Vestnik RUDN. International Relations. ISSN 2313-0660 (Print), ISSN 2313-0679 (Online)
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2026 Vol. 26 No. 2 272–285
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2026-26-2-272-285
EDN: HRIDVR

Научная статья / Research article

Киберпреступность в Латинской Америке: вызовы формирования эффективной системы безопасности в наименее защищенном регионе мира

В.А. Тимощеня, Е.В. Мартыненко

Российский университет дружбы народов, Москва, Российская Федерация
v.timoshchenya@gmail.com

Аннотация. Проблема киберпреступности в Латинской Америке приобретает критический характер на фоне технологической отсталости региона, фрагментации стратегий безопасности и растущей зависимости от иностранных технологических решений. Согласно Глобальному индексу кибербезопасности 2024 г., регион занимает последнее место в мире (35,12 пункта), уступая даже странам Африки (37,25). Данное противоречие усугубляется стремительным ростом кибератак (25 % в год) и ограниченным доступом населения к защищенным интернет-сервисам (62 %). Цель исследования – систематизировать ключевые вызовы, препятствующие формированию эффективной системы кибербезопасности, с акцентом на инфраструктурные ограничения, кадровый дефицит и геополитическую конкуренцию за влияние в цифровой сфере. Научная новизна работы определяется комбинацией методов: сетевого анализа взаимосвязей (*Network Influence Analysis*) для визуализации зон технологического доминирования (США, Китай, Европейский союз, Россия) и контент-анализа 18 национальных стратегий (2020–2026 гг.). Эмпирическая база включает данные Международного союза электросвязи, Межамериканского банка развития, IBM и документы региональных организаций (Организации американских государств (ОАГ), Общего рынка стран Южной Америки (МЕРКОСУР)). Результаты выявили поляризацию подходов: от централизованных систем управления (Бразилия, Коста-Рика) до гибридных моделей цифрового суверенитета (Венесуэла, Куба), сочетающих национальные приоритеты с зависимостью от иностранных технологий. Доминирование компаний *Huawei* (70 % *4G*-сетей) и *Microsoft* (облачные решения) повышает уязвимость критической инфраструктуры. Реактивный характер мер подтверждает пример Коста-Рики, где финансирование кибербезопасности выросло на 446 % после атак 2022 г. Ключевой вывод — необходимость синхронизации региональных инициатив в рамках ОАГ через гармонизацию стандартов (*CSIRT Americas*) и стимулирование государственно-частного партнерства. Только 23 % организаций используют искусственный интеллект для защиты данных (на 17 % ниже глобального уровня). Исследование вносит вклад в дискуссию о балансе геополитических интересов и коллективной безопасности, предлагая адаптивную модель для Латинской Америки. Ее ключевой элемент — целевые инвестиции в оптоволоконные сети, подготовку кадров и интеграцию международных практик с учетом локальной специфики, включая преодоление цифрового разрыва.

Ключевые слова: кибербезопасность, цифровая инфраструктура, региональная безопасность, технологическая зависимость, искусственный интеллект, критическая инфраструктура, геополитическая конкуренция, стратегии киберзащиты

Заявление о доступности данных. Данные, подтверждающие выводы этого исследования, получены из открытых источников и включены в опубликованную статью.

Вклад авторов. Тимощеня В.А.: концептуализация, методология, формальный анализ, проведение исследования, написание, подготовка первоначального черновика. Мартыненко Е.В.: научное руководство, валидация результатов, рецензирование и редактирование. Оба автора ознакомлены с окончательной версией статьи и одобрили ее.

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

Для цитирования: *Тимощеня В. А., Мартыненко Е. В.* Киберпреступность в Латинской Америке: вызовы формирования эффективной системы безопасности в наименее защищенном регионе мира // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2026. Т. 26, № 2. С. 272–285. https://doi.org/10.22363/2313-0660-2026-26-2-272-285; EDN: HRIDVR

Cybercrime in Latin America: Challenges for Building Effective Security in the World's Most Vulnerable Region

Viachaslau A. Tsimashchenia ✉, Evgeny V. Martynenko

RUDN University, Moscow, Russian Federation
✉v.timoshchenya@gmail.com

Abstract. The issue of cybercrime in Latin America has reached critical levels, against a backdrop of the region's technological lag, fragmented security strategies, and a growing reliance on foreign technological solutions. According to the 2024 Global Cybersecurity Index, the region ranks last globally (35.12 points), behind even African countries (37.25). This contradiction is exacerbated by the rapid annual growth in cyberattacks (25%) and limited public access to secure internet services (62%). The study aims to systematize the key challenges hindering the development of an effective cybersecurity system, focusing on infrastructure limitations, workforce shortages, and geopolitical competition for digital influence. The scientific novelty of the work lies in its combination of methods, including network influence analysis to visualize zones of technological dominance (the USA, China, the EU, Russia) and content analysis of 18 national cybersecurity strategies. The empirical foundation incorporates data from the International Telecommunication Union, the Inter-American Development Bank, IBM, and documents from regional organizations, such as the Organization of American States (OAS) and MERCOSUR. The results of this study reveal polarized approaches, ranging from centralized management systems (Brazil, Costa Rica) to hybrid models of digital sovereignty (Venezuela, Cuba), which blend national priorities with reliance on foreign technologies. The dominance of companies like Huawei (70% of 4G networks) and Microsoft (cloud solutions) has exacerbated vulnerabilities in critical infrastructure. The reactive nature of measures is exemplified by Costa Rica, which saw a 446% increase in cybersecurity funding after 2022's cyberattacks. The key conclusion of the study underscores the need for regional cooperation and harmonization of standards under the OAS framework through harmonized standards (CSIRT Americas) and enhanced public-private partnerships. Only 23% of organizations employ AI for data protection (17% below the global average). The study contributes to discussions on balancing geopolitical interests and collective security by proposing a more adaptive model for Latin America. Its core elements include targeted investments in fiber-optic networks, workforce training, and the integration of international best practices adapted to local contexts, with an emphasis on bridging the digital divide.

Key words: cybersecurity, digital infrastructure, regional security, technological dependence, artificial intelligence, critical infrastructure, geopolitical competition, cyber defense strategies

Data availability statement. The data supporting the findings of this study were obtained from public sources and included in the published article.

Authors' contributions. V.A. Tsimashchenia: conceptualization, methodology, formal analysis, investigation, original draft preparation. E.V. Martynenko: supervision, validation, review and editing. Both authors have read and approved the final version of the article.

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

For citation: Tsimashchenia, V. A., & Martynenko, E. V. (2026). Cybercrime in Latin America: Challenges for building effective security in the world's most vulnerable region. *Vestnik RUDN. International Relations*, 26(2), 272–285. https://doi.org/10.22363/2313-0660-2026-26-2-272-285; EDN: HRIDVR

Введение

В системе кризисных явлений Латинской Америки проблематика кибербезопасности представляет собой наименее изученное направление исследований. Регион, направляющий значительные ресурсы на развитие традиционных механизмов обеспечения безопасности, сталкивается с парадоксом: несмотря на развитие конвенциональных структур безопасности, страны Латинской Америки и Карибского бассейна (ЛАКБ) обнаруживают критическую неготовность к противодействию цифровым угрозам. Государства региона, демонстрируя самый высокий в мире рост кибератак — 25 % в год за последнее десятилетие[1], одновременно остаются наименее защищенным регионом со средним показателем кибербезопасности 10,2 из 20[2]. Данный диссонанс усугубляется тем, что 62 % населения не имеют доступа к шифрованным интернет-сервисам[3], а 67 % кибератак на компании ЛАКБ классифицируются как «серьезные»[4], что ставит под угрозу экономическую стабильность и социальное развитие региона.

