ПОЛИТИКА

Е.А.Виноградова

Технологии искусственного интеллекта в политической повестке *BRICS*

В период IV промышленной революции стремительный рост технологий искусственного интеллекта (ИИ) ставит перед всеми странами задачу их правомерного использования и своевременного внедрения в государственный сектор. Страны, входящие в *BRICS* (*Brazil, Russia, India, China, South Africa*), являются активными участниками процесса цифровизации в политической, экономической, социальной и военной сферах, а также в деятельности объединения, направленной на расширение технологий ИИ и коммуникационных каналов. Однако бурный рост новейших технологий на основе ИИ ставит под угрозу и без того уязвимый сектор кибербезопасности и, к сожалению, предоставляет широкие возможности для активного проведения информационно-психологических и террористических операций, дезинформационных компаний, направленных на подрыв работы политических акторов *BRICS*.

Ключевые слова: *BRICS*, технологии искусственного интеллекта, кибербезопасность, IV промышленная революция, информационно-психологическая безопасность, цифровая трансформация.

DOI: 10.31857/S0044748X0029114-4

Статья поступила в редакцию 19.08.2023.

Бурный рост технологий искусственного интеллекта (ИИ) в последние годы подтолкнул мировой коммуникационный процесс к виртуализации общественной жизни и изменил международные тенденции внешнеполитического взаимодействия на глобальном уровне. Информационно-технологическая революция помогла ряду стран *BRICS* (*Brazil, Russia, India, China, South Africa*), в частности, Китаю и Индии, стать ключевыми игроками на рынке цифровых и информационно-коммуникационных услуг, получающими огромные дивиденды и грамотно выстраивающими

Екатерина Алексеевна Виноградова — кандидат политических наук, директор Научно-исследовательского центра: технологии искусственного интеллекта в международных отношениях (НИЦТИИМО) (https://orcid.org/0000-0001-8055-6612, vinogradovacatherine7@gmail.com).

цифровую экономику. В будущем это может благоприятно отразиться на деятельности государств, входящих в объединение, которые перестанут испытывать острую цифровую зависимость от внешнего технологического давления со стороны США и смогут обрести цифровой суверенитет, который будет способствовать гармоничному развитию цифровой экономики развивающихся стран. Внедрение технологий ИИ в деятельность объединения является актуальной задачей для стран *BRICS* и активно обсуждается на многочисленных встречах.

На сегодняшний день тема использования технологий искусственного интеллекта (ИИ) в *BRICS* мало изучена. Научную литературу по данной проблематике условно можно разделить на несколько групп. К первой группе относятся работы, авторы которых изучают имежрегиональное сотрудничество *BRICS* в области развития цифровых технологий. Здесь необходимо выделить статью А.Игнатова «Повестка дня БРИКС по управлению Интернетом» [1], в которой представлен анализ приоритетов стран *BRICS* в отношении управления Интернетом. В работе исследователей Д.Саймана, Е.Громовой, Е.Юхнявичюса «Регулирование искусственного интеллекта в БРИКС и Европейском союзе» [2] детально рассмотрены проблемы использования технологий ИИ и предложены решения по оптимизации положений законодательства в этой сфере. Особенности цифровой экономики в странах *BRICS* анализируются в статье исследователей И.Лазанюка и С.Ревиновой [3]. Изучение эволюции индикаторов, упрощение процедур торговли стран *BRICS* при помощи цифровых технологий представлено в исследовании бразильских ученых М.Мартинса и С.Алмейда Биспо [4].

Во вторую группу входят труды отечественных и зарубежных специалистов, изучающих киберугрозы, направленные на подрыв различных видов деятельности в странах *BRICS.* Основные риски и угрозы, связанные с национальной и международной психологической безопасностью, и злонамеренное использование искусственного интеллекта в странах объединения рассмотрены в работе российских ученых Д.Ю.Базаркиной и Е.Н.Пашенцева [5]. В статье индийского политолога Э.Дилипрадж «Кабель БРИКС и кибербезопасность» [6] проанализирована злонамеренная деятельность с использованием американской программы *PRISM*, направленная на установление массовой электронной слежки в государствах, входящих в *BRICS*. Подробный анализ аспектов кибербезопасности в этих государствах и новейшего законодательства по защите данных представлен в монографии бразильского профессора Луки Белли [7]. В диссертации другого бразильского ученого С.М.Пиньейру де Резенде [8] рассмотрена такая технология искусственного интеллекта, как дипфейк *(deepfake)*, а также его роль в дискредитации политических лидеров Бразилии.

Целями данного исследования являются определение стратегии *BRICS* в ходе использования передовых технологий ИИ для развития цифровой коммуникации между странами-участницами, а также классификация основных киберугроз и информационно-психологических операций, направленных на подрыв деятельности объединения.

Методология исследования основана на системном подходе, направленном на изучение технологий ИИ, задействованных в цифровизации *BRICS* и классификации новых видов киберугроз. В статье задействованы следующие

группы источников: статистические данные зарубежных и российских исследовательских лабораторий, законодательные документы *BRICS* (декларации, стратегии, материалы межправительственных встреч, дорожные карты), СМИ, научные работы зарубежных и отечественных исследователей.

В данной статье применялись следующие методы исследования: *case study* для детального изучения технологий искусственного интеллекта в работе *BRICS*; метод классификации для систематизации основных киберугроз, представляющих опасность для *BRICS*.

НАЦИОНАЛЬНЫЕ СТРАТЕГИИ ПО ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ В СТРАНАХ *BRICS*: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

В период с 2017 по 2021 г. происходит планомерное внедрение технологий ИИ в государственный сектор стран *BRICS*, обусловленное принятием национальных стратегий по ИИ. Эти документы послужили своего рода отправной точкой в создании новой цифровой эры для ряда государств, входящих в *BRICS*.

