УДК: 004.056:351.86(470) DOI: 10.22394/2071-2367-2017-12-4-83-90

ДЕСТРУКТИВНОЕ ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ ВЫЗОВАМ И УГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОЙ РОССИИ

Петрищев Е. В.[1]

Одной из приоритетных задач политического управления в современном обществе выступает выявление и предотвращение вызовов и угроз национальной безопасности Российской Федерации. В статье рассматривается процесс информатизации политики, выраженной в повышении доступности информационных ресурсов, в качественном и количественном росте числа каналов получения и доведения информации до широких масс населения. В этих условиях особую актуальность приобретают вопросы обеспечения безопасности в информационной сфере. Автором обосновывается, что процессы демократизации общества повышают его открытость как для международного сотрудничества, так и для организации внешних информационных воздействий различного, в том числе деструктивного, характера. Намерения по организации такого рода воздействий декларируются и юридически закрепляются в функциональном предназначении акторов международной политики. В данной работе представлен аналитический обзор методологической основы информационного воздействия, проведен анализ возможностей по его организации с целью дестабилизации политического процесса.

Ключевые слова: информационное пространство, информационное воздействие, национальная безопасность, информационная безопасность, политический процесс, актор политики, субъект информационного воздействия.

DESTRUCTIVE INFORMATIONAL INFLUENCE IN THE CONTEXT OF COUNTERMEASURES OF CHALLENGES AND THREATS OF NATIONAL SECURITY IN MODERN RUSSIA

PETRISCHEV E.V. – Employee of the Academy of the Federal Security Service of Russia (Russian Federation, Orel), e-mail: petrishev7@yandex.ru

One of the priority tasks of political management in modern society is the identification and prevention of challenges and threats to the national security of the Russian Federation. The article deals with the process of informatization of politics, expressed in increasing the availability of information resources, in the qualitative and quantitative growth of the number of channels for obtaining and communicating information to the broad masses of the population. In these conditions, the issues of ensuring security in the information sphere acquire particular urgency. The author justifies that the processes of democratization of society increase its openness both for international cooperation and for organizing external information influences of various nature, including destructive one. Intentions to organize such influences are declared and legally fixed in the functional purpose of actors of international politics. In the article, an analytical review of the methodological basis of information impact is presented; an analysis of the possibilities for its organization with the aim of destabilizing the political process is carried out.

Keywords: information space, information impact, national security, information security, political process, policy actor, subject of information impact.

Петрищев Евгений Викторович – сотрудник Академии Федеральной службы охраны Российской Федерации, адрес: 302034, Россия, г. Орел, ул. Приборостроительная, д. 35; e-mail: petrishev7@yandex.ru

Глобальная информатизация общества, обусловленная стремительным развитием телекоммуникационных технологий, является неоспоримым фактом. Среди прочего она привела к беспрецедентному расширению возможности доступа индивидов и социальных групп к широкому спектру информационных ресурсов в кратчайшие временные сроки. Сеть Интернет стала неотъемлемой частью всех сфер деятельности человека и общества, государственных институтов, организаций и ведомств. В итоге как получение, так и распространение информации в современном обществе вышли на новый качественный уровень. Свободное распространение информации повышает информирование общества и субъектов политики, что может вызывать усиление социальной активности граждан и, как следствие, служить сугубо созидательным целям повышения эффективности общественных и государственных институтов[1].

В то же время распространители информации, руководствуясь собственными целями, имеют возможность оказывать деструктивное воздействие на политический процесс, что актуально как для российского политикума, так и для системы международных отношений. Способы и методы ведения деятельности такого рода традиционно выступают предметом исследования политической науки.

В научных оценках отмечается, что глобальная информатизация общества, обусловленная стремительным развитием телекоммуникационных технологий, сопровождается определенными изменениями как в доведении, так и в потреблении информации. Оперативность доведения информации до целевой аудитории существенно возросла. Как следствие, глобальная телекоммуникационная сеть (ГТКС) Интернет стала не только средством общения, но и мощнейшим средством воздействия не только на функциональные, но и на информационно-психологические компоненты политического процесса[2].

