

## Н.П. Ромашкина

Руководитель подразделения проблем информационной безопасности ЦМБ ИМЭМО РАН, кандидат политических наук

### НОВЕЙШИЕ ПРОДУКТЫ ИКТ: СОТРУДНИЧЕСТВО В РАМКАХ БРИКС

Новейшие или новые технологии можно определить как радикально новые и относительно быстро развивающиеся технологии, характеризующиеся определённой степенью согласованности, сохраняющейся с течением времени, и обладающие потенциалом оказывать значительное влияние на социально-экономические процессы. Это влияние наблюдается с точки зрения состава действующих лиц, институтов и моделей взаимодействия между ними, а также связанной с ними образовательной деятельности. Однако наиболее заметное влияние новых технологий будем наблюдать в будущем, и поэтому на этапе становления они характеризуются высокой степенью неопределённости и неоднозначности.

Инновационные методы и новые технологии создавались и создаются на протяжении веков как результат теоретических исследований или коммерческих разработок, могут носить постепенный характер, а могут быть прорывными, в которых новые методы заменяют предыдущую технологию.

Новые технологии охватывают множество областей: образование, строительство, медицину, биологию, сельское хозяйство, энергетику, военную сферу и, конечно, наиболее быстро развивающуюся область — электронику и информационно-коммуникационные технологии.

По сути, новые информационно-коммуникационные технологии (ИКТ) — это технические инновации, которые представляют собой прогрессивные разработки в областях, обеспечивающих конкурентное преимущество. Эти технологии могут включать и старые инструменты в сфере информационно-коммуникационных возможностей, которые находят новое применение.

К новым ИКТ-продуктам относятся *сотовая связь 6G, ИИ, блокчейн* (финансы, цифровая валюта), *гражданские технологии* (ум-



ный город, электронное правительство), *новые технологии хранения данных*, в том числе магнитного хранения данных, *масштабные вычисления, цифровая криминалистика, оптические и квантовые вычисления, технологии распознавания речи, лиц и других объектов* и т. д. Даже простое перечисление новых ИКТ, а также их характеристики определяют их уникальную роль в современном мире.

Одним из наиболее интенсивно развивающихся направлений новейших ИКТ-продуктов является *искусственный интеллект*<sup>1</sup>.

В соответствии с российскими документами под *искусственным интеллектом (ИИ)* понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. *Комплекс технологических решений* включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. *Технологии искусственного интеллекта (ТИИ)* включают в себя компьютерное зрение, обработку естественного языка, распознавание

1 Ромашкина Н. П. Искусственный интеллект в космической индустрии: состояние, проблемы, перспективы // Искусственный Интеллект. Теория и практика. — 2024. — № 2.

и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта<sup>2</sup>. Одно из наиболее распространённых направлений использования искусственного интеллекта — это машинное обучение, которое основано на получении знаний интеллектуальной системой в процессе её работы.

ИИ играет решающую роль в процессе обеспечения информационной безопасности, улучшая возможности обнаружения угроз, прогнозирования и реагирования на них. Он анализирует огромные объёмы данных для выявления закономерностей и аномалий, прогнозирует потенциальные вызовы, автоматизирует определённые задачи обеспечения безопасности и реагирует на инциденты в режиме реального времени. Это помогает укрепить обороноспособность, снизить риски и более эффективно защищаться от возникающих ИКТ-угроз.

Новейшие ИКТ определяют структуру и динамику изменений национальной экономики государств, оказывают значительное влияние на содержание отношений между государствами, меняют характер войн и взгляды на будущее устройство мира.

При осознании глобального позитивного воздействия новейших ИКТ-продуктов на развитие современного мира необходимо отметить, что в настоящее время новейшие ИКТ-продукты стали важнейшим объектом конфронтации, противоборства, ведения военных действий и несут новые информационные угрозы, то есть потенциальные возможности нарушения информационной безопасности<sup>3</sup> или потенциально возможные, несущие определённую информацию события, действия и явления, которые могут привести к нанесению ущерба чьим-либо интересам. При этом попытки реализации информационной угрозы, то есть информационные атаки с использованием новейших ИКТ, могут быть значительно более опасными и разрушительными. Таким образом, их развитие связано с повышением информационной уязвимости,

то есть любой характеристики информационной системы, использование которой нарушителем может привести к реализации угрозы. Целями информационных угроз при этом по-прежнему являются информационные ресурсы — информационная инфраструктура, а также собственно информация и её потоки.

Этот процесс требует повышенного внимания в отношении критической информационной инфраструктуры, под которой в российском законодательстве понимаются соответствующие объекты и сети электросвязи, используемые для организации взаимодействия таких объектов. Её субъектами, в частности, являются государственные органы и учреждения; российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы; информационно-телекоммуникационные сети; автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, в банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, в оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности и др<sup>4</sup>.

