ждан мешают средствам массовой информации оставаться независимыми и выполнять свои профессиональные обязанности, а вместо «представления о свободе, основанной на знании и самосознании» приходит демагогия, разрыв отношений между обществом и властью и, в конце концов, интеллектуальная деградация и извращение действительности. Достаточно красноречивым подтверждением того, насколько для тех, кто лишен конструктивизма в отношении нашей страны являются целенаправленные, достаточно грубые и лишенные изящного креатива информационные атаки на российского президента двух изданий из США и Великобритании – сказал пресс-секретарь президента Дмитрий Песков [5].

В заключении следует отметить, что политический имидж государства играет важнейшую роль в сфере международных отношений: от того является ли он позитивным или негативным, зависит успешность проведения внешней политики страны, развития торгово-экономических отношений с другими государствами. Внешнеполитический имидж оказывает воздействие и на политические процессы, протекающие в самом государстве: негативный образ страны может использоваться оппозиционными силами как один из аргументов критики в адрес правительства и проводимой им политики. Негативный характер международного имиджа РФ препятствует развитию взаимовыгодных отношений между Россией и странами Запада, мешает ее успешной интеграции в мировую экономику. Все это делает формирование позитивного внешнеполитического имиджа одной из первоначальных задач для современной России. Необходимость безотлагательного решения данной проблемы закреплена в Концепции внешней политики РФ, которая гласит: «На первый план выдвигается задача формирования за рубежом позитивного восприятия России, дружественного отношения к ней» [6, с. 4]. Таким образом, СМИ необходимо создавать внешнеполитический имидж России, вдохновляющий её граждан и вызывающий положительный резонанс в мировом общественном мнении.

Список литературы

1. Восприятие России в современном мире. – Режим доступа: http://www.promros.ru/magazine/2012/jun/vospriyatie-rossii-v-sovremennom-mire.phtml, свободный. – Загл. с экрана. – Яз. рус.

2. Bloomberg назвал семерых противников санкций против России в ЕС. – Режим доступа: https://news.mail.ru/politics/21417463/, свободный. – Загл. с экрана. – Яз. рус.

3. СМИ: Меркель опасается разделения ЕС из-за противоречий по России. – Режим доступа: https://news.mail.ru/ politics/21563899/?frommail=1, свободный. – Загл. с экрана. – Яз. рус.

4. DW: итоги года санкций против России разочаровали Запад. – Режим доступа: https://news.mail.ru/politics/21417025/?frommail=1, свободный. – Загл. с экрана. – Яз. рус.

5. Песков удивлен «прокурорским стилем» запросов иностранных СМИ // Известия. – 2015. – 25 мая.

6. Концепция внешней политики Российской Федерации // Дипломатический вестник. – 2000. – № 8. – С. 3–11.

References

1. *Vosprijatie Rossii v sovremennom mire* [Perception of Russia in the modern world]. Available at: ttp://www.promros.ru/magazine/2012/jun/vospriyatie-rossii-v-sovremennom-mire.phtml.

2. *Bloomberg nazval semeryh protivnikov sankcij protiv Rossii v ES* [Bloomberg called seven opponents of sanctions against Russia in the EU]. Available at: https://news.mail.ru/politics/21417463/.

3. *SMI: Merkel' opasaetsja razdelenija ES iz-za protivorechij po Rossii* [Mass media: Merkel is afraid of division of the EU because of contradictions across Russia]. Available at: news.mail.ru/politics/21563899/?frommail=1.

4. *DW: itogi goda sankcij protiv Rossii razocharovali Zapad* [DW: results of year of sanctions against Russia disappointed the West]. Available at: https://news.mail.ru/politics/21417025/?frommail=1.

5. *Peskov udivlen «prokurorskim stilem» zaprosov inostrannyh SMI* [Peskov is surprised with «public prosecutor's style» of inquiries of foreign mass media]. Izvestija. 2015.

6. *Koncepcija vneshnej politiki Rossijskoj Federacii* [Concept of foreign policy of the Russian Federation]. 2000, pp. 3–11.