Распространение мнений, взглядов, в том числе экстремистского и деструктивного характера, вышло на новый качественный уровень. Как подчеркивает Д.Л. Цыбаков, глубокое обоснование имеет тезис о доминировании «двойных технологий» в производственной и информационной сферах[3]. Информационные ресурсы – сайты, страницы социальных сетей, службы видео- и радиотрансляций – используются частными лицами, а равно коммерческими и ведомственными структурами зачастую в целях, существенно отличающихся от провозглашаемых. Вербовка в ряды организаций экстремистской направленности, дестабилизация политического процесса за счет информационных вбросов – лишь малая часть из обширного списка вызовов национальной безопасности.

Большинство развитых государств, понимая и адекватно оценивая возможности, предоставляемые ресурсами ГТКС «Интернет» по оказанию воздействий на идейно-политические предпочтения и массовое сознание граждан, организуют и ведут в информационном пространстве интенсивную и разноплановую деятельность, содержание которой требует дальнейшей научной типологизации[4]. Согласно авторскому подходу, выделив в качестве основного ее критерия степень активности субъектов политики и политического управления в информационном пространстве, виды их деятельности могут

[1] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. [Электронный ресурс], http://www.garant.ru (Дата обращения: 24.04.2017.)

[2] Каштанов С. А. Влияние информационных технологий на политический процесс // Вестник Саратовского государственного социально-экономического университета. – 2011. – № 4. –С. 173–176.

[3] Цыбаков Д.Л. Милитаризация общественных отношений: политическая природа, традиционные и современные формы. – Орёл: Издательство ОРАГС, 2007. – С.70.

[4] Манойло А.В. Государственная информационная политика в особых условиях: – М.: МИФИ, 2003. – С. 97–98.

носить активный, пассивный и полуактивный характер.

К пассивным/нейтральным видам деятельности в информационном пространстве относится мониторинг каналов международной системы электросвязи с целью добывания потенциально ценных сообщений. Основная задача ее субъектов – сбор информации.

Полуактивные виды деятельности в информационном пространстве связаны в первую очередь со сбором и обработкой информации от открытых источников и заключаются в выявлении потенциально информативных ресурсов с целью их последующего использования для удовлетворения информационных потребностей, заинтересованных акторов политики, включая высшее военно-политическое руководство. Особенностью информации от открытых источников применительно к сети «Интернет» является использование только документированных возможностей, не выходящих за пределы действий обычных пользователей[1]. Эффективность обеспечивается за счет комплексного подхода к выявлению источников информации. Необходимость формирования запросов к информационным ресурсам выводит вышеуказанные виды деятельности за рамки пассивных, при этом основной задачей остается сбор информации.

Активная деятельность, в свою очередь, неразрывно связана с понятиями «кибервойна» (Cyber Warfare), «информационные операции» (Information Operations), «информационная война» (Information Warfare) и предполагает воздействие как на информационные ресурсы, так и на узлы ГТКС «Интернет» для решения широкого спектра задач[2]. Некоторыми из них могут быть:

1. сбор информации, в том числе не относящейся к перечню доступной для свободного сбора и распространения (цель – удовлетворение информационного голода потребителей информации);
2. организация актов диверсии (саботажа) с целью разрушения информации или выведения из строя вычислительных (информационных) систем и сетей и их сегментов (цель – затруднение процесса обработки информации вплоть до коллапса всей системы государственного управления);
3. организация целенаправленного (информационного) воздействия на общество, социальную либо иную группу с целью корректировки (изменения) взглядов, мотиваций и устремлений (цель – дестабилизация социально-политического процесса).

