РЕГИОНАЛЬНАЯ И ОТРАСЛЕВАЯ ЭКОНОМИКА/REGIONAL AND SECTORAL ECONOMICS

DOI: https://doi.org/10.60797/IRJ.2025.159.51

ЦИФРОВАЯ ЗАВИСИМОСТЬ КАК ФАКТОР СИСТЕМНОЙ УЯЗВИМОСТИ РЕГИОНАЛЬНОЙ ИНФРАСТРУКТУРЫ

Научная статья

Калинина Е.В.[1, *]

[1] ORCID : 0009-0008-6071-1564;

[1] Российская академия народного хозяйства и государственной службы при Президенте РФ, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (souveraine[at]mail.ru)

Аннотация

Цифровая инфраструктура становится неотъемлемым элементом устойчивости и развития региональных экономических систем, но одновременно порождает новые формы зависимости, асимметрии и уязвимости. В условиях углубляющейся цифровизации ключевым вызовом для России выступает структурная зависимость от внешних технологических решений, которая формировалась в течение нескольких десятилетий и приняла институционализированную форму. Статья анализирует риски цифровой зависимости российских регионов на трёх уровнях: инфраструктурном, платформенном и институциональном. Особое внимание уделяется феномену технологического импорта, отсутствию механизмов цифрового резервирования, асимметрии в доступе к оборудованию, а также институциональной непризнанности киберугроз. На основе сопоставления международных кейсов и анализа российского опыта, показано, что цифровая зависимость формирует не только техническую уязвимость, но и снижает субъектность регионов в принятии управленческих решений. В статье поднимается вопрос о переходе от логики импортозамещения к архитектурной трансформации цифровых платформ и инфраструктур. Сделан вывод о необходимости интеграции институциональных механизмов цифровой устойчивости — в том числе через пересмотр моделей финансирования, нормативов аварийного реагирования и структуры цифрового суверенитета. Результаты исследования имеют значение для формирования политики цифровой безопасности и стратегического планирования в условиях внешнего давления и технологической нестабильности.

Ключевые слова: цифровая зависимость, инфраструктурная уязвимость, технологический импорт, киберриски, цифровой суверенитет, платформенная архитектура, региональная устойчивость.

DIGITAL DEPENDENCY AS A FACTOR IN THE SYSTEMIC VULNERABILITY OF REGIONAL INFRASTRUCTURE

Research article

Kalinina E.V.[1, *]

[1] ORCID : 0009-0008-6071-1564;

[1] Russian Presidential Academy of National Economy and Public Administration, Saint-Petersburg, Russian Federation

* Corresponding author (souveraine[at]mail.ru)

Abstract

Digital infrastructure is becoming an integral part of the sustainability and development of regional economic systems, but at the same time it is giving rise to new forms of dependence, asymmetry and vulnerability. In the context of deepening digitalisation, a key challenge for Russia is its structural dependence on external technological solutions, which has developed over several decades and taken on an institutionalised form. The article analyses the risks of digital dependence in Russian regions at three levels: infrastructural, platform and institutional. Particular attention is paid to the phenomenon of technology imports, the lack of digital backup mechanisms, asymmetry in access to equipment, and the institutional non-recognition of cyber threats. Based on a comparison of international cases and an analysis of Russian experience, it is shown that digital dependence not only creates technical vulnerability, but also reduces the subjectivity of regions in making management decisions. The paper raises the question of the transition from the logic of import substitution to the architectural transformation of digital platforms and infrastructures. It concludes that there is a necessity to integrate institutional mechanisms for digital sustainability, including through a review of financing models, emergency response standards, and the structure of digital sovereignty. The results of the research are important for shaping digital security policy and strategic planning in conditions of external pressure and technological instability.

Keywords: digital dependency, infrastructure vulnerability, technology imports, cyber risks, digital sovereignty, platform architecture, regional sustainability.

Введение

Цифровизация экономики и управления, ускоренная в последние два десятилетия, одновременно с созданием новых возможностей породила качественно новые формы уязвимости. Если ранее зависимость от внешних технологических решений носила преимущественно экономический или отраслевой характер (например, в энергетике, машиностроении или фармацевтике), то в цифровой сфере она затрагивает базовые контуры суверенитета: инфраструктуру принятия решений, каналы коммуникации, алгоритмы управления, доступ к данным. Это особенно

актуально в контексте российских регионов, где цифровая трансформация реализуется в условиях пространственной, институциональной и технологической асимметрии.

