DOI: 10.24412/2618-6888-2021-26-256-273

Я.В. Лексютина

ЗЛОНАМЕРЕННОЕ ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: РИСКИ ДЛЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ КИТАЯ[1]

Аннотация. Благодаря значительному увеличению вычислительных мощностей, взрывному росту больших данных и инновационным достижениям в алгоритмах глубокого обучения искусственный интеллект (ИИ) выходит на принципиально новый операционный уровень, что открывает широкие горизонты его применения в различных сферах реального сектора экономики и общественной жизни. Рассматривая искусственный интеллект в качестве ключевой стратегической технологии, которая будет определять будущее развитие человечества, ведущие страны мира придают огромное значение достижению превосходства в сфере ИИ. Как следует из проведенного в статье анализа официальных документов КНР, раскрывающих планы социально-экономического, научно-технологического и оборонного развития Китая, развитию и коммерциализации искусственного интеллекта Пекин придал статус национальной стратегии, нацеленной на укрепление конкурентоспособности Ки-

[1] Исследование выполнено при финансовой поддержке РФФИ и ВАОН № 21-514-92001.

тая во всех сферах. Согласно планам китайского руководства, к 2030 г. Китай должен стать мировым центром инноваций в области искусственного интеллекта.

Открывая широкие возможности для социально-экономического развития и меняя представления о военной мощи государств, искусственный интеллект, между тем, создает множество рисков. Среди прочего, особого внимания требует опасность злонамеренного использования ИИ антисоциальными негосударственными акторами и недружественными государствами с целью дестабилизации ситуации в других странах. В данной статье раскрывается проблематика злонамеренного использования искусственного интеллекта, определяются риски информационно-психологической безопасности Китая и выявляются особенности китайского подхода к обеспечению защищенности от злонамеренного использования ИИ с акцентом на обеспечение информационно-психологической безопасности.

Ключевые слова: Китай, искусственный интеллект (ИИ), информационно-психологическая безопасность, кибербезопасность, фейковые новости, информационная безопасность, информационные войны.

Автор: Лексютина Яна Валерьевна, доктор политических наук, профессор РАН, профессор Кафедры американских исследований Санкт-Петербургского государственного университета.
ORCID: 0000-0001-6766-1792; E-mail: lexyana@ya.ru

Ya.V. Leksyutina

Malicious use of artificial intelligence: risks to China's information and psychological security

Abstract. Due to a significant increase in computing power, the explosive growth of big data and innovative advances in deep learning algorithms, artificial intelligence (AI) has reached a fundamentally new operational level, which opens up wide horizons for its application in various areas of the real economy and social life. Considering artificial intelligence as a crucial strategic technology that will determine the future of all humankind, the world's leading countries attach great importance to achieving superiority in the artificial intelligence field. Having analyzed China's various official planning documents, the article reveals that the development and commercialization of artificial intelligence has become China's national strategy aimed at strengthening China's competitiveness

in all areas. According to Chinese plans, by 2030 China should become the major artificial intelligence innovation center of the world.

However, artificial intelligence not only opens up wide opportunities for socio-economic development and changes the perception of the military power of states, but also carries many risks. Among other things, special attention on the part of countries requires the danger of malicious use of artificial intelligence by antisocial non-state actors and unfriendly states to destabilize the countries' sociopolitical situation. The article exposes the problems of malicious use of artificial intelligence, determines the risks of information and psychological security to China, and reveals the specifics of the Chinese approach to ensuring protection from malicious use of AI with an emphasis on ensuring information and psychological security.

Keywords: China, artificial intelligence (AI), information and psychological security, cybersecurity, fake news, information security, information wars.

Author: Yana V. LEKSYUTINA, Dr.Sc. (Political Science), Professor of the Russian Academy of Sciences; Professor of the American Studies Department, Saint-Petersburg State University.
ORCID: 0000-0001-6766-1792 (lexyana@ya.ru).

