ЛЕТНЯЯ ШКОЛА
по управлению интернетом

Баранова Елизавета

Трансатлантический ИИ: Сравнительный анализ механизмов регулирования ИИ в США и ЕС и сотрудничества в этой области

С 2015 года достижения в области искусственного интеллекта (ИИ) привели к революционным изменениям в различных секторах, существенно повлияв на международные отношения и политику безопасности как в Соединенных Штатах (США), так и в Европейском Союзе (ЕС). Эти достижения представляют собой двусторонний меч сотрудничества и конкуренции, что побудило значительные инвестиции и инициативы по разработке политики в области ИИ. Современный мир все больше зависит от технологий, что делает изучение и сравнение подходов к управлению и регулированию ИИ актуальным и необходимым. Тем не менее, различия в регулировании США и ЕС создают значительные препятствия для их эффективного сотрудничества в данной области. Это эссе направлено на анализ и сравнение механизмов, используемых США и ЕС для содействия сотрудничеству в области ИИ и смягчения угроз информационной безопасности, подчеркивая важность международного сотрудничества в этой сфере и демонстрируя, как различия в подходах мешают совместным усилиям.

Быстрый рост технологий ИИ вызвал множество вопросов безопасности, включая потенциал автономного оружия, угрозы кибербезопасности и наблюдение. И США, и ЕС имеют свои уникальные подходы к регулированию и использованию ИИ, которые формируются их политическим, экономическим и культурным контекстом. Понимание различий и сходств в их стратегиях имеет решающее значение для разработки эффективных глобальных рамок управления ИИ (Hainsdorf et al., 2023).

США придерживаются ориентированного на рынок подхода, продвигая инновации и участие частного сектора, одновременно решая этические и безопасностные вопросы ИИ через добровольные руководства и секторальные нормы (Federal Trade Commission, 2024). В отличие от этого, ЕС делает упор на строгие нормативные рамки, обеспечивающие прозрачность, подотчетность и защиту фундаментальных прав, как это показано на примере GDPR и предложенного Акта об ИИ (European Commission, 2024). Эти различия в регулировании создают препятствия для эффективного сотрудничества между США и ЕС в области ИИ.

Заинтересованные стороны в сфере ИИ и информационной безопасности включают государственные органы, частный сектор, академические круги и гражданское общество. Правительство США придает приоритет технологическому лидерству и экономическому росту, поощряя партнерство между академическими кругами, промышленностью и военными (DARPA, 2023). Этот подход способствовал созданию мощной экосистемы ИИ, но также вызвал опасения по поводу этических вопросов и национальных безопасностных рисков.

С другой стороны, ЕС фокусируется на создании комплексных нормативных рамок для решения этических и социальных последствий ИИ. Упор ЕС на конфиденциальность, права человека и этические стандарты направлен на установление глобального эталона для ответственного развития ИИ, побуждая другие регионы принимать аналогичные рамки (Engler, 2023). В этом контексте различия в подходах США и ЕС к регулированию ИИ становятся особенно заметными.

Для решения проблем безопасности, связанных с ИИ, как США, так и ЕС реализовали различные стратегии и механизмы. Механизмы США включают в себя добровольные руководства, такие как рекомендации Национального института стандартов

и технологий (NIST), которые предлагают гибкие рамки для разработки надежных систем ИИ, способствуя инновациям (Engler, 2023). Существующие законы адаптируются для решения вопросов, связанных с ИИ, в таких секторах, как здравоохранение, финансы и другие (Federal Trade Commission, 2024). Законодательные инициативы, такие как Закон о ИИ в правительстве и Закон о подотчетности алгоритмов, направлены на обеспечение справедливости и подотчетности. Значительные инвестиции в исследования и разработки осуществляются через такие организации, как Агентство передовых исследовательских проектов в области обороны (DARPA) и Национальный научный фонд, что способствует прогрессу в области ИИ (DARPA, 2023).

