

УДК 343.231

DOI 10.37279/2413-1733-2021-7-2-191-194

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

Зоз В. А., Шроль А. Р.

Крымский филиал Краснодарского университета МВД России

В статье раскрывается вопрос внедрения информационных технологий в правоохранительную деятельность, а конкретно искусственного интеллекта. Проведен анализ того, насколько целесообразно использовать современные разработки в деятельности правоохранительных органов.

Понятие искусственного интеллекта возникло еще в первой половине прошлого века, в работах Винера, где он впервые заговорил о понятии «кибернетика». Использование понятия искусственного интеллекта в современном мире, в последнее время набирает обороты. Однако практическое использование искусственного интеллекта в правоохранительной деятельности началось только в начале 2000-х. Вместе с тем это не мешает на данный момент иметь разнообразный спектр программ и разработок, которые способствуют более быстрому и качественному предотвращению, пресечению, выявлению и раскрытию преступлений. Рассмотрено появление такого понятия как искусственный интеллект и кибернетика. Охарактеризованы виды разработок искусственного интеллекта. Рассмотрены направления деятельности правоохранительных органов по использованию искусственного интеллекта в зарубежных странах. Определены направления по улучшению работы эффективности искусственного интеллекта в деятельности правоохранительных органов.

Ключевые слова: искусственный интеллект, кибернетика, современные технологии, общественная безопасность, правоохранительные органы.

Современный мир характеризуется стремительно развивающимися информационными технологиями, которые активно внедряются в деятельность правоохранительных органов как вспомогательные элементы при обеспечении общественного порядка и общественной безопасности на территории нашего государства.

Процесс внедрения информационных технологий в деятельность правоохранительных органов стал более актуален с момента появления искусственного интеллекта (Далее – ИИ).

Если разобраться подробнее, то можно отметить, что предпосылки возникновения искусственного интеллекта проявились в 1940-х гг., когда Норберт Винер опубликовал работы по кибернетике, где впервые прозвучало понятие «искусственный интеллект» [1].

На данный момент технологии искусственного интеллекта активно используются за рубежом, в частности подразделениями ФБР совместно с корпорацией «Google».

Вместе с тем необходимо обратить внимание на то, что технологии искусственного интеллекта также нашли свое применение и в преступном мире. Из чего следует сделать вывод, что в противовес преступности также необходимо противопоставить и эффективно использовать технологии искусственного интеллекта со стороны правоохранительных органов [5].

Серьезное обсуждение и внедрение в практику искусственного интеллекта в правоохранительные органы началось в 2000-х годах. Однако наиболее активное практическое использование началось после 2010 года.

Среди программ и разработок искусственного интеллекта, в том числе связанные с робототехникой, которые сейчас активно используются, или планируются их последующее внедрение следует отметить: программы видеонаблюдения со считыванием биометрических данных человека; программы распознавания голоса; программы, которые распознают украденные транспортные средства; программы, которые способны распознавать существенное нарушение общественного порядка, митинги, акты вандализма и др.; системы судебной экспертизы; роботы, которые позволяют производить осмотр особо опасных объектов; боты, которые используются для первичных автономных контактов с гражданами и организациями [2].

Чтобы минимизировать риски и угрозы, возникающие при использовании ИИ, целесообразно разрабатывать соответствующие законы и внутренние нормативные акты учитывая положительный опыт их предупреждения и устранения, применяемый зарубежными странами, в том числе использование международных этических кодексов и рекомендаций [6].

В настоящее время достаточно остро стоит вопрос о том, насколько этично будут применяться результаты деятельности технологий ИИ, готово ли общество и его граждане допустить в свою жизнь ИИ, какие допустимые границы будет иметь ИИ, какова пропорциональность действий ИИ на выявленные угрозы, в том числе те, которые еще не реализованы. В частности, системы видеомониторинга, а также системы распознавания лиц, которые предоставляют сведения правоохранительным органам явно вторгаются в частную жизнь граждан. Кто при этом сможет распорядиться полученными данными кроме правоохранительных органов, как интернет - провайдеры будут предоставлять сведения правоохранительным органам, насколько эти данные будут корректными, и не подвержены искажению, либо обработки? В данном случае можно говорить о применении технологии ИИ «дипфейк» (Deepfake) при помощи которой преступники искажают реалистичные фото, аудио, видео и иные носители информации о лицах, местах, предметах, событиях, обстоятельствах и т.п. и тем самым создают качественную подделку, путем кибератаки на нейронные сети через введение данных (добавка «малого возмущения»), вследствие чего данные могут полностью изменить результаты работы нейронной сети, что порождает явное недоверие к любой информации.

