

Л.Н.Симонова, Е.А.Пономарев

Цифровой суверенитет, вызовы и риски цифровизации в Латинской Америке

Статья посвящена проблеме цифрового суверенитета в странах Латинско-Карибской Америки (ЛКА). Монополизация глобальной индустрии информационных технологий (ИТ) привела к резкому росту технологической зависимости менее развитых в цифровом отношении государств от более развитых. Массовое распространение социальных сетей и цифровых платформ усилило риски вмешательства внешних акторов в социально-политические и экономические процессы развивающихся стран. Государства ЛКА, активно включившиеся в цифровую трансформацию, сильно зависят от внешних поставщиков оборудования и программного обеспечения, при этом технологический потенциал и квалифицированные кадры из латиноамериканских стран активно используются в интересах североамериканских технологических гигантов (*Big Tech*). Зависимость от них и уязвимость в плане цифровой безопасности подталкивают государства ЛКА к принятию мер по развитию национальных компетенций в передовых технологиях, решению задач по обеспечению цифрового суверенитета в критически важных отраслях экономики, созданию благоприятной среды для ведения бизнеса в цифровой сфере, совершенствованию законодательного регулирования.

Ключевые слова: цифровой суверенитет, цифровая безопасность, *Big Tech*, стратегия цифровой трансформации, информационные технологии, цифровые платформы, ИТ-рынок, программное обеспечение, аутсорсинг цифровых услуг.

DOI: 10.31857/S0044748X0028265-0

Статья поступила в редакцию 30.04.2023.

В условиях интенсивных цифровых технологических трансформаций, происходящих в мире, крайне актуальной исследовательской задачей является изучение содержания и особенностей феномена цифрового суверени-

Людмила Николаевна Симонова — кандидат экономических наук, руководитель Центра экономических исследований Института Латинской Америки РАН (РФ, 115035 Москва, Б. Ордынка, 21, ludmila-simonova@yandex.ru, <https://orcid.org/0000-0003-1144-2392>); Евгений Алексеевич Пономарев — научный сотрудник Центра экономических исследований Института Латинской Америки РАН (РФ, 115035 Москва, Б. Ордынка, 21, e.samgreen2015@gmail.com, <https://orcid.org/0000-0002-8785-0096>).

тета государства. Цифровизация ключевых сфер жизнедеятельности порождает новые вызовы и угрозы в отношении обеспечения государственного суверенитета. Само понятие цифрового суверенитета на сегодняшний день до конца не определено. Его можно сформулировать как достаточный уровень контроля государства за цепочками производства высокотехнологичной продукции на своей территории — от программного обеспечения (ПО) до технических средств.

Доминирование на мировом IT-рынке нескольких технологических гигантов, которые имеют возможность распространить свои цифровые решения, платформы и инструменты, технические средства и оборудование на большое количество внешних рынков, привело к монополизации глобальной индустрии информационных технологий и резкому росту технологической зависимости менее развитых в цифровом отношении государств от более развитых. Большая пятерка североамериканских технологических корпораций (*Big Tech*) — *Alphabet (Google)*, *Amazon*, *Apple*, *Meta (Facebook)* и *Microsoft* — являются доминирующими игроками в соответствующих областях технологий: искусственный интеллект (ИИ); электронная коммерция; онлайн-реклама; бытовая электроника; облачные вычисления; компьютерное программное обеспечение; потоковое вещание; «умный дом»; самоуправляемые автомобили; социальные сети. Предлагая услуги миллионам пользователей, эти корпорации способны влиять на поведение людей и контролировать большие объемы пользовательских данных.

В последние годы все больше ученых и футурологов предупреждают о риске потери части суверенитета для тех стран, которые целиком полагаются на импортные технологические решения. Способы, с помощью которых в настоящее время функционируют онлайн-платформы, подвергаются критике за усиление поляризации, радикализацию пользователей и поощрение участия в дезинформации и экстремистском контенте.

Такие явления, как хакерские атаки, шпионаж с использованием средств связи, утечки информации и прослушки, побуждают государства с соответствующими экономическими возможностями к производству собственной высокотехнологичной продукции, включая ИИ, нейросети, мобильные средства, чтобы снизить риски внешнего вмешательства в экономические процессы или разведывательной деятельности иностранных государств. Использование отечественных средств вычислений и передачи данных критически важно в энергетике, банковской сфере и госуправлении. Это позволяет обеспечить цифровой суверенитет за счет ограничения внешнего влияния на действия государства через высокотехнологичные средства.

Цифровые технологии, включая проблемы кибербезопасности, стали объектом исследований Экономической комиссии ООН для Латинской Америки и Карибского бассейна (ЭКЛАК) и других региональных организаций с начала XXI в. В исследовании ЭКЛАК «Цифровые технологии для нового будущего» подчеркивается, что в стратегии цифрового развития важную роль должно сыграть регулирование, направленное на предотвращение процессов монополизации рынков и на защиту конкуренции. Необходимо уменьшить влияние механизмов конкуренции, действующих в пользу технологических гигантов, и в то же время не препятствовать развитию национальных и региональных компаний. При этом рекомендуется

применять различные модели регулирования в отношении таких платформ, как доступ к общей информации через поисковые системы, доступ к персональным данным, к товарам и услугам, к финансовым ресурсам, к кадровому составу, системам платежей и кибервалютам [1, pp. 79-81].

В докладе Андской корпорации развития (*Corporación Andina de Fomento, CAF*) «Опыт: данные и искусственный интеллект в государственном секторе» анализируется применение ИИ в государственном управлении в странах ЛКА. Наряду с положительными результатами использования ИИ, повышением эффективности госуправления и предоставления услуг населению, эксперты отмечают риски, которые не ограничиваются усугублением киберугроз, но также включают в себя злоупотребления, которые усиливают дискриминацию и неравенство, причиняя вред различным социальным группам. Более того, без адекватного контроля и прозрачности в ходе использования этих инструментов могут усиливаться такие тенденции, как распространение ложных (фейковых) новостей или на еще более высоких уровнях — дипфейков (*deepfake*) или фальсифицированных фактов и аргументов с видимостью реальности [2, p. 4].

