УДК 316.77:004.8+321.01 EDN KQNDWI

Экзогенные социальные технологии и эрозия государственной субъектности в цифровой среде: к концепции социокультурного иммунитета и опережающего управления

© Н.А. Чемезов

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Исследовано, как экзогенные социальные технологии, действующие в информационно насыщенной и алгоритмически опосредованной цифровой среде, снижают государственную субъектность за счет воздействия на архитектуру внимания, доверия и публичной интерпретации. Показано, что решающим становится не только распространение недостоверных сообщений, но и технологически поддержанное управление конфигурациями поведения аудитории (выбором повестки, динамикой доверия, идентичностной лояльностью и готовностью к коллективному действию), усиливаемое рекомендательными алгоритмами, микротаргетированием и сопряжением информационных операций с киберинцидентами.

Ключевые слова: *экзогенные социальные технологии, государственная субъектность, алгоритмические системы, архитектура внимания, архитектура доверия, FIMI, информационные расстройства, социокультурный иммунитет, риск-менеджмент ИИ, опережающее управление*

Смещение центров социального управления в цифровую среду сформировало парадоксальную ситуацию: рост управляемости отдельных процессов (измеримость поведения, скорость коммуникаций, автоматизация процедур) сопровождается усилением уязвимости сложных обществ к внешним воздействиям, конструируемым как воспроизводимые технологические комплексы. В информационно насыщенной среде эффективность влияния все чаще определяется не прямой принудительностью, а способностью структурировать повестку, закреплять интерпретации и задавать траектории коллективного поведения. Это сближает цифровые режимы влияния с логикой мягкой силы, где важным ресурсом власти выступает способность формировать рамки легитимации и структурировать ситуацию так, чтобы выбранные интерпретации и решения воспринимались как предпочтительные и естественные [1, с. 166, 167]. Такая динамика свидетельствует об усложнении социальных технологий, применяемых в управлении социумом [2, с. 55].

Социальные технологии, по мнению автора настоящей статьи, уместно трактовать как проектируемые и институционально закрепляемые комплексы средств, процедур и организационных решений, переводящие желаемые изменения в воспроизводимые практики. Их технологичность проявляется в стандартизации шагов, тиражируемости, управляемости ресурсов и возможности контроля результатов. В цифровую эпоху эта технологичность все чаще переносится с уровня организации действий на уровень организации условий действия: проектируются режимы видимости, доверия и убедительности, т. е. условия, при которых одни формы поведения и кооперации становятся вероятнее других. Внешнее происхождение таких комплексов само по себе не является решающим; принципиально то, что внедряемые процедуры и инфраструктуры оказываются несоразмерны локальным ценностно-нормативным основаниям и институциональным режимам. В результате повышается вероятность конфликтов интерпретации, разрыва доверия и управленческой фрагментации, а социальная технология начинает работать как механизм перестройки публичного опыта, а не только как набор инструментов коммуникации.

Цель настоящего исследования заключается в том, чтобы показать: эрозия государственной субъектности в цифровой среде чаще обусловлена не единичными информационными вбросами, а устойчивыми технологическими режимами управления вниманием и поведением, поддержанными алгоритмическими системами и платформенными инфраструктурами.

Методологическая база исследования включает, во-первых, поведенчески-ориентированное описание манипулятивных операций (FIMI), фиксирующее координированность и намеренность действий независимо от того, являются ли отдельные сообщения «ложными» и подпадают ли они под прямой запрет [3, с. 4].

Во-вторых, используется типология информационных расстройств (mis-/dis-/mal-information) и представление об их жизненном цикле, позволяющее анализировать не один фейк, а всю цепочку производства и распространения воздействия [4, с. 5, 6].

В-третьих, привлекаются нормативно-управленческие подходы к алгоритмическим системам и риск-менеджменту искусственного интеллекта (ИИ) [5, с. 20–22; 6, с. 8, 9].

