**RUDN Journal of Political Science.** ISSN 2313-1438 (Print), ISSN 2313-1446 (Online) **2026 Vol. 28 No. 3 750–764**
**Вестник Российского университета дружбы народов. Серия: ПОЛИТОЛОГИЯ** http://journals.rudn.ru/political-science

# ПРОБЛЕМЫ БЕЗОПАСНОСТИ И РАЗВИТИЯ

# SECURITY AND DEVELOPMENT ISSUES

DOI: 10.22363/2313-1438-2026-28-3-750-764
EDN: HZWFBU

Научная статья / Research article

## Информационный риск-менеджмент в системе стратегического политического управления в условиях развития искусственного интеллекта: современные модели и механизмы

**Д.А. Мальцева[1, 2], А.В. Алейников[1] ✉, К.Е. Стребкова[1]**

[1]Санкт-Петербургский государственный университет, *Санкт-Петербург, Российская Федерация*

[2]Российский университет дружбы народов, *Москва, Российская Федерация*

✉ a.alejnikov@spbu.ru

**Аннотация.** В условиях цифровой трансформации управление информационными рисками приобретает системообразующее значение в архитектуре стратегического политического управления, определяя устойчивость институциональной среды, качество управленческих решений и уровень информационного суверенитета государства. Раскрываются три ключевые аналитические модели информационного риск-менеджмента — менеджмент знаний, коммуникационный менеджмент и информационный менеджмент — и прослеживается их качественная трансформация под воздействием технологий искусственного интеллекта. Особое внимание уделено смещению от реагирующих к проактивным стратегиям управления, в рамках которых ИИ выступает инструментом сценарного прогнозирования, ранней идентификации рисков и опережающего конструирования информационной повестки. Прослеживается, как современная система управления информационными рисками формируется в логике новой культуры принятия политических решений, основанной на данных (data-driven, data-informed, data-augmented) и предполагающей интеграцию инструментов прогнозирования, мониторинга, верификации и стратегической интерпретации информации. Рассматриваются актуальные практики применения больших языковых моделей, графов знаний, технологий поисковой генерации (RAG) и мультиагентного моделирования социально-политических процессов в контуре государственного управления. Обосновано, что обеспечение кибербезопасности, цифрового суверенитета и институционального доверия, а также развитие интеллектуализированных механизмов

© Мальцева Д.А., Алейников А.В., Стребкова К.Е., 2026

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License
https://creativecommons.org/licenses/by-nc/4.0/legalcode

противодействия деструктивным информационным воздействиям приобретают ключевое значение в условиях гибридных вызовов и возрастающей неопределенности. Сделан вывод о необходимости формирования суверенной ИИ-инфраструктуры и нормативно-этической рамки алгоритмического управления как условий обеспечения долгосрочной политической устойчивости государства.

**Ключевые слова:** информационный риск-менеджмент, стратегическое политическое управление, искусственный интеллект, кибербезопасность, цифровой суверенитет, институциональное доверие, информационная безопасность, гибридные угрозы

**Благодарности.** Публикация выполнена в рамках Госзадания № FSSF-2026-0078 «Риск-менеджмент в экосистеме стратегического политического управления РФ: архитектура решений в условиях развития искусственного интеллекта».

**Заявление о конфликте интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Для цитирования:** *Мальцева Д.А., Алейников А.В., Стребкова К.Е.* Информационный риск-менеджмент в системе стратегического политического управления в условиях развития искусственного интеллекта: современные модели и механизмы // Вестник Российского университета дружбы народов. Серия: Политология. 2026. Т. 28. № 3. С. 750–764. https://doi.org/10.22363/2313-1438-2026-28-3-750-764 EDN: HZWFBU

# Information Risk Management in the System of Strategic Political Governance in the Context of Artificial Intelligence Development: Contemporary Models and Mechanisms

**Daria A. Maltseva[1, 2], Andrei V. Aleinikov[1] ✉, Karina E. Strebkova[1]**

[1]Saint Petersburg State University, *St Petersburg, Russian Federation*

[2]RUDN University, *Moscow, Russian Federation*

✉ a.alejnikov@spbu.ru

**Abstract.** Under conditions of digital transformation, information risk management assumes a system-forming role within the architecture of strategic political governance, determining the resilience of the institutional environment, the quality of managerial decision-making, and the level of the state's information sovereignty. The article elaborates three core analytical models of information risk management — knowledge management, communication management, and information management — and traces their qualitative transformation under the influence of artificial intelligence technologies. Particular attention is devoted to the shift from reactive to proactive governance strategies, in which AI functions as an instrument of scenario-based forecasting, early risk identification, and anticipatory agenda construction. The research further examines how the contemporary system of information risk management is taking shape within the logic of a new data-based culture of political decision-making (data-driven, data-informed, and data-augmented), one that presupposes the integration of forecasting, monitoring, verification, and strategic information interpretation tools. Current practices involving large language models, knowledge graphs, retrieval-augmented generation (RAG), and multi-agent simulation of socio-political processes within public governance frameworks are analysed.

