

Е.А.Виноградова

Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке

Технологии искусственного интеллекта (ИИ) стали настоящим прорывом в мире виртуальной коммуникации для современного общества. Страны Латинской Америки лишь начинают внедрять этот тип технологий с целью достижения парадигмы «умного правительства» и ускорения темпов построения цифровой экономики. Ряд государств инвестируют в стратегии развития технологий ИИ, сосредотачиваясь на повышении уровня экономического развития, прилагая значительные усилия для активизации сотрудничества на региональном уровне. Экономическая комиссия для Латинской Америки и Карибского бассейна (ЭКЛАК) на протяжении нескольких лет также стремится использовать огромный потенциал ИИ, включая цифровую трансформацию госсектора. Мировая концепция кибербезопасности становится особенно актуальной в связи с растущим использованием киберпространства как виртуальной среды для политического, экономического, социального и культурного взаимодействия. На сегодняшний день кибербезопасность стала важной темой национальных стратегий латиноамериканских стран в связи с участвовавшими случаями вредоносного использования ИИ в политической и экономической жизни региона.

Целями данного исследования являются выявление особенностей национальных стратегий внедрения ИИ в госсектор стран Латинской Америки и определение основных кибер-инструментов, направленных на подрыв национальной безопасности и дестабилизацию политических акторов.

Ключевые слова: Латинская Америка, искусственный интеллект, национальная стратегия, киберугрозы, социальные сети, дипфейк, боты, СМИ.

DOI: 10.31857/S0044748X0024415-5

Статья поступила в редакцию 05.01.2023.

Одной из наиболее ярких особенностей XXI в. является повсеместное использование технологий искусственного интеллекта (ИИ) во все аспекты жизни современного общества. Правительства внедряют ИИ для построения эффективной модели предоставления государственных услуг гражданам. Страны латиноамериканского региона, несмотря на заметное цифро-

Екатерина Алексеевна Виноградова — кандидат политических наук, независимый исследователь (<https://orcid.org/0000-0001-8055-6612>, vinogradovacatherine7@gmail.com).

вое отставание, являются важными международными акторами, которые внедряют ИИ в различные сектора, а также задействуют его в интеграционных процессах на региональном уровне.

В отчете за 2021 г., опубликованном Андской корпорацией развития (*Corporación Andina de Fomento, CAF*), отмечается, что такие страны, как Аргентина, Бразилия, Чили, Колумбия, Мексика, Перу и Уругвай, уже находятся в процессе внедрения национальной цифровизации и экспериментируют с системами ИИ в госуправлении [1, р. 43]. В последние годы в регионе появилось много научно-исследовательских центров, работающих в области изучения передовых технологий ИИ, которые проводят специализированные научные и образовательные мероприятия, направленные на увеличение квалифицированного кадрового резерва. В качестве примера можно привести работу Передового института искусственного интеллекта, созданного в 2018 г. при активном участии исследователей из крупнейших университетов Сан-Паулу в Бразилии.

Развитие виртуального киберпространства на основе технологий ИИ, контролируемого государственными и финансовыми органами латиноамериканских стран, — идеальный анклав для консолидации новых средств информации, коммуникации, предоставления и совершенствования сферы услуг, но вместе с тем до сих пор это — уязвимое звено перед киберугрозами. Несмотря на постоянные региональные усилия по углублению сотрудничества государств-членов в области кибербезопасности и наращиванию киберпотенциала, страны Латинской Америки находятся лишь на стадии разработки национального стратегического плана в области киберзащиты.

Методология данного исследования основана на системном подходе, направленном на изучение технологий ИИ и новых видов виртуальных преступлений в странах Латинской Америки. В статье использовались две основные группы источников: официальные документы государственных и военных органов, статистические данные, экономические отчеты; научные работы ведущих латиноамериканских и отечественных экспертов в области ИИ.

НАЦИОНАЛЬНЫЕ СТРАТЕГИИ ЛАТИНОАМЕРИКАНСКИХ СТРАН В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В период 2018—2022 гг. латиноамериканские государства приступили к активным разработкам национальных стратегий в области ИИ. Согласно отчету Организации экономического сотрудничества и развития (*Organización de la Cooperación y el Desarrollo Económico, OCDE*) и *CAF* от 14 января 2022 г., семь стран Латинской Америки (Аргентина, Бразилия, Чили, Колумбия, Мексика, Перу и Уругвай) разработали национальные стратегии в области ИИ [2, р. 10].

Мексика считается первой страной в Латинской Америке, которая в 2018 г., в период пребывания у власти Энрике Пеньи Ньето (2012—2018 гг.), скоординировала задачи по запуску стратегии ИИ. Одним из пер-

вых документов в этом направлении стал отчет «На пути к стратегии ИИ». Координационный совет по национальной цифровой технологии разработал руководство по принципам и анализу воздействия для разработки и использования систем на базе ИИ в федеральном государственном управлении. В то же время действующий президент Андрес Мануэль Лопес Обрадор (2018 — н/в) до сих пор не принял мер по созданию национальной стратегии в сфере ИИ. На сегодняшний день в стране существует лишь некая структура под названием «Искусственный интеллект 2030 Мх», состоящая из государственных и частных учреждений, а также специалистов в области ИИ, которые формируют мексиканскую национальную технологическую повестку дня [3, р. 10].

