



DOI: 10.22363/2313-1438-2025-27-3-560-578

EDN: NFGVYC

Научная статья / Research article

Цифровой суверенитет на Южном Кавказе: вызовы интеграции в международные цифровые коридоры

В.С. Давтян 

Российско-Армянский университет, Ереван, Республика Армения

Институт Китая и современной Азии РАН, Москва, Российская Федерация

✉ vahedavtyan@yandex.ru

Аннотация. Страны Южного Кавказа в настоящее время находятся в стадии становления цифрового суверенитета. Изучение политологического измерения феномена цифрового суверенитета позволило установить концептуальные рамки исследования, сводящиеся к определению уровня цифрового развития и суверенитета южнокавказских стран в условиях новых рисков и угроз региональной безопасности. Изучение институциональных основ развития цифровых инфраструктур в странах Южного Кавказа дало возможность оценить уровень их готовности к осуществлению цифровой трансформации. В этой связи особое внимание уделено вопросам законодательного регулирования цифровой отрасли. Выявлены стратегические подходы стран региона к перспективам цифрового развития и суверенитета, отраженные в официальных стратегических документах. Показано, что проистекающая на Южном Кавказе ожесточенная конкуренция между двумя ключевыми транспортно-логистическими стратегиями «Север — Юг» и «Восток — Запад» сказывается также на логике и географии проложения цифровых коридоров. В частности, многосторонняя интеграция в телекоммуникационные коридоры интернет-трафика рассматриваются нами в качестве ключевого вызова диверсификации путей обеспечения национальной цифровой безопасности и повышения цифрового суверенитета стран региона. В этой связи анализ логистической архитектуры цифровых коридоров на двух уровнях — региональном и макро-региональном — позволил определить основные проблемы и перспективы цифровой интеграции на Южном Кавказе. Методология работы включает межстрановой сравнительный анализ, а также методы количественной оценки уровня цифровизации (индекс сетевой готовности, проникновение мобильного и фиксированного интернета и пр.).

Ключевые слова: цифровизация, суверенитет, безопасность, Южный Кавказ, коридоры, коммуникации, диверсификация, «Цифровой шелковый путь», TASIM

Заявление о конфликте интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Давтян В.С. Цифровой суверенитет на Южном Кавказе: вызовы интеграции в международные цифровые коридоры // Вестник Российского университета дружбы народов. Серия: Политология. 2025. Т. 27. № 3. С. 560–578. <https://doi.org/10.22363/2313-1438-2025-27-3-560-578>

© Давтян В.С., 2025



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

Digital Sovereignty in the South Caucasus: Navigating Challenges Towards Integration within Global Digital Corridors

Vahe S. Davtyan 

Russian-Armenian University, Yerevan, Republic of Armenia

Institute of China and Modern Asia, Russian Academy of Sciences, Moscow, Russian Federation

✉ vahedavtyan@yandex.ru

Abstract. The article explores key challenges in the formation and development of digital sovereignty across the South Caucasus region. Adopting a political science perspective, it outlines the conceptual framework of the study, which focuses on assessing the level of digital advancement and sovereignty in the context of emerging regional security risks and threats. The analysis examines the institutional foundations underpinning digital infrastructure development in the region, offering an assessment of national readiness for digital transformation. Particular emphasis is placed on the legislative regulation of the digital sector, as well as on strategic approaches to digital development and sovereignty as reflected in national policy documents. The study demonstrates that the ongoing strategic competition between the “North–South” and “East–West” transport and logistics corridors in the South Caucasus also shapes the logic and geography of emerging digital routes. In this context, multilateral integration into international internet traffic corridors is identified as a critical challenge for diversifying access routes, enhancing national digital security, and strengthening digital sovereignty. The analysis of the logistical architecture of digital corridors — at both regional and macro-regional levels — enables the identification of the main barriers and prospects for digital integration in the South Caucasus. Methodologically, the study employs a cross-country comparative approach alongside quantitative measures of digitalization, including the Network Readiness Index, mobile and fixed internet penetration, and related indicators.

Keywords: digitalization, sovereignty, security, South Caucasus, corridors, communications, diversification, “Digital Silk Road”, TASIM

Conflicts of interest. The author declares no conflicts of interest.

For citation: Davtyan, V.S. (2025). Digital sovereignty in the South Caucasus: Navigating challenges towards integration within global digital corridors. *RUDN Journal of Political Science*, 27(3), 560–578. (In Russian). <https://doi.org/10.22363/2313-1438-2025-27-3-560-578>

Введение, или Политологическое измерение концепции «цифрового суверенитета»

В условиях стремительного развития цифровых технологий и возрастания их роли в глобальных политических и экономических процессах концепция цифрового суверенитета приобретает особую значимость. В свою очередь, анализ проблем цифрового суверенитета в его политологическом измерении сегодня представляется не только уместным, но и необходимым в связи с ростом его влияния на обеспечение национальной безопасности и государственно-го суверенитета.

Достижение цифрового суверенитета сопряжено с комплексом проблем и трудностей, среди которых следует выделить, например, монополизацию мировой цифровой среды транснациональными корпорациями; международное регулирование интернета, который в целом находится под контролем либо стран Запада, либо аффилированных с ними бизнес-субъектов; зависимость от зарубежных технологий, существенно понижающих возможности реализации государством суверенной политики, и пр. Разумеется, красной нитью сквозь рассматриваемое проблемное поле проходит распространение киберугроз и кибершпионажа, создающих серьезные риски как для цифровых, так и в целом для критических инфраструктур.

Одним из ключевых инструментов проведения политики цифрового суверенитета является формирование т.н. «цифровых коридоров», представляющих собой по сути транспортные инфраструктуры, используемые с целью обеспечения логистических маршрутов передачи данных между государствами. Чем диверсифицированнее маршруты передачи данных, тем безопаснее национальная цифровая экосистема государства. Следовательно, государство, нацеленное на повышение собственного суверенитета, как правило, стремится к созданию альтернативных маршрутов с использованием как подводных, так и наземных оптоволоконных линий.

Вместе с тем наличие как активных, так и замороженных вооруженных конфликтов, территориальных споров, блокада со стороны соседних государств и ряд других геополитических факторов, отражающих региональные реалии, напрямую сказываются на безопасности функционирования уже существующих цифровых коридоров, равно как и на проектировании новых, при прочих условиях, экономически более целесообразных маршрутов передачи данных. Все указанные проблемы в той или иной мере свойственны Южному Кавказу — региону, продолжающему демонстрировать высокую турбулентность, обусловленную набирающей обороты конкуренцией как между региональными, так и внерегиональными акторами. При этом выгодное географическое расположение региона, его нахождение на перекрестке двух транспортно-логистических мегастратегий — «Север — Юг» и «Восток — Запад» — определяют высокий интерес к нему со стороны ключевых геополитических акторов.