В-четвертых, учитывается междоменная связка информационных операций и киберкомпонента, повышающая правдоподобие и масштабируемость воздействия [7, с. 4], а также прогнозные оценки усложнения киберугроз на горизонте до 2030 г. [8, с. 1].

Государственная субъектность в данном контексте рассматривается как интегральная способность политико-административной системы формулировать и удерживать целеполагание, обеспечивать согласование институтов, поддерживать доверие к процедурам принятия решений и сохранять автономию публичной интерпретации, т. е. способность задавать устойчивые рамки допустимых смыслов и воспроизводить политико-правовой порядок. В цифровой среде эта субъектность становится зависимой от управления архитектурой внимания и архитектурой доверия: если ключевые механизмы видимости, ранжирования и распространения смыслов вынесены в инфраструктуры, не подотчетные национальным процедурам, государство сталкивается с дефицитом управленческой автономии даже при формальном сохранении юридических полномочий.

Важнейшая особенность современных экзогенных воздействий состоит в том, что они все чаще действуют на уровне организации поведения аудитории, а не на уровне проверки истинности отдельных сообщений. В рамках FIMI объектом анализа становится координированная и преднамеренная активность, способная негативно влиять на ценности, процедуры и политические процессы, причем значимая часть таких действий может оставаться «в основном не незаконной», что принципиально осложняет правовое реагирование [3, с. 4]. Отсюда следует, что эффективность экзогенных технологий проявляется даже при ограниченном объеме прямой дезинформации, достаточно системно смещать повестку, усиливать поляризацию, изменять распределение доверия и подрывать предсказуемость коллективного действия.

Типология информационных расстройств уточняет «материал», на котором работают экзогенные технологии. Разведение misinformation (ложное без намерения вреда), disinformation (ложное с намерением вреда) и mal-information (основанное на реальности, но используемое для причинения вреда) позволяет анализировать не только фабрикации, но и технологическое использование фактов для делегитимации и разрушения доверия [4, с. 20, 21]. Именно mal-information оказывается особенно значимой в ситуациях утечек, доксинга, селективной публикации и вырывания данных из контекста: формально опираясь на реальность, такая коммуникация разрушает доверие через контекстуальную подмену и моральную дискредитацию. Представление о жизненном цикле информационных расстройств (создание — производство — распространение) задает практический вывод: борьба с отдельными фейками структурно недостаточна, поскольку эффект достигается не единичным объектом, а воспроизводимой цепочкой производства и усиления воздействия [4, с. 23].

Алгоритмические системы[1] выступают центральным усилителем экзогенных технологий, поскольку они формируют «невидимую конституцию» цифровой публичности: определяют, какие сообщения получают преимущество в видимости, какие аудитории считаются релевантными, какие формы поведения вознаграждаются вовлеченностью, а какие вытесняются. В такой конфигурации воздействие переносится с уровня убеждения на уровень селекции и распределения внимания. Нормативные подходы к алгоритмическим системам подчеркивают необходимость оценивать их через призму прав человека, недискриминации, прозрачности, ответственности и оценки воздействия, поскольку системное влияние алгоритмов затрагивает доступ к информации, равенство возможностей и реализацию свобод [6, с. 8, 9]. Для государственной субъектности это означает, что утрата процедурной подотчетности над инфраструктурами ранжирования и распространения смыслов трансформируется в утрату способности стабильно удерживать повестку и легитимность, даже если государство сохраняет формальные компетенции в иных областях.

Существенным обстоятельством является гибридизация экзогенных технологий, в которой информационное влияние сопрягается с киберинцидентами: взломами, утечками, подменой контента, атаками на инфраструктуры коммуникации. Междоменный анализ Агентства Европейского союза по кибербезопасности (ENISA) и Европейской службы внешних действий (EEAS) показывает, что киберэлементы нередко выступают ускорителями информационного воздействия: обеспечивают доступ к данным, повышают правдоподобие нарратива, создают событийные триггеры и усиливают распространение [7, с. 4, 5].

