УДК 004.056.32 + 343.142.91 Вестник УрФО № 1(35) / 2020, с. 65–71

Минбалеев А. В.

DOI: 10.14529/secur200107

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ В РОССИИ И ЗА РУБЕЖОМ: ОСНОВНЫЕ ПРОБЛЕМЫ[1]

Статья посвящена анализу основных проблем обеспечения информационной безопасности в Российской Федерации и в мире в процессе создания и использования искусственного интеллекта, которые являются стратегическим направлением в области обеспечения безопасности личности, общества и государства. Весьма актуальной сегодня становится проблема замещения искусственным интеллектом человека в процессе его собственной жизнедеятельности. Она поднимается сегодня, поскольку человек прекращая совершать значительное количество операций по поиску, обработке, передаче информации становится полностью зависимым от роботов, доверяет им все больше и готов пожертвовать рядом своих свобод, законных интересов, в том числе и в сфере информационной безопасности, в ходе передачи тех или иных видов человеческих процессов роботам.

В статье анализируются проблемы обеспечения информационной безопасности при использовании искусственного интеллекта при осуществлении террористической деятельности, а также использования искусственного интеллекта в противодействии терроризма. Анализируются угрозы информационной безопасности при осуществлении массового наблюдения и анализа данных с использованием технологий искусственного интеллекта, в том числе в процессе противодействия преступности.

Ключевые слова: *информационная безопасность, искусственный интеллект, противодействие преступности, массовой наблюдение, вызовы и угрозы.*

[1] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации (грант МД-2209.2020.6) «Развитие системы правовых средств обеспечения кибербезопасности в Российской Федерации».

Minbaleev A. V.

THE USE OF ARTIFICIAL INTELLIGENCE AND LEGAL SUPPORT OF INFORMATION SECURITY AND CYBERSECURITY IN RUSSIA AND ABROAD: MAIN PROBLEMS

The article analyzes the main problems of ensuring information security in the Russian Federation and in the world in the process of creating and using artificial intelligence, which are a strategic direction in the field of ensuring the security of individuals, society and the state. The problem of replacing a person with artificial intelligence in the process of their own life activity is becoming very urgent today. It rises today as people continuing to make a significant number of operations for searching, processing, transmission of information becomes completely dependent on robots, trusts them more and is willing to sacrifice some of its freedoms, legitimate interests, including in the field of information security during transmission of certain kinds of human processes robots.

The article analyzes the problems of ensuring information security when using artificial intelligence in carrying out terrorist activities, as well as the use of artificial intelligence in countering terrorism. The article analyzes threats to information security in the implementation of mass surveillance and data analysis using artificial intelligence technologies, including in the process of countering crime.

Keywords: *information security, artificial intelligence, crime prevention, mass surveillance, challenges and threats.*

Современная система развития искусственного интеллекта в мире свидетельствует о стремительных темпах технологической части развития данных технологий, ее постоянном экспоненциальном росте, но при этом регулирование использование технологий искусственного интеллекта, обеспечение информационной безопасности личности, общества и государства практически находится на стадии обсуждения, а не реализации системных решений. В результате весьма актуальной становится проблема замещения искусственным интеллектом человека в процессе его собственной жизнедеятельности. Она поднимается сегодня, поскольку человек прекращая совершать значительное количество операций по поиску, обработке, передаче информации становится полностью зависимым от роботов, доверяет им все больше и готов пожертвовать рядом своих свобод, законных интересов, в том числе и в сфере информационной безопасности, в ходе передачи тех или иных видов человеческих процессов роботам. Современный мир уже столкнулся с появлением возможностей искусственного интеллекта, превышающих интеллектуальные возможности человека. В связи с этим возникает проблема обеспечения безопасности человечества (причем как информационной, так и физической) и необходимости как на техническом, правовом, так и на этическом уровне, на уровне других регуляторов предусмотреть ограничения по использованию и развитию искусственного интеллекта.

Обеспечение информационной безопасности предполагает в первую очередь введе-

ние требований об информировании тех или иных субъектов об использовании технологий искусственного интеллекта и обязательного получения письменного согласия на обработку данных с использованием таких технологий. В этой связи важно ввести в законодательстве требования о таком информировании и специальном порядке получения согласия субъектами персональных данных, а также об ответственности за не информирование, отсутствие получения согласия на обработку данных в процессе использования искусственного интеллекта [1, с. 201-204].

