

Роль информационной безопасности в политике

© О.Г. Ламинина

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

В статье отображена роль информационных технологий и информационной безопасности в современной политике. Автор раскрывает важность сети Интернет и электронных СМИ при ведении информационно-психологических войн, на примере арабской весны, а также указывает на незащищенность Российской Федерации от комплексных информационных наступательных операций геополитических противников.

Ключевые слова: информационная политика, информационные технологии, информационная безопасность, информационная война, информационное противоборство, Интернет, электронные СМИ.

В настоящее время всеобщий процесс глобализации характеризуется ростом масштабов применения различных информационных технологий. Складывается информационное общество, которое постоянно трансформируется под воздействием высоких технологий. Важнейшая роль в российской политической жизни принадлежит глобальной сети Интернет. Следует отметить, что:

Веб-аудитория в России ежегодно увеличивается, в т. ч. месячная, недельная и суточная. Нас — пользователей интернета, по данным Минкомсвязи РФ на начало 2012 года, 70 млн чел. По этому показателю Россия вышла на первое место в Европе, которое ранее занимала Германия и на шестое место в мире. Первое место в мире занимает Китай, где веб-пользователей более 500 млн. человек, далее идут США, Япония, Индия и Бразилия.

Рост числа пользователей интернета в России будет продолжаться и далее. Согласно результатам исследования «Российского рынка интернет-торговли: товары 2012», проведенного агентством РБК.research, весной 2013 года уровень проникновения интернета составит 63,6%, а в 2018 году он превысит отметку в 80%. Достижению данных прогнозов будут способствовать, прежде всего, рост пользования интернетом в городах РФ с населением менее 100 тыс. чел. и селах, где уровень интернетизации пока еще не превышает соответственно 50% и 37%.

Распределение общего числа пользователей интернета по регионам РФ крайне неравномерно. Например, в ЦФО (Центральный Федеральный Округ) месячная веб-аудитория, по данным ФОМ на лето 2012 г., 29% или 17,2 млн чел., а в Дальневосточном ФО — 4% или 2,6 млн чел.

Из чего можно сделать вывод о том, что формирование информационного общества в России переходит в тотальную фазу и начинает охватывать практически все стороны общественной жизни.

Сегодня Интернет — это независимая и бесперебойная глобальная система коммуникации. Она включает в себя такие средства представления и пересылки информации, как электронная почта, веб-сайты (страницы), различные протоколы передачи данных, для которых используется модемная или беспроводная связь. Средствами для связи с Интернетом оснащаются персональные компьютеры, мобильные телефоны и т. д. Интернет становится реальным фактором не только экономического роста, но и формирования новых отношений на мировой арене.

Среди вопросов, исследование которых имеет прикладной характер, можно отметить обеспечение информационной безопасности государства в избирательных кампаниях и разработку федеральных целевых программ обеспечения информационной безопасности, разработку политических программ и нормативных документов, регулирующих информационную безопасность государства и совершенствование нормативно-правовой базы информационной сферы, организацию функционирования систем обеспечения региональной безопасности и совершенствование существующих нормативных документов в области информационной безопасности, включая «Доктрину информационной безопасности Российской Федерации» и «Концепцию национальной безопасности Российской Федерации».

СМИ становятся универсальным медиатором во всех политических процессах. Именно контроль над системой массового информирования и грамотно выстроенная коммуникационная политика являются на сегодняшний день ключевым фактором успеха политического деятеля. Более того, все больший вес приобретают такие понятия, как информационная безопасность, информационная война и прочие.

В научной литературе представлены различные точки зрения на природу информационной политики. Например, Ю.А. Нисневич утверждает, что «информационная политика рассматривается как совокупность целей, отражающих национальные интересы в информационной сфере, стратегии, тактике, задачах государственного управления, управленческих решений и методов их реализации, разрабатываемых и реализуемых государственной властью для регулирования и совершенствования как собственно процессов информационного взаимодействия в общественно-политической жизни и социально-экономической сфере жизнедеятельности общества и государства, так и процессов обеспечения такого взаимодействия»[3].

С.Э. Зуев в своей работе «Измерения информационного пространства политики, технологии, возможности» характеризует информационную политику как способ обращения с имеющимися информационными потоками и ресурсами со стороны различных институциональных субъектов, например, государства, или государственных органов, или отдельных организаций и учреждений, которые могут иметь свои представления и интересы при работе с информацией [4].

Одним из важнейших факторов определяющим эффективность государственного управления является уровень ее информационного обеспечения. Сейчас очень быстрыми темпами развивается компьютерная техника, разрабатывается и внедряется новое программное обеспечение, системы управления базами данных (СУБД), автоматизированные системы управления технологическими процессами (АСУТП), большое распространение получают программно-аппаратные комплексы, выполняющие различные функции.