В перспективе до 2030 г. ожидается дальнейшее усложнение киберугроз и рост роли гибридных сценариев, что делает проблему экзогенных технологий устойчивой характеристикой будущей среды управления, а не временным отклонением [8, с. 1].

Для описания способности общества и государства сохранять управленческую автономию при таких воздействиях необходимо ввести ключевое понятие для данного исследования — социокультурный иммунитет. Под ним понимается способность общества и государства распознавать экзогенные социальные технологии и их поведенческие цели, удерживать ценностно-нормативное ядро при

---

[1] Под алгоритмическими системами будем понимать социотехнические комплексы, включающие алгоритмы, данные, вычислительную инфраструктуру и организационные процедуры, которые автоматически или полуавтоматически осуществляют отбор, ранжирование, профилирование, рекомендацию, модерацию, прогнозирование и иные операции обработки информации, тем самым влияя на распределение видимости, внимания, доверия и допустимых траекторий поведения в цифровой среде.

внешнем влиянии, интегрировать внешние инновации без разрушения доверия и институциональной согласованности, а также переводить конфликт интерпретаций в публично проверяемые процедуры, не доводя его до фрагментации и радикализации. Иммунитет в данном смысле не является метафорой закрытия; он фиксирует адаптивную устойчивость, т. е. способность не только отражать воздействие, но и учиться на нем, повышая качество институтов и коммуникаций, особенно в условиях серой зоны, когда воздействие не всегда подпадает под прямые запреты и не имеет очевидного центра управления [3, с. 4]. По мнению автора настоящей статьи, социокультурный иммунитет целесообразно понимать как согласованную работу нескольких взаимосвязанных уровней, таких как:

- эпистемический: наличие у общества устойчивых практик различения фактов, мнений и манипуляций, а также привычки к проверке информации, особенно в случаях mal-information, когда используются реальные сведения, но контекст подается так, чтобы исказить смысл [4, с. 20, 21];
- нормативный: согласованные представления о допустимых целях и средствах публичной коммуникации, о границах манипуляции и критериях легитимности, на этом уровне ключевыми являются подотчетность алгоритмических систем и оценка их воздействия [6, с. 8–10];
- институциональный: способность государственных и общественных институтов координировать ответ без разрушения плюрализма и доверия; прозрачные процедуры и понятные механизмы апелляции снижают пространство для скрытого управления повесткой [6, с. 9, 10];
- инфраструктурный: наличие инструментов мониторинга, раннего предупреждения и кризисной коммуникации, поскольку информационные операции все чаще сопрягаются с киберкомпонентом, а риски усложняются [7, с. 4, 5; 8, с. 1].

В совокупности согласованность этих уровней определяет, способно ли общество сохранять доверие и управленческую связность в условиях ускоряющихся технологических изменений.

Из концепции социокультурного иммунитета следует, что укрепление устойчивости не может ограничиваться реактивной логикой (обнаружили — опровергли — заблокировали), поскольку такая логика структурно запаздывает и действует уже после разрушения доверия и координации. Более адекватным становится подход к экзогенным социальным технологиям как к рискам сложной системы, где цель управления состоит в снижении вероятности и масштаба ущерба при сохранении правомерности и легитимности мер. В этом отношении подходы риск-менеджмента ИИ предоставляют язык и процедурную

логику работы с рисками: формирование контекстов применения, измерение эффектов, управление и регулярный пересмотр мер в цикле [5, с. 20–22]. Встраивание такой логики в публичное управление позволяет оценивать не только контент, но и воздействие на поведение, доверие и процедуры, т. е. на те параметры, по которым проявляется эрозия субъектности.

Укрепление субъектности в цифровой среде требует институциональной подотчетности алгоритмических систем как условия суверенного целеполагания. Имеется в виду не технологический запрет, а создание процедур наблюдаемости и проверяемости: понимание того, кто и по каким правилам принимает решения о ранжировании, модерации и профилировании; наличие оценок воздействия на права и недискриминацию, развития механизмов объяснимости и независимого аудита; существование институциональных каналов обжалования и восстановления нарушенных прав [6, с. 8–10]. Поскольку алгоритмические системы влияют на распределение видимости и доверия, их процедурное встраивание в режимы публичной подотчетности становится прямым условием сохранения управленческой автономии [9, с. 20–22].