Национальная стратегия по ИИ в Китае

В 2017 г. Китай принял национальную стратегию по ИИ на период до 2030 г., став первой страной *BRICS*, обозначившей свою концепцию по развитию технологий ИИ. В документе особое внимание уделяется экономическому развитию, конкурентоспособности и социальному управлению [9]. Этот документ часто появляется в СМИ как основополагающий этап в развитии ИИ в Китае и является предметом политического анализа.

Согласно национальному плану, главной целью китайской стратегии в области ИИ является превращение страны к 2030 г. в главный международный центр инноваций [10, p. 301] с валовым объемом производства новой отрасли ИИ, превышающим 1 трлн юаней [11, p. 10]. В основе этой политики лежит стремление стать самодостаточным в производстве технологий ИИ за счет снижения зависимости от иностранных технологий и зарубежного опыта. Это направление приобрело особую значимость после экспортных ограничений со стороны США, введенных в 2020 г., показавших серьезную уязвимость китайского технологического рынка, развитие которого напрямую зависит от решений главного конкурента в лице Соединенных Штатов. Политика Вашингтона в области технологической изоляции Китая получила в научной литературе название «Война чипов», цель которой — отрезать страну от передовых технологий и оборудования для производства чипов [12]. Это привело к новому этапу развития китайской технологической стратегии: в 2021 г. сразу несколько крупнейших технологических компаний Китая (*Baidu, Alibaba, Huawei, Xiaomi* и *Oppo*) приступили к разработкам отечественных чипов [13].

Рынок ИИ в Китае стремительно развивается с 2015 г. Ожидается, что к 2024 г. его ежегодный темп роста будет на уровне 20%, а объем рынка составит 70,2 млрд долл. [14]. По масштабу он занимает второе место в мире после США.

Важной особенностью китайской стратегии в области ИИ является также разработка комплексной политической основы для развития технологий ИИ, в которой задействованы центральные и местные органы власти, част-

ный сектор и исследовательские организации [9, p. 42], где основной акцент делается на развитие специальной образовательной среды. ИИ как самостоятельная дисциплина изучается в ряде университетов страны и финансируется крупными технологическими компаниями. Что касается частного сектора, то Китай выбрал «национальных чемпионов в области ИИ». Например, *Baidu* было поручено разработать технологии автономного вождения, *Alibaba* — систему умных городов, *Tencent* — умное зрение для медицинской диагностики [15, p. 62].

Таким образом, в последние годы одной из основных задач Китая в области ИИ является создание технологий ИИ нового поколения для открытия новых технологических возможностей в целях развития страны, защиты ее национальной безопасности и роста конкурентоспособности.

Национальная стратегия по ИИ в Индии

Индия определила национальную политику в области искусственного интеллекта в 2018 г. в рабочем документе «Национальная стратегия в области искусственного интеллекта *AI for All*» [16]. В целом документ направлен на реализацию следующих целей: использование ИИ для экономического роста; применение ИИ для социального развития инклюзивного роста; развитие Индии как «международной станции ИИ».

На сегодняшний день Индия сталкивается с рядом проблем: отсутствие эффективных экосистем данных, малое количество исследований по ИИ, недостаточность навыков в работе с технологиями ИИ [17, p. 24].

Среди важнейших шагов на пути реализации национальной стратегии Индии в области ИИ можно выделить такие приоритетные области, как промышленность, здравоохранение, образование, сельское хозяйство, умные города и инфраструктура. 30 мая 2020 г. правительство Индии запустило национальный портал искусственного интеллекта (www.ai.gov.in), функционирующий как универсальная цифровая платформа разработок, связанных с искусственным интеллектом, обеспечивающая обмен между инвестиционными фондами, компаниями и образовательными учреждениями, работающими в сфере искусственного интеллекта. Правительство запустило также национальную программу для молодежи «Ответственный искусственный интеллект» для предоставления студентам соответствующих ресурсов для научно-исследовательской работы в области ИИ [18].

Индия применила уникальный подход к своей стратегии в области ИИ, сосредоточив внимание не только на экономическом росте, но и на социальной интеграции. Ярким примером является разработка специальных чат-ботов для обслуживания клиентов банков, образовательной среды и правительственных порталов [19, p. 4926].

Национальная стратегия по ИИ в России

В 2019 г. в России была утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 г. Она является основой для разработки государственных программ, федеральных и региональных проектов, касающихся развития ИИ [20].

За последние годы в стране сложился огромный потенциал для того, чтобы Россия стала одним из мировых лидеров в развитии и использовании технологий ИИ, чему способствуют высокий уровень базового физико-математического образования, сильная естественно-научная школа, наличие компетенций в области моделирования и программирования и высокоразвитая базовая информационно-коммуникационная инфраструктура (развитие радиотелефонной связи третьего и четвертого поколений) и доступность мобильной передачи данных [21].

По оценкам Национального центра развития искусственного интеллекта при Правительстве РФ, лидерами по внедрению технологий искусственного интеллекта являются финансовый сектор, организации ТЭК, промышленный сектор, транспортная отрасль, здравоохранение [22]. Для развития рынка ИИ в стране в 2020 г. был создан специальный федеральный проект «Цифровая экономика».

Национальная стратегия по ИИ в Бразилии

Бразильская государственная стратегия по искусственному интеллекту (*Estratégia Brasileira de Inteligência Artificial, EBIA*) была сформулирована в 2021 г. Она направлена на развитие образования, научно-исследовательских организаций, налогообложения [23]. В качестве примера передовых разработок в области ИИ в госсекторе можно выделить государственный проект *Paraná Inteligência Artificial (PIA)* для города Парана, ориентированный на предоставление услуг гражданам через специальную платформу и приложение на базе ИИ. Платформа объединяет более 380 государственных служб в одном месте и является каналом для коммуникации населения с госорганами [24].

