УДК 004.056

Современные подходы к исследованию информационной безопасности в российском политологическом дискурсе

Матвеев Евгений Александрович

Аспирант,
факультет политологии,
Санкт-Петербургский государственный университет,
199034, Российская Федерация, Санкт-Петербург,
Университетская набережная, 7/9;
e-mail: matveev.spb@mail.ru

Аннотация

В статье рассмотрены ключевые подходы к исследованию информационной безопасности в современном российском политологическом дискурсе: подход к исследованию информационной безопасности в рамках теории национальной безопасности, системный подход к исследованию информационной безопасности. Феномен информационной безопасности проанализирован в общем научном контексте теории национальной безопасности. Анализируются наиболее значимые тенденции и факторы, влияющие на обеспечение информационной безопасности в условиях процесса суверенизации информационного пространства. Определены методологические принципы системного подхода к исследованию информационной безопасности. Проанализированы основные этапы и структурные компоненты политики обеспечения информационной безопасности в рамках использования системного подхода в контексте ведения информационных войн и организации информационного противоборства. Обозначены сходства и различия данных подходов. Обосновывается целесообразность научного применения обоих методологических подходов в современных условиях.

Для цитирования в научных исследованиях

Матвеев Е.А. Современные подходы к исследованию информационной безопасности в российском политологическом дискурсе // Теории и проблемы политических исследований. 2016. Том 5. № 6А. С. 164-173.

Ключевые слова

Информационное общество, информационная политика, информационная безопасность, национальная безопасность, информационный суверенитет, системный подход.

Введение

XXI век ознаменован рядом тенденций, кардинальным образом воздействующих на современные государства и общества. Мы являемся свидетелями развития информационного общества и «общества знаний», процессов всесторонней глобализации, формирования глобальной инфраструктуры технологических нововведений [Дементьева, 2010, 61]. Обратной стороной данных процессов является виртуализация социально-экономических и политических процессов, рост международного терроризма, возрастание многочисленных угроз сетевого и информационного характера. Данные тенденции выступают важнейшими предпосылками обеспечения информационной безопасности государства и общества.

В современной российской науке информационная безопасность понимается как состояние защищенности общественной информационной среды, соответствующей общественным интересам, интересам государства и отдельно взятого индивида. Данное состояние характеризуется постоянным формированием, функционированием и развитием, независимо от влияния как внешних, так и внутренних угроз информационного характера [Самыгин, Руденко, Котлярова, 2016, 49].

Тем не менее, мы считаем, что такой подход неспособен как раскрыть реальную сущность проблематики информационной безопасности, так и не отвечает запросам со стороны современных тенденций развития научного политологического знания. Однако в современном российском политологическом дискурсе сформировались два основных подхода к исследованию информационной безопасности, которые являются наиболее релевантными современным условиям.

Исследование информационной безопасности в рамках теории национальной безопасности

Вопросы осмысления современных глобальных политических и информационных процессов являются неотъемлемой частью современной теории национальной безопасности. Национальная безопасность, отмечает И.В. Радиков, в самом общем виде представляет собой единство трех ключевых компонентов: национального выживания, национального благополучия и национального развития. В этой связи необходимо сделать существенное методологическое замечание: значение категории «безопасность» не может быть сведено к категории «защищенность»; обеспечение национальной безопасности – это процесс, разделяемый на два фундаментальных направления. К первому относится противостояние конкретным опасностям и угрозам объекта (нации, как и любого другого актора). Ко второму направлению относится утверждение безопасности как процесса укрепления и развития объекта (природы объекта) [Радиков, 2007]. В данном контексте обеспечение информаци-

онной безопасности представляет собой целенаправленное действие, находящееся в структуре реализации обоих направлений обеспечения национальной безопасности.

В российском научном дискурсе довольно часто встречаются альтернативные точки зрения. Например, в условиях развития информационного общества и стремительного возрастания значения и ценности информации, информационная безопасность и национальная безопасность отождествляются. Более того, предметное поле информационной безопасности в категориальной структуре политической науки оказывается шире, чем смысловые компоненты категории национальной безопасности [Марков, 2011, 44]. Мы согласимся с А.А. Марковым относительно некорректности данных тезисов, противоречащих современным реалиям развития информационного общества как в мировом масштабе, так и в масштабе Российской Федерации.