Сегодня активно поднимается проблема применения роботов в военных целях. Военные роботы являются одной из наиболее опасных их разновидностей и их использование должно регулироваться на международном уровне. Вопрос о регулировании использования военных роботов был поднят ещё в 2013 г. в докладе Специального докладчика ООН Кристофа Хейнса, в котором рекомендовалось: ввести национальный мораторий в отношении военных роботов; заявить в одностороннем порядке и в рамках многосторонних форумов о приверженности соблюдению норм международного гуманитарного права во всей деятельности, связанной с роботизированными системами оружия; применять строгие процедуры соблюдения данных норм на всех стадиях разработки таких систем; взять обязательство обеспечивать максимально возможную степень транспарентности применительно к своим внутренним процедурам обзора вооружений, включая параметры, используемые при испытаниях роботизированных систем [2].

Сегодня «основное направление регулирования заключается в попытках приравнять военных роботов к негуманному оружию. То есть подчинить их специальной «Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие» 1980 г. Она ограничивает либо запрещает использование специальных видов вооружения. В частности, зажигательного оружия против населения, противопехотных мин, лазерного оружия и т.д.» [3, с. 247]. Использование роботов в качестве оружия проявляется активно в их использовании при совершении кибератак, использования в качестве информационного оружия, что требует особого международного контроля и запретов.

Противодействие терроризму. Террористы, извлекают выгоду из машинного обучения и других форм искусственного интеллекта, например, при подготовке своих военных операций и сборе информации. В частности, при проведении кибератак, автоматизированные задачи, выполняемые с использованием искусственного интеллекта, могут потенциально увеличить масштаб и влияние этих атак. ИГИЛ использовало небольшие беспилотники, вооруженные гранатами, Сирии. Тем более страшны идеи об использовании террористами «роя беспилотников» [4, 5].

Для противодействия террористам и возможным кибератакам применяется ряд мер – начиная от распознавания террористов с помощью искусственного интеллекта тех или иных лиц по камерам наблюдения, по голосу; использование искусственного интеллекта для распознавания и противодействия кибератакам со стороны террористов [6].

Использование прогнозирующих технологий искусственного интеллекта в борьбе с терроризмом часто считается пагубным воздействием на права человека, порождая спектры «докриминальных» наказаний в отношении тех или иных лиц, подозреваемых в подготовке к террористическим актам. Однако хорошо регулируемое использование новых возможностей может способствовать расширению возможностей государств по защите права граждан на жизнь при одновременном улучшении соблюдения принципов, направленных на защиту других прав человека, таких, как транспарентность, соразмерность и свобода от несправедливой дискриминации. Большинство государств сосредоточено на предотвращении террористических нападений, а не на реагировании на них. Таким образом, прогнозирование уже является центральным элементом эффективного противодействия терроризму. Искусственный интеллект позволяет анализировать большие объемы данных и может воспринимать закономерности в тех данных, которые по причинам как объема, так и размерности были бы в противном случае недоступны человеческой интерпретации. Следствием этого является то, что традиционные методы расследования, которые работают вне рамок известных подозреваемых, могут быть дополнены методами, которые анализируют деятельность широкой части всего населения для выявления ранее неизвестных угроз [7].

Противодействие терроризму, кибербе-

зопасности ставится как один из ключевых факторов, обосновывающих использование систем массового наблюдения и анализа информации о гражданах с использованием технологий искусственного интеллекта. Так, по данным Фонда Карнеги «За международный мир», как минимум 75 из 176 обследованных стран мира активно используют технологии искусственного интеллекта для целей наблюдения. К ним относятся системы распознавания лиц, интеллектуальные полицейские инструменты и создание безопасных городских платформ. Ведущими поставщиками этих систем во всем мире являются китайские фирмы, возглавляемые компанией Huawei, которая поставила эти технологии по меньшей мере в 50 государств мира [8]. Китайские компании быстро проникают на африканские рынки, предлагая правительствам льготные кредиты на покупку их оборудования и обещая создать и управлять этими системами. В Кении, например, Huawei помогла установить видеосистемы, которые развернули 1800 HD-камер и 200 HD-систем наблюдения за дорожным движением по всему Найроби [9]. В Зимбабве базирующийся в Гуанчжоу разработчик CloudWalk объявил о сделке в 2018 г. [10-12] по надзору за крупномасштабной программой распознавания лиц в сотрудничестве с властями [13]. Многие видят серьезную опасность того, что под видом борьбы с преступностью массовое наблюдение и отслеживание за гражданами, использование технологий искусственного интеллекта может подавить деятельность политической оппозиции [14].