Бразилия является лидером по технологиям ИИ, применяемым в госсекторе и бизнес-среде. Уже несколько лет в стране действует национальная стратегия в области ИИ, разработанная министерством науки, технологий и инноваций. В соответствии с этой стратегией проводится политика по внедрению новых технологий; документ также является базой для разработки отраслевых таких правовых норм, как Исполнительный декрет об Интернете вещей № 9.854 от 25 июня 2019 г., в котором представлены четыре темы: промышленность, здравоохранение, умные города и сельское хозяйство [4, р. 18].

Национальный план Аргентины по искусственному интеллекту, известный как *ARGENIA*, был запущен в 2020 г. во время правления президента Маурисио Макри (2015—2019 гг.) [3, р. 12]. Основной целью является разработка политики, способствующей устойчивому росту и улучшению равных возможностей в стране при помощи технологий ИИ.

В Чили политика в области ИИ в настоящее время находится в процессе формирования. Первые попытки создания национальной стратегии можно отнести к середине 2019 г., когда правительство Себастьяна Пиньеры (2010—2014; 2018—2022 гг.) поручило министерству науки, технологий, знаний и инноваций разработать план развития ИИ в стране [3, р. 18].

Уругвай начал процесс внедрения ИИ в государственный сектор с попытки реализовать цифровые услуги, основанные на применении новейших технологий. В этом контексте искусственный интеллект — государства латиноамериканского региона — это цель внедрения плана цифрового правительства Уругвая.

Колумбия заняла третье место в рейтинге согласно Индексу цифрового правительства ОЭСР в 2020 г. Индекс измеряет прогресс в переходе на цифровые технологии среди 37 стран, входящих в Организацию экономического сотрудничества и развития (ОЭСР). В конце 2019 г. правительство Ивана Дуке Маркеса (2018—2022 гг.) совместно с Национальным советом по экономической и социальной политике утвердили Национальную политику в области цифровой трансформации и ИИ [3, р. 20]. В последние годы страна активно работает над тем, чтобы стать лидером четвертой промышленной революции в регионе.

Наконец, в Перу национальная стратегия по ИИ была запущена в июне 2021 г. по инициативе правительства. Таким образом, можно говорить о том, что по состоянию на конец 2022 г. государства латиноамериканские государства находятся лишь на стадии формирования и модернизации национальных стратегий в области ИИ. Несмотря на это, отдельные технологии ИИ успешно применяются в различных сферах.

В течение последних пяти лет в Латинской Америке проводились эксперименты по созданию систем ИИ, основанных на использовании семантики данных для автоматизации процессов и интеллектуальных прогнозов. Примером может служить пилотный проект *Prometea*, запущенный в Аргентине в 2017 г. при активном участии заместителя генерального прокурора страны по административным и налоговым вопросам. *Prometea* — одна из самых сложных разработок ИИ, направленная на оптимизацию судебной системы. Программа была успешно апробирована прокуратурой Буэнос-Айреса для рассмотрения апелляций по жилищным вопросам за более короткое время, чем при традиционной процедуре, и с точностью 96% в том, что касается решений, принятых экспертом [1, р. 45]. Аналогичные разработки были успешно внедрены в судебные органы Колумбии и Бразилии для прогнозирования результатов рассмотрения конкретных судебных дел [5]. Технологии ИИ также активно задействованы и в социальных проектах. Так, правительство аргентинской провинции Сальта при поддержке *Microsoft* внедрило систему ИИ, целью которой является прогнозирование подростковой беременности среди уязвимых групп населения [1, р. 45].

В Бразилии в госсекторе были реализованы различные проекты с использованием технологий ИИ в таких областях, как образование, здравоохранение, сельское хозяйство, охрана окружающей среды [6, р. 17]. Так, в сельском хозяйстве эти технологии используются для мониторинга урожая и состояния почвы, прогнозирования влияния факторов окружающей среды на урожайность сельскохозяйственных культур. В астрономии ИИ используется для решения сложных вычислительных задач и улучшения качества изображений [5].

Отечественные исследователи О.Г.Карпович и А.В.Чеснокова отмечают, что использование передовых технологий может способствовать решению разных проблем Латинской Америки, привлечь крупные инвестиции в научно-исследовательские работы, связанные с ИИ [7, р. 37]. Российские специалисты А.Ж.Степанян и Т.С.Заплатина указывают, что в законодательстве и доктрине ряда латиноамериканских стран намечаются «тенденции к наделению ИИ правосубъектностью» [8, р. 135].

Наиболее активно технологии ИИ внедряют коммерческие компании. На региональном уровне Бразилия лидирует по инвестициям, задействованным ресурсам и разнообразию области применения технологий ИИ. Второе место занимает Аргентина. Несмотря на то, что ее экономика в три раза меньше мексиканской, она имеет развитую технологическую экосистему, что способствует более широкому распространению техноло-

гий ИИ, чем в соседних странах [9, р. 37]. Аргентинские компании являются лидерами в области внедрения машинного обучения и системы распознавания лиц.