Цель настоящей статьи — проанализировать феномен цифровой зависимости как системный риск региональной устойчивости, с опорой на эмпирические данные и аналитические выводы, представленные в российских и международных исследованиях. В фокусе внимания находятся три взаимосвязанных аспекта: технологический импорт, износ и старение цифровой инфраструктуры, отсутствие архитектурной готовности к киберинцидентам. Показано, что российская модель цифрового развития длительное время основывалась на импортных решениях без механизмов резервирования, глубокой адаптации или стратегической локализации. Результатом стала высокая чувствительность региональных ИТ-систем к внешним шокам — санкциям, кибератакам, отказам оборудования — а также снижение институциональной автономии субъектов Российской Федерации в управлении цифровыми платформами.

Методы и принципы исследования

Методологической основой настоящего исследования является системный подход к анализу цифровой инфраструктуры как многокомпонентной иерархически организованной структуры, включающей технические, институциональные и управленческие элементы. В рамках исследования цифровая зависимость рассматривается не как частный технический дефицит, а как системный феномен, возникающий на пересечении трёх уровней: архитектурного, нормативного и управленческого. Исследование опирается на междисциплинарный подход, сочетающий элементы институциональной теории, экономики развития и анализа уязвимостей цифровых систем. Принцип сравнительного анализа применён при сопоставлении практик цифровой устойчивости в России и в ряде зарубежных государств, использованных в качестве референтных моделей. Наконец, в исследовании применяется принцип институционального соответствия: цифровые решения анализируются не только с точки зрения их функциональной эффективности, но и через призму способности быть встроенными в управленческие и правовые контуры региональной политики.

Основные результаты

Исторически складывающаяся цифровая зависимость в России проходила несколько этапов. В 1990–2010-е годы она воспринималась как инструмент модернизации, позволяющий быстро интегрировать лучшие международные практики в госуправление, здравоохранение, образование, транспорт и энергетику. Однако парадокс модернизации заключался в том, что сам процесс цифровизации сопровождался накоплением критической зависимости от иностранного ПО и оборудования. К 2010-м годам, как показывают отраслевые обзоры, более 90% программных решений, используемых в государственном секторе, были импортными. Это касалось не только офисных пакетов и операционных систем, но и всей инфраструктуры — от электронного документооборота до медицинских информационных систем и систем видеонаблюдения.

Санкционные ограничения после 2014 года обозначили проблему, но не решили её: несмотря на создание Реестра российского ПО и нормативные запреты, значительная часть критически важного функционала продолжала поддерживаться зарубежными платформами. На региональном уровне это вылилось в парадокс: цифровые системы номинально существовали, но были неавтономны, трудно масштабируемы и плохо интегрируемы с национальными инициативами. После 2022 года, на фоне ухода западных поставщиков с рынка, эта зависимость трансформировалась в прямую угрозу институциональной устойчивости: множество субъектов Федерации столкнулись с невозможностью поддерживать работу существующих ИС, дефицитом оборудования и отсутствием документации по ключевым компонентам. Параллельно с технологической зависимостью нарастала институциональная хрупкость. Проблема цифрового резервирования и аварийного восстановления практически не получила распространения в региональных администрациях [8].

Дополнительным аспектом становится пространственное цифровое неравенство. Комплексное исследование С. П. Земцова и коллег [3] показало, что увеличение охвата широкополосным интернетом коррелирует с ростом регионального ВРП на душу населения, а каждый процент отставания по использованию Интернета приводит к снижению ВРП. Эти данные подтверждают, что цифровая инфраструктура является не просто дополнением к экономике, но её структурной основой. При этом инфраструктура оказывается неравномерно распределённой, и чем выше уровень физического и институционального износа, тем выше риски.