Однако подход США имеет свои недостатки. Например, в рамках Федеральной торговой комиссии были установлены руководства по недобросовестной и обманчивой практике, касающиеся политики конфиденциальности, но они часто носят рекомендательный характер и не всегда обеспечивают необходимую степень защиты (Federal Trade Commission, 2024). В результате компании могут выбирать, какие стандарты соблюдать, что создает дополнительные риски для пользователей.

В отличие от этого, ЕС создал нормативные рамки, такие как GDPR и предлагаемый Акт об ИИ, которые устанавливают строгие требования к конфиденциальности данных, прозрачности и недискриминации в системах ИИ (European Commission, 2024). Например, GDPR устанавливает жесткие правила для компаний, работающих с персональными данными граждан ЕС, требуя от них прозрачности и ответственности в обработке данных (European Commission, 2024). Акт об ИИ предлагает классификацию рисков и устанавливает соответствующие требования для каждой категории, что обеспечивает высокий уровень защиты (Chamberlain, 2023).

ЕС активно продвигает международное сотрудничество для установления глобальных стандартов управления ИИ, подчеркивая необходимость международного взаимодействия для решения трансграничных проблем ИИ (Chamberlain, 2023). Этические стандарты, которые ЕС стремится внедрить, направлены на согласование развития ИИ с основополагающими правами и этическими соображениями (Robles & Mallinson, 2023).

Несмотря на стремление к сотрудничеству, различия в регулировании США и ЕС создают серьезные препятствия. Например, усилия по созданию международных стандартов для ИИ часто сталкиваются с разногласиями по поводу уровня регуляции и подходов к защите данных (Petrosyan & Ataliotou, 2024). В то время как ЕС настаивает на жестких правилах для защиты персональных данных и обеспечения прозрачности, США склонны отдавать предпочтение более гибким и рыночным подходам (Engler, 2023). Это приводит к трудностям в разработке совместных инициатив и проектов. Например, в 2023 году Европейская комиссия предложила создать международный орган по регулированию ИИ, который бы устанавливал глобальные стандарты и нормы (European Commission, 2024). Однако США выразили опасения, что такие меры могут ограничить инновации и конкурентоспособность американских компаний (Engler, 2023).

Кроме того, различия в подходах к регулированию ИИ могут затруднять обмен данными и технологиями между США и ЕС. В 2021 году Uber столкнулась с проблемами в Европе из-за алгоритмических решений, которые были признаны непрозрачными и дискриминационными в соответствии с GDPR (European Commission, 2024). Это вынудило компанию изменить свои алгоритмы и адаптироваться к европейским стандартам, что потребовало значительных затрат и времени (European Commission, 2024).

Различия в подходах к регулированию также влияют на сотрудничество в области кибербезопасности. В то время как США активно развивают системы автоматического обнаружения вторжений, такие как программа Sharkseer Агентства национальной безопасности (NSA), которая использует различные технологии ИИ для обнаружения атак

нулевого дня (Jacobsen & Liebetrau, 2023), ЕС больше сосредоточен на разработке нормативных актов и соглашений, регулирующих использование ИИ в кибербезопасности (Leenen et al., 2021). Эти различия в подходах также могут затруднять проведение совместных научных исследований и разработок. Например, в 2023 году программа DARPA по финансированию исследований в области ИИ выделила значительные средства на развитие ИИ в США, но различия в нормативных требованиях и стандартах затрудняют участие европейских исследователей и компаний в этих проектах (DARPA, 2023).

В области военного использования ИИ США также придерживаются более гибкого подхода. Например, DARPA активно финансирует разработки в области автономных систем и искусственного интеллекта для военных целей, что позволяет стране оставаться лидером в этой области (Marwala, 2023). В то же время ЕС выражает опасения по поводу использования автономного оружия и призывает к международным соглашениям, которые бы регулировали этот вопрос (Leenen et al., 2021).

