DOI 10.35775/PSI.2025.124.12.030
УДК 327.8

Д.В. ДРЕСВЯНИН
аспирант кафедры мировых политических процессов,
эксперт управления языковой подготовки, Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации»,
Россия, г. Москва

МОДЕЛИ УПРАВЛЕНИЯ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ В УСЛОВИЯХ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА: СТРАТЕГИЯ ДЛЯ РОССИИ И БРИКС

Статья посвящена анализу политико-правовых моделей управления искусственным интеллектом (ИИ), формирующихся в условиях усиления глобального тренда на технологический суверенитет и роста трансграничных вызовов. Цель исследования – разработка практических рекомендаций для России по укреплению национального технологического суверенитета через сбалансированное внутреннее регулирование ИИ и активное коалиционное взаимодействие в рамках БРИКС. Методологическую основу исследования составляют сравнительный анализ, направленный на выявление ключевых теоретических подходов и складывающихся регуляторных режимов, и метод кейс-стади, применяемый для определения стратегических дилемм на примере конкретных национальных стратегий ведущих держав. В результате анализа научных дискурсов выделены и критически оценены доминирующие модели управления ИИ. Показана их прямая преемственность по отношению к базовым политико-правовым режимам управления интернетом. Противостояние концепций ИИ находит прямое отражение в конкурирующих национальных стратегиях (ЕС, Китая, США, России). Несовместимость ценностно-политических подходов ключевых игроков является главным препятствием для выработки универсальных международных стандартов. Обоснована необходимость для России комплексной стратегии, сочетающей адаптивные национальные регуляторные механизмы с активным продвижением коалиционной повестки в многосторонних форматах. В качестве приоритетной платформы для продвижения российских интересов и формирования альтернативных регуляторных решений рассматривается БРИКС. Предложена матрица конкретных инициатив, направленных на минимизацию рисков технологической изоляции, укрепление международной информационной безопасности и позиционирование страны как одного из архитекторов альтернативных правил для цифровой среды.

Ключевые слова: *искусственный интеллект, технологический суверенитет, регулирование ИИ, риск-ориентированный подход, БРИКС, международная информационная безопасность, гибридная модель.*

Современный этап технологического развития характеризуется синергией экспоненциального роста возможностей искусственного интеллекта (ИИ) и его глубокой интеграции в глобальную цифровую инфраструктуру. Этот процесс трансформирует международно-политические отношения, превращая данные и алгоритмы в критический ресурс геополитической конкуренции и источник власти [25. P. 1-79]. Однако, вопреки прогнозам теоретиков технологического детерминизма [8], глобализация не привела к унификации управления. Напротив, наблюдается фрагментация цифрового пространства и обострение конкуренции между государствами и коалициями за право определять нормативные режимы и стандарты в сфере ИИ. В мире сосуществуют и конкурируют различные, подчас противоположные, регуляторные философии и этико-правовые повестки, отражающие глубинные различия в ценностных основаниях, экономических интересах и моделях государственного управления [11; 16; 20]. В качестве стратегического ответа на новые вызовы актуализируется концепция технологического суверенитета как способность государства самостоятельно определять правила, контролировать критическую инфраструктуру и защищать свои данные в цифровой сфере [2. С. 38-51].

В этих условиях для России формирование стратегии управления ИИ, способной одновременно стимулировать ускоренное развитие и безопасное внедрение ИИ внутри страны и обеспечивать внешнее влияние для продвижения собственных регуляторных моделей, приобретает характер национального императива, особенно на фоне беспрецедентного внешнего технологического давления. Стратегически важным направлением для ее реализации становится углубление кооперации в многосторонних форматах, прежде всего в рамках БРИКС+. Объединение не только декларирует курс на создание альтернативного миропорядка, но и демонстрирует общность приоритетов в защите технологического суверенитета, что делает его перспективной платформой для продвижения согласованных регуляторных подходов [4].

