www.volsu.ru

ПОЛИТИЧЕСКОЕ ПРОЕКТИРОВАНИЕ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

DOI: https://doi.org/10.15688/jvolsu4.2026.4.18

UDC 32.019.5
LBC 66.06

Submitted: 26.08.2025
Accepted: 11.10.2025

SOCIAL ARCHITECTURE OF RUSSIA'S FUTURE: KEY CHALLENGES AND RISKS IN THE CONTEXT OF CURRENT DIGITAL TRANSFORMATIONS (BASED ON EXPERT RESEARCH MATERIALS)

Sergey V. Volodenkov

Lomonosov Moscow State University, Moscow, Russian Federation;
Sevastopol State University, Sevastopol, Russian Federation

Abstract. *Introduction.* This article provides a comprehensive analysis of the challenges and risks posed by digital technologies to the formation of the social architecture of Russia's future. Within the author's conceptual framework, social architecture is understood as a dynamic process of purposeful design of institutional, normative, and communicative conditions. Grounded in specific value priorities, these conditions channel spontaneous social interactions towards the formation of a stable, equitable, and adaptive social system. The relevance of the study is determined by the systemic nature of digital transformation, which does not merely modify but fundamentally redefines traditional social institutions, values, and trust models. The aim of the work is to identify and systematize key technological risks and to assess the vulnerability of core social institutions within this context. *Materials and methods.* The research methodology is based on a qualitative content analysis of 22 structured interviews with leading Russian and international experts in political science, sociology, philosophy, and public administration. The sample was formed using purposive sampling. Data processing followed the principles of grounded theory, employing a three-level coding system (open, axial, and selective). *Analysis.* The analysis of empirical data revealed and detailed a spectrum of key clusters of technological risks: information and cognitive manipulation; ubiquitous control and surveillance; decentralized systems; virtual environments; infrastructure technologies; and technologies of direct human impact. It was established that the greatest threat originates from information management technologies implemented through platform ecosystems. An assessment of the vulnerability of specific social institutions was also conducted, identifying the education system, political institutions, and the sphere of labor as the most vulnerable. *Results.* The study yielded the following key findings: 1) a ranking of digital technologies according to their destabilizing potential, with the greatest threat stemming from the synergistic effect of their combination; 2) identification of systemic vulnerabilities within key institutions, which face a crisis of legitimacy, functional erosion, and rising inequality; 3) substantiation of the necessity for a comprehensive, interdisciplinary response, encompassing anticipatory legal regulation, the development of digital literacy, the formulation of ethical norms, and the cultivation of strategic vision among social architects. It is concluded that without coordinated action, Russia faces the prospect of significant socio-political crises. *Funding.* The study was carried out as part of the state assignment of Sevastopol State University. Project: "Design of the social architecture of Russia's future: images and scripts," registration number 1025031000058-9-5.6.1.

Key words: social architecture, digital technologies, artificial intelligence, socio-political challenges, institutional vulnerability.

Citation. Volodenkov S.V. Social Architecture of Russia's Future: Key Challenges and Risks in the Context of Current Digital Transformations (Based on Expert Research Materials). *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 4. Istoriya. Regionovedenie. Mezhdunarodnye otnosheniya* [Science Journal of Volgograd State University. History. Area Studies. International Relations], 2026, vol. 31, no. 4, pp. 212-223. (in Russian). DOI: https://doi.org/10.15688/jvolsu4.2026.4.18

© Володенков С.В., 2026

УДК 32.019.5
ББК 66.06

Дата поступления статьи: 26.08.2025
Дата принятия статьи: 11.10.2025

СОЦИАЛЬНАЯ АРХИТЕКТУРА БУДУЩЕГО РОССИИ: КЛЮЧЕВЫЕ ВЫЗОВЫ И РИСКИ В УСЛОВИЯХ АКТУАЛЬНЫХ ЦИФРОВЫХ ТРАНСФОРМАЦИЙ (ПО МАТЕРИАЛАМ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ)

Сергей Владимирович Володенков

Московский государственный университет им. М.В. Ломоносова,
г. Москва, Российская Федерация;
Севастопольский государственный университет,
г. Севастополь, Российская Федерация