Таким образом, вырисовывается цель настоящего исследования: **определить уровень цифрового суверенитета стран Южного Кавказа и влияния геополитической обстановки в регионе на формирование международных «цифровых коридоров».** Достижение поставленной цели предполагает решение нескольких задач:

- провести сравнительный анализ реализуемой в странах Южного Кавказа политики цифровизации;
- оценить уровень цифровой безопасности и цифровой готовности стран Южного Кавказа;
- рассмотреть существующие в регионе «цифровые коридоры»;
- определить уровень влияния региональных геополитических процессов на безопасность «цифровых коридоров».

Под цифровым суверенитетом ряд авторов понимает особенности регулирования и контроля сетевого оборудования, программного обеспечения, больших данных и в целом информационного пространства [Couture, Tourin 2019].

Традиционно предлагается два подхода к определению понятия «цифровой суверенитет»: узкий, в котором цифровой суверенитет ограничивается лишь информационным суверенитетом, сводящимся к праву государства контролировать распространяемую на его территории информацию, и более широкий — с акцентом на сокращение зависимости от поставок зарубежного цифрового оборудования и реализацию протекционистской поддержки отечественным ИТ-компаниям. Также к важным компонентам цифрового суверенитета относится создание национальной системы управления интернетом с обеспечением должного уровня взаимодействия между государством, гражданским обществом и ИТ-компаниями [Кочетков, Маслов 2022: 33].

Ряд исследователей исходят из необходимости рассмотрения проблем цифрового суверенитета сквозь призму продвижения национальных интересов и обеспечения безопасного функционирования национальных цифровых инфраструктур [Никонов и др. 2021: 208]. Рассматривается ряд научных и экспертных подходов, согласно которым цифровой суверенитет характеризуется наличием собственных цифровых сервисов во всех ключевых сферах жизнедеятельности государства, включая национальные цифровые платформы (социальные сети, мессенджеры, облачные хранилища и пр.). Также под цифровым суверенитетом нередко понимается наличие национальных операционных систем, собственных разработок в сфере искусственного интеллекта и пр. [Никонов и др. 2021: 210].

Заслуживают внимания попытки изучения цифрового суверенитета с позиций критической геополитики, в рамках которой политический актор рассматривается как результат дискурса о суверенитете, и его конституирование в современном мире возможно преимущественно через цифровое пространство [Романова 2023: 64].

Особое внимание в научной литературе уделяется вопросам информационного вмешательства во внутривнутриполитические процессы, учитывая возрастающее влияние цифрового пространства на формирование общественного мнения. При этом алармистские настроения свойственны не только российским, но также европейским авторам, отмечающим снижение влияния европейского капитала на рынке информационных технологий, новые угрозы информационной безопасности (напр., кибертерроризм, использование цифровых и информационных инструментов в военно-политической деятельности и пр.) [Зиновьева, Булва 2021: 45].

Выделяется ряд системообразующих компонентов цифрового суверенитета, таких как национальные цифровые платформы, программное и аппаратное обеспечение, квалифицированные специалисты, научно-образовательная база по подготовке кадров, ресурсы цифровой архитектуры, безопасность и сохранность информации и пр. [Ромашкина, Киричук 2023: 851].

Следует констатировать, что проблемы цифрового суверенитета в странах Южного Кавказа недостаточно изучены. Исключение составляют лишь исследования, посвященные вопросам формирования международных цифровых коридоров и реализации цифровых инициатив, так или иначе затрагивающих страны региона (например, «Цифровой Шелковый путь» (ЦШП) или «Цифровая инициатива ЕАЭС»). Вместе с тем нередко встречаются научные публикации, посвященные проблемам цифровизации экономики и системы государственного управления в странах Южного Кавказа [Арутюнян 2020; Huseynova, Mazanova 2020; Омарова, Шарипова 2022]. Однако целевые исследования, касающиеся региональных проблем обеспечения цифрового суверенитета, практически отсутствуют, чем и обусловлена актуальность настоящей статьи.

Цифровой суверенитет на Южном Кавказе: межстрановой анализ

Геополитические трансформации, обострившиеся в последние годы, особенно после 44-дневной войны в Нагорном Карабахе (Арцах) осенью 2020 г. оказали прямое воздействие на уровень цифрового развития и цифровой вовлеченности в регионе, и без того с начала 1990-х гг. пребывающем в состоянии глубокой дезинтеграции. В результате сложных стратегических перестановок, повлекших за собой глубинные изменения в архитектуре региональной безопасности, получили еще более отчетливые очертания процессы международной транспортно-логистической конкуренции, нашедшей отражение также в сфере цифровых коммуникаций на Южном Кавказе [Давтян, Маргарян 2022]. Таким образом, напрашивается предварительный вывод о том, что уровень цифровой безопасности и цифрового суверенитета стран региона напрямую зависит от внешнеполитической конъюнктуры, сказывающейся как на развитии национальных цифровых инфраструктур, так и на формировании интеграционных трендов.

Для структурного осмысления проблем цифрового суверенитета стран Южного Кавказа следует начать, пожалуй, с рассмотрения институциональных особенностей стран с определением как государственных органов, ответственных за политику цифровизации, так и национальных цифровых приоритетов.

В странах Южного Кавказа наблюдаются в целом схожие цели развития цифрового суверенитета, для достижения которых созданы и внедрены в систему государственного управления разные по статусу институты. Так, в Армении главными органами, ответственными за цифровизацию, являются Канцелярия премьер-министра и Министерство высокотехнологичной промышленности, располагающие в своих структурах, соответственно, двумя профильными учреждениями — Агентством по внедрению инфраструктур электронного управления и Агентством информационных систем Армении. В Азербайджане за цифровизацию ответственно Государственное агентство по общественным услугам и социальным инновациям при Президенте республики также с соответствующими профильными учреждениями — Центром развития электронного правительства, Центром предоставления государственных услуг и Центром

инноваций. Что касается Грузии, то здесь главными государственными органами, отвечающими за цифровое развитие, выступают Министерство юстиции, Министерство экономики и устойчивого развития, а также и две профильные организации — Агентство цифрового управления и Агентство по развитию государственной службы (табл. 1).