Проблема цифрового управления в политической науке и исследованиях цифрового управления, при всей своей востребованности, характеризуется значительной методологической и тематической разобщенностью. Исследования сосредоточены на отдельных ее аспектах, что препятствует формированию целостной теоретической картины.

Концептуальный уровень разработки темы остается неоднородным. Доминирующей нормативной основой остаются этико-правовые принципы западной либеральной парадигмы, получившие развитие в контексте цифровой экспансии и управления ИИ (Л. Флориди) [12. P. 51-75]. Важный политэкономический фундамент для дискуссии создает критический анализ глобальной технологической конкуренции и материальных основ данных (К. Кроуфорд) [10]. Между тем, в научный дискурс все активнее входит понимание цифрового суверенитета как динамической и эмерджентной категории, содержание которой определяется взаимодействием технологий, национальных интересов и эволюции международной системы (Е.С. Зиновьева, С.В. Шитьков) [2. С. 38-51].

Параллельно формируются альтернативные подходы, такие как «цифровой регресс», предлагающий радикальную критику цифрового колониализма (Л. Квет) [17], и исследования, фокусирующиеся на трансформирующем воздействии ИИ на политические процессы и институты, включая проблему алгоритмической предвзятости (У. Питерс) [19]. Прикладные работы – сравнительный анализ регуляторных моделей (Р. Геллерт) [14. P. 15-33], изучение проблем глобального управления ИИ (Й. Таллберг) [22], исследования технологической геополитики в логике национальной безопасности (Л. Флориди) [12. P. 51-75] – развиваются как изолированные исследовательские программы. При этом критика капитализма наблюдения как нового институционального порядка (Ш. Зубофф) [25. P. 1-79] и фундаментальные исследования социальных и экологических последствий систем ИИ (Т. Гебру, Р. Дентон) [13. P. 215-321] остаются на периферии дискуссии о суверенитете, что указывает на сохраняющуюся концептуальную разрозненность поля.

Особенно ощутим пробел в изучении институционального потенциала БРИКС для формирования коалиции технологических суверенитетов и выработки согласованных подходов к регулированию ИИ. Хотя роль объединения как платформы для альтернативного управления признается [3. С. 161-182; 5. С. 202-228], отмечаются ключевые препятствия для реализации этого потенциала: внутренняя разнородность участников (М.Ю. Лев) [6. С. 1999-2026], отсутствие консолидированных механизмов продвижения общей позиции (М.В. Ларионова) [5. С. 202-228] и ограниченное влияние отдельных членов объединения на глобальном рынке ИИ (А.В. Шелепов) [9. С. 96-113]. Критическим фактором успеха, согласно ряду исследований, называется качество государственного управления, которое опосредует влияние инвестиций в ИИ на социально-экономические результаты на национальном уровне (Ч.Ш. Саба, М. Преториус) [21. P. 5-44]. В этой связи центральным вопросом становится проектирование конкретных механизмов, способных трансформировать БРИКС в эффективную коалицию.

Комплексное исследование, синтезирующее три ключевых элемента – управление ИИ, обеспечение цифрового суверенитета и стратегическое взаимодействие в БРИКС – для формирования конкретных ориентиров российской политики, представляет собой актуальную научную проблему. Каким образом Россия может сформировать и реализовать сбалансированную стратегию управления ИИ, которая, с одной стороны, обеспечила бы укрепление национального технологического суверенитета через адаптивное внутреннее регулирование, а с другой – позволила бы активно продвигать альтернативные нормативные принципы через коалиционное взаимодействие в рамках БРИКС?

Для решения этой исследовательской задачи в работе используется двухуровневый методологический подход. На основе сравнительного анализа (Т. Ландман) [18] выявляются и сопоставляются ключевые регуляторные модели управления ИИ, определяющие глобальную конкуренцию. С помощью метода кейс-стади (Р.К. Инь) [24] анализируются национальные стратегии ключевых игроков (ЕС, США, Китая, России) и коалиционная роль БРИКС, ее возможности

в качестве стратегической платформы. Компаративистика обеспечивает системность и широту анализа, компенсируя потенциальную узость case study конкретных кейсов, наполняет теоретические модели эмпирическим содержанием, нивелируя риск излишней абстракции.