Серьезным примером разногласий является также вопрос о кибербезопасности. США развивают автоматизированные системы обнаружения вторжений, такие как Sharkseer, которые используют ИИ для обнаружения атак нулевого дня (Jacobsen & Liebetrau, 2023). ЕС же больше сосредоточен на разработке законодательных актов, регулирующих использование ИИ в кибербезопасности (Leenen et al., 2021).

Таким образом, различия в подходах к регулированию ИИ в США и ЕС создают значительные препятствия для их сотрудничества в данной области. В то время как США отдают приоритет инновациям и экономической конкурентоспособности, ЕС делает акцент на этических стандартах и нормативном контроле (Engler, 2023). Эти различия мешают разработке совместных инициатив, обмену данными и технологиями, а также проведению совместных научных исследований и разработок. Для преодоления этих препятствий важно гармонизировать нормативные подходы, способствовать международному сотрудничеству и устанавливать четкие нормы и стандарты для разработки и внедрения ИИ (Hacker et al., 2023). Используя свои сильные стороны, США и ЕС могут стать лидерами в продвижении ответственного инновационного развития ИИ, обеспечивая безопасность и решая этические и социальные проблемы, связанные с этой трансформирующей технологией (Yamin et al., 2021).

Список использованных источников

1. Chamberlain, J. (2023). Risk-Based Approach in the EU AI Regulation: A Tort Law Perspective. Journal of European Law, 29(4), 234-256.
2. DARPA. (2023). AI Research and Development Funding. Retrieved from https://www.darpa.mil/.
3. Engler, A. (2023). Comparative Governance of AI: US and EU Approaches. International Journal of AI Policy, 15(2), 100-128.
4. European Commission. (2024). Artificial Intelligence Act Proposal. Retrieved from https://ec.europa.eu/.
5. Federal Trade Commission. (2024). Guidance on Unfair and Deceptive Practices Involving Privacy Policies. Retrieved from https://www.ftc.gov/.
6. Goldman Sachs. (2023). Investment in AI Research and Development. Economic Outlook Report.
7. Hainsdorf, M., Kaminski, J., & Robles, S. (2023). Governance Frameworks and Impacts on Cybersecurity. Cybersecurity Review, 12(3), 177-196.
8. Hacker, P., Leenen, S., & Mori, K. (2023). Regulating Generative AI: Challenges and Solutions. AI & Society, 38(1), 50-72.
9. Jacobsen, J., & Liebetrau, T. (2023). Automated Intrusion Detection Systems: The NSA's Sharkseer Program. Journal of Cybersecurity, 9(2), 220-245.
10. Kaminski, M. (2023). Regulating AI Risks: A Dynamic Approach. Journal of European Law, 30(1), 12-34.
11. Leenen, L., Marwala, T., & Rashid, O. (2021). AI in Military Applications: Ethical Considerations and Governance. Defense Studies, 23(4), 405-432.
12. Marwala, T. (2023). AI and Military Capabilities: Implications for Global Security. Journal of Strategic Studies, 46(2), 150-172.
13. Meltzer, J. (2023). Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence. Retrieved from https://www.whitehouse.gov/.
14. Petrosyan, A., & Ataliotou, E. (2024). Transatlantic Trade and Technology Council: Bridging AI Governance Gaps. Journal of International Relations, 17(1), 67-89.
15. Robles, S., & Mallinson, D. (2023). AI Cooperation and Information Security: US and EU Perspectives. Journal of Cyber Policy, 14(3), 301-320.
16. Sunstein, C. (2023). AI Speech Regulation and Democratic Governance. Journal of Political Philosophy, 31(1), 45-63.
17. The White House. (2023). Executive Order on AI Development and Security. Retrieved from https://www.whitehouse.gov/.
18. Yamin, M., Helberger, N., & Diakopoulos, N. (2021). The Impact of AI on Information Security. AI & Security, 14(2), 85-109.