ВАСИЛЬЕВА Мария Михайловна – кандидат политических наук, доцент кафедры связей с общественностью Московского государственного лингвистического университета (119034, Россия, г. Москва, ул. Остоженка, 38; catmar@yandex.ru)

СЕТЕВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ВО ВНЕШНЕПОЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. *В статье рассматриваются возможности использования сетевых информационных технологий в интересах государственного управления. Автор приходит к выводу, что сегодня сетевые информационные технологии становятся все более значимой площадкой внешнеполитической деятельности. В то же время использование «мягкой силы» посредством сетевых форм расширяет возможности подрыва извне политической стабильности и суверенитета государства.*

Ключевые слова: *внешнеполитическая деятельность, сетевые информационные технологии, электронное правительство, коммуникационные технологии, «мягкая сила»*

Информация и коммуникационные технологии все в большей степени приобретают значимость в деле обеспечения стратегической стабильности и международной интеграции государств. Существенная роль в формировании единого информационного пространства отводится созданию общенациональных телекоммуникационных сетей, позволяющих обеспечить широкий доступ гражданам к соответствующим территориально распределенным информационным ресурсам. Содаваемые информационные структуры должны обеспечить включение отдельных государств в мировое экономическое, информационное и научное пространство, что является необходимым условием прогресса [Васильева 2013].

Сетевые информационные технологии предоставляют широкие технические возможности для государственного управления, международной политической деятельности, делают более прозрачным механизм функционирования государственной власти. Интернет позволяет дать более объективную и качественную оценку деятельности государственных структур [Жеглова 2014].

В последние годы в России началась реализация проектов создания так называемого электронного правительства, предполагающая, в частности, повышение как «оперативности и качества государственного управления», так и «степени участия всех избирателей в процессах руководства и управления страной» [Связи с общественностью... 2015: 42]. Однако повышение открытости власти и общества содержит в себе и определенные риски. В частности, они становятся открытыми и для внешнего воздействия, для манипулирования общественным сознанием, что в определенной степени подрывает летимность самой власти [Цаплин 2016: 80].

Весьма серьезные последствия использования Интернета в международных отношениях кроются в том, что быстро формируются и развиваются сетевые сообщества. Они постепенно становятся акторами мировой политики, принимая на себя определенные государственные функции.

Развитие «сетевых союзов» в новой глобальной ситуации способно подорвать основы международного права. Так, по отношению к Интернету до сих пор не отработан четкий свод правил и положений, регулирующих деятельность его индивидуальных пользователей и сетей. СМИ достигают своими посланиями массы людей по всему земному шару. Информатика позволяет взаимодействовать на расстоянии. «Материальные и символические коммуникации означают сжатие времени и пространства. Но нет нормативного консенсуса, отвечающего

всему этому и способного основать приемлемые для широкой общественности институты демократического глобального управления» [Мартинелли 2003: 14].

Интернет – перспективное средство не только международного политического диалога, взаимодействия; он становится все более значимой площадкой внешнеполитического противостояния. Внедрение сетевых информационных технологий вышло на первые роли и в борьбе за военно-техническое превосходство, качественное совершенствование вооружений.

В руководящих кругах США господствует мнение, что защищенность информационных систем и сетей – важнейшая задача обеспечения национальной безопасности начавшегося столетия и что степень риска, которому страна подвергается в этой области, осознана не до конца (обобщенный вывод из анализа официальных документов США, касающихся обороны и безопасности, информационного противоборства, таких как «Международная стратегия действий США в киберпространстве», «Стратегия Министерства обороны по операциям в киберпространстве», доктрина «Информационные операции» и др.) [Современные международные... 2016: 235].

В России потенциальные опасности, исходящие от Интернета, гораздо выше, чем в США, поскольку основная масса сетевого программного обеспечения в РФ либо прямо заимствована, либо построена с включением заимствованных модулей. Известно, что около 70% программного обеспечения, продаваемого в мире, создано в США. Один из главных производителей программного обеспечения компания «Майкрософт», как известно, давно и тесно сотрудничает с Пентагоном. Кроме того, в Россию в большом количестве поступает информационная техника, произведенная за рубежом. Она часто содержит специальные компоненты съема или уничтожения информации и т.п.

В Доктрине информационной безопасности Российской Федерации достаточно четко обозначены угрозы национальной безопасности в информационной сфере. В этом документе констатируется: «Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать» (ч. I, п. 1)[1].

Использование сети Интернет расширяет возможности подрыва извне политической стабильности страны, поскольку появляются новые эффективные информационные каналы, через которые, в т.ч. в нарушение российского законодательства, можно дестабилизировать отношения между социальными группами, оказывать негативное воздействие на функционирование гражданского общества. Информация, транслируемая через Интернет, может провоцировать межэтнические и межконфессиональные конфликты, экстремизм, неповиновение и противодействие представителям законной власти и др.