В Колумбии развитие проектов, основанных на ИИ, обусловлено процессами цифровой трансформации компаний. Директор по стратегии компании *Nexa* Андрес Гомес отмечал: «В рамках нашей дорожной карты преобразований мы сфокусировались на разработке проектов ИИ, приносящих видимые результаты. В течение последнего года мы внедряли технологию виртуального помощника, который в первый месяц достиг эффективности почти 40% в обслуживании клиентов и сократил численность персонала на 20%» [9, р. 42].

Одним из основных препятствий, тормозящих внедрение ИИ в коммерческие компании, латиноамериканские специалисты называют проблему нехватки квалифицированных специалистов. Для решения данного вопроса страны Латинской Америки начали активное сотрудничество с профильными университетами. Одним из самых ярких примеров является чилийская фирма *Telefónica*, которая напрямую сотрудничает с университетами для создания совместных учебных программ.

Серьезной проблемой остается ограниченный бюджет, выделяемый для инвестиций в ИИ, что связано с текущей макроэкономической ситуацией в регионе. Большинство компаний все еще связывают внедрение новых технологий с огромными расходами, не имеющим отношения к их бизнесу.

Наконец, сохраняется зависимость от технологических сверхдержав. Развитие технологий ИИ стимулируется двумя основными игроками — Китаем и США. На них приходится львиная доля инвестиций и исследований в области ИИ, а также технологий, которые являются базовым стандартом для всех стран. В случае Латинской Америки большинство крупных компаний используют цифровые платформы и продукты таких американских гигантов, как *Microsoft*, *Google* и *Amazon*. Этот факт закрепляет повсеместное присутствие американских технологических продуктов в полностью зависящих от них латиноамериканских организациях.

ИСПОЛЬЗОВАНИЕ ЧАТ-БОТОВ В ПОЛИТИЧЕСКИХ ВЫБОРАХ

В XXI в. информационно-коммуникационное киберпространство стало передовой платформой политической пропаганды во многих странах мира и, в частности, в Латинской Америке. Площадками для нее являются социальные сети, мессенджеры, в качестве технологий используются такие последние достижения в области ИИ, как социальные чат-боты (виртуальные собеседники, программы). Так, согласно данным *Latinobarómetro*, в 2010 г. около 20% взрослого населения Латинской Америки имели аккаунт в *Facebook*. К 2015 г. этот показатель вырос до 42%, а к 2020 г. — до 65%. В то же время *WhatsApp*, дочерняя платформа *Facebook*, стала еще популярнее: 73% пользователей в 2020 г. [10].

Одним из примеров использования чат-ботов в Бразилии может послужить второй тур президентских дебатов в 2014 г. Анализ, проведенный Федеральным университетом штата Эспириту-Санту, выявил признаки активности ботов, когда в течение первых 15 минут от начала дебатов количество упоминаний в *Twitter* кандидата Аэсиу Невеса было искусственно увеличено в три раза.

В 2015 г. в закрытом правительственном меморандуме указывалось на чат-боты, использовавшиеся в кампаниях Дилмы Руссефф (2011—2016 гг.) и ее оппонента А.Невеса. Обе команды применяли чат-боты для распространения информации в пользу своих выдвиженцев. Чат-боты, с помощью которых поддерживали Дилму, были деактивированы после успешной кампании, тогда как чат-боты команды Невеса продолжали быть активными уже после выборов, потенциально ускоряя движение 2015 г. за импичмент президента Руссефф. Исследование, проведенное Департаментом анализа государственной политики Фонда Жетулиу Варгаса (*Fundação Getulio Vargas*) в июне 2018 г., показало, что 20% ретвитов, связанных с Луисом Инасиу Лула да Силва (2003—2011, 2023 — н/в) или Жаиром Болсонару (2019—2023 гг.), которые проявляли активность в социальных сетях в преддверии президентских выборов, были сделаны с помощью чат-ботов [11].

В январе 2018 г. под руководством Высшего избирательного суда и Федеральной полиции Бразилии была создана группа, деятельность которой направлена на предотвращение и ограничение фальшивых новостей во время выборов. В частном секторе *Facebook* удалил почти 200 страниц, которые вели несколько человек, связанных с правой активистской организацией «Движение за свободную Бразилию» (их имена не были раскрыты) [12]. С 2018 г. в стране также действует коалиция *Comprova*, состоящая из 24 журналистов популярных бразильских новостных изданий (включая *Veja* и *Estado de S. Paulo*), отслеживающих фальшивые новости в социальных сетях. *Comprova* предоставляет онлайн-платформу, где избиратели могут проверять информацию, которую они читают в Интернете.

Исследователи Даниэль Барредо-Ибаньес (Колумбия), Даниэль-Хавьер Де ла Гарса Монтемайор (Мексика), Анхель Торрес-Тукумидис (Эквадор), Пауло-Карлос Лопес-Лопе (Испания) указывают на так называемые кибердружины, состоящие из представителей госаппарата, политических партий и СМИ [13, р. 8]. Их деятельность направлена на разработку политических манипуляций при помощи новейших технологий ИИ. В качестве примера авторы приводят президентские выборы в Колумбии в 2014 г., в рамках которой активно использовались социальные боты и ИИ в *Twitter*. Так, в 2018 г. на выборах в Колумбии в чатах поддержки кандидата в президенты И.Дуке Маркеса (2018—2022 гг.) популярного мессенджера *WhatsApp* были использованы «эхокамеры», при помощи которых через регулярный повтор искаженного содержания «накручивался» престиж этого политика, в то время как кампания по дискредитации других кандидатов усиливалась [13, р. 7]. Во время президентских выборов в Мексике 2018 г.

