DOI 10.22394/1726-1139-2022-12-10-17

Секьюритизация информационной политики: обобщая накопленный опыт 2022 года

Долженкова Е.[1], *Межевич Н. М.*[2, 3, *], *Хлутков А. Д.*[2]

[1]Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Российская Федерация
[2]Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления РАНХиГС), Санкт-Петербург, Российская Федерация
[3]Псковский государственный университет, Псков, Российская Федерация; *mez13@mail.ru

РЕФЕРАТ

В рамках любого теоретического исследования ключевой вопрос — понятийно-терминологический аппарат. Однако проблематика информационной политики имеет не только теоретический, но прежде всего практический характер. Информационная политика перестала быть заботой журналистов и чиновников. Секьюритизация — рассмотрение вопросов информационной политики в контексте вопросов национальной безопасности — это не только российский, но глобальный императив.

Ключевые слова: СМИ, информационная политика, секьюритизация, информационная война, информационное пространство, информационная безопасность, информационное превосходство

Для цитирования: *Долженкова Е.,* Межевич Н. М.*,* Хлутков А. Д. Секьюритизация информационной политики: обобщая накопленный опыт 2022 года // Управленческое консультирование. 2022. № 12. С. 10–17.

Securitization of Information Policy: A Generalization of the 2022 Experience

Ekaterina Dolzhenkova[1], *Nikolay M. Mezhevich*[2, 3, *], *Andrey D. Khlutkov*[2]

[1]Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation
[2]Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management, Branch of RANEPA), Saint Petersburg, Russian Federation
[3]Pskov State University, Pskov, Russian Federation; *mez13@mail.ru

ABSTRACT

Within the framework of any theoretical study, the key issue is the conceptual and terminological apparatus. However, the problems of information policy are not only theoretical, but primarily practical. Information policy has ceased to be the concern of journalists and officials. Securitization — considering information policy issues in the context of national security issues — is not only a Russian, but a global imperative.

Keywords: media, information policy, securitization, information war, information space, information security, information superiority

For citing: Dolzhenkova E., Mezhevich N. M., Khlutkov A. D. Securitization of Information Policy: A Generalization of the 2022 Experience // Administrative consulting. 2022. No. 12. P. 10–17.

Основной угрозой в области международной информационной безопасности является использование коммуникационных технологий в качестве информационного оружия для политических и военных целей, противодействие международному праву, национальному суверенитету государств, нарушения территориальной целостности государств и угрозы международному миру, безопасности и стратегической стабильности. «Безопасность — это самоотносимая практика, благодаря которой

проблема становится проблемой безопасности, необязательно в силу существования реальной экзистенциональной угрозы, а именно потому, что эта проблема представлена в качестве такой угрозы» [7, p. 24]. Укажем на то, что такая трактовка безопасности носит универсальный характер, а значит относится и к информационной безопасности. Трансформация «обычной» проблемы в системную угрозу безопасности — это процесс, имеющий специальное название в теории международных отношений — *секьюритизация*.

«Секьюритизация — это процесс осмысления государством ситуации, в ходе которого те или иные явления начинают им рассматриваться как угрозы безопасности, для нейтрализации которых могут быть использованы в том числе чрезвычайные действия» [6, с. 157]. Причины секьюритизации многообразны, но в наиболее общем плане они могут рассматриваться как неспособность государства и общества отражать угрозы в стандартном, традиционном формате. В этих условиях предполагаемая угроза объявляется чрезвычайной.

Рассмотрим этот тезис с позиций современных европейских практик. «Факты занимали священное место в западных либеральных демократиях. Если когда-то было похоже, что демократия пошла не туда, когда избирателями манипулировали или политики уклонялись от вопросов, мы обращались за спасением к фактам», — писал британский экономист Уильям Дэйвис [10]. Да, в настоящее время информация, набор фактов мешает комфортному существованию обществ и государств. «Европа после Второй мировой, а особенно холодной войны избавлялась от стратегического мышления в пользу прикладных мер по обеспечению комфортного существования»[1]. Что означает комфортное существование в контексте информационной политики? Ответ достаточно очевиден. Европейская «зона комфорта» предполагает добровольное отречение от ненужной, избыточной, но объективной информации. Иными словами, если объективная информация противоречит теоретической конструкции, то тем хуже для информации. Чем технологичнее общество, тем большей проблемой является сохранение свободы слова [4].