Информационная безопасность, выступая слагаемым компонентом теории национальной безопасности, представляет собой особое политическое направление, реализация которого первостепенно попадает в сферу ответственности государственной системы. Стратегическими источниками основ реализации данного направления государственной политики являются следующие документы общефедерального значения.

1) Стратегия национальной безопасности Российской Федерации до 2020 г. (документ, нормативно закрепляющий обеспечение информационной безопасности как направления политики национальной безопасности).

2) Доктрина информационной безопасности Российской Федерации (документ, определяющий условия, цели, задачи, ожидаемые результаты политики информационной безопасности).

В научной литературе встречаются тезисы о том, что наличие данных стратегических документов является свидетельством формирования нормативного подхода к определению информационной безопасности в современном российском обществе [Владимирова, 2013]. По нашему мнению, нормативный подход в данном контексте необходим для анализа стратегических документов как объективированной и концентрированно выраженной воли российской политической элиты в области реализации политики национальной безопасности и информационной политики государства. Отметим, что с точки зрения видного отечественного политолога И.Н. Панарина, именно политическая элита выступает ключевым актором обеспечения информационной безопасности и реализации интересов граждан, государства, государственной информационной среды [Панарин, 2015].

Существенной составляющей исследования информационной безопасности в рамках теории национальной безопасности является способность субъектов информационно-политических процессов максимально объективно оценивать ключевые факторы и угрозы (информационно-политические тренды), влияющие на государственное информационное пространство. К таковым трендам Т.В. Владимирова относит перемещение угроз национальной и государственной безопасности в киберпространство (пространство виртуальной реаль-

ности); наличие, отсутствие, устаревание информации как основы развития рисков и угроз для общественной системы в условиях возрастания интенсификации потоков информации [Владимирова, 2013, 36]. Способность субъекта информационной безопасности ориентироваться в развитии данных трендов (соответственно, адаптироваться к данным трендам) автор называет «знанием», которое «является элементом базовой методологии для выявления, прогнозирования угроз государственной безопасности» [Владимирова, 2013, 39].

Важнейшая для теории национальной безопасности категория «суверенитет» приобретает принципиально новое значение в условиях роста динамичности информационных потоков и развития информационного общества. Информационный суверенитет представляет собой «…верховенство и независимость государственной власти при формировании и реализации информационной политики. Верховенство реализуется в национальном сегменте, а независимость — в глобальном информационном пространстве», пишет М.М. Кучерявый [Кучерявый, 2015, 14]. К составляющим компонентам информационного суверенитета автор относит следующие.

1) «Цифровой» суверенитет (совокупность технических средств связи и коммуникаций преимущественно ответственного производства и национального сегмента интернета).

2) «Ментальный» суверенитет (уровень информационной культуры, разработанность национальной идеи и др.).

3) «Властный» суверенитет (рациональная информационная политика, устойчивость национальной валюты и т. д.).

Политика государственного информационного суверенитета должна развиваться в следующих направлениях: определение информационных интересов государства и создание актуальной нормативно-правовой базы; технологическая суверенизация государства, предполагающая создание собственных средств связи и коммуникаций; формирование информационных войск, призванных осуществлять информационное противоборство на международной арене; контроль внешних и внутренних информационных потоков. Отметим, что сама категория «информационного суверенитета» является сравнительно новой для отечественной политической науки и, вероятно, может стать объектом научных дискуссий, что повлияет на концептуальное наполнение и дальнейшее научное осмысление термина.

Невзирая на безапелляционную научную состоятельность теории национальной безопасности в современной российской политической науке, теория информационной безопасности, как структурный компонент обеспечения национальной безопасности, находится на стадии формирования, что открывает обширные научные перспективы перед современным политологическим сообществом. Декларативный характер некоторых тезисов данного теоретического направления в условиях необходимости практической реализации политики информационной безопасности может быть дополнен и/или компенсирован использованием системного подхода к анализу информационной безопасности.

Системный подход к исследованию информационной безопасности

Системный подход к исследованию информационной безопасности акцентирует внимание на взаимозависимости информационного пространства комплексных и многосоставных образований (государства, общества) и непрерывного процесса развития современных высоких технологий. Е.И. Жук отмечает, что «системный подход к информационной безопасности требует определения ее субъектов, средств и объектов, источников опасности, направленности опасных информационных потоков и принципов обеспечения информационной безопасности» [Жук, 2010].

