

15. 沐涛. 南非对外关系研究 / 沐涛. – 上海: 华东师范大学出版社, 2003. – 235 p. = *Му, Тао. Исследование о международных отношениях Южной Африки / Му Тао. – Шанхай: Изд-во Восточ.-кит. пед. ун-та, 2003. – 235 с.*
16. *Прокопенко, Л. Я. Новые политические элиты в государствах Юга Африки / Л. Я. Прокопенко. – Москва: Ин-т Африки РАН, 2011. – 252 с.*
17. 方伟. 新南非对外关系研究 / 方伟. – 杭州: 浙江人民出版社, 2014. – 190 p. = *Фан, Вэй. Исследование о международных отношениях новой Южной Африки / Фан Вэй. – Ханчжоу: Чжэцзян. нар. изд-во, 2014. – 190 с.*
18. 孙瑞. 南非促进非洲经济一体化研: 论文 ... 政治学硕士 / 孙锐; 江苏师范大学. – 江苏, 2019. – 55 p. = *Сунь, Жуй. Исследование роли Южно-Африканской Республики в продвижении экономической интеграции Африки: дис. ... магистра полит. наук / Сунь Жуй; Цзян. пед. ун-т. – Цзянсу, 2019. – 55 с.*
19. *Хаматишин, А. Д. Земельные отношения и развитие сельскохозяйственного производства на Юге Африки: автореф. дис. ... канд. экон. наук: 08.00.14 / Хаматишин Альберт Дамирович; Ин-т Африки РАН. – Москва, 2014. – 20 с.*
20. 南部非洲发展共同体 // 中华人民共和国外交部. – URL: https://www.mfa.gov.cn/web/wjb_673085/zsjg_673183/fzs_673445/dqzzhzhjz_673449/nbfzfhz_673493/gk_673495/ (date of access: 19.12.2024). = Сообщество развития Юга Африки // Министерство иностранных дел Китайской Народной Республики. – URL: https://www.mfa.gov.cn/web/wjb_673085/zsjg_673183/fzs_673445/dqzzhzhjz_673449/nbfzfhz_673493/gk_673495/ (дата обращения: 19.12.2024).

(Дата подачи: 26.02.2025 г.)

Д. А. Буконкин

Белорусский государственный университет, Минск

D. A. Bukonkin

Belarusian State University

УДК 321.011:327.8

ВНЕШНИЕ ИСТОЧНИКИ ВЫЗОВОВ И УГРОЗ ДЛЯ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА РЕСПУБЛИКИ БЕЛАРУСЬ

EXTERNAL SOURCES OF CHALLENGES AND THREATS FOR INFORMATION SOVEREIGNTY OF BELARUS

Статья посвящена исследованию внешних источников вызовов и угроз для информационного суверенитета Республики Беларусь. Проанализированы существующие подходы к определению и классификации таких вызовов и угроз, рассматриваются положения действующих нормативных правовых актов концептуального характера по проблемам информационного суверенитета и результаты академических исследований отечественных и зарубежных ученых. Автором предложен подход для обновления типологизации идентифицированных источников вызовов и угроз информационному суверенитету.

Ключевые слова: информационный суверенитет; источник вызовов и угроз; кибербезопасность; информационно-коммуникационные технологии (ИКТ); иностранное влияние.

The article is devoted to the study of external sources of challenges and threats to the information sovereignty of the Republic of Belarus. The existing approaches to the definition and classification of such challenges and threats are analyzed, the provisions of current normative legal acts of a conceptual nature on the problems of information sovereignty and the results of academic research by domestic and foreign scientists are considered. The author proposes an approach to updating the typology of identified sources of challenges and threats to information sovereignty.

Keywords: information sovereignty; source of challenges and threats; cyber security; foreign influence.

Актуализация информационного суверенитета связана в первую очередь с возрастающей ролью информации и информационных технологий в XXI в. Обеспечение национальной безопасности в информационной сфере становится одной из ключевых задач для любого государства. Республика Беларусь не является исключением, и защита ее информационного суверенитета требует пристального внимания к рискам, вызовам и угрозам в указанной сфере. Именно попытки вмешательства извне являются одним из наиболее серьезных факторов, влияющих на суверенитет Беларуси в информационной области [1].

Цель данной статьи – провести классификацию и типологизацию источников вызовов и угроз информационному суверенитету Беларуси, выработать предложения по минимизации их негативного воздействия в текущих условиях.