Аннотация. *Введение.* Статья посвящена комплексному анализу вызовов и рисков, которые несут цифровые технологии для формирования социальной архитектуры будущего России. В рамках авторского подхода социальная архитектура понимается как динамический процесс целенаправленного проектирования институциональных, нормативных и коммуникативных условий, которые, будучи основанными на определенных ценностных приоритетах, направляют спонтанные социальные взаимодействия в русло формирования устойчивой, справедливой и адаптивной социальной системы. Актуальность исследования обусловлена системным характером цифровой трансформации, которая не просто модифицирует, а фундаментально переопределяет традиционные социальные институты, ценности и модели доверия. Цель работы – идентифицировать и систематизировать ключевые технологические риски и оценить уязвимость основных социальных институтов в этом контексте. *Методы и материалы.* Методология исследования основана на качественном контент-анализе 22 структурированных интервью с ведущими российскими и зарубежными экспертами в области политологии, социологии, философии и государственного управления. Выборка формировалась целевым методом. Обработка данных проводилась в соответствии с принципами обоснованной теории с использованием трехуровневой системы кодирования (открытого, аксиального и селективного). *Анализ.* В ходе анализа эмпирических данных был выявлен и детально охарактеризован спектр из ключевых кластеров технологических рисков: манипуляция информацией и сознанием, повсеместный контроль и слежка, децентрализованные системы, виртуальные среды, инфраструктурные технологии и технологии прямого воздействия на человека. Установлено, что наибольшую угрозу несут технологии управления информацией, реализуемые через платформенные экосистемы. Также проведена оценка уязвимости конкретных социальных институтов, в результате которой наиболее уязвимыми были признаны система образования, политические институты и сфера труда. *Результаты.* По итогам исследования получены следующие результаты: 1) ранжирован спектр цифровых технологий по степени их дестабилизирующего потенциала, при этом наибольшая угроза исходит от синергетического эффекта их сочетания; 2) выявлена системная уязвимость ключевых институтов, которым грозят кризис легитимности, эрозия функций и рост неравенства; 3) обоснована необходимость комплексного междисциплинарного ответа, включающего опережающее правовое регулирование, развитие цифровой грамотности, выработку этических норм и формирование стратегического видения у социальных архитекторов. Сделан вывод о том, что без скоординированных действий России грозит реализация серьезных общественно-политических кризисов. *Финансирование.* Исследование выполнено в рамках государственного задания Севастопольского государственного университета. Проект: «Проектирование социальной архитектуры будущего России: образы и сценарии», регистрационный номер 1025031000058-9-5.6.1.

Ключевые слова: социальная архитектура, цифровые технологии, искусственный интеллект, общественно-политические вызовы, институциональная уязвимость.

Цитирование. Володенков С. В. Социальная архитектура будущего России: ключевые вызовы и риски в условиях актуальных цифровых трансформаций (по материалам экспертного исследования) // Вестник Волгоградского государственного университета. Серия 4, История. Регионоведение. Международные отношения. – 2026. – Т. 31, № 4. – С. 212–223. – DOI: https://doi.org/10.15688/jvolsu4.2026.4.18

Введение. Современная эпоха характеризуется беспрецедентным ускорением технологических, социальных и ценностных трансформаций, что актуализирует проблему целенаправленного конструирования желаемого будущего. Классические подходы к социальному прогнозированию, базирующиеся на линейных экстраполяциях, демонстрируют свою ограниченность перед лицом нарастающей сложности, нелинейности и турбулентности глобального мира [19]. Как справедливо отмечал У. Бек, мы живем в «обществе риска», где производство богатства систематически сопровождается производством рисков [2]. Данная концепция находит свое новое, усиленное звучание в условиях Четвертой промышленной революции, стирающей традиционные границы между физической, цифровой и биологической сферами [16]. В этой связи возникает острая необходимость в новых теоретико-методологических подходах, способных не только диагностировать возникающие вызовы, но и предлагать стратегии проактивного формирования социального порядка.

В ответ на эти вызовы в научный дискурс активно внедряется интегративная парадигма «социальной архитектуры будущего» [4; 8], под которой в рамках данного исследования нами понимается системный, ценностно-ориентированный и адаптивный процесс целенаправленного проектирования институциональных, нормативных и коммуникативных условий для эмерджентного возникновения просоциальных практик и устойчивых структур, обеспечивающих гармоничное развитие общества в условиях неопределенности.

Ключевым преимуществом данного подхода является его проактивный и системный характер, позволяющий не просто реагировать на вызовы, но и формировать желаемые свойства социальной среды, минимизируя риски за счет предвосхищающего проектирования «правил игры», что позволяет гибко реагировать на непредсказуемость технологических изменений, снижая риски утопического проектирования и усиливая способность социальной системы к самоорганизации и устойчивому развитию в условиях турбулентности.

Данный подход не предполагает жесткого социального инжиниринга и, в отличие от утопического социального инжиниринга XX в., представляет собой процесс целенаправленного формирования условий для эмерджентного возникновения просоциальных практик и устойчивых структур. Это перекликается с идеями П. Бурдье о социальном пространстве как структурированном ансамбле полей, где происходит непрерывная борьба за различные виды капитала и право на символическое конструирование реальности [5]. В рамках этого подхода «социальный архитектор» выступает не в роли всезнающего «инженера», предписывающего жесткие схемы, а в роли рефлексирующего субъекта, формирующего «правила игры» – институциональные рамки, стимулы и среды, – которые направляют спонтанное социальное взаимодействие в желаемое русло. Интегративная парадигма социальной архитектуры будущего обеспечивает более адекватный ответ на современные вызовы по сравнению с линейными подходами, поскольку она: 1) учитывает нелинейность и турбулентность социальных процессов; 2) ориентирована на ценности и цели общества; 3) предусматривает адаптивное и проактивное управление; 4) учитывает синергетические эффекты цифровых технологий.

Ключевым фактором, детерминирующим и одновременно усложняющим процессы социального архитектурирования, выступают глобальные цифровые трансформации. Цифровые технологии, от искусственного интеллекта (ИИ) и больших данных до распределенных реестров и нейроинтерфейсов, не являются нейтральными инструментами; они онтологически выступают носителями определенных ценностей, скрытых идеологий и встроенных предвзятостей, что формирует принципиально новые угрозы для социального суверенитета и человеческой автономии [21]. Они активно трансформируют традиционные социальные онтологии, переопределяя такие фундаментальные категории, как приватность, доверие, идентичность и социальная справедливость. Алгоритмические системы, платформенная экономика и тотальная датафикация становятся новыми метаинститутами, которые не просто дополняют, но активно вытесняют и подменяют собой традиционные институты социализации, политического участия и экономического обмена.