С нашей точки зрения, информация не может быть использована в качестве оружия в террористических целях, однако может придать теракту дополнительный поражающий эффект. Информация способна форсировать нарушение общественного порядка и способствовать разжиганию национальной, расовой и религиозной ненависти. Иными словами, информационная безопасность — элемент системы государственной и региональной безопасности, которая характеризуется в XXI в. как сугубо традиционными, так и новыми вызовами.

Российское, китайское, западное общества, иными словами, все высокотехнологические государства сталкиваются со сложнейшими информационными и гибридными угрозами. «Для поддержания безопасности и защиты государств недостаточно иметь вооруженные силы и разведку, необходимо учитывать общественность, образование и СМИ» [8]. Действительно, эффективные информационные «щит и меч» встречаются существенно реже, чем армия и/или разведка.

Информация — это любое сообщение или представление знаний, таких как факты, данные или мнения, в средствах массовой информации, в том числе в текстовой, числовой, графической, картографической, описательной или аудиовизуальной форме. Информацией является все, что способствует уменьшению неопределенности состояния системы. Обеспечение информации — это меры, которые защищают и отстаивают информацию и информационные системы путем обеспечения их доступности, целостности, аутентификации, конфиденциальности и без-

[1] *Лукьянов Ф.* Ловушка стратегического противостояния [Электронный ресурс] // Россия в глобальной политике. URL: https://globalaffairs.ru/articles/lovushka-protivostoyaniya/8.12.2022 (дата обращения: 09.12.2022).

отказности. Эти меры включают в себя обеспечение для восстановления информационных систем путем включения защиты, обнаружения и возможности реагирования [8; 9].

Информационная политика — деятельность, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая влияние на информационную инфраструктуру, саму информацию, а также на индивидуальное и общественное сознание.

Информационное политика осуществляется в информационном пространстве.

Информационное пространство — это любая среда, с помощью которой создается информация, передаются и принимаются данные, а также хранятся, обрабатываются или удаляются.

«В современных условиях происходит борьба за информационное пространство внутри государства, региона и союза. По причине того, что современные технологии позволяют стирать границы воздействия информации посредством сети Интернет, международными акторами создаются различные программы и механизмы информационного нападения и информационной защиты информационного воздействия. Так, НАТО разрабатывает и внедряет различные методы изучения информационной составляющей современного противоборства»[1].

Информационная безопасность — это достижение такого качественного состояния общества и государства, при которым обеспечивается отражение внешних и внутренних угроз, передающихся по всем коммуникационным каналам.

Можно сформулировать несколько иначе. Информационная безопасность — состояние защищенности национальных интересов в информационном пространстве; определяется сбалансированным сочетанием интересов личности, общества и государства.

Информационная война — это эскалация информационного конфликта между государствами, в которых информационные операции осуществляются государственными субъектами для военно-политических целей.

В понятие информационной войны в развернутом определении включается часть деятельности разведки, контрразведки, дезинформация, радиоэлектронная война, нападение на вражеские коммуникации, защита своих коммуникаций, классическая пропаганда и контрпропаганда.

Информационная война — это противостояние между двумя или более правительствами в информационном пространстве с целью повредить системы, процессы и ресурсы, критически важные для контрагента. В свою очередь, определение информационного оружия, принятое в ООН и РФ, — это средства и методы, используемые с целью повредить информационные ресурсы, процессы и системы другого государства; использование информации в ущерб обороне того или иного государства, административных, политических, социальных, экономических или других жизненно важных систем, а также средства массовой манипуляции населения того или иного государства с целью дестабилизации общества и государства[2].