Эти структурные ограничения особенно ярко проявляются в сфере резервирования и отказоустойчивости. Несмотря на существование формальных требований к надёжности телекоммуникационных сетей в ряде нормативных документов (в частности, в Приложении № 8 к Приказу Минсвязи России от 23.11.2006 № 151), в большинстве региональных и муниципальных цифровых платформ отсутствуют технические и организационные механизмы для обеспечения непрерывности функционирования в условиях кризисных ситуаций [5]. Это означает, что даже в случае незначительного сбоя — будь то локальная атака, физический износ оборудования или программная ошибка — существует вероятность полной остановки цифрового сервиса, будь то региональный реестр, система выдачи госуслуг или электронный документооборот. При этом случаи создания отказоустойчивых архитектур остаются единичными и не задают стандарт отрасли. Примером служит Центр обработки данных Министерства природных ресурсов и экологии РФ, в котором реализовано двухконтурное аппаратное резервирование, архитектура SAN-сетей и вычислительные кластеры с высокой доступностью [6]. Однако этот случай, по сути, исключение, отражающее федеральный уровень с высокой ресурсной обеспеченностью, тогда как абсолютное большинство региональных органов власти не располагают ни технической, ни финансовой базой для создания аналогичных решений.

Вместе с тем, на уровне отдельных регионов имеются успешные примеры цифровой зрелости и автономного развития ИТ-среды. Москва демонстрирует образцовый пример цифровой зрелости. В период COVID-19 развитая инфраструктура — в рамках программ «Электронная Москва» и «Информационный город» — позволила быстро

перевести услуги онлайн, обеспечив синхронное функционирование здравоохранения (ЕМИАС), образования (МЭШ), оказание госуслуг, платформы участия («Активный гражданин») и бизнес-взаимодействия (ICT.Moscow). Город занял первое место в рейтинге ООН по индексу электронных услуг. Это демонстрирует потенциал регионального лидерства в сфере цифровой устойчивости и возможность тиражирования подобных моделей в другие субъекты РФ.

Проблема усугубляется отсутствием институциональных механизмов оценки состояния цифровой инфраструктуры. Несмотря на усилия по разработке реестров ПО и оборудования, системная инвентаризация ИТ-ресурсов с учётом степени износа, срока эксплуатации и потребности в обновлении остаётся нерешённой. Регулярные аудиты в этой сфере практически не проводятся, а данные о состоянии серверного и сетевого оборудования, как правило, являются фрагментарными или вовсе отсутствуют в публичном пространстве. Это делает невозможным оценку рисков на основе объективной информации и лишает органы государственной власти инструментария принятия решений в условиях цифровой нестабильности.

Особый риск формируется в сегменте импортозависимости критических ИТ-компонентов. Несмотря на попытки локализации, большая часть аппаратных решений, включая серверные платформы, маршрутизаторы, СХД и элементы телеком-инфраструктуры, производится за рубежом. При этом существенная доля этих поставок уже в 2022–2023 годах оказалась под риском санкционного ограничения или полного прекращения. На практике это означает, что даже при наличии номинальной инфраструктуры — например, ЦОД — не гарантируется возможность замены комплектующих, получения обновлений или осуществления технической поддержки. Импортозамещение, провозглашённое как стратегическая цель, в условиях отсутствия полной производственной цепочки и зависимостей от микроэлектроники, остаётся фрагментарным. Отечественные платформы зачастую формально зарегистрированы как российские, но, по сути, представляют собой интерфейсные сборки на зарубежных модулях и библиотеках. Это порождает некоторую иллюзию независимости при фактической зависимости от скрытых компонентов — драйверов, прошивок, API-интерфейсов и иных элементов, критичных для функционирования ИТ-систем.

Таким образом, в совокупности выявленные аспекты — технологическая зависимость, отсутствие архитектурной устойчивости, износ оборудования и институциональная неготовность к кризисным ситуациям — формируют комплексную цифровую уязвимость. Она не ограничивается лишь техническими сбоями, но способна перерастать в управленческую и социальную нестабильность, особенно в условиях форсированной цифровизации и роста требований к качеству государственных цифровых услуг.

