Секция «Современные вызовы и угрозы международной безопасности»

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

Научный руководитель – Мартыненко Евгений Владимирович

Тимощеня Вячеслав Андреевич
Аспирант
Российский университет дружбы народов, Факультет гуманитарных и социальных наук, Москва, Россия
E-mail: v.timoshchenya@gmail.com

Латинская Америка, регион с богатой историей многостороннего сотрудничества в сфере традиционной безопасности, демонстрирует парадоксальную уязвимость в цифровой сфере. Несмотря на рост кибератак на 25% ежегодно [3], средний показатель кибербезопасности региона составляет 35,12 пункта по Глобальному индексу 2024 года — ниже африканского уровня [8]. Технологическая отсталость, фрагментация стратегий и зависимость от иностранных решений формируют *«идеальный шторм»* для криминальных групп. Проведенный контент-анализ 18 национальных стратегий и данных международных организаций позволяет выделить три ключевых направления для преодоления кризиса: модернизация инфраструктуры, преодоление кадрового дефицита и баланс геополитических интересов.

Цифровая инфраструктура Латинской Америки остается периферийной в глобальных цепочках создания стоимости. Лишь 62% населения имеют доступ к фиксированному широкополосному интернету, а мобильный ШПД охватывает 78%. Для сравнения: в Европе эти показатели достигают 90% и 105% соответственно. Нехватка точек обмена трафиком (*IXP*) и дата-центров увеличивает зависимость от международных каналов, повышая стоимость передачи данных и задержки [9]. Например, 70% *4G*-сетей региона построены на оборудовании Huawei, что создает риски монополизации и внешнего влияния [10]. Реактивный характер мер иллюстрирует Коста-Рика: после масштабных атак 2022 года финансирование кибербезопасности выросло на 446%, но подобные действия не заменяют системной модернизации.

Дефицит квалифицированных специалистов превышает 520 тыс. человек, что усугубляется низким уровнем цифровой грамотности [7]. Только 23% организаций используют ИИ для защиты данных — на 17% ниже глобального уровня. Программы вроде *Huawei ICT Academy* (36 тыс. выпускников) или инициатив Межамериканского банка развития (*Red Ciberlac*) не компенсируют дисбаланс [5]. Подготовка кадров фокусируется на базовых навыках, игнорируя потребности в экспертах по квантовой криптографии или анализу больших данных. Уругвай, внедряющий квантовые технологии, и Чили, создающий специализированные агентства, демонстрируют редкие исключения. Однако без синхронизации образовательных стандартов на региональном уровне усилия остаются фрагментарными.

Цифровая экосистема Латинской Америки стала ареной конкуренции глобальных игроков. Китай доминирует в телекоммуникациях (*Huawei, ZTE*), США — в облачных решениях (*Microsoft, AWS*), а ЕС продвигает нормативные стандарты (*GDPR*). Венесуэла и Куба, развивая «цифровой суверенитет», полагаются на российские и китайские технологии, тогда как Колумбия и Чили интегрируются в западные альянсы. Такая многовекторность повышает риски: Эквадор, получив кредит в 3,5 млрд долл. от США, отказался от китайского 5G-оборудования, что замедлило развитие инфраструктуры [2]. Региону необходим гибридный подход, сочетающий импорт технологий с локализацией критических систем.

Организация американских государств (ОАГ) играет ключевую роль через *CSIRT Americas* — сеть из 47 центров реагирования. Однако их эффективность ограничена неравномерным финансированием и слабым обменом данными. Программы вроде Цифровой повестки МЕРКОСУР или Плана действий КАРИКОМ остаются рекомендательными, а присоединение к Будапештской конвенции охватило лишь 9 стран. Успешные кейсы, такие как синхронизация стандартов в Бразилии или создание киберкоманд в Доминиканской Республике, требуют масштабирования. Критически важно усилить государственно-частное партнерство: только 12% проектов в области кибербезопасности получают поддержку бизнеса [1].

Преодоление кризиса невозможно без синтеза международного опыта и локальных приоритетов. Целевые инвестиции в оптоволоконные сети, как в Панаме [6], подготовка кадров через программы *NICE* ОАГ и гармонизация законодательства могли бы снизить зависимость от внешних игроков. Пример Коста-Рики показывает, что даже реактивные меры при достаточном финансировании дают результат [4]. Однако устойчивость системы зависит от перехода к превентивным стратегиям, учитывающим цифровой разрыв между столицами и сельскими регионами. Латинской Америке нужна не изоляция, а многоуровневое сотрудничество, где технологический суверенитет станет инструментом, а не барьером.

Источники и литература

1) Borrastero C., Juncos I. El Oligopolio Tecnológico Global, la periferia digital y América Latina //Desarrollo Económico. Revista de Ciencias Sociales. 2024. Vol. 64. №. 243. P. 110-136.
2) Cedeño P. R. F., Paz C. R. L. Government Management of Information Technology in the Latin American Context //Salud, Ciencia y Tecnologia-Serie de Conferencias. 2024. №. 3. P. 682-693.
3) Cybersecurity Economics for Emerging Markets. The World Bank, 2025. URL: https://openknowledge.worldbank.org/bitstreams/692c6149-748f-40dc-b9e6-8e09ba3e47bf/download (accessed: 02.01.2025).
4) 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. №. 1. P. 56-67.
5) 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/a978ff0a-06bf-42ad-84d4-388c8ccecef4/content (accessed: 02.01.2025).
6) Grassi J. M., Pinto D. J. A., de Conti Pagliari G. Cooperação em segurança e defesa cibernética e a proteção das democracias sul-americanas //Relações Internacionais (R: I). 2024. №. 82. P. 11-27.
7) 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, Noviembre 2024 // The World Bank URL: https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe (accessed: 02.01.2025).
8) Global Cybersecurity Index 2024. International Telecommunication Union, 2024. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed: 02.01.2025).

9) Internet Access Services: Status as of December 31, 2022. Federal Communications Commission, 2023. URL: https://www.fcc.gov/reports-research/reports/internet-access-services-reports/internet-access-services-status-december-31-2022 (accessed: 02.01.2025).

10) The State of Mobile Internet Connectivity Report. GSMA, 2023. URL: https://www.gsma.com/r/wp-content/uploads/2023/10/The-State-of-Mobile-Internet-Connectivity-Report-2023.pdf (accessed: 02.01.2025).

Иллюстрации

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, МБР	СР
Доминикана	2021-2024	Военные уязвимости	Центр операций	Э, С, О	ИИ системы	США, ЕС	В
Колумбия	2023-2026	Цифровой разрыв	Соц. 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
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	МБР, МЕРКОСУР	СР
Перу	2021-2026	Слабая защита	Центр безопасности	Э, Т, З	Аналитика	МБР, ООН	Н
Эль-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	МБР, 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

Источник: составлено автором на основании доктринальных стратегий государств Латинской Америки.

Примечание: 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-коммуникационная инфраструктура.

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

Рис. : Контент-анализ стратегий кибербезопасности государств Латинской Америки