Ключевой проблемой выступает институциональная инерция. Национальные стратегии кибербезопасности, принятые в 16 странах региона, фокусируются на реактивных мерах, таких как создание групп реагирования на компьютерные инциденты (*Computer Emergency Response Team, CERT*) после крупных атак, но игнорируют превентивные инвестиции в инфраструктуру и кадры. Формирование глобальных систем киберзащиты не учитывает специфику латиноамериканского контекста — сочетание технологической зависимости, неравномерного развития инфраструктуры и фрагментированных правовых рамок.

Цель исследования заключается в систематизации ключевых вызовов, препятствующих формированию эффективной системы кибербезопасности в ЛАКБ, с акцентом на инфраструктурные ограничения, кадровый дефицит и геополитическую конкуренцию за влияние в цифровой сфере.

Методологическая новизна работы базируется на комбинации сетевого анализа зон технологического доминирования (США, Китай, Европейский союз (ЕС)) и контент-анализа 18 национальных киберстратегий, что позволяет выявить поляризацию подходов – от централизованных моделей Бразилии и Коста-Рики до цифрового суверенитета Венесуэлы и Кубы.

Теоретическую рамку исследования составляет синтез теории секьюритизации и концепции международных режимов применительно к киберпространству. Кибербезопасность рассматривается как политико-институциональная категория — процесс, в ходе которого цифровые угрозы конструируются государствами как вопросы национальной безопасности, требующие чрезвычайных мер (Solar, 2023, p. 98). Региональные режимы кибербезопасности понимаются как совокупность норм, институтов и практик, координирующих поведение государственных и негосударственных акторов в цифровой сфере (Grassi, Jacon Ayres Pinto & de Conti Pagliari, 2024, p. 12). Такой подход позволяет связать различия в национальных стратегиях с более широкими процессами региональной фрагментации и геополитической конкуренции.

Эмпирический анализ проводился в два этапа. На первом применялся качественный контент-анализ национальных стратегий кибербезопасности. В выборку вошли 18 официальных доктринальных документов стран Латинской Америки и Карибского бассейна, принятых в 2017–2030 гг. и находящихся в открытом доступе. Критериями отбора служили официальный

[1] Vergara Cobos E. Cybersecurity Economics for Emerging Markets // The World Bank. 2024. URL: https://openknowledge.worldbank.org/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/download (accessed: 10.01.2025).

[2] Global Cybersecurity Index 2024. 5th edition// International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025).

[3] Internet Access Services: Status as of December 31, 2022 // Federal Communications Commission. September 2024. URL: https://docs.fcc.gov/public/attachments/DOC-405486A1.pdf (accessed: 10.01.2025).

[4] El 67% de los ciberataques a empresas latinoamericanas fueron considerados graves // Kaspersky. 16 de octubre de 2024. URL: https://latam.kaspersky.com/about/press-releases/el-67-de-los-ciberataques-a-empresas-latinoamericanas-fueron-considerados-graves?srsltid=AfmBOoq9nKioKhDpad__FYxy25kk2B7vswXyiG6bFQpnaARJLBFroTbU (accessed: 10.01.2025).

(правительственный или ведомственный) статус документа, его действующая редакция и наличие раздела, посвященного кибербезопасности. Кодирование осуществлялось по семи параметрам: ключевые угрозы, приоритеты, защищаемая критическая инфраструктура, используемые технологии, форматы международной кооперации и уровень государственно-частного партнерства. На основе сопоставления кодов выделены три типологические группы стратегий — централизованные, ориентированные на международное сотрудничество и нацеленные на цифровой суверенитет.

На втором этапе использовался сетевой анализ зависимостей (*Network Influence Analysis*) для визуализации зон технологического доминирования внерегиональных акторов. Узлами сети выступили четыре внешних поставщика технологий и инфраструктуры (США, Китай, Евросоюз и Россия) и страны региона. Размер узла отражает совокупный уровень влияния поставщика, а связи типологизированы по четырем каналам зависимости: цифровая инфраструктура, технологии, подготовка кадров и критическая инфраструктура. Данные о связях агрегированы из отчетов международных организаций, корпоративной отчетности технологических компаний и национальных программ цифровой трансформации.

Эмпирическую основу исследования составляют данные Международного союза электросвязи, Межамериканского банка развития, Всемирного банка, компании *IBM*, а также документы региональных организаций (Организации американских государств (ОАГ), Общего рынка стран Южной Америки (МЕРКОСУР)). Основной вывод работы указывает на необходимость «гибридной» модели, синхронизирующей международные стандарты с локальными приоритетами через инвестиции в оптоволоконные сети, подготовку кадров и стимулирование государственно-частного партнерства.

В рамках данного исследования «кибер-управление» рассматривается как система принятия решений и распределения ответственности между государственными органами, частным сектором и международными организациями в области обеспечения безопасности цифровой инфраструктуры (Fuenmayor Tobar et al., 2024, p. 15). Под «кибербезопасностью» авторы понимают комплекс технических, организационных и правовых мер, направленных на защиту компьютерных систем, сетей и данных от несанкционированного доступа, повреждения или атак с целью эксплуатации, нарушения функционирования или кражи информации.

Современные тенденции развития кибербезопасности в Латинской Америке

На фоне глобального ускорения цифровой трансформации Латинская Америка остается одним из наиболее уязвимых регионов мира, что подтверждается данными Национального индекса кибербезопасности (*National Cyber Security Index, NCSI*) (Kosevich, 2024). В настоящее время, с приходом четвертой промышленной революции, регион сталкивается с необходимостью адаптации существующих механизмов безопасности к новым технологическим вызовам (Борзова, Павлова, 2019, с. 51).

По ключевым показателям технологического развития (оптоволоконные сети, точки обмена интернет-трафиком, центры обработки данных, суперкомпьютеры, спутники, полупроводники, участие в крупных технологических компаниях, облачные технологии, патенты в области передовых технологий) регион остается на периферии технологического развития, участвуя лишь в начальных этапах цепочек создания стоимости (Flores Cedeño & López Paz, 2024, p. 685).

К 2022 г. средний уровень проникновения фиксированного широкополосного доступа в регионе достиг 62 %, что существенно ниже показателей Северной Америки и Европы (100 и 90 % соответственно). Проникновение мобильного широкополосного доступа в регионе составляет 78 активных подписок на 100 жителей против 105 в Европе и 150 в Северной Америке (табл. 1)[5].

[5] Показатель отражает число активных подписок на мобильный широкополосный доступ в расчете на 100 жителей и может превышать 100, поскольку один пользователь способен оформить несколько подписок (например, для смартфона и планшета). Методология разработана Международным союзом электросвязи.