Таблица 1

**Органы государственной власти и профильные учреждения
в сфере цифрового управления в странах Южного Кавказа**

Страна	Ответственный институт	Профильные учреждения
<i>Армения</i>	Канцелярия Премьер-министра Республики Армения (Совет по цифровизации) Министерство высокотехнологичной промышленности	ЗАО «Агентство по внедрению инфраструктур электронного управления» Фонд «Агентство информационных систем Армении» Совет управления информационными системами
<i>Азербайджан</i>	Министерство цифрового развития и транспорта Государственное агентство по общественным услугам и социальным инновациям при Президенте Азербайджана (SAPSSI)	Центр развития электронного правительства при SAPSSI Центры предоставления государственных услуг при SAPSSI Центр инноваций при SAPSSI
<i>Грузия</i>	Министерство юстиции Министерство экономики и устойчивого развития	Агентство цифрового управления Агентство по развитию государственной службы

Источник: составлено В.С. Давтяном

Table 1

**Government Authorities and Specialized Institutions in the Field of Digital Governance
in the South Caucasus Countries**

Country	Responsible Authority	Specialized Institutions
<i>Armenia</i>	Office of the Prime Minister of the Republic of Armenia (Digitalization Council) Ministry of High-Tech Industry	CJSC «e-Governance Infrastructure Implementation Agency» «Information Systems Agency of Armenia» Foundation Information Systems Management Council
<i>Azerbaijan</i>	Ministry of Digital Development and Transport State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan (SAPSSI)	E-Government Development Center under SAPSSI Public Service Centers under SAPSSI Innovation Center under SAPSSI
<i>Georgia</i>	Ministry of Justice Ministry of Economy and Sustainable Development	Digital Governance Agency Civil Service Development Agency

Source: compiled by V.S. Davtyan

Межстрановой анализ институциональных особенностей политики цифровизации на Южном Кавказе показывает, что, невзирая на официальное постулирование приоритетности цифрового развития, тем не менее, это не всегда отражается в институциональной структуре правительства. Указанные

в таблице ответственные институты — министерства и государственные агентства — по сути, не являются узкопрофильными с фокусацией лишь на цифровую повестку (отчасти исключение может составить лишь Азербайджан с выделенной цифровой компонентой в названии министерства). Для сравнения можно привести в качестве примера ряд стран, располагающих министерствами, специализирующимися исключительно или преимущественно на вопросах цифровизации: Россия (Министерство цифрового развития, связи и массовых коммуникаций), Казахстан (Министерство цифрового развития, инноваций и аэрокосмической промышленности), Кыргызстан (Министерство цифрового развития), Узбекистан (Министерство по развитию информационных технологий и коммуникаций), Польша (Министерство цифровизации), ОАЭ (Министерство искусственного интеллекта и цифровых технологий) и пр.

Для оценки приоритетности обеспечения цифрового суверенитета в странах Южного Кавказа следует обратиться также к двум важным индикаторам — отражению проблем цифровой повестки в стратегиях национальной безопасности (либо иных стратегических документах) и стратегическим инициативам в сфере цифровой трансформации. При этом в основополагающих стратегических документах государств региона наблюдаются также точки соприкосновения для развития сотрудничества между ними [Кардумян 2013].

Все три страны региона в своих стратегиях/концепциях национальной безопасности затрагивают вопросы цифрового развития и суверенитета сквозь призму вызовов информационных войн и кибербезопасности, а также отчасти цифровизации государственных услуг. В частности, в «Стратегии национальной безопасности Республики Армения» от 2020 г. отмечается, что угрозами информационной безопасности Армении являются кибератаки на информационные инфраструктуры, расположенные на территории страны, со стороны иностранных государств, международных террористических организаций, преступных группировок и отдельных лиц. Новыми и уникальными вызовами являются кибератаки, направляемые частными организациями, а также финансируемые иностранными государствами, которые нацелены на жизненно важную информационную инфраструктуру Армении и средства ее управления. «Мы будем развивать нормативно-правовую базу взаимоотношений между государством и поставщиками жизненно важной информационной инфраструктуры и цифровых услуг, в результате чего будут созданы Национальный центр кибербезопасности и группы реагирования на компьютерные инциденты»¹, — отмечается в документе, что в целом отражает ключевые риски цифрового суверенитета Армении (в том числе геополитического характера).

Обращаясь к концепции национальной безопасности Азербайджана, следует отметить особый акцент, который ставится в документе на инструментах обеспечения информационной безопасности в сфере разведки и контрразведки.

¹ *Стратегия национальной безопасности Республики Армения* (принята 10 июля 2020 г.). URL: <https://www.mfa.am/filemanager/security%20and%20defense/AA-Razmavarutyun-Final.pdf> (дата обращения: 20.03.2025).

«Одним из основных вопросов в данном секторе национальной безопасности является согласование способностей и повышение эффективности разведки и контрразведки, а также координация охраны секретной информации», — отмечается в документе². Приоритетной задачей для Азербайджана остается создание цифровой инфраструктуры, способной обслуживать электронное правительство, а также формирование цифровых идентификационных систем и развитие технологии блокчейн, равно как и информационное обеспечение государственных решений и борьбы с организованной преступностью [Гасанов 2014].

В Стратегии национальной безопасности Грузии проблемы цифрового суверенитета преимущественно сводятся к рискам кибербезопасности. В качестве важного аргумента приводятся угрозы кибербезопасности Грузии, возникшие еще в период 5-дневной войны 2008 г. «Поскольку зависимость критической инфраструктуры Грузии от информационных технологий растет, растут и проблемы, связанные с защитой грузинского киберпространства. Во время российско-грузинской войны 2008 г. Российская Федерация провела масштабные кибератаки параллельно с наземными, воздушными и морскими атаками. Эти атаки показали, что защита киберпространства так же важна для национальной безопасности, как и наземная, морская и противовоздушная оборона», — отмечается в Стратегии. Также в Стратегии особое внимание уделяется безопасности секретной информации и защите государственных информационных систем³.

В целом можно констатировать, что в действующих стратегиях/концепциях национальной безопасности стран Южного Кавказа не прослеживается комплексное видение проблем цифрового суверенитета. Рассмотренные нами документы так или иначе сводят вопросы цифровизации преимущественно к киберугрозам и информационным войнам, чего, на наш взгляд, недостаточно для оценки современных вызовов цифрового развития и суверенитета. Впрочем, это может быть обусловлено тем обстоятельством, что приведенные выше документы были составлены и утверждены в период, предшествовавший кульминации «цифрового поворота» в мире. Отметим также, что в последние годы, параллельно с динамичным развитием цифровой сферы и формированием новых цифровых угроз, в странах Южного Кавказа не менее динамично развивается также «цифровое законодательство», что является свидетельством ответственного подхода и системного видения развития цифрового суверенитета как вызова национальной безопасности. Последнее сегодня представляет особую значимость в связи с необходимостью правового регулирования обработки данных в интернете [Винник 2014]. Страны региона не первый год осуществляют активную законодательную деятельность, направленную на формирование необходимых правовых условий для цифрового развития как в сфере оказания

² Концепция национальной безопасности Азербайджанской Республики (Утверждена Распоряжением Президента Азербайджанской Республики от 23 мая 2007 г. №2198). URL: <https://ir.rudn.ru/books/b1/p5/01.pdf> (дата обращения: 20.03.2025).

³ *National Security Concept of Georgia*. URL: <https://mfa.gov.ge/en/national-security-concept> (accessed: 20.03.2025).

цифровых услуг и перехода к системе цифрового правительства, так и повышения устойчивости и безопасности киберсистем. Все это сопровождается наблюдаемыми в странах региона стратегическими инициативами, призванными обеспечить цифровую трансформацию.

Рассмотрим уровень цифровизации стран региона с применением также некоторых количественных инструментов, среди которых особый интерес представляет индекс сетевой готовности NRI (Networked Readiness Index).