Политологическая экспликация данного подхода может быть представлена посредством последовательного соотнесения структурных компонентов данной модели с элементами информационно-политической системы государства. Объектами информационного влияния выступают, с одной стороны, морально-психологическое состояние как отдельного индивида, так и населения в целом; с другой стороны, информационно-техническая инфраструктура (совокупность информационно-технологических ресурсов) общества и государства. Субъектами информационной безопасности являются многочисленные акторы информационно-политического процесса (организации, институты), ключевой функцией которых является системное и рациональное обеспечение информационной безопасности. К средствам обеспечения информационной безопасности относятся конкретные механизмы и технологии, препятствующие влиянию потенциального источника опасности на состояние критической инфраструктуры государственно-политической системы.

Направленность негативных информационных потоков сопряжена с источником информационного воздействия на общественно-политическую систему. Источником такого негативного информационного воздействия может выступать как внутренний компонент системы, так и внешний субъект. В данном контексте качественные характеристики его видов аналогично будут зависеть от объектной направленности воздействия. На примере теории информационных войн данное положение резонно дополнить тезисом И.А. Крыловой: «Если главными объектами воздействия и защиты при информационно-технической борьбе являются информационно-технические системы (системы связи, телекоммуникационные системы, радиоэлектронные средства), то при информационно-психологической борьбе – психика политической элиты и населения противостоящих сторон, системы формирования общественного сознания, мнения, выработки и принятия решений» [Крылова, 2016, 58]. Как и в направлении исследования информационной безопасности в структуре национальной безопасности, мы видим особое значение политических элит в условиях развития информационно-политического процесса.

Системный подход к анализу сущности информационной безопасности общественно-политической системы обращает особое внимание не только на сугубо институциональные аспекты развития системы, но и на особые масштабы социальных взаимосвязей акторов,

формирующихся в условиях информационно-политического процесса. Так, В.Е. Макаров определяет информационную безопасность именно как социальную систему, в основе функционирования которой лежит необходимость целенаправленного ослабления дезорганизующего воздействия внешних и внутренних угроз на многочисленные акторы современного процесса (социальные группы, общества в целом, государственные системы) [Макаров, 2015, 22]. Информационная безопасность представляет собой сложную, комплексную социальную систему, характеристиками которой выступают открытость, динамичность развития, наличие специфических структурно-функциональных компонентов.

В рамках применения системного подхода к исследованию информационной безопасности как сложной, динамической системы единовременного и последовательного взаимодействия отдельно взятой личности, общества в целом, государственно-политической системы, выделяются следующие структурные компоненты [Макаров, 2015, 23-24].

1) Цели (как объективное отражение интересов системных акторов).

2) Информационные интересы и потребности акторов.

3) Средства и ресурсы обеспечения информационных потребностей акторов системы информационной безопасности.

4) Институциональное воплощение многочисленных общественно-политических сил, вовлеченных в систему практического обеспечения информационной безопасности и обладающих соответствующей законодательно-закрепленной компетенцией.

5) Широкий спектр ценностных характеристик объектов информационной безопасности (например, объект – государство, информационно-политический суверенитет – ценностная характеристика государства).

Отметим, что системный подход не отрицает значения стратегических оснований реализации политики информационной безопасности, объективированных в конкретных стратегиях, концепциях и доктринах. Напротив, данные основания определяют векторы и принципы развития информационно-политических отношений в рамках системной политики обеспечения информационной безопасности. Системный подход к исследованию информационной безопасности позволяет получить наиболее обстоятельные данные о внешней информационной среде (глобальной информационной инфраструктуре) и о воздействии этой среды на национальную систему безопасности информационно-политического пространства.

Заключение

Мировое сообщество развивается в принципиально новом векторе развития. Формируется единое информационно-телекоммуникационное пространство, поддерживаемое функционированием глобальной информационной инфраструктуры [Горбунова, 2014, 14-15]. В данном контексте перед научным политологическим сообществом стоят объек-

тивные задачи научного осмысления противостояния обратным, негативным тенденциям современного глобального развития. Противостояние таковым тенденциям находит отражение в развитии теоретических политологических подходов к исследованию информационной безопасности.

Теория национальной безопасности, выступая одним из основных направлений современной политологии, является основой теории информационной безопасности. Подход к исследованию информационной безопасности как составной части национальной безопасности актуализирует вопросы анализа стратегических документов, выступающих нормативной основой политики информационной безопасности. В рамках данного подхода особую актуальность приобретают исследования внешних угроз и внутренних особенностей развития информационно-политических систем, что обуславливает необходимость в научном осмыслении проблем информационной суверенизации.