Развитие искусственного интеллекта как национальная стратегия Китая

Начиная с 2015—2016 гг. в планах социально-экономического и научно-технологического развития, а также оборонного строительства Китая одно из приоритетных мест начинает отводиться развитию и применению технологии искусственного интеллекта (ИИ). ИИ стал рассматриваться китайским руководством в качестве ключевой, стратегической технологии, имеющей решающее значение для всех аспектов национальной конкурентоспособности и меняющей существующие представления о военной мощи государств. Обозначив развитие ИИ в качестве важного национального приоритета совсем недавно, Китай уже сейчас достаточно эффективно использует возможности ИИ для модернизации промышленности, ускорения экономического развития, трансформации модели экономического роста, обеспечения общественного порядка, развития

своих конкурентных преимуществ в мировой экономике и усиления военного потенциала.

Свое видение роли ИИ в становлении Китая в качестве ведущей мировой державы китайское руководство четко обрисовало в серии программных документов, обнародованных начиная с 2015 г. В мае 2015 г. был выпущен 10-летний план «Сделано в Китае 2025», делавший акцент на развитии технологических инноваций с целью создания в Китае конкурентоспособной обрабатывающей промышленности, соответствующей передовому мировому уровню [Чжунго чжицзао 2025]. В плане были зафиксированы цели глубокой интеграции нового поколения информационных технологий в промышленное производство, развития интеллектуального (умного) производства, разработки интеллектуального оборудования и интеллектуальных устройств, совершенствования автоматизации производства и пр. [Чжунго чжицзао 2025]. В том же году Госсовет КНР опубликовал руководящие принципы в области активного продвижения стратегии «Интернет+», нацеленной на глубокую интеграцию Интернета во все сферы экономики и общества. Важными направлениями усилий были выделены среди прочего ускорение прорыва в развитии ИИ, содействие применению ИИ в умных домах, умных терминалах, умных автомобилях, роботах и пр., а также взращивание ключевых предприятий и инновационных групп, призванных возглавить разработку глобального ИИ [Гоуюань гуаньюй...]. В принятом в марте 2016 г. 13-м пятилетнем плане социально-экономического развития КНР (2016—2020 гг.) неоднократно подчеркивалась необходимость развития ИИ и его коммерциализации.

Однако, вплоть до 2016 г. ИИ рассматривался в качестве одной из важных технологий в ряду других [Roberts, Cowls, 2021, p. 60] (при перечислении перспективных технологий ИИ назывался не в первую очередь). Принятие Госсоветом КНР в июле 2017 г. специализированной комплексной «Программы развития искусственного интеллекта нового поколения», фиксирующей долгосрочные цели политики Китая в области ИИ, означало выход задачи развития ИИ на уровень национальной стратегии. ИИ начинает выделяться в качестве приоритетного направления инновационного развития Китая. Первый этап реализации стратегии предполагал, что к 2020 г. разви-

тие ИИ и его применение будут соответствовать передовому мировому уровню, будет сформирована кадровая команда специалистов и сформулированы предварительные этические нормы, ориентиры и правила, регламентирующие сферу ИИ. К 2025 г. Китай должен добиться «крупного прорыва» в ИИ, а по отдельным направлениям развития ИИ занять лидирующие позиции в мире; широко внедрять ИИ в сферу интеллектуального производства, интеллектуальной медицины, умных городов, умного сельского хозяйства, национальной обороны и другие сферы; разработать соответствующие законы, правила и этические нормы, создать механизмы контроля и оценки безопасности ИИ. И, наконец, к 2030 г. Китай должен стать мировым центром инноваций в области ИИ [A New Generation...].

Вслед за «Программой развития искусственного интеллекта нового поколения» Министерство промышленности и информационных технологий КНР выпустило «Трехлетний план действий по содействию развитию отрасли искусственного интеллекта нового поколения» (2018—2020 гг.), в котором были изложены конкретные рекомендации для промышленности и задействованных акторов. В Плане были закреплены четыре задачи: 1) стимулирование развития таких технологий, как интеллектуальные и сетевые транспортные средства, интеллектуальные сервисные роботы, интеллектуальные беспилотные летательные аппараты, медицинские диагностические системы с распознаванием изображений, системы видео- и голосовой идентификации, интеллектуальные голосовые интерактивные системы, интеллектуальные системы перевода, и в целом — продвижение комплексного применения умных продуктов в экономике и обществе; 2) обеспечение массового производства микросхем нейронных сетей и чипов и их широкомасштабное применение в ключевых областях; 3) стимулирование развития интеллектуального производства; 4) создание системы поддержки отрасли ИИ [Three-Year Action Plan...].