Дебаты по поводу технологий искусственного интеллекта также происходят, когда африканские правительства и активисты сталкиваются по таким вопросам, как цифровая конфиденциальность, цензура информации, наблюдение и отключение интернета. С дефицитом законов о неприкосновенности частной жизни в таких странах, как Кения, есть озабоченность по поводу того, как правительства будут использовать эти хранилища данных, где они будут храниться, и кто будет иметь к ним доступ. Информационные и коммуникационные технологии могут быть использованы для запугивания и принуждения критиков государства. Американский аналитический центр Freedom House заявил, что Пекин обучает африканские государства некоторым из своих собственных ограничительных онлайн-мер [15].

По мере расширения масштабов деятельности Huawei в Африке в последние годы все более пристальное внимание уделяется ее деятельности. В 2018 году компания опровергла утверждения о том, что техническая инфраструктура, установленная ею в Африканском Союзе, использовалась Китаем для слежки за континентальным телом. Недавнее расследование Wall Street Journal также показало, что техники Huawei якобы помогали силам кибербезопасности в Уганде и Замбии перехватывать сообщения и выслеживать противников [16]. Стесненная в средствах полиция Уганды также купила телекамеры закрытого типа за 126 миллионов долларов у Huawei—шаг, который оппозиционные деятели опасаются использовать для идентификации и целеуказания демонстрантам и оппозиционным деятелям в преддверии выборов 2021 года [17].

Технологии искусственного интеллекта и противодействие преступности. Использование технологий искусственного интеллекта государством для реализации правоохранительной функции, в том числе при выявлении преступников и их розыске, может способствовать дискриминации отдельных социальных групп или граждан. Так, полиция США охотно использует технологии искусственного интеллекта, предназначенные для прогнозирования преступлений, чтобы решить, куда направлять офицеров для патрулирования [18]. Например, такой опыт был в Чикаго [19], где чикагская полиция использовала данные и компьютерный анализ, чтобы определить районы, в которых возможны насильственные преступления, и назначить дополнительные полицейские патрули в этих районах. Кроме того, программное обеспечение идентифицировало отдельных людей, которые, как ожидается, станут, но еще не стали жертвами или исполнителями насильственных преступлений [20]. Сегодня имеются и исследования, утверждающие, что такое расширенное использование данных о гражданах полицейскими может привести к дальнейшей ориентации на отдельные сообщества или цветных людей и подвергать их дискриминации. Анализ этих систем показывает, что данные, на которых обучаются эти системы, часто оказываются необъективными, что приводит к несправедливым результатам, таким как ложное определение того, что представители афроамериканской культуры более склонны совершать преступления, чем дру-

гие группы [18]. В последние годы имеется серьезная критика данных процессов со стороны специалистов, более 100 организаций в области гражданских прав, цифровой юстиции и общественных организаций выражают обеспокоенность по поводу досудебной оценки рисков [21].

Сегодня специалисты также приводят и ряд других случаев применения искусственного интеллекта для предупреждения и выявления преступлений [22]. Но и здесь существуют проблемы нарушений прав в сфере информационной безопасности. Таким образом, риск использования технологии искусственного интеллекта правительствами возможностями для мониторинга, отслеживания и наблюдения за отдельными людьми или социальными группами в целях ограничения или нарушения их прав реально подтверждается опытом Китая, который использует высокотехнологичные технологии искусственного интеллекта в Синьцзяне для ограничений уйгурского населения и других национальных этнических групп. Кроме того, Китай активно распространяет данные технологии, прежде всего в Африке. Правительства с демократическим режимом также могут иметь искушение злоупотреблять новыми технологическими возможностями искусственного интеллекта. Так, в США активно проводятся исследования компанией Microsoft с китайскими военными учеными об использовании искусственного интеллекта для наблюдения и анализа пространственных данных; США активно использовали технологии искусственного интеллекта для сбора и обработки данных в Европе и по всему миру в процессе разведывательной деятельности за правительствами и компаниями других стран. Это обусловливает необходимость разработки международных норм и требований к использованию технологий искусственного интеллекта в процессе наблюдения за гражданами, а также требований по использованию полученных данных для обеспечения недопустимости нарушения прав и свобод человека и гражданина, обеспечения верховенства права.