It is substantiated that ensuring cybersecurity, digital sovereignty, and institutional trust, alongside the development of intelligent mechanisms for countering destructive information influence, acquire critical importance in the face of hybrid threats and escalating uncertainty. The article concludes that the formation of a sovereign AI infrastructure and a normative-ethical framework for algorithmic governance constitute essential preconditions for the long-term political resilience of the state.

**Keywords:** information risk management, strategic political governance, artificial intelligence, cybersecurity, digital sovereignty, institutional trust, information security, hybrid threats

**Acknowledgements.** This publication was prepared within the framework of State Assignment No. FSSF-2026-0078 “Risk Management in the Ecosystem of Strategic Political Governance of the Russian Federation: Solution Architecture in the Context of Artificial Intelligence Development.”

**Conflicts of interest.** The authors declare no conflicts of interest.

**For citation:** Maltseva, D.A., Aleinikov, A.V., & Strebkova, K.E. (2026). Information risk management in the system of strategic political governance in the context of artificial intelligence development: Contemporary models and mechanisms. *RUDN Journal of Political Science, 28*(3), 750–764. (In Russian). https://doi.org/10.22363/2313-1438-2026-28-3-750-764 EDN: HZWFBU

## Введение

Обращение к проблематике стратегического управления позволяет осуществлять комплексный анализ механизмов устойчивости и адаптивности государства к «большим вызовам», в котором практика минимизации рисков сопрягается с институционализацией стратегических возможностей на фоне ускоряющихся политических и технологических трансформаций.

В современных условиях стратегическое управление все заметнее переориентируется не на нейтрализацию уже состоявшихся угроз, а на формирование механизмов упреждающего реагирования в среде, где неопределенность стала фоновой характеристикой [Пригожин 1991].

О.В. Гаман-Голутвина справедливо подчеркивает, что глобальная турбулентность превратилась сегодня в устойчивую характеристику современного миропорядка: за ней стоят ускоренная эскалация конфликтов, трансформация архитектуры безопасности, геоэкономическая фрагментация и разрушение ранее стабильных моделей политического и социального взаимодействия [Гаман-Голутвина 2024]. Эту логику развивал в иной, скорее трагической, тональности О.Н. Яницкий, связывая турбулентность с предельной степенью нестабильности мировой системы, сопровождающейся ростом рисков деградации и конфликтного передела ресурсов, ценностей и сфер влияния [Яницкий 2011: 158].

Современные исследования также фиксируют и другое: риски по-прежнему распределяются асимметрично, усиливая уязвимость одних социальных групп и территорий за счет других и воспроизводя структурные формы неравенства [Hall, Winlow 2003].

В этих условиях разработка интегративных подходов к анализу и управлению рисками перестает быть сугубо академической задачей, превращаясь в политический императив, особенно в информационной сфере, которая приобретает стратегическое значение.

Таким образом, актуальность исследования обусловлена необходимостью концептуализации нового институционального и аксиологического дизайна управления информационными рисками, формирующегося на пересечении логики нового общества риска и цифровой трансформации.

В данном случае речь идет о выработке новой архитектуры информационного взаимодействия и стратегического управления, основанной на интеграции данных, знаний и технологий искусственного интеллекта.

## Аналитические модели информационного риск-менеджмента

В условиях нарастающей информационной турбулентности и усложнения политико-коммуникационной среды принципиальное значение приобретает выбор базовой стратегии имплементации управления информационными рисками.

В наиболее общем виде можно выделить две полярные логики [Дамодаран 2010].

Первая — реагирующая — ориентирована на постфактум-реакции на уже реализовавшиеся риски и отличается ограниченной способностью работать с неопределенностью. Именно в этой логике У. Бек вводит концепт «организованной безответственности», схватывающий имитационные формы контроля над рисками: «Каждый является причиной и следствием и тем самым не является причиной. Причины растворяются во всеобщей взаимозависимости между агентами и условиями, реакциями и контрреакциями» [Бек 2000: 38].

Вторая, проактивная, напротив, предполагает опережающее прогнозирование и конструирование информационной среды. Ее эффективность сегодня все заметнее определяется развитием технологий искусственного интеллекта, выступающих инструментом ранней идентификации рисков.

Очевидно, что развитие проактивных подходов актуализирует необходимость выделения аналитических моделей, обеспечивающих системное сценарирование и управление информационными рисками. В этой связи представляется обоснованным выделить три взаимодополняющие модели информационного риск-менеджмента.

Первая — модель менеджмента знаний (Knowledge Management), которая ориентирована на изучение процессов генерации, дистрибуции, аккумуляции и рециркуляции знаний с последующей их трансформацией в систематизированную архитектуру риск-менеджмента. В современных реалиях политического управления данная модель переживает качественную трансформацию под воздействием ИИ, поскольку классические системы каталогизации данных уступают место нейросетевым семантическим поисковым механизмам, алгоритмам

автоматической категоризации и разметки сложноструктурированной информации [Jarrahi et al. 2023].