активность определенных электоральных групп в социальных сетях, таких, как евангелисты, сыграла важную роль в победе А.М.Лопеса Обрадора (2018—н/в). В то же время сам кандидат использовал платформу *Facebook* скорее для продвижения своих идей и политического имиджа, а не для диалога с избирателями.

Говоря о Мексике, нужно отметить, что за последние пять лет несколько независимых кандидатов с грамотно выстроенными стратегиями в социальных сетях были избраны губернаторами штатов [14]. Благодаря социальным сетям кандидаты могут напрямую обращаться к избирателям, не пользуясь услугами традиционных СМИ. Избиратели-единомышленники, в свою очередь, могут быстро консолидироваться в целях информационной поддержки кандидата.

В Эквадоре во время президентской кампании 2021 г. инструментом продвижения послужили коммерческие боты, которые были переориентированы на избирательные кампании с целью профилирования и поляризации голосующей общественности через социальные сети. В этом случае анализ данных с помощью технологий ИИ позволил создать предсказуемые модели голосования.

Социальные сети позволяют адаптировать политические сообщения для различных сегментов электората. Встроенные технологии, такие как боты, спам, тролли и киборги, стали основными средствами манипуляции в период политических выборов. Например, микротаргетинг — маркетинговая стратегия, использующая персональные и демографические данные пользователей для выявления интересов конкретных людей или малых групп единомышленников, с целью повлиять на их отношение и поведение. Это — обычный инструмент для продвижения бизнеса в социальных сетях, однако он может быть использован пиар-службами для преднамеренного распространения дезинформации с целью манипулирования общественным мнением. Согласно отчету *Freedom House* за 2019 г., в 2018 г. 26 из 30 стран, в которых проводились выборы или референдумы, столкнулись с цифровым вмешательством в выборы [15].

ДИПФЕЙКИ В ПОЛИТИЧЕСКОЙ ПРАКТИКЕ БРАЗИЛИИ

Одной из передовых технологий ИИ, используемой для дезинформации в политических целях, является дипфейк*. Концепция глубокого обучения (*Deep Learning*), впервые появившаяся в 2006 г. как новая область исследований в машинном обучении, запустила использование искусственных нейронных сетей, которые превзошли возможности человека в распознавании речи и алгоритмической генерации лиц и пейзажей [16, р. 67]. Эта новая технология сразу же вызывала беспокойство, поскольку создает

* Дипфейк (deepfake) — технология создания и замены элементов на существующих видео при помощи искусственного интеллекта и нейронных сетей.

риски для государственных органов и кибербезопасности [17, р. 29]. Российский ученый Е.Н.Пашенцев отмечает, что «при соответствующей подготовке *deepfakes* в рамках информационно-психологического противоборства могут спровоцировать финансовую панику, торговую или «горячую» войну» [18, р. 286].

На сегодняшний день уже существуют многочисленные приложения для смартфонов и компьютеров для создания дипфейков в Интернете: *Reface* — приложение для замены лица; *MyHeritage* — оживление и реставрация антикварных фотографий; *Sway* — изменение статической позы в танцевальную или трюковую последовательность; приложение *FaceApp* позволяет пользователям состарить и исказить изображение лица; *Zao*, используя библиотеку киноклипов, позволяет модулировать голос и менять лица.

После участвовавших случаев использования технологии дипфейк в политических целях, в США в конце 2020 г. открытая лаборатория документального кино Массачусетского технологического института выпустила документально-аналитический сериал «*Deepfakery*» [19]. В октябре 2021 г. *Facebook* принял решение об удалении синтетического контента, созданного при помощи дипфейков, из своей социальной сети. Аналогичные решения приняли *Twitter* и *TikTok*.

Известны случаи, когда использование технологии дипфейк сыграло роль в развитии политических сценариев. Так, в октябре 2018 г. губернатор бразильского штата Сан-Паулу Жуан Дория за несколько дней до выборов стал жертвой фейкового видео. В упомянутом ролике политик был запечатлен во время сексуальной оргии. В социальных сетях это видео вызвало большой переполох, последовало множество разбирательств и заявлений. Однако благодаря быстро открытому уголовному делу и заявлению политика этот материал не оказал существенного влияния на его популярность. В итоге Дория был избран губернатором Сан-Паулу. После распространения этого видео дипфейк стал популярной темой новостных СМИ, которые предупреждали о потенциальном вреде этой технологии и о том, как она может повлиять на выборы в Бразилии в 2020 г.

Аналогичным образом, дезинформация при помощи технологии дипфейк сыграла важную роль и на президентских выборах в Бразилии в 2018 г. Кандидат в президенты Жаир Болсонару использовал фальшивые новости для нападок на своего соперника Фернанду Аддада и продвижения своей кампании к победе, распространяя дезинформацию для нанесения вреда репутации последнего. Распространение ложной информации действительно положительно повлияло на политическую кампанию Болсонару, навредив его оппоненту [20, р. 26].