NRI представляет собой комплексный показатель, определяющий уровень развития информационно-коммуникационных технологий (ИКТ) и сетевой экономики страны. Разработанный в 2002 г. в рамках Всемирного экономического форума, позже, в 2019 г., Индекс был переработан и передан в ведение «Института Портуланса» (США), который и публикует ежегодный рейтинг сетевой готовности стран в сотрудничестве со Всемирным альянсом информационных технологий и услуг. В основу расчета Индекса заложен метод корреляции между развитием ИКТ и экономическим ростом. Измерение осуществляется по 62-м контрольным показателям, которые объединены в четыре группы:

- 1) технологии;
- 2) люди;
- 3) управление;
- 4) влияние.

Первое место в рейтинге соответствует высшему значению, и наоборот. В 2024 г. в рейтинге 133 стран по индексу сетевой готовности страны Южного Кавказа расположились следующим образом (табл. 2).

Таблица 2

Рейтинг стран Южного Кавказа по индексу сетевой готовности в 2024 г.

Страны	Место в рейтинге	Индекс
Армения	66	49,54
Азербайджан	75	46,8
Грузия	68	49,30

Источник: Network Readiness Index 2024: Building a Digital Tomorrow // Portulans Institute. URL: <https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf> (accessed: 21.03.2025).

Table 2

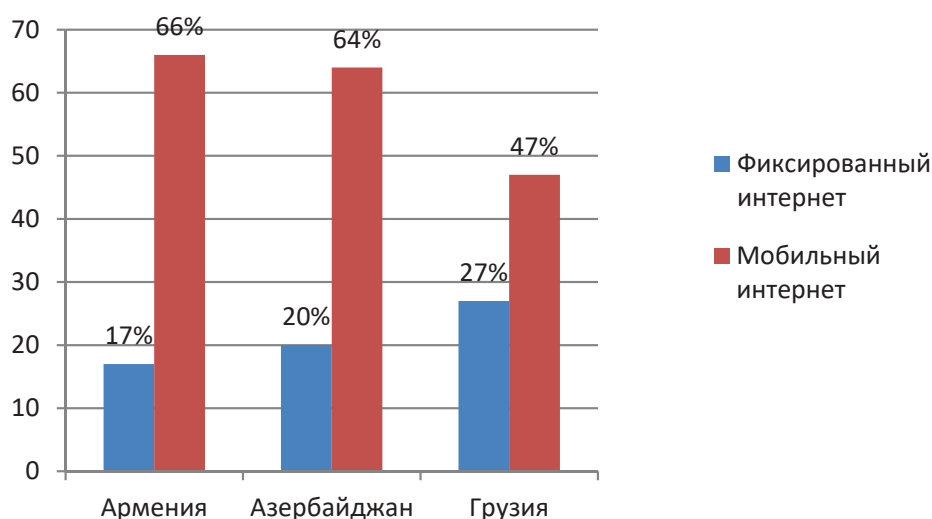
Network Readiness Index Rankings of South Caucasus Countries, 2024

Country	Rank	Index Score
Armenia	66	49.54
Azerbaijan	75	46.80
Georgia	68	49.30

Source: Network Readiness Index 2024: Building a Digital Tomorrow. Portulans Institute. Retrieved March 21, 2025, from <https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf>

Означают ли приведенные данные, что среди стран Южного Кавказа Армения лидирует по уровню цифровизации? Согласно NRI, ответ очевиден. Однако по целому ряду отдельно взятых показателей картина не представляется столь радужной. В частности, если обратиться к такому значимому сегодня показателю, как внедрение беспроводного интернета нового поколения 5G, среди стран региона лидером выступает Грузия (в 2023 г. в двух районах Тбилиси и на некоторых зимних курортах была запущена сеть 5G)⁴. В Армении⁵ и Азербайджане⁶ постепенное внедрение 5G планируется в 2025 г. Более того, важным фактором продолжает оставаться также геополитическая напряженность в регионе, которая в большей степени сказывается на транспортно-коммуникационных возможностях Армении.

Другим важным количественным показателем является также соотношение проникновения мобильного и фиксированного интернета (рис.)⁷.



Соотношение проникновения мобильного и фиксированного интернета

Источник: Преодоление цифрового разрыва в Центральной Азии и на Южном Кавказе // GSMA 2023. URL: <https://>

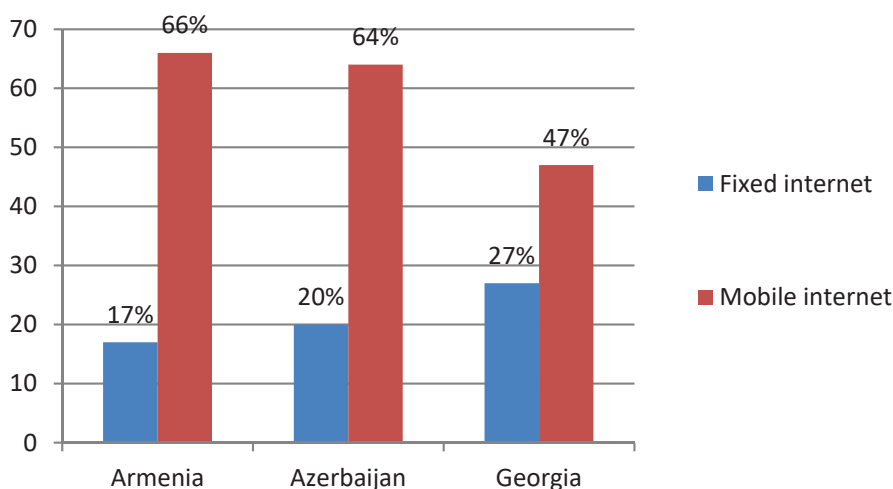
⁴ 5G в Грузии — уже реальность: быстрый Интернет появился в Тбилиси и на горных курортах // Спутник Грузия. 21 декабря 2023 г. URL: <https://sputnik-georgia.ru/20231221/5g-v-gruzii--uzhe-realnost-bystryy-internet-poyavilsya-v-tbilisi-i-na-gornyykh-kurortakh-285107627.html> (accessed: 21.03.2025).

⁵ В Армении начнут внедрять сеть 5G по всей территории страны и в аэропортах // АРКА. 18 декабря 2024 г. URL: https://arkatelecom.am/news/internet/v_armenii_nachnut_vnedryat_set_5g_po_vsey_territorii_strany_i_v_aeroportakh/ (дата обращения: 21.03.2025).

⁶ Стало известно время запуска 5G в Азербайджане // Report.az. 8 октября 2019 г. URL: <https://report.az/ru/ikt/oglasheni-investicii-v-razvertivanie-i-vnedrenie-5g-v-sng/?ysclid=m8k79l193j820082095> (дата обращения: 21.03.2025).