«Информационная война — это форма коммуникативных технологий, целью которой является достижение информационного превосходства в интересах достижения целей национальной стратегии.

Субъектом информационных войн являются нации, государства, компании, а *объектом* — массовое сознание.

---

[1] *Долженкова Е.В.* Роль Латвии в обеспечении информационного превосходства НАТО // Вектор науки Тольяттинского государственного университета. 2016. № 1. С. 73.

[2] NATO Cooperative Cyber Defence Centre of Excellence. Terms and Definition [Электронный ресурс]. URL: https://ccdcoe.org/cyber-definitions.html (дата обращения: 09.11.2022).

Придерживающиеся аналогичных взглядов ученые видят информационную войну как форму борьбы с использованием социальных средств и методов влияния на чужие информационные ресурсы с защитой собственных»[1]. В психологическом контексте объектом информационной войны выступает когнитивно-эмоциональная сфера индивидов, а целью — управление интеллектуально психологическими и социокультурными процессами, обязательным элементом которого выступает неосознанность данного воздействия лицами, подверженными завуалированному влиянию и следующими линии запрограммированного поведения.

Л. Н. Кунакова одной из первых в рамках российского академического сообщества попыталась проанализировать понятие информационных войн. С ее точки зрения, «подготовленный информационный поток одного государства с определенными целями конкурирует с информационным потоком другого государства.

В рамках психологической парадигмы информационная война понимается как латентное воздействие информации на индивидуальное, групповое и массовое сознание при помощи методов пропаганды, дезинформации, манипулирования с целью формирования новых взглядов на социально-политическую организацию общества через изменение ценностных ориентаций и базовых установок личности» [3].

В настоящее время введены в работу различные методы информационной войны, одним из которых можно считать создание ложной информации для дезинформации общества. Это можно наблюдать не только в странах, ведущих гибридную войну напрямую, но и косвенно к ним относящихся, что позволяет сформировать ложное мнение общества по тем или иным вопросам, а также сформировать сознание мирового сообщества в нужном направлении.

В информационной войне достигаются такие цели, как дезинформация общественного сознания, распространение идеологии, привлечение сторонников, доступ к информационным ресурсам, снижение или увеличение роли государства, создание негативного отношения общества к определенным вопросам, распространение ложных мнений. В интернет-ресурсах активно развивается сектор агитационного и пропагандистского характера. Средства массовой информации также активно ведут работу с интернет-ресурсами как источниками информации. Информация в интернет-сети с каждым днем набирает силу в воздействии на общество, формируя мнение население по тем или иным вопросам[2]. Этому способствует общедоступность и быстрое распространение информации без каких-либо ограничений. Все это позволяет достигать целей информационной войны, таких как изменение сознания общества, формирование его мировоззрения и отношения к определенным вопросам. Если изменение сознания — цель, то обретение информационного превосходства — средство.

Информационное превосходство — это такое состояние конкуренции в информационной сфере, при котором одна из сторон добилась преимущества в проведении своей информационной политики или в обеспечении безопасности от чужих информационных нарративов.

«Идеи современного информационного противоборства сформированы с развитием глобальной информационной среды и информационной сферы общества при участии высших должностных лиц государства, а также при участии правительственных и неправительственных структур. Информационное противоборство в современных условиях рассматривается совместно с вооруженной борьбой, политико-дипломатическим противоборством, экономической конкуренцией, межгосударственным научно-техни-

[1] Формирование общественного мнения [Электронный ресурс]. URL: https://mybiblioteka.su/5-29600.html (дата обращения: 09.11.2022).

[2] *Долженкова Е.В.* Роль Латвии в обеспечении информационного превосходства НАТО. С. 76.

ческом соперничеством, где объектами информационного воздействия являются высшее политическое и военное руководство, общественное мнение, информационные и телекоммуникационные системы, средства и системы связи противоборствующих государств, информационные ресурсы, средства информатизации вооружения и военной техники, информационные системы органов государственной власти, банковская и хозяйственная сферы. Информационное превосходство сейчас — это, прежде всего, способность органов управления к сбору, обработке и распространению непрерывного потока информации. Психологическая готовность войск с одновременным затруднением управления и управляемости противника стали возможны благодаря технологиям современного мира, расширяющим места конфликта с помощью социальных сетей, электронных баз данных и телевизионных экранов [2]»[1].