В современном дискурсе цифровой суверенитет понимается как сложный, многокомпонентный конструкт, призванный служить основой для стабилизации международных отношений и выработки общих норм в цифровой сфере. Ключевая его роль, когда «мир разбит на суверенные государства», видится в том, чтобы стать общей платформой для диалога и «выступить в роли общего знаменателя» [2. С. 38-51]. Суверенитет представляет собой не только барьер для защиты, но и необходимый фундамент для кооперации.

На практике различные регуляторные подходы неодинаково интерпретируют эту двойственную логику. Научная дискуссия о регулировании ИИ структурируется вокруг нескольких подходов – этико-гуманистического, технологического, общего (агентского) и риск-ориентированного, каждый из которых предлагает свой ответ на вызовы технологического суверенитета.

Этико-гуманистический подход к регулированию ИИ смещает акцент с управления рисками на безусловный приоритет прав человека и общественных ценностей, стремясь интегрировать этические принципы (справедливость, прозрачность) непосредственно в процесс разработки технологий. Его основными инструментами выступают мягкие регуляторные форматы – этические хартии, руководства и добровольная сертификация, которые формируют общий язык для публичной дискуссии и укрепляют доверие. Однако ключевой проблемой подхода остается дисбаланс между декларацией абстрактных принципов и их конкретной правовой и технической реализацией.

Как полагают Т. Гебру и Р. Дентон, преодоление этого несоответствия требует не уточнения самих норм, а радикальной переориентации исследований на нужды сообществ, подотчетность и отказ от вредоносных разработок. Поскольку многие виды вреда «не имеют чисто «технических» решений» [13. С. 14], необходим выход за рамки «этики по дизайну» в сторону трансформации целей и властных отношений в самой области компьютерного зрения. Ученые видят решение в смене парадигмы: от регулирования принципов к созданию «исследований, укорененных в сообществе», когда приоритетом является не технологический прогресс, а благополучие конкретных людей [13. С. 66].

Особую сложность реализация парадигмы приобретает в глобальном контексте, где сталкиваются несовпадающие культурные и правовые традиции. Например, баланс между приватностью и национальной безопасностью или между автономией личности и коллективным благом в разных обществах выстраивается по-разному. В результате этико-гуманистический подход сам становится полем геополитического позиционирования: Евросоюз продвигает модель «доверенного ИИ», основанную на либерально-демократических ценностях [20], тогда как Россия и страны БРИКС развивают собственные концепции «ответственного ИИ», делающие акцент на государственном суверенитете,

коллективных интересах и технологической независимости [4]. Это ценностное противостояние находит свое прямое отражение в дискуссиях и документах международных организаций [23]. Следовательно, практическая эффективность любых этических принципов в регулировании ИИ будет зависеть от их гибкости – способности получать легитимное наполнение в рамках несовпадающих, а порой и конфликтующих, глобальных ценностных систем.

Технологически-нейтральный подход предлагает регулировать не абстрактный ИИ, а конкретные применения программного обеспечения в критических сферах. Его суть заключается в «регуляторном компромиссе»: соблюдении принципа технологической нейтральности права и создании гибких, ориентированных на результат правовых рамок. Вместо фиксации технических решений эти механизмы фокусируются на вредоносных последствиях, что позволяет законодательству сохранять актуальность, не сдерживая инновации избыточными предписаниями. Однако критики (К. Кроуфорд, Ш. Зубофф) уточняют, что фокус на отдельных применениях может недооценивать кумулятивные системные риски массового внедрения ИИ, такие как усиление социального неравенства или эрозию приватности [10; 25. P. 1-79].