Использование технологий искусственного интеллекта государством для реализации правоохранительной функции, в том числе при выявлении преступников и их розыске, бесспорно, имеет весьма положительный опыт в США, Китае и активно распространяется в других странах. Искусственный интеллект позволяет как выявлять нарушителей, прогнозировать совершение преступлений, осуществлять розыск подозреваемых. Однако, как показывают исследования, данная практика может способствовать дискриминации отдельных социальных групп или граждан. В связи с этим необходима разработка требований о недопустимости при использовании таких технологий дискриминации отдельных социальных групп или граждан, нарушения иных прав и свобод человека и гражданина, а также требование минимизировать риск ошибки отнесения тех или иных граждан к подозреваемым в совершении преступления или к лицам, которые могут быть ошибочно отнесены к потенциальным правонарушителям. Кроме того, исследования технологий искусственного интеллекта, связанных с гендерным фактором свидетельствует, что темнокожие женщины являются наиболее неправильно классифицированной группой при распознавании, (с частотой ошибок до 34,7%). Максимальная же частота ошибок для светлокожих мужчин составляет 0,8%. Существенные различия в точности классификации более темных женщин, более светлых женщин, более темных мужчин и более светлых мужчин в системах гендерной классификации требуют безотлагательного внимания, если коммерческие компании хотят построить подлинно справедливые, прозрачные и подотчетные алгоритмы анализа лица [23].

Литература

1. Правовое регулирование цифровой экономики в современных условиях развития высокотехнологичного бизнеса в национальном и глобальном контексте : монография / под общ. ред. В. Н. Синюкова, М. А. Егоровой. Московский государственной юридический университет имени О. Е. Кутафина (МГЮА). – М.: Проспект, 2019. – 240 с.

2. Доклад Специального докладчика по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях Кристофа Хейнса. [Электронный ресурс] – URL.: http://undocs.org/ru/A/HRC/23/47 (дата доступа 18.03.2020).

3. Аналитический обзор мирового рынка роботизации. М.: Сбербанк, 2018. С. 247

4. Renske van der Veer Terrorism in the age of technology. [Электронный ресурс] – URL.: https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/(дата доступа 18.03.2020).

5. Miles Brundage et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, (February 2018). [Электронный ресурс] – URL.: https://www.experian.co.uk/blogs/latest-thinking/data-and-innovation/ai-counter-fraud-and-the-government-opportunities-in-emerging-technologies/(дата доступа 18.03.2020).

6. Yasmin Tadjdeh Algorithmic Warfare: DoD Seeks AI Alliance to Counter China, Russia. [Электронный ресурс] – URL.: https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia(дата доступа 18.03.2020).

7. Kathleen McKendrick Artificial Intelligence Prediction and Counterterrorism. [Электронный ресурс] – URL.: https://www.chathamhouse.org/publication/artificial-intelligence-prediction-and-counterterrorism (дата доступа 18.03.2020).

8. Steven Feldstein The Global Expansion of AI Surveillance / Carnegie Endowment for International Peace. [Электронный ресурс] – URL.: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final.pdf (дата доступа 18.03.2020).

9. Video Surveillance as the Foundation of "Safe City" in Kenya. [Электронный ресурс] – URL.: https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya (дата доступа 18.03.2020).

10. Lynsey Chutel China is exporting facial recognition software to Africa, expanding its vast database. [Электронный ресурс] – URL.: https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/ (дата доступа 18.03.2020).

11. Shan Jie China exports facial ID technology to Zimbabwe. [Электронный ресурс] – URL.: http://www.globaltimes.cn/content/1097747.shtml (дата доступа 18.03.2020).

12. Zhang Hongpei Chinese facial ID tech to land in Africa. [Электронный ресурс] – URL.: http://www.globaltimes.cn/content/1102797.shtml (дата доступа 18.03.2020).

13. Abdi Latif Dahir Chinese firms are driving the rise of AI surveillance across Africa . [Электронный ресурс] – URL.: https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/ (дата доступа 18.03.2020).

14. China's AI package for Africa includes mass surveillance technology. [Электронный ресурс] – URL.: https://mindmatters.ai/2019/05/chinas-ai-package-for-africa-includes-mass-surveillance-technology/ (дата доступа 18.03.2020).