За последние несколько лет министерство науки, технологий и инноваций Бразилии разработало несколько проектов, связанных с ИИ, среди которых можно выделить создание центров прикладных технологий, ориентированных на ИИ, и инициатив по технологическому предпринимательству на основе ИИ [24].

Согласно данным *CNPq Lattes Platform,* специалисты в сфере искусственного интеллекта работают по большей части в федеральных исследовательских центрах и университетах, и их почти нет в технологических компаниях [24]. Наиболее активно технологии ИИ внедряют коммерческие фирмы. На региональном уровне Бразилия лидирует по инвестициям, задействованным ресурсам и разнообразию сфер применения технологий ИИ [25, с. 43]. Однако одной из ключевых проблем, затрудняющих внедрение технологий ИИ в государственный сектор, по мнению бразильских ученых Уолтера Б.Госпара и Ясмина Курзи де Мендосы, является отсутствие четкого описания структуры управления ИИ, а также точных целей и сроков реализации стратегии [26, p. 8].

Национальная стратегия по ИИ в ЮАР

ЮАР — единственная страна *BRICS*, где не существует четко сформулированной государственной стратегии по ИИ. Ее предтечей является

лишь доклад Президентской комиссии по четвертой промышленной революции, опубликованный в 2020 г., где ИИ признается одной из высокотехнологичных отраслей, в которых страна «серьезно отстает».

Тем не менее ЮАР занимает лидирующие позиции среди стран Африки по объему внедрения технологий ИИ в работу коммерческих структур. На данный момент 726 компаний страны задействуют в своей работе технологии ИИ. Кроме того, ЮАР имеет самые высокие баллы среди других африканских стран по индексу готовности правительства к использованию ИИ [27]. В стране действуют несколько передовых центров: сетевой международный Центр исследований в области искусственного интеллекта (*Artificial Intelligence in South Africa, CAIR*); Центр четвертой промышленной революции, созданный 23 декабря 2021 г. министерством науки и инноваций ЮАР и управляемый Советом по научным и промышленным исследованиям *(Council for Scientific and Industrial Research, CSIR*) [28]. Одной из целей *CSIR* является повышение конкурентоспособности ЮАР за счет перехода к цифровой экономике.

Технологии ИИ активно применяются в ЮАР для развития социальной сферы и, в частности, системы здравоохранения. В качестве примера можно привести работу Национального департамента здравоохранения, создавшего специального чат-бота *MomConnect* для виртуального ведения беременности, услугами которого воспользовались уже 1,8 млн женщин [29].

СОТРУДНИЧЕСТВО СТРАН *BRICS* В ОБЛАСТИ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Лидеры государств, входящих в *BRICS*, рассматривают цифровизацию как новую возможность для укрепления сотрудничества и расширения партнерских отношений [7]. Одной из приоритетных задач является создание целевой группы по цифровым технологиям, которая сможет дать возможность странам *BRICS* обрести цифровой суверенитет и выбрать независимый путь для гармоничного построения цифровой экономики.

BRICS обладает всеми преимуществами, которые есть у межрегиональных организаций. Созданный в 2014 г. Новый банк развития *BRICS* (*New Development Bank, NDB*) представляет собой институциональную структуру, сформированную по типу неформального клуба [30, p. 36]; банк доказывает свою устойчивость и способность принимать коллективные решения, несмотря на политические и экономические разногласия между некоторыми членами организации [1, p. 89].

Цифровой разрыв стран *BRICS* на сегодняшний день является барьером для внедрений технологий ИИ в работу объединения. Решение этой проблемы стало важным пунктом Стратегии энергетического партнерства *BRICS* до 2030 г., выпущенной 20 ноября 2020 г. Согласно документу, страны объединения в ближайшие годы собираются устранить цифровой разрыв путем преодоления неравномерности в доступе населения государств *BRICS* к цифровой инфраструктуре, навыкам и услугам, а также путем повышения цифровой инклюзивности населения, проживающего в сельских районах, и людей с ограниченными возможностями посредством улучшения условий доступа к Интернету [31].

Согласно статистическим данным, в период 2020—2023 гг. политика в области преодолении цифрового разрыва путем доступа к сети Интернет становится более активной. В Бразилии в 2020 г. доля населения, пользующегося Интернетом, составляла 81,34% [32], а к 2023 г. она выросла почти на 3 п.п., составив 84,3% [33]. В ЮАР в 2020 г. этот же показатель был равен 67,91%, к 2023 г. он вырос до 82,2% [34]. В России в 2020 г. доля интернет-пользователей составляла 84,99% [35], к 2023 г. — 88,2% [36]. В Индии в 2020 г. доступ к Интернету имели 45% жителей страны [37], к 2023 г. — 48,7% [38]. В Китае в 2020 г. тот же показатель равнялся 70,4%, а к 2023 г. вырос почти на 6%, достигнув 76,4% [39].

С 2014 г. страны *BRICS* планомерно сотрудничают в цифровой сфере. Ярким примером может послужить созданный в 2014 г. Сетевой университет *(BRICS Network University)* — образовательный проект, состоящий из учебных организаций высшего образования стран-участниц.

В 2022 г. в рамках цифрового сотрудничества был проведен первый конкурс «Инженерные технологии искусственного интеллекта» для развития навыков и технологических инноваций по программе «Один пояс, один путь», направленный на построение качественных партнерских отношений и содействие глобальному развитию [40].