Значительные трудности этот подход встречает в контексте генеративного ИИ, где требуется переосмысление существующих этико-правовых рамок для решения сквозных дилемм ответственности и справедливости. Российские эксперты указывают на отсутствие целостного правового регулирования, охватывающего все этапы жизненного цикла генеративного ИИ – от разработки до внедрения. Быстрое развитие ИИ «формирует новые риски в области общественной безопасности», главными из которых являются рост некачественного контента и цифрового мошенничества [1. С. 4]. В отличие от политики либерального регулирования (США, Сингапур) и жестких императивных моделей (ЕС, Китай), в России, по оценкам аналитиков, сохраняется баланс между контролем и созданием условий для развития технологии. Для совершенствования правового поля предлагается адаптировать зарубежные подходы, развивать механизмы отраслевого саморегулирования и разрабатывать точечные меры против конкретных угроз: дезинформации, использования ложных данных, нарушения этико-культурных норм и др. [1].

Будучи полезным для регулирования конкретных приложений, технологически-нейтральный подход оказывается недостаточным для комплексного управления сложными трансформативными технологиями.

Общий подход к регулированию ИИ, ориентированный на «парадигму агента», фокусируется на автономных системах, перенося внимание законодателя с алгоритмов на их поведение и последствия. В рамках этой концепции формируются отраслевые требования к проектированию и применению таких систем в высокорисковых сферах, что позволяет создавать точные технические стандарты (например, для сертификации беспилотных автомобилей). Ключевым ограничением подхода является его узкая применимость [10; 25. P. 1-79]. Эффективная для регулирования физических автономных систем, она

плохо масштабируется на технологии с информационным или социальным воздействием. Генеративные модели или системы поддержки решений, чьи риски связаны с манипуляцией контентом и трансформацией общественных процессов, часто остаются за ее пределами.

По оценке Й. Таллберга и его коллег, современное глобальное управление ИИ представляет собой фрагментированный «режимный комплекс» противоречивых норм, где нормативирование автономных систем составляет лишь один сегмент наряду с этическими рекомендациями и стандартами данных [22]. Как следствие, «попытки регулировать ИИ часто отстают от технологического развития», а узкоагентный подход упускает системные социотехнические риски, требующие межотраслевой координации [22. С. 7]. Авторы видят главное препятствие в дисбалансе академического дискурса, где преобладают исследования применения ИИ над анализом институтов глобального регулирования, и предлагают сочетать эмпирический анализ механизмов управления с нормативной разработкой стандартов [22].

Дальнейшее развитие подхода требует как национальных технико-правовых решений, так и международного регулирования для ответа на вызовы технологий, выходящих за рамки классического агентства.

В качестве доминирующей парадигмы в международной регуляторной повестке сегодня утвердился риск-ориентированный подход, основанный на принципе соразмерности. Его суть заключается в установлении прямой зависимости между уровнем потенциального вреда от системы ИИ и строгостью предъявляемых к ней регуляторных требований. Данный подход фокусируется не на запрете технологий как таковых, а на адресном управлении сопутствующими угрозами, в первую очередь для прав и свобод личности, реализуясь через иерархию рисков и дифференцированные меры регулирования – от жестких предварительных требований к сертификации для систем высокого риска до рекомендательных рамок для систем с минимальным уровнем угроз.

На практике подход принимает различные формы. Как отмечает Р. Геллерт, в Общем регламенте по защите данных (GDPR) он служит инструментом метарегулирования соблюдения норм, тогда как в Законе Европейского Союза (ЕС) об ИИ выступает механизмом риск-регулирования, определяющим перечень систем «высокого риска». В первом случае риск задает интенсивность мер, а во втором – критерий отбора объектов, формируя разный баланс между инновациями и контролем [14. P. 15-33].