Вопросы цифровой трансформации и кибербезопасности в Латинской Америке нашли отражение в ряде статей исследователей, опубликованных в 2020—2023 гг. В них даются оценки уровня цифровизации и перспектив внедрения технологий цифровой экономики в странах ЛКА [3; 4; 5], анализируются законодательные акты, раскрывающие усилия стран региона в сфере цифровизации, а также государственные стратегии цифровизации [6; 7]. В фокусе исследований авторов — такие важнейшие аспекты цифровизации, как проблема кибербезопасности и угрозы дестабилизации политической и экономической жизни региона в результате вредоносного использования ИИ [8-13]. Вместе с тем в отечественной литературе практически отсутствуют публикации, посвященные вопросам цифровой безопасности, которые определяют возможности и перспективы адаптации государств региона к глобальным сдвигам в технологической парадигме. Цели данной статьи — выявить риски и проблемы процесса цифровизации в странах ЛКА, наметив пути обеспечения цифрового суверенитета и восполнив существующий пробел в исследовании этого вопроса в литературе. Главными методами исследования являются содержательный и контент-анализ, кросстемпоральное и кроссрегиональное сравнение. При проведении анализа ИТ-рынка и определении уровня зависимости стран ЛКА от импорта зарубежных технологий использовались открытые базы данных Конференции ООН по торговле и развитию (ЮНКТАД), Межамериканского банка развития, немецкой компании *Statista*, специализирующейся на рыночных и потребительских данных, оценки национальных ассоциаций разработчиков ПО, Европейского центра цифровой конкурентоспособности и иных международных организаций.

ПОЗИЦИИ ЕВРОСОЮЗА, США И КИТАЯ

Высокий уровень концентрации в сфере информационно-коммуникационных технологий (ИКТ) и ослабление конкуренции требуют разработки норм антимонопольного регулирования и стратегии ведения переговоров с

крупными технологическими компаниями и платформами по вопросу о доступе к данным, о защите персональных данных, об интеллектуальной собственности. Весной 2016 г. Европа решительно выступила в защиту конфиденциальности пользователей в Интернете, укрепив свой и без того надежный набор законов принятием Общих правил защиты данных. Документ признан самым жестким и всеобъемлющим законом о конфиденциальности в области цифровых технологий и основан на культурной приверженности защите права отдельных лиц контролировать доступ к своей личной информации [14].

Обеспокоенность зависимостью цифровой сферы от внешних поставщиков и разработчиков с новой силой прозвучала в Европе в 2020 г., когда президент Франции Эммануэль Макрон (2017 — н/в) заявил, что самостоятельность Европы зависит от ее экономической и цифровой суверенности [15]. В том же году правительство Германии в ее программе председательства в Совете Евросоюза заявило о желании сделать концепцию цифрового суверенитета лейтмотивом европейской политики в цифровой сфере. Среди ключевых задач в первую очередь были названы работы над ИИ и квантовыми технологиями [16, р. 8]. В 2021 г. в аналогичном документе, принятом в рамках председательства в совете, Словения подчеркнула свою приверженность задаче достижения цифрового суверенитета [17, р. 28]. В 2022 г. идея цифрового суверенитета и стремление к его достижению были вновь упомянуты в программе председательства Франции в Совете ЕС [18, р. 53]. В более общем региональном контексте стоит выделить такой документ, как «Стратегический компас» (2022 г.), посвященный тематике безопасности Европы. В нем также отстаивается необходимость «уменьшения стратегической зависимости» и сохранения потенциала европейской интеллектуальной собственности [19, р. 35].

По ту сторону Атлантики США придерживаются другой концепции и культуры конфиденциальности. Американский режим конфиденциальности в основном направлен на защиту частных лиц от вмешательства государства, а компаний — от бюрократии. В то время, как некоторые компании хранят беспрецедентный объем личной информации о своих пользователях, в США отсутствует всеобъемлющий федеральный закон о конфиденциальности, регулирующий сбор и использование персональных данных технологическими корпорациями.

В США вопрос цифрового суверенитета чаще рассматривается с позиции противодействия растущей технологической конкуренции со стороны Китая. Позиция Вашингтона заключается в лоббировании деятельности технологических корпораций, которые, являясь крупными рыночными игроками, ответственны за технологическое развитие страны [20]. Политические круги США в целом руководствуются мнением, что государственное регулирование сверх обеспечения свободного рынка обременительно и препятствует технологическим инновациям [21]. С этим сложно поспорить, учитывая, что такие крупнейшие технологические компании, как *Apple*, *Amazon*, *Google*, *Microsoft*, *Meta* и другие, находятся в США и формируют значительную часть национального ВВП. Отсюда следует принцип невмешательства государства в их деятельность, более того, параллельно идет процесс сращения интересов технокорпораций и государства.

Для крупных игроков цифровой сферы — США, Китая и Европы — важными аспектами проблематики цифрового суверенитета являются вопросы собственного производства полупроводников и программного обеспечения (*software*) с открытым исходным кодом*. В Соединенных Штатах с августа 2022 г. действует Закон о микросхемах и науке, поощряющий национальное производство полупроводников. Европа также ставит задачу уменьшить зависимость от иностранных производителей полупроводников. В феврале 2022 г. председатель Европейской комиссии Урсула фон дер Ляйен представила Европейский закон о микросхемах, направленный на поддержку регионального производства полупроводников. Поставлена цель к 2030 г. увеличить долю ЕС в мировом производстве микросхем с 9% до 20% [23].

Китай обращает повышенное внимание на создание собственных репозиторий ПО с открытым кодом. Национальное правительство выдвинуло в 2020 г. китайский репозиторий *Gitee* в качестве альтернативы *GitHub*, которым владеет *Microsoft* [24]. Рост конкуренции следует ожидать и в сфере машинного обучения, разработки нейросетей и ИИ. На данный момент ведущими игроками в области сред глубокого обучения (*deep learning frameworks*) с открытым кодом, нацеленных на развитие нейронных сетей и ИИ, остаются *TensorFlow* от *Google* и *PyTorch* от *Meta*. Китай тем временем продвигает свои альтернативы, такие, как *PaddlePaddle* от *Baidu* и *MindSpore* от *Huawei* [21].

ПРОБЛЕМА ЦИФРОВОГО СУВЕРЕНИТЕТА В ЛАТИНСКОЙ АМЕРИКЕ

Проблема технологического суверенитета особенно остро стоит перед развивающимися странами, которые (включая страны ЛКА) не обладают достаточной производственной базой, кадровым потенциалом и в целом экономическими возможностями, чтобы вести собственные разработки ПО и современной техники. О высокой степени зависимости стран ЛКА от импорта компьютеров, периферийного оборудования и бытовой электроники свидетельствуют данные *UNCTADStat*, приведенные в таблице 1. В 2021 г. страны ЛКА импортировали ИКТ-товаров на сумму 134 млрд долл., главным образом из Китая (50,3%) и США (14,6%); при этом региональный экспорт составил всего 72,7 млрд долл.

Массовые протесты последних лет в Латинской Америке продемонстрировали проблему угрозы манипуляций настроениями граждан через основные социальные сети и мессенджеры. Все чаще можно встретить исследования «цифрового следа» массовых событий, в которых коммуникация посредством цифровых платформ может служить как триггером, так и усилителем определенной повестки. Наряду с североамериканскими социальными сетями, получившими широкое распространение в странах региона, в последние годы стремительно растет популярность китайских платформ, в частности *TikTok*. Учитывая, что латиноамериканцы традиционно

* Открытый исходный код — это децентрализованная модель разработки, которая позволяет любому человеку изменять технологию и обмениваться ею, поскольку ее структура находится в открытом доступе [22].