Российские эксперты в области обеспечения информационной безопасности обратили внимание на необъяснимую природу компьютерных сбоев и случаи исчезновения информации. В результате исследований, проведенных в 2012 г. сотрудниками Лаборатории Касперского, был обнаружен вирус, получивший название *Flame*. Детальное его изучение показало наличие уникального вредоносного кода, превосходящего все ранее известные виды угроз. При этом большинство фактов заражения было отмечено в Иране, остальные – в Палестине, Ливане, Саудовской Аравии и Египте. Специалисты сходятся во мнениях, что вредоносная программа была активна в течение как минимум 2 лет до ее обнаружения [Современные международные... 2016: 239].

[1] Выступление президента Российской Федерации В.В. Путина на восьмом совещании послов и постоянных представителей Российской Федерации. Москва. МИД. 30 июня 2016 г. Доступ: http://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2338996

Распространяясь через сменные носители, локальные и глобальные сети, этот вирус имел достаточно богатый арсенал инструментов в своем активе: возможность перехватывать сетевой трафик, обнаруживать сетевые ресурсы и собирать пароли, сканировать диски в поиске определенных расширений и контента, осуществлять захват экрана, передачу сохраненных данных на контрольные серверы в обход современных антивирусных программ.

Спустя некоторое время газета «Вашингтон Пост» обвинила в создании *Flame* специалистов США и Израиля[1]. Следует отметить, что Иран и ранее становился объектом кибернетических атак. Предположительно, выявленные ранее вирусы *Stuxnet* и *Duqu* были звеньями той же самой цепи. *Stuxnet* чуть не уничтожил высокотехнологичное оборудование, используемое в иранской ядерной программе, вызывая необъяснимые сбои.

Комментируя эти события, Е. Касперский отметил: «...уже на протяжении нескольких лет опасность военных операций в киберпространстве является одной из самых серьезных тем информационной безопасности»[2]. Установить лицо (государство), организовавшее кибератаку, можно только по косвенным фактам.

Другое громкое дело было связано с созданием «уязвимостей», позволяющих получать конфиденциальную информацию пользователей устройств под управлением *Mac OS*. Факт заражения троянской программой *Flashback* впервые был обнаружен компанией *Dr. Web*. При этом только за первые сутки специалисты установили, что вирус функционирует более чем на 550 тыс. рабочих станций, преимущественно расположенных на территории США и Канады.

Регулярно возникают претензии пользователей в адрес компании *Google*, которая собирает необходимую информацию о пользователях через созданный браузер *Google Chrome*. Ряд экспертов, изучающих операционную систему *Android*, также нашли в ней технологические решения компании *Google*, которые регулярно передают данные о пользователях в компанию без соответствующего запроса. В одном из интервью бывший директор компании Эрик Шмидт (*Eric Schmidt*) признал, что мобильный телефон – это персональный шпион, позволяющий узнать, где человек проводит время, что покупает, какую слушает музыку и смотрит фильмы, с кем общается и по каким вопросам. В перспективе эта информация также может быть использована для создания рентабельного с экономической точки зрения контента (содержания).

Сетевые информационные технологии широко использовались в революциях в Молдавии, Ираке, Тунисе и Египте. Интересен тот факт, что при смене власти в Египте правительство адекватно оценило масштабы угрозы, формируемой в сети Интернет, поэтому временно отключило ее и заблокировало сотовую связь. Однако принятые властью меры оказались запоздалыми, и Хосни Мубараку (*Hosni Mubarak*) пришлось уйти в отставку.

Несколько иная стратегия, уже с применением военной силы, для обеспечения комплексного сетецентрического воздействия была реализована в Ливии. В данном случае информационные технологии позволили дискредитировать политический режим лишь в глазах мирового сообщества.

В Сирии, как и в Египте, через компании *Google* и *Twitter* готовились революционные блоггеры, которые манипулировали общественным мнением через представление искаженной и блокирование нежелательной для Запада информации.

---

[1] U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. – *The Washington Post*. 2012. 19 June. URL: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

[2] Мирошкин А. Вирус Flame нацелен на ядерную программу Ирана. – *Lifenews*. 2012. Доступ: http://lifenews.ru/news/93192

Для предупреждения возможности отключения Интернета властями Сирии был запущен известный сервис *speak2tweet*, позволяющий людям оставлять голосовые сообщения, которые затем записываются в файлы на *Twitter* в качестве информационных обновлений.

Как показывает опыт событий в Ливии, Сирии, Украине, в провоцировании «управляемого хаоса» используются два типа сетевых сообществ – локальные и региональные сетевые структуры.

Локальные сетевые структуры – сетевое сообщество, которое состоит из замкнутых на себя тайных децентрализованных групп со свободным горизонтальным общением.

Региональные сетевые структуры ориентированы на экспансию, распространение в регионе, на привлечение новых элементов. Для региональных сетей характерна подвижная, проницаемая и не всегда явно выраженная граница сети в пределах региона.

В условиях развития конфликта локальные и региональные сетевые структуры используются для решения мобилизационных задач, связанных с изучением возможностей, вербовкой и подготовкой боевиков. Локальные сетевые мобилизационные каналы обычно привлекаются для организации массовых волнений, как это было в Турции.