В отличие от модели, принятой в ЕС, где оценка рисков напрямую служит защите фундаментальных прав, российская регуляторная парадигма интегрирует принцип соразмерности в более широкий контекст государственной политики, отдающей приоритет задачам технологического суверенитета и национальной безопасности [7]. В этой системе координат риск-ориентированный подход выступает не самостоятельной философией регулирования, а инструментом суверенно-охранительной политики. Фокус оценки рисков смещается в сторону угроз, связанных с использованием иностранных платформ, утечкой

критически важных данных или потерей технологического контроля. При этом защита прав граждан (например, в киберпространстве) и стимулирование инноваций не исключаются, а осуществляются в рамках приоритета построения независимой и безопасной технологической экосистемы.

Специфика российской модели становится особенно заметной на фоне других ключевых регуляторных парадигм, формирующих глобальный ландшафт управления ИИ. Наиболее структурированное воплощение риск-ориентированный подход получил в регулировании ЕС, где Закон об ИИ реализует его через детализированное жесткое регулирование, основанное на категоризации уровней риска [20]. Эта модель, претендуя на установление глобальных стандартов для доступа к европейскому рынку, сама становится вызовом для технологического суверенитета других стран [1].

В отличие от этого, подход США исторически тяготел к парадигме отраслевого саморегулирования и мягкого права, сосредоточенного на конкретных применениях. Однако растущее общественное и законодательное давление указывает на формирующийся сдвиг в сторону более жестких федеральных рамок, отражая внутреннюю дилемму между стимулированием инноваций и сдерживанием рисков [11].

Китайская модель представляет собой синтез жесткого государственного контроля с активным государственным инвестированием и стратегическим планированием. Регулирование становится инструментом технологической геополитики, направленным не только на внутренний контроль, но и на продвижение собственных стандартов на международной арене [16].

На этом фоне инициативы по созданию общепризнанных принципов [15] демонстрируют попытку преодоления фрагментации через поиск минимального глобального консенсуса, хотя их практическая реализация – сложная задача.

Противоречия между этими подходами коренятся в фундаментально разных философиях: превентивного контроля (ЕС) [20], инновационно-ориентированного прагматизма (США) [11], государственно-стратегического управления (Китая) [16]. Их преодоление для выработки общих принципов является не столько технико-юридической, сколько политической задачей, требующей учета факторов коллективной безопасности, справедливого распределения выгод от технологий и сохранения культурно-цивилизационного разнообразия. В этих условиях будущее глобального регулирования видится не в победе одной модели, а в синергии их ключевых элементов. В такой архитектуре риск-ориентированный подход мог бы задавать общий уровень строгости требований, технологически нейтральные принципы – обеспечивать необходимую гибкость, а система этических координат – определять цели развития в интересах человека.

Для России, стремящейся укрепить технологический суверенитет в условиях конкуренции глобальных регуляторных моделей, ключевой возможностью становится продвижение собственной повестки через многосторонние форматы, в первую очередь БРИКС. Стратегическая цель заключается не в унификации

подходов, а в гармонизации интересов и создании инструментов кооперативного суверенитета. Это предполагает выявление зон совпадающих интересов, где совместные действия могут снизить коллективную зависимость от доминирующих технологических экосистем и создать альтернативные точки роста. На основе проведенного анализа для системной реализации данной стратегии была сформирована матрица стратегических инициатив, связывающая ключевые риски для России, возможности в рамках БРИКС и конкретные предложения для продвижения (Таблица 1).