Дополнительным элементом опережающего управления является инфраструктура раннего предупреждения и сценарного прогнозирования. Экзогенные технологии развиваются быстрее формальных регуляторных циклов, поэтому требуются постоянный мониторинг координированного манипулятивного поведения (в терминах FIMI) [3, с. 11, 12], интеграция мониторинга информационных операций с реагированием на киберинциденты [7, с. 4, 5] и сценарное прогнозирование на горизонтах нескольких лет с учетом гибридизации угроз [8, с. 1]. Практически значимым критерием становится способность выявлять ранние признаки смены тактик и процедур воздействия, а не только повторяющиеся тематические нарративы, поскольку именно технологическая эволюция формирует будущие траектории рисков.

Наконец, опережающее управление упирается в доверие как стратегический ресурс. В логике мягкой силы легитимность и привлекательность институтов снижают сопротивление и повышают готовность следовать нормам и решениям [1, с. 167]. В цифровую эпоху доверие приобретает одновременно культурный и инфраструктурный характер: оно зависит от прозрачности процедур, качества публичных объяснений, согласованности институтов и предсказуемости правил. Экзогенные технологии, нацеленные на эрозию субъектности, в первую очередь атакуют доверие как универсального посредника между государством и обществом. Поэтому укрепление иммунитета предполагает не только информационные меры, но

и управленческую этику: честные процедуры, минимизацию манипулятивных практик в собственной коммуникации, отказ от решений, которые краткосрочно выгодны, но долгосрочно снижают доверие, включая непрозрачные алгоритмические решения в публичном секторе.

Таким образом, экзогенные социальные технологии в цифровой среде целесообразно анализировать как технологически оформленные комплексы, воздействующие на поведение, доверие и процедуры, а не только на содержание сообщений.

Эрозия государственной субъектности проявляется в снижении способности удерживать повестку, воспроизводить легитимность и обеспечивать институциональную согласованность. Поведенчески-ориентированные рамки FIMI фиксируют, что манипулятивные операции могут быть координированными и эффективными даже при минимальном объеме прямой дезинформации [3, с. 4], а типология информационных расстройств показывает, что значимую роль играют mal-information и контекстуальная подмена [4, с. 20, 21]. Алгоритмические системы усиливают экзогенные воздействия, формируя архитектуру видимости и доверия, что делает правозащитно-ориентированное управление алгоритмами необходимым условием устойчивости [6, с. 8–10]. Сопряжение информационных операций и киберкомпонента переводит проблему в междоменную плоскость, требующую единой рамки наблюдения и реагирования [7, с. 4, 5], а прогнозные оценки до 2030 г. указывают на необходимость сценарной подготовки и опережающей модернизации [8, с. 1].

В перспективе центральным становится развитие социокультурного иммунитета как институционально закрепленной способности распознавать и перерабатывать внешние технологически поддержанные воздействия без разрушения доверия и управленческой автономии, что предполагает связку подотчетности алгоритмических систем, риск-менеджмента ИИ в публичном секторе и инфраструктуры раннего предупреждения и прогнозирования.

ЛИТЕРАТУРА

[1] Nye J.S. Jr. Soft Power. *Foreign Policy*, 1990, no. 80, pp. 153–171. DOI: 10.2307/1148580

[2] Tabassi E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. DOI: 10.6028/NIST.AI.100-1

[3] *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies)*. Strasbourg, Council of Europe, 2020, 15 p. URL: https://rm.coe.int/09000016809e1154 (дата обращения 03.04.2026).

[4] Magonara E., Malatras A. *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity — Threat Landscape*. DOI: 10.2824/7501

[5] European External Action Service. Strategic Communications, Task Forces and Information Analysis (STRAT.2), Data Team. *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence. February 2023*. URL: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf (дата обращения 03.04.2026).

