МРНТИ 20.01.17; 20.01.80

10.51889/2959-5894.2024.87.3.011

Н.Ж. Айтенов[1*], Б.О. Куламбаев[2], Д.К. Жекенов[3], Д.И. Губина[4]

[1]Университет Нархоз, г. Алматы, Казахстан
[2]Университет Туран, г. Алматы, Казахстан
[3]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
[4]Уральский Федеральный Университет имени Первого Президента России Б.Н. Ельцина, г. Екатеринбург, Россия
[*]*e-mail: nurakhmet.aitenov@narxoz.kz*

ОТКРЫТЫЕ ДАННЫЕ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ США И КИТАЯ

Аннотация

Цель исследования – изучение открытости практик больших данных среди крупных IT-компаний США и Китая, с упором на их последствия для развития искусственного интеллекта и международного сотрудничества. В исследовании применяется структура качественного анализа, использующая тематические исследования для оценки доступности данных, прозрачности и совместных инициатив. Результаты исследования показывают, что американские компании, такие как Microsoft и Google, демонстрируют более высокий уровень открытости данных, поддерживаемый нормативной средой, которая уравновешивает инновации с защитой конфиденциальности. Напротив, китайские компании, такие как Tencent и Alibaba, отдают приоритет внутреннему использованию данных в рамках строгого нормативного контроля, подчеркивая безопасность данных и суверенитет. Эти различия создают проблемы для международного сотрудничества в области искусственного интеллекта, усугубляемые геополитической напряженностью и расходящимся нормативным ландшафтом. Несмотря на барьеры, существуют возможности для гармонизации посредством общих фреймворков и совместных инициатив, направленных на использование объединенного опыта для продвижения технологий искусственного интеллекта во всем мире.

Ключевые слова*:* искусственный интеллект, большие данные, международное сотрудничество, IT-компании, открытые данные, цифровизация.

Н.Ж. Айтенов[1], Б.О. Куламбаев[2], Д.К. Жекенов[3], Д.И. Губина[4]
[1]Нархоз Университеті, Алматы қ., Қазақстан
[2]Тұран Университеті, Алматы қ., Қазақстан
[3]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[4]Ресейдің Тұңғыш Президенті Б.Н. Ельцин атындағы Орал Федералды Университеті, Екатеринбург қ., Ресей

АШЫҚ ДЕРЕКТЕР ЖӘНЕ ЖАСАНДЫ ИНТЕЛЛЕКТ: АҚШ ЖӘНЕ ҚЫТАЙДЫ САЛЫСТЫРМАЛЫ ТАЛДАУ

Аңдатпа

Зерттеу мақсаты – жасанды интеллект пен халықаралық ынтымақтастықты дамытуға ықпалы негізінде АҚШ және Қытай IT-компаниялары арасындағы үлкен деректер тәжірибелерінің ашықтығын зерттеу. Зерттеуде деректердің қолжетімділігін, ашықтығын және бірлескен бастамаларды бағалау үшін тақырыптық зерттеулерді пайдалана отырып, сапалы талдау құрылымы қолданылады. Зерттеу нәтижелері көрсеткендей, Microsoft және Google сияқты американдық компаниялар инновация мен құпиялылықты қорғауды теңестіретін нормативті орта қолдауымен деректер ашықтығының жоғары деңгейін көрсетіп отыр. Керісінше, Tencent және Alibaba сияқты қытайлық компаниялар қауіпсіздік мен деректер егемендігіне баса назар аудара отырып, қатаң нормативті бақылау шеңберінде деректерді ішкі пайдалануды басшылыққа алады. Бұл өзгешеліктер геосаяси шиеленіс пен нормативті ландшафт әртүрлілігі салдарынан күшейіп отырған жасанды интеллект саласындағы халықаралық ынтымақтастық үшін қиындықтар туғызады. Кедергілерге қарамастан, әлем бойынша жасанды

интеллект технологияларын ілгерілету барысында біріктірілген тәжірибені пайдалану үшін ортақ фреймворк пен бірлескен бастамалар арқылы үйлестіру мүмкіндіктері бар.

Түйін сөздер: жасанды интеллект, үлкен деректер, халықаралық ынтымақтастық, IT-компаниялар, ашық деректер, цифрландыру.

N.Zh. Aitenov[1], B.O. Kulambayev[2], D.K. Zhekenov[3], D.I. Gubina[4]
[1]Narxoz University, Almaty, Kazakhstan
[2]Turan University, Almaty, Kazakhstan
[3]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[4]Ural Federal University named after the first President of Russia B.N. Yeltsin, Yekaterinburg, Russia

OPEN DATA AND ARTIFICIAL INTELLIGENCE:
A COMPARATIVE ANALYSIS OF THE USA AND CHINA

Abstract

The purpose of this study is to examine the openness of big data practices among major IT companies in the United States and China, with an emphasis on their implications for the development of artificial intelligence and international cooperation. The study employed a qualitative analysis framework incorporating case studies to evaluate data availability, transparency, and collaborative initiatives. The findings indicate that American companies such as Microsoft and Google exhibit higher levels of data openness, supported by a regulatory environment that balances innovation with privacy protection. In contrast, Chinese companies like Tencent and Alibaba prioritize internal data use under stringent regulatory control, emphasizing data security and sovereignty. These differences pose challenges for international cooperation in the field of artificial intelligence, exacerbated by geopolitical tensions and divergent regulatory landscapes. Despite these barriers, there are opportunities for harmonization through common frameworks and collaborative initiatives aimed at leveraging collective expertise to advance AI technologies globally.

Keywords: artificial intelligence, big data, international cooperation, IT companies, open data, digitalization.