Таблица 1. **Ключевые показатели цифровой инфраструктуры по регионам**

Основные показатели	Латинская Америка	Северная Америка	Европа	Азия	Африка
Доступ к Интернету (подписки на 100 жителей)					
Фиксированный широкополосный доступ	62	100	90	41,9	4,6
Мобильный широкополосный доступ	78	150	105	55	48
Инфраструктура					
Дата-центры и IXP	Ограниченные	Развитая сеть	Развитая сеть	Широкая сеть	Низкое
Спутниковая связь	Низкое	Высокое	Среднее	Высокое	Низкое
Технологический потенциал					
Облачные технологии и искусственный интеллект	Ограниченные	Развиты	Развиты	Развиты	Ограниченные
Полупроводниковая индустрия	Начальные стадии	Развита	Развита	Широкая сеть	Ограниченная

Источник: составлено В.А. Тимощеней и Е.В. Мартыненко на основе данных: Facts and Figures 2023 // International Telecommunication Union. URL: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-subscriptions/ (accessed: 10.01.2025); Internet Access Services: Status as of December 31, 2022 // Federal Communications Commission. September 2024. URL: https://docs.fcc.gov/public/attachments/DOC-405486A1.pdf (accessed: 10.01.2025); The State of Mobile Internet Connectivity Report // GSMA Intelligence. October 2023. URL: https://www.gsmaintelligence.com/research/the-state-of-mobile-internet-connectivity-2023 (accessed: 10.01.2025); The Digital Economy and Society Index (DESI) // European Commission. 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 10.01.2025); Global Broadband Subscriptions in Q1 2023: Fibre Glides Past Two Thirds // Point Topic. July 19, 2023. URL: https://www.point-topic.com/post/global-broadband-subscriptions-q1-2023 (accessed: 10.01.2025).

Ограниченное распространение высокоскоростных сетей обусловлено высокими затратами на инфраструктуру, недостаточным финансированием, а также сложностями с обеспечением равномерного покрытия в удаленных и сельских районах. Кроме того, несмотря на более высокий уровень проникновения мобильного широкополосного доступа (78 %), в ЛАКБ данный показатель также остается ниже, чем в развитых странах, таких как США и страны Европы, что ограничивает доступ населения региона к онлайн-услугам, образовательным и медицинским ресурсам, а также к возможностям для бизнеса, особенно в районах с низким уровнем дохода и недостаточной цифровой грамотностью (Flores Cedeño & López Paz, 2024, p. 685).

Ключевые технологические показатели, такие как количество точек обмена интернет-трафиком (*Internet Exchange Point, IXP*) и доступ к дата-центрам, в регионе также остаются ограниченными. В отличие от Северной Америки и Европы Латинская Америка сталкивается с нехваткой критической инфраструктуры для хранения и обработки данных, что влечет за собой высокие затраты на международный трафик и увеличивает задержки при передаче данных (Grassi, Jacon Ayres Pinto & de Conti Pagliari, 2024, p. 14). Данный факт ограничивает местные компании в возможностях конкурировать на глобальном рынке и создает дополнительные риски для обеспечения кибербезопасности в регионе (Симонова и др., 2023). Низкая степень участия Латинской Америки в развитии полупроводниковой промышленности и облачных технологий также указывает на зависимость ЛАКБ от импорта передовых технологий, что затрудняет переход к инновационной экономике и повышает уязвимость перед кибератаками (Vila Seoane, 2021, p. 102). В связи с этим усилия, направленные на расширение доступности высокоскоростного интернета и увеличение инвестиций в технологическую инфраструктуру, становятся особенно актуальными для региона (Fuenmayor Tobar et al., 2024, p. 17).

Масштабы киберпреступности и ее экономические последствия

В 2023 г. Латинская Америка и Карибский бассейн заняли второе место в мире по росту еженедельных криминальных кибератак (29 %), уступая только Северной Америке

Таблица 2. **Сравнительный анализ показателей кибербезопасности и кибератак по регионам**

Регион	Рост еженедельных кибератак, %	Средний показатель по Глобальному индексу кибербезопасности	Позиция в мире	Основной уровень уязвимости	Среднемировой уровень
Северная Америка	52	65,78	1	Умеренный	55,64
ЛАКБ	29	35,12	5	Низкий	
Африка	21	37,25	4	Высокий	
Европа	18	70,15	2	Низкий	
Азия	24	56,50	3	Умеренный	

Источник: составлено В.А. Тимощеней и Е.В. Мартыненко по данным: Global Cybersecurity Index 2024. 5th edition // International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025).

Таблица 3. **Крупные кибератаки на критическую инфраструктуру Латинской Америки в 2022–2023 гг. и их последствия**

Год	Страна	Атакованная инфраструктура	Тип атаки	Последствия	Финансовые потери, млн долл. США
2022	Коста-Рика	Система социального обеспечения	Вымогательское ПО	Остановка социальных служб, шифрование данных	800
2022	Колумбия	Системы здравоохранения	Утечка данных	Утечка конфиденциальной медицинской информации, задержка в обслуживании	550
2023	Мексика	Государственные агентства	Вымогательское ПО	Прерывание работы госуслуг, требование выкупа	700

Источник: составлено В.А. Тимощеней и Е.В. Мартыненко по данным: Cost of a Data Breach Report 2024 // IBM. URL: https://www.ibm.com/reports/data-breach (accessed: 10.01.2025).

(52 %)[6]. Согласно Глобальному индексу кибербезопасности 2024 г., регион демонстрирует самый низкий средний показатель в мире — 35,12 пункта, что ниже африканского (37,25) и среднемирового (55,64) уровней (табл. 2).

Согласно оценкам *LatAm Cyber Security Summit*, годовые убытки от кибератак в Латинской Америке и Карибском бассейне (табл. 3) могут превысить 90 млн долл. США к 2026 г. при среднем показателе более 18,5 млн атак в год[7]. Наиболее заметным примером стала атака на правительственные учреждения Коста-Рики в апреле 2022 г., которая затронула многочисленные государственные структуры с требованием выкупа в размере 10 млн долл. США (Datta & Acton, 2024, p. 60). Последующая атака в мае 2022 г. на фонд социального страхования Коста-Рики вынудила правительство объявить чрезвычайное положение, что стало первым случаем применения чрезвычайных фондов для борьбы с последствиями кибератаки (Datta & Acton, 2024, p. 62).

Согласно отчету *IBM*, компании, внедрившие искусственный интеллект (ИИ) в свои стратегии киберзащиты, сократили жизненный цикл атак с утечкой данных на 94 дня, что позволило сэкономить свыше 1 млн долл. США на устранение последствий[8]. При этом только 23 % организаций региона используют ИИ для защиты, что на 17 % ниже среднемирового уровня (Виноградова, 2023, p. 34). Недостаточная подготовленность и слабая киберзащита создают высокий риск для государственных

[6] Díaz R.M., Núñez G. Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe // CEPAL. 2023. URL: https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content (accessed: 30.10.2024).

[7] LatAm Cyber Summit 2024 Annual Report // CS4CA. URL: https://latam.cs4ca.com/wp-content/uploads/LatAm-Cyber-Summit-2024-Annual-Report.pdf (accessed: 10.01.2025).

[8] См.: Cost of a Data Breach Report 2024 // IBM. URL: https://www.ibm.com/reports/data-breach (accessed: 10.01.2025).

и частных секторов государств ЛАКБ (Urbanovics, 2022, p. 87). В условиях растущей зависимости от цифровых технологий регион должен сосредоточиться на укреплении кибербезопасности, внедрении более строгих мер защиты и развитии кадрового потенциала для противодействия угрозам.