По данным *Impressions App*, одного из самых популярных приложений для смартфонов в области биометрических разработок, Бразилия является второй страной после США по количеству пользователей данной платформы (20% от общего числа пользователей во всем мире). Несмотря на то, что подобные приложения обычно разрабатываются в

США или Китае, Бразилия оказывается их постоянным потребителем. Популярность данной технологии среди создателей контента в Бразилии увеличивает вероятность использования ложных новостей и дезинформации [20, р. 7].

Одним из активных пользователей дипфейков в Бразилии является маркетолог и видеомейкер Бруно Сартори, получивший известность благодаря целой серии видеороликов, высмеивающих политических лидеров. В одном из роликов Б.Сартори продемонстрировал политическую сатиру, создав мемы президентов Бразилии Ж.Болсонару и его основного политического оппонента Л. да Силвы, который был представлен в ролике в виде козла отпущения [19].

Бразильское законодательство не предусматривает уголовной ответственности за использование дипфейков, а скорее рассматривает эту тему на основе других существующих законов. Так, можно подать иск в суд с обвинением в клевете. Для выигрыша по этому делу потребуются доказать, что ответчик создал или заказал фальшивый контент и распространил его. В то же время интересно отметить, что, несмотря на отсутствие законодательства, касающегося именно технологии дипфейков, Бразилия приняла некоторые меры по защите своего населения от дезинформации. После распространения фальшивых новостей в период выборов в 2021 г. был утвержден закон, направленный на сокращение количества пересылаемых сообщений в *WhatsApp* и на аналогичных платформах.

КИБЕРУГРОЗЫ И НОВЫЕ ФОРМЫ ВИРТУАЛЬНЫХ ПРЕСТУПЛЕНИЙ

В начале XXI в. кибербезопасность стала важным вопросом национальной безопасности для всех государств. Латинская Америка является одним из наиболее уязвимых регионов, занимая третье место в мире по количеству кибератак — 84 млн., согласно отчету компании «Лаборатория Касперского» [21, р. 30]. Потенциальный ущерб от кибератак из-за отсутствия грамотной политики, направленной на своевременное реагирование на киберугрозы, составляет в среднем 90 млрд долл. в год.

Согласно отчету компании *PandaLabs*, занимающейся кибербезопасностью, в 2014 г. такие страны, как Гватемала, Боливия, Эквадор, Бразилия и Перу, вошли в десятку государств мира с наибольшим количеством компьютеров, зараженных вредоносными вирусами. Компания *IBM Security* в отчете за 2020 г. рассматривает Латинскую Америку как место, где сосредоточено 5% всей мировой активности киберпреступников [22, р. 21].

Для воздействия на интересы страны можно использовать два типа методов: эксплуатация компьютерных сетей (шпионская деятельность с целью получения конкретной информации, которая может быть использована для извлечения прибыли или подготовки будущих атак на сети); киберата-

ки (внедрение вирусов, приводящих к потере информации и влияющих на нормальное функционирование сетей или веб-сайтов государственных структур или частных компаний) [23, р. 185]. Как отмечает Е.Н.Пашенцев, ИИ может стать как «технологическим фундаментом нового более социально-ориентированного мироустройства, так и опорой технологических антидемократических диктатур и активно использоваться в антисоциальных целях различными негосударственными акторами» [24].

В 2008 г. компания, *PackRat*, используя готовые инструменты удаленного доступа (*RAT*), осуществляла хакерские кибератаки в Венесуэле, Эквадоре и Аргентине с целью подрыва авторитета действующих политиков и влиятельных людей. Киберпреступники продемонстрировали глубокое знание политической специфики региона, создавая поддельные интернет-организации в Венесуэле (*Pancaliente.info*, *Venezuela365.com* и *Chavistas24.com*) и Эквадоре (*Movimento Anti Correista*», *justicia-desvinculados.com*) с размещением на сайтах оригинального контента для привлечения внимания политических сторонников. Целью киберпреступлений в Аргентине стали известные политические деятели, а также другие известные лица, в том числе Хорхе Ланата — ведущий теленовостей, и Альберто Нисман — прокурор, убитый накануне слушаний в конгрессе [25].

В 2011 г. в Колумбии был схвачен известный киберпреступник Хорхе Максимилиан «Пачо» Виола», а в феврале 2012 г. страна возглавила многонациональную операцию «Разоблачение», направленную на ликвидацию кольца преступных группировок, которая была начата в ответ на постоянные атаки на критически важные инфраструктуры в Чили и Колумбии [26].

В 2014 г. российская компания «Лаборатория Касперского» разоблачила кибернетическую наступательную кампанию «Мачете» (2010—2012 гг.), целью которой были взломы профессиональных профилей сотрудников спецслужб, посольств, военных и правительственных учреждений Венесуэлы, Эквадора, Колумбии, Перу и России [25]. За один только 2017 г. «Лаборатория Касперского» нейтрализовала атаки на 38,9% латиноамериканских систем промышленной автоматизации (по сравнению с 37,6% нейтрализованных атак во все мире) [27].

В марте 2016 г. служба налогового управления Мексики подверглась хакерской атаке, приписываемой группе «Анонимная Мексика». В ноябре 2019 г. была совершена крупнейшая кибератака на мексиканскую нефтяную компанию *Petróleos Mexicanos (PEMEX)*. Это нарушило работу компании по выплате международных долгов и начислению заработной платы и что нанесло ущерб ее престижу на международном уровне. Выкуп, запрошенный за возвращение контроля над операционной сетью, составил 4,9 млн долл., что стало одной из самых дорогих сделок в истории Латинской Америки [22, р. 37]. В феврале 2020 г. кибератака была направлена на внутреннюю сеть министерства экономики Мексики. [22, р. 37].

