УДК 327
DOI: 10.21209/2227-9245-2022-28-5-70-76

ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИЙ ПРОЦЕСС И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАБАЙКАЛЬЯ КАК ЗАЩИЩЕННОСТЬ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ

SOCIO-POLITICAL PROCESS AND INFORMATION SECURITY OF TRANSBAIKALIA AS PROTECTION OF NATIONAL INTERESTS

А. В. Новикова, Забайкальский государственный университет, г. Чита
novikova2010@mail.ru

A. Novikova, Transbaikal State University, Chita

Дан анализ информационной безопасности Забайкалья, показана взаимосвязь общественно-политического процесса, информационных технологий и безопасности. Угрозами информационной безопасности являются вирусные атаки, хакерские взломы как элементы кибернетической преступности. Очевидно, что социальные риски расширяются и негативно влияют на защищенность жизненно важных интересов России и её субъектов. Среди направлений национальной безопасности особое внимание уделяется информационной безопасности с точки зрения защиты информационного пространства РФ. Каждое государство считает актуальной и приоритетной задачей обеспечение информационной безопасности своей страны и граждан. Как следствие, возникает проблема защиты информации. В условиях возросших опасных информационных воздействий в мире защита личной, общественной и государственной информации имеет первостепенное значение для любого государства. Целесообразно объединить все усилия по преодолению информационных рисков, которые имеют не только социальную, но и политическую составляющую. Дана характеристика политического процесса, понятие которого заимствовано из кибернетики, обоснована его структура: субъекты и участники процесса; объект процесса; методы, средства, ресурсы, которые соединяют субъект и объект. Требующими внимания субъектами процесса, характеризующего политику, выступают индивиды, политические системы, государство, партии. К субъектам политического процесса также относится информационная составляющая. В современный период в России взят курс на реализацию национальных интересов в информационной сфере. Национальные интересы предполагают систему обеспечения безопасности информации. Главным в информационной сфере является защита органов власти от информационного манипулирования, что, безусловно, связано с общественно-политическим процессом. Целесообразно использование сети Интернет, развитие электронного документооборота, наличие системного администратора, что будет способствовать созданию единого информационного пространства

Ключевые слова: *информационная безопасность, общественно-политический процесс, информационная угроза, Забайкалье, хакерский взлом, киберпреступность, технизация управления*

The paper analyzes the information security of Transbaikalia and shows the relationship of the socio-political process, information technology and security. Threats to information security are virus attacks, hacker hacks as elements of cybernetic crime. It is obvious that social risks are expanding and negatively affect the protection of vital interests of Russia and its subjects. Among the areas of national security, special attention is paid to information security from the point of view of protecting the information space of the Russian Federation. Each state considers it an urgent and priority task to ensure the information security of its country and citizens. As a consequence, there is a problem of information protection. In the conditions of increased dangerous information impacts in the world, the protection of personal, public and state information is of paramount importance for any state. It is advisable to combine all efforts to overcome information risks that have not only a social, but also a political component. The

characteristic of the political process, the concept of which is borrowed from cybernetics, is given, its structure is substantiated: subjects and participants of the process; the object of the process; methods, means, resources that connect the subject and the object. Individuals, political systems, the state, and parties are the subjects of the process characterizing politics that require attention. The subjects of the political process also include the information component. In the modern period, Russia has set a course for the realization of national interests in the information sphere. National interests presuppose a system for ensuring the security of information systems. The main thing in the information sphere is the protection of authorities from information manipulation, which, of course, is connected with the socio-political process. It is advisable to use the Internet, the development of electronic document management, the presence of a system administrator, which will contribute to the creation of a unified information space

Key words: *information security, socio-political process, information threat, Transbaikalia, hacker hacking, cybercrime, technization of management*

Введение. Стремительно усиливается процесс политизации информационной сферы. Современные информационные технологии проникли во многие направления развития государства. В Доктрине информационной безопасности РФ отмечено: «информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества» [3].