ЗАРУБЕЖНЫЙ ОПЫТ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА

Пенкина Валентина Александровна, аспирант

Российская Академия народного хозяйства и государственной службы при Президенте Российской Федерации (РАНХиГС)

119571, Российская Федерация, г. Москва, ул. Академика Анохина, 5

E-mail: vapenkina@mail.ru

Рассмотрена практика защиты информационного суверенитета в США, Китае и ряде мусульманских стран, как форма противодействия деструктивному влиянию по политическим и религиозным мотивам, выявлены особенности и приоритеты информационных аспектов безопасности, выделены две стратегии защиты информационного суверенитета, которые условно можно назвать как «наступательная» и «оборонительная». Наступательная стратегия используется для информационных войн для достижения и закрепления своего политического доминирования (прежде всего – США и инструменты американской инфор-

мационной политики – современное руководство Украины, стран Балтии), наступательной тактики также придерживаются террористические организации (ИГИЛ, Аль-Каида). «Оборонительная» тактика заключается в реформировании законодательства в сфере защиты своего информационного суверенитета. Сделан вывод об оптимальном сочетании первого и второго методов, ориентированном не на конфронтацию, а на использование soft power для прекращения информационных войн, стабилизации и конструктивной информационной глобализации.

Ключевые слова: информационный суверенитет, глобализация, информационная безопасность

FOREIGN EXPERIENCE OF DEVELOPMENT OF INFORMATION SOVEREIGNTY

Penkina Valentina A., postraduate student

Russian Presidential Academy of National Economy and Public Administration
5 Akademika Anokhina st., Moscow, 119571, Russian Federation
E-mail: vapenkina@mail.ru

The practice of protection of information of sovereignty in the USA, China and some Muslim countries, as a form of combating destructive influence on political and religious grounds, the characteristics and priorities of the information security aspects allocated two strategies of protection of information of sovereignty, which can be called as «offensive» and «defensive». Offensive strategy is used for information warfare to achieve and consolidate their political dominance (primarily the United States and the instruments of U.S. information policy – the current leadership of Ukraine, the Baltic States), offensive tactics also adhere to a terrorist organization (the ISIS, al-Qaeda). «Defensive» tactic is to reform the legislation in the sphere of protection of information sovereignty. The conclusion is made about the optimal combination of the first and second methods, based not on confrontation but to use soft power to stop information warfare, stabilization and structural information globalization.

Keywords: information sovereignty, globalization, information security

Основоположник теории государственного суверенитета, французский политик и философ Ж. Бодэн полагал, что суверенитет – это один из главных признаков государства, позволяющих ему играть ведущую роль в международной системе отношений [2, с. 138]. Сегодня в условиях глобализации, процессов межгосударственной интеграции, стремительного развития информационно-коммуникационных технологий смысловое наполнение суверенитета постепенно изменилось и традиционные концепции суверенитета уже не в полной мере способны выразить сложность современных реалий международной жизни. Заключая международные соглашения, государства вынуждены вести политику на основе договоренностей, объединяясь в политические союзы, и тем самым ограничивать объем своих суверенных полномочий. Но независимо от процессов глобализации и интеграции, государство обязано пресекать военную агрессию и другие формы посягательства на суверенитет, а также обеспечивать свою экономическую, политическую и, что становится все более актуальным, информационную безопасность. Для того, чтобы государство могло проводить самостоятельную информационную политику, необходима «информационная суверенизация», при которой будет гарантироваться неприкосновенность информационного пространства со стороны других стран.

Зарубежный опыт свидетельствует о том, что достижение информационного суверенитета – это очень сложная задача для большинства государств, так как обеспечение безопасности своего информационного пространства вступает в противоречие с группой факторов: 1) процессом информационной глобализации; 2) целями мирового доминирования и ведущимися в его интересах информационными войнами, накал и интенсивность которых быстро растут.

Концептуальное и оформление и институализация идеологии информационного суверенитета прошли (для современных темпов распространения и репликации знаний) длительный путь. Понятие «информационная война» (Information War) было введено в научный и политологический оборот Т. Рона в 1976 г. в специальном отчете [11] для «Боинг». Уже тогда автор прямо указал на то, информационная инфраструктура как базовый компонент американской экономики (идеи информационного общества только зарождались), также есть и весьма уязвимая цель, причем и в мирное время. Концепция Т. Рона дала толчок дискуссии, но лишь к середине 1990-х гг. эти идеи были концептуально оформлены и воплощены в нормативные документы.

В США во второй половине 1990-х гг. институализирован приоритет информационных аспектов безопасности в военно-доктринальных документах, приняты «Доктрина борьбы с системами контроля и управления» (1996 г.) [9], «Объединенная доктрина информационных операций» (1998 г.) [8], согласно которым информационные операции включают в себя весь спектр действий в информационно сфере, в том числе и психологические операции.