Мероприятия, связанные с решением первых двух из вышеуказанных задач, в силу специфики их реализации отличаются низкой скрытностью, что позволяет в ряде случаев своевременно их выявить и организовать противодействие инициированным ими вызовам и угрозам международной или национальной безопасности. Механизмы обеспечения безопасности в таких случаях широко известны, описаны в теории информационной безопасности, являются преимущественно техническими либо организационными по своей природе. Что касается информационного воздействия, то оно вполне может быть организовано с высокой степенью скрытности[3]. Причем под скрытностью понимается не только сокрытие факта воздействия, но и его субъект и реальная цель. В комплексе с другими методами информационное воздействие становится источником вызовов и в ряде случаев угроз национальной безопасности Российской Федерации.

---

[1] ATP 2-22.9 Open-Source Intelligence, Army Techniques Publication, Headquarters, Department of Army 10.07. 2012. – P. 21 – 23.

[2] Stauffer, Don. “Electronic Warfare: Battles Without Bloodshed.” Futurist, January/February 2000, v. 34, no. 1 P.27.

[3] Вепринцев В., Манойло А., Петренко А., Фролов Д, Операции информационно-психологической войны. [Электронный ресурс], http://psyfactor.org/psyops/psyops4.htm (Дата обращения: 25.04.2017.).

Провозглашенная высшим руководством США глобальная война с терроризмом, принятие Патриотического Акта привели к переосмыслению принципов и методов информационного противоборства, включая организацию информационного воздействия.

Для лучшего понимания взглядов военно-политического истеблишмента США на информационное пространство и проводимые в нем операции, необходимо обратиться к документам, регламентирующим такого рода деятельность. Одним из них является публикация Объединенного комитета начальников штабов США «Информационные операции»[1], созданная на основе ряда источников. В их числе «Стратегия национальной безопасности», «План объединенного командования», «Деятельность разведки Соединенных Штатов» и т.д.

Являясь документом Объединенного комитета начальников штабов США, концепт «Информационные операции» представляет собой объединенную доктрину планирования, подготовки, проведения и оценки эффективности информационных операций, проводимых Вооруженными Силами как самостоятельно, так и совместно с иными государственными структурами США, в том числе на межнациональном уровне, и содержит основные термины и определения, определяет задачи информационных операций, предлагает методы и способы решения.

Информационное пространство, согласно доктринальным документам атлантических держав, это совокупность персон, организаций и систем, которые собирают, обрабатывают, распространяют информацию, либо воздействуют на нее. Это пространство состоит из трех взаимосвязанных измерений, непрерывно взаимодействующих с персонами, организациями и системами. Эти измерения – физическое, информационное и когнитивное (познавательное).

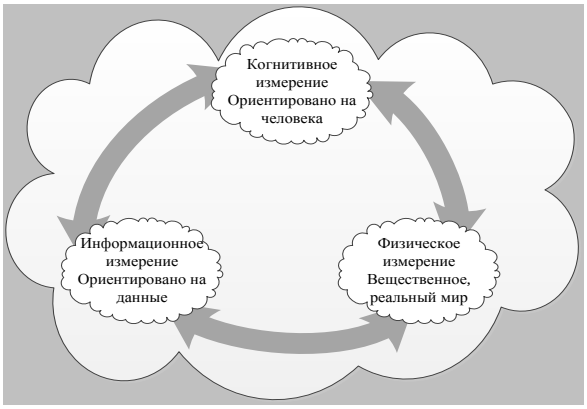


Рисунок 1 – Информационное пространство
Figure 1 – Information Space

В случае необходимости воздействия на любое из измерений и при отсутствии возможностей провести воздействие непосредственно целью может стать любое другое из трех. Взаимосвязанность измерений в большинстве случаев обеспечит успешное решение поставленных задач. Однако для обеспечения гарантированного достижения поставленной цели воздействие организуется в отношении всего информационного пространства.

[1] JP 3-13 Information Operations, Joint Publication, Joint Chiefs of Staff, 02.11.2014. – P.24.