Стремительному развитию отрасли ИИ способствовало создание китайским руководством исключительно благоприятных условий, комплексное государственное стимулирование, в том числе путем оказания финансовой поддержки технологическим компаниям, стартапам и исследовательским группам.

В целях повышения эффективности участия частного сектора в развитии ИИ Министерство науки и технологий закрепило развитие отдельных секторов ИИ за конкретными технологическими «национальными чемпионами». Им надлежало разработать «открытые инновационные платформы» в закрепленных за ними секторах и тем самым установить соответствующие стандарты [Kim, p. 13]. За *Baidu* было закреплено автономное вождение, за *Alibaba* — умные города, *Tencent* — умное здравоохранение, *iFlyTek* — распознавание голоса, *Sensetime* — интеллектуальное восприятие [Hearing on Technology..., p. 46].

Небольшие китайские технологические компании также получают государственную поддержку и субсидии на разработку технологий ИИ. Например, *Zhongguancun Innovation Town* — это специально созданный, субсидируемый государством инкубатор, помогающий китайским технологическим стартапам добиться успеха, в том числе в секторах, закрепленных за «национальными чемпионами» [Roberts, Cowls, p. 61]. Есть и сектора индустрии ИИ, где пока нет назначенного «национального чемпиона» (например, интеллектуальное судопроизводство).

Усилия по внедрению ИИ особенно интенсифицировались на фоне появления и распространения COVID-19. Китайские компании были активно вовлечены в разработку специализированных систем ИИ для контроля и предотвращения эпидемий, а также налаживания нормальной общественной и деловой активности.

В Китае видят огромный потенциал внедрения ИИ в производство, сельское хозяйство, логистику, финансы, торговлю, административное управление, менеджмент, освоение подводного мира, создание умных домов и пр. Разработки в области ИИ и его применения продиктованы стремлением Китая обеспечить дальнейшее устойчивое и гармоничное социально-экономическое развитие, а также национальную конкурентоспособность Китая.

Большое значение китайские власти придают применению ИИ в социальной сфере. Как следует из «Программы развития искусственного интеллекта нового поколения», использование ИИ в таких областях, как здравоохранение, пенсионное обеспечение, образование, защита окружающей среды, административное и городское

управление, судопроизводство и прочие способно повысить уровень предоставляемых социальных услуг и улучшить качество жизни населения [A New Generation...]. Китайское правительство широко использует предоставляемые ИИ возможности социального мониторинга в целях обеспечения социальной стабильности и национальной безопасности. Это прежде всего — технологии системы распознавания лиц (эффективные для купирования, например, террористических угроз) или система социального кредита, оценивающая китайских граждан на основе их поведения в обществе.

И, наконец, Пекин не скрывает и даже, напротив, всячески подчеркивает важность военно-гражданской интеграции в процессе развития отрасли ИИ и использования потенциала ИИ в целях модернизации вооруженных сил и военно-промышленного комплекса Китая [Каменнов, с. 147]. В изданной в 2019 г. Белой книге по обороне Китай акцентирует внимание на происходящих исторических переменах в военном деле, обусловленных новым витком технологической и промышленной революции, расширением применения в военной сфере передовых технологий, таких как ИИ, квантовая информация, большие данные, облачные вычисления и Интернет вещей [China's National Defense...]. Развитие ИИ рассматривается Китаем как дающее преимущество в ассиметричных войнах.

Риски злонамеренного использования ИИ

Целенаправленно стимулируя развитие отрасли ИИ, китайские власти осознают и оборотную сторону развития этой технологии и ее широкого использования. В силу объективных причин ИИ может оказывать влияние на государственное управление, экономическую безопасность и социальную стабильность. Например, широкое применение ИИ способно негативно отразиться на структуре занятости населения, повлиять на правовую систему, общественную этику и мораль, нарушить неприкосновенность частной жизни и бросить вызов международным отношениям [A New Generation...].