⁷ Преодоление цифрового разрыва в Центральной Азии и на Южном Кавказе // GSMA 2023. URL: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/06/Closing-the-Digital-Divide-in-Central-Asia-and-the-South-Caucasus-2023-RUSSIAN.pdf> (дата обращения: 21.03.2025).

www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/06/Closing-the-Digital-Divide-in-Central-Asia-and-the-South-Caucasus-2023-RUSSIAN.pdf (дата обращения: 21.03.2025).



Ratio of mobile and fixed internet penetration

Source: Closing the Digital Divide in Central Asia and the South Caucasus, GSMA 2023. Retrieved March 21, 2025, from <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/06/Closing-the-Digital-Divide-in-Central-Asia-and-the-South-Caucasus-2023-RUSSIAN.pdf>

Ожидается, что широкое внедрение сети 5G на Южном Кавказе приведет к существенному увеличению роли мобильных устройств в цифровой трансформации благодаря меньшей задержке и большей пропускной способности. В целом наличие более качественного и доступного интернета неизбежно скажется на уровне политической вовлеченности граждан, а также приведет к сокращению динамики урбанизации, являющейся одной из важных социально-экономических проблем во всех странах Южного Кавказа.

Диверсификация цифровых коридоров как вызов безопасности

Геополитическая напряженность на Южном Кавказе оказывает существенное влияние на транспортно-логистическую и коммуникационную системы региона. Наблюдаемые здесь неразрешенные или замороженные военно-политические конфликты не только ограничивают возможности проложения экономически наиболее целесообразных международных коммуникационных коридоров, но также сказываются на безопасности и стабильности национальных коммуникационных инфраструктур. Продолжающаяся конкуренция, а по сути — «транспортная война» между бенефициарами двух ключевых для Большой Евразии мегапроектов: «Север — Юг» и «Восток — Запад», во многом предопределяет ход и логику региональных цифровых коммуникаций [Федоровская 2022].

Осуществление атак по проходящим как по суше, так и по морскому дну интернет-кабелям сегодня стало одним из ключевых инструментов ведения войны. Достаточно обратиться в этой связи к повреждению подводных интернет-коммуникаций в Красном море (февраль 2024 г.)⁸, обрыву телекоммуникационных кабелей на дне Балтийского моря (ноябрь 2024 г.)⁹ и прочим аналогичным инцидентам, свидетельствующим о проведении целенаправленных диверсий против критических инфраструктур в ходе разного рода геополитических конфликтов.

Аналогичные риски могут угрожать также цифровой безопасности стран Южного Кавказа. Для наиболее комплексной оценки этих рисков прежде всего следует обратиться к основным внешним маршрутам интернет-трафика в регионе.

Южный Кавказ соединен с международными интернет-хабами посредством нескольких цифровых коридоров, пролегающих в европейском, российском, ближневосточном и центральноазиатском направлениях. География этих маршрутов выглядит следующим образом.

Начнем с общеевразийских маршрутов, обеспечивающих связь в регионе:

- Caucasus Cable System: Болгария-Грузия;
- MedNautilus: Европа-Турция;
- AAE-1: Турция-Азия;
- SEA-ME-WE: Иран-Персидский залив-Азия;
- FLAG, FALCON: Иран-Индия;
- TransCaspian Fiber Optic: Азербайджан-Казахстан.

Все перечисленные маршруты напрямую или косвенно влияют на цифровую безопасность стран Южного Кавказа, следовательно, выстраивание эффективной внешней политики по указанным направлениям представляется важным вызовом для всех стран региона.

В настоящее время Армения получает интернет по двум основным коридорам: через Грузию (главный маршрут) и Иран (резервный маршрут). При этом через Грузию Армения имеет выход на Европу и Россию (как сухопутным, так и морским маршрутом). Обращаясь к проблемам грузинского маршрута, следует обратить внимание, во-первых, на отмечаемую экспертами ограниченную пропускную способность и, во-вторых, на возможные перебои в случае кризиса — политического или техногенного. Основания для подобных опасений имеются: в 2019 г. — 49 %, а в 2021 г. оставшиеся 51 % акций компании Caucasus Online, являющейся оператором оптического кабеля, связывающего Болгарию и Грузию через Черное море и обеспечивающего трафик интернета в Армению (80 %), были переданы компании NEQSOL Holding, имеющей азербайджанское

⁸ Хуситы атаковали подводные интернет-кабели, связывающие Европу и Азию // РБК. 27 февраля 2024 г. URL: <https://www.rbc.ru/politics/27/02/2024/65dd643d9a7947adc6142781> (дата обращения: 21.03.2025).

⁹ Китайское судно заподозрили в обрыве кабелей на дне Балтийского моря // Lenta.ru. 20 ноября 2024 г. URL: <https://lenta.ru/news/2024/11/20/v-obryve-telekabeley-v-baltiyskom-more-obvinili-rossiyanina-chto-izvestno/> (дата обращения: 21.03.2025).

происхождение. Естественно, что данная сделка не могла не быть оценена в контексте армяно-азербайджанского конфликта. Особое внимание привлекал тот факт, что, согласно сообщению армянских СМИ, в ходе 44-дневной войны в Нагорном Карабахе 2020 г. проходящий через грузинский город Марнеули интернет-кабель неоднократно повреждался¹⁰. Переход этой критически значимой для Армении инфраструктуры под контроль азербайджанского бизнеса вызвал необходимость поиска новых маршрутов интернет-трафика. После известной сделки официальный Ереван предложил Тбилиси начать реализацию проекта строительства нового цифрового коридора, связывающего Европу и Армению через Черное море, однако по настоящее время инфраструктура не построена. Важно также отметить, что в рамках уже существующего интернет-маршрута армянские операторы выступали в качестве транзитеров интернета в Иран, Афганистан, а начиная с 2019 г. — также в Катар. Таким образом, формирование нового, альтернативного цифрового коридора из Европы в Армению является вызовом развития цифрового суверенитета не только в плане обеспечения внутренней безопасности, но и продвижения своих позиций на коммуникационных рынках Ближнего Востока и Южной Азии.

Узловой транспортной точкой Южного Кавказа продолжает оставаться Грузия, что отражается также на логистике региональных цифровых маршрутов. Основным источником интернет-трафика в Грузию является подводный кабель из Европы (Caucasus Cable System), пролегающий по маршруту Варна — Батуми. Параллельно с этим Грузия располагает также цифровыми коридорами с Россией. Сухопутный кабель проходит по маршруту Тбилиси — Владикавказ — Москва, подводный же соединяет Поти, Новороссийск и Сочи, создавая диверсификационные возможности как для Грузии, так и для Армении, зависящей от грузинского маршрута. Важно при этом отметить, что в настоящее время диверсификацию внешних интернет-маршрутов в Армении часто связывают с возможным налаживанием армяно-турецких отношений с последующим открытием государственных границ и разблокированием транспортных и экономических коммуникаций.