Одним из ключевых понятий в области информационных операций является Information-Related Capabilities (IRC), что, основываясь на контексте, можно перевести как «информационно-зависимые возможности», ИЗВ (альтернативный термин – «Информационно-сопряженные возможности», ИСВ[1]) и подразумевает средства, методы и мероприятия, предназначенные для оказания воздействия на любое из измерений информационного пространства.

Методика организации информационного воздействия в общем случае представляется как совокупность определенных этапов.

Первый этап – определение целевой аудитории. Когда целевая аудитория определена, выявляется, каким образом целевая аудитория воспринимает свое окружение, в том числе определить нормы, правила и убеждения граждан, на основании чего вырабатывается перечень применимых методов воздействия. В числе методов дипломатические, информационные, военные, экономические действия, а также заявления по научным, коммерческим, религиозным и этническим вопросам.

Второй этап – воздействие на поведение индивидов и социальных групп посредством корректировки правил, норм и убеждений. Эффект такого рода может быть достигнут воздействием на то, как целевая аудитория получает, обрабатывает, воспринимает, распространяет и использует (или не использует) информацию.

Затем на основе данных о возможностях применения методов воздействия выбирается способ – убеждение либо принуждение[2].

Вышеизложенное наглядно дает понять, что воздействие рассматривается как комплекс взаимосвязанных способов, методов и средств, не ограниченных какой-либо одной сферой деятельности, и планируется исходя из оценки возможностей по всем возможным направлениям. Например, ограничение доступа к каналам получения информации техническими способами (физическое измерение) приведет к информационному дефициту, для удовлетворения которого можно воспользоваться другими каналами, находящимися под контролем субъекта информационной деятельности.

Оценка методических наставлений и рекомендаций по ведению информационных операций, опубликованных в США, показывает, что истинная цель информационного воздействия заключается во вмешательстве во внутренние дела суверенных государств. Весомым доказательством в пользу сделанного вывода служит идентификация противостоящей стороны, то есть тех объектов, на которые должен направляться вектор военно-информационного потенциала США и их союзников. В качестве идентификации противника в официальных документах используется преимущественно термин «оппозиционные силы» (в оригинале – adversary, враг, противник, оппонент). Из контекста изложенного можно сделать вывод, что вмешательство при помощи информационных технологий должно осуществляться во *внутренний* политический процесс, имея цель информационной, финансовой, военной и иной поддержки лояльных атлантическому курсу элитарных группировок.

Информационное воздействие на целевую аудиторию в ходе развития ситуации используется для корректировки сценария развития событий, при этом начальная фаза информационного воздействия по времени может не совпадать с начальной фазой ситуации. Напротив, информационное воздействие наряду с иными может начать осуществляться заранее. Причем возможности по организации и проведению успешного воздействия на

[1] Туляков О. Информационная война в планах Пентагона, Зарубежное военное обозрение.–2015.– № 11.– С.3 – 15.
[2] JP 3-13 Information Operations, Joint Publication, Joint Chiefs of Staff, – 20.11. 2014. – P.31.

ситуацию через целевую аудиторию меняются в зависимости от фазы ситуации.

Известный американский политик и эксперт Майкл Т. Флинн представил свое видение зависимости возможностей по оказанию воздействий и связанных с ними рисков от фазы развивающейся конфликтной ситуации[1].