В плоскости практической реализации это предполагает использование технологий глубокого семантического анализа на базе архитектур больших языковых моделей (NLP/LLM) для автоматического извлечения неявного знания из слабоструктурированных массивов данных [Taherdoost, Madanchian 2023]. Ключевыми инструментами здесь становятся онтологический инжиниринг и построение динамических графов знаний, позволяющие выявлять скрытые каузальные связи и корреляции между разнородными политическими процессами, латентными акторами и зарождающимися гибридными угрозами [Earley 2023].

В своей современной конфигурации данная модель ориентирована на капитализацию государственного организационного знания и развитие когнитивной инфраструктуры общества, что способствует системному снижению рисков принятия управленческих решений [Baert, Rubio 2011].

Вторая модель — коммуникационного менеджмента (Communication Management) предполагает системный мониторинг и анализ рискогенных коммуникационных процессов, включая многостороннее взаимодействие политических акторов, траектории распространения информации и механизмы формирования общественного восприятия рисков. В условиях платформенного капитализма и алгоритмически опосредованной коммуникации данная модель претерпевает качественную трансформацию под воздействием искусственного интеллекта [Battista, Mangone 2025].

Ключевыми практиками в этой сфере становятся развертывание ИИ-платформ прослушивания социальных медиа для ранней идентификации кризисных сигналов, дезинформационных кампаний и аномалий в поведении сетевых сообществ; применение алгоритмов эмоционально-смыслового анализа тональности и нейросетевого тематического картирования для фиксации динамики общественных настроений и выявления латентных точек социальной напряженности; интеграция генеративного ИИ и интеллектуальных диалоговых ассистентов в контур государственных коммуникаций для обеспечения интерактивного взаимодействия с населением в условиях кризиса; применение генеративных языковых моделей для динамического конструирования и адаптации риторических фреймов политических сообщений с учетом ценностных и поведенческих профилей целевых аудиторий [Duberry 2022].

При этом сохраняется фундаментальная проблема, обозначенная К. Дэвисом и соавторами: асимметрия восприятия риск-коммуникации, приводящая к когнитивным искажениям и снижению эффективности взаимодействия [Davies, Covello, Allen 1987]. В современных условиях эта проблема существенно усложняется алгоритмической фильтрацией контента рекомендательными системами, что ведет к формированию замкнутых «информационных пузырей» (эхо-камер), затрудняющих трансляцию консолидирующих государственных нарративов [Cinelli et al. 2021].

В данном контексте особую актуальность приобретает концепция Н. Талеба «шкуры на кону» (skin in the game) [Талеб 2022], фиксирующая разрыв между распределением рисков и ответственности. В цифровой среде эта асимметрия проявляется с особой остротой: акторы, генерирующие и распространяющие деструктивный контент, практически избавлены от рисков ответственности, в то время как последствия их дезинформационной активности несут общество и государственные институты. Следовательно, управление коммуникационными рисками требует институционального выравнивания ответственности участников информационного обмена.

На современном этапе данная концепция получает развитие в рамках цифровых платформенных экосистем («Макс», ВКонтакте и др.), где политические акторы стремятся формировать управляемые информационные среды со своими алгоритмическими и поведенческими «правилами игры». Вместе с тем следует констатировать, что интеграция сквозных технологий ИИ в контур отечественных платформ пока носит фрагментарный характер и находится на этапе транзита. Если базовые функции автоматизации (чат-боты со строго запрограммированной логикой, модерация по ключевым словам и др.) реализованы достаточно масштабно, то технологии предиктивной аналитики и динамического когнитивного фрейминга внедрены лишь частично. Это создает стратегический вызов для отечественной ИТ-индустрии и государства, определяя необходимость форсированного развития собственных интеллектуальных инструментов управления коммуникациями для обеспечения безопасности суверенного медиапространства.

Завершая анализ, следует выделить модель информационного менеджмента (Information Management), ориентированную на разработку и реализацию стратегических сценариев в условиях, где ключевое значение приобретает комплексное управление информационными потоками, их содержанием, каналами распространения и эффектами восприятия [Мальцева, Сафонова, Тузова 2023]. В отличие от менеджмента знаний, ориентированного преимущественно на создание, накопление и трансфер знаний, а также коммуникационного менеджмента, сфокусированного на организации взаимодействия между акторами, информационный менеджмент охватывает полный цикл управления информацией — от ее отбора, верификации и интерпретации до обработки, распространения и оценки управленческих эффектов. [Davenport 1997].

В контексте стратегического политического управления информационный менеджмент представляет собой не просто совокупность технических процедур обращения с данными, но и самостоятельное направление риск-менеджмента, связанное с управлением информацией как стратегически значимым политическим ресурсом [McKnight 2013]. Его функциональное назначение заключается в выявлении и оценке информационных рисков, выборе адекватных механизмов реагирования и интеграции риск-ориентированных подходов в процессы политико-управленческого взаимодействия. В прикладном аспекте это предполагает организацию информационных процессов, аналитическую обработку

и интерпретацию данных, а также планирование информационного воздействия с учетом особенностей и ожиданий целевых аудиторий.