Более того, по мере широкого распространения и расширения доступности ИИ, возрастает вероятность его злонамеренного ис-

пользования антисоциальными акторами или недружественными государствами. При этом можно провести условное разграничение между «*злонамеренным использованием ИИ*» и «*злоупотреблением ИИ*», где под первым понимается использование злоумышленниками технологий с использованием ИИ для достижения своих целей, а под вторым — взломы, перепрограммирование или подчинение[1] своим целям уже существующих систем ИИ [Ciancaglini, Gibson, p. 5]. Так, злоупотребление ИИ может состоять в проникновении в интеллектуальные системы критически важной инфраструктуры с целью нанесения ущерба или провоцирования паники среди населения (это особенно актуально в связи с созданием умных городов), в перепрограммировании умных домов, беспилотных летательных аппаратов или роботизированных транспортных средств. Такого рода риски актуализируются ввиду динамичного развития в Китае умных городов, умного общественного транспорта, роботакси и пр.

Способы злонамеренного использования ИИ разнообразны и включают, но не ограничиваются, злонамеренным использованием технологий «deep fake», «fake people», «fake news», «умных» ботов или фишинговых атак в целях создания ложных новостей, влияния на общественный дискурс, подрыв общественного доверия или шантажа чиновников и дипломатов. Новые технологии, основанные на ИИ, могут становиться эффективным информационно-психологическим [Bazarkina, Pashentsev, p. 156] орудием дестабилизации социально-политической ситуации в государствах, а также нанесения вреда межгосударственным отношениям.

В зависимости от преследуемых злоумышленниками целей злонамеренное использование ИИ можно разделить на три уровня: 1) хулиганство, при котором отсутствует намерение получения выгоды, а целью является демонстрация целевой аудитории своих возможностей или просто развлечение; 2) бытовой уровень, где злоумышленниками могут становиться компании, преступные группы, отдельные индивиды и пр., преследующие цели извлечения материальной прибыли или ведущие недобросовестную конкуренцию (кража личной

[1] При этом взлом существующих систем ИИ может также осуществляться при помощи ИИ.

банковской информации, личной информации с целью шантажа, сбор информации о клиентах с целью таргетированной рекламы, разрушение корпоративного имиджа конкурирующей компании и пр.); 3) злонамеренное использование ИИ в политической сфере с целью нанесения вреда государству, межгосударственным отношениям, дестабилизации политической или социально-экономической ситуации и пр.

В руках злоумышленников ИИ может превращаться в эффективное орудие информационно-психологического воздействия на население. Так, технологии «deep fake», «fake people», «fake news» потенциально могут использоваться в политических целях для дискредитации национальных лидеров, политиков и кандидатов в ходе выборов (путем, например, создания ложно-негативных видеороликов с их участием), распространения дезинформации и манипулирования общественным мнением, подстрекательств к актам насилия в отношении нацменьшинств, распространения идеологий экстремистских или террористических групп, разжигания социальных волнений и политической поляризации общества и пр. Например, созданные с использованием ИИ фальшивые видеоролики о жестоком обращении правительства с гражданами могут вызвать возмущение общественности, угрожая стабильности политической системы.

Тот факт, что вплоть до текущего момента возникшая в 2017 г. технология «deep fake» крайне редко злонамеренно использовалась с преступными или политическими целями [Ciancaglini, Gibson, p. 59], а применялась в развлекательных целях, не исключает потенциала ее злонамеренного использования по мере совершенствования данной технологии. Для антисоциальных негосударственных акторов, таких как террористические организации, преступные группы, оппозиционные политические силы, корпоративные группы интересов или секты, технологии с использованием ИИ могут оказаться мощным, недорогим и легкодоступным инструментом оказания информационно-психологического давления на целевую аудиторию.

Злонамеренное использование ИИ может проявиться в международных отношениях. Например, заинтересованные страны

способны при помощи ИИ создавать ложные информационные поводы, фабриковать «доказательства», оправдывающие их вмешательство во внутренние дела других государств (по аналогии с фабрикацией «данных», сделавших возможной операцию в Ираке [Лун Кунь, Ма Юэ, с. 26]). Недружественные государства могут также, создавая фальшивый контент, разжигать внутренние противоречия в государствах, дискредитировать национальных лидеров, правящие политические партии, инспирировать «цветные революции» и пр.