сильно зависят от электронных видов коммуникации, риск внешних манипуляций общественными настроениями становится фактором внутривнутриполитической нестабильности.

Т а б л и ц а 1

**ВНЕШНЯЯ ТОРГОВЛЯ ИКТ-ТОВАРАМИ СТРАН ЛКА
В 2021 г. (в млн долл.)**

Страна	Экспорт	Импорт	Сальдо
ЛКА, всего	72702	133986	-61284
Мексика	71000	76924	-5924
Бразилия	730	21078	-20348
Доминиканская Республика	278	1218	-940
Чили	259	8277	-8018
Колумбия	120	5875	-5755
Коста-Рика	119	1310	-1191
Гватемала	42	1652	-1610
Перу	36	4490	-4454
Сальвадор	24	983	-959
Аргентина	22	5742	-5720

Источник: составлено по [25].

Угроза потери контроля над средствами коммуникации и формулирования общественной повестки дополняется новыми растущими рисками передачи данных об экономической деятельности или даже контроля над ней внешним актором. Большинство промышленных предприятий в Латинской Америке изначально ориентировались на использование программных и аппаратных решений по автоматизации процессов американского или европейского происхождения. При этом «точечное» применение цифровых решений в промышленности не позволяет условному внешнему «контролеру» получить контроль над данными обо всех хозяйственных связях в конкретной стране/компании. Более серьезную угрозу суверенитету представляет формирование экономической деятельности на базе логистических платформ, большинство из которых разработаны в США и Китае.

Китай активно продвигает проект «Электронного Шелкового пути» как дополнение к масштабному одноименному инфраструктурному мегапроекту. Компонентами предлагаемых решений являются системы управления мультимодальными логистическими цепочками (например, *Logink*), позволяющие производителям, транспортным компаниям, перевозчикам и потребителям взаимодействовать в электронном формате. Помимо значительного экономического эффекта от внедрения таких систем управления, заключающегося в повышении скорости взаимодействия участников рынка и снижении транзакционных издержек, появляется и риск передачи данных об экономических взаимосвязях в национальной экономике внешнему оператору системы. При гипотетическом сценарии кибервойны против кон-

кретного государства отключение подобных систем управления хозяйством может привести к катастрофическим последствиям [3, р. 28].

Опасность кибератак и угроза развязывания кибервойн заставляют многие крупные страны ЛКА принимать меры по обеспечению цифрового суверенитета. Решить эту задачу возможно несколькими основными способами. Крупные государства, обладающие достаточной технологической базой и кадрами, стремятся самостоятельно разрабатывать критические элементы цифровой инфраструктуры для полного контроля над их управлением. Второй подход, по мнению российских ученых Д.В.Разумовского и Ю.Н.Мосейкина, заключается в переходе от практики покупки преимущественно готовых программных решений у ведущих поставщиков к совместной разработке решений с участием зарубежных партнеров. Этот вариант требует от иностранных разработчиков готовности делиться технологиями, передавая заказчику не традиционную лицензию, а, по сути, открытый код с возможностью его дальнейшей самостоятельной доработки. Латиноамериканская сторона, обучаясь в процессе совместного взаимодействия, приобретает необходимые ей компетенции, но главное — получает контроль над системой, исключая риск внешнего вмешательства в управление цифровой системой [3, р. 30].

По мнению экспертов ЭКЛАК, одним из методов регулирования цифрового рынка и поддержки национальных разработчиков программного обеспечения (ПО) является налогообложение технологических гигантов, которое применяется во многих странах мира и представляет собой источник финансовых средств для государственных бюджетов. Поскольку прямое налогообложение иностранных компаний зачастую затруднительно, так как они предоставляют свои услуги из-за границы, большинство стран используют косвенные налоги, прежде всего, налог на добавленную стоимость цифровых услуг. В мире этот налог применяют 77 стран, в том числе 12 латиноамериканских. В настоящее время эти налоги действуют в одностороннем порядке, но расширение позиций иностранных технологических компаний ставит задачу по активизации усилий и выработке многосторонних соглашений о налогообложении иностранных компаний, предоставляющих цифровые услуги [1, pp. 79-81].

Вопросы национального цифрового суверенитета постепенно включаются в официальные документы стран латиноамериканского региона. Так, в сентябре 2021 г. в Мексике была опубликована Национальная цифровая стратегия на 2021—2024 гг., в которой упомянут «принцип технологического суверенитета» [26]. Он определен как исключительное право страны определять политику и стратегии в цифровой и технологической сфере, исключая внешнее вмешательство. Документ также включает в себя два других понятия: технологическая независимость, подразумевающая отказ от следования условиям поставщиков и разработчиков технологий, выдвинутому в одностороннем порядке, и технологическая автономия, определяемая как способность предлагать собственные решения и использовать собственные кадры в технологической сфере.

Мексика является основным поставщиком ИКТ-продукции на внешние рынки из стран ЛКА. В 2021 г. на ее долю пришлось почти 98% латиноамериканского экспорта компьютеров, коммуникационного оборудования

и бытовой электроники на общую сумму 71 млрд долл.; импорт достиг 77 млрд долл., из которых 37% составили электронные компоненты [25].

В Бразилии в последние несколько лет принято несколько важнейших национальных программ, нацеленных не просто на достижение самостоятельности, но и лидерства в перспективных технологиях. Главным политическим документом, регулирующим и координирующим государственные инициативы в области цифровых технологий, является Бразильская стратегия цифровой трансформации 2018 г., предусматривающая использование потенциала цифровых технологий для содействия устойчивому и инклюзивному росту и повышения конкурентоспособности, производительности и занятости [15]. Выделены три основных плана действий в секторе ИКТ: интернет вещей (*Internet of Things, IoT*), искусственный интеллект, кибербезопасность. Национальный план интернета вещей, известный как *IoT.Br*, охватывает четыре главных направления: промышленность, здравоохранение, умные города и сельское хозяйство [28].

В стране несколько лет действует Национальная стратегия в области искусственного интеллекта, в которой определены шесть целей: разработка этических принципов и ответственное использование ИИ; устранение барьеров для инноваций; улучшение сотрудничества между правительством, частным сектором и исследователями; развитие навыков в области ИИ; содействие инвестициям в технологии; продвижение бразильских технологий за рубежом [29]. Ведется работа по созданию Национальной инновационной сети ИИ при участии министерства науки, технологий и инноваций (*Ministério da Ciência, Tecnologia e Inovações, MCTI*) и Бразильской компании промышленных исследований и инноваций (*Empresa Brasileira de Pesquisa e Inovação Industrial, EMBRAPPI*). Сеть исследовательских центров призвана поддерживать стартапы и поощрять разработку продуктов и услуг на основе ИИ [30]. В принятой в 2020 г. Национальной стратегии кибербезопасности (*E-Ciber*) особое внимание уделено подготовке ИТ-специалистов, развитию НИОКР и внедрению национальных решений в сфере безопасности с соблюдением международных стандартов при разработке новых продуктов [31].