Консолидация научного сообщества в экспертировании проблемы взаимосвязи информационной безопасности, общественно-политического процесса и цифровых технологий обусловлена появлением современных политических акторов и возрастанием угроз национальным интересам государств. Информационные угрозы связаны, по мнению А. Н. Кухарского, с «информационным воздействием на политические объединения, личность, социальные группы и направлены на развал политической системы, дестабилизацию созданных ценностей, уничтожение личности, нарушение внутриполитической составляющей информационной безопасности» [7].

Так синтезируются как внутренние, так и внешние источники информационных угроз.

Актуальность темы заключается в том, что через информационную среду реализуются угрозы национальной безопасности страны, поэтому информационная безопасность становится важнейшим условием функционирования России и реализации её национальных интересов во внутренней и внешней политике. Вопрос национальных интересов в информационной сфере приобретает актуальное звучание в аспекте информационной безопасности Российской Федерации. Это обусловлено тем, что по своей значимости информационная составляющая национальной безопасности имеет первостепенное значение. Информационная безопасность занимает одно из центральных мест в системе национальной безопасности. Таким образом, информационная безопасность стоит на защите национальных интересов. Актуальность темы исследования обусловлена тем, что в условиях усиления борьбы за доминирование в глобальном информационном пространстве проблема информационной безопасности перешла в плоскость международных отношений. В частности, возрастает опасность ведения информационной войны между государствами, которая неизменно приведёт к дестабилизации политической системы, нарушению территориальных границ отдельных государств и, как следствие, к экономической и политической катастрофе во всём мире.

Объектом исследования является информационная безопасность Российской Федерации как общественно-политический процесс.

Предметом исследования выступают национальные интересы Российской Федерации в информационной сфере.

Теоретические рамки исследования обусловлены взаимосвязью понятий «общественно-политический процесс», «информационная безопасность», «цифровые технологии».

Цель исследования – выделить безопасность в информационной сфере с позиции информационно-компьютерных технологий, ориентированных на «общественно-опасные преступления, совершение террористических актов, вмешательство в дела суверенных государств, развязывание межгосударственных конфликтов, разжигание межэтнической розни» [7].

По свидетельству М. Ю. Величко, «возникновение данных угроз на фоне медленного и недостаточного развития российской законодательной базы связано, прежде всего, с бурным развитием рыночных отношений, интеграцией России в глобальные мировые социально-политические отношения. Все это требует переосмысления и разработки новых механизмов организации противодействия национальной и транснациональной преступности, а также нейтрализации внутренних и внешних угроз» [2].

Методы исследования. С учётом степени разработанности проблемы, её недостаточной изученности использовались следующие методы: индукция, дедукция, компаративистское исследование, системный, структурно-функциональный методы.

Разработанность темы. В научной литературе тема национальных интересов в информационной сфере освещается достаточно широко. Анализ государственной информационной политики содержится в трудах А. В. Манойло, категория национального интереса изучена Гансом Моргентау. Мартин Либицки известен всему миру своими исследованиями в области кибервойн и их влияния на политику государства.

В последние годы, в свете современной действительности, внимание авторов к национальному интересу и информационной безопасности резко возросло. В. Н. Лопатин в своих работах уделяет особое внимание информационной безопасности России. Проблемы информационной войны и информационного противостояния рассматривают Л. В. Воронцова, Г. В. Грачёв, И. И. Завадский, И. К. Мельник, Н. М. Панарин, Г. Г. Почепцов, Д. Б. Фролов, Н. Н. Чернякова, Я. С. Шатило и др.

Результаты исследования. На методологию общественно-политического процесса существенное влияние оказали основоположники политической мысли Д. Истон, Б. Пауэлл, Г. Алмонд. А. Н. Кухарский для характеристики информационной безопасности выделял информационно-коммуникативную модель «политической системы Карла Дойча... с особенностями информационно-коммуникативного действия» [7]. Обоснование составляющих общественно-политического процесса дано Н. А. Барановым [1. С. 35], А. В. Новиковой[1], М. Ю. Зеленковым [4. С. 254]. «Общественно-политический процесс включает «субъекты и участников процесса; объект процесса; средства, методы, ресурсы, которые связывают субъект и объект–цель» [6]. Акторами общественно-политического процесса являются «политические системы, политические институты (государство, гражданское общество, политические партии и т. д.), организованные и неорганизованные группы людей, индивиды» [5; 6]. На базе указанных разработок общественно-политического процесса мы выделяем важный актор – информационную составляющую.