В результате масштабной электронной атаки на Венесуэлу 17 мая 2019 г. Интернет в стране был отключен на 35 часов, после чего венесуэльское руководство обвинило правительство США во вмешательстве во внутренние дела [21, р. 31].

На протяжении почти двух десятилетий Организация американских государств (ОАГ) является ключевым игроком в продвижении потенциала кибербезопасности в регионе. В 2004 г. была принята Межамериканская стратегия по борьбе с угрозами кибербезопасности [28, р. 29]. В период 2012—2014 гг. Южноамериканский союз наций (*Unión de Naciones Suramericanas, Unasur*) включил эту тему в свои планы действий. Однако, несмотря на постоянные региональные усилия по углублению сотрудничества государств-членов в области кибербезопасности и укрепления киберпотенциала, когда дело доходит до кибер-операций, страны Латинской Америки все еще продолжают вырабатывать свое понимание этой проблемы.

Руководитель программ по цифровой безопасности Бразилии Луиза Мари Хюрель отмечает, что после публикации документов Эдварда Сноудена, когда стало известно, что США шпионили за президентом Д.Руссефф и другими важными политическими лидерами, Бразилия открыто обвинила Вашингтон в кибершпионаже и начала активно включать вопросы кибербезопасности в свою политическую стратегию [28, р. 28]. Страна запустила «План безопасной цифровой трансформации». Сегодня в Бразилии существует национальная сеть полицейских участков, занимающихся расследованием киберпреступлений. Полиция сотрудничает с другими органами государственной безопасности, такими, как Управление комплексных операций (*Secretaria de Operações Integradas, SEOPI*) министерства юстиции и общественной безопасности по вопросам оперативной разведки для расследования и реагирования на кибершпионаж.

В 2017 г. в Мексике была запущена круглосуточная сеть по борьбе с киберпреступностью и создана Национальная стратегия кибербезопасности, сфокусированная на соответствующем технологическом развитии. Колумбия, в свою очередь, стала первой латиноамериканской страной, разработавшей всеобъемлющую национальную стратегию кибербезопасности и киберзащиты. В стране был принят новый закон, направленный на повышение кибербезопасности путем развития двустороннего сотрудничества и увеличение объема технологических услуг за рубежом. Правительство Аргентины создало Национальное управление информационных технологий для оценки и внедрения системы модернизации и эффективного использования цифровых ресурсов [26]. Пионером в области повышения стандартов кибербезопасности оказалась Боливия. Уровень интернет-грамотности в стране составляет 100%, наблюдается серьезная приверженность борьбе с киберпреступностью [26].

Таким образом, можно констатировать, что благодаря разработке мер, позволяющих сократить количество кибервзломов, некоторые латиноамериканские

риканские страны уже сейчас добились прогресса в области кибербезопасности. В регионе используется множество прогрессивных технологий в области кибербезопасности, в частности, управляемые межсетевые экраны, защита от *DDoS*-атак, управление уязвимостью. Однако эти технологии не обеспечивают должного уровня безопасности, поэтому существует необходимость разработки комплексной региональной стратегии.

Искусственный интеллект в странах Латинской Америки стал передовой технологией, направленной на модернизацию политической, экономической и социальной жизни региона. Во многих странах были созданы национальные стратегии по развитию и дальнейшему внедрению технологий ИИ в государственный сектор и в работу интеграционных объединений. Данные технологии с успехом встроены в сферу образования, систему здравоохранения (например, использование робототехники при проведении сложных операций), а также в судебные органы. При активном участии латиноамериканского бизнеса ИИ внедряются в работу коммерческих компаний.

Вместе с тем, как и большинство стран мира, государства Латинской Америки используют для создания своих приложений технологии ИИ, разработанные и предоставленные крупными технологическими гигантами США. Многие латиноамериканские компании приобрели услуги корпораций *Microsoft AI*, *Google Tensorflow*. Американская цифровая платформа *Meta Platforms* с ее социальными сетями *Facebook*, *Instagram* и мессенджером *WhatsApp* является основными каналами политической и социальной коммуникации, лишая регион цифровой независимости.

Еще одной проблемой, тормозящей развитие ИИ в Латинской Америке, является отсутствие квалифицированных специалистов в сфере информационных технологий. Цифровая и технологическая зависимость от США в любой момент может быть использована ими для оказания внешнеполитического давления на государственные и региональные акторы.

Латинская Америка занимает лидирующие позиции по числу крупнейших киберпреступлений за последние пять лет. Тем не менее на региональном уровне до сих пор не приняты согласованные стратегии противостояния в киберсфере. Технологическая революция и заметное цифровое отставание региона бросает вызовы дальнейшей консолидации стран Латинской Америки, направленной на модернизацию собственной цифровой экономической модели, основанной на региональных технологических возможностях ИИ. На наш взгляд, ускорить процесс модернизации по внедрению технологий ИИ в региональную повестку дня помогут такие меры, как разработка независимых цифровых платформ, создание регионального рынка труда в сфере информационных технологий и, наконец, ускоренный процесс подготовки специалистов в области ИИ.