Не исключена ситуация, когда недружественное государство вознамерится создавать информационные поводы для нанесения вреда межгосударственным отношениям третьих стран, способствовать разрушению взаимного доверия между ними или даже провоцировать межгосударственные конфликты.

Гипотетически для Китая подобного рода риски, связанные с использованием ИИ и нацеленные на дестабилизацию его внутреннего социально-политического положения посредством информационно-психологического воздействия, могут проистекать как от недружественных государств (сейчас в Китае такие риски связывают прежде всего с США и их некоторыми союзниками, а также с Индией), так и со стороны, например, террористических, экстремистских и сепаратистских сил (например, связанных с уйгурским терроризмом), диссидентских групп, преступных групп, сект (например, Фалуньгун). Технологии с использованием ИИ могут быть использованы, например, в целях дискредитации китайских высокопоставленных официальных лиц и КПК. Действия злоумышленников могут быть направлены на такие «болевые точки» Китая, как уйгурская, тибетская и тайваньская проблемы, гонконгский вопрос, правозащитная проблематика.

Весьма показательна в этом отношении практика хакерских атак в китайском сегменте Интернета. Так, в 2018 г. в Китае был зафиксирован самый высокий в мире уровень распределенных атак типа «отказ в обслуживании» (DDOS) — в среднем более 800 млн в день. При этом около 97 % кибератак было проведено местными (китайскими) хакерами, а кибератаки из-за границы исходили в основном из США, Южной Кореи и Японии [Lyu Jinghua, 2019].

Обеспечение защищенности Китая от злонамеренного использования ИИ

Способность стран справляться с рисками, связанными с развитием ИИ и возможностью их злонамеренного использования, в Китае связывают с уровнем технологического развития соответствующей страны. Для многих развивающихся стран, чей технологический уровень остается относительно отсталым, риски столкнуться с высокотехнологичным информационно-психологическим воздействием существенно выше, чем у стран с высоким уровнем технологического развития. Из-за отсутствия необходимых технологий развивающиеся страны не имеют эффективных способов защиты данных, а также не способны справиться с проблемами, вызванными ИИ-алгоритмами. Мировое развитие технологий искусственного интеллекта еще больше подчеркнет их слабость в области обеспечения безопасности от злонамеренного использования ИИ и информационно-психологической безопасности [Фэн Шуай, Лу Чуаньин, с. 34].

Опережающее развитие ИИ рассматривается в Китае как способ помочь избегать, предупреждать, блокировать, справляться со злонамеренным использованием ИИ антисоциальными акторами. Так, ИИ может быть эффективным в обнаружении и реагировании на операции, направленные на оказание информационно-психологического воздействия. Он может помочь контролировать онлайн-среду (в том числе социальные сети), выявлять ранние признаки злонамеренных операций, таких как рост активности частных или социальных ботов, а также обнаруживать измененный цифровой контент, включая синтетические медиа. Развитие ИИ позволяет усиливать защитные функции систем от кибератак, содействуя обеспечению кибербезопасности, а также злонамеренного использования ИИ. Задача Китая в этой связи состоит в опережающем развитии ИИ, достижении превосходства в этой сфере.

В обеспечении безопасного, надежного и контролируемого развития ИИ Китай большое значение придает разработке нормативно-правовой базы, правил и этических норм, регламентирующих сферу ИИ, усилению надзорной деятельности над сферой ИИ и ки-

берпространством, а также созданию механизмов контроля и оценки безопасности искусственного интеллекта [A New Generation...]. В Китае уже сформирована обширная нормативно-правовая база, регламентирующая деятельность различных акторов в киберпространстве, аккумулирован обширный успешный опыт управления китайским сегментом Интернета. Кроме того, в КНР действует одна из наиболее жестких систем цензуры Интернета. В связи с этим в части обеспечения информационно-психологической безопасности от рисков злонамеренного использования ИИ, таких как «deep fake», «fake people», «fake news», «умных» ботов или фишинговых атак, Китай уже имеет разнообразный инструментарий их обнаружения, предупреждения и блокирования.

