012)
10. Литвинцев Г. Заслон духовному насилию. Взгляд // См. – URL: http://vz.ru/opinions/2012/11/20/608066.html (дата обращения 20.11.2012)
11. Совет Федерации запустит собственный телеканал, Lenta.ru// См. – URL: http://www.lenta.ru/news/2012/09/26/sovettv/ (дата обращения 15.11.2012)

References (transliteration):

1. Karyakin V.V., Nastupila epokha sleduyushchego pokoleniya voyn – informatsionno-setevykh. Nezavisimaya Gazeta, 22.04.2011// Sm. – URL: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html?mpril (data obrashcheniya 03.11.2012)
2. Litvintsev G. Zaslon dukhovnomu nasiliyu. Vzglyad // Sm. – URL: http://vz.ru/opinions/2012/11/20/608066.html (data obrashcheniya 20.11.2012)