Возвращаясь к российско-грузинскому цифровому коридору, отметим, что само его существование рассматривается в качестве потенциальной угрозы со стороны ЕС. Оценивая данный маршрут как инструмент укрепления российского влияния на Южном Кавказе, в мае 2023 г. Еврокомиссия приняла решение о проложении альтернативного интернет-кабеля по дну Черного моря до Грузии с целью снижения «зависимости Кавказа от наземной оптиковолоконной связи, проходящей транзитом через Россию»¹¹. Исторически выступая

¹⁰ Ереван взялся за интернет-безопасность и предложит Тбилиси проложить кабель мимо Баку // *Спутник Армения*. 29 сентября 2021 г. URL: <https://am.sputniknews.ru/20210929/erevan-vzyalsya-za-internet-bezopasnost-i-predlozhit-tbilisi-prolozhit-kabel-mimo-baku-33727932.html> (дата обращения: 22.03.2025).

¹¹ В Черном море проложат новый кабель из-за тревог ЕС о России // *РБК*. 12 мая 2023 г. URL: https://www.rbc.ru/technology_and_media/12/05/2023/645de2e39a794759c57d5615 (дата обращения: 22.03.2025).

зоной российского влияния, Южный Кавказ сегодня продолжает рассматриваться рядом западных акторов как важное направление внешней политики с целью осуществления в регионе глубинных стратегических перестановок [Буторов и др. 2022]. Проект охватывает более широкую географию, выходя далеко за пределы Южного Кавказа. Согласно обнародованным данным, планируется, что кабель стоимостью 45 млн евро и протяженностью 1,1 тыс. км соединит Украину с Болгарией, Турцией и Грузией, затем подземным путем дойдет до территории Армении и далее через Азербайджан — в страны Центральной Азии. Подобная Черноморско-Каспийская геостратегия вполне вписывается в комплекс инфраструктурных проектов, реализуемых ЕС (например, электроэнергетический кабель по дну Черного моря между Азербайджаном, Грузией, Венгрией и Румынией)¹².

Азербайджан связан цифровыми коридорами с Россией, Грузией и Турцией. Также в настоящее время разрабатывается проект проложения транскаспийского оптоволоконного кабеля протяженностью 370 км и стоимостью 50 млн долл. США, призванного связать Азербайджан с Казахстаном¹³. Впрочем, данный проект преследует намного более амбициозные цели, выходя далеко за пределы обеспечения интернет-трафика между двумя странами. Цель — формирование на территории Азербайджана международного цифрового хаба с дальнейшей интеграцией в т.н. «Цифровой Шелковый путь», представляющий собой глобальную инициативу, реализуемую в рамках проекта «Пояс и Путь» и направленную на развитие цифровой инфраструктуры в странах-участницах [Гамза 2022]. Инициатива охватывает широкую географию — Азию, Африку, Европу и Латинскую Америку, чем и обусловлена периодически звучащая из стран Запада критика, сводящаяся преимущественно к опасениям относительно возможного сбора данных через контролируемые цифровые инфраструктуры. Следуя мегатрендам «четвертой промышленной революции», ЦШП охватывает также проблемы в сфере искусственного интеллекта, больших данных, интернета вещей, облачной логистики, технологий финтеха и пр. Согласно некоторым оценкам, ЦШП служит также своего рода инструментом экономической экспансии посредством создания зон свободной торговли, выстраивания новейшей транспортно-логистической инфраструктуры и пр. [Лю, Авдокушин 2019].

Транскаспийский оптоволоконный кабель, проектируемый через Азербайджан, Грузию, Турцию, а также Казахстан и Туркменистан, по сути, рассматривается как составная часть ЦШП. В связи с подключением Туркменистана к данному маршруту следует отметить, что в ноябре 2019 г. между Баку и Ашхабадом было заключено межгосударственное соглашение о создании интернет-маршрута. Предполагается проложение цифрового коридора

¹² В Черном море проложат новый кабель из-за тревог ЕС о России // РБК. 12 мая 2023 г. URL: https://www.rbc.ru/technology_and_media/12/05/2023/645de2e39a794759c57d5615 (дата обращения: 22.03.2025).

¹³ Trans-Caspian fiber-optic line between Kazakhstan and Azerbaijan could cost \$50 mln // Interfax. 18 June, 224. URL: <https://interfax.com/newsroom/top-stories/103474/> (accessed: 22.03.2025).

протяженностью 300 км от Сиазаньского района Азербайджана до туркменского порта Туркменбаши, что позволит обеспечить интернет-трафик из Европы в Южную Азию и обратно по территории Азербайджана¹⁴. В целом в эти же стратегические цели вписывается также приобретение в 2021 г. Caucasus Online, о чем было сказано выше.

В контексте интеграции Южного Кавказа в международные цифровые коридоры отдельного интереса заслуживает также проект «Трансевразийская информационная супермагистраль» (TASIM), инициированный Азербайджаном в 2008 г. и направленный на создание транснациональной оптиковолоконной магистрали, связывающей страны Евразии от Западной Европы до Восточной Азии [Ure 2021: 24]. Проект предусматривает строительство крупного транзитного маршрута от Франкфурта до Гонконга/Шанхая. Проект получил поддержку ООН, принявшей две резолюции (в 2009 и 2012 гг.) по содействию информационной супермагистрали¹⁵.

Планируется, что маршрут объединит крупнейшие центры по обмену информацией Европы и Азии, пройдет через Китай, Казахстан, Азербайджан, Грузию, Турцию и достигнет Германии. Параллельно с этим также рассматривается резервная магистраль, которая будет проходить по маршрутам Трансанатолийского и Трансдариатического газопроводов (ТАР и TANAP), связывающих Южный Кавказ (Азербайджан и Грузию) с Турцией и Европой с выходом на Италию. Важно отметить, что изначально Россия в лице компании «Ростелеком» рассматривалась в качестве участника международного консорциума по реализации проекта TASIM. Однако в последние годы наблюдается отсутствие активной вовлеченности российской стороны в данный проект. По сути, TASIM — это одна из инициатив формирования цифрового коридора по маршруту Европа — Кавказ — Азия в обход России, полностью вписывающегося в продвигаемую ЕС стратегию «Восток — Запад».

Как видим, страны Южного Кавказа, с одной стороны, нацелены на диверсификацию цифровых телекоммуникационных коридоров, с другой — стремятся интегрироваться в международные маршруты интернет-трафика, что вызвано прежде всего потенциальными рисками и угрозами цифровой и — шире — национальной безопасности. С этой целью страны региона не только поднимают собственный цифровой суверенитет путем развития конвенционных — сухопутных и морских — цифровых коммуникаций, но также делают ставку на применение спутниковой интернет-связи. Свидетельством тому является выстраивание работы с принадлежащей Илону Маску

¹⁴ Азербайджан и Туркменистан подписали соглашение о прокладке фибер-оптической кабельной линии // Исполком СНГ. 28 ноября 2019 г. URL: <https://cis.minsk.by/news/12598/azerbajdzan-i-turkmenistan-podpisali-soglasenie-o-prokladke-fiber-opticeskoj-kabelnoj-linii> (дата обращения: 22.03.2025).