Бразилия — первый в Латинской Америке пример страны, применяющей комплексный подход к развитию национальных компетенций в передовых технологиях. Вместе с тем даже для технологически продвинутой Бразилии задача по обеспечению цифрового суверенитета в критически важных отраслях экономики представляется весьма сложной, учитывая существенную зависимость страны от поставок импортного оборудования и ПО. По данным *UNCTADStat*, с 2010 по 2021 г. ИКТ-экспорт из Бразилии сократился в 2,8 раза и составил всего 730 млн долл. В этот же период импорт увеличился на 17% — до 21,1 млрд долл. [25].

Бразилия является лидером среди стран ЛКА по размеру рынка ПО и цифровых услуг — 19,2 млрд долл. В 2021 г. по данному показателю страна заняла 12-ю позицию в мировом рейтинге с долей в 1,3%. Несмотря на определенные успехи в разработке цифровых продуктов в госуправлении, сфере безопасности и обороны, а также в финансовом секторе, телекоммуникациях и торговле, основной объем бразильского рынка ПО, оцениваемого в 11,25 млрд долл., приходится на зарубежные цифровые решения. По данным Бразильской ассоциации компаний — разработчиков программно-

го обеспечения (*Associação Brasileira das Empresas de Software, ABES*), в 2021 г. сегмент локального производства обеспечил около 26% объема рынка, при этом он рос существенно более высокими темпами по сравнению с инвестициями в зарубежные ПО (на 48,1% против 9,5%) [32, pp. 8-9].

В последние годы в Бразилии растет число компаний, предоставляющих ИТ-услуги. В 2021 г. в стране насчитывалось около 7600 компаний по разработке и производству ПО и более 9300 фирм, занимающихся его распространением и маркетингом. Самой известной бразильской компанией — разработчиком «софта» является *TOTVS* (основана в Сан-Паулу в 1983 г.), ее офисы открыты в США, Португалии и других странах Латинской Америки. В 2021 г. на бразильском рынке программного обеспечения были заняты около 133 тыс. человек, в основном в Сан-Паулу. Тем не менее прогнозы показывают, что ИТ-индустрия в ближайшие годы будет нуждаться в новых талантах: к 2025 г. потребуется около 150 тыс. специалистов [33].

Наличие технологической базы, квалифицированных кадров и благоприятной бизнес-среды способствовали превращению Бразилии в крупнейший в регионе рынок аутсорсинга ИТ-услуг*. Такие глобальные игроки, как *Amazon, Dell, Google* и *Meta*, передают проекты в области пользовательского ПО, обслуживания электронной коммерции, телекоммуникаций, финансов и интернета вещей на аутсорсинг бразильским компаниям. Бразилия лидирует в Латинской Америке по экспорту компьютерных услуг, объем которого в 2021 г. достиг 2,7 млрд долл. (см. таблицу 2). При этом экспорт собственно бразильских разработок ПО и цифровых услуг, по данным *ABES*, составил 675 млн долл., т.е. четверть общей суммы [32, p. 9].

Т а б л и ц а 2

ЭКСПОРТ КОМПЬЮТЕРНЫХ УСЛУГ СТРАН ЛКА (в млн долл.)

Страна	2014 г.	2015 г.	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.	2021 г.
ЛКА, всего	4120	4682	5213	6736	7220	7339	7511	9314
Бразилия	947	1094	1316	1726	1972	1994	2072	2707
Аргентина	1214	1328	1459	2020	2052	1886	1789	2000
Коста-Рика	783	928	994	1076	1037	1123	1220	1346
Уругвай	163	283	213	551	592	733	779	1087
Чили	245	239	283	285	350	356	388	493
Колумбия	285	254	271	299	331	341	398	462
Другие страны ЛКА	482	556	676	778	887	905	865	1218

Примечание: ИТ-услуги включают в себя услуги, связанные с аппаратным и программным обеспечением, а также услуги по обработке данных.

Источник: составлено по [34].

* По определению ЮНКТАД, цифровая экономика — это применение цифровых интернет-технологий в производстве товаров и услуг [35, p. 156].

В последние годы в Бразилии все громче звучат «голоса», призывающие к постановке вопроса цифрового суверенитета на национальном уровне. Накануне президентских выборов 2022 г. группа общественных деятелей (в основном левых политических взглядов), представителей неправительственных организаций и научно-образовательных кругов направили баллотировавшемуся в президенты Луису Инасиу Луле да Силве (2003—2011 гг.; 2023 — н/в) открытое письмо, подняв в нем тему цифрового суверенитета.

Для достижения независимости от международного капитала в технологической сфере составители письма предлагали создать бразильскую инфраструктуру для хранения и обработки данных университетов, исследовательских институтов, неправительственных организаций и госорганов, работать над созданием ИИ для нужд государственного и частного секторов на национальной основе, создать специальные исследовательские отделы при министерстве науки, технологий и инноваций для научных исследований на благо стратегических секторов.

Среди важнейших направлений обеспечения цифрового суверенитета выделены следующие: подготовка кадров, в том числе в рамках программ министерства образования, для «ликвидации зависимости от крупных ТНК»; финансовая поддержка национальных разработчиков цифровых платформ для сферы услуг; интенсификация исследований, разработки и подготовки кадров для поиска решений по автоматизации, робототехнике, квантовым вычислениям, внедрению чипов, высокоскоростных коммуникационных сетей и проч.; поддержка разработки и использование ПО с открытым исходным кодом для распространения и совершенствования технологических решений; возврат в собственность государства компании *Telebras* [36]. Хотя данные предложения подверглись критике, касающейся их практической реализации, важен сам факт подобных настроений определенной части интеллектуального общества страны. Несмотря на то, что президент не дал прямого ответа на вышеупомянутое письмо, в январе 2023 г. была принята Национальная политика цифрового образования, где среди прочих задач в общих чертах предписывалась реализация в Бразилии телекоммуникационных и информационных исследований [37].

Стремление Бразилии к цифровой «независимости» укладывается в общее с другими участниками альянса *BRICS* (*Brazil, Russia, India, China, South Africa*) видение технологической картины мира. На саммите *BRICS* в 2019 г., проходившем в г. Бразилиа, ключевыми были вопросы цифровой экономики, цифровой безопасности, сотрудничества в области науки, инновационного и технологического развития. Из заявлений представителей стран — членов *BRICS* можно понять, что цифровизация воспринимается ими как новое поле для сотрудничества [38, pp. 284-285].