Национальные меры противодействия киберпреступности в странах Латинской Америки

Контент-анализ национальных стратегий кибербезопасности стран Латинской Америки выявил значительные различия в подходах к обеспечению цифровой безопасности. Из 18 проанализированных стратегий полноценные национальные документы разработаны в 16 странах. В Боливии и Венесуэле формальные кибердоктрины отсутствуют, а Куба и Колумбия интегрировали вопросы кибербезопасности в программы цифровой трансформации. Страны региона можно разделить на три группы:

1) государства с централизованной системой управления кибербезопасностью (Бразилия, Чили);

2) страны, ориентированные на международное сотрудничество (Перу, Панама, Парагвай);

3) страны, развивающие цифровой суверенитет (Венесуэла, Куба, Никарагуа).

Наиболее устойчивые модели управления характеризуются государственно-частным партнерством, четкой идентификацией критической инфраструктуры и технологическим развитием (табл. 4).

Центральная Америка и Карибский бассейн сосредоточены на защите госсистем и борьбе с киберпреступностью. Коста-Рика после атак 2022 г. увеличила финансирование кибербезопасности на 446 %[9], а Панама интегрировала цифровую защиту в систему охраны Панамского канала[10]. Доминиканская Республика развивает военную «киберэкспертизу»[11], а Уругвай внедряет квантовую криптографию[12].

Таблица 4. **Контент-анализ стратегий кибербезопасности государств Латинской Америки**

Страна	Год	Ключевые угрозы	Приоритеты	КИ	Технологии	Кооперация	ГЧП
Аргентина	2023	Киберпреступность, утечки данных	КИ, международное сотрудничество	Э, Т, С, Ф	ИИ, блокчейн	ООН, МЕРКОСУР	В
Бразилия	2020–2023	Атаки на инфраструктуру	Централизация управления	Э, Т, В, С, Ф	5G, квантовые	Forum IRS, США	В
Венесуэла	2024	Электоральные атаки	Защита суверенитета	Э, Н, ИС	Нац. система	Россия, Иран	Н
Гватемала	2018	Фишинг	Защита КИ	Э, Т	Облачные	ОАГ, Межамериканский банк развития	СР
Доминикана	2021–2024	Военные уязвимости	Центр операций	Э, С, О	ИИ-системы	США, ЕС	В
Колумбия	2023–2026	Цифровой разрыв	Социальная трансформация	Э, С, Т	ИИ, спутники	ОЭСР, США	СР
Коста-Рика	2023–2027	Вымогатели	Центр кибербезопасности	С, Э, З	Блокчейн, ИИ	США, ЕС	В
Куба	2024	Санкции	Развитие нац. ПО	Э, З, ИКТ	Облачные	Россия, Китай	Н

[9] MICITT lidera la respuesta nacional ante el creciente panorama de ciberamenazas // Presidencia de la República de Costa Rica. Octubre 2024. URL: https://www.presidencia.go.cr/noticias/micitt-lidera-la-respuesta-nacional-ante-el-creciente-panorama-de-ciberamenazas (accessed: 10.01.2025).

[10] Resolución N° 17 del Consejo Nacional para la Innovación Gubernamental, de 10 de septiembre de 2021. Estrategia Nacional de Ciberseguridad 2021–2024 // Gaceta Oficial de Panamá. URL: https://www.gacetaoficial.gob.pa/storage/gacetas/2021/12/29434_A/88864.pdf (accessed: 01.03.2026).

[11] Decreto 313-22. Estrategia Nacional de Ciberseguridad 2021–2030 de la República Dominicana // Centro Nacional de Ciberseguridad. URL: https://cncs.gob.do/decreto-313-22/ (accessed: 10.01.2025).

[12] Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030 // Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). 27 de febrero de 2025. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-2024-2030-0 (accessed: 01.03.2026).

Окончание табл. 4

Страна	Год	Ключевые угрозы	Приоритеты	КИ	Технологии	Кооперация	ГЧП
Мексика	2017	Киберпреступность	Международная координация	Э, Т, Ф	Системы защиты	ООН, ОАГ	СР
Никарагуа	2020–2025	Внешние угрозы	Центр реагирования	Э, Т	–	Россия, ОАГ	Н
Панама	2021–2024	Атаки на Панамский канал	КИ, обучение	К, Э, З	ИИ-мониторинг	ОАГ	В
Парагвай	2024–2028	Целевые атаки	Центр реагирования	Э, В, С	Биометрия	Межамериканский банк развития, МЕРКОСУР	СР
Перу	2021–2026	Слабая защита	Центр безопасности	Э, Т, З	Аналитика	Межамериканский банк развития, ООН	Н
Сальвадор	2024	Атаки на госсистемы	Агентство защиты	Э, С, Ф	ИИ-системы	CISCO, ЕС	СР
Уругвай	2024–2030	Вымогатели	Квантовая защита	Э, Ф, Т	Квантовая	Межамериканский банк развития, ОАГ	В
Чили	2023–2028	Дефицит кадров	Агентство безопасности	Э, Т, З	ИИ-системы	Испания	В
Эквадор	2022–2025	Устаревшие системы	Центр реагирования	Э, Т, Ф	Анализ данных	ЕС, ОАГ	СР

Примечания. КИ (критическая инфраструктура): Э — энергетика, Т — транспорт, С — связь, Ф — финансы, З — здравоохранение, В — водоснабжение, О — оборона, Н — нефтяной сектор, К — канал, ИС — избирательные системы, ИКТ — информационно-коммуникационные технологии.

ГЧП (государственно-частное партнерство): В — высокий уровень, СР — средний уровень, Н — низкий уровень.