Основные положения

В статье подчеркивается ключевая роль искусственного интеллекта в ускорении технологических и экономических достижений современного мира. Центральным элементом эффективности искусственного интеллекта является использование больших данных для принятия решений, персонализации и предиктивной аналитики. В исследовании изучаются практики открытых данных среди ведущих IT-компаний США и Китая, где выявляется, что американские компании в целом выступают за большую открытость данных по сравнению со своими китайскими коллегами, которые ограничены строгими национальными регуляторами. В заключении подчеркивается необходимость решения вопросов конфиденциальности, коммерческих интересов и геополитических соображений для улучшения международного сотрудничества в области искусственного интеллекта.

Введение

2023 год ознаменовался появлением у широкого круга общественности возможностей ознакомиться с принципами работы искусственного интеллекта (далее – ИИ) во многом благодаря ChatGPT. Это позволило обществу осознать, что ИИ становится движущей силой современных технологий и экономического роста стран. ИИ с его возможностями обучения, рассуждения и самокоррекции произвел революцию в различных отраслях: от здравоохранения и финансов до производства и розничной торговли [1]. При этом для работы ИИ требуются большие данные, характеризующиеся своим объемом, скоростью и разнообразием. Большие данные – пища, на которой работают алгоритмы ИИ, обеспечивая принятие решений на основе данных, персонализацию и предиктивную аналитику. Вместе ИИ и большие данные способствуют инновациям, повышают производительность и создают

новые бизнес-модели, тем самым внося значительный вклад в экономическую конкурентоспособность.

В ускорении разработки и развития ИИ решающее значение приобретают открытые данные, в том числе на международном уровне. Открытые данные – это данные, которые находятся в свободном доступе для любого человека, могут использоваться, повторно использоваться и распространяться, способствуя прозрачности, инновациям и совместному прогрессу. Предоставляя доступ к обширным наборам данных, открытые данные могут улучшить обучение и уточнение моделей ИИ, гарантируя более надежные и достоверные результаты. Кроме того, открытые данные способствуют международному сотрудничеству, позволяя исследователям и компаниям из разных стран сотрудничать, обмениваться идеями и разрабатывать решения для глобальных проблем.

Целью данной статьи является изучение открытости практик больших данных среди крупных IT-компаний США и Китая, с упором на их последствия для развития искусственного интеллекта и международного сотрудничества. Работа направлена на выявление проблем и возможностей, связанных с доступностью данных и практиками обмена в этих ведущих странах мира. Анализируя политику, практику и последствия открытости данных, это исследование формирует представление о том, как открытые данные могут быть использованы для продвижения развития ИИ и содействия международному сотрудничеству, в конечном итоге стимулируя технологический и экономический прогресс в глобальном масштабе.

Обзор литературы. ИИ добился значительных успехов во всем мире, оказав влияние на различные секторы с помощью новаторских достижений. В здравоохранении ИИ повысил точность диагностики, персонализировал планы лечения и улучшил результаты лечения пациентов с помощью сложной аналитики данных и моделей машинного обучения [2]. В финансах алгоритмы ИИ революционизируют торговые стратегии, помогают обнаружить мошенничество и персонализируют финансовые услуги. Производственный сектор получает выгоду от ИИ за счет автоматизации, предиктивного обслуживания и оптимизации производственных процессов, что приводит к повышению эффективности и сокращению простоев. Розничная торговля увидела улучшения в персонализированном опыте покупок, управлении запасами и обслуживании клиентов с помощью чат-ботов и рекомендательных систем на основе ИИ [3]. Эти достижения подчеркивают преобразующий потенциал ИИ в повышении производительности и инноваций в различных отраслях.

Во всех вышеназванных прорывах ИИ в жизнедеятельности человечества основополагающим компонентом выступали большие данные в соответствующей области. Объем информации, их разнообразность, скорость их обработки позволяют проводить всесторонний анализ и получать информацию, которая подпитывает возможности обучения ИИ. Интеграция больших данных и ИИ позволяет принимать расширенные решения на основе данных, проводить аналитику в реальном времени и выполнять предиктивное моделирование, что имеет решающее значение для конкурентного преимущества в современном мире, ориентированном на данные [4]. Огромные объемы данных, собранных из различных источников, помогают системам ИИ выявлять закономерности, делать прогнозы и со временем совершенствоваться, стимулируя инновации и эффективность в различных секторах [5].

Тем самым можем определить, что вопросы развития и совершенствования ИИ будут сводиться к доступности данных. При открытости данных, предоставленных общественности в свободном доступе для первичного и повторного использования, их распространения, формируются широкие возможности разработки и развития ИИ на основе принципов прозрачности, доступности и совместного использования.

Открытые данные способствуют инновациям, предоставляя исследователям и разработчикам наборы данных, необходимые для обучения и улучшения алгоритмов ИИ, обеспечивая более точные и надежные результаты [4]. Важность открытых данных

заключается в их потенциале демократизировать доступ к информации, повысить прозрачность и стимулировать экономический рост посредством инноваций и сотрудничества.

В этом контексте возрастает роль нормативного регулирования данных на международном и национальном уровнях. Так, регулирование данных в рассматриваемых странах существенно различается, отражая разные подходы к конфиденциальности данных, безопасности и доступности. В Соединенных Штатах регулирование данных осуществляется сочетанием федеральных и государственных законов, среди которых следует отметить Закон о переносимости и подотчетности медицинского страхования (HIPAA) для данных здравоохранения и Закон Калифорнии о защите прав потребителей (CCPA) для конфиденциальности данных потребителей. Эти нормативные документы направлены на защиту личной информации, одновременно балансируя между необходимостью инноваций и экономического роста [6].

Напротив, регулирование данных в Китае характеризуется более централизованным и строгим контролем с такими законами, как Закон о кибербезопасности и Закон о защите личной информации (PIPL). Эти правила подчеркивают суверенитет данных, безопасность и защиту личной информации, отражая сосредоточенность правительства на сохранении контроля над данными в пределах своих границ [7]. Несмотря на эти различия в регулировании, обе страны признают важность регулирования данных для защиты конфиденциальности и обеспечения их этичного использования.

