УДК 343.341

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СРЕДСТВО ПРОГНОЗИРОВАНИЯ И ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

В. А. Мазуров, М. А. Стародубцева
Алтайский государственный университет (Барнаул, Россия)

Раскрывается понятие «искусственный интеллект», а также другие, связанные с ним термины. Проанализированы приемы и методы использования достижений научно-технического прогресса в противоправной деятельности, выявлены приоритетные направления противодействия преступности в целом и ее конкретным видам.

***Ключевые слова*:** искусственный интеллект, глубинное обучение, большие данные, цифровая криминология, современные технологии противодействия преступности.

ARTIFICIAL INTELLIGENCE AS A MEANS FOR FORECASTING AND COUNTERING CRIME

V. A. Mazurov, M. A. Starodubtseva
Altai State University (Barnaul, Russia).

The article reveals the concepts of “artificial intelligence”, other related definitions and concepts. Techniques and methods for using the achievements of scientific and technological progress in illegal activities and priority areas for combating crime in general and its specific types are indicated.

***Keywords*:** artificial intelligence, deep learning, Big data digital criminology, modern technologies for combating crime.

Рождение искусственного интеллекта как научного направления связывают с 1940 гг., когда Норберт Винер опубликовал свои основополагающие работы по кибернетике. Собственно термин «искусственный интеллект» (англ. artificial intelligence) был предложен в 1956 г. в Дартмутском колледже (США) на семинаре с одноименным названием, где был выдвинут ключевой тезис: «Каждый аспект обучения или любая другая особенность интеллекта могут быть в принципе так точно описаны, что машина сможет сымитировать их» [1, с. 44].

Система искусственного интеллекта — это программная система, имитирующая на компьютере процесс мышления человека. Искусственный интеллект представляет собой направление информатики, целью которого является разработка аппаратно-программных средств, позволяющих пользователю-непрограммисту ставить и решать свои традиционно считающиеся интеллектуальными задачи, общаясь с ЭВМ на ограниченном подмножестве естественного языка [2, с. 5].

Так, например, информационные подразделения ФБР совместно с лабораторией искусственного интеллекта корпорации Google выработали следующее инженерное определение искусственного интеллекта: «Искусственный интеллект — это программно-аппаратный комплекс, обеспечивающий поддержку и/или принятие результативных решений в динамичной, неустойчивой среде в установленное время на основе заведомо неполной, нечеткой и не имеющей полной доказательственной базы информации».

В последнее время понятие «искусственный интеллект» упоминается наряду с такими терминами, как «большие данные» (Big Data), «машинное обучение», «глубинное обучение» и «нейронные сети».

Большие данные, согласно терминологии ООН, представляют собой накопление и анализ значительно возросшего объема информационных ресурсов, который повышает возможности их хранения и анализа с использованием созданных ранее аппаратных и программных средств [3, с. 129]. Появ-

ление больших данных стало возможным благодаря расширению возможностей хранения данных и круга имеющихся в наличии их источников, в число которых входят данные спутниковых изображений, сетей мобильной телефонной связи, социальных сетей и сканирующих устройств [3, с. 130–132].

Машинное обучение — одно из направлений искусственного интеллекта, основной принцип которого заключается в том, что машины получают данные и «обучаются» на их основе. В настоящее время это наиболее перспективный инструмент для бизнеса, науки и сферы принятия важных управленческих решений. Системы машинного обучения позволяют быстро применять знания, полученные при обучении на больших наборах данных, за счет чего преуспевают в распознавании лиц, речи, объектов, переводе и многом другом.

Глубинное обучение является подмножеством машинного обучения. Оно использует некоторые методы машинного обучения для решения реальных задач, применяя нейронные сети, которые могут имитировать принятие решений человеком.

Нейронные сети возникли в результате исследований в области искусственного интеллекта, и спустя уже 20 лет были разработаны однослойные нейронные системы (*перцептроны*), которые в ряде случаев оказались способны обучаться, осуществлять предсказания и распознавать образы. К 1980-м гг. в этой области произошел прорыв благодаря революционным работам Джона Хопфилда и Тейво Кохонена. Многослойные нейронные сети нового поколения успешно справлялись с задачами, недоступными для перцептронов [2, с. 112–113].

Теоретические, практические и этико-правовые аспекты использования искусственного интеллекта в противодействии преступности широко освещаются в работах зарубежных авторов, а с недавних пор — и в отечественных исследованиях. Неоценимый вклад в познание возможностей современных технологий внесли В. С. Овчинский и Е. С. Ларина [3, с 18], рассматривающие искусственный интеллект как технологию тройного назначения, которая может быть использована для гражданских, военных и криминальных целей [2, с. 374].