Говоря о сотрудничестве стран *BRICS* в области развития технологий ИИ, необходимо отметить совместную работу институтов судебной власти. В октябре 2019 г. состоялся практический семинар высших судов государств, входящих в *BRICS*, на котором детально изучался уникальный опыт Бразилии по внедрению технологий искусственного интеллекта в судебные органы страны. Участники семинара представили разработки виртуальной реальности для проведения коллегиального судебного заседания в рамках так называемого виртуального пленума, который ко всему прочему позволяет следить за результатами голосований судей в режиме реального времени на веб-сайте суда, что гарантирует прозрачность и публичность принимаемых решений [41].

Новаторской технологией на основе ИИ в бразильской судебной системе также является инструмент для консультаций по судебной практике, который используется для облегчения доступа к решениям суда в более удобной цифровой среде. Инструмент на основе ИИ *VICTOR* является передовой разработай бразильских судов и университета Бразилиа и предназначен для выявления неординарных обращений, связанных с вопросами, имеющими общественный резонанс. Данный инструмент повышает эффективность судебного анализа и значительно экономит время и человеческие ресурсы. Ряд задач, которые судебные органы выполняют в среднем за 44 минуты, *VICTOR* решает менее чем за пять секунд [41].

Количество совместно принимаемых решений *BRICS* в области содействия цифровому росту и развитию ИКТ на протяжении ряда лет стабильно растет, а уровень их исполнения достиг отметки в 74% [42, p. 88].

Развитие технологий ИИ в странах *BRICS* активно обсуждалось 17 сентября 2020 г. в рамках шестой встречи министров стран — членов организации. Важным пунктом декларации, принятой по итогам встречи, стал тезис о «содействии ускорению инклюзивного экономического роста и реализации цели в области устойчивого развития» при помощи технологий

ИИ, а также их «способности приносить большую пользу маргинализированным обществам стран *BRICS* » [43].

14 октября 2020 г. была выпущена дорожная карта *BRICS* до 2025 г., направленная на активное расширение стратегического партнерства стран-участниц в области энергетики при помощи цифровых технологий на основе ИИ [44]. Среди перспективных направлений можно выделить совместные разработки виртуальной реальности и комплексного анализа данных ИИ. В мае 2022 г. на девятой встрече министров стран *BRICS* особое внимание было уделено применению технологий ИИ для «ускорения цифровой трансформации в области образования и политической среды» [45].

ЗЛОНАМЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОВЕДЕНИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ОПЕРАЦИЙ И КИБЕРАТАК В СТРАНАХ *BRICS*

Политика *BRICS* в сфере информационной безопасности является одним из важнейших направлений в работе объединения. В 2013 г. во время заседания 68 генеральной ассамблеи ООН речь президента Бразилии Дилмы Руссефф (2011—2016 гг.) была посвящена осуждению американской программы массовой слежки *PRISM* [6]. Бразильского лидера поддержали государства — участницы *BRICS*. Несанкционированное использование информационных ресурсов со стороны США в странах *BRICS* в 2013 г. показало наличие пассивной угрозы информационной безопасности. Именно в этот период началось активное сотрудничество объединения в сфере кибербезопасности.

В 2018 г. по итогам состоявшегося в Йоханнесбурге саммита *BRICS* была принята декларация, в которой фигурировал пункт о создании объединенной киберполиции. Несколькими годами позже был запущен проект *Cyber BRICS* для разработки нормативных актов и предложений по политике в области управления кибербезопасностью (включая использование персональных данных), политики доступа в Интернет и стратегий цифровизации государственного управления в странах *BRICS* [46].

Самым опасным видом киберугроз признаны угрозы, направленные на нарушение нормального процесса функционирования той или иной системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы [47, с. 28]. В последние годы передовым инструментом для подобного вида киберугроз являются так называемые фишинговые атаки, цель которых заключается в получении доступа к конфиденциальным данным пользователей путем проведения массовых рассылок электронных писем от имени популярных брендов и цифровых агентств, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. За последние годы данный вид киберугроз в странах *BRICS* является предметом постоянных обсуждений на различных саммитах.

Целая серия крупных фишинговых атак на банковский сектор потрясла Южную Африку в 2005 г. [48]. С 2020 г. Бразилия является мировым лидером по фишинговым атакам: каждый пятый интернет-пользователь в стране хотя бы раз подвергался нападению [49]. 9 февраля 2023 г. была совершена крупнейшая фишинговая атака на популярный сайт социальных

новостей *Reddit* в Индии. По данным портала, после получения доступа к учетным данным сотрудника, злоумышленнику стали доступны внутренние документы, информационные панели, бизнес-системы и код. Атака привела к раскрытию контактной информации сотен пользователей, сотрудников компании и информации о рекламодателях [50]. В марте 2023 г. была раскрыта деятельность хакерской группы по шпионажу, нацеленная на взлом данных китайской атомной энергетики [51]. В июне 2023 г. Лаборатория Касперского заявила о новой мошеннической схеме киберпреступников, которые запускают фишинговые атаки в России при помощи *ChatGPT*. По итогам первого квартала 2023 г., по данным Роскомнадзора, в России было удалено и заблокировано более 7,2 тыс. фишинговых ресурсов, что намного превышает прошлогодние показатели [52]. В этой связи кибербезопасность стала одним из важнейших приоритетов, обозначенных лидерами стран *BRICS* на тринадцатом саммите организации, состоявшемся 9 сентября 2021 г. Согласно компендиуму, выпущенному по итогам встречи, были разработаны рекомендательные тезисы для каждой страны-участницы в области защиты финансовых учреждений от различного рода кибератак [53].

По мере усовершенствования технологий ИИ расширяется сфера и частота их применения в информационно-психологических операциях, направленных на подрыв деятельности политических институтов в странах *BRICS*. Российские исследователи Д.Ю.Базаркина, Е.Н.Пашенцев в своей статье «Злонамеренное использование искусственного интеллекта. Новые риски психологической безопасности в странах БРИКС» выделяют следующие виды угроз от использования технологий ИИ: «фишинг ИИ, а также использование дипфейков и умных ботов в информационных компаниях для различных целей, например для подмывания репутации оппонента, будь то человек, организация или даже страна» [5, p. 155].