Различия в нормативном регулировании, проблемы конфиденциальности данных и геополитическая напряженность осложняют международное сотрудничество в области ИИ. Существующие модели сотрудничества включают международные исследовательские партнерства, трансграничные соглашения об обмене данными и многонациональные проекты по разработке ИИ. Эти модели направлены на использование разнообразного опыта и ресурсов разных стран для стимулирования инноваций в области ИИ и решения глобальных проблем [8].

Однако такие проблемы, как различные правила конфиденциальности данных, опасения по поводу безопасности данных и различные национальные интересы, могут препятствовать эффективному сотрудничеству. Например, Общий регламент по защите данных Европейского союза (GDPR) налагает строгие требования к конфиденциальности данных, которые могут усложнить обмен данными со странами, не входящими в ЕС [9]. Кроме того, геополитическая напряженность между основными державами в области ИИ, такими как США и Китай, может препятствовать сотрудничеству и привести к фрагментарному подходу к разработке ИИ [10].

Решение этих проблем требует гармонизации правил конфиденциальности данных, создания рамок доверия для обмена данными и содействия диалогу и сотрудничеству между странами. Преодолевая эти препятствия, мировое сообщество может использовать весь потенциал ИИ для стимулирования инноваций и решения насущных глобальных проблем.

Методология исследования

В этом исследовании используется качественный подход к анализу с использованием тематических исследований крупных технологических гигантов США и Китая для оценки открытости их практик работы с большими данными. Качественный дизайн позволяет проводить углубленное исследование сложных явлений, предоставляя богатые знания о практиках, проблемах и возможностях, связанных с открытостью данных в контексте ИИ.

Первичные данные включают корпоративные отчеты, официальные документы и пресс-релиз отдельных технологических компаний США и Китая. Вторичные данные включают академическую литературу, нормативные документы и отраслевые отчеты.

Сравнительная структура анализа основана на нескольких критериях оценки открытости практик данных:

- Доступность: степень, в которой данные предоставляются общественности или конкретным заинтересованным лицам.

- Прозрачность: ясность и открытость политик и практик, связанных с данными.
- Инициативы по сотрудничеству: усилия по вовлечению в сотрудничество по обмену данными как на национальном, так и на международном уровне.

Аналитические инструменты: в исследовании используется контент-анализ и тематическое кодирование для выявления закономерностей и выводов из собранных данных. Контент-анализ включает в себя систематическую категоризацию текстовых данных для выявления тенденций и тем, в то время как тематическое кодирование помогает организовывать и интерпретировать качественные данные на основе повторяющихся тем и концепций.

Результаты исследования

На сегодняшний день ключевые направления развития искусственного интеллекта задаются такими странами, как США и Китай. Ведущие технологические компании этих государств, среди которых Microsoft, Apple, Amazon, Google, Facebook, Tencent и Alibaba, оказывают существенное влияние на распространение практик открытых данных. Это, в свою очередь, способствует увеличению уровня прозрачности, стимулирует инновации и содействует международному сотрудничеству в сфере ИИ. Таблица 1 иллюстрирует примеры применения открытых данных компаниями из США и Китая.

Таблица 1. Практика открытых данных технологических компаний США и Китая

Компании	*Обмен данными и инициативы*	*Конфиденциальность и безопасность*
Microsoft	*активно продвигает обмен данными через свои инициативы как Open Data, направленная на решение проблемы разрыва в данных и содействия обмену данными для общественного блага. Запустил платформу Azure Open Datasets, которая предоставляет широкий спектр набора данных для поддержки машинного обучения и исследований в области ИИ*	*подчеркивает строгие практики конфиден-циальности данных и соответствие таким нормам, как GDPR и CCPA*
Apple	*консервативна в вопросах обмена данными, уделяет первостепенное внимание конфиденциальности и безопасности пользователей. Компания предоставляет ограниченные ресурсы открытых данных по сравнению с конкурентами. Время от времени публикует исследовательские данные, особенно в области здравоохранения и ИИ, в рамках сотрудничества с академическими учреждениями*	*сильный акцент на конфиденциальности, подчеркиваемый такими функциями, как дифференциальная конфиденциальность и меры защиты данных пользователей*
Amazon	*через AWS Public Datasets Amazon предоставляет доступ к огромному массиву наборов данных для поддержки инноваций и исследований. Упрощает обмен данными через такие сервисы как AWS Marketplace и AWS Data Exchange*	*реализует надежные политики защиты данных и соблюдает различные глобальные правила конфиденциальности*
Google	*Осуществляет обмен наборами данных через платформу Google Cloud Public Datasets, и участвует в инициативах по открытым данным. Активно публикует наборы данных и результаты исследований через такие платформы, как Google AI*	*уделяет первостепенное внимание конфиден-циальности пользователей с помощью комплексных мер защиты данных и отчетов о прозрачности*
Facebook	*инициатива Facebook Data for Good делится данными для проектов социального воздействия, а платформа Facebook Research предоставляет наборы данных для академических исследований. Участвует в обмене данными через*	*балансирует между открытостью данных и проблемами конфиденциальности,*

	исследовательские партнерства и выпуски публичных наборов данных	*повышая прозрачность усилий*
Tencent	*относительно консервативна в отношении открытого обмена данными, уделяя больше внимания внутреннему использованию и стратегическим партнерствам. WeChat Open Platform предоставляет разработчикам ограниченный доступ к данным.*	*придерживается строгих законов Китая о защите данных, уделяя особое внимание безопасности пользовательских данных и соблюдению таких правил, как PIPL и CSL*
Alibaba	*Alibaba Cloud предоставляет доступ к некоторым публичным наборам данных и поддерживает инициативы открытых данных через свою платформу Big Data. Предлагает службы данных и платформы, такие как DataV, для визуализации и анализа, но с ограниченными открытыми данными по сравнению с аналогами из США.*	*реализует комплексные меры безопасности данных в соответствии с нормативными правилами Китая, обеспечивая защиту данных и конфиденциальность*
Примечание – составлено авторами на основе данных из сайта указанных компаний		

Сравнение технологических гигантов из США и Китая выявляет различия в уровне открытости данных и подходах к поддержке сотрудничества. Американские корпорации, включая Microsoft, Google и Amazon, демонстрируют более высокий уровень прозрачности, активно содействуя свободному доступу к данным и поддерживая инициативы, направленные на открытость. Эти меры подкреплены законодательной базой, способствующей инновациям при соблюдении мер по защите конфиденциальности. В то время как китайские компании, такие как Tencent и Alibaba, действуют в условиях более строгого регулирования, что сказывается на их более сдержанных практиках обмена данными, делая акцент на стратегических партнерствах и внутреннем использовании ресурсов.