Отличительная особенность современной преступности — ее способность брать на вооружение передовые технологические решения, что обусловлено ее безграничными финансовыми возможностями и определенной прозрачностью научных достижений.

Изучение современной высокотехнологичной преступности позволяет выделить следующие способы и сферы использования преступниками искусственного интеллекта.

Фишинг (англ. fishing — рыбная ловля, выуживание) представляет собой вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя — логинам и паролям.

Дроны стали применяться для слежки за агентами и сотрудниками правоохранительных органов, за свидетелями преступлений и членами конкурирующих преступных группировок, а также в поисках объектов для краж и ограблений, с целью слежения за контейнерами с контрабандным товаром и съемок интимных встреч для дальнейшего шантажа.

Синтезирование фейковой информации тесно связано с хакерскими атаками, призванными дискредитировать органы власти и должностных лиц, спровоцировать панику.

Использование автоматизированных автономных систем, управляемых искусственным интеллектом, применяется в качестве способа компенсации низкой квалификации людей: так, активное применение наводящихся с использованием искусственного интеллекта снайперских винтовок дальнего действия, имеющих джойстики для управления, заметно снижает требования к профессиональной подготовке боевиков [3, с. 45].

Наблюдается процесс автоматизации *социальной инженерии*, примером чего являются так называемые боты. *Бот (сокр. от «робот»)* — это программа, способная по определенному алгоритму выполнять какие-либо действия через интерфейсы, предназначенные для людей, например вести диалог с посетителями форума либо в соцсети.

Беспрецедентная атака ботов, зазывающих пользователей в печально известные «группы смерти», была отмечена в 2017 г. в социальной сети «ВКонтакте». В марте 2017 г. руководитель отдела модерации «ВКонтакте» И. Коренев сообщил, что с начала января на сайте этой соцсети было сгенерировано около 3 млн сообщений с хештегами и стишками, возможно, призывающими к суициду. Подобные сообщения при этом постоянно менялись, размывались какими-либо символами. Руководство «ВКонтакте» увидело за таким всплеском «целенаправленную атаку ботов», что было очевидно,

так как «в этот период появилось несколько тысяч страниц, созданных исключительно для того, чтобы публиковать такие хештеги» [4, с. 12].

Специалисты Центра исследований легитимности и политического протеста провели анализ страниц, с которых пошла новая волна стихотворений с хештегом, выяснили время запуска стихов, а также использованные для этого аккаунты. Анализ аккаунтов позволил сделать вывод, что имела место автоматизированная рассылка стихов по страницам «ВКонтакте». Большинство рассылок выявлено на устройствах, работающих под операционной системой Android, программой рассылки оказалась VK iHA bot. Этот робот появился в Сети в 2014 г., его следы привели к человеку, известному под ником Dr. Failov.

Раскрытая схема ботов показала, что вовлечение подростков в «игру» производилось в автоматическом режиме программными средствами. Робот сам мог вести диалог с пользователями, отвечая на стандартные вопросы и распознавая сленг молодежной аудитории. Машина предлагала написавшему подростку сделать выбор («Если да, напишите 1, если нет, напишите 0»), таким образом отсеивая других ботов и допуская несовершеннолетнего на следующий уровень в «игре». В результате сначала один робот делал посев стиха, сам фильтровал его и находил посты реальных подростков. Все эти действия робот совершал через так называемое API VK (англ. application programming interface). Внутри API есть функция автоматического размещения записей, которую и использовал данный бот. Человек-куратор, купивший бота, подключался к работе с уже готовыми к серьезной «игре» подростками [2, с. 15].

Продвинутым вариантом социальной инженерии является ситуация, когда человек, участвующий в диалоге с ботом, уверен, что общается с человеком, поскольку программа способна обратиться к пользователю-человеку и поддерживать с ним беседу, оперируя такими репликами, которые человек-собеседник сочтет естественными.

То есть эта программа способна оправдать ожидания человека-собеседника, она «социализирована», ведет диалог в рамках, принятых в данном обществе, ориентирована разработчиками на побуждение человека к выполнению определенных действий, что и является критерием ее успешности.

Впрочем, человек, участвующий в диалоге с ботом, может и осознавать, что он общается с программой. Чаще всего боты используются при покупке-продаже наркотиков бесконтактным способом.

Рассмотренные примеры свидетельствуют о том, что преступления, совершенные с использованием технологий искусственного интеллекта, отличает высокая степень анонимности, а иногда, как в случае с ботами, практически выводит личность правонарушителя из процесса преступных взаимодействий, что не может не порождать ощущения безнаказанности.