Актуальным методологическим инструментом описания данной логики выступает модель DIKAR, отражающая последовательный переход от данных к результату: Data — Information — Knowledge — Action — Result [Amodu, Ologbosere 2021]. На первом этапе данные, аккумулируемые в информационно-технологической инфраструктуре, проходят отбор, очистку и аналитическую подготовку. На втором — они трансформируются в информацию, приобретая контекст, структуру и первичную интерпретацию. На третьем этапе информация преобразуется в знание, обеспечивающее понимание причинно-следственных связей и потенциальных последствий происходящих процессов. Четвертый этап предполагает трансформацию знания в действие-принятие стратегических, административных и коммуникационных решений. На завершающем этапе осуществляется оценка результатов с точки зрения снижения рисков, стабилизации ситуации, корректировки поведения акторов и повышения эффективности управления.

Вместе с тем в условиях цифровой трансформации и усложнения архитектуры современных политических процессов классическая модель DIKAR требует концептуальной актуализации. Линейная логика перехода от данных к результату оказывается недостаточной. Данные могут характеризоваться неполнотой, фрагментарностью, алгоритмической предвзятостью, манипулятивной сконструированностью либо использоваться в ущерб публичным интересам. В этой связи модель DIKAR целесообразно дополнить контуром институционального контроля, верификации и защиты информации, обеспечивающим баланс между открытостью данных и требованиями информационной безопасности. В этих условиях одной из ключевых задач государства становится обеспечение прозрачности и доступности общественно значимой информации при одновременной минимизации рисков утечек, фальсификаций, кибервоздействий, дезинформационных кампаний и несанкционированного использования данных.

Особую актуальность в этом контексте приобретает проблема доступа к информации. Ограниченность цифровых архивов, фрагментарность государственных баз данных, устаревшие технологические инфраструктуры и несовершенство правовых режимов доступа снижают качество информационного обмена и ослабляют доверие к государственным решениям [McDermott 2008]. Однако противоположная крайность — неконтролируемая открытость — также порождает риски: уязвимость персональных данных, манипулятивное использование статистики, киберпреступность и распространение недостоверной информации.

Следовательно, современный информационный менеджмент должен быть ориентирован не только на расширение доступа к данным, но и на создание защищенной, проверяемой и управляемой информационной среды.

Именно в логике установления баланса между открытостью и безопасностью технологии искусственного интеллекта приобретают системообразующее значение в архитектуре современного информационного менеджмента. ИИ позволяет перейти от универсальных режимов доступа к информации

к их дифференцированным и адаптивным моделям, обеспечивая селективную прозрачность при одновременном сохранении контроля над чувствительными данными. В частности, системы на базе искусственного интеллекта могут использоваться для автоматической классификации информации по уровням доступа, выявления конфиденциальных данных с их последующей защитой или деперсонализацией, а также для мониторинга попыток несанкционированного доступа и аномалий в информационных потоках. Тем самым обеспечивается возможность расширения открытых данных без увеличения уязвимости системы: ИИ формирует управляемую архитектуру распространения информацией, где открытость становится контролируемым параметром.

Таким образом, на сегодняшний день искусственный интеллект выступает ключевым инструментом институционализации баланса между прозрачностью и безопасностью. Современная модель информационного менеджмента трансформируется в интеллектуализированную систему управления информационными рисками, где данные, знания, действия и результаты связываются не линейно, а через постоянный цикл мониторинга, анализа, верификации, прогнозирования и корректировки решений. В такой конфигурации искусственный интеллект не подменяет политическое решение, но становится инструментом его аналитического сопровождения, позволяя повысить скорость обработки информации, выявить скрытые закономерности, снизить неопределенность и обеспечить более ответственное управление информационными рисками.

## Новая архитектура принятия политических решений в условиях информационной турбулентности: культура данных

В условиях нарастающей информационной турбулентности и усложнения политико-коммуникационной среды формирование новой архитектуры принятия решений становится не просто следствием цифровизации, но ответом на необходимость институционализации обозначенного выше баланса между открытостью и безопасностью информационного пространства. В этих условиях особую значимость приобретает культура данных как основа рационализации управленческих процессов, которая предполагает не только расширение доступа к информации, но и ее структурированное, селективное и контролируемое использование в логике управления информационными рисками.

В авторской интерпретации данные выступают ключевым структурообразующим ресурсом доказательной политики (evidence-based policy). Ее практическое воплощение выражается в трех сопряженных моделях — алгоритмо-детерминированной (data-driven), доказательной (data-informed) и интеллектуально-расширенной (data-augmented), дифференцирующихся по степени интеграции алгоритмических систем в процессы принятия решений и уровню распределения субъектности между человеком и технологией [Höchtl et al. 2016].