Для преодоления цифровой уязвимости и формирования устойчивой цифровой архитектуры в регионах необходимо внедрение многоуровневых технических и институциональных решений. На инфраструктурном уровне — реализация принципов георазпределённого резервирования (размещение зеркал критически важных сервисов в независимых ЦОДах), использование отказоустойчивых SAN-сетей и кластерных решений с автоматическим восстановлением. На платформенном уровне — создание открытых архитектур с модульной заменяемостью компонентов, минимизацией проприетарных зависимостей, а также сертифицированными механизмами безопасной интеграции. На институциональном уровне — формализация процедуры регулярной технической инвентаризации, введение нормативов цифровой отказоустойчивости (например, MTTR/MTBF), обязательный аудит ИТ-инфраструктуры и включение цифровых рисков в региональные паспорта безопасности. Вместо декларативных критериев зрелости предлагается переход к измеримым показателям: коэффициент доступности ИС, доля локализованного ПО, время восстановления при сбое и др.

Заключение

Анализ цифровой зависимости регионов России позволяет сделать ряд принципиальных выводов, имеющих значение как для оценки устойчивости цифровой инфраструктуры, так и для проектирования долгосрочной стратегии цифрового развития.

Во-первых, выявлена системная зависимость региональных ИТ-платформ от импортных аппаратных и программных решений, сформировавшаяся в результате длительного институционального бездействия в области цифрового суверенитета. Эта зависимость проявляется в невозможности полноценного функционирования информационных систем без доступа к зарубежным поставкам, сервису и компонентной базе.

Во-вторых, критически значимым фактором риска выступает износ оборудования и отсутствие инфраструктурных механизмов его обновления. При дефиците региональных бюджетов, отсутствии централизованной политики технической инвентаризации и отсутствии правил плановой замены, большинство региональных ИТ-ресурсов эксплуатируются за пределами допустимых сроков, что существенно снижает их надёжность.

В-третьих, подтверждена институциональная неготовность к кризисным ситуациям: механизмы цифрового резервирования и аварийного управления в большинстве субъектов отсутствуют, а существующие — не протестированы. Это означает, что подавляющее большинство региональных ИС находятся в режиме «нулевой избыточности», то есть не имеют способности к восстановлению при инциденте.

В-четвёртых, пространственная дифференциация цифровой инфраструктуры не только воспроизводит социально-экономическое неравенство между регионами, но и ограничивает потенциал устойчивого роста. Чем выше уровень технологического износа и институциональной зависимости, тем ниже цифровая зрелость и, соответственно, тем выше чувствительность региона к внешним и внутренним шокам.

Наконец, текущая модель цифрового развития требует не столько косметических мер по импортозамещению или нормативному регулированию, сколько архитектурной трансформации всей системы. Это предполагает:

- внедрение многоуровневых отказоустойчивых решений: от физического резервирования в ЦОДах до автоматического восстановления сервисов;
- переход к открытым архитектурам с модульной заменяемостью и сертифицированными интеграционными интерфейсами;

- институционализацию цифровой устойчивости через аудит, нормативы восстановления (MTTR), обязательную инвентаризацию и контроль жизненного цикла ИТ-компонентов;

- расширение системы мониторинга и оценки цифровых рисков в региональных стратегиях и паспортах безопасности.

- Только при реализации таких системных изменений возможно формирование надежной, управляемой и суверенной цифровой среды на региональном уровне, способной противостоять как технологическим, так и институциональным вызовам.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности / В.В. Бухарин // Вестник МГИМО. — 2016. — № 6 (51).

2. Борисов С.А. Оценка цифровой зрелости регионов в условиях глобальных вызовов / С.А. Борисов, Н.С. Соменкова // Экономическая безопасность. — 2025. — Т. 8. — № 6. — С. 1693–1712. — DOI: 10.18334/ecsec.8.6.123457. — EDN: WBJSYV.

3. Zemtsov S.P. Internet diffusion and interregional digital divide in Russia: trends, factors, and the influence of the pandemic / S.P. Zemtsov, K.V. Demidova, D.Yu. Kichaev // Baltic Region. — 2022. — Vol. 14. — № 4. — P. 57–78.

4. Селезнев П.С. Цифровые вызовы социально-политической консолидации и коллективной идентичности общества / П.С. Селезнев, В.Ш. Сургуладзе // Век глобализации. — 2021. — № 4.