Вместе с тем от государств, входящих в *BRICS*, следует ожидать более частых апелляций к цифровому суверенитету как к концепции, являющейся опорой для обеспечения классического национального суверенитета, что в 2020-х годах становится особенно актуальным в контексте геополитических обстоятельств. Ярким примером практического воплощения в жизнь некоторых аспектов идеи цифрового суверенитета среди членов *BRICS* является так называемый Закон о «суверенном Интернете», принятый в России в 2019 г. В

ноябре 2022 г. в России началась разработка собственного репозитория открытого кода, завершение которой планируется к 2024 г. [39].

Согласно отчету Европейского центра цифровой конкурентоспособности, в котором содержится информация о странах, где цифровая экономика развивается наиболее динамично, существенный прогресс в 2021 г. (помимо Бразилии) отмечался в Аргентине, Уругвае, Колумбии, Доминиканской Республике, Парагвае и Чили [40, pp. 22-23]. В большинстве перечисленных стран, а также в Коста-Рике развитие цифровых услуг, включая разработку и экспорт ПО, в значительной степени определялось заинтересованностью североамериканских *Big Tech* в использовании технологического потенциала и квалифицированных ИТ-специалистов ЛКА.

Аргентина в последние годы нарастила объемы экспорта программного обеспечения. В 2021 г. экспорт ПО составил 2,1 млрд долл.; ожидается, что в 2026 г. этот показатель достигнет отметки в 2,5 млрд долл. В настоящее время в стране осуществляется Программа укрепления цифровой повестки: взаимосвязанность, электронное правительство и цифровая трансформация производства (*Programa para el Fortalecimiento de la Agenda Digital: Conectividad, Gobierno Electrónico y Transformación Productiva Digital*). В 2019 г. Межамериканский банк развития предоставил Аргентине кредит на сумму 300 млн долл. в качестве помощи для реализации программы [41]. Страна занимает 34-е место в мировом рейтинге образования, имеет хорошо развитую индустрию разработки программного обеспечения и прочную репутацию производителя высококачественных профессионалов в области ПО и инженерии. Успешно развиваются технологические стартапы, имеются всемирно признанные технологические компании, включая *Mercado Libre* и *Despegar*, создавшие центры разработки ПО не только в Аргентине, но и других странах ЛКА. Существует также ряд бизнес-инкубаторов и акселераторов, предоставляющих ресурсы и поддержку предпринимателям. Так, *Aceleradoras BA Emprende*, инициатива Буэнос-Айреса, которая софинансирует высокоэффективные предприятия для стимулирования роста, инвестировала более 3,5 млн долл. в местные компании [42].

Аргентинская компания интернет-коммерции *Mercado Libre*, основанная в 1999 г., является крупнейшей электронной торговой площадкой в ЛКА. В 2022 г. ее выручка превысила 10 млрд долл., операционная прибыль — 1 млрд долл. [43]. В 2017 г. *Mercado Libre* заняла 71-е место в рейтинге наиболее быстро растущих инновационных компаний мира (*Innovative Growth Companies*) по версии *Forbes* [44]. Платформа также предлагает услуги в области финансовых технологий (*fintech*) с возможностью проведения платежей, заимствования средств, вывода наличности и т.д. В 2020 г. через платформу было продано 719,3 млн товаров, в 2021 г. — 1,014 млрд [45]. *Mercado Libre* действует во всех странах Южной и Центральной Америки (кроме Гайаны и Суринама).

Уругвай является одним из крупнейших экспортеров программного обеспечения в латиноамериканском регионе. В стране работает более 1 тыс. компаний — разработчиков «софта», а объем экспорта ПО в 2021 г. впервые превысил 1 млрд долл., несмотря на относительный дефицит квалифицированных кадров. В расчете на душу населения Уругвай по данной статье экспорта зани-

мает первое место в Латинской Америке и выходит в мировые лидеры. На долю США приходится более 59% экспортной выручки ИТ-компаний Уругвая [46].

Правительство Уругвая считает цифровые технологии одной из сфер своих государственных интересов. В рамках господдержки развития цифровой индустрии были приняты Повестка Цифровой Уругвай [47] и Стратегия развития искусственного интеллекта цифрового правительства [48], призванные обеспечить безопасность процесса цифровой трансформации и ответственное использование цифровых технологий на национальном уровне. В стране организовано обучение специалистов по тестированию ПО. Программа не имеет аналогов в других странах, учитывая объем и совместные усилия государственного и частного секторов по ее поддержке. Обучение осуществляет некоммерческая лаборатория по тестированию ПО — Центр испытаний программного обеспечения при содействии государственного Республиканского университета и частной ассоциации «Палаты информационных технологий Уругвая» [49]. Уругвай активно позиционирует себя как страна, благоприятная для цифровых и другого рода инновационных стартапов. Об этом свидетельствует и запуск в 2019 г. Национальным агентством исследований и инноваций программы *Proyecta Uruguay* для повышения инвестиционной привлекательности страны. Тогда же Уругвай стал первым государством региона, где государственной компанией *Antel* была запущена коммерческая сеть связи 5G [50, p. 38].

Отдельного упоминания заслуживает и Коста-Рика, которая превратилась в регионального лидера по уровню развития отрасли информационных технологий. Ее рынок ПО и ИТ-услуг составляет 1,4% всей национальной промышленности, а на его долю приходится более 1,7% ВВП страны. Начиная с 2000 г. данный сектор экономики демонстрировал уверенный и постоянный рост. В стране работают около 2000 предприятий, деятельность которых связана с разработкой ПО, главным покупателем которого являются США. Индустрия разработки ПО в Коста-Рике поддерживается рядом университетов и научно-исследовательских институтов, а также бизнес-инкубаторами и акселераторами. Рабочая сила в Коста-Рике — высококвалифицированная; многие специалисты имеют ученую степень. Страна занимает пятое место в Латинской Америке в отчете *Coursera Global Skills Report* за 2022 г., в котором измеряется уровень владения бизнесом, технологиями и наукой о данных. Сильные национальные традиции предпринимательства и инноваций помогли создать множество успешных технологических стартапов. Коста-Рика имеет благоприятную для бизнеса среду, являясь «домом» для ряда транснациональных корпораций, создавших центры разработки программного обеспечения в Коста-Рике, включая *Intel*. По оценке Межамериканского банка развития, к 2025 г. страна станет одним из пяти важнейших мировых центров развития цифровой индустрии — своего рода «латиноамериканской Кремниевой долиной» [51].

Однако экспортный потенциал Коста-Рики в сфере компьютерных технологий в значительной степени зависит от иностранного капитала. Показателен случай *Intel* и с ее деятельностью в Коста-Рике. Завод *Intel* по производству и тестированию микропроцессоров был открыт в стране в 1997 г. В 2014 г. компания приняла решение о закрытии предприятия, что было связано с сокращением производства персональных компьютеров и

переориентацией на рынок мобильных устройств и приложений, а также с необходимостью снижения издержек за счет переноса производственных и бизнес-процессов в страны Азии и непосредственно в США. Тем не менее *Intel* вернулась в Коста-Рику в 2020 г., производство и тестирование микропроцессоров было возобновлено в 2021 г. [52]. Возвращение было обусловлено экономической обстановкой, сложившейся в период пандемии коронавируса, когда часть американских предприятий по сборке компонентов электроники в Малайзии, Вьетнаме, Китае и Тайване закрылась, а цепочки поставок были нарушены.