В основном законе, регулирующем киберсферу, принятом в 2017 г. Законе КНР о кибербезопасности содержится целый ряд положений, которые также имеют непосредственное отношение к проблематике злонамеренного использования ИИ. Так, Закон запрещает ставить под угрозу кибербезопасность и использовать Интернет в целях подстрекательства к подрыву национального суверенитета и ниспровержения социалистической системы, разжигания сепаратизма, разрушения национального единства, пропаганды терроризма или экстремизма, этнической ненависти и этнической дискриминации, распространения ложной информации для подрыва экономического или общественного порядка [Cybersecurity Law..., art. 12].

В силу развития ИИ перед Китаем стоит задача обогащения уже существующей нормативно-правовой базы в области обеспечения кибербезопасности новыми законами и правилами, регламентирующими использование технологий ИИ. Так, в ноябре 2019 г. китайские регулирующие органы обнародовали правила, регулирующие видео- и аудиоконтент в Интернете. В них, в частности, запрещается поставщикам и пользователям сетевых аудио- и видеоинформационных услуг публиковать и распространять ложную информацию или «deep fake» в Интернете без четкого обозначения того, что соответствующий контент был создан с использованием технологии ИИ или виртуальной реальности [Ванло инь..., ст. 10—12]. Правила также запрещают использовать новые технологии, основанные на глубоком

обучении, виртуальной реальности и т. п., для создания, публикации или распространения ложной новостной информации, а также вменяют поставщикам контента обязанность усилить контроль над размещаемой пользователями информацией. Таким образом китайские власти намерены сдерживать распространение фейковых новостей и информации, способных поставить под угрозу национальную безопасность или вызвать негативное воздействие на общество.

В целях обеспечения безопасного развития ИИ и предупреждения его злонамеренного использования китайские регулирующие органы поддерживают тесные контакты и направляют деятельность китайских технологических компаний, социальных сетей, новостных организаций, неправительственных организаций и пр. Так, в марте 2021 г. китайские власти в целях усиления контроля над соответствующей сферой пригласили 11 технологических компаний, включая *Tencent, Alibaba* и *TikTok*, для обсуждения вопросов развития технологии «deep fake» и кибербезопасности [China summons...]. Такая работа ведется китайскими властями на регулярной системной основе.

В целом применяемые Китаем меры в целях обеспечения безопасного, надежного и контролируемого развития ИИ включают: использование технологий ИИ для решения проблем кибербезопасности и информационно-психологической безопасности (обнаружение вредоносного кода, уязвимостей и пр.); усиление защитных функций систем с использованием ИИ; разработку технических инструментов и политических средств для борьбы со злонамеренным использованием ИИ; развитие законодательства, правил и этических норм, регламентирующих сферу ИИ; осуществление и усиление надзорной деятельности над киберпространством и сферой ИИ; повышение бдительности и осведомленности граждан о возможностях злонамеренного использования ИИ.

Заключение

Как следует из анализа официальных документов КНР, раскрывающих планы социально-экономического, научно-технологического, инновационного, оборонного развития Китая, примерно с

2017 г. приоритетное значение начинает придаваться развитию и коммерциализации ИИ. Развитие ИИ видится как фактор, способный придать динамику экономическому развитию Китая на фоне утраты традиционных конкурентных преимуществ (таких, например, как дешевая и многочисленная рабочая сила), могущих содействовать построению «гармоничного общества», обеспечению общественного порядка и национальной безопасности, а также укреплению национальной конкурентоспособности Китая во всех сферах. При соответствующей комплексной государственной поддержке к 2030 г. Китай должен стать мировым центром инноваций в области ИИ.

Искусственный интеллект, между тем, представляет собой «обоюдоострый меч», открывающий широкие возможности, но и несущий многочисленные риски, вызовы и даже угрозы. Эти риски, вызовы и угрозы весьма многозначны, включая неопределенность последствий внедрения ИИ для экономического развития (например, потенциальное негативное влияние на структуру занятости населения), возможное негативное воздействие на общество (например, кризис общественного доверия, связанный с тем, что население будет неспособно отделить правду от лжи, столкнувшись с массовой практикой генерирования ИИ дезинформации), на правовую систему, риски дестабилизации финансово-экономической системы (как следствия, например, распространения ложной информации, вызывающей обвал на финансовых рынках, или злонамеренного использования ИИ в целях нанесения урона корпоративному имиджу) и т. д., и т. п. С точки зрения обеспечения национальной безопасности, социальной стабильности и общественного порядка угрозу представляет злонамеренное использование ИИ антисоциальными негосударственными акторами и недружественными государствами. В их руках ИИ способен превратиться в действенный инструмент оказания информационно-психологического воздействия на общество с целью дестабилизации ситуации в государстве.