5. Об утверждении Требований к системам синхронной цифровой передачи: Приказ от 23.11.2006 № 151 / Минсвязи РФ // КонсультантПлюс. — URL: https://www.consultant.ru/document/cons_doc_LAW_64797/ (дата обращения: 20.07.2025).

6. ЦОД Минприроды России // Минприроды РФ. — URL: https://rfi.mnr.gov.ru/projects/83/ (дата обращения: 20.07.2025).

7. Южаков В.Н. Цифровизация взаимодействия граждан и государства: оценка гражданами эффектов, рисков и перспектив / В.Н. Южаков, А.Н. Покида, Н. Зыбуновская [и др.] // Вопросы государственного и муниципального управления. — 2023. — № 2. — URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-vzaimodeystviya-grazhdan-i-gosudarstva-otsenka-grazhdanami-effektov-riskov-i-perspektiv (дата обращения: 20.08.2025).

8. Российский рынок резервного копирования 2025 // Anti-Malware.ru. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-BackUp-systems-2025 (дата обращения: 20.07.2025).

9. New Horizons for a Data-Driven Economy / Ed. by J.M. Cavanillas, E. Curry, W. Wahlster. — Springer, 2016. — DOI: 10.1007/978-3-319-21569-3.

10. Digital divide and regional development in Russia in the context of artificial intelligence // NEA Journal. — 2025. — № 67. — P. 225–233.

11. Estratégia brasileira para a transformação digital. — URL: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf (acessado: 20.08.2025).

12. OECD Reviews of Innovation Policy: Korea 2023. — Paris: OECD Publishing, 2023. — DOI: 10.1787/bdcf9685-en.

13. Makumbirofa S. Country-level assessment of Africa’s readiness for a digital single market / S. Makumbirofa, R. Banya. — Cape Town: Research ICT Africa, 2023. — 74 p.

14. 2023 OECD Digital Government Index: Results and key findings // OECD Public Governance Policy Papers. — Paris: OECD Publishing, 2024. — № 44 — DOI: 10.1787/1a89ed5e-en.

15. OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. — Paris: OECD Publishing, 2023. — DOI: 10.1787/c74f03de-en.

16. Government at a Glance 2025. — Paris: OECD Publishing, 2025. — DOI: 10.1787/0efd0bcd-en.

17. The 2020 ERP Report / Panorama Consulting Group. — Denver: Panorama Consulting, 2020. — 23 p. — URL: https://cdn2.hubspot.net/hubfs/4439340/Pan (accessed: 20.08.2025).

18. Partridge A. Digital inequalities in the post-pandemic recovery: the case of South Africa / A. Partridge. — Cape Town: Research ICT Africa, 2023. — 46 p.

19. Staab P. Technological sovereignty in Germany: techno-industrial policy as a form of economic statecraft? / P. Staab, M. Pirogan, D. Piétron // Global Political Economy. — 2025. — № 4 (1). — P. 51–70. — DOI: 10.1332/26352257Y2023D000000005.

20. Zenglein M.J. Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership / M.J. Zenglein, A.E. Holzmann // MERICS Papers on China. — 2019. — № 8.

Список литературы на английском языке / References in English

1. Buharin V.V. Komponenty cifrovogo suvereniteta Rossijskoj Federacii kak tehnicheskaja osnova informacionnoj bezopasnosti [Components of the digital sovereignty of the Russian Federation as a technical basis for information security] / V.V. Buharin // Vestnik MGIMO [MGIMO Bulletin]. — 2016. — № 6 (51). [in Russian]

2. Borisov S.A. Ocenka cifrovoj zrelosti regionov v uslovijah global'nyh vyzovov [Assessment of digital maturity of regions in the conditions of global challenges] / S.A. Borisov, N.S. Somenkova // Jekonomicheskaja bezopasnost' [Economic security]. — 2025. — Vol. 8. — № 6. — P. 1693–1712. — DOI: 10.18334/ecsec.8.6.123457. — EDN: WBJSYV. [in Russian]

3. Zemtsov S.P. Internet diffusion and interregional digital divide in Russia: trends, factors, and the influence of the pandemic / S.P. Zemtsov, K.V. Demidova, D.Yu. Kichaev // Baltic Region. — 2022. — Vol. 14. — № 4. — P. 57–78.