В связи с этим К. Н. Евдокимов выделяет также такую характеристику технотронной преступности, как неконтролируемость, и выдвигает научную (частную) теорию «анекселенктотичной технотронной преступности» (греч. — неконтролируемый, неуправляемый; технотронный в переводе с англ. — связанный с технотроникой, т. е. техникой с использованием электроники, оказывающей влияние на развитие общества). Иначе говоря, возникновения «преступности нового поколения, основанной на использовании IT-технологий, пришедшей на смену традиционной компьютерной преступности и вышедшей из-под контроля личности, общества и государства в силу своей социальной латентности, технической сложности и многогранности» [2, с. 39].

В то же время нельзя говорить о том, что только преступность берет на вооружение современные программно-технологические достижения. Имеется немало примеров различных программных решений с использованием искусственного интеллекта, направленных на противодействие преступности и ее профилактику.

В качестве такого примера рассмотрим ситуацию с использованием правоохранительными органами нейросетей.

Специалисты из Индии и Великобритании в августе 2017 г. опубликовали доклад, в котором описали, как работает нейронная сеть, которая распознает людей, прячущих лица. Для тренировки нейронной сети использовалась тысяча фотографий мужчин и женщин от 18 до 30 лет, лица которых были замаскированы. Вначале нейросеть обнаруживает 14 лицевых ключевых точек, которые были определены как существенные для идентификации лица. Затем обнаруженные точки образуют звездно-сетчатую структуру, по которой выполняется идентификация лица.

Однако на точность разработанного алгоритма влияют различные факторы. Например, если на анализируемом снимке присутствуют здания, точность распознавания может снизиться с 85 до 56%.

К тому же чем больше закрыто лицо, тем сложнее его идентифицировать. В ходе тестирования точность распознавания лица, закрытого шляпой, шарфом и очками, составила всего 43% [3, с. 58].

Но даже при распознавании лиц нейронные сети подвержены стереотипам. В ходе исследования выяснилось, что при анализе фотографий белых мужчин алгоритмы неверно определяли пол лишь в 0,8% случаев, а среди темнокожих женщин процент ошибок составлял в среднем около 30%. Удалось установить, что чем темнее фототип кожи — тем больше вероятность, что алгоритм допустит ошибку.

Гражданский кодекс Российской Федерации устанавливает охрану изображения гражданина [5, с. 42], а также закрытый перечень возможностей свободного использования произведения [6, с. 34], в который не входит создание выборки для нейронной сети. Также изображение человека является биометрическими персональными данными, для обработки которых в случае создания объема данных для обучения необходимо письменное согласие субъекта [7, с. 29]. Таким образом, в России затруднительно получить доступ к объему данных для обучения нейросети.

С сентября 2018 г. московская городская сеть видеонаблюдения, состоящая из 170 тыс. камер, была подключена к нейронной сети. Искусственный интеллект от компании NtechLab распознает лица прохожих и сравнивает их с базой данных МВД. За два месяца пилотного проекта нейросеть помогла поймать шестерых преступников [4, с. 46].

В марте 2018 г. Управление МВД России по Рязанской области представило первый в России мобильный биометрический комплекс (МБК), оснащенный технологией распознавания лиц. Сервер комплекса и рабочее место оператора размещаются в транспортном средстве полиции. Во время массовых мероприятий система подключается к десяти камерам, установленным на рамках металлодетекторов, и одновременно анализирует видео с каждой из них. Кроме того, МБК оснащен собственной обзорной камерой с оптическим зумом [8, с. 62].

Сообщается, что система может идентифицировать правонарушителей в режиме реального времени и отправлять на мобильные устройства сотрудников полиции уведомления с фотографией человека и краткой информацией о совершенном им правонарушении.

Биометрические персональные данные могут обрабатываться без согласия субъекта персональных данных в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, об оперативно-разыскной деятельности. Так что обработка нейронной сетью видео для идентификации скрывающихся от правосудия лиц законна (несмотря на то что она обрабатывает данные для установления личности снятого человека) [9, с. 35].

IT-технологии возможно применить и для прогнозирования преступности. Исследователи проблем использования искусственного интеллекта в криминологии В. С. Овчинский и Е. С. Ларина приводят данные Интерпола и Европола, согласно которым более чем в 70 странах мира полицейские на практике используют те или иные данные *предиктивной аналитики*, опираясь на программные средства более чем 25 корпораций-производителей [3, с. 114]. Предиктивная, или предсказательная, аналитика представляет собой совокупность методов анализа данных, направленных на прогнозирование поведения людей.