Алгоритмо-детерминированная модель предполагает глубокую автоматизацию управленческих процессов на базе непрерывного потокового

анализа больших данных. В плоскости управления информационными рисками данный подход реализуется через развертывание предиктивных систем раннего предупреждения, где алгоритмы машинного обучения в автоматическом режиме выявляют аномалии в медиасреде. На смену классическим методам обработки естественного языка (NLP) приходят мультимодальные большие языковые модели (LLMs) и алгоритмы семантического векторного поиска [Zhao et al. 2026]. Они позволяют в режиме реального времени обрабатывать гетерогенные потоки данных (социальные медиа, мессенджеры, платформенные экосистемы) с целью обнаружения скрытых признаков манипулирования общественным мнением. При достижении математически заданных критических порогов система автоматически инициирует превентивные сценарии (например, таргетированное распределение верифицированного контента или генерацию встречных информационных импульсов). Для минимизации неопределенности до практического внедрения решений применяются методы мультиагентного социодинамического моделирования (где поведение общества симулируется популяциями автономных ИИ-агентов) и контролируемые поведенческие микротесты, оценивающие реакцию целевых аудиторий на альтернативные форматы государственной повестки [Park J.S. et al. 2023].

Доказательная модель представляет собой гибкий и институционально сбалансированный формат управления, в рамках которого искусственный интеллект выступает в качестве инструмента аналитической поддержки, сохраняя исключительную монополию на принятие окончательных решений за политическим субъектом. В рамках данной логики развертываются государственные интеллектуальные системы поддержки принятия решений, агрегирующие гетерогенные потоки данных из ведомственных и открытых источников в единые интерактивные когнитивные карты. Искусственный интеллект применяется здесь для многовариантного сценарного прогнозирования, выявления зарождающихся рискогенных трендов и оценки устойчивости социально-политической системы, что позволяет минимизировать когнитивные искажения и субъективизм административного аппарата в условиях неопределенности [Канеман, Словик, Тверски 2005]. В сфере стратегических коммуникаций данная модель реализуется через внедрение генеративных ИИ-архитектур, контролируемых технологиями поисковой генерации (RAG — Retrieval-Augmented Generation) [Lewis P. et al. 2020]. Это обеспечивает оперативную выработку верифицированных фактологических аргументов, адаптацию государственных сообщений под ценностные и поведенческие профили различных аудиторий, а также быстрое реагирование на информационные вызовы, существенно снижая риски асимметрии в восприятии рисков государством и обществом.

Интеллектуально-расширенная модель (data-augmented) ориентирована на качественное масштабирование когнитивного и прогностического потенциала субъекта управления без директивного навязывания алгоритмических траекторий. Ключевым инструментарием выступают здесь цифровые двойники

(digital twins) социально-политических процессов [Ratti, Claudel 2015] и системы динамического имитационного моделирования, позволяющие воспроизводить альтернативные варианты развития событий под воздействием внешних и внутренних шоков в условиях высокой неопределенности. В практической плоскости данная модель реализуется через интеллектуальные платформы партисипаторного (соучаствующего) проектирования и обратной связи [Zolkafli, Salleh 2025]. На таких платформах ИИ преобразует сложные массивы ведомственной информации в доступные для граждан интерактивные визуализации, объясняя логику принимаемых решений. Это не только повышает уровень легитимности государственной политики, но и вовлекает общество в процессы совместной верификации данных, создавая распределенную архитектуру снижения информационных рисков.

Вместе с тем интеграция обозначенных моделей работы с данными порождает специфические риски: скрытую алгоритмическую предвзятость базовых нейросетевых моделей, уязвимость данных к внешнему деструктивному воздействию и системное снижение доверия к обезличенным автоматизированным решениям. Особую угрозу в этой связи представляет когнитивная зависимость — латентное заимствование чуждых ценностных установок через алгоритмы зарубежных ИИ-платформ. В этих условиях критически важной становится институционализация механизмов выравнивания ценностей (AI Alignment) [Gabriel 2020] — проектирование суверенных моделей ИИ, обученных на национальных социокультурных и исторических базах знаний. Таким образом, требуется внедрение стандартов объяснимого искусственного интеллекта (XAI-Explainable AI) [Arrieta et al. 2020], гарантирующих прозрачность, интерпретируемость и воспроизводимость алгоритмических выводов для всех акторов политической системы. Только через формирование строгой нормативно-этической рамки и механизмов государственного аудита алгоритмов возможно превратить ИИ в безопасный элемент инфраструктуры стратегического политического управления.

Следовательно, современный информационный риск-менеджмент трансформируется в интеллектуализированную архитектуру стратегического управления, в которой технологии искусственного интеллекта обеспечивают переход от реактивных практик реагирования к проактивным моделям выявления, прогнозирования и предупреждения рисков. В этих условиях ключевое значение приобретают задачи обеспечения цифрового суверенитета, кибербезопасности и общественного доверия, гармонизация которых становится необходимым условием устойчивости и эффективности государственного управления в условиях нарастающей технологической сложности и глобальной турбулентности.