4. Seleznev P.S. Cifrovye vyzovy social'no-politicheskoj konsolidacii i kollektivnoj identichnosti obshhestva [Digital challenges of socio-political consolidation and collective identity of society] / P.S. Seleznev, V.Sh. Surguladze // Vek globalizacii [Age of globalization]. — 2021. — № 4. [in Russian]

5. Ob utverzhdenii Trebovanij k sistemam sinhronnoj cifrovoj peredachi: Prikaz ot 23.11.2006 № 151 [On the approval of Requirements for systems of synchronous digital transmission: Order from 23.11.2006 151] / Ministry of Communications of the Russian Federation // ConsultantPlus. — URL: https://www.consultant.ru/document/cons_doc_LAW_64797/ (accessed: 20.07.2025). [in Russian]

6. Data Centre of the Ministry of Nature and Environment of Russia // Ministry of Nature and Environment of the Russian Federation. — URL: https://rfi.mnr.gov.ru/projects/83/ (accessed: 20.07.2025). [in Russian]

7. Juzhakov V.N. Cifrovizacija vzaimodejstvija grazhdan i gosudarstva: ocenka grazhdanami jeffektov, riskov i perspektiv [Digitalization of interaction between citizens and the state: assessment by citizens of effects, risks and prospects] / V.N. Juzhakov, A.N. Pokida, N. Zybunovskaja [et al.] // Voprosy gosudarstvennogo i municipal'nogo upravlenija [State and municipal administration]. — 2023. — № 2. — URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-vzaimodeystviya-grazhdan-i-gosudarstva-otsenka-grazhdanami-effektov-riskov-i-perspektiv (accessed: 20.08.2025). [in Russian]

8. Rossijskij rynok rezervnogo kopirovanija 2025 [Russian backup market 2025] // Anti-Malware.ru. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-BackUp-systems-2025 (accessed: 20.07.2025). [in Russian]

9. New Horizons for a Data-Driven Economy / Ed. by J.M. Cavanillas, E. Curry, W. Wahlster. — Springer, 2016. — DOI: 10.1007/978-3-319-21569-3.

10. Digital divide and regional development in Russia in the context of artificial intelligence // NEA Journal. — 2025. — № 67. — P. 225–233.

11. Estratégia brasileira para a transformação digital [Brazilian strategy for digital transformation]. — URL: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf (accessed: 20.08.2025). [in Portuguese]

12. OECD Reviews of Innovation Policy: Korea 2023. — Paris: OECD Publishing, 2023. — DOI: 10.1787/bdcf9685-en.

13. Makumbirofa S. Country-level assessment of Africa’s readiness for a digital single market / S. Makumbirofa, R. Banya. — Cape Town: Research ICT Africa, 2023. — 74 p.

14. 2023 OECD Digital Government Index: Results and key findings // OECD Public Governance Policy Papers. — Paris: OECD Publishing, 2024. — № 44 — DOI: 10.1787/1a89ed5e-en.

15. OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. — Paris: OECD Publishing, 2023. — DOI: 10.1787/c74f03de-en.

16. Government at a Glance 2025. — Paris: OECD Publishing, 2025. — DOI: 10.1787/0efd0bcd-en.

17. The 2020 ERP Report / Panorama Consulting Group. — Denver: Panorama Consulting, 2020. — 23 p. — URL: https://cdn2.hubspot.net/hubfs/4439340/Pan (accessed: 20.08.2025).

18. Partridge A. Digital inequalities in the post-pandemic recovery: the case of South Africa / A. Partridge. — Cape Town: Research ICT Africa, 2023. — 46 p.

19. Staab P. Technological sovereignty in Germany: techno-industrial policy as a form of economic statecraft? / P. Staab, M. Pirogan, D. Piétron // Global Political Economy. — 2025. — № 4 (1). — P. 51–70. — DOI: 10.1332/26352257Y2023D000000005.

20. Zenglein M.J. Evolving Made in China 2025: China's industrial policy in the quest for global tech leadership / M.J. Zenglein, A.E. Holzmann // MERICS Papers on China. — 2019. — № 8.