Как американские, так и китайские компании ставят на первое место вопросы конфиденциальности и безопасности данных, однако действуют в разных правовых рамках. Американские корпорации следуют международным стандартам, таким как GDPR и CCPA, обеспечивая защиту данных при обмене. В то время как китайские компании ориентируются на национальные нормы, такие как PIPL и CSL, которые акцентируют внимание на безопасности данных и строгом контроле. Это различие в нормативной среде приводит к тому, что в США поддерживается обмен данными с соблюдением мер конфиденциальности, а в Китае акцент делается на безопасности, что влияет на уровень открытости данных.

Нормативное регулирование открытости данных в США и Китае оказывает значительное влияние на уровень доступности данных, а также на обеспечение их конфиденциальности и безопасности. В США правовая система, регулирующая открытые данные, характеризуется многоуровневой структурой, включающей федеральные и региональные законы, а также отраслевые рекомендации (Таблица 2).

Как показано в таблице 2, федеральные законы, такие как Закон о переносимости и подотчетности медицинского страхования (HIPAA), Закон о защите конфиденциальности детей в Интернете (COPPA), Закон Грэмма-Лича-Блайли (GLBA), Закон о добросовестной кредитной отчетности (FCRA) и Закон о Федеральной торговой комиссии (FTC Act), формируют правовые рамки для защиты конфиденциальных данных и предотвращения мошеннических действий.

Таблица 2. Нормативные документы, регулирующие открытые данные в США

№	Название документа	Описание
		Федеральные законы
1	Закон о переносимости и подотчетности медицинского страхования (HIPAA)	устанавливает стандарт защиты конфиденциальных данных пациентов. Приложения ИИ в здравоохранении должны соответствовать правилам HIPAA для обеспечения конфиденциальности и безопасности данных пациентов
2	Закон о защите конфиденциальности детей в Интернете (COPPA)	COPPA налагает требования на веб-сайты и онлайн-сервисы, ориентированные на детей младше 13 лет, обеспечивая защиту их личной информации
3	Закон Грэмма-Лича-Блайли (GLBA)	Закон GLBA требует от финансовых учреждений защищать данные потребителей и объяснять свою практику обмена информацией, которая применяется к системам ИИ, используемым в финансовых услугах
4	Закон о добросовестной кредитной отчетности (FCRA)	FCRA обеспечивает точность, справедливость и конфиденциальность информации о потребителях в кредитной отчетности, влияя на системы искусственного интеллекта, используемые при оценке кредитоспособности и кредитовании
5	Закон о Федеральной торговой комиссии (FTC Act)	FTC Act запрещает недобросовестную или обманную практику, в том числе на системы ИИ, которые могут вводить потребителей в заблуждение или неправомерно использовать их данные
		Законы штатов
6	Закон Калифорнии о защите прав потребителей (CCPA)	CCPA предоставляет жителям Калифорнии права на их персональные данные и налагает обязанности по защите данных на предприятия, что существенно влияет на практику использования данных ИИ
7	Закон Калифорнии о правах на конфиденциальность (CPRA)	CPRA усиливает CCPA, добавляя новые меры защиты и создавая Агентство по защите конфиденциальности Калифорнии для обеспечения соблюдения этих правил
8	Закон Нью-Йорка SHIELD	Этот закон усиливает требования к защите данных и уведомлению об утечках, затрагивая системы ИИ, которые обрабатывают персональные данные жителей Нью-Йорка
		Руководства и рамочные соглашения
9	Закон об алгоритмической ответственности	Предлагаемое законодательство, которое потребует от компаний оценивать воздействие автоматизированных систем принятия решений и устранять потенциальный вред
10	Структура управления рисками ИИ НИСТ	Национальный институт стандартов и технологий (НИСТ) предоставляет рекомендации по повышению надежности систем ИИ, уделяя особое внимание таким принципам, как точность, объяснимость и безопасность
11	Проект Белого дома по Биллю о правах ИИ	В этом документе изложены принципы защиты людей от вреда, связанного с ИИ, с упором на прозрачность, справедливость и подотчетность при использовании ИИ
		Отраслевые рекомендации
12	Глобальная инициатива IEEE по этике автономных и интеллектуальных систем	IEEE предоставляет стандарты и рекомендации по этичному проектированию и внедрению систем ИИ, продвигая такие ценности, как прозрачность и подотчетность
13	Партнерство по ИИ	Отраслевой консорциум, который разрабатывает лучшие практики для технологий ИИ, включая руководящие принципы справедливости, прозрачности и подотчетности
Примечание – составлено авторами на основе данных из источников [11-23]		

Эти законы играют ключевую роль в регулировании применения ИИ в сферах здравоохранения, финансов и потребительской отчетности, обеспечивая безопасность и прозрачность данных. Законы отдельных штатов, включая Закон Калифорнии о защите конфиденциальности потребителей (CCPA), Закон Калифорнии о правах на конфиденциальность (CPRA) и Закон Нью-Йорка SHIELD, существенно усиливают меры по защите данных, обеспечивая дополнительные гарантии для пользователей. Эти нормативные акты оказывают значительное влияние на использование данных и внедрение ИИ в пределах их юрисдикций, формируя более строгие стандарты безопасности и конфиденциальности.

