

Матвеев Евгений Александрович

аспирант Санкт-Петербургского государственного университета

НЕКОТОРЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНА**Аннотация:**

Статья посвящена политике обеспечения информационной безопасности субъектов Российской Федерации в современных условиях. Определено значение информационной безопасности в соответствии со стратегическими основаниями российской политики в области информатизации российских регионов. Проанализированы базовые аспекты создания системы информационной безопасности региональной информационно-политической системы. Рассмотрены эффективные принципы и пути интеграции негосударственных акторов в процесс создания системы информационной безопасности региона.

Ключевые слова:

информационная безопасность, региональная подсистема, информатизация, национальные интересы, сетевая политика, бенчмаркинг.

Matveev Evgeny AleksandrovichPhD student,
Saint Petersburg State University**SOME IMPLEMENTATION ASPECTS OF INFORMATION SECURITY POLICY OF REGION****Summary:**

The article looks at information security policy of the constituent entities of the Russian Federation in the current context. The author identified the information security meaning in accordance with strategic basis of the Russian policy concerning informatization of Russian regions. The paper analyzed the basic aspects to create the information security of the regional information and political system. The research considered the effective principles and the ways of integration of non-state actors into the process of creating the regional information security system.

Keywords:

information security, regional subsystem, informatization, national interests, network policy, benchmarking.

Развитие политической системы Российской Федерации на современном историческом этапе во многом определяется процессами глобального информационного обмена и совершенствования информационно-коммуникативных технологий. Информатизация систем административно-политических отношений, развитие сетевого общества, всесторонняя демократизация и появление новых акторов общественно-политических процессов в киберпространстве выступают факторами, оказывающими особое влияние на национальную безопасность страны.

Одним из наиболее значительных направлений политики национальной безопасности является обеспечение информационной безопасности (ИБ), представляющей особое состояние информационных ресурсов, технологий и систем коммуникаций, позволяющее формировать их создание и эксплуатацию в процессе функционального (целенаправленного) использования в интересах общегосударственной системы, общества в целом и индивида в информационном пространстве отдельного государства, систем межгосударственного взаимодействия, виртуального пространства (интернета) [1, с. 26]. Федеративный характер устройства России обуславливает необходимость создания многоуровневой системы обеспечения ИБ, предполагающей становление общефедеральной системы ИБ, состоящей из региональных подсистем.

С нормативной точки зрения вопросы развития системы ИБ как одной из фундаментальных основ современной российской информационно-политической сферы определяются рядом стратегических оснований (Стратегией национальной безопасности, Доктриной информационной безопасности и т. д.), где общефедеральные государственные институты выступают основной движущей силой развития системы ИБ. По нашему мнению, эффективные региональные системы обеспечения ИБ в перспективе могут выступить фундаментальной основой действенной и стабильно функционирующей общегосударственной системы ИБ.

К настоящему моменту времени ключевым документом, определяющим значение регионов в становлении государственной системы ИБ, является «Концепция региональной информатизации до 2018 года» [2]. Основными целями, стоящими перед российской политической системой, являются выравнивание уровня развитости информационного общества в разных субъектах Федерации; создание эффективно функционирующей системы государственного и муниципального управления, основанной на использовании передовых ИКТ (информационно-коммуникативных технологий); формирование современной региональной ИКТ-инфраструктуры как основы общегосударственной информатизации. Формирование и развитие критически важной инфраструк-

туры попадает в сферу ответственности государства, что, по нашему мнению, ограничивает возможную вовлеченность негосударственных акторов в процесс создания условий для общефедеральной и региональной информатизации. Вопросы ИБ в данном документе рассматриваются с сугубо технической точки зрения: уделяется внимание использованию программных и аппаратных средств борьбы с вредоносным программным обеспечением, предоставлению целостной и доступной информации. Определяется необходимость соотношения региональных стандартов защиты информации со стандартами, определяемыми федеральным законодательством.

