ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА КРИТИЧЕСКИ ВАЖНЫХ СТРУКТУР

Евгений ОГНЕВ

аспирант кафедры национальной безопасности РАГС

Приоритетное направление деятельности государства как генерального субъекта в формировании информационного общества – обеспечение безопасности его информационной сферы [1] , от состояния которой зависит экономическая, политическая, военная мощь страны, степень развитости производительных сил и общественных отношений и в целом – положение в мировом сообществе государств. Эти факторы определяют и вектор действий в мировом политическом процессе, имеющем, как производное от политики, информационно-коммуникативную основу. Так, К. Дойч, характеризуя политическую систему, отмечал, что возникающие в процессе общения информационные потоки позволяют коммуникативным субъектам выполнять политические роли и функции по распределению ресурсов и полномочий власти [2].

Анализ основных источников угроз национальной безопасности также указывает на их информационную природу: семантическую, семиотическую, лингвистическую, когнитивную, массово-коммуникативную. Эти признаки проявляются как во внешних, так и во внутренних угрозах, например в недобросовестном использовании информационных ресурсов в государственном управлении (проблема инсайдерской информации, представляющая угрозу интересам государства в экономической сфере), разведывательной деятельности специальных служб и организаций иностранных государств, действиях террористических и экстремистских группировок и структур и т.д.

Определяя информационную безопасность государства как невозможность нанесения вреда (ущерба) свойствам объекта безопасности, обусловленным информацией и информационной инфраструктурой [3], обозначим последние как факторы субъективного порядка. К таким компонентам, воздействующим на информационную безопасность государства, относится деятельность его критически важных объектов (КВО). Это системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность. К ним традиционно относят и органы государственного управления, имеющие своей основой информацию как совокупность сведений, данных, фактов, характеристик о какомлибо предмете, явлении, процессе, отношении и т.д., систематизированную в соответствии с поставленной задачей [1, 4].

По нашему мнению, в этом перечне должны находиться национальные системы массовой политической информации и коммуникации, а также производные от них (или произведенные ими) информационно-коммуникативные продукты, представленные в виде общественного мнения. Поясним свою позицию.

В государстве как иерархической системе органы государственного управления занимают высший уровень, на котором осуществляется целеполагание и принятие управленческих решений. Они же и наиболее уязвимы при формировании угрозы потери устойчивости сложной системы. Эти органы имеют критические нормы информационного насыщения или информационный потенциал, от распределения мощи которого зависит обеспечение безопасности управляющих подсистем. Опасность для существования системы может исходить как от внешней среды (информационное воздействие извне), так и изнутри, когда нарушаются основополагающие принципы истока и генерации власти.

Массовая информационно-коммуникативная подсистема политической системы государства, представленная средствами массовой информации и коммуникации, является одновременно механизмом интерактивной коммуникации между властью, политической и экономической элитой и обществом, а также инструментом информационно-психологического воздействия как на индивида, так и на информационно-политические отношения общества в целом. Она занимает верхний подуровень критически важной структуры. Ее продукт – общественное мнение, выполняющее функции актора в государственно-гражданских отношениях, одновременно влияющее как на властные структуры, так и на средства массовой информации и массовой коммуникации.

Основными информационными угрозами для информационно-коммуникативных ресурсов критически важных объектов являются: отсутствие четко сформулированной идеологии государственного строительства, отвечающей национальным целям, ценностям и интересам; размытость правового и политического пространства реализации государственной власти; разрушение целостного информационного и духовного пространства России.

В соответствии с информационным подходом, кроме традиционно понимаемых компонентов, составляющих триаду «источник-канал-приемник», отнесем к компонентам, формирующим свойства критически важных объектов, сознание (метасознание), психосемантическое и информационное поле [5]. Тогда в число угроз информационной устойчивости политической системе Российского государства войдут информационные угрозы, выраженные в недостоверности и неполноте сообщений (слухи); в информации, возбуждающей социальную, расовую, национальную, религиозную ненависть или вражду; призывы к войне, к свержению политического режима и конституционного строя; в пропаганде ненависти, враждебности и превосходства, бездуховности; сообщения, содержащие посягательство на честь, доброе имя и деловую репутацию людей и организаций; недобросовестная реклама; информация, оказывающая деструктивное воздействие на психологию людей; антироссийская пропаганда, дискредитация российской истории и институтов власти; отсутствие социального контроля за деятельностью власти и т.д. Манипулирование сообщениями на общественном сознании при критическом несовпадении целей генерализованного субъекта управления представляет угрозу устойчивости и целостности объекта управления, формирует основной показатель критичности безопасности – доверие легитимным органам власти.

Иными словами, главным объектом информационно-психологического воздействия на критически важные структуры является общественное мнение, содержащее определенные элементы угроз стабильности органов власти в виде их делегитимации. Таким образом, можно сделать вывод о том, что средства массовой информации и коммуникации, как обладающие свойствами существенного воздействия на состояние верхнего уровня системы обеспечения информационной безопасности, должны быть отнесены к разряду критически важных структур в системе национальной безопасности государства. На них следует распространить те же принципиальные подходы к обеспечению защиты, что и на иные КВО. Информационная политика в области обеспечения информационной безопасности политической системы должна быть ориентирована на достижения понимания и ответственности между всеми участниками информационно-коммуникативных взаимодействий в политической сфере, прежде всего органов государственной власти и средств массовой информации и коммуникации.

Справедливо ожидание подобного понимания проблемы и вследствие реализации принятой почти год назад Стратегии национальной безопасности Российской Федерации до 2020 года, содержащей систему стратегических приоритетов, целей и мер в области внутренней и внешней политики, от которых зависят состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу.