В информационной безопасности общественно-политического процесса целесообразна стандартизация методов обмена и транспортные протоколы, а также инновационные программы «Электронное Правительство», «Электронный муниципалитет» и информационный продукт «СБИС», обеспечивающий доступ к информационным ресурсам.

По свидетельству А. Н. Кухарского, «существуют следующие основные направления по обеспечению информационной безопасности политического процесса России:

1) выявление угроз информационной безопасности;

2) совершенствование информационных средств;

3) реализация уровней защиты информации путем создания системы защиты информации, которая сводится к ответственности за защиту персональных данных, коммерческой и профессиональной тайны, к реагированию на несанкционированное воздействие как на технические каналы, так и на информационные системы» [7].

Пропагандистская деятельность государств мира проявляется в террористических организациях, которые «стремительно принимают на вооружение информационные технологии с целью выполнения конкретных террористических операций. Очевидно, что террористические организации нарушают целостность и работоспособность информационных сетей, что дает им возможность оперативно согласовывать свои действия, а также пропагандировать свои взгляды» [7].

Очевидно, что в социально-политической сфере должно быть действенное реагирова-

[1] Новикова А. В. Регионы РФ в политическом процессе модернизирующейся России и их влияние на обеспечение национальной безопасности. – Чита: ЗабГУ, 2016. – 230 с.

ние на возникающие вызовы в информационном пространстве по сетевой информационной террористической структуре организаций. Так, по свидетельству А. Н. Кухарского, «внутри организации личностное воздействие лидера все больше уступает место упрощенной децентрализованной системе управления» [7].

Противовесом информационной безопасности является информационная война. Понятие «информационная война» связано с именем профессора Мартина Либицки, специалиста из корпорации RAND (американский аналитический центр, основанный 14 мая 1948 г. в Санта-Моника (Калифорния). В августе 1995 г. опубликована его статья «Что такое информационная война?» [9]. Более 20 лет назад М. Либицки писал, что психологическое воздействие на противника в ходе военных действий используется с древних времен, однако в войнах нашего времени технические методы и психологические информационные операции имеют одинаковое по важности значение и применяются в комплексе. Профессор М. Либицки предложил одну из первых классификаций информационных войн. Он выделяет семь различных аспектов этого феномена:

1) война в сфере контроля и управления;
2) разведывательная война;
3) электронная война;
4) психологическая война;
5) хакерская война;
6) экономическая информационная война;
7) кибервойна [9].

На современном этапе особую актуальность приобрели хакерская атака и кибервойна, которые ориентированы на управление сознанием людей. Труды М. Либицки, одного из самых влиятельных американских исследователей и теоретиков в информационной сфере, стали базисом для концепций и стратегий вооруженных сил Соединенных Штатов, а также соответствующих документов Министерства юстиции США.

В современный период ярким примером информационной войны является ситуация с Украиной. Информационная война на Украине и во всём мире преследует цель – создать из России образ врага, агрессора. В связи с последними событиями во всем мире насаждается ненависть к Российской Федерации, к русским людям, ко всему русскому. Непосредственное руководство этой информационной войной осуществляется специалистами США.

Поводя итоги, можно сделать следующие выводы:

– информационная война – угроза безопасности Российской Федерации;

– сущность информационной войны – манипулирование массовым сознанием с целью реализации национальных интересов агрессора в ущерб других национальных интересов;

– такая форма противоборства и противостояния эффективней реальных боевых действий;

– информационная война связана с информационной безопасностью.

Современный этап развития информационной безопасности основывается на глобальных процессах, таких как интеграция всех информационных систем мировых государств в единую систему и создание единого информационного пространства. Это ставит вопросы безопасности на новый глобальный уровень.

Возрастает необходимость защиты систем информации. Российская Федерация в современных условиях повышения спроса на защиту информационных систем берёт направление на развитие рынка услуг по разработке и применению систем информационной безопасности. Подтверждением этому является федеральный проект «Цифровая экономика Российской Федерации», подпрограмма кибербезопасность (срок реализации 2018-2024 гг.) [8]. В рамках проекта предусмотрено развитие рынка средств информационной безопасности и создание нескольких крупных компаний – игроков мирового уровня в области безопасности информационных систем. Достижению поставленной цели способствует увеличение затрат на продукты и услуги в области информационной безопасности (табл. 1) и увеличение количества подготовленных специалистов в области информационной безопасности (табл. 2).