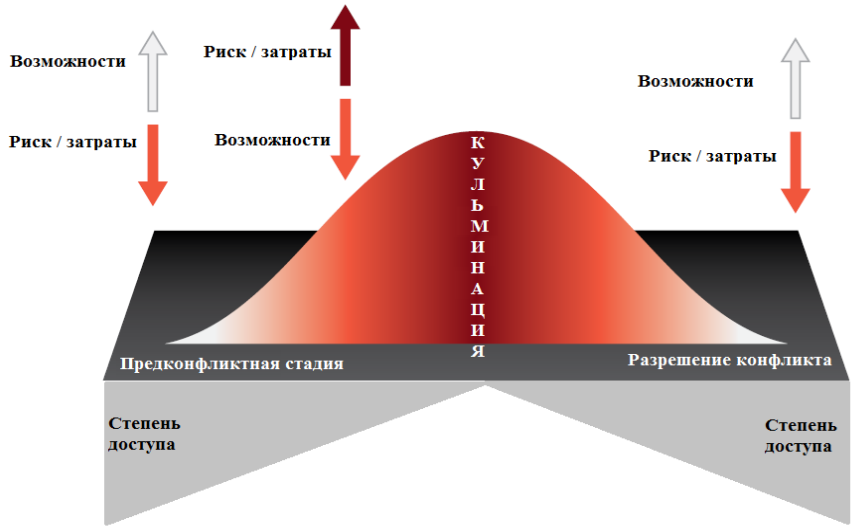


Рисунок 2 – Диаграмма зависимости возможностей и связанных с ними рисков от фазы развивающейся конфликтной ситуации

Figure 2 – Diagram of dependence of opportunities and risks associated with them from the phase of the developing conflict situation

Страна в наибольшей степени уязвима для внешних воздействий (в том числе информационных) в период до того, как конфликтная ситуация сложилась. Именно в этот период возможности существенно превышают затраты при минимальных рисках, что наиболее благоприятно для субъекта воздействия. Приближение течения конфликта к кульминации уменьшает это соотношение за счет одновременного снижения количества возможностей и повышения как затрат, так и рисков.

Стадии развития социальных и политических конфликтов подробно изучены в конфликтологии. Обычно выделяются три стадии (фазы):

1. Предконфликтная, в ходе этой фазы происходит вызревание конфликта.
2. Конфликтная, противостоящие стороны применяют все наличные средства для решительного навязывания своей позиции противнику, может протекать в форме восстаний, революций, гражданской войны.
3. Стадия разрешения, либо прекращения конфликта.

Ряд ученых выделяет более трех стадий, сценарии развития событий могут отличаться, тем не менее в различных конфликтах можно выявить схожие черты[2]. В контексте данной

[1] Flynn, M., Sisco, J. and Ellis, D., «Left of Bang» The Value of Sociocultural Analysis in Today`s Environment, Prism, 3(4) 2012. – P.38.

[2] Манойло А.В. Политические конфликты в международных отношениях и мировой политике //Журнальный клуб Интелрос. – 2013. – №2. [Электронный ресурс]. (http://www.intelros.ru/readroom/mir-i-politika/m2-

работы существенным является следующее соображение: еще до начала конфликта субъект воздействия обладает наибольшими возможностями по вмешательству в политический процесс при минимальных затратах и риске. Схожий вывод сделан в работе М. Флинна[1].

Ввиду вышеизложенного предлагается сформулировать основные способы разрешения социальных и политических конфликтов:

1. раннее обнаружение предпосылок конфликтов за счет анализа состояния общества;
2. институционализация конфликта;
3. формирование психологических установок на разрешение конфликта.

Все перечисленные способы тесно связаны со степенью информирования субъектов политического процесса как о потенциальных «точках напряженности» в обществе, так и о возможных действиях заинтересованной стороны по подготовке информационного и иного воздействия. Полученная информация должна быть использована для *оценки* вызовов и угроз с высокой степенью точности. Оценка информации становится фундаментом для принятия решений по противодействию вызовам и угрозам национальной безопасности. Все вместе это – цепочка зависимых событий, в том числе вероятностных, что в условиях информационного противодействия (например, при наличии интенсивного «информационного шума») и с учетом широкого ассортимента способов и методов, доступных для применения возможным противником, может привести к ошибкам как первого, так и второго рода на любом из этапов.

На основании вышеизложенного становится очевидной необходимость организации комплексного противодействия деструктивному внешнему воздействию на политическую стабильность Российской Федерации и ее национальные интересы в информационной сфере. Задачей экспертного сообщества, представленного как аналитическими структурами государственного управления, так и научными ассоциациями гражданского общества, в обозримом будущем будет оставаться выработка направлений и приоритетов совершенствования системы и методов обеспечения информационной безопасности личности, общества и государства.