Источник: составлено В.А. Тимощеней и Е.В. Мартыненко на основании: Resolución 44/2023 de la Secretaría de Innovación Pública. Segunda Estrategia Nacional de Ciberseguridad // Boletín Oficial de la República Argentina. 1 de septiembre de 2023. URL: https://servicios.infoleg.gob.ar/infolegInternet/anexos/385000-389999/389245/norma.htm (accessed: 01.03.2026); Decreto N° 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber) // Presidência da República. URL: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm (accessed: 01.03.2026); Decreto 4975 sobre Consejo Nacional de Ciberseguridad // Gaceta Oficial de la República Bolivariana de Venezuela. 20 de agosto de 2024. URL: https://tugacetaoficial.com/leyes/decreto-4975-sobre-consejo-nacional-de-ciberseguridad/ (accessed: 01.03.2026); Estrategia Nacional de Seguridad Cibernética // Ministerio de Gobernación de Guatemala. 2018. URL: https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad de la República Dominicana 2021–2024 (ENCS) // Agenda Digital. URL: https://agendadigital.gob.do/wp-content/uploads/2022/02/Plan-de-Accion-2021-2024-v2.pdf (accessed: 01.03.2026); Estrategia Nacional Digital de Colombia 2023–2026 // Ministerio de Tecnologías de la Información y las Comunicaciones. 2023. URL: https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad de Costa-Rica 2023–2027 // Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). 2023. URL: https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf (accessed: 01.03.2026); Decreto-Ley No. 35 de las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y del Uso del Espectro Radioeléctrico // Cubalex. 17 de agosto de 2021. URL: https://cubalex.org/2021/08/17/nuestros-abogados-opinan-sobre-el-decreto-ley-35-recien-aprobado-por-el-consejo-de-estado-y-el-consejo-de-ministros/ (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad // Gobierno de México. 2017. URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (accessed: 01.06.2026); De aprobación de la "Estrategia nacional de ciberseguridad 2020–2025". Decreto presidencial n°. 24-2020, aprobado el 24 de septiembre de 2020 // Cyber Policy Portal Database. URL: https://database.cyberpolicyportal.org/entity/xsbof4xi99n?page=6&file=1658413502730hn23ut3iucl.pdf (accessed: 01.03.2026); Resolución N° 17 del Consejo Nacional para la Innovación Gubernamental, de 10 de septiembre de 2021. Estrategia Nacional de Ciberseguridad 2021–2024 // Gaceta Oficial de Panamá. URL: https://www.gacetaoficial.gob.pa/storage/gacetas/2021/12/29434_A/88864.pdf (accessed: 01.03.2026); Decreto Ejecutivo N° 3900, de 22 de mayo de 2025. Estrategia Nacional de Ciberseguridad 2025–2028 // Ministerio de Tecnologías de la Información y la Comunicación (MITIC) de Paraguay. 23 de mayo de 2025. URL: https://drive.mitic.gov.py/s/ZS7YXfEJrxfgdia?dir=/&editing=false&openfile=true (accessed: 01.03.2026); Propuesta de la Estrategia Nacional de Ciberseguridad del Perú 2026–2028 (ESNACIB) // Secretaría de Gobierno y Transformación Digital — Presidencia del Consejo de Ministros. 15 de agosto de 2025. URL: https://www.gob.pe/institucion/pcm/informes-publicaciones/7046161-estrategia-nacional-de-ciberseguridad-del-peru-2026-2028-esnacib (accessed: 01.03.2026); Decreto N° 143. Ley de Ciberseguridad y Seguridad de la Información // Asamblea Legislativa de la República de El Salvador. 12 de noviembre de 2024. URL: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/D056D9A1-299D-4188-941A-9C3B5898D3F3.pdf (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad del Uruguay 2024–2030 // Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). 27 de febrero de 2025. URL: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciberseguridad-2024-2030-0 (accessed: 01.03.2026); Decreto N° 164/2023 del Ministerio del Interior y Seguridad Pública. Aprueba la Política Nacional de Ciberseguridad 2023–2028 // Ministerio del Interior y Seguridad Pública. 4 de diciembre de 2023. URL: https://www.bcn.cl/leychile/navegar?idNorma=1198702 (accessed: 01.03.2026); Estrategia Nacional de Ciberseguridad // Gobierno Electrónico del Ecuador. 2022. URL: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf (accessed: 01.03.2026).

Финансирование остается ключевым фактором эффективности национальных стратегий. Крупнейшие экономики (Бразилия, Мексика) инвестируют в технологии и подготовку кадров, тогда как страны с ограниченными ресурсами (Парагвай, Гватемала) зависят от международных доноров, что усложняет реализацию долгосрочных проектов.

Международное сотрудничество также неоднородно: Венесуэла и Куба ориентируются на партнерство с Россией и Китаем, а Колумбия, Чили и Перу укрепляют связи с Организацией экономического сотрудничества и развития (ОЭСР) и США. Различие стратегий отражает более широкий геополитический контекст и влияет на модели регулирования, выбор технологий и интеграцию в глобальные системы цифровой безопасности.

Развитие региональных режимов кибербезопасности

В контексте данного исследования под «режимами кибербезопасности» понимаются структурированные системы управления, норм, институтов и практик, регулирующих поведение государственных и негосударственных субъектов в киберпространстве (Grassi, Jacon Ayres Pinto & de Conti Pagliari, 2024, p. 12). Региональные режимы могут быть классифицированы по степени централизации (от иерархических до сетевых), по ориентации (технико-инфраструктурные, государственно-центричные или ориентированные на права пользователей), а также по уровню институционализации (Solar, 2023, p. 98).

В сфере развития региональных режимов и институтов управления кибербезопасностью наиболее значительные достижения отмечаются на межамериканском уровне. Развитие региональных режимов кибербезопасности в Латинской Америке опирается на координацию в рамках ОАГ, реализующей комплексную программу через Межамериканский комитет по борьбе с терроризмом (*Comité Interamericano contra el Terrorismo, CICTE*). В рамках инициативы создана сеть групп реагирования на инциденты кибербезопасности (*Computer Security Incident Response Team, CSIRT*) — *CSIRT Americas*, объединяющая 47 национальных центров реагирования из 20 стран региона, что позволяет организовывать обмен оперативными данными об угрозах, координировать защитные меры и проводить совместные учения (Guevara, 2022, p. 420). Финансирование сети осуществляется за счет государственных взносов стран-участниц, международных грантов и технической помощи частного сектора, включая крупные технологические компании (табл. 5).

Дополнительно при поддержке ОАГ в структуре КАРИКОМ действует Региональный центр сбора и анализа оперативной информации (*Regional Intelligence Fusion Centre, RIFC*), обеспечивающий мониторинг угроз и защиту критической инфраструктуры через распределенную систему анализа и моделирование кибератак в реальном времени. Информация поступает от национальных центров кибербезопасности и частных технологических партнеров, что позволяет оперативно выявлять новые методы атак и вырабатывать защитные меры.

ОАГ также реализует масштабную программу подготовки специалистов, направленную на сокращение кадрового разрыва. В рамках Центра образования и развития трудовых ресурсов в области кибербезопасности (*National Initiative for Cybersecurity Education, NICE*) подготовлено более 6000 специалистов, однако этого недостаточно для покрытия существующего дефицита кадров[13]. Программы финансируются при участии Межамериканского банка развития и ведущих технологических компаний, включая *Microsoft, Amazon Web Services (AWS)* и *Cisco*, которые также оказывают техническую поддержку образовательным инициативам. Дополнительно Межамериканский банк развития финансировал программу «Создание карьерного пути в сфере кибербезопасности (2017–2024)» (*Creating a Career Path in Cybersecurity (2017–2024)*), направленную на формирование долгосрочных карьерных маршрутов в сфере кибербезопасности[14].

[13] Vergara Cobos E., Diao H. De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo // Banco Mundial Blogs. 28 de noviembre de 2024. URL: https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe (accessed: 10.01.2025).

[14] Creating a Career Path in Cybersecurity (2017–2024) // OAS. URL: https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1173&lang=1 (accessed: 10.01.2025).

Таблица 5. **Региональные инициативы кибербезопасности в Латинской Америке**

Инициатива	Запуск / обновление*	Цели	Финансирование
CSIRT Americas (ОАГ)	2004/2023	Создание сети центров реагирования на кибератаки	Государственные взносы, гранты ОАГ, частные спонсоры
План действий КАРИКОМ по кибербезопасности и борьбе с киберпреступностью (CARICOM Cyber Security and Cybercrime Action Plan)	2016/2019	Гармонизация стандартов кибербезопасности, борьба с преступностью	USAID, взносы государств КАРИКОМ, международные доноры
Цифровая повестка МЕРКОСУР (MERCOSUR Digital Agenda)	2017/2023	Развитие цифровой безопасности, единые регламенты	Государственные бюджеты МЕРКОСУР, гранты
eLAC2026 (CEPAL (ООН))	2005/2024	Расширение цифровой инфраструктуры, повышение кибербезопасности	Государственные взносы, поддержка ООН, инвестиции ЕС
Иберо-американский форум киберзащиты (Ibero-American Cyber Defense Forum)	2016/2024	Сотрудничество военных и оборонных ведомств стран в сфере киберзащиты	Государственные бюджеты, оборонные инвестиции
Цифровая повестка Тихоокеанского альянса (Pacific Alliance Digital Agenda)	2016/2023	Цифровая интеграция и развитие кибербезопасности	Государственные бюджеты, международные фонды
SICA Cybersecurity Initiative (Центральная Америка)	2019/2024	Разработка единой правовой базы по киберпреступности	Внутренние ресурсы, поддержка России
Будапештская конвенция (Совет Европы)	2001/2022	Унификация уголовного законодательства, борьба с киберпреступностью	Страны-участницы, гранты ЕС

Примечание. * — Данные о годах обновления инициатив актуальны на февраль 2025 г. согласно последним доступным отчетам организаций.