¹⁵ Резолюции Генеральной Ассамблеи ООН 64/186 «Расширение доступа к Интернету благодаря трансевразийской высокоскоростной информационной магистрали» от 21.12.2009 и 67/194 «Расширение доступа к Интернету путем создания трансевразийской высокоскоростной информационной магистрали» от 21.12.2012.

компанией SpaceX, предоставляющей услуги спутникового интернета Starlink. Если Армения и Азербайджан пока находятся на стадии согласования сотрудничества с этой компанией (в Азербайджане уже зарегистрировано представительство компании¹⁶, в Армении же впервые заявили о соответствующих целях в конце 2024 г.¹⁷), то в Грузии Starlink доступен с 2023 г.¹⁸ Эта тенденция также является свидетельством неравномерного развития интернета и, следовательно, указывает на разницу в «цифровой готовности» стран Южного Кавказа.

Заключение

Как показал проведенный межстрановой анализ, повышение цифрового суверенитета рассматривается странами Южного Кавказа как один из ключевых компонентов обеспечения национальной безопасности. В свою очередь, достижение цифрового суверенитета и его дальнейшее поддержание требуют комплексного решения ряда политических и экономических проблем, включая сокращение зависимости от зарубежных технологий, повышение цифровой грамотности населения, обеспечение национального контроля над интернет-трафиком и пр. В случае же со странами Южного Кавказа особую актуальность обретает также проблема диверсификации международных цифровых коридоров, что обусловлено сложной геополитической ситуацией в регионе, не способствующей развитию стабильных и безопасных цифровых коммуникаций.

Характерно, что все страны Южного Кавказа практически в равной степени демонстрируют понимание стратегической значимости цифрового развития, что находит свое отражение как в имеющихся профильных государственных институтах, так и в стратегиях национальной безопасности и «цифровом законодательстве».

Вместе с тем в странах региона наблюдается разный уровень «цифровой готовности», что вызвано геополитическими реалиями и вытекающими из них транспортно-логистическими особенностями. Так, если Грузия фигурирует в качестве регионального «цифрового узла», а Азербайджан демонстрирует потенциал формирования более масштабного цифрового хаба между Центральной Азией и Европой, то находящаяся в полублокадном состоянии Армения сегодня пребывает в состоянии зависимости от пролегающего через Грузию маршрута, что обязывает ее искать новые пути цифровой интеграции с внешним миром и обеспечения национальной цифровой безопасности. Важно при этом учесть проводимую ЕС политику по сокращению цифрового влияния России на Южном Кавказе посредством проложения альтернативных

¹⁶ Starlink открыла представительство в Азербайджане // Trend. 30 декабря 2022 г. URL: <https://www.trend.az/business/3689590.html> (дата обращения: 22.03.2025).

¹⁷ Starlink может стать началом новой технологической эры для Армении: Forbes // Арменпресс. 17 декабря 2024 г. URL: <https://armenpress.am/ru/article/1207629> (дата обращения: 22.03.2025).

¹⁸ Starlink доступен в Грузии, — сообщил Илон Маск // Sputnik Грузия. 1 ноября 2023 г. URL: <https://sputnik-georgia.ru/20231101/starlink-dostupen-v-gruzii-soobschil-ilon-mask-283872026.html> (дата обращения: 22.03.2025).

маршрутов интернет-трафика (например, TASIM): по сути, «транспортная война» между стратегиями «Восток — Запад» и «Север — Юг» все больше скажется на ожесточении конкуренции в сфере выстраивания цифровых коридоров. Одним из ключевых акторов этой конкуренции продолжает оставаться Китай, который посредством своей инициативы ЦШП нацелен на обеспечение интеграции двух указанных стратегий (как и в целом в случае с инициативой «Пояс и путь»). При этом в региональном срезе активность в виде новых коридоров и инфраструктурных решений наблюдается в основном в направлении «Восток — Запад», что также объясняется рассмотренными выше геополитическими реалиями.

Поступила в редакцию / Received: 13.01.2025

Доработана после рецензирования / Revised: 23.04.2025

Принята к публикации / Accepted: 19.04.2025

Библиографический список

- Арутюнян Г.А.* Армения на пути к цифровизации. Вопросы управления и экономики: современное состояние актуальных проблем // Сб. ст. по материалам XLII Междунар. науч.-практ. конф. Москва : Интернаука, 2020. С. 86–91.
- Буторов А.С., Турава Г.М., Плиев С.М.* Особенности российского влияния на обеспечение региональной безопасности на Южном Кавказе // Постсоветские исследования. 2022. Т. 5. № 8. С. 780–786. EDN: JGJSNO
- Винник Д.В.* Цифровой суверенитет: политические и правовые режимы фильтрации данных // Философия науки. 2014. № 2 (61). С. 95–113. EDN: SMIDUD
- Гамза Л.А.* Цифровой Шёлковый путь Китая // Проблемы Дальнего Востока. 2022. № 2. С. 63–79. <https://doi.org/10.31857/S013128120019578-6> EDN: LJYUAW
- Гасанов А.М.* Политика национального развития и безопасности Азербайджанской Республики. Баку: «Zərdabi LTD» ММС, 2014. 672 с.
- Давтян В.С., Маргарян Н.И.* Транспортные коммуникации Южного Кавказа после войны в Нагорном Карабахе // Россия и новые государства Евразии. 2022. № I (LIV). С. 123–135. <https://doi.org/10.20542/2073-4786-2022-1-123-135> EDN: HQRIFY
- Зиновьева Е., Булга В.* Цифровой суверенитет Европейского Союза // Современная Европа. 2021. № 2. С. 40–49. <https://doi.org/http://dx.doi.org/10.15211/soveurope220214049> EDN: IOMTFV
- Кардунян В.* Коллективная безопасность на Южном Кавказе: концептуальный аспект // Россия и новые государства Евразии. 2013. № 3. С. 15–23. EDN: SVKQSB
- Кочетков А.П., Маслов К.В.* Цифровой суверенитет как основа национальной России в глобальном цифровом обществе // Вестник Московского университета. Серия 12. Политические науки. 2022. № 2. С. 31–45. EDN: BJJUXI
- Лю Ижу, Авдокушин Е.Ф.* Формирование основ «цифрового шелкового пути» // Мир новой экономики. 2019. Т. 13. № 3. С. 62–71. <https://doi.org/10.26794/2220-6469-2019-13-4-62-71> EDN: JKFHZZ
- Никонов В.А., Воронов А.С., Сажина В.А., Володенков С.В., Рыбакова М.В.* Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) // Вестник Томского государственного университета. Философия. Социология. Политология. 2021. № 60. С. 206–216. <https://doi.org/10.17223/1998863X/60/18> EDN: PCWPLD