Библиография/References:

1. Вепринцев В, Манойло А., Петренко А., Фролов Д. Операции информационно-психологической войны. – URL: http://psyfactor.org/psyops/psyops4.htm.

2. Каштанов С. А. Влияние информационных технологий на политический процесс // Вестник Саратовского государственного социально-экономического университета. – 2011. – № 4. – С. 173–176.

3. Манойло А.В. Государственная информационная политика в особых условиях. – М.: МИФИ, 2003.

4. Манойло А.В. Политические конфликты в международных отношениях и мировой политике // Журнальный клуб Интелрос. – 2013. – №2. – URL: http://www.intelros.ru/readroom/mir-i-politika/m2-2013/18205-politicheskie-konflikty-v-mezhdunarodnyh -otnosheniyah-i-mirovoy-politike.html.

5. Туляков О. Информационная война в планах Пентагона // Зарубежное военное обозрение. – 2015. – № 11. – С. 3–15.

2013/18205-politicheskie-konflikty-v-mezhdunarodnyh-otnosheniyah-i-mirovoy-politike.html). (Дата обращения: 24.04.2017.).

[1] Flynn, M., Sisco, J. and Ellis, D., «Left of Bang». P. 13–21.

6. Цыбаков Д.Л. Милитаризация общественных отношений: политическая природа, традиционные и современные формы. – Орёл: Издательство ОРАГС, 2007. – 168 с.
7. JP 3-13 Information Operations, Joint Publication, Joint Chiefs of Staff, 20.11. 2014.
8. ATP 2-22.9 Open-Source Intelligence, Army Techniques Publication, Headquarters, Department of Army, 10.07.2012.
9. Flynn, M., Sisco, J. and Ellis, D., «Left of Bang» The Value of Sociocultural Analysis in Today`s Environment, Prism, 3(4) 2012.
10. Stauffer, Don. "Electronic Warfare: Battles Without Bloodshed." Futurist, January/February 2000, v. 34, no. 1.

1. Veprintsev, V, Manoilo, A., Petrenko, A., Frolov, D, Operatsii informatsionno-psikhologicheskoi voiny [Operations of information-psychological warfare]. – URL: http://psyfactor.org/psyops/psyops4.htm. (In Russ.)
2. Kashtanov, S. A. (2011) Vliianie informatsionnykh tekhnologii na politicheskii protsess [The influence of information technology on the political process] // Vestnik Saratovskogo gosudarstvennogo sotsial'no-ekonomicheskogo universiteta [Vestnik of Saratov State Socio-Economic University]. – № 4. – P. 173–176. (In Russ.)
3. Manoilo, A.V. (2003) Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh [State information policy in special conditions]. – M.: MIFI. (In Russ.)
4. Manoilo, A.V. (2013) Politicheskie konflikty v mezhdunarodnykh otnosheniiakh i mirovoi politike [Political conflicts in international relations and world politics] // Zhurnal'nyi klub Intelros. – №2. – URL: http://www.intelros.ru/readroom/mir-i-politika/m2-2013/18205-politicheskie-konflikty-v-mezhdunarodnyh-otnosheniyah-i-mirovoy-politike.html. (In Russ.)
5. Tuliakov, O. (2015) Informatsionnaia voina v planakh Pentagona [Information war in the plans of the Pentagon] // Zarubezhnoe voennoe obozrenie. – № 11. – P. 3–15. (In Russ.)
6. Tsybakov, D.L. (2007) Militarizatsiia obshchestvennykh otnoshenii: politicheskaia priroda, traditsionnye i sovremennye formy [Militarization of public relations: political nature, traditional and modern forms]. – Orel: Izdatel'stvo ORAGS. – 168 p. (In Russ.)