Секция «Искусственный интеллект и «умное» государственное управление: от ретроспективности к проспективности контроля (надзора)»

АСПЕКТЫ ПРИМЕНЕНИЯ ARTIFICIAL INTELLIGENCE В СФЕРЕ ГОСУДАРСТВЕННОЙ ОБОРОНЫ И БЕЗОПАСНОСТИ: АНАЛИТИКА ЗАРУБЕЖНОГО ОПЫТА

Научный руководитель – Власенко Николай Александрович

Musina Kamilla

Аспирант

Российский университет дружбы народов, Юридический факультет, Москва, Россия

E-mail: camillamusina2015@mail.ru

В условиях сложившейся ситуации в Украине и информационной войны, которую пытаются вести страны НАТО, жестких санкций и нестабильной ситуации в сфере авиации, связанных с «закрытием неба» с 25 февраля 2022, на мой взгляд, актуализировалась тема укрепления обороны и безопасности России, которую целесообразнее осуществлять путём активного внедрения искусственного интеллекта (*далее* - ИИ). Более подробно будет рассмотрен опыт зарубежных стран, в частности в США агентство перспективных исследований в сфере обороны (*DARPA*) в 70-х годах представило финальный проект картографирования городских улиц. Что послужило стартапом для автоматизации. Кроме того, разрабатываются нормативные документы и активно внедряются разработки ИИ. В том числе и в большей степени военные милитаристские цели и космос продолжают оставаться в этой стране в приоритете. В период президентства Д. Трампа Белый дом акцентировал на сфере развития ИИ. Так, был разработан и внесен законопроект об ИИ на Федеральном уровне[1]. Одновременно стремительно продолжает активно финансироваться инновации ИИ. В 2018 г. в США венчурные инвесторы в развитие разработок ИИ вложили более 9,3 млрд $ [2]. Вышеизложенные факты как *de facto*, так и *de jure* являются свидетельством того, что США стремится завоевать приоритет в кибер цифровой сфере. Одной из острых, нерешённых до сих пор в полном объёме проблем является сохранение восприимчивости к попыткам оказывать латентное манипулирование и преднамеренное причинение вреда (ИИ) киборга. Так, «злоумышленники» могут применить ИИ для кибератак либо физических атак на инфраструктуру населенных пунктов. Кроме того, сохраняется риск использования программ с исходным кодом в целях проникновения в системы ИИ вражеских стран. ИИ используются в обороне с 70-х годов. Так, в июле 2016 Министерство внутренней безопасности США опубликовало доклад «Критическая инфраструктура США до 2025: стратегическая оценка рисков»[3]. Управление анализа кибер-инфраструктуры Министерства выявило 6 основных тенденций. Указанные в докладе факторы повлияют на безопасность США в течение следующих 10 лет. В 2017 г. ИИ дополнен в «Стратегию национальной безопасности США»[4] в связи с его «ролью в руководстве технологическими инновациями и важнейшим значением в информационном управлении государством, обороной и контролем». В 2018 ИИ был закреплен в Стратегии национальной обороны [5], где он описан «как одна из технологий, которые изменят характер войны и дадут все более изощренные возможности нашим противникам, включая негосударственные субъекты». В июле 2018 Министерство обороны США создало Объединенный центр ИИ (*Joint AI Center*) для изучения использования Агентством ИИ. Цели Центра - улучшение сотрудничества с частным сектором, академическими кругами и военными союзниками, привлечение талантов и создание этических рамок для ИИ, оказание помощи в стратегии национальной обороны. Минобр США в 2018 заявило, что в течение

5 лет инвестирует 2 млрд $ в развитие ИИ [6]. Что дополнит гос. расходы, которые в 2017 превысили 2 млрд $, не считая бюджеты Пентагона и разведки. Финансирование последовало за объявлением Комиссии нац.безопасности по ИИ (*NDAA*)[7], ставшей легальной после вступления в 2018 в силу Закона «Об авторизации национальной обороны на 2019 финансовый год»[8], оценивает последствия использования ИИ для безопасности США. Кроме того, власти США не ограничиваются лишь документами, носящими рекомендательный характер в сфере ИИ, ведётся большая правотворческая деятельность как на уровне штатов, так и на федеральном уровне.

«В госсекторе актуально применять ИИ в координации деятельности субъектов информационной инфраструктуры РФ по вопросам обнаружения, предупреждения и ликвидации последствий атак и реагирования на инциденты — того, что делает сейчас Национальный координационный центр (НКЦКИ) при помощи государственной системы обнаружения, предупреждения и ликвидации последствий хакерских зарубежных атак (ГосСОПКА)», по мнению эксперта, искусственный интеллект уже может использоваться для разделения угроз по различным отраслям, обработки больших данных и выявления паттернов актуальных угроз со стороны прогосударственных хакерских группировок и прогнозирования влияния их воздействия на экономическую экосистему страны[9]. В связи с вышеизложенным и ситуацией с Украиной, и НАТО целесообразно взять курс на:

1) Модернизацию инноваций ИИ в сфере космического, спутникового обнаружения ядерной активности с идентификацией точного местоположения по масштабу;
2) Сосредоточить финансирование разработок ИИ для Минобороны России;
3) Возложить на органы исполнительной власти [10] в осуществлении государственного управления и на военную прокуратуру миссию по кибертизации всех подразделений и структур, что ускорит и упростит работу сотрудников.

Президентом В. Путиным издан Указ № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития ИИ на период до 2030 года»). В связи с этим целесообразнее в дальнейшем взять курс и стратегию направленные на укрепление и усиление обороны и безопасности России, в том числе и от информационных кибер-атак зарубежных хакеров и иностранных мошенников. Для решения данной актуальнейшей проблемы необходимо производить финансирование и развитие цифровизации и систем искусственного интеллекта благодаря активной модернизации ИИ по специальным Оборонзаказам и закупкам «кибер - проектов», с последующим тестированием и устранением возникновения сбоев программ «Электронных лиц», минимизируя все возможные сбои и взломы извне.

Источники и литература

1) Закон о разрешении национальной обороны на финансовый год 2019. URL: https://www.congress.gov/bill/115th-congress/house-bill/5515/text#toc-H6C2FA09C23154F80B0D293929D5ACFB5
2) Комиссия национальной безопасности по искусственному интеллекту. URL: https://dig.watch/updates/members-appointed-us-national-security-commission-artificial-intelligence
3) U.S. Critical Infrastructure 2025: A Strategic RIsk Assessment. URL: https://publicintelligence.net/dhs-ocia-critical-infrastructure-2025
4) URL: https://www.nitrd.gov/pubs/2017supplement/FY2017NITRDSupplement. pdf
5) URL: https://www.cbinsights.com/research/artifi cial-intelligence-startup-us-map
6) URL:https://partner-mco-archive.s3.amazonaws.com/client_fi les/1513628003.pdf

7) URL:https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense Strategy-Summary.pdf

8) URL:https://www.washingtonpost.com/technology/2018/09/07/defense-depart ment-pledges-billions-toward-artificial-intelligence-research/?utm_term=.0f0e8bde2477

9) Искусственный интеллект в госсекторе. URL:https://ecm-journal.ru/material/Iskusstv ennyjj-intellekt-v-gossektore-Obzor-kejjsov-2021

10) Пикулькин А. В. Система государственного управления. 3-е изд. М., 2004