Над вопросами вызовов и угроз информационному суверенитету работал целый ряд зарубежных исследователей, среди которых Д. Мур, Д. Веллер, Д. Стефенеску. Указанная проблематика является предметом анализа как российских, так и отечественных ученых: А. Иванцова, М. Фалеева, М. Бажиной, Т. Филипповой и др.

Для определения источников угроз и атак на информационный суверенитет Беларуси приняты положения, зафиксированные в Концепции национальной безопасности Республики Беларусь. Согласно документу, *источник угроз* определяется как «фактор или совокупность факторов, а также субъектов, их продуцирующих, способных при определенных условиях привести к возникновению угрозы национальной безопасности» [2]. Источники угроз разделяются на внутренние и внешние.

Основными *внешними источниками угроз* названы:

- доминирование ведущих иностранных государств в глобальном информационном пространстве с монополизацией ключевых сегментов информационных рынков иностранными информационными структурами. Это ограничивает возможности Беларуси самостоятельно формировать и продвигать свою информационную повестку на мировой арене;
- действия иностранных государств, международных и иных организаций и отдельных лиц, наносящие вред национальным интересам Республики Беларусь в информационной сфере путем формирования негативного образа государства в мире. Данный фактор направлен на подрыв

международного авторитета Беларуси и ее способности защищать свои национальные интересы;

- усиление информационной конфронтации между ведущими мировыми центрами власти, проведение иностранными государствами информационной войны, что создает обстановку повышенной геополитической напряженности, в которой Беларусь должна найти выход для сохранения своего суверенитета;

- препятствия для распространения национальных интересов Республики Беларусь, ограничения возможностей страны для представления своей точки зрения международному сообществу. Следствие – формирование искаженного образа нашей страны и серьезный ущерб для имиджа;

- широкое распространение в мировом информационном пространстве явлений массовой культуры, противоречащих национальным ценностям, представляющих угрозу сохранению белорусской культурной самобытности. Подобные явления ведут к утрате культурного кода и ориентации общества во времени и пространстве;

- неэффективность механизмов международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационных и коммуникационных технологий, препятствующая эффективно противодействовать угрозам информационной безопасности Беларуси [2];

- эксплуатация международными террористическими и экстремистскими организациями современных ИКТ для достижения своих противоправных целей.

В Концепции информационной безопасности 2019 г. в качестве источников угроз информационному суверенитету страны обозначены:

- увеличение числа киберпреступлений, где информационные системы становятся как объектом нападения, так и средством совершения преступлений;

- информационное противоборство между ведущими мировыми центрами силы и целенаправленное формирование информационных поводов для дискредитации политики государства как внутри, так и за его пределами;

- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

- угроза утечки и незаконного вмешательства в частную жизнь граждан, включая похищение персональных данных и компрометацию реквизитов доступа;

- необходимость соблюдения законодательства относительно защиты служебной информации и персональных данных, что становится актуальным в условиях сетевой доступности [3].

Таким образом, анализ внешних источников вызовов и угроз для информационного суверенитета Республики Беларусь показывает, что они являются реальной опасностью, требующей пристального внимания и своевременных мер по их нейтрализации.

Признавая ценность и широкий охват изложенных в указанных документах проблем, с нашей точки зрения, целесообразно уточнить подходы к определению и классификации вызовов и угроз. Можно разделить все вызовы и угрозы на *общие*, свойственные для всех стран и регионов без исключения, *специальные*, связанные с географическим положением и принадлежностью к геополитическим блокам, социально-политическим и экономическим развитием государства, а также *уникальные*, присущие той или иной стране в определенный период.

В качестве общих вызовов и угроз допустимо назвать целенаправленное использование современных ИКТ для совершения различных противоправных действий: незаконный сбор и использование персональных данных, распространение недостоверной, компрометирующей или экстремистской информации, использование киберпространства для скрытого информационно-психологического воздействия и др.

В качестве специальной угрозы для Республики Беларусь может быть названа высокая степень ее зависимости от импорта технологий и оборудования, которые могут быть использованы для оказания давления на республику и ограничения ее суверенных прав в информационной сфере.

Среди уникальных для Республики Беларусь угроз – деятельность ряда международных неправительственных организаций и политизированных групп, направленных на подрыв политической стабильности и пропаганду протестных настроений в белорусском обществе (наподобие «Киберпартизаны») [4].

По нашему мнению, нормативное закрепление предложенной классификации позволит более точно определять приоритеты работы по защите информационного суверенитета, согласовывать действия государственных органов по актуализации мер противодействия.