Так, злонамеренное использование технологии дипфейк в последние годы было направлено против репутации целого ряда государственных деятелей стран *BRICS* для влияния на выборы и репутацию действующих политиков. В 2020 г. политический дипфейк оказал повлиял на выборы в Индии [54]. За период 2018—2022 гг. Бразилия стала лидером среди стран *BRICS* по количеству дипфейк-атак на политических лидеров страны. Один из последних политических дипфейков с элементами доксинга был направлен на президента Луиса Инасиу Лула да Силва (2003—2011, 2023—н/в). 5 августа в социальных сетях появилось фальшивое видео, где популярная телеведущая Рената Васконселлос якобы дает ложную информацию об итогах голосования на президентских выборах [55, с. 40].

В марте 2023 г. провокационный политический дипфейк был направлен против действующего президента ЮАР. На видео, опубликованном в *Twitter*, президент ЮАР Сирил Рамафоса (2018—н/в) якобы обращается к стране, излагая «ложный план правительства» по преодолению продолжающегося энергетического кризиса [56]. В июне 2023 г. жертвой злонамеренного политического дипфейка стал российский президент В.В.Путин (2000—2008, 2012 — н/в). В ложном видеоролике транслировалось «обращение Путина» о введении военного положения в ряде областей России. Вирусный ролик был показан не только в российских соцсетях, но и в эфире межгосударственной телерадиокомпании «Мир», сервер которой был взломан злоумышленни-

ками для размещения провокационного видео [57]. На сегодняшний день Китай является единственной среди стран *BRICS*, которая не только регламентирует дипфейки на законодательном уровне, но и ввела специальное ограничение ИИ для использования изображений действующего президента страны Си Цзиньпина (2012 — н/в) для создания дипфейк роликов [58].

Активное использование чат-ботов для влияния на выборы в ряде стран *BRICS* было отмечено в период 2014—2019 гг. Расследование, проведенное компанией *Superlinear* в ЮАР, раскрыло политические манипуляции целого ряда международных ультраправых организаций в период 2014—2018 гг., которые действовали в социальной сети *Twitter* посредством чат-ботов и так называемых «троллей», распространяя расистский контент и призывы к госпереворотy [59]. В Бразилии политические чат-боты оказывали существенное влияние на выборы в 2014 и 2019 гг. [25, с. 42].

Одной из ключевых проблем для интеграции стран *BRICS* в сфере информационно-психологической и кибербезопасности является американская информационная кампания, направленная на дискредитацию ряда государств *BRICS*, в частности Китая и России, в глазах стран — участниц объединения. Антироссийская и антикитайская риторика в последние годы неоднократно фигурировала в ряде американских стратегических документов. Например, в «Заключительном отчете Комиссии национальной безопасности по искусственному интеллекту» от 1 марта 2021 г. указывалось, что «искусственный интеллект усиливает угрозы, создаваемые кибератаками и кампаниями по дезинформации, которые Россия, Китай и другие государственные и негосударственные субъекты используют для проникновения в американское общество, кражи данных и для вмешательства в демократию США» [60]. Во-вторых, согласно Стратегии национальной безопасности США, опубликованной в октябре 2022 г., главные военные угрозы для американцев представляют Китай и Россия. В тексте доклада США делают попытки в очередной раз подорвать международный авторитет России, обвинив ее в организации кибератак «для подрыва способности стран предоставлять услуги гражданам во всем мире». Китай, согласно документу, использует свой технологический потенциал и растущее влияние на международные институты, чтобы создать более благоприятные условия для своей авторитарной модели, а также для того, чтобы «изменить глобальное использование технологий в пользу своих интересов и ценностей» [61]. Кроме того, большинство американских научных статей в области ИИ носят дискредитирующий характер в отношении Китая и России, что тормозит сотрудничество стран *BRICS* в этом направлении.

Серьезные опасения вызывает также февральское заявление минобороны США, в котором подчеркивается намерение вести интернет-пропаганду и организовывать злонамеренные дезинформационные онлайн-кампании при помощи дипфейков для оказания психологического воздействия на граждан других стран [62]. Эти действия ставят под угрозу информационно-психологическую безопасность в странах *BRICS*, некоторые из которых являются серьезными конкурентами США в сфере цифровой экономики и производстве технологий ИИ.

Уязвимость таких стран, как Бразилия, ЮАР, Индия в области использования ИИ обусловлена также их зависимостью от американских техноло-

гических гигантов, которые являются основными поставщиками передовых технологий ИИ в вышеперечисленных странах.

В последние годы государства *BRICS* стали глобальными лидерами в области цифровых технологий, планомерно внедряющими ИИ в государственные, экономические и социальные сектора своих стран и в работу объединения. В качестве прогрессивных начинаний можно выделить преодоление цифрового разрыва путем роста количества интернет-пользователей в странах *BRICS* , а также совместные разработки в области кибербезопасности.

Важным направлением сотрудничества государств, входящих в *BRICS*, является выстраивание собственной концепции в области кибербезопасности. Целая серия фишинговых атак, имевших место в странах объединения в 2023 г., актуализирует проблемы, связанные со своевременным реагированием на возрастающие киберугрозы нового поколения.

Ключевой проблемой, тормозящей работу по внедрению технологий ИИ в деятельность *BRICS*, является заметное цифровое отставание некоторых стран объединения, в частности Бразилии и ЮАР, которые используют цифровые услуги и технологии ИИ, предоставляемые им американскими технологическими компаниями. Кроме того, цифровая коммуникация осуществляется посредством тех же американских социальных сетей, являющихся площадками для проведения информационно-психологических операций в странах *BRICS.* Серьезную угрозу для объединения представляет нерегламентированная политика в области применения технологий ИИ, оказывающих влияние на политические институты страны.

