Список источников

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 27.12.2020) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1).
2. Маслова О. С. Распространенные правонарушения, совершаемые несовершеннолетними // Научный журнал «NovaUm». – 2019. – № 17. URL: http://novaum.ru/public/p1136 (дата обращения: 29.01.2020).
3. Михайлова Е. Н., Михайлов И. В. Отдельные вопросы взыскания алиментных обязательств в Российской Федерации // Ученые записки Орловского государственного университета. Серия: Гуманитарные и социальные науки. – 2014. – № 1. – С. 326–328.

УДК 004.8

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ. ВОЗМОЖНОСТИ И ПРОБЛЕМЫ

А. В. Рыбак, *профессор кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России, кандидат технических наук, доцент*

В статье рассматриваются возможности искусственного интеллекта (далее ИИ), а также проблемные вопросы его применения правоохранительными органами; анализируется международный опыт применения технологии ИИ в борьбе с преступностью.

Ключевые слова: искусственный интеллект, информационное пространство, робототехника, борьба с преступностью, этичность применения ИИ.

THE USE OF ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT. OPPORTUNITIES AND PROBLEMS

A. V. Rybak, *Professor of the Department of Information and Technical Support of the Ministry of Internal Affairs of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, Candidate of Technical Sciences, Associate Professor*

The article discusses the possibilities of artificial intelligence (hereinafter referred to as AI), as well as problematic issues of its use by law enforcement agencies; An international experience of applying technology in AI in the fight against crime is analyzed.

Keywords: artificial intelligence, information space, robotics, control of crime, ethiculture of use of AI.

Ключевым фактором, определяющим сегодня развитие технологий ИИ, считается темп роста вычислительной мощности компьютеров, так как принципы работы человеческой психики по-прежнему остаются неясными, по крайней мере, на доступном для моделирования уровне детализации. Но рост производительности современных компьютеров в сочетании с повышением качества алгоритмов делает возможным применение систем ИИ практически во всех видах человеческой деятельности. Преимущества этой технологии признаны и уже являются частью жизни современного общества. Безусловно, достижения в области ИИ создают новые беспрецедентные возможности для правоохранительной деятельности, прежде всего, в области:

– сбора информации, хранения и обработки информации;
– создания и применения аналитических и прогнозных моделей;
– осуществления цифровых расследований;
– обеспечения коммуникаций и взаимодействия.

Результаты внедрения в правоохранительную область элементов систем ИИ активно способствуют значительному повышению качества аналитики и прогнозирования криминальной деятельности; решению задач идентификации фигурантов или транспортных средств, связанных с уголовными делами и другими нарушениями; созданию эффективных комплексов противодействия поведенческой агрессии в виде манипулирования контентными потоками, загрязнением информационного пространства фейками и т. п. Но при всех возможностях ИИ он остается лишь инструментарием, который точно также активно используется преступными элементами в целях подготовки, организации и совершения преступлений.

Правоохранительные органы втянуты в бесконечное соревнование по эффективности использования ИИ с криминалом. При этом следует отметить, что деятельность в этой области правоохранительных органов затрагивает широкий диапазон проблем экономического, юридического, этического, политического и даже демографического характера.

На прошедшей в Вене 23–24 сентября 2021 г. Ежегодной встрече полицейских экспертов ОБСЕ были обсуждены и сформулированы два, в значительной степени не пересекающихся направления развития ИИ и робототехники.

Первое носит поисковый, исследовательский характер и на сегодняшний момент не может похвастаться сколько-нибудь значимыми практическими результатами. Речь идёт о так называемом «сильном» (универсальном) ИИ, в полном объеме способном заменить человека.

Другое направление развивается ошеломительными темпами. Это – так называемый, *«слабый» ИИ*, и базирующиеся на нем полностью автоматизированные робототехнические системы. В рамках этого направления ИИ не стремится заменить человека по всему диапазону его способностей и возможностей. Он решает конкретные задачи, связанные либо с распознаванием, либо с установлением взаимосвязей на основе матричных и статистических методов. Другими словами, «слабый» ИИ может быть уподоблен механическим вычислительным машинам, типа арифмометра, в том же смысле, в котором реактивный самолет может быть уподоблен воздушным шарам. ИИ и робототехника такого рода не стремятся полностью заменить человека. Их задача научиться выполнять конкретные операции на порядки лучше, чем человек [2].

Современная преступность активно берет на вооружение технологии так называемого «слабого» искусственного интеллекта. В основном на сегодняшний день это происходит по следующим направлениям:

– первое – цифровые нападения, когда «слабый» ИИ используется высокотехнологичным криминалом при совершении сложных киберпреступлений. Они включают в себя как элементарный автоматизированный фишинг, так и разработку и применение многофункциональных платформенных вредоносных программ. Такие программы нацелены не только на проникновение в защищенные сети и изъятие из корпоративных сетей информации, но и на разрушение или перехват управления физическими структурами, управляемыми корпоративным или федеральным ИИ;

– второе – экономические нападения, когда продвинутые преступники используют ИИ и боты для атак на финансовую инфраструктуру банков, инвестиционных компаний, финансовых институтов. В настоящее время уже более 80 % объёма транзакций на рынках капитала осуществляется в рамках полностью автоматической торговли на базе электронных платформ. Преступники стремятся нарушить целостность этих платформ и либо украсть деньги, либо осуществлять манипуляцию рынками путем внесения изменений в программы;

– третье – политические нападения. В современном мире это отнюдь не покушения или убийства политических деятелей. Это – манипулирование коллективным поведением на основе создания эхо-интернет камер, потоков фейковых новостей, запуска фальсифицированных видеороликов и фотографий, и в целом дискредитация любой информации в сети, особенно той, которая могла быть использована в качестве доказательств, предъявляемых в суде;

– четвертое – физические нападения. Если раньше преступники нападали на человека, используя физическую силу или оружие, то сегодня уже зарегистрированы нападения с использованием интернета вещей. В Соединенных Штатах зафиксировано несколько случаев взятия под контроль при помощи вредоносного софта имплантатов – физических устройств, вживленных в человеческое тело. Также для физических нападений, особенно террористами, используются дроны и беспилотные автомобили.