Таблица 1. Матрица стратегических инициатив России
в сфере регулирования ИИ и цифрового пространства в рамках БРИКС

Сфера	**Ключевые риски для России**	**Возможности в рамках БРИКС**	**Инициативы для продвижения России**
Правовые рамки ИИ	Несовместимость с западными стандартами, создающая барьеры для экспорта решений и усиливающая регуляторное давление.	Гармонизация подходов для формирования общего рынка ИИ-решений и выработки коллективной переговорной позиции на глобальных площадках.	1. Разработка и продвижение «Типового закона БРИКС об основах регулирования ИИ». 2. Создание постоянного Форума регуляторов ИИ стран БРИКС.
Безопасность ИИ	Втягивание в гонку ИИ-вооружений и связанные с этим репутационные, правовые и стратегические риски.	Выработка общих принципов контроля за военным ИИ и формирование ответственной повестки.	1. Создание экспертной рабочей группы БРИКС по этике и безопасности военного ИИ. 2. Продвижение концепции «гуманитарного мониторинга» применения автономных систем в ООН.
Управление данными	Изоляция от глобальных потоков данных, угрожающая развитию отечественных ИИ-моделей.	Создание общего пространства доверенных данных для совместных разработок, снижающего зависимость от западных платформ.	1. Проект «Data Bridge БРИКС» – соглашение о трансграничной передаче данных с общими стандартами. 2. Запуск совместного проекта по созданию многоязычных открытых датасетов для обучения AI-моделей, ориентированных на языковое и культурное разнообразие стран БРИКС+

Сфера	Ключевые риски для России	Возможности в рамках БРИКС	Инициативы для продвижения России
Кибербезопасность и инфраструктура	Уязвимость цепочек поставок и критической инфраструктуры, зависимость от иностранного программного обеспечения и оборудования.	Технологическая кооперация в импортозамещении, разработка общих стандартов киберустойчивости.	1. Создание «Цифрового коридора безопасного взаимодействия БРИКС» на базе российских технологий. 2. Учреждение Консорциума по киберустойчивости критической инфраструктуры БРИКС.
Кадровый потенциал и научные разработки	«Утечка мозгов», отставание в ключевых областях ИИ.	Формирование сетевых научных центров, реализация совместных образовательных программ и грантов.	1. Запуск программы «Стипендии БРИКС в сфере AI & Data Science» в российских вузах. 2. Учреждение совместного конкурса исследовательских грантов «BRICS AI Research Challenge».
Этика и общественное доверие	Использование этической повестки как инструмента дискредитации российских технологий.	Выработка культурно-чувствительной рамки «ответственного ИИ», отражающей многообразие подходов.	1. Разработка и подписание «Хартии БРИКС об этических принципах использования ИИ». 2. Проведение ежегодного Форума «ИИ для Целей устойчивого развития БРИКС».

Успешная реализация обозначенных внешнеполитических инициатив невозможна без параллельного проведения внутренних преобразований, направленных на укрепление национальной цифровой экосистемы и формирование весомой доказательной базы (практических результатов) для их международного продвижения. Ключевыми направлениями такой внутренней политики должны стать:

1. Разработка стандартов и методологий: создание национальных стандартов качества данных для ИИ, внедрение системы обязательной или рекомендованной маркировки контента, генерируемого ИИ, и разработка требований к системам верификации для противодействия дипфейкам.

2. Совершенствование правового регулирования: нормативное закрепление и структурирование отраслевого саморегулирования на основе расширенной этической декларации, адаптация законодательства об авторском праве

к реалиям ИИ, введение процедуры оценки воздействия ИИ на рынок труда в рамках «регуляторных песочниц».

3. Развитие компетенций и инфраструктуры: запуск федеральной программы цифровой грамотности с акцентом на критическое восприятие контента ИИ, создание грантового фонда для междисциплинарных исследований и учреждение национального центра компетенций по генеративному ИИ.

Предлагаемый двухуровневый подход – стратегическое позиционирование через БРИКС в сочетании с системным внутренним развитием – позволит России не только эффективно противодействовать ключевым рискам (минимизировать уязвимости), но и активно формировать новые правила и институциональные альтернативы в глобальной цифровой архитектуре.

Проведенное исследование подтверждает, что формирование глобальных норм в сфере ИИ происходит в условиях жесткой конкуренции национальных моделей, каждая из которых отражает глубинные ценности и стратегические приоритеты своих создателей. Европейский превентивный контроль, американский инновационный прагматизм и китайское государственно-стратегическое управление очерчивают контуры нового технологического порядка, где технологический суверенитет становится ключевым императивом.