Источник: составлено В.А. Тимощеней по данным: Protecting the Americas in Cyberspace // Organization of American States (OAS) — Cybersecurity Program. URL: https://csirtamericas.org/en/ (accessed: 01.03.2026); Updated CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) launched // CARICOM Implementation Agency for Crime and Security (IMPACS). November 1, 2025. URL: https://www.caricomimpacs.org/articles/updated-caricom-cyber-security-and-cybercrime-action-plan-ccscap-launched (accessed: 01.03.2026); Grupo Agenda Digital del MERCOSUR // MERCOSUR. URL: https://www.mercosur.int/temas/agenda-digital/ (accessed: 01.03.2026); Digital Agenda for Latin America and the Carribean (eLAC2026) // CEPAL. November 8, 2024. URL: https://www.cepal.org/en/publications/80861-digital-agenda-latin-america-and-caribbean-elac2026 (accessed: 01.03.2026); España lidera en 2022 el Foro Iberoamericano de Ciberseguridad // Ministerio de Defensa de España. 17 de marzo de 2022. URL: https://www.defensa.gob.es/comun/slider/2022/03/220317-presidencia-fic-2022.html (accessed: 01.03.2026); Technical Group Digital Agenda // Alianza del Pacífico. URL: https://alianzapacifico.net/en/technical-group-digital-agenda/ (accessed: 01.03.2026); Región SICA avanza en Ciberseguridad e Inteligencia Artificial // Sistema de la Integración Centroamericana (SICA). 28 de agosto de 2024. URL: https://www.sica.int/noticias/region-sica-avanza-en-ciberseguridad-e-inteligencia-artificial_1_134432.html (accessed: 01.03.2026); Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 г. Неофициальный перевод // Совет Европы. URL: https://rm.coe.int/1680081580 (дата обращения: 01.03.2026).

Различия в уровне цифрового развития стран региона создают барьеры для построения единого механизма кибербезопасности. В то время как Бразилия, Мексика, Чили и Колумбия внедряют передовые технологии защиты, развивают национальные центры киберкомпетенций и интегрируют кибербезопасность в стратегическое планирование, малые государства региона испытывают нехватку базовой инфраструктуры и кадров (Lemos, de Espíndola & Tosatti, 2024). ОАГ стремится сократить этот разрыв через программы технической помощи и целевого финансирования, однако эффективность этих мер во многом зависит от способности стран-получательниц адаптировать и применять предлагаемые механизмы.

Помимо инициатив ОАГ на региональном уровне действуют программы цифровой интеграции, такие как Цифровая повестка МЕРКОСУР, ориентированная на унификацию стандартов защиты данных[15], и План действий КАРИКОМ по кибербезопасности и киберпреступности, направленный на выработку единых подходов к борьбе с киберпреступностью

[15] Grupo Agenda Digital del MERCOSUR // MERCOSUR. URL: https://www.mercosur.int/temas/agenda-digital/ (accessed: 01.03.2026).

в Карибском регионе[16]. Центральноамериканская система интеграции (*SICA*) реализует программу по гармонизации законодательства и созданию совместных механизмов кибербезопасности. Важным шагом к международной координации стало присоединение девяти стран региона к Будапештской конвенции Совета Европы, что упрощает сотрудничество в расследовании киберпреступлений и способствует унификации правовых механизмов[17].

Несмотря на активную работу ОАГ и других организаций, отсутствие централизованной координации и неравномерность финансирования остаются основными вызовами для государств ЛАКБ (Косевич, 2022, с. 114). Дальнейшее развитие регионального режима кибербезопасности требует усиления финансовой поддержки менее развитых стран и расширения технической помощи для преодоления цифрового разрыва.

Уязвимость цифрового суверенитета: зависимость Латинской Америки от внешних технологий

Кибербезопасность стран Латинской Америки определяется зависимостью от технологий и инфраструктуры, поставляемых США, Китаем, Европейским союзом и Россией. Китайские компании *Huawei* и *ZTE* доминируют в сегменте телекоммуникационной инфраструктуры, обеспечивая до 70 % *4G*-сетей в регионе и активно участвуя в строительстве *5G* (Mendez & Estrada, 2025, p. 200). Наиболее показательны примеры Бразилии, где *Huawei* поставляет оборудование для шести из семи мобильных сетей (Borrastero & Juncos, 2024, p. 126), и Венесуэлы, где *ZTE* реализовала проект цифровой идентификации *Carnet de la Patria* (Arsentyeva, 2024, p. 61). Системы видеонаблюдения китайского производства также развернуты в Аргентине, Боливии, Эквадоре, Панаме и Уругвае.

В сфере программного обеспечения и облачных технологий доминируют американские компании *Microsoft, Amazon* и *Google*. США активно инвестируют в развитие кибербезопасности через различные программы, включая выделение 25 млн долл. США на создание центра кибероперациий в Коста-Рике[18] и 10 млн долл. США Ямайке через Агентство США по международному развитию (*USAID*)[19]. Европейский союз, в свою очередь, продвигает нормативное регулирование через Цифровой Альянс ЕС — ЛАКБ, внедряя стандарты Общего регламента по защите данных (*General Data Protection Regulation, GDPR*), в то время как Россия сосредотачивается на системах мониторинга и сотрудничестве с Венесуэлой и Никарагуа (Solar, 2023).

В регионе наблюдается существенный кадровый дефицит: несмотря на реализацию китайской программы *Huawei ICT Academy* в 90 университетах (выпущено 36 000 подготовленных специалистов)[20] и сети *Red Ciberlac* Межамериканского банка развития (26 университетов из 12 стран)[21], нехватка

[16] CARICOM Cyber Security and Cybercrime Action Plan // Caribbean Telecommunications Union. URL: https://ctu.int/wp-content/uploads/2021/02/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan_Final_Ver3-copy.pdf (accessed: 10.01.2025).