Распространение ложно-негативного образа Китая как ведущей страны мира в области разработок ИИ также является барьером для изучения и применения китайских технологий ИИ в киберсфере стран *BRICS*. По результатам проведенного анализа автор предлагает следующие рекомендации:

— разработка общей для стран *BRICS* законодательно-правовой основы для регулирования применения ряда технологий ИИ (дипфейков, чат-ботов) в политической сфере. За основу могут быть взяты китайские нормативно-правовые наработки в области ограничения дипфейков во время проведения выборов;

— создание на базе сетевого университета *BRICS* лабораторий для разработок дипфейк-детекторов и других инструментов, выявляющих дезинформационные провокации, осуществляемые при помощи технологий ИИ;

— создание информационно-коммуникационных каналов (социальных сетей, новостных платформ) для расширения сотрудничества стран *BRICS*;

— разработка национальных чат-ботов и введение ограничения на использование чат-бота *GPT* в связи с участившимися случаями его злонамеренного использования как инструмента фишинговых атак и дезинформационной деятельности в странах *BRICS;*

— активное сотрудничество между ведущими научными и образовательными центрами, занимающимися разработками технологий ИИ.

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

1. Ignatov A. The BRICS Agenda on Internet Governance. *International Organisations Research Journal*, Moscow, 2022, Vol. 17(2), pp. 86–109. (DOI:10.17323/1996-7845-2022-02-04).

2. Cyman D., Gromova E., Juchnevicius E. Regulation of Artificial Intelligence in BRICS and the European Union. *BRICS Law Journal,* Tyumen, 2021, Vol. 8(1), pp. 86-115 (DOI:10.21684/2412-2343-2021-8-1-86-115).

3. Lazanyuk I., Revinova S. Digital economy in the BRICS countries: myth or reality? 1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019). *Advances in Economics, Business and Management Research*, Paris, 2019, Vol. 105, pp.510-514. (DOI:10.2991/iscde-19.2019.97).

4. Martins M., Almeida Bispo S. Facilitação de comércio e tecnologias digitais: análise para os países do BRICS. *Boletim de Economia e Política Internacional*. BEPI, Vol. 33, 2022, pp.59-86. (DOI: http://dx.doi.org/10.38116/bepi33art3).

5. Bazarkina D.Y., Pashentsev E.N. Malicious Use of Artificial Intelligence. New Psychological Security Risks in BRICS Countries. *Russia in Global Affairs*, Moscow, 2020, Vol. 18, N 4, pp.154-177. (DOI:10.31278/1810-6374-2020-18-4-154-177).

6. Dilipraj E. BRICS cable and cyber security. Available at: https://www.academia.edu/7531188/BRICS_CABLE_AND_CYBER_SECURITY (accessed 07.09.2023).

7. Belli L. Cyber BRICS: Cybersecurity Regulations in the BRICS Countries. Available at: https://cyberbrics.info/wp-content/uploads/2020/11/CyberBRICS-Book-FINAL-author-version.pdf (accessed 17.06.2023).

8. 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.

9. Johansson A.C. China's AI ecosystem. Stockholm School of Economics, Stockholm, 2022, 68 p.

10. Knox J. Artificial intelligence and education in China. *Learning, Media and Technology*. 2020, pp. 298-311. (DOI: https://doi.org/10.1080/17439884.2020.1754236).

11. Ding J. Deciphering China's AI Dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI. Centre for the Governance of AI, Future of Humanity Institute, University of Oxford, 2018, 44p.

12. Chiang Sh. China's top chipmaker will 'struggle' to make cutting-edge chips competitively. Available at: https://www.cnbc.com/2023/04/28/chinas-smic-may-struggle-to-make-cutting-edge-chips-competitively.html (accessed 11.06.2023).

13. Yang Z. Chinese companies are making their own semiconductors. Available at: https://www.protocol.com/china/chinese-companies-make-own-semiconductors (accessed 21.06.2023).

14. Artificial Intelligence – China. Available at: https://www.statista.com/outlook/tmo/artificial-intelligence/china (accessed 14.06.2023).

15. Roberts H., Cowls J., Morley J., Taddeo M., Wang V., Floridi L. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society*, London, 2021, Vol 36, pp.59–77. (DOI: https://doi.org/10.1007/s00146-020-00992-2).

16. Government of India. Minister of Electronics and Information Technology Lok Sabha starred question no. *461 to be answered on: 05.04.2023. Available at: https://pqals.nic.in/annex/1711/AS461.pdf (accessed 21.06.2023).

17. Kumar A. National AI Policy. Strategy of India and China: A Comparative Analysis. India Habitat Centre Lodhi Road, New Delhi, 2021, 40p.

18. Artificial Intelligence (AI) Policies in India-A Status Paper Future Networks (FN). Division, Telecommunication Engineering Center, Janpath, New Delhi. August 2020. Available at: https://www.tec.gov.in/pdf/Studypaper/AI%20Policies%20in%20India%20A%20status%20Paper%20final.pdf (accessed 23.06.2023).

19. Malik P., Kavita D., Singal K. AI initiatives by Indian Government: Journey towards becoming global technology leader. *Journal of Critical Reviews,* 2020, Vol. 7(19), pp. 4921-4930.

20. Национальная стратегия развития искусственного интеллекта на период до 2030 года. Available at: https://standartgost.ru/g/pkey-14293726917?ysclid=lmoo4tenr218003898 (accessed 29.06.2023).