В этих условиях для России актуален отказ от простого заимствования регуляторных шаблонов в пользу выработки собственной гибридной стратегии, которая представляет собой сложный управленческий вызов. Ее внутренний контур требует тонкого баланса: создания «жесткого» правового каркаса для сфер национальной безопасности при одновременном развитии «мягкого» стимулирующего регулирования для науки и бизнеса. Ключевым становится вопрос о том, как предотвратить подавление инноваций избыточным контролем.

На международном уровне стратегическим ответом на давление доминирующих технологических экосистем должно стать активное коалиционное строительство. БРИКС+, объединяющий страны с общей заинтересованностью в предотвращении «цифрового колониализма» и построении многополярной архитектуры, представляет для этого уникальную платформу. Его потенциал заключается в создании точечных, но значимых прецедентов: запуске совместных исследовательских проектов в области «доверенного ИИ», гармонизации стандартов для трансграничного обезличенных данных, формировании общих принципов киберустойчивости.

Таким образом, успех России будет зависеть от двух взаимосвязанных факторов: способности построить жизнеспособную и привлекательную национальную экосистему ИИ и умения трансформировать совпадающие интересы с партнерами по БРИКС в конкретные технологические альянсы. Реализация этой стратегии позволит России не просто адаптироваться к правилам, диктуемым другими центрами силы, но и стать активным архитектором альтернативных принципов будущего технологического миропорядка, определив свое место в формирующейся многополярной цифровой реальности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Болотских М.Н., Абанитов Н.М., Власов Н.В., Гилязова А.И.** Регулирование генеративного ИИ: правовой анализ и риски для РФ. М.: ООО «Яков и Партнеры», 2024. 52 с.
2. **Зиновьева Е.С., Шитьков С.В.** Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3.
3. **Игнатов А.А.** Регулирование цифровых платформ в БРИКС: приоритеты и опыт ЮАР // Вестник международных организаций: образование, наука, новая экономика. 2024. Т. 19. № 2.
4. Казанская декларация XVI саммита БРИКС: принята в г. Казани 23 октября 2024 г. // Президент России // https://static.kremlin.ru/media/events/files/ru/MUCfWDg0QRs3xfMUiCAmF3LEh02OL3Hk.pdf.
5. **Ларионова М.В.** Тенденции и риски формирования глобального цифрового управления // Вестник международных организаций: образование, наука, новая экономика. 2025. Т. 20. № 1.
6. **Лев М.Ю., Лещенко Ю.Г., Медведева М.Б.** Регулирование искусственного интеллекта международными организациями как фактор обеспечения технологической безопасности в национальных юрисдикциях // Экономическая безопасность. 2024. Т. 7. № 8.
7. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10 октября 2019 года № 490 // Президент России // http://www.kremlin.ru/acts/bank/44731.
8. **Тоффлер Э.** Третья волна / пер. с англ. К.Ю. Бурмистрова и др. Москва: АСТ, 2010. 795 с.
9. **Шелепов А.В.** Влияние политики лидеров цифровизации – членов «Группы двадцати» на механизмы международного регулирования и условия развития цифровой экономики // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17. № 1.
10. **Crawford K.** Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021. 336 p.
11. Executive Order No. 14179: Removing Barriers to American Leadership in Artificial Intelligence // The White House. January 23, 2025 // https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence.
12. **Floridi L., Roberts H., Hine E.** Digital Sovereignty, Digital Expansionism and the Prospects for Global AI Governance // Quo Vadis, Sovereignty?: New Conceptual and Regulatory Boundaries in the Age of Digital China / ed. by M. Timoteo, B. Verri, R. Nanni. Cham: Springer, 2023.
13. **Gebru T., Denton R.** Beyond Fairness in Computer Vision: A Holistic Approach to Mitigating Harms and Fostering Community-Rooted Computer Vision Research // Foundations and Trends® in Computer Graphics and Vision. 2024. Vol. 16. No. 3.