Помимо этого, специальные руководства и рамки для ИИ, такие как Закон об алгоритмической ответственности, Структура управления рисками ИИ, разработанная НИСТ, и Проект Белого дома по Биллю о правах ИИ, направлены на этическое развитие технологий. Эти документы акцентируют внимание на таких принципах, как справедливость, прозрачность и подотчетность.

Отраслевые инициативы, такие как Глобальная инициатива IEEE по этике автономных и интеллектуальных систем и Партнерство по ИИ, играют важную роль в формировании передовых стандартов для разработки и внедрения ИИ. Эти инициативы способствуют ответственному развертыванию и использованию технологий, обеспечивая соблюдение этических норм. В совокупности нормативные акты и руководства направлены на поддержание баланса между технологическими инновациями, защитой конфиденциальности и этическими принципами, что особенно актуально в условиях стремительного развития ИИ в Соединенных Штатах.

Централизованное регулирование в Китае на национальном уровне охватывает такие ключевые аспекты, как защита конфиденциальности данных, кибербезопасность и этические стандарты в области ИИ. Это подчеркивает стремление страны не только развивать технологии искусственного интеллекта, но и гарантировать, что их развитие соответствует интересам национальной безопасности и социальной стабильности.

Основные нормативно-правовые акты Китая в области управления открытыми данными, применимыми к ИИ, представлены в таблице 3.

Таблица 3. Нормативные документы, регулирующие открытые данные в Китае

№	*Название документа*	*Содержание*
		Национальные законы
1	*Закон о защите личной информации (PIPL)*	*PIPL регулирует сбор, использование и хранение личной информации, налагая строгие требования на обработчиков данных, в том числе тех, кто использует системы ИИ*
2	*Закон о кибербезопасности (CSL)*	*CSL регулирует операторов сетей и критически важную информационную инфраструктуру (CII), налагая строгие требования на локализацию данных и меры безопасности. Этот закон имеет решающее значение для систем ИИ, которые обрабатывают значительные объемы персональных и конфиденциальных данных*
3	*Закон о безопасности данных (DSL)*	*DSL устанавливает структуру для категоризации данных на основе их важности для национальной безопасности и экономики. Он требует от организаций, обрабатывающих критически важные данные, внедрять меры безопасности и проводить оценку рисков*
		Руководства и рамочные документы
4	*План развития искусственного интеллекта нового поколения (AIDP)*	*AIDP описывает стратегический подход Китая к тому, чтобы стать мировым лидером в области ИИ к 2030 году. Он подчеркивает разработку стандартов ИИ и этических принципов, особенно касающихся конфиденциальности и безопасности данных*
5	*Этические нормы для искусственного*	*выпущенные в 2021 году, эти нормы содержат этические принципы разработки и использования ИИ, уделяя особое внимание таким вопросам, как защита конфиденциальности, справедливость и*

	интеллекта нового поколения	*прозрачность. Они направлены на обеспечение ответственной и этичной разработки технологий ИИ*
6	*Руководящие принципы управления искусственным интеллектом*	*В данных руководящих принципах подчеркивается важность этической разработки ИИ, включая уважение конфиденциальности, обеспечение справедливости и повышение прозрачности в системах ИИ*
7	*Принципы управления ИИ в Китае*	*Разработанные Пекинской академией искусственного интеллекта (BAAI), эти принципы излагают основные положения этического ИИ, включая защиту конфиденциальности, безопасность данных и социальное воздействие технологий ИИ*
Примечание – составлено авторами на основе данных из источников [24-25]		

Как показано в таблице 3, национальные законы Китая, такие как Закон о защите персональных данных (PIPL), Закон о кибербезопасности (CSL) и Закон о безопасности данных (DSL), регулируют сбор, использование и хранение данных, устанавливая строгие требования для обработчиков данных, включая те, кто использует системы ИИ. В дополнение к этому, такие документы, как План развития искусственного интеллекта нового поколения (AIDP) и Этические нормы для ИИ нового поколения, подчеркивают важность соблюдения стандартов и этических принципов при разработке ИИ, уделяя особое внимание защите конфиденциальности, справедливости и прозрачности. Также рекомендации Пекинской академии искусственного интеллекта способствуют внедрению этических практик, обеспечивая ответственное развертывание ИИ и его позитивное влияние на общество.

Соблюдение законодательства и нормативных актов в Китае контролируется такими государственными органами, как Администрация киберпространства Китая (CAC), Министерство промышленности и информационных технологий (MIIT) и Министерство общественной безопасности (MPS). Эти учреждения проводят инспекции, накладывают штрафы и требуют корректирующих мер для обеспечения соблюдения норм. Таким образом, компании, использующие технологии ИИ, обязаны регулярно проводить аудиты, внедрять эффективные меры защиты данных и обеспечивать прозрачность в своих практиках обработки информации. Невыполнение требований может повлечь за собой серьезные последствия, включая значительные штрафы, приостановление деятельности и даже уголовную ответственность.

Анализ практики открытости у американских и китайских технологических гигантов, а также нормативных актов, регулирующих эти вопросы в обеих странах, выявил ряд препятствий, которые можно классифицировать на три категории:

- проблемы конфиденциальности;
- коммерческие интересы;
- геополитические факторы.

Проблемы конфиденциальности имеют первостепенное значение, поскольку как американским, так и китайским компаниям необходимо ориентироваться в сложной нормативной среде для обеспечения защиты данных. Например, такие компании, как Google и Facebook, собирают огромные объемы пользовательских данных для своих приложений ИИ, что вызывает обеспокоенность в отношении согласия пользователей, безопасности данных и возможности их неправомерного использования. В свою очередь, китайские компании, такие как Alibaba и Tencent, также занимаются сбором значительных объемов пользовательской информации, однако контроль за вопросами конфиденциальности и доступом к личным данным осуществляется правительственными органами.