Социологи рассматривают информационное превосходство на социально-коммуникативном уровне, где в основном исследуется сама информация, оказывающая влияние в интерактивной реальности и формирующая когнитивные ориентации.

Однако нам важнее подход специалистов в сфере международных отношений. Они рассматривают информационное превосходство в рамках глобализации, проводят связь с геополитическими отношениями, когда одни акторы международного процесса с помощью активного воздействия на информационное пространство других стремятся получить превосходство в экономической, военной, политической и других областях. В этом же контексте можно рассматривать информационную войну через призму военно-стратегического направления, где информационное превосходство выступает в виде альтернативы классического военного конфликта, который может выступать как в самостоятельной форме, так и в форме военных действий с образованием сетевой и кибервойны.

Изначально информационное превосходство или информационная война использовалась в военных действиях и деятельности разведки. В современном мире произошли качественные изменения, и цель информационного превосходства направлена на всех, т. е. на массовое сознание.

Массовое информационное доминирование достигается за счет компьютеризации военной техники и формирования сетевой организации вооруженных сил, с применением собственных электронных технологий, а также с разрушением информационных систем противника.

Таким образом, *информационное превосходство* — результат информационных акций, осуществляемых на стратегическом, оперативном и тактическом уровнях в мирное и военное время, в информационной сфере, как среди своих граждан, так и среди населения страны-противника.

Современные технологии позволили создать новые способы ведения военных действий. Одним из таких способов является гибридная война. *Гибридная война* — современный способ ведения военных действий, сочетающий в себе классические методы военных операций с партизанской войной, терроризмом, информационной (кибервойной), биологической войной [5]. В. А. Романова отмечает, что увеличение роли информации привело к увеличению роста информационных противоборств. Политические и военные элиты осознали тот факт, что в современном мире общество зависит от информационно-телекоммуникационных систем, что учитывается при разработке технологий воздействия на сознание людей. Сегодня является общепризнанным фактом то, что информация может быть оружием, обладающим массовым воздействием на умы людей. Соответственно, признан факт существования гибридной войны[2].

---

[1] Там же, с. 75–76.

[2] *Долженкова Е.* Положение русскоязычного населения во внешней политике Латвийской Республики : дис. … канд. полит. наук. СПб., 2018.

Существующие определения гибридной войны весьма разнообразны. Однако во всех есть два общих звена. Гибридная война — это, во-первых, вид враждебных действий, как тайных, так и явных. Во-вторых, в рамках гибридной войны нападающая сторона не осуществляет классическое военное вторжение, но при этом достигает поставленных целей, т. е. победы.

Ряд авторов указывает на то, что гибридная война — это сочетание регулярных методов военной разведки и контрразведки, а также информационной и кибер-войны [см., например, 9].

Гибридная война с масштабной информационной составляющей — это достаточно очевидное основание для секьюритизации внешней и внутренней политики. «В процессе секьюритизации определяется, какие угрозы носят характер экзистенциальной опасности, требуют принятия неотложных мер и проведения политики особого рода» [1, с. 21].

В контексте секьюритизации и вопросов СВО это выглядит следующим образом: информационная мина, связанная с дискредитацией России, подкладывается в первоисточник — европейское издание с «пониженной информационной ответственностью», но расположенное в западноевропейской стране с позитивной репутацией, на втором этапе осуществляется «раскрутка» уже в Чехии, Польше, Литве, причем максимально массово. При этом параллельно — точечно ставится задача проникновения в российские «околооппозиционные» СМИ. На третьем этапе собственно украинскому читателю сбрасывается «единое европейское мнение» в сочетании «с российскими признаниями».