Таблица 1 / Table 1

Объём затрат на продукты и услуги в области информационной безопасности / The amount of costs for products and services in the field of information security

Год / Year	Объём затрат, млрд р. / The volume of costs, billion rubles. /
2019	67,20
2020	80,64
2021	96,77
2022	116,12
2023	139,35
2024	167,22

Таблица 2 / Table 2

Количество подготовленных специалистов в области информационной безопасности / Number of trained specialists in the field of information security

Год / Year	Количество специалистов, тыс. чел. / Number of specialists, thousand people
2020	10,08
2021	12,10
2022	14,52
2023	17,42
2024	20,90

На основе данных таблиц можно сделать вывод, что в Российской Федерации создаются условия для осуществления политики безопасности информационных систем.

Таким образом, в настоящее время на территории Российской Федерации:

– отмечается рост количества угроз безопасности информационных систем;

– повышение спроса на обеспечение безопасности информационных систем;

– активно проводится государственная политика, направленная на обеспечение безопасности информационных систем.

Заключение. В современном мире стремительными темпами идёт процесс информатизации во всех сферах деятельности человека, общества и государства. При этом информационные технологии могут использоваться как для обеспечения национальных интересов, так и для создания угроз национальной безопасности государств. Совершенствование информационно-коммуникационных технологий в условиях информационной глобализации и противоборства государств на мировой арене способствует созданию реальных возможностей для возникновения новых внутренних и внешних угроз. В таких условиях любое государство заинтересовано в защите национальных интересов во всех сферах, в частности информационной.

Проведённый анализ законодательной базы позволил говорить о том, что в настоящее время в России взят курс на реализацию национальных интересов в информационной сфере. Это подтверждается политико-правовыми документами (Конституция Российской Федерации, Доктрина информационной безопасности Российской Федерации, Стратегия национальной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. и др.), которые стали основой для осуществления целей и задач государственной политики в аспекте национальных интересов в информационной сфере. Очевидно, созданный управленческий механизм в системе обеспечения безопасности информационных систем позволяет говорить об эффективности государственной политики в сфере информации. Можно сделать следующие выводы:

1. Очевидно, что главным в информационной безопасности является защита органов власти от информационного манипулирования, что, безусловно, связано с общественно-политическим процессом.

2. Для защиты информации необходимо знать мнение граждан о всех сферах жизнедеятельности общества и эффективно на него воздействовать.

3. Существуют направления противодействия информационным угрозам: борьба с неэффективными управленческими системами, международным терроризмом, информационными провокациями.

4. Целесообразно использование сети Интернет, развитие электронного документооборота, наличие системного администратора, что будет способствовать созданию единого пространства функционирования информации в РФ.

5. Выделяем два направления улучшения информационной безопасности Забайкальского края: административный (нормативно-правовая база) и организационный, предполагающий технизацию управления.

В информационной сфере должна быть установлена эффективная коммуникация между органами власти РФ и её субъектами, негосударственными организациями по защите персональных данных, государственному лицензированию информационных систем.

Список литературы

1. Баранов Н. А. Политические отношения и политические процессы в современной России. СПб.: БГТУ, 2014. 137 с.

2. Величко М. Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект. URL: http://lawtheses.com/informatsionnaya-bezopasnost-v-deyatelnosti-organov-vnutrennih-del-teoretiko-pravovoy-aspekt#ixzz5IfdhgH2A (дата обращения: 20.03.2022). Текст: электронный.

3. Доктрина информационной безопасности Российской Федерации [утверждена Указом Президента РФ от 5 декабря 2016 г. № 646]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (дата обращения: 20.03.2022). Текст: электронный.

4. Зеленков М. Ю. Политология. М.: Юрид. ин-т МИИТ, 2009. 302 с.

5. Зеленков М. Ю. Политология. URL: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm (дата обращения: 11.03.2022). Текст: электронный.