Коммерческие интересы также могут служить препятствием для открытости данных, так как они предоставляют компаниям конкурентные преимущества. Например, американские гиганты, такие как Google и Amazon, используют открытые данные и свои собственные базы данных для оптимизации алгоритмов ИИ, особенно в таких областях, как поиск, реклама и

облачные вычисления. Аналогично, китайские компании, такие как Alibaba и Tencent, применяют открытые данные для инноваций в электронной коммерции и ИИ-услугах. Однако в отличие от своих американских коллег, китайское правительство активно способствует обмену данными между национальными технологическими компаниями, что помогает ускорить технологический прогресс.

Геополитические факторы значительно затрудняют открытость данных в сфере разработки ИИ, особенно между компаниями США и Китая. В обеих странах действуют строгие законы о локализации данных, требующие хранения и обработки собранной информации внутри страны. Это ограничивает свободный трансграничный поток данных. Кроме того, США вводят экспортные ограничения на технологии ИИ, чтобы предотвратить их передачу в Китай, ссылаясь на угрозы национальной безопасности. В то же время, Китай также разрабатывает правила, регулирующие экспорт технологий, связанных с ИИ, с целью защиты своих технологических достижений. Правительство США рассматривает китайские технологические компании как потенциальную угрозу для своей национальной безопасности.

Продолжающиеся торговые войны и экономическая политика США в отношении Китая создают атмосферу неопределенности и недоверия. Введение тарифов, санкций и других торговых барьеров нарушает цепочки поставок технологий и поток данных, критически важных для исследований и разработок в области ИИ. Эта геополитическая напряженность препятствует участию IT-компаний обеих стран в инициативах и сотрудничестве, касающемся открытых данных.

Несмотря на существующие препятствия, имеются значительные возможности для расширения сотрудничества в области открытых данных и развития ИИ. Эти возможности охватывают совместные исследовательские инициативы, создание общих репозиториев данных, стандартизацию и академические партнерства.

Например, компании Google и Tencent работают вместе над развитием ИИ, стремясь объединить свои сильные стороны в технологиях и инновациях. Объединив свои ресурсы и экспертизу, они могут более эффективно решать сложные задачи и стимулировать инновации в сфере ИИ. Кроме того, сотрудничество между Microsoft Research и Пекинским университетом в рамках проекта открытых данных позволило создать общий репозиторий на основе анонимизированных и агрегированных данных. Это сотрудничество значительно упрощает доступ к разнообразным наборам данных, необходимым для обучения моделей ИИ.

США и Китай имеют перспективы для развития сотрудничества в рамках Международной организации по стандартизации (ISO) в области разработки общих фреймворков для взаимодействия и обеспечения безопасности данных, что может положительно сказаться на глобальной технологической экосистеме. Кроме того, академическое сотрудничество (академические программы, конференции, семинары) может способствовать обмену знаниями и формированию следующего поколения исследователей в области ИИ. Например, партнерство между Stanford University и Tsinghua University привело к значительным достижениям в исследованиях ИИ, продемонстрировав огромный потенциал академического сотрудничества.

Также стоит отметить участие Alibaba и IBM в консорциуме, который нацелен на разработку решений для решения глобальных проблем, что является примером совместной отраслевой инициативы. Эти усилия направлены на конкретные области, такие как создание ИИ-приложений, здравоохранение или строительство умных городов.

Эти совместные возможности подчеркивают потенциал американских и китайских IT-компаний для стимулирования инноваций и прогресса в области ИИ через инициативы открытых данных.

Дискуссия

Данное исследование подчеркивает значительные различия в практиках открытости данных среди крупных технологических компаний США и Китая, выявляя различные

подходы к содействию развитию ИИ через использование открытых данных. Сравнительный анализ таких компаний, как Microsoft, Apple, Amazon, Google, Facebook, Tencent и Alibaba, демонстрирует различные уровни прозрачности, доступности и сотрудничества в их практиках обмена данными.

Американские технологические гиганты, такие как Microsoft, Google и Amazon, характеризуются более высоким уровнем открытости данных. Они активно продвигают публичный доступ и поддерживают инициативы, связанные с открытыми данными. Например, компания Microsoft Open Data Campaign и платформа Google Cloud Public Datasets предоставляют обширные наборы данных для широкой аудитории, способствуя инновациям и исследовательской деятельности. Публичные наборы данных AWS и AWS Marketplace от компании Amazon облегчают обмен данными и доступ к ним, поддерживая разнообразные приложения в области ИИ.

Эти усилия поддерживаются нормативной средой, которая поощряет инновации, одновременно защищая конфиденциальность. Федеральные законы, такие как Закон о переносимости и подотчетности медицинского страхования (HIPAA) и Закон Калифорнии о защите прав потребителей (CCPA), обеспечивают защиту конфиденциальности и безопасности данных, создавая сбалансированную структуру для обмена информацией. Отраслевые руководства и структуры, такие как Структура управления рисками ИИ Национального института стандартов и технологий (НИСТ), дополнительно способствуют развитию этических аспектов использования ИИ.

В отличие от этого, китайские технологические компании, такие как Tencent и Alibaba, проявляют более консервативный подход к обмену данными. Эти компании акцентируют внимание на внутреннем использовании данных и стратегических партнерствах, а не на открытости для широкой аудитории. Например, WeChat Open Platform и Alibaba Cloud предоставляют ограниченный доступ к наборам данных по сравнению с американскими аналогами, что свидетельствует о более осторожном подходе, обусловленным строгим нормативным контролем.

Централизованная нормативная база Китая акцентирует внимание на безопасности данных и суверенитете, при этом законы, такие как Закон о защите личной информации (PIPL) и Закон о кибербезопасности (CSL), устанавливают строгие меры по защите данных. Эти правила подчеркивают стремление правительства сохранять контроль над данными в пределах своих границ, что сказывается на степени открытости в практике обмена данными.