21. Замминистра Оксана Тарасенко в интервью CNews — о развитии искусственного интеллекта в России. Министерство экономического развития РФ. 09.02.2021. Available at: https://www.economy.gov.ru/material/news/zamministra_oksana_tarasenko_v_intervyu_cnews_o_razvitii_iskusstvennogo_intellekta_v_rossii.html?ysclid=lmooh0k7wp462593172 (accessed 29.06.2023).

22. Внедрение искусственного интеллекта: как государство подцеживает отрасль. *РБК*. 21.11.2022. Available at: https://www.rbc.ru/technology_and_media/21/11/2022/6373b9d99a7947fa230d041d (accessed 27.06.2023).

23. Summary of the Brazilian Artificial Intelligence Strategy. EBIA. 2021. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf (accessed 23.06.2023).

24. Órgão: Ministério da Ciência, Tecnologia e Inovações Gabinete do Ministro PORTARIA GM Nº 4.617, 6 abril 2021. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria_mcti_4-617_2021.pdf (accessed 17.06.2023).

25. Виноградова Е.А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке. *Латинская Америка*, М, 2023, № 3, сс. 34-48. [Vinogradova E.A. Tekhnologii iskusstvennogo intellekta i narastayushchiye kiberugrozy v Latinskoy Amerike. [Artificial intelligence technologies and the rise of cyber threats in Latin America]. *Latinskaya Amerika*, Moscow, 2023, N 3, pp. 34-48. (In Russ.). (DOI: 10.31857/S0044748X0024415-5).

26. Gaspar W., de Mendonça Y. Artificial Intelligence in Brazil still lacks a strategy. Report by the Center for Technology and Society at FGV Law School. Available at: https://cyberbrics.info/wp-content/uploads/2021/05/EBIA-en-2.pdf (accessed 23.08.2022).

27. Artificial intelligence in Africa: National strategies and initiatives. Available at: https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-national-policies/ (accessed 21.08.2023).

28. Centre for the Fourth Industrial Revolution. Available at: https://centres.weforum.org/centre-for-the-fourth-industrial-revolution/southafrica (accessed 21.06.2023).

29. Jaldi A. Artificial Intelligence Revolution in Africa: Economic Opportunities and Legal Challenges. *Policy Paper*, 2023. Available at: https://www.policycenter.ma/sites/default/files/2023-07/PP_13-23%20%28Jaldi%20%29.pdf (accessed 30.07.2023).

30. Cooper A. F., Farooq A. B. Testing the Club Dynamics of the BRICS: The New Development Bank from Conception to Establishment. *International Organisations Research Journal*, Moscow, 2015, Vol. 10(2), pp. 39–58. Available at: (DOI: https://doi.org/10.17323/1996-7845-2015-02-39).

31. Strategy for BRICS Economic Partnership 2025. Available at: https://www.economy.gov.ru/material/file/3a71260309ef290a0cfa3fe698a55e83/Strategy%20for%20BRICS%202025.pdf?ysclid=lmdjae22do334659164 (accessed 9.07.2023).

32. Percentage of population using the internet in Brazil from 2000 to 2022. Available at: https://www.statista.com/statistics/209106/number-of-internet-users-per-100-inhabitants-in-brazil-since-2000/ (accessed 10.07.2023).

33. Digital 2023: Brazil. Available at: https://datareportal.com/reports/digital-2023-brazil (accessed 11.07.2023).

34. Mobile internet user penetration in South Africa from 2019 to 2028. Available at: https://www.statista.com/statistics/972866/south-africa-mobile-internet-penetration/ (accessed 15.07.2023).

35. Share of population using the internet in Russia from 2000 to 2021. Available at: https://www.statista.com/statistics/255129/internet-penetration-in-russia/ (accessed 12.07.2023).

36. Digital 2023 Global Overview Report. Available at: https://datareportal.com/reports/digital-2023-global-overview-report (accessed 20.07.2023).

37. Internet penetration rate in India 2007-2022. Available at: https://www.statista.com/statistics/792074/india-internet-penetration-rate/ (accessed 18.07.2023).

38. Digital 2023: India. Available at: https://datareportal.com/reports/digital-2023-india#:~:text=Internet%20use%20in%20India%20in,at%20the%20start%20of%202023 (accessed 24.07.2023).

39. Penetration rate of internet users in China from 2012 to H1 2023. Available at: https://www.statista.com/statistics/236963/penetration-rate-of-internet-users-in-china/ (accessed 27.07.2023).

40. 2022一带一路暨金砖国家技能发展与技术创新大赛 【人工智能工程技术 （边缘计算）】赛项技术规程 金砖国家工商理事会（中方） 技能发展 工作组一带一路暨金砖国家技能发展与技术创新大赛组委会 竞赛技术委员会专家组制定 2022 年5 月 Available at: http://www.chinajxedu.com/uploadfile/ 2022/0527/20220527053945589.pdf (accessed 29.07.2023).

41. Seminário das Altas Cortes dos BRICS «Tecnologia da Informação e Inteligência Artificial: boas práticas, oportunidades e desafios para o Judiciário». 25 outubro 2019. Conferência inaugural Tema: «Tecnologia da informação e inteligência artificial no Judiciário brasileiro, com ênfase na cidadania: boas práticas e novos desafios». Available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.conjur.com.br%2Fdl%2Fdiscurso-toffoli-evento-brics.docx&wdOrigin=BROWSELINK (accessed 10.06.2023).

42. Larionova M.V., Rakmangulov M.R., Shelepov A.V. Explaining G20 and BRICS Compliance. *International Organisations Research Journal*, Moscow, 2016, Vol. 11(2), pp. 86–111. (DOI: https://doi.org/10.17323/1996-7845-2016-03-99).

43. Declaration of the 6th BRICS Communication Ministers Meeting 17 September 2020, Russian Federation. Available at: https://brics2021.gov.in/BRICSDocuments/2020/Declaration%20of%20the%206th%20BRICS%20Communication%20Ministers%20Meeting.pdf (accessed 11.07.2022).