Таким образом, формируется своего рода «цифровая антиномия»: с одной стороны, технологии открывают беспрецедентные возможности для повышения эффективности управления, развития государства и общества, а также расширения их коммуникативных практик; с другой – они генерируют системные риски, угрожающие самим основам социально-политического устройства. В этом контексте возникает насущная потребность в строгой научной идентификации и ранжировании этих рисков, что и составляет основную цель данного исследования.

В связи с этим целью настоящего исследования является выявление и комплексный анализ ключевых вызовов и рисков, генерируемых актуальными цифровыми трансформациями, для процесса формирования социальной архитектуры будущего России. Основной исследовательский вопрос заключается в следующем: *какие конкретные цифровые технологии обладают наибольшим дестабилизирующим потенциалом для ключевых элементов социальной архитектуры (институтов, ценностей, доверия) и порождают наиболее значимые общественно-политические риски?* Ответ на этот вопрос позволит перейти от констатации угроз к выработке конкретных мер упреждающего управления и построения стратегической устойчивости социальной системы.

Методы и материалы. Для получения эмпирических данных был применен метод качественного контент-анализа 22 структурированных экспертных интервью с ведущими российскими экспертами в области политологии, социологии, философии и государственного управления. Выборка формировалась целевым методом с охватом экспертов, специализирующихся на проблематике цифровизации и социальных изменений, и включала профессоров и доцентов ведущих вузов России (МГУ им. М.В. Ломоносова, НИУ ВШЭ, РАНХиГС при Президенте РФ, Финансовый университет при Правительстве РФ, Дальневосточный федеральный университет, Южный федеральный университет, СПбГУ, РУДН, Тихоокеанский государственный университет и др.), Республики Беларусь (Белорусский государственный экономический университет, Республиканский институт высшей школы), Сербии (Центр стратегических альтернатив, Центр Евразийских исследований Института международной политики и экономики), Китая (Центр изучения Азии Цзилиньского университета), США (University of Texas Rio Grande Valley), главных научных сотрудников академических институтов РАН (Институт системного анализа Федерального исследовательского центра «Информатика и управление» РАН). Все респонденты имеют ученые степени докторов или кандидатов наук, публикации в журналах Q1 / Q2 и опыт участия в разработке государственных программ и стратегий в сфере цифровой трансформации и социальной политики.

Интервью проводились по структурированному гайду, включавшему следующие тематические блоки: 1) оценка влияния различных цифровых технологий на социальные институты; 2) идентификация наиболее рискогенных технологий для социальной архитектуры; 3) оценка уязвимости конкретных социальных институтов России.

Интервью строилось вокруг центрального вопроса о дестабилизирующем потенциале цифровых технологий в социально-политической сфере, а также включало тематические блоки, касающиеся: а) оценки рисков конкретных технологических кластеров; б) уязвимости социальных институтов; в) возможных мер регулирования. Такой подход позволил реконструировать систему аргументации экспертного сообщества относительно деструктивного потенциала цифровых технологий.

Методология анализа данных была основана на принципах обоснованной теории [18] и предусматривала трехуровневую систему кодирования полученных в ходе исследования эмпирических материалов:

1. *Микроуровень (открытое кодирование)*: идентификация базовых семантических единиц и ключевых понятий. На этапе открытого кодирования были выявлены такие часто встречающиеся семантические единицы, как «фильтрующий пузырь», «алгоритмическая дискриминация», «эрозия доверия», «симулякр», «цифровая стратификация», «алгоритмическая колонизация повседневности», «эрозия эпистемического доверия», «биоразрыв».

2. *Мезоуровень (аксиальное кодирование):* кластеризация выявленных единиц по

концептуальным парадигмам (таким как «технологии манипуляции информацией и сознанием», «технологии всепроникающего контроля»). В процессе аксиального кодирования эти единицы были сгруппированы в шесть концептуальных кластеров рисков (например, единицы «таргетированная реклама», «дипфейки», «бот-сети» объединились в кластер «манипуляция информацией и сознанием»), которые и легли в основу представленного ниже анализа. В результате процедуры открытого и аксиального кодирования транскриптов интервью были сформированы шесть ключевых концептуальных кластеров технологических рисков, которые и структурируют последующий анализ: 1) манипуляция информацией и сознанием; 2) всепроникающий контроль и слежка; 3) децентрализованные и распределенные технологии; 4) технологии создания виртуальных сред (VR / AR, метавселенные); 5) инфраструктурные и вычислительные технологии следующего поколения; 6) технологии прямого воздействия на человека. Эти кластеры отражают консенсус экспертного сообщества относительно основных векторов цифровых угроз;

3. *Макроуровень (селективное кодирование)*: построение концептуальных взаимосвязей между категориями и идентификация ключевых консенсусных точек экспертов.

Анализ. Анализ эмпирических данных, полученных в ходе экспертных интервью, позволил выявить спектр технологических рисков, сгруппированных в несколько взаимосвязанных кластеров, каждый из которых представляет собой вызов для различных элементов социальной архитектуры, что соответствует цели исследования.