Приведенные оценки не означают того, что раньше такого явления не было. Однако 20–30 лет назад не существовало технологических возможностей фактически одномоментного строительства «эхо-комнаты». Описанная задача решалась в течение недели, теперь все этапы можно провести за день-два.

Побочный эффект описанной ситуации заключается в том, что сформированное методом «эхо-комнаты» общественное мнение анализируется с большей или меньшей академичностью, но в любом случае «заказчик» сам становится жертвой собственного информационно-политического заказа. Экстраполируя эту позицию на общую проблему безопасности, отметим, что в реальной жизни секьюритизация информационной политики может выступать и как реальная проблема, и как способ решения иных задач экономического, политического, военного характера через отвлечение общественного внимания «на негодные объекты».

Парадоксально, но попытки секьюритизации информационных потоков могут работать против организаторов этого процесса. Крайне серьезной проблемой является то, что лицо, принимающее решение, в большей или меньшей степени является потребителем пропаганды, инициированной им самим. Когда политики Польши или Эстонии заявляют о том, что в России заканчиваются ракеты, хлеб и ежи, они не только выдают желаемое за действительное, но и демонстрируют свое пребывание в «эхо-комнате», где эстонская газета ссылается на телевидение Латвии, телевидение Латвии на польское радио, а польское радио, в свою очередь, на эстонскую газету. Круг замкнулся, показав нам отсутствие изначального информационного контента при обилии информационных сбросов.

Подведем итоги. «Любая теория функциональна и способна работать, если фокусируется лишь на определенном круге явлений и фактов» [1, с. 24]. Теории секьюритизации предполагают превращение информационной политики в ключевой компонент системы национальной безопасности. Однако еще важнее практическая сторона вопроса. Позиционирование информации как условия победы в войне трансформировалось в понимание информационного превосходства как самой победы.

Литература

1. *Гайдаев О. С.* Теория секьюритизации, или Хорошо забытое старое: к вопросу о теоретико-философских истоках и зарождении теории // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2021. Т. 21. № 1. С. 20–32. DOI: 10.22363/2313-0660-2021-21-1-20-32.
2. *Комлева Е. В.* Социальная роль ядерных технологий и общественное сознание // Философия науки. 2003. № 2. С. 109–117.
3. *Кунакова Л. Н.* Информационная война как объект научного анализа (понятие и основные характеристики информационной войны) // Альманах современной науки и образования. 2002. № 6. С. 93–96.
4. *Ровинская Т. Л.* Свобода слова в условиях цифровой диктатуры IT-корпораций // Полис. Политические исследования. 2022. № 2. С. 22–36. DOI: 10.17976/jpps/2022.02.03.
5. *Романова В. А.* Информационная составляющая гибридных войн современности // Государственное и муниципальное управление. Ученые записки СКАГС. 2015. № 2. С.293–299.
6. *Эйвазов Д.* Секьюритизация и региональная активность держав на примере политики России в украинском кризисе // Международные процессы. 2017. Т. 15. № 4. С. 156–173. DOI: 10.17994/IT.2017.15.4.51.9.
7. *Buzan B., Waever O., de Wilde J.* Security: A New Framework for Analysis. London: Lynne Rienner Publishers, 1998.
8. *Daugulis M.* The Challenges of Hybrid-Warfare and Cyber-Threats: The Role of Self-Defense in a Changing Security Environment // Towards Reassurance and Solidarity in the Euro-Atlantic Community. Riga Conference Papers. 2015. P. 151–156.
9. *Daugulis M.* The Role of Cyber Defence in Hybrid Warfare Conditions: Proper Way for Latvia in Redefinition of Defence and Educational Policy Areas Under the Changing Security Circumstances // Latvian Foreign and Security Policy. Yearbook. 2016. P. 89–96.
10. *Davies W. The* Age of Post-Truth Politics // The New York Times, Aug. 24, 2016. URL: https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post- truth-politics.html (дата обращения: 09.11.2021).