Без всякого сомнения, предмет ИБ существенно шире, нежели решение сугубо технической стороны вопроса относительно информационного обеспечения компонентов федеральной и региональной политических систем. С точки зрения стратегических оснований российской национальной безопасности техническое обеспечение процессов информатизации является одним из слагаемых системы национальных интересов, которые, как было отмечено выше, должны находиться в состоянии конвергенции с региональными интересами в политико-информационной сфере. В связи с этим представляется целесообразным обратить внимание на возможные направления развития региональных систем ИБ и информатизации в политической перспективе.

Обратимся к анализу результатов одного из наиболее обстоятельных исследований в области проектирования системы региональной ИБ в современной российской политической науке. По мнению Д.П. Кафтаникова, к базовым компонентам региональной системы обеспечения ИБ относятся следующие [3, с. 158–159]:

- Орган, управляющий процессом информатизации (институт исполнительной власти Российской Федерации в административно-политической системе региона). На данный институт возлагаются функции управления функционированием системы ИБ, разработки нормативно-правовых стандартов функционирования системы, правового воздействия на многочисленных субъектов данной системы посредством права на законодательную инициативу.

- Фонд информатизации (институт, курирующий экономическую сторону данной системы). Такой фонд может представлять собой государственную некоммерческую организацию, исполняющую функции «генерального заказчика» в области создания средств информатизации в рамках освоения регионального бюджета.

- Социальная подсистема обеспечения ИБ, интегрирующая бизнес-структуры и НКО, общественные организации и объединения, способные эффективно воздействовать на реализацию национальных и региональных интересов в системе информационно-политических отношений в кооперации с административно-политическими институтами.

Автор обозначает данные аспекты развития системы региональной ИБ, одновременно отвечающей требованиям стратегических оснований национальной безопасности России и интересам в информационной сфере абстрактно взятого субъекта Федерации. Особое значение, по нашему мнению, имеет функционирование социальной подсистемы, агрегирующей так называемых «новых» акторов политического процесса, политические и экономические интересы которых в последнее время все чаще артикулируются в виртуальном (кибернетическом) измерении.

Роль данных акторов (представляющих так называемый «частный сектор») особенно важна в контексте развития современной инфраструктуры ИКТ и обеспечения безопасности в киберсфере. Актуален вопрос соотношения интересов институтов власти и участников рынка ИКТ, обеспечивающих существенные инвестиции в развитие информационных отношений и, следовательно, влияющих на состояние критической инфраструктуры государственной информатизации, что обуславливает необходимость «вмешательства» государства в данный сегмент рыночных отношений» [4, р. 14].

По нашему мнению, эффективное и конструктивное взаимодействие государственных и негосударственных акторов в области развития региональных систем ИБ возможно при соблюдении ряда современных принципов развития политического процесса. К таким принципам резонно отнести построение матричных структур, функционирование которых обеспечивает модификацию иерархических отношений в сетевые отношения, что, в свою очередь, обеспечивает горизонтальное движение информационных потоков. В общеполитическом смысле данной модели взаимодействия участников информационно-политического процесса происходит ускоренное движение информации, стирание барьеров между бюрократическими институтами, экспертным сообществом и многочисленными институтами гражданского общества (НКО, представителей коммерческих структур) [5, с. 148]. Построение сетевого взаимодействия участников информационно-политического процесса в условиях формирования региональной системы ИБ является перспективной моделью политической кооперации по принципу государственно-частного партнерства.

В рамках анализа проблемы взаимодействия государственных институтов как основных акторов построения региональной системы ИБ и негосударственных акторов, потенциально заинтересованных в развитии информационно-политического процесса, особую актуальность приобретает механизм «бенчмаркинга», являющегося одной из форм «современного участия» гражд-

данского общества в политико-административном управлении [6, с. 65]. В политические отношения данный механизм пришел из экономики и может быть охарактеризован как ориентация деятельности одной организации на реальные достижения и стратегические ходы другой организации, где вторая является «эталон» и ориентиром.