Выявленные в ходе кодирования интервью шесть кластеров технологических рисков были проанализированы через призму их воздействия на ключевые элементы социальной архитектуры, определенные выше: институциональные рамки, ценностные основания и модели доверия. Это позволяет перейти от общей диагностики рисков к оценке их влияния на конкретные социальные конструкции.

Центральное место в системе угроз занимают *технологии манипуляции информацией и сознанием*, включающие генеративный ИИ, дипфейки, социальных ботов и алгоритмы Big Data. Единогласно признанные экспертами как наиболее значимый источник риска, эти технологии реализуют на практике концепцию «гиперреальности» Ж. Бодрийяра, где симулякры активно замещают собой объективную реальность [3]. Их деструктивный потенциал многогранен: от целенаправленного манипулирования общественным мнением и эрозии доверия к ключевым социальным институтам до фундаментального подрыва основ рациональной публичной дискуссии и самого понятия истины [12].

Ключевым механизмом воздействия здесь выступает феномен «алгоритмической власти» [13], которая через инструменты микротаргетирования и персонализированного управления вниманием ведет к атомизации общества и его радикальной поляризации. Алгоритмы платформ, оптимизированные под максимизацию вовлеченности, создают замкнутые «фильтрующие пузыри» [14], где пользователи оказываются изолированы в информационных экосистемах, усиливающих их существующие убеждения и предубеждения. Это не только создает прямую угрозу таким базовым ценностям, как социальная справедливость и солидарность, но и подрывает саму возможность формирования общего символического пространства, необходимого для функционирования любого общества, формирует своего рода алгоритмическую колонизацию повседневности.

Особую опасность представляет синергетический эффект от сочетания этих технологий. Генеративный ИИ способен производить убедительный персонифицированный контент в промышленных масштабах, социальные боты обеспечивают его вирусное распространение, а системы анализа больших данных позволяют с беспрецедентной точностью идентифицировать уязвимые группы и индивидуальные психографические профили для последующего манипулятивного воздействия [22]. Возникающая система тотального охвата общества синтетическим контентом ведет к глубокой эрозии эпистемического доверия – способности общества различать истинное и ложное и разделять общую реальность [3; 12]. Это создает принципиально новые вызовы для социального суверенитета и человеческой автономии, требуя переосмыс-

ления традиционных моделей медиавоздействия и выработки новых механизмов защиты публичной сферы. Как подчеркнул один из респондентов, «платформенные экосистемы становятся ключевым оператором по перераспределению символической власти в цифровую эпоху».

Не менее значимую угрозу социальной архитектуре будущего воплощают *технологии всепроникающего контроля и слежения*, включающие биометрическую идентификацию, системы массового наблюдения, интернет вещей (IoT) и инфраструктуру «умных городов». Данные технологии материализуют и трансформируют метафору фукианского «паноптикона» [7], где индивид внутренне усваивает возможность постоянного наблюдения, в цифровой «сентоптикон» [11], характеризующийся тотальной видимостью индивида для невидимых алгоритмических систем при их собственной непрозрачности.

Ключевые риски этого кластера носят системный характер: они включают не только кардинальное снижение уровня приватности и создание системы предиктивного контроля, основанного на анализе больших данных и алгоритмическом прогнозировании поведения, но и формирование мощного потенциала для политической и социальной дискриминации. Последняя реализуется через механизмы скоринга и ранжирования граждан, что ведет к возникновению новой формы социального неравенства – «цифровой стратификации», где возможности индивида определяются его алгоритмическим профилем [22].

Важнейшим аспектом становится то, что эти технологии не просто наблюдают, но и активно конструируют социальную реальность через управление поведением на основе предсказаний и автоматизированного принятия решений. Это приводит к эрозии автономии личности и добровольному самоограничению свободы действий из-за осознания постоянной видимости – феномен, известный как «хантингтоновская самоцензура» в цифровой среде. В совокупности это подрывает саму основу доверительных отношений в триаде «государство – общество – человек», трансформируя социальный договор в систему тотального подчинения алгоритмическим метрикам и нечеловеческим регуляторам.

Особый вызов монополии государства на регулирование финансовых и информационных потоков несут *децентрализованные и распределенные технологии* (блокчейн, DLT – Distributed Ledger Technology). Их фундаментальная угроза заключается не только в технической децентрализации, но и в концептуальной дезинтермедиации – устранении традиционных посредников (банков, нотариусов, государственных реестров), которые исторически выступали проводниками государственной политики и гарантами институционального доверия.

Это создает благоприятные условия для интенсификации криминальной и антигосударственной деятельности: от масштабирования теневой экономики через криптовалютные платежи до организации децентрализованных автономных образований (DAO), действующих в правовых серых зонах. Технологии смарт-контрактов и анонимные криптовалюты обеспечивают не только обход санкций и отмывание средств, но и создают инфраструктуру для новых форм координации противоправной деятельности, устойчивых к традиционным механизмам государственного вмешательства.

Ключевой риск заключается в том, что дестабилизация традиционных финансовых и социальных институтов приводит к эрозии монополии государства на легитимное насилие и обеспечение безопасности. В контексте децентрализованных технологий эксперты отмечали парадокс: «Технологии, провозглашаемые инструментами прозрачности, на практике могут способствовать фрагментации публичного пространства». Это созвучно с выводами Ш. Зубофф [22] о смещении доверия от институциональных гарантий к алгоритмической достоверности, что косвенным образом подрывает легитимность государства как верховного гаранта порядка и социального контракта. На практике применение такого рода технологий может способствовать фрагментации публичного пространства и созданию альтернативных систем власти, неподконтрольных традиционным демократическим институтам.