Различия в нормативной среде и практике открытости данных в США и Китае имеют значительные последствия для международного сотрудничества в сфере развития ИИ. Активное участие американских компаний в инициативах по открытым данным способствует трансграничному исследовательскому сотрудничеству и инновациям, способствуя глобальному развитию ИИ. Прозрачность и доступность данных, предлагаемые этими компаниями, позволяют исследователям и разработчикам со всего мира создавать и улучшать модели ИИ, что в свою очередь способствует прогрессу в различных секторах.

Однако ограничительная практика обмена данными и строгий нормативный контроль в Китае создают препятствия для международного сотрудничества. Акцент на безопасности данных и суверенитете сдерживает доступность китайских наборов данных для глобальных исследований, что мешает совместным усилиям. Геополитическая напряженность дополнительно усложняет соглашения об обмене данными, так как опасения по поводу конфиденциальности и безопасности могут подрывать доверие и сотрудничество.

Несмотря на эти проблемы, существуют возможности для гармонизации правил обработки данных и содействия международному сотрудничеству. Разработка рамок для надежного обмена данными, которые сбалансируют проблемы конфиденциальности и безопасности с необходимостью открытых данных, может способствовать улучшению взаимодействия. Такие инициативы, как предлагаемый Закон об алгоритмической ответственности в США и международные партнерства, такие как Глобальная инициатива IEEE по этике автономных и

интеллектуальных систем, могут служить руководством для этичной и прозрачной разработки ИИ.

Создание платформ для диалога и сотрудничества между американскими и китайскими компаниями и регулирующими органами может помочь устранить пробелы в практике обмена данными. Устанавливая общие стандарты и протоколы для конфиденциальности и безопасности данных, обе страны могут работать над более совместным подходом к разработке ИИ, используя свои объединенные опыт и ресурсы.

Заключение

В разработке ИИ международное сотрудничество играет ключевую роль, в частности в области открытых данных. Сравнительный анализ технологических компаний США и Китая выявляет различные подходы к обмену данными, на которые влияют разность в нормативной среде и политические-экономические приоритеты каждой страны.

Американские компании демонстрируют более высокую степень открытости данных, поддерживаемую нормативной базой, которая балансирует инновации и защиту конфиденциальности. Это способствует глобальному исследовательскому сотрудничеству и развитию ИИ в различных секторах. В то время как китайские компании придерживаются более консервативных практик обмена данными, что отражает строгий нормативный контроль и акцент на безопасности данных и суверенитете.

Эти различия создают препятствия для международного сотрудничества, подчеркивая необходимость гармонизированных правил и надежных рамок обмена данными. Содействуя диалогу и сотрудничеству между компаниями и регулирующими органами обеих стран, можно преодолеть эти проблемы и максимально использовать потенциал ИИ для решения глобальных вызовов.

Будущие исследования должны сосредоточиться на стратегиях повышения открытости данных при обеспечении конфиденциальности и безопасности, подчеркивая влияние меняющихся правил на развитие ИИ. Кроме того, изучение успешных моделей международного сотрудничества в области ИИ может предоставить полезные рекомендации по передовым практикам для содействия глобальному сотрудничеству в этой быстро развивающейся сфере.

Благодарность

Данное исследование проведено в рамках реализации научного проекта ИРН AP19678623, финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

[1] Haenlein M., Kaplan A. A brief history of artificial intelligence: On the past, present, and future of artificial intelligence // California Management Review. – 2019. – Vol. 61(4). – P. 5-14.

[2] Davenport T., Kalakota R. The potential for artificial intelligence in healthcare // Future Healthcare Journal. – 2019. – Vol. 6(2). – P. 94-98.

[3] Li D., Xi, Y. Research on the development strategy of artificial intelligence industry in China // Management Review. – 2018. – Vol. 30(5). – P. 123-131.

[4] McAfee A., Brynjolfsson E. Big data: The management revolution // Harvard Business Review. – 2012. – Vol. 90(10). – P. 61-67.

[5] Chen M., Mao S., Liu Y. Big data: A survey // Mobile Networks and Applications. – 2014. – Vol. 19(2). – P. 171-209.

[6] McQuinn A., Castro D. A Grand Bargain on Data Privacy Legislation for America. – Information Technology and Innovation Foundation, 2019. – 75 p.

[7] Yang Y. The evolution of data protection law in China: Privacy and security regulation from a comparative perspective // Information & Communications Technology Law. – 2021. – Vol. 30(2). P. 183-199.

[8] Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Vayena E. AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations // Minds and Machines. – 2018. – Vol. 28(4). – P. 689-707.

[9] Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR). A Practical Guide, 1st Edn. Cham. – Springer International Publishing, 2017. DOI: https://doi.org/10.1007/978-3-319-57959-7

[10] Zeng J. China's Artificial Intelligence Revolution: Progress and Challenges // International Journal of Chinese Studies. – 2020. – Vol. 11(1). – P. 45-60.

[11] Health Insurance Portability and Accountability Act (HIPAA) [Электронный ресурс] // Department of Health and Human Services. – 2020. – URL: https://www.hhs.gov/hipaa/index.html (дата обращения: 25.05.2024).

[12] Children's Online Privacy Protection Act (COPPA) [Электронный ресурс] // Federal Trade Commission. – 2020. – URL: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (дата обращения: 25.05.2024).

[13] Gramm-Leach-Bliley Act (GLBA) [Электронный ресурс] // Federal Trade Commission. – 2020. – URL: https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act (дата обращения: 25.05.2024).

[14] Fair Credit Reporting Act [Электронный ресурс] // Consumer Financial Protection Bureau. – 2020. – URL: https://www.consumerfinance.gov/rules-policy/regulations/1039/ (дата обращения: 25.05.2024).