За последние 15–20 лет наибольший упор все технологические компании мира делают на развитие технологии передачи данных между различными локально-вычислительными сетями (ЛВС). Благодаря этим технологиям и получила глобальное распространение сеть Интернет.

В связи с тем, что доступ в глобальную сеть разрешен всем без исключения, и в большинстве случаев деятельность в сети не отслеживается, сеть превратилась в источник угроз всему информационному полю.

Пропаганда и психологическая война всегда играли важную роль во внутренних и внешних конфликтах. Вместе с тем с возникновением «информационного общества» значение этого средства борьбы существенно возросло. Ярким примером тому являются события, происходящие в арабских странах.

Основная роль в пропагандистской войне отводится спутниковому телевидению, создающему стереотипы и внедряющему их в массовое сознание. Ведущее место в этом отношении принадлежит «Аль-Джазире» и «Аль-Арабийе», передачи которых на арабском и английском языках, призванные породить симпатии к восставшим, стали важнейшим источником информации как для арабских стран, так и для западного мира. Эффективность ТВ предопределяется, во-первых, его широким распространением и, во-вторых, воздействием зрительного ряда, который навязывает зрителю «картинку», не оставляя времени для анализа обрушивающейся на него информации.

Что касается Интернета, то он сыграл немаловажную роль в происходящих событиях, хотя эту роль и не следует абсолютизировать.

Здесь необходимо прежде всего иметь в виду, что уровень охвата всемирной сетью населения арабских стран является довольно низким — в Египте доступ к ней с личных компьютеров имеет 24% населения, а в Ливии — 6%, в то время как, например, в России — 50%, а в США — 81%. Вместе с тем на Ближнем Востоке и в Северной Африке среди пользователей Интернета преобладают молодежь и политическая, деловая и культурная элиты, т. е. наиболее социально активная часть общества.

Интернет выполняет двойную функцию. Во-первых, через него осуществляется информирование населения о природе выступлений и о развитии ситуации, что позволяет протестующим противодействовать пропаганде властей. И что важно, при этом открываются широкие возможности для подтасовки фактов. Во-вторых, социальные сети используются в организационных целях для распространения сведений, где и когда демонстрантам следует собираться, какими будут маршруты следования, надо ли быть готовыми к столкновениям с полицией и т. п.

Арабская смута продемонстрировала, таким образом, значимость и высокую эффективность современных информационных технологий. И было бы, как представляется, крайне опасной ошибкой надеяться, что «электронное цунами» будет обходить стороной Россию. В 2008 г. РФ уже стала объектом массивной информационной атаки, построенной по тому же принципу, что и пропагандистские кампании против Югославии в 1999 г., Ирака в 2003 г., Ливии в 2011 г. и Сирии в 2012 г. Снятый тогда российским ТВ документальный фильм об утюживших Цхинвали грузинских танках, от которого, по словам итальянских исследователей Дж. Пьезо и П. Кабраса, «до сих пор стынет кровь в жилах», демонстрировался западными телеканалами как репортаж о русской танковой атаке на Гори.

В связи с этим закономерно возникает вопрос, будет ли — и в какой мере — Россия готова отразить неизбежную пропагандистскую атаку в случае, если она вновь окажется втянутой в какую-либо конфликтную ситуацию.

Доктрина информационной безопасности России была принята 9 сентября 2000 года. Предполагалось, что затем будет разработана и принята российская Доктрина информационного противоборства (в США она была принята в 1998 году). Однако из-за субъективных факторов она не была разработана. Ее отсутствие и проявилось в августе 2008 года, когда против России была впервые развернута грязная информационная война, прежде всего американскими и британскими СМИ. Россия оказалась не готова к информационной агрессии, но

никаких решений по созданию системы информационного противодействия принято не было.

Информационный шум, созданный после выборов 04.12.2011 г. во-круг митингов внесистемной оппозиции, ядро которого составляют неолибералы-западники очень напоминает об августе 2008 года. Власть опять, как и в августе 2008 года, оказалась не готова отражать комплексные информационные наступательные операции геополитических противников. Хотя сейчас информационное воздействие оказывается тоньше, с использованием реальных ошибок действующей российской власти, ее неготовности к активному информационному противоборству в сети Интернет. Например, анализируя телесюжеты о декабрьских митингах протеста в Москве западных телеканалов, можно говорить о синхронности их действий (как и в августе 2008 года), направленных прежде всего на то, чтобы показать западному, да и российскому обывателю гораздо больший размах протестов, чем есть на самом деле. Кроме того, прошедшие парламентские выборы показали значительный рост популярности у населения в первую очередь левых оппозиционных партий — «Справедливой России» и Коммунистической партии Российской Федерации. Одновременно можно констатировать, что либеральная оппозиция в лице партии «Яблоко» вновь потерпела сокрушительное поражение. Тем не менее западные СМИ пытаются сформировать совершенно иной образ волеизъявления российских избирателей. Во главе радикальных оппозиционных либеральных организаций — политики, которые не пользуются никаким авторитетом после того урона стране, который они нанесли, пребывая у власти в лихие 90-е годы. Открытое недоверие им выражают около 60% россиян. Несмотря на это, британо-американские СМИ исподволь внушают людям мысль об их якобы всенародной поддержке.