Временный уход *Intel* из Коста-Рики серьезно отразился на экспортных показателях страны: в 2006—2014 гг. экспорт электронных компонентов из Коста-Рики составлял 13,4 млрд долл., в 2015—2021 гг. — 400 млн долл., уменьшившись в 34 раза. При этом экспорт компьютеров и периферийного оборудования, достигавший в 2000—2010 гг. 10,6 млрд долл., в 2011—2021 гг. составил всего 153 млн долл., сократившись в 70 раз [25]. Помимо *Intel* такие технологические гиганты, как *IBM* и *HP*, оценивали перспективы производства в Коста-Рике, но ограничились открытием в стране центров обслуживания [53, р. 38].

НА ПУТИ К ЦИФРОВОЙ САМОСТОЯТЕЛЬНОСТИ

Применительно к развитию концепции цифрового суверенитета широкое присутствие иностранных ТНК на цифровых и технологических рынках государств региона является фактором, способным улучшить макроэкономические показатели латиноамериканских стран и продемонстрировать их потенциал в производстве высокотехнологичной продукции. С другой стороны, растущая зависимость от технологических гигантов и уязвимость в плане цифровой безопасности подталкивают государства ЛКА к принятию мер по формированию собственной кадровой и технологической базы для развития национальных корпораций и компаний. В интересы стран региона входит становление Латинской Америки как самодостаточного центра инноваций и цифровизации, а не только как площадки для оптимизации бизнес-процессов зарубежных компаний.

Первостепенную роль на отмеченном выше направлении играют человеческие ресурсы — кадры, специализирующиеся в сфере ИТ. В 2022 г. в регионе насчитывалось около 1 млн разработчиков ПО, занятых в проектах для компаний из других стран [54]. Образовательные инициативы государств ЛКА в области цифровых технологий служат основой для формирования специализированных кадров. Немаловажное значение имеет и благоприятная обстановка для ведения бизнеса в цифровой сфере, которая может выражаться в таких показателях, как востребованность цифровых компетенций в различных секторах экономики, наличие специалистов, государственных и предпринимательских инициатив и совершенство законодательного регулирования. Привлекательность Латинской Америки для инвесторов отражается, в том числе, в высоких позициях ведущих стран региона в мировых рейтингах, оценивающих цифровой потенциал государств и готовность к цифровому переходу в экономике. Одним из таких рейтингов является *Kearney Global Services Location Index*, высоко оценивший в 2021 г. некоторые ведущие страны региона, такие, как Бразилия, Мексика, Колумбия и Чили, по степени их готовности к поддержанию экономической деятельности в цифровой среде [55].

Цифровая самостоятельность латиноамериканского региона будет определяться и его инновационным потенциалом, поддерживаемым развитием инфраструктуры венчурного финансирования и ростом количества технологических компаний. За последние пять лет в Латинской Америке появилось порядка 50 «компаний-единорогов»: 60% из них находятся в Бразилии, 17% — в Мексике, 11% — в Аргентине*. Кроме того, в регионе базируется около 100 стартапов, капитал которых оценивается в 100 млн долл. и более [56]. В целом же совокупная стоимость региональных технологичных стартапов в 2019—2021 гг. выросла с 38 млрд до 216 млрд долл. [57]. Самыми известными примерами стартапов в ЛКА являются бразильский цифровой банк *Nubank*, аргентинское мобильное приложение для финансового менеджмента *Uala*, мексиканская цифровая биржа криптовалют *Bitso* и уругвайская платежная система *dLocal*.

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

1. CEPAL. Digital technologies for a new future. Santiago, 2021, 94 p. Available at: https://repositorio.cepal.org/bitstream/handle/11362/46817/1/S2000960_en.pdf (accessed 30.08.2022).
2. CAF. Experiencia: Datos e Inteligencia Artificial en el sector publico. Caracas, 2021, 530 p. Available at: <https://scioteca.caf.com/handle/123456789/1793> (accessed 30.08.2022).
3. Razumovskiy Dmitriy V., Moseykin Yuri N. Digitalización en América Latina y oportunidades para empresas rusas. *Iberoamerica*, Moscow, 2022, N 1, pp. 5-37.
4. Яковлев П.П. Экономика Латинской Америки на старте цифровой модернизации. *МЭМО*. М., 2022, № 3, сс. 110–118. [Yakovlev P.P. Ekonomika Latinskoj Ameriki na starte cifrovoj modernizacii. [The Latin American economy at the start of digital modernization]. *MEiMO*. Moscow, 2022, N 3, pp. 110–118 (In Russ.).
5. Симонова Л.Н. Цифровая трансформация экономики Латинской Америки. *Латинская Америка*. М., 2022, №5, сс. 8-27. [Simonova L.N. Cifrovaya transformaciya ekonomiki Latinskoj Ameriki. [Digital transformation of the Latin American economy]. *Latinskaya Amerika*. Moscow, 2022, N 5, pp. 8-27 (In Russ.).
6. Смаль С.В. Государственная политика цифровизации в странах Латинской Америки. Опыт применения многомерных интегральных индексов на примере Бразилии. *Латинская Америка*. М., 2021, № 4, сс. 40-55. [Smal' S.V. Gosudarstvennaya politika cifrovizacii v stranah Latinskoj Ameriki. Opyt primeneniya mnogomernyh integral'nyh indeksov na primere Brazilii. [State policy of digitalization in Latin America. Experience in the application of multidimensional integral indices on the example of Brazil]. *Latinskaya Amerika*. Moscow, 2021, N 4, pp. 40-55 (In Russ.).
7. Лавут А.А. Роль ЭКЛА в разработке основ региональной стратегии цифровизации экономики. *Латинская Америка*. М., 2022, № 7, сс. 6-20. [Lavut A.A. Rol' EKLA v razrabotke osnov regional'noj strategii cifrovizacii ekonomiki. [The role of ECLA in developing the foundations of a regional strategy for digitalization of the economy]. *Latinskaya Amerika*. Moscow, 2022, N 7, pp. 6-20 (In Russ.).
8. Стадник И.Т., Цветкова Н.Л. Место и роль стран Латинской Америки в системе международной и региональной кибербезопасности. *Латинская Америка*. М., 2021, № 4, сс. 69-84. [Stadnik I.T., Cvetkova N.L. Mesto i rol' stran Latinskoj Ameriki v sisteme mezhdunarodnoj i regional'noj kiberbezopasnosti. [The place and role of Latin American countries in the system of international and regional cybersecurity]. *Latinskaya Amerika*. Moscow, 2021, N 4, pp. 69-84 (In Russ.).
9. Kosévich E. Yu. Estrategias de seguridad cibernética en los países de América Latina. *Iberoamerica*. Moscow, 2020, N 1, pp. 137-159.
10. Косевич Е.Ю. Защита киберпространства в странах Латинской Америки. *Политические исследования*. М., 2022, № 3, сс. 108-123. [Kosevich E.Yu. Zashchita kiberprostranstva v stranah Latinskoj Ameriki. [Protecting Cyberspace in Latin America]. *Polis. Politicheskie issledovaniya*. Moscow, 2022, N 3, pp. 108-123 (In Russ.).