В свою очередь, технологии создания виртуальных сред (VR/AR, метавселенные) представляют угрозу иного, экзистенциально-

го порядка: их деструктивный потенциал заключается не просто в дополнении, но в прогрессирующем замещении реальных социальных связей и практик виртуальными суррогатами. Это порождает комплекс взаимосвязанных рисков, начиная с глубокой манипуляции индивидуальным и коллективным восприятием реальности через создание иммерсивных, но контролируемых сред, где граница между действительным и смоделированным постепенно размывается [3].

Такое замещение ведет к формированию деструктивных нормативных моделей и кризису идентичности, что находит теоретическое обоснование в концепции «бегства от свободы» Э. Фромма [6]: индивиды, сталкиваясь с атомизацией и неуверенностью в реальном мире, могут добровольно уходить в регулируемые цифровые пространства, жертвуя автономией ради чувства принадлежности и определенности.

В долгосрочной перспективе это угрожает устойчивости реальных социальных институтов, поскольку подрывает саму основу социального воспроизводства – непосредственное человеческое взаимодействие, общие переживания и коллективные ритуалы [5]. Возникает парадокс: технологии, предлагающие беспрецедентные возможности для подключения и коммуникации, могут фактически затруднять формирование подлинных общих ценностей и коллективной идентичности, основанных на разделяемом опыте физического мира и совместном преодолении реальных вызовов. Это создает риск возникновения «цифрового раскола» нового типа – не только в доступе к технологиям, но и в способности сохранять аутентичные социальные связи в условиях тотальной виртуализации [20].

Роль катализатора и системного усилителя рисков всех предыдущих групп выполняют *инфраструктурные и вычислительные технологии* следующего поколения (квантовые вычисления, сети 5G / 6G). Квантовые компьютеры создают фундаментальную угрозу взлома существующих криптографических протоколов – алгоритм Шора позволяет взламывать асимметричные криптосистемы (RSA, ECC), составляющие основу современной цифровой безопасности. Это ставит под угрозу конфиденциальность данных, целостность финансовых систем и защищенность критической национальной информационной инфраструктуры.

Параллельно сети связи нового поколения (5G / 6G) обеспечивают сверхбыструю генерацию и распространение синтетического контента (включая дипфейки высокой точности), а также реализацию массового анализа данных для слежения и контроля в реальном времени. Низкая латентность и высокая пропускная способность этих сетей создают условия для беспрецедентной масштабируемости атак на общественное сознание и системы коллективного принятия решений.

Особую опасность представляет их синергетический эффект: квантовые вычисления могут нейтрализовать криптографическую защиту данных, в то время как сети 5G / 6G обеспечивают практически мгновенную передачу этих данных и координацию распределенных систем управления. Это многократно увеличивает не только масштаб и скорость реализации угроз из других кластеров, но и их разрушительный потенциал – от тотального компрометирования государственных тайн до дестабилизации всей финансовой системы и систем военного управления. Возникает качественно новая модель угроз, где технологическая конвергенция создает непреодолимые вызовы для традиционных систем безопасности и социально-политической стабильности.

Качественно новый уровень антропологических и социальных рисков связан с *технологиями прямого воздействия на человека* (нейротехнологии, биотехнологии, генная инженерия), открывающими возможность фундаментального вмешательства в сознание и биологию человека в рамках парадигмы «H+» (трансгуманизм). Данный кластер порождает беспрецедентные этические дилеммы, связанные с переопределением самой человеческой природы и границ телесной автономии.

Нейротехнологии (интерфейсы «мозг-компьютер», глубокая стимуляция мозга) ставят под вопрос традиционное понимание свободы воли и психической целостности личности, создавая возможности для целенаправленной модификации когнитивных процессов и эмоциональных состояний без осознанного

согласия индивида. Биотехнологии и CRISPR-Cas9 системы редактирования генома, в свою очередь, открывают путь к формированию «биологического неравенства» – стратификации общества на основе генетических характеристик и искусственно расширенных биологических возможностей.

Это ведет к риску возникновения новой формы социальной сегрегации – «биоразрыва», где привилегированный доступ к технологиям создает непреодолимый разрыв между «улучшенными» и «естественными» людьми не только в экономическом, но и физиологическом измерении. Такая трансформация бросает вызов самим основам социальной справедливости и правам человека, требуя пересмотра существующих правовых парадигм и выработки новых механизмов защиты человеческой идентичности в условиях технологий, способных изменить онтологический статус человека.

Проведенный анализ позволил также выявить ключевую консенсусную позицию среди экспертов: *приоритетная угроза исходит от технологий управления информацией; центральная роль в этом процессе принадлежит платформенным экосистемам и Big Data; фундаментальными являются угрозы приватности и автономии личности; а социальная поляризация выступает системным следствием распространения алгоритмического управления.*

Второй блок анализа был сфокусирован на оценке уязвимости конкретных социальных институтов России. Наиболее уязвимым был признан институт образования, которому грозит девальвация роли педагога, утрата монополии на знание и усиление образовательного неравенства. Оценивая уязвимость данного института, эксперты указывали на риск «подмены глубинного обучения симуляцией вследствие неконтролируемой интеграции генеративного ИИ». Один их респондентов прямо констатировал: «Мы наблюдаем начало трансформации “цифрового разрыва” в устойчивое “когнитивное неравенство”, что создает прямые вызовы национальной безопасности». В связи с этим возникает существенный риск снижения качества человеческого капитала и ослабления роли образования как ключевого института социализации, что уже отмечают в своих исследованиях современные ученые [1; 9; 20].