В Тунисе, Египте, Ливии, теперь в Сирии и Украине реализовывались отличающиеся друг от друга сценарии. Однако во всех случаях отчетливо видна решающая роль новых сетевых информационных технологий, которые создают выгодную иллюзию происходящих событий; внедряют в общественное сознание эту иллюзию через Интернет, СМИ; блокируют или обесценивают реальную, объективную информацию.

В этих целях используются и средства, нарушающие работу информационно-коммуникационных систем. В конце 2012 г. о новых решениях в области подавления информационной инфраструктуры противника сообщили компания Боинг (*Boeing*) и научно-исследовательская лаборатория ВВС США (*AFRL*).

Успешно прошло испытание новое оружие – ракета *CHAMP*. Основное ее предназначение – вывод из строя электронных приборов, находящихся в зоне ее воздействия. «Эта технология знаменует собой новую эру в ведении войн»[1], – заявил руководитель проекта Кит Коулман (*Keith Koleman*). Такие ракеты бесконтактным способом приводят в негодность электронные и информационные системы противника еще до появления первых самолетов.

Рассмотренные сетевые информационные технологии входят в комплекс инструментов и методов достижения внешнеполитических целей государства, который называют «мягкой силой». С ее помощью можно манипулировать политикой другого государства, навязывать определенные нормы, эталоны поведения людям, общественным организациям, институтам политической власти.

Эти механизмы президент РФ В.В. Путин охрактеризовал следующим образом: «Задействуется как веками копившийся опыт подавления, ослабления, сталкивания конкурентов лбами, так и усовершенствованные политические, экономические, финансовые, а сегодня уже и информационные рычаги. Имею в виду вмешательство во внутренние дела других стран, провоцирование региональных конфликтов, экспорт так называемых цветных революций»[2].

Реализовать политику мягкой силы без широкого использования сети Интернет

---

[1] Загорский И. Компания «Боинг» испытала новое микроволновое оружие. – *Вести.Ру*. 2012. 30 окт. Доступ: http://www.vesti.ru/doc.html?id=945973&cid=2161

[2] Выступление президента РФ В.В. Путина на восьмом совещании послов и постоянных представителей Российской Федерации. Москва. МИД. 30 июня 2016 г. Доступ: http://www.mid.ru/ru/foreign_policy/news/-asset_publisher/cKNonkJE02Bw/content/id/2338996

очень сложно, поэтому государства становятся заложниками ситуации, когда развиваться в информационном плане необходимо, но неумелое управление этим процессом создает существенную угрозу для целостности страны.

В Доктрине информационной безопасности РФ отмечается: «Особенность международного сотрудничества Российской Федерации в области обеспечения информационной безопасности состоит в том, что оно осуществляется в условиях обострения международной конкуренции за обладание на рынках сбыта, в условиях продолжения попыток создания структуры международных отношений, основанной на односторонних решениях ключевых проблем мировой политики»[1]. Эти вызовы во внешнеполитичской деятельности, безусловно, нужно парировать, учитывая реальные опасности и используя неоспоримые преимущества сетевых информационных технологий.

Список литературы

Васильева М.М. 2013. Формирование единого информационного пространства России в условиях глобализации. – *Вестник Московского государственного лингвистического университета*. Сер. Исторические и политические науки. Вып. 24(684): Актуальные проблемы внешней и внутренней политики Российской Федерации. С. 92-104.

Жеглова Ю.Г. 2014. Роль внешнеполитического имиджа России в США в системе российско-американского стратегического партнерства. – *Вестник Московского государственного лингвистического университета*. Вып. 2(668): Актуальные проблемы внешней и внутренней политики Российской Федерации. С. 51-69.

Мартинелли А. 2003. Рынки, правительства и глобальное управление (Доклад XV Конгрессу Международной социологической ассоциации, Брисбен, 2002). – *Социс. Социологические исследования*. № 1. С. 12-16.

Связи с общественностью в органах власти: учебник для академического бакалавриата (под ред. М.М. Васильевой). 2015. М.: Юрайт. 495 с.

Современные международные отношения: учебник для академического бакалавриата (под ред. А.И. Позднякова, В.К. Белозерова, М.М. Васильевой). 2016. М.: Юрайт. 341 с.

Цаплин А.Ю. 2016. Электронное правительство или двуликий Янус? – *Власть*. № 9. С. 79-83.

VASIL'EVA Mariya Mikhailovna, Cand.Sci.(Pol.Sci.), Associate Professor of the Chair of Public Relations, Moscow State Linguistic University (38 Ostozhenka St, Moscow, Russia, 119034; catmar@yandex.ru)

NETWORKING INFORMATION TECHNOLOGIES: OUTLOOK FOR FOREIGN POLICY

Abstact. *The main question tackled in this research deals with networking information technologies that provide great opportunities for state governance. The author concludes that networking information technologies become significant means to carry out foreign policy. At the same time, the use of soft power through network forms of Internet technologies increases the risk of undermining political stability of the country.*

Keywords: *networking information technologies, foreign policy, e-government, communication technologies, soft power*

[1] Доктрина информационной безопасности Российской Федерации от 09.09.2000 № Пр-1895. Доступ: http://dehack.ru/zak_akt/npa_prezidentarf/doktrina_ib/?all