Главная проблема — это явная «пробуксовка» организационно-управленческих решений в информационной сфере после принятия в 2000 году Доктрины информационной безопасности России, в условиях усиления информационной войны против России. Федеральные выборы в России прошли в условиях активизации антироссийской информационной войны. Трагические июльские события 2012 года на Кубани также выявили проблемы в сфере информационного противодействия слухам и дезинформации.

В начале 2012 года на сайте Министерства обороны РФ появился документ «Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве». В данной концепции описана стратегия поведения России в кибернетической войне. Вследствие уязвимости информационно-коммуникационных систем

к радиоэлектронным и программно-аппаратным воздействиям в мире возникло и стало быстро распространяться информационное оружие, обладающее трансграничными поражающими факторами, резко возросла роль информационной войны.

Также отмечается, что в современных условиях обороноспособность Российской Федерации во многом зависит от эффективности деятельности Вооруженных Сил в информационном пространстве и во многом определяется их возможностями по сдерживанию, предотвращению и разрешению конфликтов, возникающих в информационном пространстве.

Придерживаясь настоящей Концепции, Вооруженные Силы Российской Федерации будут стремиться к максимальному использованию возможностей информационного пространства для укрепления обороноспособности государства, сдерживания и предотвращения военных конфликтов, развития военного сотрудничества, а также формирования системы международной информационной безопасности в интересах всего мирового сообщества.

Следует отметить, что в данном документе не исключается возможность ответа на угрозу в виртуальном пространстве действиями, принятыми в реальных войнах. В частности, в разделе «Разрешение конфликтов» говорится: «В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права».

Впервые такая идея (ответ на киберугрозу реальными военными действиями) была высказана США в опубликованном документе «Глобальная стратегия развития киберпространства» в 2011 году.

Еще одним интересным пунктом Концепции является то, что в интересах индивидуальной и коллективной самообороны предполагается размещение своих сил и средств обеспечения информационной безопасности на территории других государств.

ЛИТЕРАТУРА

- [1] Нисневич Ю.А. Информация и власть. М., 2000, с. 9.
- [2] Зуев С.Э. Измерения информационного пространства (политики, технологии, возможности).
- [3] Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. URL: <http://www.scrf.gov.ru/documents/5.html>.
- [4] Концептуальные взгляды на деятельность вооруженных сил российской федерации в информационном пространстве. URL: <http://www>.

km.ru/tekhnologii/2012/03/14/ministerstvo-oborony-rf/ministerstvo-oborony-rf-opublikovalo-strategiyu-kiber.

- [5] Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М., 2013.
- [6] Халидов Д. Информационный террор против России и роль массмедиа. URL: <http://www.km.ru/spetsproekty/2012/01/30/nedostovernaya-informatsiya-i-lozh-v-smi/informatsionnyi-terror-protiv-rossii>.
- [7] Грибков А. Министерство обороны РФ опубликовало стратегию кибервойны. URL: <http://www.km.ru/tekhnologii/2012/03/14/ministerstvo-oborony-rf/ministerstvo-oborony-rf-opublikovalo-strategiyu-kiber>.
- [8] Панарин И. О Доктрине информационного противоборства России. URL: <http://www.km.ru/spetsproekty/2012/07/17/otnosheniya-rossii-i-stran-zapadnoi-evropy/o-doktrine-informatsionnogo-proti>.
- [9] Поляков А.В. Проблематика информационной безопасности в политических научных направлениях.

Статья поступила в редакцию 05.08.2013

Ссылку на эту статью просим оформлять следующим образом:

Ламинина О.Г. Роль информационной безопасности в политике. *Гуманитарный вестник*, 2013, вып. 4. URL: <http://hmbul.bmstu.ru/catalog/polit/hidden/62.html>

Ламинина Ольга Глебовна — канд. филос. наук, доцент кафедры «Политология» МГТУ им. Н.Э. Баумана. e-mail: vv11754@yandex.ru