## Заключение

Проведенное исследование позволило установить, что в условиях возрастающей сложности, взаимосвязанности и динамичности современных угроз управление информационными рисками становится одним

из ключевых компонентов стратегического управления, определяющим способность государства обеспечивать устойчивость политической системы и качество принимаемых решений. В работе предложена целостная аналитическая рамка, интегрирующая информационный менеджмент, менеджмент знаний и коммуникационный менеджмент как взаимодополняющие элементы единой системы управления информационными рисками. Показано, что эффективность данной системы зависит не только от управления информационными потоками, но и от способности государства формировать, интерпретировать и использовать знания, обеспечивая контроль над когнитивными и коммуникационными процессами в политическом пространстве.

Особое значение в этих условиях приобретают технологии искусственного интеллекта, трансформирующие механизмы обработки информации, прогнозирования и поддержки принятия решений. Использование ИИ позволяет перейти от анализа отдельных угроз к выявлению сложных взаимосвязей между ними, моделированию сценариев развития и формированию более адаптивных управленческих стратегий. Вместе с тем расширение алгоритмического участия в политико-управленческих процессах актуализирует вопросы технологической зависимости, защиты данных, сохранения политической субъектности и обеспечения контроля над критически значимыми информационно-аналитическими функциями государства.

Анализ российской практики свидетельствует о формировании институциональных механизмов обеспечения информационного суверенитета и противодействия деструктивным информационным воздействиям. Вместе с тем дальнейшее развитие системы стратегического управления требует совершенствования нормативно-правовых и организационных механизмов интеграции интеллектуальных технологий с учетом задач национальной безопасности, цифрового суверенитета и устойчивого функционирования государственных институтов.

Таким образом, в условиях глобальной цифровой трансформации способность государства эффективно управлять информацией, знаниями и интеллектуальными технологиями становится одним из ключевых факторов обеспечения национальной безопасности, цифрового суверенитета и общественного доверия. В этой связи развитие интеллектуализированных механизмов управления информационными рисками следует рассматривать не только как направление технологической модернизации государственного управления, но и как важнейшее условие сохранения стратегической устойчивости и субъектности государства в XXI веке.

Поступила в редакцию / Received: 17.07.2026
Доработана после рецензирования / Revised: 30.07.2026
Принята к публикации / Accepted: 15.08.2026

## Библиографический список

*Бек У.* Общество риска: На пути к другому модерну. Москва : Прогресс-Традиция, 2000. 383 с.

*Гаман-Голутвина О.В.* Преддверие глобального конфликта или contra spem spero? // Сравнительная политика. 2024. № 3. С. 4–18. https://doi.org/10.46272/2221-3279-2024-3-15-8 EDN: FMXZIV

*Дамодаран А.* Стратегический риск-менеджмент : принципы и методики. Москва : И.Д. Вильямс, 2010.496 с.

*Канеман Д., Словик П., Тверски А.* Принятие решений в неопределенности : правила и предубеждения. Харьков : Гуманитарный Центр, 2005. 632 с.

*Мальцева Д.А., Сафонова О.Д., Тузова П.Р.* Стратегическое политическое планирование: управление информационными рисками // Проблемы национальной безопасности России: уроки истории и вызовы современности. Краснодар : Перспективы образования, 2023. С. 281–284. EDN: TBMYOQ

*Пригожин И.* Философия нестабильности // Вопросы философии. 1991. № 6. С. 16–57. EDN: PCHHNF

*Талеб Н.* Рискуя собственной шкурой: Скрытая асимметрия повседневной жизни. Москва : Колибри, 2022.384 с.

*Яницкий О.Н.* «Турбулентные времена» как проблема общества риска // Общественные науки и современность. 2011. № 6. С. 155–164. EDN: OJDVHZ

*Amodu A., Ologbosere T.* Critical overview of information management, DIKAR model and technology in the 21st century // Open Access. 2021. Vol. 1. No. 1. P. 35–39.

*Andress J.* Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Elsevier, 2013.

*Arrieta A.B. et al.* Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI // Information fusion. 2020. Vol. 58. P. 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

*Baert P., Rubio F.D.* The Politics of Knowledge. Milton Park : Routledge, 2011.

*Balasubramanian P. et al.* A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing // Decision Analytics Journal. 2025. Vol. 14. P. 100545. https://doi.org/10.1016/j.dajour.2025.100545

*Battista D., Mangone E.* Technological culture and politics: artificial intelligence as the new frontier of political communication // Societies. 2025. Vol. 15. No. 4. P. 75. https://doi.org/10.3390/soc15040075

*Cinelli M. et al.* The echo chamber effect on social media // Proceedings of the national academy of sciences. 2021. Vol. 118. No. 9. Article no. e2023301118. https://doi.org/10.1073/pnas.2023301118

*Davenport T.H.* Information ecology. Oxford : Oxford University Press, 1997.

*Davies C., Covello T.C., Allen F.W.* Risk Communication. Washington D.C : The Conservation Foundation, 1987.

*Duberry J.* Artificial intelligence and democracy: risks and promises of AI-mediated citizen–government relations. Cheltenham : Edward Elgar Publishing, 2022. https://doi.org/10.4337/9781788977319

*Earley S.* What executives need to know about knowledge management, large language models and generative AI // Applied Marketing Analytics. 2023. Vol. 9. No. 3. P. 215–229.