В феврале 2003 г. администрацией президента Дж. Буша-младшего была принята «Национальная стратегия достижения безопасности в киберпространстве, описывающая пять приоритетов в деятельности США по обеспечению информационной безопасности и основные задачи в рамках этих приоритетов на среднесрочную и долгосрочную перспективу:

– становление и развитие национальной системы реагирования на происшествия в сфере информационной безопасности;

– реализация комплексной системы мер по уменьшению угроз информационной безопасности; обеспечение подготовки специалистов в сфере компьютерной безопасности и обеспечение ответственного отношения всего населения страны к вопросам защиты информации;

– обеспечение защиты информационных систем, имеющих отношение к государственным органам;

– развитие различных форм кооперации, в том числе и международной, в сфере обеспечения информационной безопасности [10].

И, наконец, в феврале 2014 г. уже администрация Б. Обамы совместно с Национальным институтом стандартов и технологий США опубликовала первую версию «Рамочного руководства по улучшению информационной безопасности». Подготовка документа проходила совместно с Министерством внутренней безопасности. На протяжении года эксперты составляли список правил и стандартов для обнаружения рисков, а также дальнейшей защиты и восстановления системы. Данная версия руководства представляет собой ряд отраслевых стандартов и примеров их эксплуатации, которые могут быть полезны компаниям для более качественного обеспечения информационной безопасности [7].

Информационные и психологические операции являются неотъемлемой частью ведения современной войны, что диктует необходимость информационного щита, защиты информационного суверенитета государства и национального информационного пространства. Здесь показательна политика Китая в сфере создания своей информационной независимости, построении так называемого «великого китайского файрвола» [12].

Анализируя документы, принятые в последнее время китайским высшим политическим руководством в области информационной безопасности, мы обращаем внимание на ряд фундаментальных отличий от других стран, корни которых, судя по всему, лежат в культурном различии западного и восточного типов цивилизаций. В частности, руководство КНР при планировании своей информационной политики исходит из двух постулатов, вытекающих из «китайской ментальности»: жесткие запретительные меры, с одной стороны, и неотвратимость, строгость наказания за «непослушание», с другой. Нарушение законодательства в информационной сфере в Китае влечет обвинение в разглашении государственной тайны и карается высшей мерой наказания или пожизненным заключением. В 2000 г. Всекитайское собрание народных представителей (ВСНП), принял ряд законов, направленных против «преступного использования» Интернета, в первую очередь в антигосударственных целях. Был составлен список «Интернет-преступлений». В него, в частности, вошли: проникновение в государственные сайты, шпионаж в сфере передовых технологий, а также распространение компьютерных вирусов [13]. Так же, с весны 2012 г. запрещено использовать псевдонимы (ники), кроме настоящего имени, при регистрации в сети необходимо ввести паспортные данные, адрес и телефон, что упрощает систему контроля пользователей Интернета.

Несмотря на внутренние меры, направленные на защиту своего информационного суверенитета, Пекин стремится к созданию внешнего «дружественного пояса» безопасности своего «киберпространства». Соперничая с США в сфере информационного доминирования, Китай, беспокоясь о возможных столкновениях в информационном пространстве, ищет пути к партнерству с другими странами в этой сфере. В 2015 г. планируется к подписанию российско-китайское Соглашение о сотрудничестве в сфере международной информационной безопасности в развитие аналогичного коллективного документа ШОС [1]. Проект соглашения предусматривает предотвращение возможных киберинцидентов, а также определяет направления сотрудничества в сфере предоставления национальных сегментов Интернета [4].

Китай принимает серьезные меры по созданию «надежного щита» своему информационному пространству, законодательство в информационной сфере развивается в русле, которое было определено на специальной сессии парламента КНР: информационная сфера и электронная сеть должны оставаться под контролем государства и способствовать экономическому росту страны.

Зарубежный опыт формирования и обеспечения информационного суверенитета целесообразно рассмотреть и на примере исламских стран с прочными религиозными принципам и традициям. Несмотря на постоянное давление и обвинения Запада в ущемлении свободы слова, государственные институты исламских государств вынуждены создавать жесткие барьеры и фильтры, защищающие их национальное информационное пространство от потока информации из глобальных информационно-телекоммуникационных сетей, особенно, на «просторах» глобальной сети Интернет. И этим мерам есть вполне логичное объяснение, опять же речь идет о защите «информационного суверенитета». В противном случае, потеря государством «рычагов управления» своим информационным пространством может привести к неконтролируемым, стихийным процессам, и, как следствие, даже к краху политической системы и развалу страны.