При классификации источников угроз и вызовов важно учитывать, что цели и технологии их реализации направлены как на решение стратегических задач, так и на получение конкретных ситуационных выгод. Можно спрогнозировать потенциальные действия внешних акторов по:

- 1) нанесению ущерба информационной инфраструктуре и каналам связи;
- 2) оказанию информационно-психологического воздействия на белорусское общество с целью посеять панические настроения;
- 3) нанесению ущерба имиджу, репутации и престижу Республики Беларусь на международной арене;
- 4) овладению стратегически важными информационными ресурсами и сведениями, составляющими государственную тайну;
- 5) подрыву доверия населения к органам государственной власти, формированию сомнения в их эффективности и легитимности [5, с. 45].

В этой связи в качестве основных внешних факторов, формирующих источники вызовов и угроз для информационного суверенитета Республики

Беларусь, опираясь на наработки зарубежных и отечественных исследователей, можно выделить:

- усиление информационного противоборства, приобретающего все более выраженный геополитический характер [6];
- расширение масштабов использования ИКТ в целях давления на суверенные государства, вмешательства во внутренние дела, дестабилизации политической обстановки [7, с. 15];
- усиление конкуренции между формирующимися на постсоветском пространстве геополитическими объединениями за контроль над информационными потоками, ресурсами и каналами коммуникации в регионе;
- стремление мировых центров силы к доминированию в киберпространстве, что создает риски вторжения в национальные информационные системы и подрыва критически важной инфраструктуры государства [8, р. 178].

Современные международные отношения характеризуются нарастанием состязательности между ведущими державами за глобальное информационное доминирование. Развертывается новый этап «информационной войны», в ходе которой противоборствующие стороны используют все доступные методы и средства для воздействия на массовое сознание и дискредитации друг друга [9]. Республика Беларусь, стремясь к сохранению государственного суверенитета, вынуждена реагировать на эти вызовы и противостоять попыткам внешнего информационного давления. Стремительное распространение ИКТ не только позволяет государствам расширять возможности контроля над информационным пространством, но и создает предпосылки возникновения новых угроз информационному суверенитету. Беларусь все активнее использует современные цифровые платформы и сервисы в своей деятельности. Актуальной проблемой является также конкуренция за доминирование в сети Интернет, контроль над которой – ключевой фактор информационного суверенитета в условиях цифровой эпохи [10].

Стирание национальных границ в информационной сфере, усиление роли транснациональных потоков данных и информации также порождает вызовы для государственного суверенитета Беларуси.

В этих условиях автором данной статьи предлагается дополнить список источников вызовов и угроз информационному суверенитету и безопасности Беларуси следующими пунктами:

- активность иностранных СМИ и негосударственных организаций, направленная на нанесение ущерба национальным интересам Республики Беларусь;
- развитие технологий искусственного интеллекта и производства фейков недружественными Беларусью странами;
- создание недружественными Беларусью международными организациями и военно-политическими блоками подразделений, ответственных за ведение киберопераций и организацию кибератак;

- кибертерроризм, киберпреступность и кибершпионаж, использование их различными акторами международных отношений.

Каждый из перечисленных источников формирует спектр вызовов и угроз информационному суверенитету нашей страны. Например, деятельность иностранных СМИ может нести следующие существенные угрозы информационному суверенитету:

- распространение искаженной информации и пропаганды для манипуляции общественным мнением и дестабилизации внутренней политической ситуации;

- атаки на внутренние дела государства для разжигания конфликтов и ухудшения международных отношений;

- подрыв традиций, ценностей и норм общества, что угрожает культурному суверенитету и может привести к культурному колониализму;

- распространение информации, которая противоречит местным законам и нормам, может привести к правовым конфликтам и проблемам с регулированием СМИ на национальном уровне;

- зависимость от зарубежных информационных технологий и платформ, как следствие – неспособность контролировать информационные потоки;

- разработка и применение методов, таких как VPN или обходные сайты, что делает невозможным для государств контролировать и регулировать информацию, поступающую в страну [11, с. 6–86].

Итак, вызовом информационному суверенитету Республики Беларусь является усиление деструктивных информационно-психологических операций внешних акторов, направленных на подрыв внутривнутриполитической стабильности в стране, дискредитацию государственного руководства и действующих институтов власти. Зарубежные информационные каналы (Радио «Свобода», NEXTA, Belaste и др.) целенаправленно распространяют ложную и тенденциозную информацию, пытаются формировать в белорусском обществе ощущение непрочности власти, неспособности государственного управления решать существующие проблемы.