6. Зеленков М. Политология. URL: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm (дата обращения: 20.03.2022). Текст: электронный.

7. Кухарский А. Н. Информационная безопасность политического процесса как элемент государственного и муниципального управления России: дис. ... канд. полит. наук: 23.00.02. Чита, 2019. URL: http://dlib.rsl.ru (дата обращения: 24.03.2022). Текст: электронный.

8. Паспорт федерального проекта «Информационная безопасность». URL: https://files.data-economy.ru/Docs/Pass_Cybersecurity.pdf (дата обращения: 10.03.2022). Текст: электронный.

9. Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995. URL: http://www.dodccrp.org/files/Libicki_What_Is.pdf (дата обращения: 20.03.2022). Текст: электронный.

References

1. Baranov N. A. *Politicheskiye otnosheniya i politicheskih protsess v sovremennoy Rossii* (Political relations and political process in modern Russia). St. Petersburg: BSTU, 2014, 137 p.

2. Velichko M. Yu. *Informatsionnaya bezopasnost v deyatelnosti organov vnutrennikh del: teoretiko-pravovoy aspekt* (Information security in the activities of internal affairs bodies: theoretical and legal aspect). Available at: http://lawtheses.com/informatsionnaya-bezopasnost-v-deyatelnosti-organov-vnutrennih-del-teoretiko-pravovoy-aspekt#ixzz5IfdhgH2A (date of access: 03/20/2022). Text: electronic.

3. *Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii* [utverzhdzhena Ukazom Prezidenta RF ot 5 dekabrya 2016 g. № 646] (Doctrine of information security of the Russian Federation [approved by Decree of the President of the Russian Federation dated by December 5, 2016 No. 646]. Available at: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (date of access: 20.03.2022). Text: electronic.

4. Zelenkov M. Yu. *Politologiya* (Political science). Moscow: Yurid. in-t MIIT, 2009, 302 p.

5. Zelenkov M. Yu. *Politologiya* (Political science). Available at: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm (date of access: 03/11/2022). Text: electronic.

6. Zelenkov M. *Politologiya* (Political science). URL: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm (date of access: 03/20/2022). Text: electronic.

7. Kukharsky A. N. *Informatsionnaya bezopasnost politicheskogo protsessa kak element gosudarstvennogo i munitsipalnogo upravleniya Rossii*: dis. ... kand. polit. nauk: 23.00.02 (Information security of the political process as an element of state and municipal government in Russia: dis. ... cand. polit. Sciences: 23.00.02). Chita, 2019. Available at: http://dlib.rsl.ru (date of access: 03/24/2022). Text: electronic.

8. *Pasport federalnogo proyekta «Informatsionnaya bezopasnost»* (Passport of the federal project “Information Security”). Available at: https://files.data-economy.ru/Docs/Pass_Cybersecurity.pdf (date of access 03/10/2022). Text: electronic.

9. Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995 (What is Information Warfare? United States Government Printing, Washington DC, 1995). Available at: http://www.dodccrp.org/files/Libicki_What_Is.pdf (date of access 3/20/2022). Text: electronic.

Информация об авторе **Information about the author**

Новикова Анна Владимировна, канд. полит. наук, доцент кафедры государственного, муниципального управления и политики, Забайкальский государственный университет, г. Чита, Россия. Область научных интересов: политические науки, государственное управление, политические процессы, информационная безопасность
anna_novikova2010@mail.ru

Anna Novikova, candidate of political sciences, associate professor, State, Municipal Administration and Policy department, Transbaikal State University, Chita, Russia. Research interests: political science, public administration, political processes, information security

Для цитирования

Новикова А. В. Общественно-политический процесс и информационная безопасность Забайкалья как защищенность национальных интересов // Вестник Забайкальского государственного университета. 2022. Т. 28, № 5. С. 70–76. DOI: 10.21209/2227-9245-2022-28-5-70-76.

Novikova A. Socio-political process and information security of Transbaikalia as protection of national interests // Transbaikal State University Journal, 2022, vol. 28, no. 5, pp. 70–76. DOI: 10.21209/2227-9245-2022-28-5-70-76.

Статья поступила в редакцию: 11.05.2022 г.
Статья принята к публикации: 18.05.2022 г.