Кроме того, в настоящее время новейшие ИКТ-продукты уже усиливают различные угрозы, в том числе возможности манипулирования мнением отдельных людей, социальных групп и государств, а также используются для обеспечения военно-политического превосходства, силового противоборства и шантажа, меняют представление о кризисах и конфликтах, тактике и стратегии ведения боевых действий и открывают качественно новые направления гонки вооружений через сближение гражданских и военных технологий.

Таким образом, новейшие ИКТ-продукты уже используются во вредоносных военно-политических целях, а также как принципиально

2 Национальная стратегия развития искусственного интеллекта на период до 2030 года (в редакции Указа Президента Российской Федерации от 15 февраля 2024 г. № 124). <http://www.kremlin.ru/acts/bank/44731>.

3 Угроза информационной безопасности Российской Федерации (далее — информационная угроза) — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере. Доктрина информационной безопасности Российской Федерации. <http://www.kremlin.ru/acts/bank/41460>.

4 Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». <http://www.kremlin.ru/acts/bank/42128>.

новые инструменты ведения боевых действий. В связи с этим вооружённые конфликты всё более приобретают характер многомерных информационных войн, которые могут одновременно вестись на различных фронтах и уровнях. Так, по заявлению Президента Российской Федерации В.В. Путина, «по сути, против России развязана настоящая агрессия, война в информационном пространстве»<sup>5</sup>. И в ней применяются новейшие ИКТ.

А, следовательно, такие технологии оказывают глобальное влияние на национальную и международную безопасность<sup>6</sup>. И поэтому требуется развитие международного сотрудничества для отстаивания верховенства международного права, принципа суверенного равенства государств; для предотвращения превращения этих технологий в страшное оружие.

Безусловно, важнейшей платформой для сотрудничества России в сфере ИКТ является объединение БРИКС. По заявлению Президента Российской Федерации В.В. Путина, «БРИКС притягивает всё больше сторонников и единомышленников — государств, которые разделяют принципиальные установки, лежащие в основе его деятельности. Это суверенное равенство, уважение выбора собственного пути развития, взаимный учёт интересов, открытость, консенсус, стремление к формированию многополярного мироустройства и справедливой модели глобальной финансовой и торговой системы, поиск коллективных решений наиболее острых проблем современности... В числе приоритетов — дальнейшее продвижение взаимодействия в сфере науки, высоких технологий, здравоохранения, экологии...»<sup>7</sup>.

Впервые тема информационной безопасности появилась в Декларации саммита

БРИКС 2011 года: стороны заявили о «приверженности сотрудничеству в укреплении международной информационной безопасности» и в «борьбе с киберпреступностью»<sup>8</sup>. С тех пор проблематика международной информационной безопасности (МИБ) присутствует во всех декларациях БРИКС. Кроме того, со странами-членами Объединения у России подписаны двусторонние документы о сотрудничестве в области МИБ. Отдельное внимание сегодня привлекают динамично развивающиеся технологии ИИ. Так, в 2023 году на саммите БРИКС, который проходил в Йоханнесбурге (ЮАР) с 22 по 24 августа 2023 г., Председатель КНР Си Цзиньпин призвал создать общую структуру управления искусственным интеллектом. По его мнению, «ИИ — это новая область, которая может принести риски странам, входящим в саммит, поэтому необходимо создать единый подход к использованию и контролю технологий»<sup>9</sup>.

В сентябре 2024 г. в Москве под эгидой ТАСС проходил Медиясаммит БРИКС, на котором собрались представители более 60 средств массовой информации из 45 стран. По заявлению Министра иностранных дел Российской Федерации С.В. Лаврова, важнейшей задачей саммита является создание общей для БРИКС и других дружественных стран новостной повестки, основанной на правде, на фактах<sup>10</sup>. В условиях информационной войны против России с применением всех современных новых ИКТ роль СМИ в построении многополярного мира существенно возрастает.

Что нужно для решения этой задачи? Создавать и развивать собственные медиаресурсы в рамках БРИКС. На данном этапе работает международная телевизионная сеть БРИКС, издаётся деловой журнал БРИКС.

5 Заседание Совета Безопасности Российской Федерации. <http://www.kremlin.ru/events/president/news/68451>.

6 Ромашкина Н. П., Марков А. С., Стефанович Д. В. Международная безопасность, стратегическая стабильность и информационные технологии / Отв. ред. А. В. Загорский, Н. П. Ромашкина. — Москва : ИМЭМО РАН, 2020. — 98 с. <https://www.imemo.ru/publications/info/romashkina-np-markov-as-stefanovich-dv-mezhdunarodnaya-bezopasnosty-strategicheskaya-stabilynosty-i-informatsionnie-tehnologii-otv-red-av-zagorskiy-np-romashkina-m-imemo-ran-2020-98-s>.

7 Обращение Владимира Путина в связи с началом председательства России в БРИКС. 1 января 2024 г. <http://www.kremlin.ru/events/president/news/73202>.