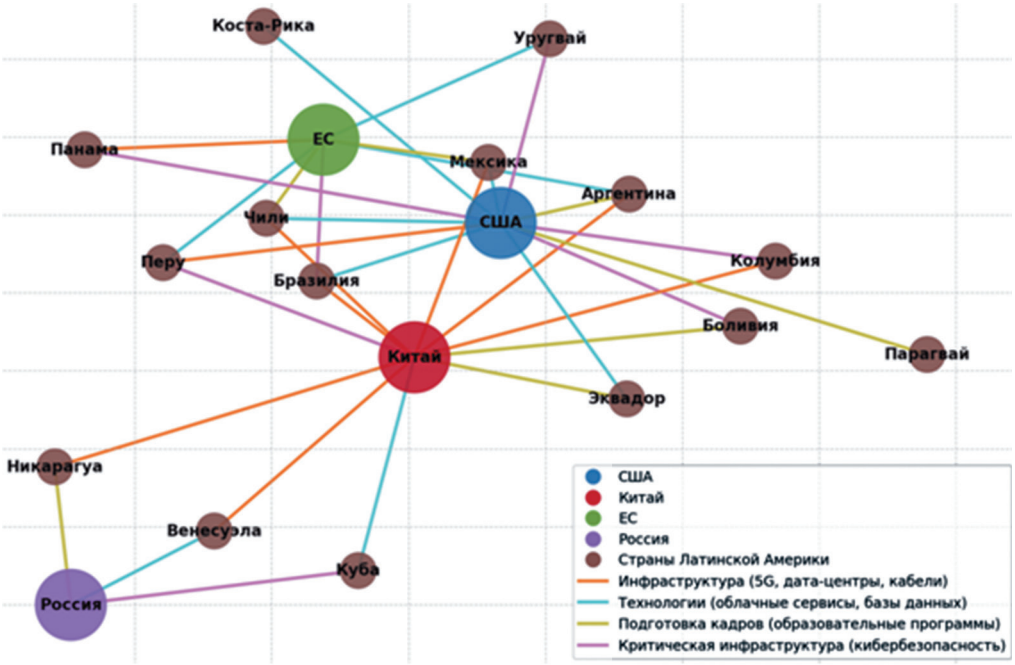
[17] The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols // The Council of Europe. 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 10.01.2025).

[18] United States Announces $25 Million to Strengthen Costa Rica's Cybersecurity // U.S. Embassy in Costa Rica. March 29, 2023. URL: https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/ (accessed: 10.01.2025).

[19] Patterson C. Jamaica's Cybersecurity Infrastructure Strengthened Through Stakeholder Initiatives // The Jamaica Information Service, Government of Jamaica. June 28, 2023. URL: https://jis.gov.jm/jamaicas-cybersecurity-infrastructure-strengthened-through-stakeholder-initiatives/ (accessed: 10.01.2025).

[20] Baisotti P. La ofensiva del encanto de China en América Latina y el Caribe: Un análisis exhaustivo de la estrategia de comunicación de China en la región [Parte II: Influir en los medios de comunicación] // Diálogo Américas. 6 de marzo de 2024. URL: https://dialogo-americas.com/es/articles/la-ofensiva-del-encanto-de-china-en-america-latina-y-el-caribe-un-analisis-exhaustivo-de-la-estrategia-de-comunicacion-de-china-en-la-region-parte-ii-influir-en-los-medios-de-comunicacion/ (accessed: 10.01.2025).

[21] Cyber Range por Red Ciberlac: una plataforma para la creación de capacidades en ciberseguridad en América Latina y el Caribe // Inter-American Development Bank. 30 de abril de 2024. URL: https://www.iadb.org/es/blog/modernizacion-del-estado/administracion-publica/cyber-range-por-red-ciberlac-una-plataforma-para-la-creacion-de-capacidades-en-ciberseguridad-en (accessed: 10.01.2025).



Зависимость стран Латинской Америки от иностранных поставщиков кибербезопасности:
размер узлов отражает уровень влияния поставщика. Цвета узлов: синий — США, красный — Китай, зеленый — ЕС, фиолетовый — Россия, коричневый — страны Латинской Америки. Линии: оранжевые — цифровая инфраструктура, голубые — технологии, желтые — подготовка кадров, розовые – критическая инфраструктура

Источник: составлено В.А. Тимощеней и Е.В. Мартыненко по данным: 2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean // Inter-American Development Bank, Organization of American States. URL: https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and (accessed: 01.03.2026); Global Cybersecurity Index 2024. 5th edition // International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 10.01.2025); Digital Connectivity for Inclusion and Growth. Latin America and the Caribbean Economic Review // World Bank. October 2023. URL: https://openknowledge.worldbank.org/entities/publication/e046afb8-c194-499b-8fdd-f88ac767c33a (accessed: 01.03.2026); 2023 Annual Report // Huawei Investment & Holding Co., Ltd. 2024. URL: https://www-file.huawei.com/minisite/media/annual_report/annual_report_2023_en.pdf (accessed: 01.03.2026); 2023 Annual Report 2023 // Microsoft Corporation. URL: https://www.microsoft.com/investor/reports/ar23/index.html (accessed: 01.03.2026); Amazon Web Services in Latin America // Amazon Web Services, Inc. URL: https://aws.amazon.com/solutions/case-studies/innovators/latam-innovators/ (accessed: 01.03.2026); Creating a World of Potential: 2023 Annual Report // Cisco Systems, Inc. 2023. URL: https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-summary-2023.pdf (accessed: 01.06.2026); 2023 Annual Report // ZTE Corporation. 2024. URL: https://www.zte.com.cn/content/dam/zte-site/investorrelations/en_annual_report/20240326.pdf (accessed: 01.03.2026).

квалифицированных специалистов, по оценкам ОАГ, превышает 520 000 человек[22]. Рост спроса на специалистов опережает темпы подготовки из-за цифровой трансформации. Технологическая зависимость усугубляется низким уровнем проникновения Интернета — только 62 % населения региона имеют доступ к сети против 100 % в Северной Америке и 90 % в Европе (см. табл. 1).

Как показывает анализ зависимости стран Латинской Америки от иностранных поставщиков кибербезопасности (рис.), крупнейшие поставщики технологий разделяют регион на зоны влияния: США контролируют облачные сервисы и кибербразведку, Китай доминирует в телекоммуникационной инфраструктуре, ЕС внедряет правовые стандарты, а Россия развивает программы кибероборонны.

В условиях геополитической конфронтации такая многовекторная зависимость создаёт риски для устойчивости цифровых систем региона и вписывается в более широкую логику цифрового развития государств Глобального Юга в условиях технологического соперниче-

[22] Reporte sobre el desarrollo de la Fuerza Laboral de Ciberseguridad en una Era de Escasez de Talento y Habilidades // OEA. 2022. URL: https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf (accessed: 10.01.2025).

ства США и КНР (Столетов, 2022). Это особенно заметно в контексте американской стратегии противодействия китайскому влиянию через предложение альтернативных инвестиционных проектов (Дегтерев, Пискунов, Еремин, 2023), как в случае с Эквадором, получившим заем в 3,5 млрд долл. США от Международной финансовой корпорации развития США (*U.S. International Development Finance Corporation, DFC*) при условии отказа от китайских технологий в *5G*-инфраструктуре (Flor-Unda et al., 2023, p. 3).

Заключение

Проведенное исследование выявило парадоксальную ситуацию: регион с богатым опытом многостороннего взаимодействия в традиционных сферах безопасности демонстрирует неспособность сформировать эффективную систему коллективной киберзащиты, что обусловлено сочетанием трех ключевых факторов: технологической фрагментацией при интеграции в конкурирующие экосистемы (американскую, китайскую и европейскую), рекомендательным характером региональных механизмов без обязательных норм взаимодействия и существенным разрывом в уровне цифрового развития между странами.

Ключевым вызовом остается отсутствие всеобъемлющей стратегии кибербезопасности, учитывающей специфику латиноамериканского контекста. Несмотря на функционирование механизмов сотрудничества (*CSIRT Americas*, программы ОАГ), их эффективность ограничивается недостаточным обменом информацией об угрозах и успешных практиках. Формирование единой региональной платформы обмена данными о кибератаках становится необходимым условием преодоления фрагментации.

Преодоление выявленных ограничений требует перехода от национальных подходов к интегрированной региональной системе, включающей постоянно действующий механизм координации между центрами реагирования, гармонизацию законодательства и общие протоколы защиты критической инфраструктуры. Ключевую роль приобретает государственно-частное партнерство для стимулирования инвестиций в подготовку кадров и модернизацию цифровой инфраструктуры.