На первый взгляд спонтанно возникшая «Арабская весна» имеет свои «сетевые» корни, Именно материалы сайта «WikiLeaks» стали катализатором настоящей революционной ситуации в Тунисе, а сам процесс применительно к Тунису на Западе называют «WikiLeaks-революцией» [6]. В Египте ко всему прочему оппозиционные силы для организации забастовок и митингов использовали социальные сервисы Twitter и Facebook. Спустя три дня после начала волнений наученные «горьким опытом» Туниса власти «страны пирамид» незамедлительно блокировали все социальные сети. В итоге египетскому правительству впервые в мировой истории удалось отключить от Интернета почти 80 миллионов пользователей [3]. Вместе с тем был осуществлен ряд хакерских атак на государственные порталы, в том числе и сайт президента. Уже в последствии новые власти Египта и лично вновь избранный президент страны А. Эс-Сиси, проанализировав эту ситуацию, в сентябре 2014 г. стали разрабатывать новую программу по «глобальной информационной защите Арабской Республики Египет» [5].

В других арабских странах также, и не безосновательно, «заботятся» о своем информационном суверенитете. Так, в ОАЭ существует система сетевой защиты, которая блокирует любые материалы, связанные с порнографией, а также чаты, сайты знакомств и сервисы «видеообщения», такие как Skype. В стране заблокированы даже отдельные страницы Wikipedia. В 2007 г. в Абу-Даби был принят закон о виртуальном пространстве, запрещающий любые действия по созданию сайтов и ресурсов антиисламской или террористической направленности.

Еще несколько примеров. В Иордании с 2010 г. на всех рабочих местах заблокировано 48 местных новостных сайтов, так как веб-серфинг считается пустой тратой рабочего времени. Заблокированы даже сайты, касающиеся рабочего законодательства. А в интернет-кафе пользователи не могут получить доступ к ресурсам, которые пропагандируют азартные игры, наркотики и табак. Все интернет-кафе также обязаны на протяжении шести месяцев хранить данные об имени и идентификационной информации пользователя. Нарушение законодательства относительно интернета может привести к штрафу или исправительным работам.

В Иране с 2008 г. на основании действующего законодательства заблокировано более 5 млн «аморальных» сайтов, в число которых вошли Facebook и Youtube. При подключении к интернету, каждый пользователь обязан дать письменное обязательство не посещать «антиисламские» сайты, за нарушение которого можно получить до 15 лет тюрьмы. Также ограничена скорость интернета, как для служебного использования в госучреждениях, так и домашнего применения. В Иране, чтобы «облегчить» государству контроль за интернет пользователями, строго регламентированы условия работы провайдеров. Кроме того, в целях выстраивания четкой информационной политики иранскими властями в 2003 г. был создан Высший совет по информационным технологиям и информационной политике. Совет состоит из нескольких комиссий, в состав которых входят представители различных министерств и ведомств. Главными задачами Совета являются: выработка концепции информационной политики государства, подготовка концепции формирования информационного общества в Иране, разработка и утверждение нормативных документов, регламентирующих деятельность государственных органов в сфере информационных технологий, реализация программы международного сотрудничества Ирана в указанной области, внедрение информационных и телекоммуникационных технологий.

В целом, власти многих мусульманских стран, на своем опыте ощутили какой огромной силой и воздействием обладает Интернет, глобальные коммуникационные сети, и какое влияние может оказать «цифровой» фактор на устойчивость политической системы и национальную безопасность государства.

В современном мире реализуются две стратегии защиты информационного суверенитета, которые условно можно назвать как «наступательная» и «оборонительная». Наступательной стратегии придерживаются страны, ведущие информационные войны в целях достижения и закрепления своего политического доминирования (прежде всего – США). Ту же стратегию в рамках информационной политики США и под их непосредственным руководством, реализуют инструменты американской информационной политики – современное руководство Украины, стран Балтии и т.п. Отличием последних, является контент, формирующийся в большей части как продукт «психо-политической шизофрении» (термин В.В. Жириновского), не содержащий адекватной информации и направленный исключительно на деструктивное воздействие как сознания собственного населения, так и объекта воздействия (России, мирового сообщества). Наступательной тактики также придерживаются террористические организации (ИГИЛ, Аль-Каида).

«Оборонительная» тактика заключается в реформировании законодательства в сфере защиты своего информационного суверенитета. Многие страны, не имея достаточных материальных ресурсов, собственной электронной инфраструктуры, в основу «информационной суверенизации» власти полагая идеологические, культурные и религиозные факторы идут путем ограждения своих граждан от деструктивного влияния, используя жесткие сетевые ограничения и суровые меры наказания.

Оптимальным является сочетание первого и второго методов, ориентированное не на конфронтацию, а на использование soft power для прекращения информационных войн, стабилизации и конструктивной информационной глобализации.