8 Декларация, принятая по итогам саммита БРИКС (г. Санья, о. Хайнань, Китай, 14 апреля 2011 г.). 14 апреля 2011 г. <http://www.kremlin.ru/supplement/907>.

9 БРИКС сформирует общую структуру управления ИИ. Что ждёт страны-участницы? <https://ai.gov.ru/mediacenter/briks-sformiruet-obshchuyu-strukturu-upravleniya-ii-chto-zhdet-stran-uchastnits-/>.

10 Более сотни руководителей и работников СМИ из 45 стран собрались в Москве на медиасаммит стран БРИКС. 14 сентября 2024 г. [https://www.1tv.ru/news/2024-09-14/486189-bolee\\_sotni\\_rukovoditeley\\_i\\_rabotnikov\\_smi\\_iz\\_45\\_stran\\_sobralis\\_v\\_moskve\\_na\\_mediasammit\\_stran\\_briks](https://www.1tv.ru/news/2024-09-14/486189-bolee_sotni_rukovoditeley_i_rabotnikov_smi_iz_45_stran_sobralis_v_moskve_na_mediasammit_stran_briks).

Однако этого недостаточно. Безусловно, необходимо более широкое распространение российских СМИ. Необходимо создавать новые цифровые платформы, обеспечивающие более широкие возможности взаимодействия между пользователями, предоставления доступа к контенту, услугам или продуктам, в том числе возможность создавать видеохостинги, маркетплейсы, социальные сети и т.д. Кроме того, максимально важно странам-членам БРИКС делиться опытом, в том числе новейшими техническими способами борьбы с дезинформацией и распространением фейков.

Глобальной целью, безусловно, является формирование системы регулирования новейших ИКТ на основе юридически обязывающих документов, создание режима контроля над ИКТ. При этом России целесообразно взять на себя инициативную роль в подготовке соглашений и договоров для подписания.

Для того чтобы документы были эффективными и обеспечивали выгоды для участников, этот процесс подготовки играет решающую роль. К нему необходимо привлекать в первую очередь ИТ-специалистов, математиков и программистов. На следующих этапах важна роль политологов и юристов. Затем — опять математики, чтобы проанализировать подготовленный документ не на основе бытовой логики, как зачастую бывает у экспертов-гуманитариев, а на основе законов математической логики, математических моделей эффективности будущего документа. Все эти шаги целесообразно проходить с максимальным использованием новейших ИКТ-продуктов.

И на протяжении всего этого процесса максимально важна роль дипломатии для подготовки населения и руководства государств, для донесения позиции России, и в результате — для обеспечения принятия международно-правовых норм в области ИКТ. Это так называемая цифровая дипломатия, которая включает методы и инструменты с использованием самих новых ИКТ для реализации внешнеполитических задач и защиты национальных интересов страны. Она включает, в частности, цифровые платформы для взаимодействия с иностранной аудиторией, СМИ, информационно-разъяснительную работу, конференции, выставки и т.д. И наконец,

сами переговоры и подготовка к подписанию документов по регулированию цифровых технологий.

С 22 по 24 октября 2024 г. в Казани пройдет XVI саммит БРИКС с участием глав государств под председательством России. Как действующий председатель БРИКС в текущем году, Россия с большой ответственностью подошла к организации совместной деятельности в рамках Объединения. По заявлению Президента Российской Федерации В.В. Путина, «на наше председательство была возложена особая миссия — всячески содействовать максимально быстрой и органичной интеграции новых стран-участниц во все бриксовские механизмы. На сегодня о желании в той или иной форме подключиться к деятельности нашего объединения заявило уже свыше трёх десятков стран, точнее 34 государства... Подчеркну, что программа российского председательства весьма содержательна и разнообразна. Она включает в себя свыше 200 мероприятий, нацеленных на продвижение партнёрства по всем ключевым направлениям: политика и безопасность, экономика и финансы, культурные и гуманитарные связи. К настоящему времени план председательства выполнен более чем на 70 процентов, проведено порядка 150 мероприятий, совещаний, отраслевых форумов, состоялось большинство экспертных и министерских встреч... Среди конкретных результатов совместной работы государств БРИКС отмечу создание специального электронного реестра для обмена данными о компьютерных атаках и инцидентах»<sup>11</sup>.

Одной из приоритетных задач председательства России в БРИКС в 2024 году в сфере политики и обеспечения безопасности названо наращивание сотрудничества в интересах формирования системы обеспечения МИБ в целях предотвращения и урегулирования конфликтов в информационном пространстве и недопущения его милитаризации. И, безусловно, вопросы новейших ИКТ, как важнейшей составляющей информационной безопасности на текущем этапе развития общества, стали частью обсуждения на саммите. И, вероятно, найдут своё отражение в принятых документах.

<sup>11</sup> Встреча с представителями государств БРИКС, курирующими вопросы безопасности. 12 сентября 2024 г. <http://www.kremlin.ru/events/president/news/75086>.