Секция «Современная политика в условиях цифровых трансформаций и развития технологий искусственного интеллекта.»

Глобальные технологические риски современности: основные тренды, реагирование государств и международные последствия

Сорокова Екатерина Дмитриевна
Аспирант
Московский государственный институт международных отношений, Москва, Россия
E-mail: sorokova.e.d@my.mgimo.ru

Риски, связанные с прогрессом и применением технологий, стали выделяться учеными в качестве самостоятельной группы рисков современности с начала их активных исследований в 1970-х гг. В рамках социологического подхода значимый вклад в изучение технологических рисков внесли У.Бек, Э.Гидденс, Н.Луман. С конца XX в. рискология развивалась в направлении социализации и гуманитаризации исследуемых феноменов, сочетала различные методологические подходы, становилась более междисциплинарной [1].

Оценить **ландшафт современных технологических рисков** и выделить среди них сквозные - приоритетные для экспертного сообщества, государственных деятелей и бизнеса позволяет анализ экспертных докладов Всемирного экономического форума (ВЭФ). Изучив доклады ВЭФ и перечни технологических рисков за 16 лет их выпуска (2006 г. - н.в.), автор построил «карту рисков», чтобы выявить тенденции и проанализировать изменения. Риски были расположены в хронологическом порядке, а после сгруппированы автором в четыре однородные группы, название которым дал «стабильный» риск, повторяющийся в докладах ежегодно в течение нескольких лет. Выделенные группы связаны с критической информационной инфраструктурой, защитой данных, угрозами от новых технологий (в т.ч., непреднамеренными последствиями их развития и применения, уязвимостью информационного пространства, слабостью режима глобального управления технологиями), а также новейшими рисками (концентрация цифровых силовых ресурсов, цифровое неравенство) [6]. Отметим, что помимо «традиционных» военных и инфраструктурных рисков [3], растущее внимание уделяется социально-гуманитарным аспектам и последствиям применения технологий, которые становятся для государств самостоятельным объектом реагирования.

Можно выделить **несколько основных способов реагирования на обозначенные категории рисков**. Первый связан с ужесточением законодательного регулирования отдельных сфер развития технологий и поведения акторов, в т.ч. для ограничения предсказуемых нежелательных последствий рисков. Среди них - меры по поддержанию стабильности и независимости инфраструктуры (закон «о суверенном Рунете» и импортозамещение в РФ; проект Gaia X в ЕС), требования по защите персональных данных и их локализации (GDPR в ЕС), регулирование деятельности транснациональных цифровых платформ (закон «о приземлении» в РФ; законопроект о цифровых услугах в ЕС).

Однако для регулирования менее предсказуемых последствий рисков требуются более гибкие подходы. Исследователи отмечают, что для этого необходима более кооперативная, мультистейкхолдерная и многоуровневая модель взаимодействия. В частности, предлагается разделить ответственность за создание и соблюдение норм поведения между различными акторами в зависимости от степени риска (государство - в высокорисковых сферах, профессиональные отраслевые объединения - в области средних рисков, компании - низких рисков [2]), а также рассматривать законодательные и «мягкие» этические нормы как взаимодополняющие, а не антагонистические [5].

На уровне международных организаций и профессиональных конференций также ведутся переговорные процессы по созданию технических стандартов (это, например, МСЭ, IEEE, ISO) и «мягких норм» в сфере цифровых технологий - например, в области управления Интернетом (IGF) или этики искусственного интеллекта (в ЮНЕСКО, ОЭСР, Совете Европы и т.д.). Кодификация этических норм делает их более применимыми на практике, позволяет четче сформулировать ответственность акторов на всех этапах жизненного цикла систем искусственного интеллекта (ИИ) и повысить доверие общественности к технологиям [4].

Основываясь на **международных тенденциях**, можно **сделать следующие выводы**.

Государства стремятся сохранить за собой ведущую роль в регулировании цифровых технологий и суверенитет над своим цифровым пространством, хотя в последние годы происходит видимое усиление негосударственных акторов, особенно ТНК - Google, Apple, Meta, Tencent и др.

В отдельных сферах предпринимаются попытки выработать глобальные «правила игры» до возникновения катастрофических последствий, но расхождения в подходах (например, к этике ИИ между ЕС, Китаем и США) уже намечаются. Требования этики также могут стать инструментом «мягкого» влияния и повышения конкурентоспособности своих технологий на мировом рынке.

Режим глобального управления цифровыми технологиями пока нельзя считать сформированным: отсутствуют общепринятые определения ключевых понятий (кибератака, кибер- и информационная безопасность и т.д.), позиции и подходы стран существенно расходятся, остается нерешенным вопрос о полномочиях мультистейкхолдерных форумов и их сочетании с межгосударственными форматами. При всем стремлении международного сообщества предотвратить фрагментацию как Интернета, так и формирующегося регулирования технологий, на данный момент эта риск кажется вполне осязаемым, и выработать стратегию реагирования на него только предстоит.

Источники и литература

1) Зубков В.А. Риск как предмета социологического анализа // Социс, № 4, 1999. С.3-9.
2) Ибрагимов Р.С. и др. Этика и регулирование искусственного интеллекта // Закон, №8, 2021. С. 85-95.
3) Сорокова Е.Д. Глобальные риски военно-политического использования искусственного интеллекта в обществе модерна // Материалы Международного молодежного научного форума «Ломоносов-2021», ООО МАКС Пресс, М, 2021.
4) A.Kuleshov, A.Ignatiev et al. Addressing AI Ethics through Codification // Conference Paper. Proceedings – 2020 International Conference Engineering Technologies and Computer Science, EnT, 2020. С. 24-30.
5) Delacroix S., Wagner B. Constructing a mutually supportive interface between ethics and regulation // Computer Law Security Review, №40, 2021.
6) Global Risks Report / World Economic Forum. 2006-2022.