Особенность китайского подхода к обеспечению защищенности от злонамеренного использования ИИ состоит в том, что ключом к успеху в данном направлении видится форсированное опережающее

(а не догоняющее) развитие ИИ, обретение мирового превосходства в области ИИ. Новейшие разработки в сфере ИИ должны обеспечить защищенность от его злонамеренно использования, включая информационно-психологическую безопасность. Более того, существующая в Китае комплексная система государственного регулирования и контроля Интернета и общественного дискурса повышает устойчивость КНР к высокотехнологичным информационно-психологическим атакам. Важным здесь является обогащение нормативно-правовой базы и применяемой охранительной практики за счет новых законов, правил и практик, регулирующих связанные с ИИ специфические вопросы.

Библиографический список

Каменнов П.Б. Развитие искусственного интеллекта — важнейшее направление инновационной политики КНР // Экономика КНР в годы 13-й пятилетки (2016—2020) / под ред. А.В. Островского. М.: ИДВ РАН, 2020. С. 141—156.

Ванло инь шипинь синьси фуу гуаньли гуйдин : [Положения об администрировании сетевых аудио- и видеоинформационных служб]. URL: http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm (дата обращения: 18.03.2021). (На кит. яз.).

Гоуюань гуаньюй цзицзи туйцзинь «хуляньван+» синдун дэ чжидао ицзянь : [Руководящие заключения Госсовета по активному продвижению акции «Интернет +»]. URL: http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm (дата обращения: 01.03.2021). (На кит. яз.).

Лун Кунь, Ма Юэ. Шэньду вэйцзао дуй гоцзя аньцюань дэ тяочжань цзи индуй : [Вызов «глубокой подделки» для национальной безопасности и ответ на него] // Синьси аньцюань юй тунсинь баоми. 2019. № 10. С. 21—34. (На кит. яз.).

Фэн Шуай, Лу Чуаньин. Жэньгун чжинэн шидай де гоцзя аньцюань: фэнсянь ю чжили : [Национальная безопасность в эпоху искусственного интеллекта: риски и управление] // Синьси аньцюань ю тунсинь баоми. 2018. № 10. С. 30—49. (На кит. яз.).

Чжунго чжицзао 2025 : [Сделано в Китае 2025]. URL: http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm (дата обращения: 08.05.2020. (На кит. яз.).

A New Generation of Artificial Intelligence Development Plan. URL: https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf (accessed: 08.03.2021).

Bazarkina D., Pashentsev E. Artificial Intelligence and New Threats to International Psychological Security // Russia in Global Affairs. Vol. 17. № 1. 2019. P. 147—170. DOI: 10.31278/1810-6374-2019-17-1-147-170

China summons Alibaba, Tencent and others over 'deep fakes', internet security. URL: https://www.wionews.com/world/china-summons-alibaba-tencent-and-others-over-deep-fakes-internet-security-371351 (accessed: 18.03.2021).

China's National Defense in the New Era. July, 2019. URL: http://www.scio.gov.cn/zfbps/ndhf/39911/Document/1660528/1660528.htm (accessed: 11.03.2021).

Ciancaglini V., Gibson Cr., Sancho D., et. al. Malicious Uses and Abuses of Artificial Intelligence: Europol Public Information. Trend Micro Research, 2020. 80 p.

Cybersecurity Law of the People's Republic of China. Effective: 1.06.2017. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law- peoples-republic-china/ (accessed: 27.03.2021).

Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy: Transcript. — Washington: United States-China Economic and Security Review Commission, 2019. 242 p.

Kim D. Artificial Intelligence Policies in East Asia: An Overview from the Canadian Perspective: Artificial Intelligence Report. Asia Pacific Foundation of Canada, 2019. 40 p.