Список литературы

1. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Утв. распоряжением Правительства РФ от 16.07.2009 № 984-р. Вступило в силу 02.06.2011 // Бюллетень международных договоров. – 2012. – № 1. – С. 13–21.

2. Бодэн Ж. Метод познания истории / Ж. Бодэн ; пер. с фр. – М. : Наука, 2000. – Серия «Памятники исторической мысли».

3. Блинов А.А. Интернет в арабском мире / А. А. Блинов // Восточная аналитика. – 2011. – № 2.

4. Коммерсантъ. Газета. – 2014. – 21 октября (№ 191). – С. 1.

5. Правительство Арабской республики Египет. – Режим доступа: http://www.egypt.gov.eg/english/home.aspx, свободный. – Загл. с экрана. – Яз. рус.

6. First Wikileaks Revolution: Tunisia descends into anarchy as president flees after cables reveal country's corruption // Daily Mail. – 2011. – 15 January.

7. Framework for Improving Critical Infrastructure Cybersecurity/ Version 1.0// National Institute of Standards and Technology (NIST). – Режим доступа: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, свободный. – Загл. с экрана. – Яз. рус.

8. Joint Pub 3-13 «Information Operations», DOD US. December 1998. – Режим доступа: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13sd.pdf, свободный. – Загл. с экрана. – Яз. рус.

9. Joint Pub 3-13.1 «Command and Control Warfare». DOD US, February 1996. – Режим доступа: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1.pdf, свободный. – Загл. с экрана. – Яз. рус.

10. National Strategy to Secure Cyberspace // Президент США. – Режим доступа: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html, свободный. – Загл. с экрана. – Яз. англ.

11. Thomas P. Rona «Weapon Systems and Information War» / Thomas P. Rona. – Boeing Aerospace Co., Seattle, WA, 1976.

12. Режим доступа: http://allrefs.net/c9/2yzzb/, свободный. – Загл. с экрана. – Яз. рус.

13. The National People's Congress of the People's Republic of China. – Режим доступа: http://www.npc.gov.cn/englishnpc/news/index.htm, свободный. – Загл. с экрана. – Яз. рус.

References

1. Soglashenie mezhdu pravitelstvami gosudarstv-chlenov Shankhayskoy organizatsii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoy informatsionnoy bezopasnosti ot 16 iyunya 2009 g. Utv. rasporyazheniem Pravitelstva RF ot 16.07.2009 № 984-r. Vstupilo v silu 02.06.2011. *Byulleten mezhdunarodnykh dogovorov*. 2012, no. 1, pp. 13–21.

2. Boden Zh. *Metod poznaniya istorii*; per. s fr. M.: Nauka, 2000. Seriya «Pamyatniki istoricheskoy mysli».

3. Blinov A.A. Internet v arabskom mire. *Vostochnaya analitika*. 2011, no. 2.

4. *Kommersant. Gazeta*. 2014, 21 oktyabrya (№ 191), p. 1.

5. *Pravitelstvo Arabskoy respubliki Yegipet*. Rezhim dostupa: http://www.egypt.gov.eg/english/home.aspx, svobodnyy. Zagl. s ekrana. Yaz. rus.

6. First Wikileaks Revolution: Tunisia descends into anarchy as president flees after cables reveal country's corruption. *Daily Mail*. 2011, 15 January.

7. *Framework for Improving Critical Infrastructure Cybersecurity/Version 1.0//National Institute of Standards and Technology (NIST)*. Rezhim dostupa: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, svobodnyy. Zagl. s ekrana. Yaz. rus.

8. *Joint Pub 3-13 «Information Operations», DOD US. December 1998*. Rezhim dostupa: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13sd.pdf, svobodnyy. Zagl. s ekrana. Yaz. rus.

9. *Joint Pub 3-13.1 «Command and Control Warfare». DOD US, February 1996*. Rezhim dostupa: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1.pdf, svobodnyy. Zagl. s ekrana. Yaz. rus.

10. National Strategy to Secure Cyberspace // *Prezident SShA*. Rezhim dostupa: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html.

11. Thomas P. Rona *«Weapon Systems and Information War»*. Boeing Aerospace Co., Seattle, WA, 1976.

12. Rezhim dostupa: http://allrefs.net/c9/2yzzb/, svobodnyy. – Zagl. s ekrana. – Yaz. rus.

13. *The National People's Congress of the People's Republic of China*. Rezhim dostupa: http://www.npc.gov.cn/englishnpc/news/index.htm, svobodnyy. Zagl. s ekrana. Yaz. rus.