Секция «Коммуникация в современном мире»

# Негативное действие искусственного интеллекта на международную информационно-психологическую безопасность в Северо-Восточной Азии

**Научный руководитель – Дам Ван Ньить -**

***Дам Ван Ньитъ***
*Кандидат наук*
Национальный исследовательский университет «Высшая школа экономики», Факультет компьютерных наук, Москва, Россия
*E-mail: vdam@hse.ru*

К 2020 году элементы искусственного интеллекта (ИИ) уже присутствуют во всех новых программных продуктах и сервисах. ИИ станет приоритетом для инвестиций почти трети компаний в мире. Вместе с своими преимуществами ИИ скрывает в себе ряд негативных влияний, в том числе влияния на международную информационно-психологическую безопасность (МИПБ) путем целевого высокотехнологичного информационно-психологического воздействия на сознание граждан [1, 2, 6, 7].

Северо-Восточная Азия (СВА) — один из самых важных с геополитической точки зрения регионов в мире. В последнее время с быстрым подъемом Китая, увеличением присутствия и роли США политическая ситуация и безопасность в регионе претерпевают резкие и неожиданные изменения. В СВА присутствуют зоны потенциальных конфликтов, такие как Корейский полуостров с его ядерной проблемой [8], стратегическая конкуренция между Японией и Китаем в спорных островах Сенкаку/Дяоюйдао [9], а также Японией и Южной Кореей вокруг островов Такэсима/Докдо [10]. Китай, Япония и Южная Корея считаются странами с самым быстрым темпом развития технологий ИИ как в регионе, так и в мире [3, 4, 5]. Это влечет за собой непредвиденные угрозы, включая злонамеренное использование искусственного интеллекта (ЗИИИ).

В обучении нейронной сети одним из важнейших этапов является подготовка наборов данных, а эти наборы данных подготовляются людьми. Поэтому процесс обучения интеллектуальных систем носит прежде всего носит антропогенный характер, изменение в наборах данных проводит к изменению работы обученной нейронной сети. Злоумышленники могут использовать это свойство для создания и распространения намеренных информационных продуктов на разные аудитории. Кроме этого, интеллектуальные системы, разработанные на благо людей, могут использоваться против них. Среди возможных угроз ЗИИИ для МИПБ можно назвать следующие [4]:

**Перепрофилирование коммерческих систем искусственного интеллекта**. Коммерческие системы могут быть использованы во вред (даже не всегда намеренно). Возможно использование беспилотных летательных аппаратов или автономных транспортных средств для доставки взрывчатых веществ и организации аварий.

**Создание deepfakes**. Это метод синтеза человеческого изображения, голоса и видео на основе использования ИИ, например, нейронной сети GAN. Создание deepfakes уже стало очень простым благодаря доступным открытым кодам в Интернете. Поэтому любой специалист в области ИИ без трудностей может создавать ложные изображения и видео для использования в своих целях, и это вызывает непредсказуемые угрозы для общества.

**Боты**. Это инструмент помогает быстро разослать на целевую аудиторию намеренную информацию.

**Прогностическое оружие**. ИИ, машинное обучение и анализ тональности текста позволяют предсказывать будущее путем анализа прошлого. Неправильное предсказание

проводит к ложной сигнализации, и если это происходит на государственном уровне, то будет вызывать панику в обществе.

**Компьютерные игры с использованием ИИ**. В Китае, Японии и Южной Корее существуют много сообществ компьютерных игр, в которых участвуют подростки. Эта среда может повысить эффективность информационно-психологического воздействия.

Чтобы избежать вышесказанных угроз, самому обществу необходимо повышать свои знания об ИИ, одновременно осознавая и принимая коллективную ответственность за общее будущее.

### Источники и литература

1) Пашенцев Е.Н., Фан К.Н.А., Дам В.Н. Злонамеренное использование искусственного интеллекта в Северо-Восточной Азии и угрозы международной информационно-психологической безопасности // Государственное управление. Электронный вестник. 2020, № 80, С. 175 – 196.
2) Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // Государственное управление. Электронный вестник. 2019, № 76. С. 279 – 300.
3) Ким С.С., Чой Й.С. Программа инновационных платформ как новый драйвер экономического роста Южной Кореи // Форсайт. 2019, Т. 13, № 3. С. 13 – 22.
4) Комиссина И.Н. Современное состояние и перспективы развития технологий искусственного интеллекта в Китае // Проблемы национальной стратегии. 2019, № 1(52). С. 137 – 160.
5) Костюкова К.С. Политика цифровой трансформация Японии на примере развития технологии искусственного интеллекта // Мир (Модернизация. Инновации. Развитие). 2019, Т. 10, № 4. С. 516 – 529.
6) Horowitz M.C., Scharre P., Allen G.C., Frederick K., Cho A., Saravalle E. Artificial Intelligence and International Security. Washington: Center for a New American Security (CNAS), 2018.
7) Pashentsev E. AI and Terrorist Threats: The New Dimension for Strategic Psychological Warfare // Bazarkina D., Pashentsev E., Simons G. (eds.) (Forthcoming) Terrorism and advanced technologies in psychological warfare: new risks, new opportunities to counter the terrorist threat. New York: Nova Science Publishers, 2020.
8) Gentile G., Crane Y.K., Madden D., Bonds T.M., Bennett B.W., Mazarr M.J., Scobell A. Four Problems on the Korean Peninsula: North Korea's Expanding Nuclear Capabilities Drive a Complex Set of Problems. Arroyo Center. 2019.
9) Zhang Y., Liu J., Wen J. Nationalism on Weibo: Towards a Multifaceted Understanding of Chinese Nationalism. The China Quarterly. 2018, Vol. 235. p. 758 – 783.
10) Tsuchiyama J. The Balance of Power in Korea, and Japan // Japan Review. 2019, Vol. 2, No. 4. p. 29 – 33.