Бенчмаркинг может быть рассмотрен в качестве первичного звена информационной безопасности системы (коммерческой, политико-административной системы) [7, с. 45]. Исследовательский интерес к данной технологии вызван «разведывательными» возможностями, которые предлагает бенчмаркинг. Координация политики актора относительно поставленных целей (применительно к созданию региональной системы ИБ – анализ вероятных источников угроз, мониторинг актуальных форм взаимодействия субъектов информационно-политических отношений) позволяет принимать эффективные управленческие решения, независимо от статуса контрагентов (конкурентов/сотрудников).

Итак, информационно-политические системы государств подвергаются значительным рискам в условиях становления информационного общества и возрастания скорости движения информации. В данном контексте актуализируется проблематика обеспечения информационной безопасности и развития информатизации государства как фундаментальных слагаемых обеспечения национальной безопасности.

Федеративная модель устройства России обуславливает потребность в создании эффективной системы обеспечения ИБ, основанной на политике региональной информатизации и разработке систем обеспечения ИБ компонентами региональных политических систем. Крайне существенным аспектом создания региональных систем ИБ является использование современных сетевых механизмов государственно-частного партнерства и технологии бенчмаркинга.

Ссылки:

1. Стратегический вектор обеспечения международной информационной безопасности : сборник / сост. М.А. Вус, О.С. Макаров ; авт. предисл. чл.-кор. РАН Р.М. Юсупов. СПб., 2016. 122 с.
2. Концепция региональной информатизации до 2018 года [Электронный ресурс] : утв. распоряжением Правительства Российской Федерации от 29 дек. 2014 г. № 2769-р. URL: <http://government.ru/media/files/Ea8O35fPr3l.pdf> (дата обращения: 10.03.2017).
3. Кафтanchиков Д.П. Информационная безопасность регионов Российской Федерации: современное состояние и приоритеты обеспечения : дис. ... канд. полит. наук. Орел, 2009. 181 с.
4. Brangetto P., Aubyn M.K.-S. Economic aspects of national cyber security strategies // Brangetto P., Aubyn M.K.-S. Economic Aspects of National Cyber Security Strategies : project report. Annex 1. Tallinn, 2015. P. 9–16.
5. Курочкин А.В., Шерстобитов А.С. Политика и государственное управление в условиях сетевого общества. СПб., 2012. 151 с.
6. Парфенова Ю.В. Новые формы политического участия в условиях общества, основанного на знании // Вестник Санкт-Петербургского университета. Серия 6. Политология. Международные отношения. 2016. № 2. С. 63–71.
7. Баранников А.Л., Равкин В.Н., Силин В.В. О применении технологий бенчмаркинга (корпоративной разведки) в менеджменте организации // Экономика, статистика и информатика. Вестник УМО. 2014. № 6. С. 42–46.

References:

- Barannikov, AL, Ravkin, VN & Silin, VV 2014, 'On the application of benchmarking (corporate intelligence) technology in the management of the organization', *Ekonomika, statistika i informatika. Vestnik UMO*, no. 6, pp. 42–46, (in Russian).
- Brangetto, P & Aubyn, MK-S 2015, 'Economic aspects of national cyber security strategies', *Brangetto P., Aubyn M.K.-S. Economic Aspects of National Cyber Security Strategies: project report. Annex 1*, Tallinn, pp. 9–16.
- Kaftanchikov, DP 2009, *Information security of the Russian Federation regions: the current state and priorities of provision*, PhD in Political Science thesis, Oryol, 181 p., (in Russian).
- Kurochkin, AV, Sherstobitov, AS 2012, *Politics and public administration in a network society*, St.-Petersburg, 151 p., (in Russian).
- Parfenova, YuV 2016, 'New forms of political participation in the context of a network society based on knowledge', *Vestnik Sankt-Peterburgskogo universiteta. Seriya 6. Politologiya. Mezhdunarodnyye otnosheniya*, no. 2, pp. 63–71, (in Russian).
- Vus, MA, Makarov, OS (comps.) & Yusupov, RM 2016, *Strategic vector of international information security*, St.-Petersburg, 122 p., (in Russian).