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

1. García De Lara. J. Inteligencia Artificial y Justicia: Experiencias en América Latina. *Publicación semestral*, Tunja, 2022, Vol. 9, N 17, pp. 41-46.
2. Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe. Estudios de la OCDE sobre Gobernanza Pública. OECD Publishing, Paris, 2022, 209 p.
3. García Benítez V.H., Ruvalcaba-Gómez E.A. Análisis de las estrategias nacionales de inteligencia artificial en América Latina: Estudio de los enfoques de ética de Ética y de Derechos Humanos. *Revista de Gestión Pública*, Guadalajara, 2021, Vol. 10, N 1, pp. 5-32. (DOI: 10 (1) ISSN: 0719-1839).
4. Veronese A, Lopes Espiñeira Lemos A. N. Trayectoria normativa de la inteligencia artificial en los países de Latinoamérica con un marco jurídico para la protección de datos: límites y posibilidades de las políticas integradoras. *Revista Latinoamericana de Economía y Sociedad Digital*, Buenos Aires, 2021, Issue 2, pp 1-31 (DOI:10.53857/MZBU2371).
5. Repaso de las políticas y desarrollos latinoamericanos sobre inteligencia artificial. Informe de Desarrollo de Políticas de IA. Telecommunications Management Group, Inc, Valencia, 2020, pp. 1-38. Available at: [TMG-Informe-de-Desarrollo-de-Políticas-de-IA.pdf](https://tmgtelecom.com/TMG-Informe-de-Desarrollo-de-Políticas-de-IA.pdf) (tmgtelecom.com) (accessed 21.01.2021).
6. Hernández L., Paz Canales M., Souza M. Inteligencia Artificial y participación en América Latina: Las estrategias nacionales de IA. *Derechos digitales América Latina*. International Development Research Centre, Ottawa, 2022, 56 p.
7. Карпович О.Г., Чеснокова А.В. Искусственный интеллект в Латинской Америке: реальность и перспективы цифрового будущего. *Вестник дипломатической академии МИД России. Россия и мир*, М., 2022, № 3(33), сс. 24-40. [Karpovich O.G., Chesnokova A.V. Iskusstvennyy intellekt v Amerike: real'nost' i perspektiva budushchego. [Artificial Intelligence in Latin America: the reality and promise of a digital future]. *Vestnik sledstvennoy akademii MID Rossii. Rossiya i mir*. Moscow, 2022, N 3(33), pp. 24-40 (In Russ.).
8. Степанян А.Ж., Заплата Т.С. Правовое регулирование роботов и искусственного интеллекта в странах Латинской Америки, проблема прав человека и ИИ. *Lex Russica*, М., 2022, 73 (7), сс. 127-136. [Stepanyan A.ZH., Zaplatina T.S. Pravovoye regulirovaniye problemy robotov i iskusstvennogo intellekta v stranakh Latinskoy Ameriki, prav cheloveka i II. [Legal regulation of robots and artificial intelligence in Latin America, the issue of human rights and AI]. *Lex Russica*. Moscow, 2022, 73 (7), pp. 127-136 (In Russ.). (DOI: <https://doi.org/10.17803/1729-5920.2020.164.7.127-136>)
9. La Inteligencia Artificial en las compañías latinoamericanas. Visión panorámica de la adopción y tendencias en la Región. *MIT Technology Review*, Montreal, 2020, 60 p.
10. Latinobarometro. Santiago de Chile. Available at: <https://www.latinobarometro.org/lat.jsp?Idioma=0> (accessed 17.01.2023).
11. FGV Dapp: sabatina de Bolsonaro no JN motivou 1,37 milhão de tweets. *PODER360*, São Paulo, 2018. Available at: <https://www.poder360.com.br/eleicoes/fgv-dapp-sabatina-de-bolsonaro-no-jn-motivou-137-milhao-de-tweets/> (accessed 10.01.2022).
12. Allen A. Bots in Brazil: The Activity of Social Media Bots in Brazilian Elections. Washington, 2018. Available at: <https://www.wilsoncenter.org/blog-post/bots-brazil-the-activity-social-media-bots-brazilian-elections> (accessed 11.01.2022).
13. Barredo-Ibáñez D., De la Garza-Montemayor D.J., Torres-Toukoumidis Á., López-López P.C. Inteligencia artificial, comunicación y democracia en América Latina: una revisión de los casos de Colombia, Ecuador y México. *Profesional de la información*, Madrid, 2021, Vol. 30, N 6, pp.1-17. (DOI: <https://doi.org/10.3145/epi.2021.nov.16>)
14. Vlaicu R. Is Social Media Remaking Latin American Elections? Washington, 2021. Available at: <https://blogs.iadb.org/ideas-matter/en/is-social-media-remaking-latin-american-elections/> (accessed 3.11.2022).