*Gabriel I.* Artificial Intelligence, Values, and Alignment // Minds and machines. 2020. Vol. 30. No. 3. P. 411–437. https://doi.org/10.1007/s11023-020-09539-2

*Hall S., Winlow S.* Rehabilitating Leviathan: Reflections on the State, Economic Regulation and Violence Reduction // Theoretical Criminology. 2003. Vol. 7. No. 2. P. 139–162. https://doi.org/10.1177/1362480603007002415

*Höchtl J., Parycek P.R., Schöllhammer R.* Big data in the policy cycle: Policy decision making in the digital era // Journal of Organizational Computing and Electronic Commerce. 2016. Vol. 26. No. 1–2. P. 147–169. https://doi.org/10.1080/10919392.2015.1125187

*Jarrahi M.H. et al.* Artificial intelligence and knowledge management: A partnership between human and AI // Business horizons. 2023. Vol. 66. No. 1. P. 87–99. https://doi.org/10.1016/j.bushor.2022.03.002

*Lewis P. et al.* Retrieval-augmented generation for knowledge-intensive NLP tasks // Advances in neural information processing systems. 2020. Vol. 33. P. 9459–9474.

*McDermott P.* Who Needs to Know? The State of Public Access to Federal Government Information. Lanham : Bernan Press, 2008.

*McKnight W.* Information Management: Strategies for Gaining a Competitive Advantage with Data. Oxford : Newnes, 2013.

*Park J.S. et al.* Generative agents: Interactive simulacra of human behavior // Proceedings of the 36th annual acm symposium on user interface software and technology. 2023. P. 1–22. https://doi.org/10.1145/3586183.3606763

*Ratti C., Claudel M.* Futurecra: Tomorrow by Design // Techne. Journal of Technology for Architecture and Environment. 2015. No. 10. P. 28–33.

*Taherdoost H., Madanchian M.* Artificial intelligence and knowledge management: Impacts, benefits, and implementation // Computers. 2023. Vol. 12. No. 4. P. 72. https://doi.org/10.3390/computers12040072

*Zhao W.X. et al.* A survey of large language models // Frontiers of Computer Science. 2026. Vol. 20. No. 12. P. 2012627. URL: https://arxiv.org/abs/2303.18223

*Zolkafli A., Salleh D.* Community Engagement in AI-Driven Urban Development // AI-Driven Strategies for Inclusive and Sustainable Urbanization. Boca Raton : CRC Press, 2025. P. 54–81.

## References

Amodu, A., & Ologbosere, T. (2021). Critical overview of information management, DIKAR model and technology in the 21st century. *Open Access*, *1*(1), 35–39.

Andress, J. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Elsevier.

Arrieta, A.B. et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58,* 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Baert, P., & Rubio, F.D. (2011). *The Politics of Knowledge*. Routledge.

Balasubramanian, P. et al. (2025). A cognitive platform for collecting cyber threat intelligence and real-time detection using cloud computing. *Decision Analytics Journal*, 14, 100545. https://doi.org/10.1016/j.dajour.2025.100545

Battista, D., & Mangone, E. (2025). Technological culture and politics: artificial intelligence as the new frontier of political communication. *Societies, 15*(4), 75. https://doi.org/10.3390/soc15040075

Beck, J. (2000). *Risk Society: Towards Modernity*. Moscow: Progress-Tradition. (In Russian).

Cinelli, M. et al. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, *118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

Damodaran, A. (2010). *Strategic Risk Management: Principles and Methods*. Moscow: Williams. (In Russian).

Davenport, T.H. (1997). *Information Ecology*. Oxford University Press.

Davies, C., Covello, T.C., & Allen, F.W. (1987). *Risk Communication*. The Conservation Foundation.

Duberry, J. (2022). *Artificial intelligence and democracy: risks and promises of AI-mediated citizen–government relations.* Edward Elgar Publishing. https://doi.org/10.4337/9781788977319

Earley, S. (2023). What executives need to know about knowledge management, large language models and generative AI. *Applied Marketing Analytics*, *9*(3), 215–229. https://doi.org/10.69554/YQBV7690.

Gabriel, I. (2020). Artificial Intelligence, Values, and Alignment. *Minds and Machines*, *30*(3), 411–437. https://doi.org/10.1007/s11023-020-09539-2

Gaman-Golutvina, O.V. (2024). The Threshold of Global Conflict or Contra Spem Spero? *Comparative Politics*, (3), 4–18. https://doi.org/10.46272/2221-3279-2024-3-15-8 EDN: FMXZIV

Hall, S., & Winlow, S. (2003). Rehabilitating Leviathan: Reflections on the State, Economic Regulation and Violence Reduction. *Theoretical Criminology*, *7*(2), 139–162. https://doi.org/10.1177/1362480603007002415

Höchtl, J., Parycek, P.R., & Schöllhammer, R. (2016). Big data in the policy cycle: Policy decision making in the digital era. *Journal of Organizational Computing and Electronic Commerce,* 26(1–2), 147–169. https://doi.org/10.1080/10919392.2015.1125187

Jarrahi, M.H. et al. (2023). Artificial intelligence and knowledge management: A partnership between human and AI. *Business Horizons*, *66*(1), 87–99. https://doi.org/10.1016/j.bushor.2022.03.002

Kahneman, D., Slovic, P., & Tversky, A. (2005). *Decision Making under Uncertainty: Rules and Biases.* Kharkov: Humanitarian Center. (In Russian).