Высокую уязвимость демонстрируют и политические институты, и система управления, сталкивающиеся с кризисом легитимности, технологической неадекватностью посреднических функций, рисками манипуляции волеизъявлением [22] и общей дискредитацией. Суммарный эффект этих вызовов формирует реальную угрозу системного политического кризиса, трансформации моделей политического участия и усиления отрыва власти от реальных социальных запросов.

В свою очередь, системообразующая для социальной стабильности сфера труда и социально-экономических отношений подвергается рискам массового вытеснения человеческого труда [10], радикальной трансформации и поляризации рынка труда, девальвации традиционных трудовых институтов и эрозии профессиональной идентичности [17], что угрожает ростом социального неравенства [15], массовой безработицей и кризисом смысла труда.

Критически уязвимым является и институт средств массовой коммуникации, учитывая его центральную роль в конструировании национального символического и ценностно-смыслового пространства. Риски включают утрату монополии государства и традиционных СМИ на производство и распространение информации, усиление манипулятивного потенциала, фрагментацию информационного поля и распространение дезинформации, что в конечном итоге подрывает доверие к информации как таковой и затрудняет формирование целостного общественного мнения.

Наконец, эксперты особо выделили риски эрозии традиционных ценностей и институтов (семья, религия), которые сталкиваются с конкуренцией со стороны новых ценностных систем и цифровой социализации, продвигающей нормы, зачастую противоречащие традиционным, что формирует вызовы кризиса национально-культурной идентичности и ослабления социальной сплоченности.

Результаты. Проведенное экспертное исследование позволило выявить системную и взаимосвязанную природу технологических рисков, угрожающих социальной архитектуре будущего России. Анализ эмпирических дан-

ных свидетельствует о том, что дестабилизирующий потенциал цифровых трансформаций проистекает не столько из отдельных технологий, сколько из их синергетического эффекта, который превращает их в инструменты беспрецедентного масштаба воздействия. Ранжирование рисков по степени дестабилизирующего потенциала, выполненное на основе экспертных оценок, показало, что наиболее значительную угрозу несут технологии манипуляции информацией и сознанием (генеративный ИИ, дипфейки, социальные боты), реализуемые через масштабные платформенные экосистемы. Их применение ведет к эрозии эпистемического доверия, то есть коллективной способности различать истинное и ложное и разделять общую реальность, подрыву рациональной публичной дискуссии и радикальной социальной поляризации посредством механизмов алгоритмического управления и создания «фильтрующих пузырей». В совокупности это ставит под вопрос саму возможность формирования общего символического пространства и консенсусной реальности – фундаментальных предпосылок для целенаправленного социального проектирования.

Центральным выводом работы является установление системной, но при этом дифференцированной уязвимости ключевых социальных институтов, которые оказываются неадекватны скорости и глубине технологических изменений. Анализ экспертных оценок выявил, что угрозы носят не абстрактный, а конкретный характер, по-разному воздействуя на различные элементы социальной архитектуры. При этом кризисные явления имеют кумулятивный характер, затрагивая самые основы социального договора. Так, система образования сталкивается с риском подмены глубинного обучения симуляцией, а не просто с его цифровизацией, что на фоне неконтролируемой интеграции генеративного ИИ ведет к девальвации роли педагога-наставника и трансформации «цифрового разрыва» в устойчивое «когнитивное неравенство», угрожая качеству человеческого капитала – ключевому «строительному материалу» будущего, а также национальной идентичности. Политические институты демонстрируют нарастающий кризис легитимности, обусловленный технологической неадекватностью их традиционных посреднических функций, рисками манипуляции волеизъявлением и растущим отрывом от реальных социальных интересов. Это создает предпосылки для системного кризиса самих основ общественного договора. Сфера труда и социально-экономических отношений, в свою очередь, оказывается под угрозой массового вытеснения человеческого труда алгоритмами, радикальной трансформации рынка труда и эрозии не только традиционных моделей социальной защиты, но и профессиональной идентичности, что чревато не только ростом социального неравенства, но и кризисом смысла труда как важнейшего социального института.

Обобщая, можно констатировать, что совокупность выявленных рисков формирует комплексный вызов и деформируют *ключевые элементы социальной архитектуры, определенные в данном исследовании как проектируемые институциональные и ценностные рамки.* Так, технологии всепроникающего контроля и слежки, материализующие модель «сентоптикона», подрывают основу доверия – фундамент любых социальных институтов. Манипуляция сознанием через платформенные экосистемы разрушает общее символическое пространство и консенсусную реальность, без чего невозможна координация ценностно-ориентированных действий. В свою очередь, прямое воздействие на человеческую природу (H+) ставит под вопрос сами антропологические основания социальной справедливости и институциональной устойчивости. Это обусловливает необходимость не реактивного, а проактивного и комплексного междисциплинарного ответа, каждая мера которого должна быть адресована конкретному вызову и направлена на укрепление конкретных элементов социальной архитектуры. Такой ответ должен включать развитие опережающего правового регулирования, формирование высокой цифровой и медиаграмотности населения, разработку четких этических норм для ИИ, укрепление реальных социальных институтов и локальных сообществ, а также формирование стратегического, ценностно-ориентированного видения у «социальных архитекторов».