* Частные компании-стартапы, оцениваемые в 1 млрд долл. и выше.

11. Виноградова Е.А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке. *Латинская Америка*. М., 2023, № 7, сс. 34-48. [Vinogradova E.A. Tekhnologii iskusstvennogo intellekta i narastayushchie kiberugrozy v Latinskoj Amerike. [Artificial Intelligence Technologies and Growing Cyber Threats in Latin America]. *Latinskaya Amerika*. Moscow, 2023, N 7, pp. 34-48 (In Russ.).]
12. Цветкова Н.А., Гришанина Т.А. Цифровая сила в странах Латинской Америки: хэштеги и дипфейки как политические инструменты. *Латинская Америка*. М., 2023, №3, сс. 21-33. [Cvetkova N.A., Grishanina T.A. Cifrovaya sila v stranah Latinskoj Ameriki: heshtegi i dipfejki kak politicheskie instrumenty. [Digital Power in Latin America: Hashtags and Deepfakes as Political Tools]. *Latinskaya Amerika*. Moscow, 2023, N 3, pp. 21-33 (In Russ.).]
13. Виноградова Е.А. Злонамеренное использование политических дипфейков и попытки их нейтрализации в странах Латинской Америки. *Латинская Америка*. М., 2023, №5, сс. 35-48. [Vinogradova E.A. Zlonamerennoe ispol'zovanie politicheskikh dipfejkov i popytki ih nejtralizacii v stranah Latinskoj Ameriki. [Malicious use of political deepfakes and attempts to neutralize them in Latin American countries]. *Latinskaya Amerika*. Moscow, 2023, N 5, pp. 35-48 (In Russ.).]
14. Hendrickson C., Galston W. Big tech threats: Making sense of the backlash against online platforms. Brookings Institution. Washington, 2019, 20 p.
15. Bosoer L. Digital Sovereignty: Voices from Latin America. European University Institute, Latin American Focus Group. October 26, 2022. Available at: <https://blogs.eui.eu/latin-american-working-group/digital-sovereignty-voices-from-latin-america/> (accessed 12.02.2023).
16. Together for Europe's recovery. Programme for Germany's Presidency of the Council of the European Union. Berlin, 2020, 27 p.
17. Council of the European Union. Programme of the Slovenian Presidency of the Council of the European Union. Brussels, 2021, 44 p. Available at: <https://www.gov.si/assets/vlada/Projekti/PSEU2021/The-programme-of-the-Slovenian-Presidency-of-the-Council-of-the-European-Union.pdf> (accessed 21.08.2022).
18. Council of the European Union. Recovery, Strength and a Sense of Belonging. Programme for the French Presidency of the Council of the European Union. Brussels, 2022, 76 p. Available at: https://wayback.archive-it.org/12090/20221120104852/https://presidence-francaise.consilium.europa.eu/media/qh4cg0qq/en_programme-pfue-v1-2.pdf (accessed 25.01.2023).
19. Council of the European Union. Strategic Compass for Security and Defence. Brussels, 2022, 47 p. Available at: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf> (accessed 25.01.2023).
20. Cath C., Wachter S., Mittelstadt B., Taddeo M., and Floridi L. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*. Volume 24, issue 2, April 2018, pp.505–528. Available at: <https://doi.org/10.1007/s11948-017-9901-7> (accessed 25.07.2022).
21. Larsen B. The geopolitics of AI and the rise of digital sovereignty. Report. The Brookings Institution, December 8, 2022.
22. What Is Open Source? Available at: https://aws.amazon.com/what-is/open-source/?nc1=h_ls (accessed 25.01.2023).
23. European Commission. Digital sovereignty: Commission proposes Chips Act to confront semiconductor shortages and strengthen Europe's technological leadership. Press release, February 8, 2022. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_729 (accessed 12.12.2022).
24. Liao R. China is building a GitHub alternative called Gitee. *TechCrunch*, August 21, 2020. Available at: <https://techcrunch.com/2020/08/21/china-is-building-its-github-alternative-gitee/> (accessed 12.06.2022).
25. UNCTADStat. Bilateral trade flows by ICT goods categories, annual. Available at: <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=15850> (accessed 12.03.2023).
26. Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024. Secretaría de gobernación. Diario Oficial de la Federación. Mexico, 6 de septiembre, 2021. Available at: https://www.dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0 (accessed 12.07.2022).
27. MCTI. Brazilian Digital Transformation Strategy, E-Digital. Brasília, 2018. Available at: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/digitalstrategy.pdf> (accessed 12.07.2022).
28. MCTI. Plano Nacional de Internet das Coisas. Decreto nº 9.854, de 25 de junho de 2019. Brasília, 2019, 4 p. Available at: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinternetdascoisas/d9854.pdf> (accessed 16.07.2022).