Фиксируются попытки со стороны различных иностранных центров навязать белорусскому обществу нарратив о нелегитимности действующей власти, экономической несостоятельности белорусской модели. Главными проводниками указанных «вбросов» являются зарубежные СМИ, специально созданные telegram-каналы и различные тематические группы в иных социальных сетях, популярных в обществе [12].

Остановился на угрозах кибербезопасности. Инфраструктура критически важных объектов, системы управления государственными информационными ресурсами являются мишенями для кибератак извне, а их взлом способен нанести серьезный ущерб суверенитету страны. Наиболее опасны попытки проникновения во внутренние информационные сети органов власти, выведение из строя ключевых элементов критической инфраструктуры, хищение конфиденциальной информации [13]. Подобной

активностью на белорусском направлении занимаются «Киберпартизаны», ведя целенаправленную работу из-за рубежа. Так, за время своей деятельности они осуществили атаки на железнодорожную инфраструктуру страны, похитили паспортные данные граждан Беларуси, осуществили взлом информационного агентства «БелТА» и похитили более 90 гигабайт личной и финансовой информации [14]. В этих условиях очевиден вопрос о необходимости обеспечения кибербезопасности государственных структур и объектов критической инфраструктуры (АЭС, нефтеперерабатывающие заводы и т. д.).

Для поддержания информационной безопасности и сохранения возможностей государства по реализации суверенной политики в медийно-информационной сфере Беларуси необходимо реализовать следующие меры:

1. Совершенствование правовой базы и механизмов государственного регулирования информационной деятельности в сети Интернет и социальных сетях, в том числе ограничение распространения недостоверной информации и пресечение попыток внешнего вмешательства.

2. Развитие национальной системы кибербезопасности, повышение устойчивости критической информационной инфраструктуры к внешним деструктивным воздействиям.

3. Стимулирование развития национальных информационных ресурсов, способных составить конкуренцию зарубежным медиа, расширение присутствия белорусской государственной информационной повестки в глобальном цифровом пространстве.

4. Укрепление информационной безопасности государства, совершенствование системы защиты государственных информационных ресурсов, обеспечение надежной охраны конфиденциальных сведений.

5. Повышение медиаграмотности граждан, формирование устойчивости общества к деструктивным информационным воздействиям, способность критически воспринимать и противостоять манипуляциям сознанием.

6. Расширение международного сотрудничества в области информационной безопасности, обмен опытом и практиками противодействия угрозам суверенитету государства в цифровом пространстве.

7. Комплексное развитие национальной информационной инфраструктуры, включая системы связи, вещания, хранения и обработки данных, что обеспечит технологическую независимость и безопасность Беларуси в информационной сфере [15].

Таким образом, обеспечение информационного суверенитета Республики Беларусь диктуется прагматическими потребностями сохранения государственной самостоятельности и национальных интересов в условиях глобальной информационной взаимозависимости. Наша страна сталкивается с комплексом внешних источников и угроз информационному суверенитету. Ключевым вызовом становится необходимость защиты критически

важных государственных информационных систем и ресурсов от *внешних* угроз кибербезопасности, а также противодействие *экспансии зарубежных* медиа, способных оказывать существенное влияние на массовое сознание. Комплекс взаимосвязанных мер для обеспечения информационного суверенитета Беларуси включает совершенствование нормативной правовой базы, развитие национальной системы кибербезопасности, поддержку отечественных СМИ и повышение медиаграмотности общества. Эффективная реализация мероприятий позволит поддерживать устойчивое социально-политическое развитие и сохранить национальную государственность.