[6] Wardle C., Derakhshan H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg, Council of Europe, 2017, 109 p.

[7] Mattioli R., Malatras A. *Foresight Cybersecurity Threats for 2030 — Update 2024*. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf (дата обращения 03.04.2026).

[8] Василенко Л.А., Мещерякова Н.Н. *Социология цифрового общества*. Томск, Изд-во Томского политехнического университета, 2021, 226 с.

[9] Талапина Э.В. Прозрачность алгоритмов искусственного интеллекта. *Право. Журнал Высшей школы экономики*, 2025, т. 18, № 3, с. 4–27. DOI: 10.17323/2072-8166.2025.3.4.27

Статья поступила в редакцию 30.03.2026

Ссылку на эту статью просим оформлять следующим образом:

Чемезов Н.А. Экзогенные социальные технологии и эрозия государственной субъектности в цифровой среде: к концепции социокультурного иммунитета и опережающего управления. *Гуманитарный вестник*, 2026, вып. 2. EDN KQNDWI

Чемезов Никита Андреевич — аспирант кафедры «Философия» МГТУ им. Н.Э. Баумана. e-mail: nikita.chemez@gmail.com

Exogenous Social Technologies and the Erosion of State Agency in the Digital Environment: Toward a Concept of Sociocultural Immunity and Proactive Governance

© N.A. Chemezov

Bauman Moscow State Technical University, Moscow, 105005, Russia

The impact of exogenous social technologies operating within an information-rich and algorithmically mediated digital environment on the reduction of state agency was examined. State agency is shown to be diminished through effects exerted on the architecture of attention, trust, and public interpretation. It is demonstrated that the decisive role is played not only by the dissemination of unreliable information, but also by the technologically enabled management of audience behavior configurations (including agenda selection, trust dynamics, identity-based loyalty, and readiness for collective action). These processes are reinforced by recommendation algorithms, microtargeting, and the integration of information operations with cyber incidents.

Keywords: *exogenous social technologies, state agency, algorithmic systems, attention architecture, trust architecture, FIMI, information disorders, sociocultural immunity, AI risk management, proactive governance*

REFERENCES

[1] Nye J.S. Jr. *Soft Power*. *Foreign Policy*, 1990, no. 80, pp. 153–171. https://doi.org/10.2307/1148580

[2] Tabassi E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. https://doi.org/10.6028/NIST.AI.100-1

[3] *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (adopted on April 8, 2020 at the 1373rd meeting of the Ministers' Deputies)*. Strasbourg, Council of Europe, Committee of Ministers, 2020, 15 p. Available at: https://rm.coe.int/09000016809e1154 (accessed April 3, 2026).

[4] Magonara E., Malatras A. *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity — Threat Landscape*. https://doi.org/10.2824/7501

[5] European External Action Service. Strategic Communications, Task Forces and Information Analysis (STRAT.2), Data Team. *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence*. February 2023. Available at: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf (accessed April 3, 2026).

[6] Wardle C., Derakhshan H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg, Council of Europe, 2017, 109 p.

[7] Mattioli R., Malatras A. *Foresight Cybersecurity Threats for 2030 — Update 2024*. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf (accessed April 3, 2026).

[8] Vasilenko L.A., Mescheryakova N.N. *Sotsiologiya tsifrovogo obschestva* [Sociology of the digital society]. Tomsk, Tomsk Polytechnic University Publ., 2021, 226 p.
[9] Talapina E.V. Prozrachnost algoritmov iskusstvennogo intellekta [Transparency of artificial intelligence algorithms]. *Pravo. Zhurnal Vysshey shkoly ekonomiki — Law. Journal of the Higher School of Economics*, 2025, vol. 18, no. 3, pp. 4–27. https://doi.org/10.17323/2072-8166.2025.3.4.27

Chemezov N.A., Postgraduate Student, Department of Philosophy, Bauman Moscow State Technical University. e-mail: nikita.chemez@gmail.com