Ряд тезисов данного теоретического направления может быть дополнен и/или компенсирован посредством использования системного подхода к анализу информационной безопасности в условиях необходимости практической реализации информационной политики. Системный подход артикулирует довольно ясную и последовательную модель анализа информационной безопасности как научно-методологическом ключе, так и в условиях обеспечения информационной безопасности в реальном политическом процессе.

Резонно отметить, что оба подхода акцентируют внимание на едином предмете анализа, невзирая на существенные изначальные различия в теоретико-методологических основаниях и предпосылках, что, по нашему мнению, не преуменьшает значения какого-либо из подходов в структуре современной политической науки, но лишь подтверждает целесообразность последовательного использования научных разработок в рамках обоих подходов.

Библиография

1. Владимирова Т.В. К социальной природе понятия «информационная безопасность» // NB: Национальная безопасность. 2013. № 4. С. 78-95. URL: http://e-notabene.ru/nb/article_596.html
2. Владимирова Т.В. О необходимом знании для идентификации угроз государственной безопасности // Научно-информационный журнал Армия и общество. 2014. № 2. С. 34-40.
3. Горбунова Ю.И. Информационная инфраструктура: современная сущность, подотрасли ее составляющие // Социально-экономические явления и процессы. 2014. № 2. С. 14-21.
4. Дементьева А.Г. Современные условия глобализации и роль транснациональных корпораций // Инициативы XXI века. 2010. № 1. С. 59-64.

5. Доктрина информационной безопасности Российской Федерации : утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
6. Жук Е.И. Концептуальные основы информационной безопасности // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2010. № 4. URL: http://technomag.bmstu.ru/doc/143237.html
7. Крылова И.А. Новые виды войн и безопасность России // Знание, понимание, умение. 2016. № 3. С. 58-71.
8. Кучерявый М.М. Государственная политика информационного суверенитета России в условиях современного глобального мира // Управленческое консультирование. 2015. № 2. С. 8-15.
9. Макаров В.Е. Политические и социальные аспекты информационной безопасности. М.: Таганрог: С. А. Ступин, 2015. 351 с.
10. Марков А.А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник С.-Петерб. ун-та. 2011. № 1. С. 43-48.
11. Панарин И.Н. Информационная безопасность. URL: http://panarin.com/info_voina/86-informacionnaya-bezopasnost.html
12. Радиков И.В. Национальная безопасность как главный национальный проект России: типичные проблемы реализации // Политэкс. 2007. № 1. С. 64-81. URL: http://www.politex.info/content/view/327/
13. Самыгин С.И., Руденко А.М., Котлярова В.В. Историко-философское осмысление проблемы информационной безопасности // Социум и власть. 2016. № 2. С. 47-51.
14. Стратегия национальной безопасности Российской Федерации до 2020 г. // Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». URL: https://rg.ru/2009/05/19/strategia-dok.html

Modern approaches to the study of information security in the Russian discourse of political science

Evgenii A. Matveev
Postgraduate student,
Faculty of political science,
St. Petersburg State University,
199034, 7/9 Universitetskaya emb., St. Petersburg, Russian Federation;
e-mail: matveev.spb@mail.ru

Abstract

This article focuses on the most significant methodological approaches in the studying of scientific problems of information security in the framework of the modern Russian political science. The author identifies an approach to the study of information security in the framework of the theory of national security. The article designates theoretical framework for the analysis of normative-legal basis of information security policy, analyzes the most significant trends and factors affecting information security in the development of the information society and the process of constructing a sovereign informational space of the state. The author focuses on the use of a systematic approach to the analysis of the phenomenon of information security. He explores the basic principles of a systematic approach to the study of information security. The most important structural components and political science contents of information security policy are analyzed. Special attention is drawn to the factor of the deployment of the information warfare and the neutralization of different negative types of impact of the information warfare. In conclusion, the author notes the desirability of the scientific use of methodological approaches in terms of development of the modern world.

For citation

Matveev E.A. (2016) Sovremennye podkhody k issledovaniyu informatsionnoi bezopasnosti v rossiiskom politologicheskom diskurse [Modern approaches to the study of information security in the Russian discourse of political science]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 5 (6A), pp. 164-173.

Keywords

Information society, information policy, information security, information warfare, information sovereignty, systemic approach.