44. Road Map for BRICS Energy Cooperation up to 2025. Available at: https://brics2021.gov.in/BRICSDocuments/2020/Road%20Map%20for%20BRICS%20Energy%20Cooperation%20up%20to%202025.pdf (accessed 19.07.2022).

45. Declaration of the 9th Meeting of BRICS Ministers of Education 26 May, 2022. Available at: http://brics2022.mfa.gov.cn/eng/hywj/ODMM/202206/P020220607349467952397.pdf (accessed 19.07.2022).

46. Cyber BRICS. Available at: https://cyberbrics.info/about-us/ (accessed 13.07.2023).

47. Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере. *Стратегия гражданской защиты: проблемы и исследования*, М, 2014, № 1(6), сс. 21–34. [Faleyev M.I., Chernykh G.S. Ugrozi natsionalnoy bezopasnosti gosudarstva v informatsionnoy sfere [Threats to the national security of the state in the information sphere]. *Strategiya grazhdanskoy zashchity: problemy i issledovaniya*, Moscow, 2014, № 1(16), pp. 21-34 (In Russ.).

48. South Africa banks hit by phishing scams. Available at: https://www.computerworld.com/article/2559147/south-africa-banks-hit-by-phishing-scams.html (accessed 7.07.2023).

49. Brazil leads in phishing attacks. Available at: https://www.zdnet.com/article/brazil-leads-in-phishing-attacks/ (accessed 5.07.2023).

50. Reddit hacked in phishing attack platform confirms no user data was leaked. Available at: https://indianexpress.com/article/technology/tech-news-technology/reddit-hacked-in-phishing-attack-8437340/ (accessed 8.08.2023).

51. Bitter' espionage hackers target Chinese nuclear energy org. Available at: https://www.bleepingcomputer.com/news/security/bitter-espionage-hackers-target-chinese-nuclear-energy-orgs/ (accessed 10.08.2023).

52. Kaspersky: мошенники в России начали использовать ChatGPT в фишинговых атаках. Available at: https://www.kommersant.ru/doc/6044090 (accessed 12.08.2023).

53. Compendium BRICS Best Practices Information Security Risks: Supervision and Control. Available at: https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-54.pdf (accessed 15.08.2023).

54. We've Just Seen the First Use of Deepfakes in an Indian Election Campaign. Available at: https://vice.com/en/article/jgedjb/the-first-use-of-deepfakes-in-indian-election-by-bjp (accessed 15.08.2023).

55. Виноградова Е.А. Злонамеренное использование политических дипфейков и попытки их нейтрализации в странах Латинкой Америки. *Латинская Америка*, М., 2023, № 5, сс. 35-48. [Vinogradova E.A. Zlonamerennoye ispol'zovaniye politicheskikh dipfeykov i popytki ikh neytralizatsii v stranakh Latinkoy Ameriki. [The malicious use of political deepfakes and attempts to neutralize them in Latin America]. *Latinskaya Amerika*, Moscow, 2023, N 5, pp. 35-48. (In Russ.). (DOI: 10.31857/S0044748X0025404-3).

56. Deepfakes go South African — Ramaphosa in video of plan to tear down Voortrekker Monument and Loftus. Available at: https://mybroadband.co.za/news/internet/487811-deepfakes-go-south-african-ramaphosa-in-video-of-plan-to-tear-down-voortrekker-monument-and-loftus.html/amp (accessed 17.08.2023).
57. На ТВ показали «обращение Путина» о военном положении в ряде областей России. Это был взлом, а ролик оказался дипфейком. Available at: https://rusnewshub.ru/2023/06/05/ (accessed 20.07.2023).
58. AI image generator Midjourney bans deepfakes of China's Xi Jinping 'to minimize drama'. Available at: https://www.foxnews.com/tech/ai-image-generator-midjourney-bans-deepfakes-china-xi-jinping-minimize-drama (accessed 22.07.2023).
59. How Twitter bots and internet trolls sow racial and political division in SA. Available at: https://businesstech.co.za/news/internet/280673/how-twitter-bots-and-internet-trolls-sow-racial-and-political-division-in-sa/ (accessed 24.07.2023).
60. Final Report National Security Commission on Artificial Intelligence. Available at: https://nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (accessed 24.09.2022).
61. The Biden-Harris Administration's National Security Strategy. The White House. October 12, 2022. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/ (accessed 11.10.2022).
62. U.S. Special Forces Want to Use Deepfakes for Psy-Ops. Available at: https://d-russia.ru/wp-content/uploads/2023/03/us-socom-procurement-document-announcing-desire-to-utilize-deepfakes_compressed.pdf (accessed 11.08.2023).

Ekaterina A.Vinogradova (vinogradovacatherine7@gmail.com)
Cand. Sci. (Political Science), Director of the Research Center: Artificial Intelligence Technologies in International Relations, Moscow, Russian Federation

Artificial intelligence technologies in the BRICS political agenda

Abstract. In the period of the Fourth Industrial Revolution, the rapid growth of artificial intelligence (AI) technologies poses a challenge to all countries for their legitimate use and timely implementation in the public sector. The BRICS countries are active participants in the digitalization process in the political, economic, social and military spheres, as well as in the association's activities aimed at enhancing AI technologies and communication channels. However, the rapid growth of the latest AI-based technologies threatens the already vulnerable cybersecurity sector and facilitates active information-psychological and terrorist operations aimed at putting BRICS political actors out of work and conducting disinformation campaigns.

Key words: BRICS, artificial intelligence technologies, cyber security, IV industrial revolution, information and psychological security, digital transformation.

DOI: 10.31857/S0044748X0029114-4

Received 19.08.2023.