Об авторах:

Долженкова Екатерина, доцент Высшей школы юриспруденции и судебно-технической экспертизы Санкт-Петербургского политехнического университета Петра Великого (Санкт-Петербург, Российская Федерация), кандидат политических наук; skinx@inbox.lv

Межевич Николай Маратович, заведующий лабораторией стратегического планирования и евразийской интеграции Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация), главный научный сотрудник научно-исследовательской лаборатории «Центр комплексного изучения проблем региональной безопасности» Псковского государственного университета (Псков, Российская Федерация), доктор экономических наук, профессор; mez13@mail.ru

Хлутков Андрей Драгомирович, директор Северо-Западного института управления — филиала РАНХиГС (Санкт-Петербург, Российская Федерация), доктор экономических наук, доцент; khlutkov-ad@ranepa.ru

References

1. Gaidaev O. S. Securitization Theory or a Well Overlooked Old: On the Philosophical and Theoretical Premises and Origins of the Theory // Vestnik RUDN. International Relations [Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Mezhdunarodnye otnosheniya]. 2021. Vol. 21, N 1. P. 20–32. DOI: 10.22363/2313-0660-2021-21-1-20-32 (In Rus).
2. Komleva E. V. Social role of nuclear technologies and social consciousness // Philosophy of science [Filosofiya nauki]. 2003. N 2. P. 109–117. (In Rus).
3. Kunakova L. N. Information war as an object of scientific analysis (concept and main characteristics of information war) // Almanac of modern science and education [Al'manakh sovremennoi nauki i obrazovaniya]. 2002. N 6. P. 93–96. (In Rus).
4. Rovinskaya T. L. Freedom of speech amid the digital dictatorship of IT corporations // Polis. Political Studies [Polis. Politicheskie issledovaniya]. 2022. N 2. P. 22–36. DOI: 10.17976/jpps/2022.02.03 (In Rus).

5. Romanova V. A. Information component of hybrid wars of our time // State and municipal administration. SCAGS scientific notes [Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski SKAGS]. 2015. N 2. P. 293–299. (In Rus).
6. Eyvazov J. Securitization and regional activity of a major power the case of Russia's policy during the Ukrainian crisis // International Trends [Mezhdunarodnye protsessy]. 2017. Vol. 15, N 4. P. 156–173. DOI: 10.17994/IT.2017.15.4.51.9 (In Rus).
7. Buzan B., Waever O., de Wilde J. Security: A New Framework for Analysis. London: Lynne Rienner Publishers, 1998.
8. Daugulis M. The Challenges of Hybrid-Warfare and Cyber-Threats: The Role of Self-Defense in a Changing Security Environment // Towards Reassurance and Solidarity in the Euro-Atlantic Community. Riga Conference Papers. 2015. P. 151–156.
9. Daugulis M. The Role of Cyber Defence in Hybrid Warfare Conditions: Proper Way for Latvia in Redefinition of Defence and Educational Policy Areas Under the Changing Security Circumstances // Latvian Foreign and Security Policy. Yearbook. 2016. P. 89–96.
10. Davies W. The Age of Post-Truth Politics // The New York Times, Aug. 24, 2016. URL: https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post- truth-politics.html (date of application: 09.11.2021).

About the authors:

Ekaterina Dolzhenkova, Associate Professor of the Higher School of Jurisprudence and Forensic Technical Expertise, Peter the Great St. Petersburg Polytechnic University (St. Petersburg, Russian Federation), PhD in Politic Science; skinx@inbox.lv

Nikolay M. Mezhevich, Head of the Laboratory of Strategic Planning and Eurasian Integration of the North-West Institute of Management, Branch of RANEPA (St. Petersburg, Russian Federation), Chief Researcher of the Research Laboratory "Center for the Integrated Study of Regional Security Problems" of Pskov State University (Pskov, Russian Federation), Doctor of Economic Sciences, Professor; mez13@mail.ru

Andrey D. Khlutkov, Director of North-West Institute of Management, Branch of RANEPA (St. Petersburg, Russian Federation), Doctor of Science (Economics), Associate Professor; khlutkov-ad@ranepa.ru