- Омарова Т., Шарипова Д. Цифровизация предоставления государственных услуг и инновации в деятельности государственных органов в Центральной Азии и на Кавказе // Международный журнал реформы и практики государственной службы. 2022. Т. 7, № 1. <https://doi.org/10.56289/ijcsrp.159>
- Романова Т. Эволюция концепции «цифровой суверенитет» в Евросоюзе: константы и дихотомии // Современная Европа. 2023. № 4. С. 62–76. <https://doi.org/10.31857/S0201708323040022> EDN: BVRRNQ
- Ромашкина А.Б., Киричук Д.А. Политическая субъектность цифровых актантов в контексте обеспечения цифрового суверенитета // Вестник Российского университета дружбы народов. Серия: Политология. 2023. Т. 25, № 4. С. 848–861. <https://doi.org/10.22363/2313-1438-2023-25-4-848-861> EDN: WRRDXQ
- Федоровская И. Проекты развития транспортной инфраструктуры в Закавказье // Россия и новые государства Евразии. 2022. № IV (LVII). С. 123–131. <https://doi.org/10.20542/2073-4786-2022-4-123-131> EDN: YFRWMD
- Couture S., Toupin S. What does the notion of “sovereignty” mean when referring to the digital? // New media & society. 2019. Т. 21, № 10. P. 2305–2322 / <https://doi.org/10.1177/1461444819865984>
- Huseynova A.D., Mazanova O. Expansion of E-Services in Azerbaijan: Directions and Perspectives // 55th International Scientific Conference on Economic and Social Development Development. Baku, Azerbaijan, 14–17 February 2020. Vol. 2. P. 656–662.
- Ure J. Digital Solutions Centre in Central Asia // Asia-Pacific Information Superhighway Working Paper. Series No. 7. October 2021. 54 p.

References

- Butorov, A.S., Turava, G.M., & Pliev, S.M. (2022). Features of Russian Influence on Regional Security in the South Caucasus. *Post-Soviet Studies*, 5(8), 780–786. (In Russ.). EDN: JGJSNO
- Couture, S., Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322 / <https://doi.org/10.1177/1461444819865984>
- Davtyan, V.S., & Margaryan, N.I. (2022). Transport Communications of the South Caucasus After the War in Nagorno-Karabakh. *Russia and New States of Eurasia*, I (LIV), 123–135. (In Russ.). <https://doi.org/10.20542/2073-4786-2022-1-123-135> EDN: HQRTFY
- Fedorovskaya, I. (2022). Transport Infrastructure Development Projects in Transcaucasia. *Russia and New States of Eurasia*, (IV), 123–131. (In Russ.). <https://doi.org/10.20542/2073-4786-2022-4-123-131> EDN: YFRWMD
- Gamza, L.A. (2022). China’s Digital Silk Road. *Problems of the Far East*, (2), 63–79. (In Russ.). <https://doi.org/10.31857/S013128120019578-6> EDN: LJYUAW
- Harutyunyan, G.A. (2020). Armenia on the Path to Digitalization. Issues of Management and Economics: Current State of Relevant Problems. *Proceedings of the XLII International Scientific and Practical Conference*. Moscow: Interscience Publishing House, pp. 86–91. (In Russ.).
- Hasanov, A.M. (2014). *National Development and Security Policy of the Republic of Azerbaijan*. Baku: “Zərdabi LTD” MMC, 672 p. (In Russ.).
- Huseynova, A.D., & Mazanova, O. (2020). Expansion of E-Service. In *Azerbaijan: Directions and Perspectives. 55th International Scientific Conference on Economic and Social Development Development*. Baku, Azerbaijan, 14–17 February 2020 (vol. 2, pp. 656–662).
- Kardumyan, V. (2013). Collective Security in the South Caucasus: Conceptual Aspect. *Russia and New States of Eurasia*, (3), 15–23. (In Russ.). EDN: SVKQSB
- Kochetkov, A.P., & Maslov, K.V. (2022). Digital Sovereignty as the Basis of National Russia in the Global Digital Society. *Moscow University Bulletin. Series 12: Political Science*, (2), 31–45. (In Russ.). EDN: BJJUXI

- Liu Yizhu, Avdokushin E.F. (2019). Formation of the Foundations of the “Digital Silk Road”. *World of the New Economy*, 13(3), 62–71. (In Russ.). <https://doi.org/10.26794/2220-6469-2019-13-4-62-71> EDN: JKFHZL
- Nikonov, V.A., Voronov, A.S., Sazhina, V.A., Volodenkov, S.V., & Rybakova, M.V. (2021). Digital Sovereignty of the Modern State: Content and Structural Components (Based on Expert Research). *Tomsk State University Journal of Philosophy, Sociology and Political Science*, (60), 206–216. (In Russ.). <https://doi.org/10.17223/1998863X/60/18> EDN: PCWPLD
- Omarova, T., & Sharipova, D. (2022). Digitalization of Public Service Delivery and Innovations in the Activities of State Bodies in Central Asia and the Caucasus. *International Journal of Civil Service Reform and Practice*, 7(1). <https://doi.org/10.56289/ijcsrp.159>
- Romanova, T. (2023). Evolution of the Concept of “Digital Sovereignty” in the European Union: Constants and Dichotomies. *Contemporary Europe*, (4), 62–76. (In Russ.). <https://doi.org/10.31857/S0201708323040022> EDN: BVRNMQ
- Romashkina, A.B., & Kirichuk, D.A. (2023). Political Agency of Digital Actants in the Context of Ensuring Digital Sovereignty. *RUDN Journal of Political Science*, 25(4), 848–861. (In Russ.). <https://doi.org/10.22363/2313-1438-2023-25-4-848-861> EDN: WRRDXQ
- Ure, J. (2021). Digital Solutions Centre in Central Asia. *Asia-Pacific Information Superhighway Working Paper*. Series No. 7. October 2021. 54 p.
- Vinnik, D.V. (2014). Digital Sovereignty: Political and Legal Regimes of Data Filtering. *Philosophy of Science*, (2), 95–113. (In Russ.). EDN: SMIDUD
- Zinovieva, E., Bulva V. (2021). Digital Sovereignty of the European Union. *Contemporary Europe*, (2), 40–49. (In Russ.). <https://doi.org/http://dx.doi.org/10.15211/soveurope220214049> EDN: IOMTFV

Сведения об авторе:

Давтян Ваге Самвелович — доктор политических наук, профессор, профессор кафедры политологии Российско-Армянского университета, старший научный сотрудник Сектора кавказских исследований Института Китая и современной Азии Российской академии наук (e-mail: vahedavtyan@yandex.ru) (ORCID: 0000-0002-0848-3436)

About the author:

Vahe S. Davtyan — Doctor of Political Sciences, Professor, Professor at the Department of Political Science of Russian-Armenian University, Senior Researcher of the Sector of Caucasian Studies of the Institute of China and Modern Asia of the Russian Academy of Sciences (e-mail: vahedavtyan@yandex.ru) (ORCID: 0000-0002-0848-3436)