Lewis, P. et al. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. *Advances in Neural Information Processing Systems*, *33,* 9459–9474.

Maltseva, D.A., Safonova, O.D., & Tuzova, P.R. (2023). Strategic Political Planning: Information Risk Management. In *Problems of National Security in Russia: Lessons from History and Challenges from the Present* (pp. 281–284). Krasnodar: Prospects of Education. (In Russian). EDN: TBMYOQ

McDermott, P. (2008). *Who Needs to Know? The State of Public Access to Federal Government Information*. Bernan Press.

McKnight, W. (2013). *Information Management: Strategies for Gaining a Competitive Advantage with Data*. Newnes.

Park, J.S. et al. (2023). Generative agents: Interactive simulacra of human behavior. *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, 1–22. https://doi.org/10.1145/3586183.3606763

Prigogine, I. (1991). The Philosophy of Softness. *Voprosy filosofii*, (6), 16–57. (In Russian). EDN: PCHHNF

Ratti, C., & Claudel, M. (2015). Futurecra: Tomorrow by Design. Techne. *Journal of Technology for Architecture and Environment*, (10), 28–33.

Taherdoost, H., & Madanchian, M. (2023). Artificial intelligence and knowledge management: Impacts, benefits, and implementation. *Computers*, *12*(4), 72. https://doi.org/10.3390/computers12040072

Taleb, N. (2022). *Painting with Our Own Skin. The Open Asymmetry of Everyday Life*. Moscow: Kolibri. (In Russian).

Yanitsky, O.N. (2011). Turbulent Times as a Risk Problem in Society. *Social Sciences and Modernity*, (6), 155–164. (In Russian). EDN: OJDVHZ

Zhang, A.K. et al. (2025). Cybench: A framework for evaluating cybersecurity capabilities and risks of language models. *International Conference on Learning Representations*, *2025,* 25094–25243.

Zhao, W.X. et al. (2026). A survey of large language models. *Frontiers of Computer Science*, *20*(12), 2012627. Retrieved from https://arxiv.org/abs/2303.18223

Zolkafli, A., & Salleh, D. (2025). Community Engagement in AI-Driven Urban Development. *In AI-Driven Strategies for Inclusive and Sustainable Urbanization* (pp. 54–81). CRC Press.

**Сведения об авторах:**

*Мальцева Дарья Александровна* — кандидат политических наук, доцент кафедры теории и философии политики, Санкт-Петербургский государственный университет, доцент кафедры сравнительной политологии, Российский университет дружбы народов (e-mail: buenafiesta@mail.ru) (ORCID: 0000-0002-0213-6919, SPIN-код: 5762-6370, AuthorID: 795594, Scopus ID: 56610201800, Web of Science ResearcherID K-5875-2015).

*Алейников Андрей Викторович* — доктор философских наук, доцент, профессор кафедры конфликтологии, Санкт-Петербургский государственный университет (e-mail: a.alejnikov@spbu.ru) (ORCID: 0000-0003-2942-5021, SPIN-код: 4954-7128, AuthorID: 257000, Scopus ID: 56690673600, Web of Science ResearcherID F-5286-2013).

*Стребкова Карина Евгеньевна* — магистр психологии, преподаватель кафедры общей психологии, Санкт-Петербургский государственный университет (e-mail: streb.karina@gmail.com) (ORCID: 0009-0001-7017-1310, SPIN-код: 2335-5955, AuthorID: 1098292, Scopus ID: 60236725600, WOS ID: AHD-1100-2022).

**About the authors:**

*Daria A. Maltseva* — PhD in Political Science, Associate Professor of the Department of Theory and Philosophy of Politics, Saint-Petersburg State University, Associate Professor of the Department of Comparative Politics, RUDN University (e-mail: buenafiesta@mail.ru) (ORCID: 0000-0002-0213-6919, SPIN-code: 5762-6370, AuthorID: 795594, Scopus ID: 56610201800, Web of Science ResearcherID K-5875-2015).

*Andrei V. Aleinikov* — Doctor of Philosophy, Associate Professor, Professor of the Department of Conflictology, Saint Petersburg State University (e-mail: a.alejnikov@spbu.ru) (ORCID: 0000-0003-2942-5021, SPIN-code: 4954-7128, AuthorID: 257000, Scopus ID: 56690673600, Web of Science ResearcherID F-5286-2013).

*Karina E. Strebkova* — Master in Psychology, Lecturer at the Department of General Psychology, Saint Petersburg State University (e-mail: streb.karina@gmail.com) (ORCID: 0009-0001-7017-1310, SPIN-code: 2335-5955, AuthorID: 1098292, Scopus ID: 60236725600, WOS ID: AHD-1100-2022).