15. Abdi Latif Dahir China is exporting its digital surveillance methods to African governments. [Электронный ресурс] – URL.: https://qz.com/africa/1447015/china-is-helping-african-countries-control-the-internet/ (дата доступа 18.03.2020).

16. Joe Parkinson, Nicholas Bariyo and Josh Chin Huawei Technicians Helped African Governments Spy on Political Opponents. [Электронный ресурс] – URL.: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (дата доступа 18.03.2020).

17. Musa Okwonga On returning to Uganda, Museveni's staying power and the significance of Bobi Wine. [Электронный ресурс] – URL.: https://qz.com/africa/1631116/returning-to-uganda-musevenis-reign-and-bobi-wines-music/ (дата доступа 18.03.2020).

18. Why big-data analysis of police activity is inherently biased. [Электронный ресурс] – URL.: https://theconversation.com/why-big-data-analysis-of-police-activity-is-inherently-biased-72640&usg=ALkJrhhJAILrqlCIewb2Kby9hP_4t5a5Dg (дата доступа 18.03.2020).

19. Электронный ресурс. – URL.: https://www.nbcnews.com/news/us-news/chicago-police-department-goes-high-tech-fight-rise-killings-n713206&usg=ALkJrhhHo866Kk6_sm86Gy6WOtFAtZiq_A (дата доступа 18.03.2020).

20. Andrew V. Papachristos CPD's crucial choice: Treat its list as offenders or as potential victims? [Электронный ресурс] – URL.: https://www.chicagotribune.com/opinion/commentary/ct-gun-violence-list-chicago-police-murder-perspec-0801-jm-20160729-story.html&usg=ALkJrhhGNFNEg9CVZfpdgbscS95C0X4rZA (дата доступа 18.03.2020).

21. How well do IBM, Microsoft, and Face++ AI services guess the gender of a face?[Электронный ресурс] – URL.: https://z5h64q92x9.net/proxy_u/en-ru.ru/gendershades.org/ (дата доступа 18.03.2020).

22. More than 100 Civil Rights, Digital Justice, and Community-Based Organizations Raise Concerns About Pretrial Risk Assessment. [Электронный ресурс] – URL.: https/civilrights.org/2018/07/30/more-than-100-civil-rights-digital-justice-and-community-based-organizations-raise-concerns-about-pretrial-risk-assessment/ ; Karen Hao AI is sending people to jail—and getting it wrong, Jan 21, 2019 // https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/ (дата доступа 18.03.2020).

23. Daniel Faggella AI for Crime Prevention and Detection – 5 Current Applications. [Электронный ресурс] – URL.: https://emerj.com/ai-sector-overviews/ai-crime-prevention-5-current-applications/ (дата доступа 18.03.2020).

References

1. Pravovoye regulirovaniye tsifrovoy ekonomiki v sovremennykh usloviyakh razvitiya vysokotekhnologichnogo biznesa v natsional'nom i global'nom kontekste : monografiya / pod obshch. red. V. N. Sinyukova, M. A. Yegorovoy. Moskovskiy gosudarstvennoy yuridicheskiy universitet imeni O. Ye. Kutafina (MGYUA). – M.: Prospekt, 2019. – 240 s.

2. Doklad Spetsial'nogo dokladchika po voprosu o vnesudebnykh kaznyakh, kaznyakh bez nadlezhashchego sudebnogo razbiratel'stva ili proizvol'nykh kaznyakh Kristofa Kheynsa. [Elektronnyy resurs] – URL.: http://undocs.org/ru/A/HRC/23/47 (data dostupa 18.03.2020).

3. Analiticheskiy obzor mirovogo rynka robotizatsii. M.: Sberbank, 2018. S. 247.

МИНБАЛЕЕВ Алексей Владимирович, заведующий кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), профессор кафедры теории государства и права, конституционного и административного права Южно-Уральского государственного университета (национального исследовательского университета), доктор юридических наук, доцент. 123001, г. Москва, ул., Садовая-Кудринская, 9. 454080, г. Челябинск, пр. Ленина, 76. Email: alexmin@bk.ru

MINBALEEV Aleksey, head. Department of information law and digital technologies of the Moscow state law University named after O. E. Kutafin (MSAL), Professor of the Department of theory of state and law, constitutional and administrative law, South Ural state University (national research university) Doctor of Law, Associate Professor. 123001, г. Москва, ул., Садовая-Кудринская, 9. 454080, г. Челябинск, пр. Ленина, 76. Email: alexmin@bk.ru