При сохранении геополитической конкуренции за цифровое влияние критически важным становится баланс между интеграцией в глобальные технологические цепочки и развитием собственного потенциала кибербезопасности. Наблюдается дисбаланс между растущими инвестициями и их эффективностью: отсутствие системного подхода к развитию человеческого капитала снижает результативность вложений. Заслуживает внимания и проблема цифрового суверенитета, когда стремление к технологической независимости при ограниченных ресурсах может привести к изоляции от передовых решений. Региону требуется многоуровневая модель сотрудничества с дифференцированными форматами взаимодействия для стран с разным технологическим потенциалом при сохранении общего вектора развития коллективной кибербезопасности.

Поступила в редакцию / Received: 05.12.2024
Доработана после рецензирования / Revised: 27.02.2026
Принята к публикации / Accepted: 27.03.2026

Список литературы

Борзова А. Ю., Павлова М. П. Сотрудничество стран Латинской Америки и Карибского бассейна по поддержанию устойчивого развития региона // Латинская Америка. 2019. № 8. С. 47–60. EDN: NQMLZY

Виноградова Е. А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке // Латинская Америка. 2023. № 3. С. 34–48. EDN: ODEFBD

Дегтерев Д. А., Пискунов Д. А., Еремин А. А. 5G-конкуренция США и КНР в странах Латинской Америки: у истоков технологического декаплинга // Полис. Политические исследования. 2023. № 3. С. 20–38. https://doi.org/10.17976/jpps/2023.03.03; EDN: OPJLVI

Косевич Е. Ю. Защита киберпространства в странах Латинской Америки // Полис. Политические исследования. 2022. № 3. С. 108–123. https://doi.org/10.17976/jpps/2022.03.09; EDN: HCOGEP

Симонова Л. Н., Лавут А. А., Мацур В. А., Разумовский Д. В., Кучинов П.А. и др. Цифровая трансформация в Латинской Америке. Москва : ИЛА РАН, 2023. EDN: UMFZEK

Столетов О. В. Стратегии цифрового развития ключевых государств «Глобального Юга» в условиях американо-китайского технологического соперничества // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2022. Т. 22, № 2. С. 221–237. https://doi.org/10.22363/2313-0660-2022-22-2-221-237; EDN: SYEGYC

Arsentyeva I. I. China's Digital Silk Road: Challenges and Opportunities for Latin America and the Caribbean // Vestnik RUDN. International Relations. 2024. Vol. 24, no. 1. P. 51–64. https://doi.org/10.22363/2313-0660-2024-24-1-51-64; EDN: EUXXHM

Borrastero C., Juncos I. El Oligopolio Tecnológico Global, la Periferia Digital y América Latina // Desarrollo Económico. Revista de Ciencias Sociales. 2024. Vol. 64, no. 243. P. 110–136. https://doi.org/10.59339/de.v64i243.699; EDN: VMVODL

Datta P. M., Acton T. Ransomware and Costa Rica's National Emergency: A Defense Framework and Teaching Case // Journal of Information Technology Teaching Cases. 2024. Vol. 14, iss. 1. P. 56–67. https://doi.org/10.1177/20438869221149042; EDN: JPSPVH

Flores Cedeño P. R., López Paz C. R. Government Management of Information Technology in the Latin American Context // Salud, Ciencia y Tecnologia — Serie de Conferencias. 2024. No. 3. P. 682–693. https://doi.org/10.56294/sctconf2024682; EDN: KFTAEO

Flor-Unda O., Simbaña F., Larriva-Novo X., Acuña Á., Tipán R., Acosta-Vargas P. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America // Informatics. 2023. Vol. 10, no. 3. P. 1–24. https://doi.org/10.3390/informatics10030071

Fuenmayor Tobar J. H., Torres Lozano D. K., Monsalve Pérez L. D., Becerra Moreno A. M. La Inteligencia Artificial y Blockchain, Dos Elementos Decisivos en el Futuro de la Ciberseguridad // Revista Agunkuyâa. 2024. Vol. 14, no. 1. P. 13–26. URL: https://revia.areandina.edu.co/index.php/Cc/article/view/2431/2760 (accessed: 02.12.2025).

Grassi J. M., Jacon Ayres Pinto D., de Conti Pagliari G. Cooperação em Segurança e Defesa Cibernética e a Proteção das Democracias Sul-Americanas // Relações Internacionais. 2024. No. 82. P. 11–27. https://doi.org/10.23906/ri2024.82a02; EDN: LZIFNL

Guevara M. B. C. América Latina, Relaciones Políticas Internacionales, Medios de Comunicación. Discriminación (Revisión) // Roca: Revista Científico-Educaciones de la Provincia de Granma. 2022. Vol. 18, no. 2. P. 410–426. URL: https://revistas.udg.co.cu/index.php/roca/en/article/view/3365/7606#info (accessed: 01.12.2025).

Kosevich E. Cybersecurity, Cyberspace and Cyberthreats at the Beginning of the 21st Century: A Latin America Typology and Review // Area Development and Policy. 2024. Vol. 9, iss. 1. P. 86–107. https://doi.org/10.1080/23792949.2023.2259972; EDN: DEZTKI

Lemos G., de Espíndola M. B., Tosatti N. C. M. Soberania Digital: Definições, Desafios e Implicações na Era da Datificação // Logeion: Filosofia da Informação. 2024. Vol. 11. P. 1–22. https://doi.org/10.21728/logeion.2024v11e-7364; EDN: EBORFM

Mendez A., Estrada G. Geopolitical Game-Changer: China's Expanding Role in Latin America's Defense, Aerospace, and Telecommunications // The Great Power Competition / ed. by A. Farhadi, M. Grzegorzewski, A. J. Masys. Cham, Switzerland : Springer, 2025. P. 185–206. https://doi.org/10.1007/978-3-031-70767-4_9

Solar C. Cybersecurity Governance in Latin America : States, Threats, and Alliances. Albany : State University of New York Press, 2023. https://doi.org/10.1515/9781438491424

Urbanovics A. Cybersecurity Policy-Related Developments in Latin America // Academic and Applied Research in Military and Public Management Science. 2022. Vol. 21, no. 1. P. 79–94. https://doi.org/10.32565/aarms.2022.1.6; EDN: JOBKFG

Vila Seoane M. F. Chinese and U.S. AI and Cloud Multinational Corporations in Latin America // Towards an International Political Economy of Artificial Intelligence / ed. by T. Keskin, R. D. Kiggins. Cham, Switzerland : Palgrave Macmillan, 2021. P. 85–111. https://doi.org/10.1007/978-3-030-74420-5_5

Сведения об авторах:

Тимощеня Вячеслав Андреевич — аспирант кафедры теории и истории международных отношений, Российский университет дружбы народов; 117198, Российская Федерация, г. Москва, ул. Миклухо-Маклая, д. 10, к. 2; ORCID: 0000-0002-0961-2244; e-mail: v.timoshchenya@gmail.com

Мартыненко Евгений Владимирович — кандидат юридических наук, доцент кафедры теории и истории международных отношений, Российский университет дружбы народов; 117198, Российская Федерация, г. Москва, ул. Миклухо-Маклая, д. 10, к. 2; eLibrary SPIN-код: 7588-8419; ORCID: 0000-0003-4285-9959; e-mail: martynenko-evl@rudn.ru