В данном случае проблематика заключается в возможности нарушения всеобщих правах человека, одним из принципов которых является неприкосновенность частной жизни. В связи с чем возникает вопрос, можно ли использовать информационные технологии, которые будут, затрагивать частную жизнь общества и граждан для достижения целей правоохранительных органов.

С одной стороны, неправильно, независимо для каких целей, несанкционированно вторгаться в частную жизнь граждан, однако общество, в то же время, заинтересовано в своей безопасности, и использование ИИ для предотвращения преступлений, только улучшит состояние безопасности граждан, общества и государства в целом.

Данный вопрос требует тщательной проработки на законодательном уровне.

Проблематика применения и использования технологий ИИ и робототехники рассматривалась также на международном уровне, а именно в организации по безопасности и сотрудничеству в Европе (далее – ОБСЕ) [7].

На основе обсуждений полиции стран ОБСЕ предложено обратить особое внимание на следующие факторы: пресечение постоянно расширяющейся эксплуатации преступниками ИИ, как, в первую очередь, инструмента кибер-, финансовой и иной высокотехнологичной преступности; более активном использовании информационных технологий, также искусственного интеллекта для предвидения дальнейших действий преступников, и также к решению и выбору других средств, методов и способов в борьбе с преступностью; более широком использовании робототехники при патрулировании и оказании поддержки, а также обеспечении информационной осведомленности полицейских на земле, экипажей полицейских машин и т.п.; необходимости преодоления невысокого уровня компетенций рядовых сотрудников полиции в сфере ИИ; расширение международных контактов, связанных с использованием ИИ, ликвидации дублирования усилий и бессмысленной траты ресурсов, когда каждая полицейская структура стремится решить задачи в одиночку; особую чувствительность общественности к угрозам вмешательства в частную жизнь граждан и недопустимость перехода этических границ правоохранительными органами при практическом использовании ИИ [3].

Итогами внедрения ИИ и робототехники должно являться предупреждение, пресечение противоправных действий, повышение уровня раскрываемости преступлений, совершаемых в общественных местах.

При рассмотрении теоретических аспектов использования сегментов искусственного интеллекта, необходимо уяснить, что данная система является важнейшим элементом оснащения современными техническими средствами и системами информирования правоохранительных органов и всех экстренных служб. Искусственный интеллект должен являться средством защиты населения и территории, увеличения уровня безопасности в рамках различных сфер жизнедеятельности современного общества [4]. Этот продукт включает в себя разработку мер, направленных на предупреждение террористических угроз, обеспечение большей безопасности в местах значительного скопления людей. Данный комплекс мер направлен на сохранение безопасности стратегически важных объектов. Его внедрение дает возможность оптимизировать контроль рабочей силы, более эффективно распределять средства, которыми располагают ответственные за порядок структуры.

Для того чтобы программы искусственного интеллекта могли полноценно работать, должны быть сформированы подразделения, на которые будет возложена ответственность за развитие технического обеспечения рабочих процессов. При этом, по нашему мнению, передача указанных функций сторонним организациям нецелесообразна и может создать угрозу безопасности личных данных граждан, создать препятствия в работе правоохранительных органов.

Учитывая возможные риски внедрения технологий ИИ необходимо понимать важность данного вопроса, в частности имеется потребность развития системы фотографирования, записи видео, с целью повышения уровня безопасности. В первую очередь это касается ситуации на дорогах. Полезными будут комплексы,

которые созданы для фиксации нарушений норм и правил дорожного движения. Не менее важно развивать ситуационное видеонаблюдение в качестве инструментов, которые позволят повысить уровень общественной безопасности.