Опережающее правовое регулирование призвано создавать устойчивые институциональные рамки, ограничивающие деструктив-

ный потенциал технологий и риски всепроникающего контроля («сентоптикон») и децентрализованных систем, угрожающих монополии государства на легитимное регулирование. Развитие цифровой и медиаграмотности населения необходимо для защиты и воспроизводства здоровых ценностных оснований общества, повышения его резистентности к манипуляциям, сохранения и развития ценностно-смыслового фундамента общества. Выработка этических норм для ИИ и укрепление локальных сообществ должны способствовать восстановлению и поддержанию социального доверия – базового «цемента» любой социальной архитектуры, подвергаемого в настоящее время эрозии со стороны алгоритмической дискриминации и виртуализации социальных связей. Наконец, формирование стратегического видения у управленцев необходимо для обеспечения самой возможности проактивного и системного проектирования желаемого будущего, позволяющего направлять технологическое развитие в русло укрепления, а не разрушения социальной целостности, а не реактивного латания возникающих проблем. Таким образом, успешное проектирование социальной архитектуры будущего России напрямую зависит от способности государства и общества перейти от диагностики актуальных угроз к активному формированию таких институциональных, правовых и ценностных рамок, которые обеспечат просоциальное применение технологий для построения гармоничной и устойчивой социальной системы.

БЛАГОДАРНОСТИ

Автор выражает благодарность за помощь в проведении исследования д-ру полит. наук, профессору А.Ю. Мамычеву и д-ру полит. наук, доценту С.Н. Федорченко.

ACKNOWLEDGMENTS

The author expresses gratitude for assistance in conducting the research to Doctor of Sciences (Politics), Professor A.Yu. Mamychev and Doctor of Sciences (Politics), Associate Professor S.N. Fedorchenko.

СПИСОК ЛИТЕРАТУРЫ

1. Арамисов Т. Р. Социальное государство в цифровую эпоху: цифровые возможности или цифровое неравенство // Цифровая социология. 2025. Т. 8, № 2. С. 27–44. DOI: https://doi.org/10.26425/2658-347X-2025-8-2-27-44

2. Бек У. Общество риска. На пути к другому модерну. М.: Прогресс-Традиция, 2000. 384 с.

3. Бодрийяр Ж. Символический обмен и смерть. М.: Добросвет, 2000. 387 с.

4. Борисенков А. А., Макаров А. В., Лайков М. А. Социальная архитектура как новое направление деятельности внутриполитического блока // Вопросы политологии. 2025. Т. 15, № 3 (115). С. 823–832. DOI: https://doi.org/10.35775/PSI.2025.115.3.006

5. Бурдье П. Социальное пространство: поля и практики. М.: Ин-т эксперимент. социологии; СПб.: Алетейя, 2005. 576 с.

6. Фромм Э. Бегство от свободы. М.: АСТ, 2018. 288 с.

7. Фуко М. Надзирать и наказывать. Рождение тюрьмы. М.: Ad Marginem, 1999. 480 с.

8. Харичев А. Д. Социальная архитектура: от запросов в настоящем к горизонтам будущего // Блокнот гражданского просвещения. 2025. № 12. С. 5–7.

9. Шпак А. А., Кирко В. И. Социальное неравенство в цифровую эпоху: концепция Йорга Шеффера // Социология искусственного интеллекта. 2024. Т. 5, № 4. С. 21–48.

10. Acemoglu D., Restrepo P. Artificial Intelligence, Automation and Work // NBER Working Paper. 2018. № 24196. 41 p. URL: Artificial Intelligence, Automation and Work. DOI: https://doi.org/10.3386/w24196

11. Bauman Z., Lyon D. Liquid Surveillance: A Conversation. Cambridge: Polity Press, 2013. 186 p.

12. Habermas J. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. Cambridge: MIT Press, 1991. 301 p.

13. Napoli P. M. Automated Media: An Institutional Theory Perspective on Algorithmic Media Production and Consumption // Communication Theory. 2014. Vol. 24, № 3. P. 340–360. DOI: https://doi.org/10.1111/comt.12039

14. Pariser E. The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011. 294 p.

15. Piketty T. Capital in the Twenty-First Century. Cambridge, MA: Belknap Press, 2014. 685 p.

16. Schwab K. The Fourth Industrial Revolution. Geneva: World Economic Forum, 2016. 192 p.
17. Sennett R. The Corrosion of Character: The Personal Consequences of Work in the New Capitalism. New York: W.W. Norton & Company, 2000. 176 p.
18. Strauss A., Corbin J. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Thousand Oaks: SAGE Publications, 2015. 456 p.
19. Toffler A. Future Shock. New York: Random House, 1970. 505 p.
20. van Dijk J. A. G. M. The Digital Divide. Cambridge: Polity Press, 2020. 208 p.
21. Winner L. Do Artifacts Have Politics? // Daedalus. 1980. Vol. 109, № 1. P. 121–136.
22. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 704 p.