Список использованных источников

1. *Иванцов, А. В.* The meaning, origins and relevance of information sovereignty / А. В. Иванцов // Journal of the Belarusian State University. International Relations. – 2023. – Vol. 2. – P. 33–38.
2. Об утверждении Концепции национальной безопасности Республики Беларусь: решение Всебелорусского народного собрания, 25 апреля 2024 г. № 5 // Национальный правовой Интернет-портал Республики Беларусь. – URL: <https://pravo.by/document/?guid=3871&p0=P924v0005> (дата обращения: 18.02.2025).
3. О Концепции информационной безопасности Республики Беларусь: постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., № 1 // Национальный правовой Интернет-портал Республики Беларусь. – URL: <https://pravo.by/document/?guid=3871&p0=P219s0001> (дата обращения: 15.02.2025).
4. *Дудчик, А. Ю.* Partisans go cyber: The hacker ethic and partisans legacy / А. Ю. Дудчик // Вестник Санкт-Петербургского университета. – Философия и конфликтология. – 2023. – Т. 39, № 2. – С. 322–339.
5. *Фалеев, М. И.* Угрозы национальной безопасности государства в информационной сфере / М. И. Фалеев, Г. С. Черных // Стратегия гражданской защиты: проблемы и исследования. – 2014. – Т. 4, № 1(6). – С. 21–96.
6. *Moore, D.* The geopolitics of information / D. Moore // Business Horizons. – 1981. – Vol. 24, Issue 5. – P. 80–82.
7. Цифровой суверенитет: как государства защищают интересы в сети // Институт изучения мировых рынков. – 2024. – С. 2–21.
8. *Ștefănescu, D. C.* New threats to the national security of states – cyber threat. / D. C. Ștefănescu, A. Papoi // Scientific Journal of Silesian University of Technology. – Series Transport. – 2020. – P. 177–182.
9. *Ventre, D.* La guerre de l'information / D. Ventre // Hermes Science. Lavoisier. – 2007. – P. 282.
10. *Yakushev, M.* Internet governance: politics and geopolitics / M. Yakushev // Security Index: A Russian Journal on International Security. – 2010. – № 16(2). – P. 33–42.
11. *Колосов, Ю. М.* Массовая информация и международное право / Ю. М. Колосов. – 2-е изд., стер. – Москва: Статут, 2014. – 160 с.
12. *Николаева, А. Д.* Информационная война против Беларуси: сравнительный анализ / А. Д. Николаева // Гражданин. Выборы. Власть. – 2022. – № 4(26). – С. 158–168.
13. *Филиппова, Т. А.* Кибербезопасность в Республике Беларусь / Т. А. Филиппова, Е. А. Крачун // Актуальные проблемы современных экономических систем: сб. науч. тр. / редкол.: А. Г. Проровский [и др.]. – Брест: Изд-во БрГТУ, 2022. – С. 92–98.
14. Белорусские «КиберПартизаны» – хактивисты, которые бросили вызов режиму. – URL: <https://www.dekoder.org/ru/article/belaruskie-kiberpartizany-haktivisty-kotorye-brosili-vyzov-rezhimu> (дата обращения: 22.02.2024).

15. Бажина, М. А. Содержание и актуальные угрозы обеспечению информационного суверенитета: на примере Республики Беларусь и Российской Федерации / М. А. Бажина, И. В. Шахновская // Вестник Полоцкого государственного университета. Сер. D. – 2023. – № 2 (64). – С. 63–67.

(Дата подачи: 25.02.2025 г.)

М. А. Гребенчук

Белорусский государственный медицинский университет, Минск

М. А. Hrebianchuk

Belarusian State Medical University, Minsk

УДК 323.232

ИСТОРИЧЕСКАЯ ПОЛИТИКА КАК АКТУАЛЬНОЕ НАПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

HISTORICAL POLICY AS AN CURRENT DIRECTION OF STATE POLICY IN THE REPUBLIC OF BELARUS

В статье рассмотрена историческая политика в качестве актуального направления государственной политики Республики Беларусь. Проанализирован процесс развития данного концепта в нашей стране, изучены основные подходы. На основе проведенного исследования сделан вывод о том, что историческая политика является важным инструментом воздействия на политическую и идеологическую сферы общества.

Ключевые слова: историческая политика; государственная политика; институционализация; институционализация исторической политики; власть; общество; глобальная цифровизация; национальная идентичность.

The article examines historical policy as a current direction of state policy in the Republic of Belarus. The author analyzed the process of development of this concept in our country, studied the main approaches. Based on the conducted research, it was concluded that historical policy is an important instrument of influence on the political and ideological spheres of society.

Keywords: historical policy; state policy; institutionalization; institutionalization of historical policy; authority; society; global digitalization; national identity.

На сегодняшний день актуальность рассмотрения понятия «историческая политика» определяется значимостью интерпретации исторического прошлого в эпоху крупных социальных, политических трансформаций и перемен. Многие государства, особенно расположенные на постсоветском пространстве, испытывают на себе негативные последствия глобальных политических изменений. Республика Беларусь в этом вопросе не стала исключением. Как «унитарное демократическое социальное правовое государство, которое защищает свою независимость и территориальную целостность, конституционный строй, обеспечивает законность и правопорядок» [1], белорусскому государству необходима собственная легитимация, осуществляемая посредством активной государственной политики.