15. The Crisis of social media. Freedom on the net 2019. Freedom House, New York. 32 p. Available at: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf. (accessed 5.01.2022).
16. Pantoja De Moraes C. «Deepfake» como ferramenta de manipulação e disseminação de «fakenews» em formato de vídeo nas redes sociais. *Biblios*, Rio de Janeiro, 2020, N 79, pp. 63-72. (DOI: 10.5195/biblios.2020.864)
17. Gomes-Gonçalves S. Los deepfakes como una nueva forma de desinformación corporativa – una revisión de la literature. *International review (Irocamm)*, Sevilla, 2022, Vol. 5, N 2, pp. 22-38. (DOI: [dx.doi.org/10.12795/IROCMM.2022.v05.i02.02](https://doi.org/10.12795/IROCMM.2022.v05.i02.02))
18. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации. *Государственное управление. Электронный вестник*, М., 2019, № 76, сс. 279-300. [Pashentsev E.N. Zlonamerennoye ispol'zovaniye iskusstvennogo intellekta: novyye vybrosy dlya mezhdunarodnoy informatsionno-psikhologicheskoy bezopasnosti i puti ikh neytralizatsii [Malicious Use of Artificial Intelligence: New Threats to International Psychological Security and Ways to Neutralize Them]. *Gosudarstvennoye upravleniye. Elektronnyy vestnik*. Moscow, 2019, N 76, pp. 279-300. (In Russ.). (DOI: 10.24411/2070-1381-2019-10013)]
19. Just Joking. Deepfakes, satire, and the politics of synthetic media. Cambridge, 2022. Available at: <https://cocreationstudio.mit.edu/wp-content/uploads/2021/12/JustJoking.pdf> (accessed 3.01.2023).
20. Pinheiro de Resende S.M. The effects of deepfakes on politics and on data justice issues – a perspective from Brazil and the United States. A thesis submitted for the degree of Master of Law & Technology, Tilburg, 2021, 52 p.
21. Pavón E., Guaytarilla L. F., Cueva C., Durango K. Perspectivas sobre la ciberseguridad y ciberdefensa en América Latina. *Athena Journal*, Quito, 2022, Vol. 3, N 9, pp. 26-37. (DOI: <https://doi.org/10.47460/athenea.v3i9.43>)
22. Aguilar Antonio J.M. La brecha de ciberseguridad en América Latina frente al context global de ciberamenazas. *Revista de Estudios en Seguridad Internacional*, México, 2020, Vol. 6, N 2, pp. 17-43. (DOI: <https://doi.org/10.18847/1.12.2>)
23. Olmedo J. I., Gavilanez F. León. Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal*, Guayaquil, 2018, Vol. 3, N 9, pp.180-189.
24. Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта и вызовы международной информационно-психологической безопасности. [Pashentsev E.N. Zlonamerennoye ispol'zovaniye iskusstvennogo intellekta i vyzovy mezhdunarodnoy informatsionno-psikhologicheskoy bezopasnosti [Malicious Use of Artificial Intelligence and the challenges of international information-psychological security]. (In Russ.). Available at: <https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/zlonamerennoe-ispol-zovanie-iskusstvennogo-intellekta-i-vyzovy-mezhdunarodnoy-informatsionno-psikholo/> (accessed 20.12.2022).
25. Izycki E. Is Latin America the lost continent of cyberspace? Conference Paper July 2021, Lisbon. Available at: <https://www.cyber-insights.org/is-latin-america-a-forgotten-continent-of-cyberspace/> (accessed 11.11.2022).
26. Latin American and Caribbean Cybersecurity Trends and Government Responses. Organization of American States. Puna, 2022. 30 p. Available at: <https://informationsecurity.report/articles/latin-american-and-caribbean-cybersecurity-trends-and-government-responses> (accessed 01.01.2023).
27. Penaranda L. Cyberattacks on critical infrastructure in Latin America. La Paz. Available at: https://www.academia.edu/35717004/CYBERATTCKS_ON_CRITICAL_INFRASTRUCTURE_IN_LATIN_AMERICA (accessed 3.01.2023).
28. Hurel L.M. Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America. *Global Security Review*, New York, 2022, Vol 2, N 7, pp. 21-32. (DOI: 10.25148/GSR.2.009786).

Екатерина Виноградова

Ekaterina A. Vinogradova (vinogradovacatherine7@gmail.com)
Cand. Sci. (Political Science), Independent researcher

Artificial intelligence technologies and the rise of cyber threats in Latin America

Abstract. Artificial Intelligence (AI) technologies have been a real revolution and breakthrough in the world of virtual communication for modern society. Latin American countries are just beginning to adopt this type of technology to achieve the smart government paradigm and accelerate the pace of building a digital economy. A number of countries in the Latin American region are investing in strategies to develop AI technologies, focusing on improving economic development, with significant efforts to create a broader cooperation network at the regional level. The Economic Commission for Latin America and the Caribbean (ECLAC) also has been striving for several years to harness the huge potential of AI, including the digital transformation of the public sector.

The global concept of cybersecurity becomes particularly relevant due to the increasing use of cyberspace as a virtual environment for political, economic, social and cultural interaction. To date, cybersecurity has become an important issue for national strategies of Latin American countries due to the increasing incidence of malicious use of AI in the political and economic life of the region.

The purpose of this study is to demonstrate main dimensions of national strategies for the implementation of AI in the public sector in Latin America and to identify the main cyber tools aimed at undermining national security and putting political actors out of work.

Key words: Latin America, artificial intelligence, national strategy, cyber threats, social media, deepfake, bots, media.

DOI: 10.31857/S0044748X0024415-5

Received 05.01.2023.