REFERENCES

1. Aramisov T.R. Sotsialnoe gosudarstvo v tsifrovuyu epokhu: tsifrovye vozmozhnosti ili tsifrovoe neravenstvo [Welfare State in the Digital Age: Digital Opportunities or Digital Inequality]. *Tsifrovaja sotsiologiya* [Digital Sociology], 2025, vol. 8, no. 2, pp. 27-44. DOI: https://doi.org/10.26425/2658-347X-2025-8-2-27-44
2. Beck U. *Obshchestvo riska. Na puti k drugomu modernu* [Risk Society: Towards a New Modernity]. Moscow, Progress-Traditsiya Publ., 2000. 384 p.
3. Baudrillard J. *Simvolicheskiy obmen i smert* [Symbolic Exchange and Death]. Moscow, Dobrosvet Publ., 2000. 387 p.
4. Borisenkov A.A., Makarov A.V., Laykov M.A. Socialnaya arkhitektura kak novoe napravlenie deyatelnosti vnutripoliticheskogo bloka [Social Architecture as a New Direction of Activity Within the Domestic Policy Bloc]. *Voprosy politologii* [Political Science Issues], 2025, vol. 15, no. 3 (115), pp. 823-832. DOI: https://doi.org/10.35775/PSI.2025.115.3.006
5. Bourdieu P. *Sotsialnoe prostranstvo: polya i praktiki* [Social Space: Fields and Practices]. Moscow, In-t eksperiment. sotsiologii; Saint Petersburg, Aleteyya Publ., 2005. 576 p.
6. Fromm E. *Begstvo ot svobody* [Escape from Freedom]. Moscow, AST Publ., 2018. 288 p.
7. Fuko M. *Nadzirat i nakazyvat. Rozhdenie tyurmy* [Discipline and Punish: The Birth of the Prison]. Moscow, Ad Marginem Publ., 1999. 480 p.
8. Kharichev A.D. Sotsialnaya arhitektura: ot zaprosov v nastoyashhem k gorizontam budushhego [Social Architecture: From Demands in the Present to the Horizons of the Future]. *Bloknot grazhdanskogo prosveshcheniya* [Civic Education Notebook], 2025, no. 12, pp. 5-7.
9. Shpak A.A., Kirko V.I. Sotsialnoe neravenstvo v tsifrovuyu epokhu: kontseptsiya Yorga Sheffera [Social Inequality in the Digital Age: The Concept of Jörg Scheffer]. *Sotsiologiya iskusstvennogo intellekta* [Sociology of Artificial Intelligence], 2024, vol. 5, no. 4, pp. 21-48.
10. Acemoglu D., Restrepo P. Artificial Intelligence, Automation and Work. *NBER Working Paper*, 2018, no. 24196. 41 p. DOI: https://doi.org/10.3386/w24196
11. Bauman Z., Lyon D. *Liquid Surveillance: A Conversation*. Cambridge, Polity Press, 2013. 186 p.
12. Habermas J. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, MIT Press, 1991. 301 p.
13. Napoli P.M. Automated Media: An Institutional Theory Perspective on Algorithmic Media Production and Consumption. *Communication Theory*, 2014, vol. 24, no. 3, pp. 340-360. DOI: https://doi.org/10.1111/comt.12039
14. Pariser E. *The Filter Bubble: What the Internet Is Hiding from You*. New York, Penguin Press, 2011. 294 p.
15. Piketty T. *Capital in the Twenty-First Century*. Cambridge, MA, Belknap Press, 2014. 685 p.
16. Schwab K. *The Fourth Industrial Revolution*. Geneva, World Economic Forum, 2016. 192 p.
17. Sennett R. *The Corrosion of Character: The Personal Consequences of Work in the New Capitalism*. New York, W.W. Norton & Company, 2000. 176 p.
18. Strauss A., Corbin J. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, SAGE Publications, 2015. 456 p.
19. Toffler A. *Future Shock*. New York, Random House, 1970. 505 p.
20. van Dijk J.A.G.M. *The Digital Divide*. Cambridge, Polity Press, 2020. 208 p.
21. Winner L. Do Artifacts Have Politics? *Daedalus*, 1980, vol. 109, no. 1, pp. 121-136.
22. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, Public Affairs, 2019. 704 p.

Information About the Author

Sergey V. Volodenkov, Doctor of Sciences (Politics), Professor, Department of Public Policy, Lomonosov Moscow State University, Prosp. Lomonosovskiy, 27, Bld. 4, 119991 Moscow, Russian Federation; Leading Researcher, Research Laboratory "Socio-Political Analysis and Forecasting", Sevastopol State University, Universitetskaya St, 33, 299053 Sevastopol, Russian Federation, s.v.cyber@gmail.com, https://orcid.org/0000-0003-2928-6068

Информация об авторе

Сергей Владимирович Володенков, доктор политических наук, профессор кафедры государственной политики, Московский государственный университет им. М.В. Ломоносова, просп. Ломоносовский, 27, корпус 4, 119991 г. Москва, Российская Федерация; ведущий научный сотрудник, научно-исследовательская лаборатория «Социально-политический анализ и прогнозирование», Севастопольский государственный университет, ул. Университетская, 33, 299053 г. Севастополь, Российская Федерация, s.v.cyber@gmail.com, https://orcid.org/0000-0003-2928-6068