References

1. Dement'eva A.G. (2010) Sovremennye usloviya globalizatsii i rol' transnatsional'nykh korporatsii [Modern conditions of globalization and the role of transnational corporations]. *Initsiativy XXI veka* [The initiatives of the XXI century], 1, pp. 59-64.
2. *Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii : utv. Ukazom Prezidenta Rossiiskoi Federatsii ot 5 dekabrya 2016 g. № 646* [Doctrine of Information Security of the Russian Federation: approved by the President of the Russian Federation No. 646 of December 5, 2016]. Available at: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html [Accessed 25/11/16].
3. Gorbunova Yu.I. (2014) Informatsionnaya infrastruktura: sovremennaya sushchnost', podotrasli ee sostavlyayushchie [Information infrastructure: a modern entity, sub-industry components]. *Sotsial'no-ekonomicheskie yavleniya i protsessy* [Socio-economic phenomena and processes], 2, pp. 14-21.

4. Krylova I.A. (2016) Novye vidy voin i bezopasnost' Rossii [New types of war and security of Russia]. *Znanie, ponimanie, umenie* [Knowledge, understanding, ability], 3, pp. 58-71.
5. Kucheryavyi M.M. (2015) Gosudarstvennaya politika informatsionnogo suvereniteta Rossii v usloviyakh sovremennogo global'nogo mira [Public policy of information sovereignty of Russia in the conditions of the modern global world]. *Upravlencheskoe konsul'tirovanie* [Management consulting], 2, pp. 8-15.
6. Makarov V.E. (2015) *Politicheskie i sotsial'nye aspekty informatsionnoi bezopasnosti* [Political and social aspects of information security]. Moscow: Taganrog: S. A. Stupin Publ.
7. Markov A.A. (2011) Nekotorye aspekty informatsionnoi bezopasnosti v kontekste natsional'noi bezopasnosti [Some aspects of information security in the context of national security]. *Vestnik S.-Peterb. un-ta* [The Bulletin of SPSU], 1, pp. 43-48.
8. Panarin I.N. *Informatsionnaya bezopasnost'* [Information security]. Available at: http://panarin.com/info_voina/86-informacionnaya-bezopasnost.html [Accessed 21/11/16].
9. Radikov I.V. (2007) Natsional'naya bezopasnost' kak glavnyi natsional'nyi proekt Rossii: tipichnye problemy realizatsii [National security as the main national project of Russia: the typical problems of realization]. *Politeks* [Politex], 1, pp. 64-81. Available at: http://www.politex.info/content/view/327/ [Accessed 23/11/16].
10. Samygin S.I., Rudenko A.M., Kotlyarova V.V. (2016) Istoriko-filosofskoe osmyslenie problemy informatsionnoi bezopasnosti [Historical and philosophical understanding of problems of information security]. *Sotsium i vlast'* [Society and government], 2, pp. 47-51.
11. Strategiya natsional'noi bezopasnosti Rossiiskoi Federatsii do 2020 g. [The national security strategy of the Russian Federation until 2020]. *Ukaz Prezidenta Rossiiskoi Federatsii ot 12 maya 2009 g. № 537 "O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii do 2020 goda"* [Decree of the President of the Russian Federation of May 12, 2009, No. 537 "On the National Security Strategy of the Russian Federation until 2020"]. Available at: https://rg.ru/2009/05/19/strategia-dok.html [Accessed 26/11/16].
12. Vladimirova T.V. (2013) K sotsial'noi prirode ponyatiya "informatsionnaya bezopasnost'" [About the social nature of the term "Information security"]. *NB: Natsional'naya bezopasnost'* [NB: National security], 4, pp. 78-95. Available at: http://e-notabene.ru/nb/article_596.html [Accessed 26/11/16].
13. Vladimirova T.V. (2014) O neobkhodimom znanii dlya identifikatsii ugroz gosudarstvennoi bezopasnosti [About the necessary knowledge to identify threats to public safety]. *Nauchno-informatsionnyi zhurnal Armiya i obshchestvo* [Scientific-information journal The army and society], 2, pp. 34-40.
14. Zhuk E.I. (2010) Kontseptual'nye osnovy informatsionnoi bezopasnosti [Conceptual foundations of information security]. *Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana* [Science and education: scientific publication of Bauman Moscow State University], 4. Available at: http://technomag.bmstu.ru/doc/143237.html [Accessed 29/11/16].