Lyu Jinghua. What Are China's Cyber Capabilities and Intentions? URL: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 (accessed: 21.03.2021).

Roberts, H., Cowls, J., Morley, J. et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation // AI & Society. London: Springer-Verlag London Ltd, 2021. No. 36. Pp. 59—77. DOI: 10.1007/s00146-020-00992-2

Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018—2020). URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/ (accessed: 12.12.2020).

References

A New Generation of Artificial Intelligence Development Plan. URL: https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf (accessed: 8 March, 2021).

Bazarkina, D., Pashentsev, E. (2019). Artificial Intelligence and New Threats to International Psychological Security, *Russia in Global Affairs*, vol. 17: 1: 147—170. DOI: 10.31278/1810-6374-2019-17-1-147-170

China summons Alibaba, Tencent and others over 'deep fakes', internet security. URL: https://www.wionews.com/world/china-summons-alibaba-tencent-and-others-over-deep-fakes-internet-security-371351 (accessed: 18 March, 2021).

China's National Defense in the New Era. July, 2019. URL: http://www.scio.gov.cn/zfbps/ndhf/39911/Document/1660528/1660528.htm (accessed: 11 March, 2021).

Ciancaglini V., Gibson Cr., Sancho D., et. al. (2020). Malicious Uses and Abuses of Artificial Intelligence: *Europol Public Information. Trend Micro Research*, 80 p.

Cybersecurity Law of the People's Republic of China. Effective: 1.06.2017. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed: 27 March, 2021).

Feng Shuai; Lu Chuanying (2018). Réngōng zhìnéng shídài de guójiā ānquán: Fēngxian yu zhìli [National Security in the Era of Artificial Intelligence: Risk and Governance], *Xìnxī ānquán yu tōngxìn baomì [Information Security and Communication Confidentiality]*, no. 10: 30—49. (In Chinese).

Guówùyuàn guānyú jījí tuījìn "hùliánwang +" xíngdòng de zhidao yijian [Guiding Opinions of the State Council on Actively Promoting the "Internet +" Action]. URL: http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm (accessed: 1 March, 2021) (In Chinese).

Hearing on Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy: Transcript (2019). *Washington: United States-China Economic and Security Review Commission,* 242 p.

Kamennov P.B. (2020) Razviti·yye iskusstvennogo intellekta — vazhne·yshe·yye napravleni·yye innovatsionno·y politiki KNR [The development of artificial intelligence — the most important direction of China's innovation police], *Ekonomika KNR v gody 13-y pyatiletki (2016—2020) [The PRC Economy in the period of the 13-th Five Year Plan (2016—2020)],* editor-in-chief A.V.Ostrovskii. Moscow: IFES RAS: 141—156. (In Russian).

Kim D. (2019). Artificial Intelligence Policies in East Asia: an Overview from the Canadian Perspective: *Artificial Intelligence Report. Asia Pacific Foundation of Canada*, 40 p.

Long Kun, Ma Yue (2019). Shēndù wèizào duì guójiā ānquán de tiaozhàn jí yìngduì [The Challenges and Responses of Deepfake to National Security], *Xìnxī ānquán yu tōngxìn baomì [Information Security and Communication Confidentiality],* no. 10: 21—34. (In Chinese).

Lyu Jinghua. What Are China's Cyber Capabilities and Intentions? URL: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 (accessed: 21 March, 2021).

Roberts, H.; Cowls, J.; Morley, J. et al. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation, *AI & Society*. London: Springer-Verlag London Ltd., no. 36: 59—77. DOI: 10.1007/s00146-020-00992-2

Three-Year Action Plan for Promoting Development of a New Generation Artificial Intelligence Industry (2018—2020). URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-government-outlines-ai-ambitions-through-2020/ (accessed: 12 December, 2020).

Wangluò yīn shìpín xìnxī fúwù guanli guīdìng [Provisions on the Administration of Network Audio and Video Information Services]. URL: http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm (accessed: 18 March, 2021) (In Chinese).

Zhōngguò zhìzào 2025 [Made in China 2025]. URL: http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm (accessed: 8 May, 2020) (In Chinese).