29. MCTI. Estratégia Brasileira de Inteligência Artificial. MCTI. Brasília, 2021, 52 p. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf (accessed 16.07.2022).
30. MCTI e Embrapii lançam rede de Inovação em Inteligência Artificial no País. MCTI, 31.10.2020. Available at: <https://inforchannel.com.br/2020/10/31/mcti-e-embrapii-lancam-rede-de-inovacao-em-inteligencia-artificial-no-pais/> (accessed 12.07.2022).
31. Estratégia nacional de segurança cibernética – E-CIBER. Decreto Nº 10.222, de 5 de fevereiro de 2020. Brasília, 2020, 52 p. Available at: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf> (accessed 12.07.2022).
32. ABES. Estudo Mercado Brasileiro de Software – Panorama e Tendências 2022. São Paulo, 2022, 40. p. Available at: <https://abes.com.br/en/dados-do-setor/> (accessed 12.02.2023).
33. Software industry in Brazil - statistics & facts. Available at: <https://www.statista.com/topics/9905/software-industry-in-brazil/#topicOverview> (accessed 12.03.2023).
34. UNCTADStat. Services (BPM6): Exports and imports by service category, trading partner world, annual. Available at: <https://unctadstat.unctad.org/wds/TableView/tableView.aspx> (accessed 18.03.2023).
35. UNCTAD. World Investment Report 2017: Investment and the Digital Economy. Geneva, 2017, 252 p. Available at: https://unctad.org/en/PublicationsLibrary/wir2017_en.pdf (accessed 18.07.2022).
36. Carta Soberania Digital. Programa de Emergência para a soberania digital. Available at: <https://cartasoberaniadigital.lalivre.wiki.br/carta/> (accessed 19.03.2023).
37. Borges I. Política Nacional de Educação Digital é sancionada. Rádio Senado, 13 de janeiro, 2023. Available at: <https://www12.senado.leg.br/radio/1/noticia/2023/01/13/politica-nacional-de-educacao-digital-e-sancionada> (accessed 19.02.2023).
38. CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Springer, 2021, 292 p. Available at: <https://cyberbrics.info/wp-content/uploads/2020/11/CyberBRICS-Book-FINAL-author-version-1.pdf> (accessed 12.06.2022).
39. В России появится национальный репозиторий открытого кода. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. М., 12 октября 2022 г. [V Rossii pojavitsya nacional'nyj repozitorij otkrytogo koda. Ministerstvo cifrovogo razvitiya, svyazi i massovyh kommunikacij Rossijskoj Federacii [Russia will have a national repository of open source. Ministry of Digital Development, Communications and Mass Media of the Russian Federation]. Moscow, 12 October 2022 (In Russ.). Available at: <https://digital.gov.ru/ru/events/42098/> (accessed 12.12.2022).
40. Digital Riser Report 2021. European Center for Digital Competitiveness. Berlin, 2021, 104 p. Available at: <https://digital-competitiveness.eu/digitalriser/> (accessed 15.06.2022).
41. BID. Argentina fortalecerá su agenda digital con apoyo del BID. Comunicados de prensa. Febrero 28, 2019. Available at: <https://www.iadb.org/es/noticias/argentina-fortalecera-su-agenda-digital-con-apoyo-del-bid> (accessed 16.07.2022).
42. Smith A. Top Latin American Countries for Nearshore Software Development in 2023. February 3, 2023. Available at: <https://hatchworks.com/nearshore-latin-america/> (accessed 19.03.2023).
43. Time100 Most Influential Companies 2023. Available at: <https://time.com/collection/time100-companies-2023/6285124/mercado-libre-leaders/> (accessed 19.04.2023).
44. Profile, Mercado Libre. *Forbes*. Available at: <https://www.forbes.com/companies/mercadolibre/?sh=132eeb49376a> (accessed 12.04.2023).
45. Número de artículos vendidos con éxito por MercadoLibre de 2015 a 2021. Statista. Available at: <https://es.statista.com/estadisticas/1203349/numero-articulos-vendidos-mercadolibre/> (accessed 12.06.2022).
46. IT Exports Boom in Uruguay Despite Talent Shortage. Available at: <https://nearshoreamericas.com/talent-shortage-uruguay-it-exports/> (accessed 25.04.2022).
47. Agenda Uruguay Digital 2025 - Sociedad digital resiliente. AGESIC, Presidencia República Oriental del Uruguay. Montevideo, 2020, 14 p. Available at: <https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025> (accessed 25.06.2022).
48. Estrategia de Inteligencia Artificial para el Gobierno Digital, AGESIC. Presidencia República Oriental del Uruguay. Montevideo, 2019, 16 p. Available at: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia> (accessed 29.06.2022).
49. Centro de Ensayos de Software. Available at: <https://www.ces.com.uy/> (accessed 29.04.2023).

50. How Uruguay's Antel is flexing its muscles internationally. Available at: <https://www.bname-ricas.com/en/features/how-uruguays-antel-is-flexing-its-muscles-internationally> (accessed 12.04.2023).
51. A prolific IT Services Market is Emerging in Costa Rica. Available at: <https://nearshore-americas.com/a-prolific-it-services-market-is-emerging-in-costa-rica/> (accessed 19.03.2023).
52. Lunes J. ¿Por qué Intel decidió reanudar operaciones de ensamblaje en Costa Rica? *La Republica*, 14 diciembre, 2020. Available at: <https://www.larepublica.net/noticia/por-que-intel-decidio-reanudar-operaciones-de-ensamblaje-en-costa-rica> (accessed 19.07.2022).
53. CEPAL. Cadenas globales de valor y diversificación de exportaciones. El caso de Costa Rica. Santiago, 2014, 102 p. Available at: <https://www.cepal.org/es/publicaciones/36719-cadenas-globales-valor-diversificacion-exportaciones-caso-costa-rica-asistencia> (accessed 19.07.2022).
54. Number of software developers involved in offshore development in Latin America in 2022, by country. Available at: <https://www.statista.com/statistics/1290785/software-developers-involved-in-offshore-development-latin-america/> (accessed 17.01.2023).
55. Toward a global network of digital hubs. The 2021 Kearney Global Services Location Index. Available at: <https://www.kearney.com/service/digital/article/-/insights/the-2021-kearney-global-services-location-index> (accessed 15.07.2022).
56. IT Outsourcing to Latin America: All You Need to Know. Available at: <https://www.griddynamics.com/global-team-blog/outsourcing-latin-america> (accessed 16.02.2023).
57. Ferrand G. An Expert Overview of The Latin America Software Industry. October 4, 2022. Available at: <https://www.tecla.io/blog/latin-america-software-industry-expert-overview#Index8> (accessed 16.12.2022).

Liudmila N.Simonova (ludmila-simonova@yandex.ru)
Ph.D. (Economic Sciences), Head of the Center for Economic Research, Institute of Latin America, Russian Academy of Sciences
B. Ordynka Str., 21, 115035 Moscow, Russian Federation

Evgueniy A.Ponomarev (e.samgreen2015@gmail.com)
Researcher, Center for Economic Research, Institute of Latin America, Russian Academy of Sciences
B. Ordynka Str., 21, 115035 Moscow, Russian Federation

Digital sovereignty, challenges and risks of digitalization in Latin America

Abstract. The article is devoted to the problem of digital sovereignty in the countries of Latin and Caribbean America (LCA). The monopolization of the global information technology (IT) industry has led to a sharp increase in the technological dependence of less digitally developed countries. The mass spread of social networks and digital platforms has increased the risks of external actors interfering in the socio-political and economic processes of developing countries. LCA states that are actively involved in digital transformation continue to depend on external suppliers of equipment and software, while their technological potential and qualified personnel are widely used in the interests of North American Big Tech. Dependence on tech giants and vulnerability in terms of digital security are pushing the countries of the region to take measures to develop national competencies in advanced technologies, solve the problem of ensuring digital sovereignty in critical sectors of the economy, create a favorable environment for doing business in the digital sphere, and improve legislative regulation.

Key words: digital sovereignty, digital security, Big Tech, digital transformation strategy, information technology, digital platforms, IT-market, software, outsourcing of digital services.

DOI: 10.31857/S0044748X0028265-0

Received 30.04.2023.