В России примером программы прогнозирования может считаться система «Искусственный интеллект» («Объединенная приборостроительная корпорация»), тестируемая с 2016 г. Ее целью является фиксация нарушений на границах России с помощью инфракрасных датчиков, сейсмосенсоров, радиолокационных устройств с целью наработки базы данных для дальнейшего компьютерного анализа информации о нарушении границ, дистанционного контроля ситуации и прогнозирования опасностей [3, с. 74–76].

Повсеместное внедрение и совершенствование информационных технологий побуждают и нашу страну принимать соответствующие правовые и управленческие решения.

Уже принята государственная программа Российской Федерации «Информационное общество (2011–2020 гг.)»; указом Президента РФ утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.; реализуются мероприятия программы «Цифровая экономика Российской Федерации». Основные направления обеспечения информационной безопасности в области государственной и общественной безопасности определены Доктриной информационной безопасности Российской Федерации, утвержденной указом Президента РФ от 5 декабря 2016 г. № 646 [10, с. 42].

В отраслевых документах обозначается значимость повышения эффективности противодействия *преступности, использующей информационные технологии,* но стратегическая задача применения информационных технологий *в прогнозировании и предупреждении* преступности не выдвигается.

В государственной программе «Обеспечение общественного порядка и противодействие преступности» предусмотрено «внедрение в служебную деятельность новых информационных технологий», однако можно предположить, что речь идет преимущественно о технологиях, направленных на фиксацию и раскрытие преступлений. В сфере использования возможностей искусственного интеллекта в противостоянии преступности и особенно в сфере профилактики наша страна не на передовых позициях.

Между тем происходящие изменения, обусловленные развитием цифровых технологий, отличаются такой характеристикой, как *стремительность*.

В подтверждение тезиса укажем, что в 2011 г. на Ганноверской выставке была изложена концепция четвертой промышленной революции («Индустрии 4.0»), которая, по мнению участников мероприятия, должна была привести к слиянию технологий и размыть границы между физической, цифровой и биологической сферами, а спустя совсем непродолжительное время под эгидой японской федерации крупного бизнеса «Кэйданрэн» были разработаны основы программы создания суперинтеллектуального общества, или «Общества 5.0».

На сегодняшний день анализ практики борьбы с преступностью в сфере высоких технологий позволяет выявить определенные недостатки в данной работе, к которым можно отнести уже отмеченное нами некоторое отставание нормативно-правовой базы, регулирующей деятельность искусственного интеллекта в правоохранительной сфере; низкий уровень взаимодействия между законодательными органами, учеными и практиками в данной области; недостаточный уровень специалистов по IT-технологиям в российских правоохранительных органах.

Таким образом, представляется целесообразным в противодействии преступности с использованием технологий искусственного интеллекта в качестве приоритетных задач выделить следующие:

1. Органам законодательной власти, используя опыт борьбы с преступностью в России, теоретические и практические разработки ученых-юристов и специалистов технических вузов, рекомендуется разрабатывать нормативно-правовые акты, направленные на повышение эффективности данной работы.

2. Повысить уровень подготовки специалистов по противодействию преступности в сфере высоких технологий. Так, например, в Алтайском государственном университете по инициативе преподавателей физико-технического факультета и Юридического института создан Региональный научно-методический центр правовой и технической защиты информации. На базе физико-технического факультета успешно функционирует программа подготовки студентов по обеспечению информационной безопасности техническими средствами. Проводится обучение студентов основам российского права по защите информации.

3. Требуется четко отработанное взаимодействие между практическими работниками и учеными, что позволит более эффективно работать над совершенствованием законотворческой и правоприменительной практики. Так, например, Управление «К» ГУВД РФ по Алтайскому краю принимает активное участие в подготовке специалистов на базе физико-технического факультета Алтайского государственного университета, а также в работе научно-практических конференций, проводимых университетом.

Библиографический список

1. Цифровая цивилизация. Россия и «электронный» мир XXI в. / С. Ю. Глазьев и др. М., 2018.

2. Reese H. Understanding the differences between AI, machine learning, and deep learning. URL: https: // www.techrepublic.com/article/understandingthedifferencesbetweenaimachine learninganddeeplearning.

3. Боровская Е. В., Давыдова Н. А. Основы искусственного интеллекта. М., 2018.

4. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М., 2018.

5. Кравцов Д. А. Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского ун-та МВД России. 2018. № 3.

6. Овчинский В. С. Мафия: новые мировые тенденции. М., 2016.

7. Овчинский В. С. Технологии будущего против криминала. М., 2017.

8. Овчинский В. С. Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. М., 2018.

9. Ларина Е. С., Овчинский В. С. Криминал будущего уже здесь. М., 2018.

10. Овчинский В. С. Криминология цифрового мира : учеб. для магистратуры. М., 2018.