[15] Federal Trade Commission Act [Электронный ресурс] // Federal Trade Commission. – 2020. – URL: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (дата обращения: 15.05.2024).

[16] California Consumer Privacy Act (CCPA) [Электронный ресурс] // California State Legislature. – 2018. – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (дата обращения: 15.05.2024).

[17] California Privacy Rights Act (CPRA) [Электронный ресурс] // California State Legislature. – 2020. – URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1281 (дата обращения: 15.05.2024).

[18] New York SHIELD Act [Электронный ресурс] // New York State Legislature. – 2019. – URL: https://www.nysenate.gov/legislation/bills/2019/s5575 (дата обращения: 10.05.2024).

[19] Algorithmic Accountability Act [Электронный ресурс] // U.S. Congress. – 2019. – URL: https://www.congress.gov/bill/116th-congress/house-bill/2231/text (дата обращения: 10.05.2024).

[20] NIST AI Risk Management Framework [Электронный ресурс] // National Institute of Standards and Technology. – 2021. – URL: https://www.nist.gov/artificial-intelligence/ai-risk-management-framework (дата обращения: 23.04.2024).

[21] Blueprint for an AI Bill of Rights [Электронный ресурс] // White House Office of Science and Technology Policy. – 2022. – URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (дата обращения: 15.04.2024).

[22] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems [Электронный ресурс] // IEEE. – 2020. – URL: https://ethicsinaction.ieee.org/ (дата обращения: 16.04.2024).

[23] About a partnership [Электронный ресурс] // Partnership on AI. – 2020. – URL: https://www.partnershiponai.org/about/ (дата обращения: 25.05.2024).

[24] Personal Information Protection Law (PIPL) [Электронный ресурс] // Standing Committee of the National People's Congress. – 2021. – URL: http://www.npc.gov.cn/ (дата обращения: 20.05.2024).

[25] New Generation Artificial Intelligence Development Plan (AIDP) [Электронный ресурс] // State Council of the People's Republic of China. – 2017. – URL: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 23.05.2024).

References

[1] Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. California Management Review, 61(4), 5-14

[2] Davenport, T., & Kalakota, R. (2019). The potential for artificial intelligence in healthcare. Future Healthcare Journal, 6(2), 94-98

[3] Li, D., & Xi, Y. (2018). Research on the development strategy of artificial intelligence industry in China. Management Review, 30(5), 123-131.

[4] McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review, 90(10), 61-67.

[5] Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. Mobile Networks and Applications, 19(2), 171-209.

[6] McQuinn, A., & Castro, D. (2019). A Grand Bargain on Data Privacy Legislation for America. Information Technology and Innovation Foundation, 75 p.

[7] Yang, Y. (2021). The evolution of data protection law in China: Privacy and security regulation from a comparative perspective. Information & Communications Technology Law, 30(2), 183-199.

[8] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689-707.

[9] Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide, 1st Edn. Cham: Springer International Publishing, https://doi.org/10.1007/978-3-319-57959-7.

[10] Zeng, J. (2020). China's Artificial Intelligence Revolution: Progress and Challenges. International Journal of Chinese Studies, 11(1), 45-60.

[11] Health Insurance Portability and Accountability Act (HIPAA) (2020) [Electronic source]. Department of Health and Human Services. Retrieved from: https://www.hhs.gov/hipaa/index.html (accessed: 25.05.2024).

[12] Children's Online Privacy Protection Act (COPPA) (2020) [Electronic source]. Federal Trade Commission. Retrieved from: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa (accessed: 25.05.2024).

[13] Gramm-Leach-Bliley Act (GLBA) (2020) [Electronic source]. Federal Trade Commission. Retrieved from: https://www.ftc.gov/enforcement/statutes/gramm-leach-bliley-act (accessed: 25.05.2024).

[14] Fair Credit Reporting Act (2020) [Electronic source]. Consumer Financial Protection Bureau. Retrieved from: https://www.consumerfinance.gov/rules-policy/regulations/1039/ (accessed: 25.05.2024).

[15] Federal Trade Commission Act (2020) [Electronic source]. Federal Trade Commission. Retrieved from: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act (accessed: 15.05.2024).

[16] California Consumer Privacy Act (CCPA) (2018) [Electronic source]. California State Legislature. Retrieved from: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (accessed: 15.05.2024).

[17] California Privacy Rights Act (CPRA) (2020) [Electronic source]. California State Legislature. Retrieved from: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1281 (accessed: 15.05.2024).

[18] New York SHIELD Act (2019) [Electronic source]. New York State Legislature. Retrieved from: https://www.nysenate.gov/legislation/bills/2019/s5575 (accessed: 10.05.2024).

[19] Algorithmic Accountability Act (2019) [Electronic source]. U.S. Congress. Retrieved from: https://www.congress.gov/bill/116th-congress/house-bill/2231/text (accessed: 10.05.2024).

[20] NIST AI Risk Management Framework (2021) [Electronic source]. National Institute of Standards and Technology. Retrieved from: https://www.nist.gov/artificial-intelligence/ai-risk-management-framework (accessed: 23.04.2024).

[21] Blueprint for an AI Bill of Rights (2022) [Electronic source]. White House Office of Science and Technology Policy. Retrieved from: https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (accessed: 15.04.2024).

[22] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (2020) [Electronic source]. IEEE. Retrieved from: https://ethicsinaction.ieee.org/ (accessed: 16.04.2024).

[23] About a partnership (2020) [Electronic source]. Partnership on AI. Retrieved from: https://www.partnershiponai.org/about/ (accessed: 25.05.2024).

[24] Personal Information Protection Law (PIPL) (2021) [Electronic source]. Standing Committee of the National People's Congress. Retrieved from: http://www.npc.gov.cn/ (accessed: 20.05.2024).

[25] New Generation Artificial Intelligence Development Plan (AIDP) (2017) [Electronic source]. State Council of the People's Republic of China. Retrieved from: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (accessed: 23.05.2024).