Обеспечению безопасности критически важных структур прямо или косвенно посвящены практически все главы раздела IV «На-

циональная безопасность» Стратегии. Содержание раздела V «Организационные, нормативные правовые и информационные основы реализации настоящей Стратегии» раскрывает принципы обеспечения национальной безопасности РФ (п. 97), содержит описание формализованных механизмов организации, а также правовых, информационных и информационно-аналитических средств поддержки реализации настоящей системы национальной безопасности. Так, в п. 109 прямо декларируется: «Угрозы информационной безопасности в ходе реализации настоящей Стратегии предотвращаются за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности» [6].

Для оценки состояния национальной безопасности Стратегия предписывает использовать следующие характеристики: уровень безработицы; децильный коэффициент; уровень роста потребительских цен; уровень государственного внешнего и внутреннего долга в процентном отношении от валового внутреннего продукта; уровень обеспеченности ресурсами здравоохранения, культуры, образования и науки в процентном отношении от валового внутреннего продукта; уровень ежегодного обновления вооружения, военной и специальной техники; уровень обеспеченности военными и инженерно-техническими кадрами. Как видно, собственно информационной безопасности, не говоря уж о системе массовой информации и коммуникации, в Стратегии уделено недостаточно внимания. Лишь один из показателей – уровень обеспеченности ресурсами здравоохранения, культуры, образования и науки в процентном отношении от валового внутреннего продукта может опосредованно характеризовать состояние системы СМИ и МК.

Однако именно от эффективной деятельности системы этих институтов как критически важных структур зависит информационно-психологическая безопасность и нормальное функционирование социально-политических акторов. Ведь общественное сознание и массовая психика являются главными объектами информационно-психологического воздействия в процессе политического обмена, содержащего определенные элементы угроз легитимности государственной власти. При этом они наиболее восприимчивы к такого рода воздействиям, а следовательно, и наиболее уязвимы для информационно-политических угроз.

Таким образом, с позиций информационного подхода основными объектами обеспечения безопасности критически важной структуры являются: а) собственно управленческая информация; б) лица, принимающие властные решения; в) деятельность средства массовой информации и коммуникации; г) общественное мнение как отражение состояния общественного сознания объекта управления.

Концентрация управленческой информации, получаемой на основе переработки массовой информации посредством прямых и обратных связей в контурах циркуляции власти, усиливает позиции органов управления, государственного аппарата в сравнении с политическими силами, не обладающими таковым информационным ресурсом, а равно и наоборот. Недостаточное внимание к социально-коммуникативной основе власти может привести к нарушению функций управляющих органов, ухудшению качества самого управления, а в перспективе – к перерождению государства как системы

Литература

1. *Федоров А.В., Цыгичко В.Н.* Информационные вызовы национальной и международной безопасности. М., 2001.
2. *Дойч К.* Нервы управления: модели политической коммуникации и контроля. М., 1993.
3. *Стрельцов А.А.* Обеспечение информационной безопасности России: теоретические и методологические основы. М., 2009.
4. *Шевченко А.В.* Управление безопасностью информационных процессов. М.: Изд-во РАГС, 2009.
5. *Полонников Р.И.* Информационный подход к нестареющему парадоксу психофизических явлений. СПб.: «Анатолия», 1997.
6. Стратегия национальной безопасности Российской Федерации до 2020 года // Российская газета. 2009. 19 мая.

SUMMARIES

It is our duty to celebrate Victory Day properly (p. 4)

Legal support for regulation of conflict of interest (p. 6)

Gulnara Sergeeva, Deputy Chairman of the Russian State Duma Committee for Federation Affairs and Regional Policy, Candidate of Sciences (Political science) (mgs@ur.rags.ru/~sergeeva)

Summary: If the fight against corruption is to be successful, reliable mechanisms should be created to verify compliance with the public service code of practice and anticorruption standards should be introduced. These will allow to prevent and resolve conflicts of interest. Corresponding amendments to the Law on Public Service as well as measures aimed to eliminate indirect vested interest of public officials are in preparation.

Keywords: corruption; anticorruption standards; conflict of interest.

Samara region: comfort for the investor (p. 11)

Samara Region Governor **Vladimir Artyakov's** presentation of the region's investment projects at a meeting of the Expert Council for Regional Investment Policy of the Ministry of Regional Development of the RF.

* При отправке почты на электронные адреса формата *mgs@ur.rags.ru/~someone*, указывайте *mgs@ur.rags.ru* в поле «адрес» и */~someone* в поле «тема».

The ruble can become an international brand (p. 14)

Alexander Pankrukhin, Research Advisor of the Guild of Experts in Marketing, Doctor of Economics, Professor, RAPA Chair of Management (pankr@ur.rags.ru)

Sergey Sorokoumov

Summary: The ruble can only become a regional reserve currency when it is a stable, readily convertible monetary unit backed by highly liquid assets. The state should generate a constantly growing demand for rubles in world trade, particularly for energy exports. Society should foster the same attitude of the Russian citizens to the national currency as to the national coat of arms, flag and anthem.

Promotion in the name of development (p. 17)

State objectives and plans of the Russian Register (p. 19)

Valery Perevalov. A meeting in RAPA to discuss reorganization of the Federal Service of State Registration, Land Register and Mapping.

Problems of improvement of legal regulation of state civil service (p. 23)

Rizvan Kurbanov, doctoral candidate, RAPA (mgs@ur.rags.ru/~kurbanov)

Summary: The article analyzes the problems associated with the functioning of state civil service, suggests ways of their legislative solution through the legal provision of this type of activity.

Keywords: state civil service; legislation; organ of state power; legal act.