14. **Gellert R.** The risk-based approach in the General Data Protection Regulation and the proposed Artificial Intelligence Act: «business as usual»? // Journal of Ethics and Legal Technologies. 2021. Vol. 3. No. 2.
15. Global Digital Compact. United Nations. 2024. 22 Sept. // https://www.un.org/techenvoy/global-digital-compact.
16. Internet Information Service Algorithmic Recommendation Management Provisions(《互联网信息服务算法推荐管理规定»)//Cyberspace Administration of China. 2022 // http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.
17. **Kwet M.** Digital Degrowth: Technology in the Age of Survival. London: Pluto Press, 2024. 320 p.
18. **Landman T.** Issues and Methods in Comparative Politics: An Introduction. 3rd ed. London: Routledge; 2008. 355 p.
19. **Peters U.** Algorithmic Political Bias in Artificial Intelligence Systems // Philosophy and Technology. 2022. Vol. 35 (2), 25 // https://doi.org/10.1007/s13347-022-00512-8.
20. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on laying down harmonised rules on artificial intelligence // Official Journal of the European Union // https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.
21. **Saba Ch.Sh., Pretorius M.** The mediating role of governance in creating a nexus between investment in artificial intelligence (AII) and human well-being in the BRICS countries // BRICS Journal of Economics. 2024. Vol. 5. No. 2.
22. **Tallberg J., Erman E., Furendal M., Geith J., Klamberg M., Lundgren M.** The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research // SSRN Electronic Journal**.** 2023. May 2 // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4424123.
23. United Nations General Assembly. Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development: resolution adopted by the General Assembly on 21 March 2024. A/RES/78/265 // https://undocs.org/A/RES/78/265.
24. **Yin R.K.** Case Study Research and Applications: Design and Methods. 6th ed. Thousand Oaks, CA: SAGE Publications, 2018. 352 p.
25. **Zuboff S.** Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization // Organization Theory. 2022. Vol. 3. No. 4.

D.V. DRESVYANIN
PhD student in the Department of world political processes,
expert at Directorate of language training, Moscow State Institute
of International Relations (MGIMO University),
Moscow, Russia

ARTIFICIAL INTELLIGENCE REGULATION MODELS IN THE CONTEXT OF TECHNOLOGICAL SOVEREIGNTY: A STRATEGY FOR RUSSIA AND BRICS

This article analyzes political and legal models for artificial intelligence (AI) regulation, which are emerging in the context of a strengthening global trend towards technological sovereignty and growing cross-border challenges. The aim of the study is to develop practical recommendations for Russia to strengthen national technological sovereignty through balanced domestic AI regulation and active coalition cooperation within the BRICS. The methodological basis of the study is a comparative analysis aimed at identifying key theoretical approaches and emerging regulatory regimes, and a case study method applied to identify strategic dilemmas using individual national strategies of leading powers as examples. An analysis of key scholarly discourses allows us to identify and critically evaluate dominant models of AI regulation, demonstrating their direct continuity with the established political and legal regimes for internet governance. The confrontation of AI approaches is directly reflected in the competing national strategies (those of the EU, China, the US, and Russia). The incompatibility of key players' value and political approaches is the main obstacle to the development of universal international standards. The article substantiates the need for a comprehensive strategy for Russia that combines flexible national regulatory mechanisms with the active promotion of a coalition agenda in multilateral formats. BRICS is considered a priority platform for advancing Russian interests and developing alternative regulatory solutions. We propose a matrix of specific initiatives aimed at minimizing the risks of technological isolation, strengthening international information security, and positioning Russia as an architect of alternative rules for digital environment.

Key words: *artificial intelligence, technological sovereignty, AI regulation, risk-based approach, BRICS, international information security, hybrid model.*