В целях повышения эффективности работы указанных систем, необходимо создать единую сеть, которая будет объединять базы данных, системы наблюдения, мониторинга и т.п., накапливать и анализировать полученную информацию. И в последующем прогнозировать дальнейшее развитие ситуаций, связанных с безопасностью дорожного движения, общественной безопасности, серийностью совершаемых преступлений, оперативной обстановки, складывающейся как на определенной территории, так и по стране в целом.

Список литературы

1. Reese H. Understanding the differences between AI, machine learning, and deep learning [Electronic resource]. – Mode of access: <https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning>.
2. Боровская Е.В. Основы искусственного интеллекта / Е.В. Боровская, Н.А. Давыдова. – М.: Лаборатория знаний, 2018. – 127 с.
3. Авторский блог Владимир Овчинский 12:43 25 сентября 2019 / Электронный ресурс: https://zavtra.ru/blogs/iskusstvennij_intellekt_dlya_politcii
4. Ларина Е.С. Роботы-убийцы против человечества. Кибер-апокалипсис сегодня / Е.С. Ларина, В.С. Овчинский. – М.: Кн. мир, 2018. – 416 с.
5. Евдокимов К.Н. Анекселентотичная технотронная преступность (частная теория) // Российский судья. – 2018. – № 4. – С. 35–39.
6. Уэмюра Н. Стратегия «Общество 5.0» // Известия. – 2017. – 13 марта.
7. Яковец Е.Н. Оперативно-разыскные меры полиции по обеспечению информационной безопасности Российской Федерации // Труды Академии управления МВД России. – 2017. – № 3. – С. 127–131.

Zoz V.A., Shrol A.R. Use of Artificial Intelligence Technologies in Law Enforcement Agencies // Scientific notes of V. I. Vernadsky Crimean federal university. Juridical science. – 2021. – 2021. – Т. 7 (73). № 2. – Р. – 191-194.

The article reveals the process of implementing information technology in law enforcement, specifically the introduction of artificial intelligence. It is analyzed how qualitatively and expediently to use modern developments in the activities of law enforcement agencies. Artificial Intelligence began to arise in the first half of the last century, in the works of Wiener, where he first spoke of the concept of cybernetics. The use of artificial intelligence in the modern world, is gaining momentum since the last century. However, the use of artificial intelligence in law enforcement began only in the early 2000s. But this does not prevent at the moment have a diverse range of programs and developments that contribute to a faster and better prevention, suppression, detection and solving of crimes. Examined the emergence of such a concept as artificial intelligence and cybernetics. Types of developments of artificial intelligence are characterized. Methods to improve the effectiveness of artificial intelligence in law enforcement have been defined.

Key words: artificial intelligence, cybernetics, modern technology, public safety, law enforcement agencies.

Spisok literatury

1. Reese H. Understanding the differences between AI, machine learning, and deep learning [Electronic resource]. – Mode of access: <https://www.techrepublic.com/article/understanding-the-differences-between-ai-machine-learning-and-deep-learning>.
2. Borovskaya E.V. Osnovy iskusstvennogo intellekta / E.V. Borovskaya, N.A. Davydova. – М.: Laboratoriya znaniy, 2018. – 127 s.
3. Avtorskiy blog Vladimir Ovchinskij 12:43 25 sentyabrya 2019 / Elektronnyj resurs: https://zavtra.ru/blogs/iskusstvennij_intellekt_dlya_politcii
4. Larina E.S. Roboty-ubijcy protiv chelovechestva. Kiber-apokalipsis segodnya / E.S. Larina, V.S. Ovchinskij. – М.: Кн. мир, 2018. – 416 s.
5. Evdokimov K.N. Anekselenkotichnaya tekhnotronnaya prestupnost' (chastnaya teoriya) // Rossijskiy sud'ya. – 2018. – № 4. – С. 35–39.
6. Uemura N. Strategiya «Obshchestvo 5.0» // Izvestiya. – 2017. – 13 marta.
7. Yakovec E.N. Operativno-razysknyye mery policii po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii // Trudy Akademii upravleniya MVD Rossii. – 2017. – № 3. – С. 127–131.