Всерьез обсуждение использования ИИ и робототехники в правоохранительной и правоприменительной практике началось с конца нулевых годов. Практическое использование – с середины десятых. Ряд стран, прежде всего Соединенные Штаты, Великобритания, Китай, Япония, Южная Корея, Израиль не только создали в структуре правоохранительных органов Центры адаптации ИИ и робототехники к повседневной работе правоохранителей, но и широко осуществляют контакты с университетами и бизнесом как для создания полицейского софта с элементами ИИ, так и для обучения сотрудников правоохранительных органов ИИ и робототехнике. При этом в подавляющем большинстве случаев правоохранительные органы не используют какой-то уникальный, специально разработанный полицейский софт на базе ИИ, а адаптируют уже имеющиеся военные, разведывательные и бизнесовые разработки под нужды полиции.

Среди технологий, которые уже вошли в повседневную жизнь сотрудников полиции ряда зарубежных стран, можно выделить в первую очередь:

– алгоритмы ИИ, нацеленные на распознавание подозрительных или украденных транспортных средств;

– программы машинного распознавания образов, способные, в том числе, в толпе выделять и распознавать в толпе лиц, находящихся в розыске, либо подозреваемых полицией в совершении преступлений (не только по полному, но и частичному изображению);

– программы контент- и латентно-семантического анализа, позволяющие на основе содержательного анализа письменных или аудио текстов определять психологическое состояние их автора, а также скрытые смыслы, заложенные в сообщения;

– платформенное решение на основе ИИ, позволяющее собирать, хранить и проводить интеллектуальный анализ информации с целью превентивного выявления слабых сигналов, указывающих на всплеск уличной преступности, неконтролируемые волнения, беспорядки, выступления и акты вандализма;

– биометрические методы, позволяющие проводить идентификацию граждан, распознавать преступников и обнаруживать подозрительное поведение по микромоторике мускулов лица и движения тела и т. п.;

– функционирующий на основе ИИ полностью автоматизированный комплекс поиска и анализа контента детской порнографии в сети;

– интеллектуальные программы на базе ИИ, позволяющие распознавать аномалии при проведении финансовых транзакций, при заключении хозяйственных договоров и т. п., способствующие раскрытию финансовых преступлений;

– специализированные программы распознавания необычных колебаний цен на активы, указывающие на инсайдерскую торговлю или криминальное поведение на финансовых рынках;

– боты, используемые правоохранительными органами для первичных информационных контактов с гражданами и организациями [1].

При этом следует помнить, что использование ИИ правоохранительными органами затрагивает широкий диапазон проблем экономического, юридического, этического, политического и даже демографического характера. В этой связи в настоящий момент важнейшей задачей государства становится поиск реально реализуемых гарантий, которые обеспечивают для общества уверенность в этичном использовании правоохранительными органами систем ИИ.

Проблема в том, что сам по себе термин «этичный» является многогранным, сложным и в значительной степени зависит от культурного контекста. Более того, он зависит не только от культурных традиций, но и от повседневности, от контекста конкретной ситуации. То, что может быть этичным в одной организации, вполне может оказаться неэтичным – в другой. Пожалуй, центральный вопрос, который российское общество должно разрешить сообразно собственным культурным традициям, стереотипам поведения и нормам жизни, является вопрос о полноте цифрового досье и масштабах наблюдения через видеокамеры и данных интернета вещей.

Не менее важным вопросом внедрения ИИ является различие в этических рекомендациях применения ИИ в правоохранительных органах и судебной системе. Во всех недавно принятых международных документах по вопросам использования ИИ в полицейской и судебной деятельности эти рекомендации и ограничения одинаковы как для полиции, так и для судей. Но, на самом деле, здесь возникают серьезные противоречия. Например, в применении принципа прозрачности баз данных для судов и полиции. Если транспарентность судебных баз данных не вызывает сомнения, то относительно полицейских, особенно полученных в ходе оперативно – розыскных мероприятий, имеются серьезные ограничения, связанные с их секретностью и возможными негативными последствиями как для источников информации, так и для потерпевших, подозреваемых и обвиняемых.

Следует обратить внимание на управленческие риски применения ИИ правоохранительными органами. Прежде всего внедрение ИИ в правоохранительную деятельность в совокупности с другими современными технологиями могут привести к изменению численности правоохранительных органов. Речь здесь может идти не о сокращении, как это происходит, например, в банковских

структурах России, а об увеличении количества специалистов, работающих в этой сфере правоохранительной деятельности. Например, внедрение ИИ в систему видеонаблюдения и расширение этой системы безусловно увеличит объём поступающей информации о противоправных проявлениях, которым надо давать уголовно-процессуальную оценку. А это означает, что автоматически потребуется увеличить штат оперативных работников, дознавателей, следователей, экспертов. Уже сейчас требуется подготовка большого числа специалистов новой профессии – аналитиков Больших Данных. Поэтому внедрение ИИ вызовет необходимость не сокращения, а увеличения штатной численности сотрудников МВД России.

Безусловно – это далеко не полный перечень проблемных вопросов, которые будут возникать по мере внедрения ИИ в правоохранительную деятельность. Но чтобы минимизировать риски и угрозы, создаваемые использованием ИИ в правоохранительной сфере, целесообразно разрабатывать соответствующие законы и внутренние нормативные акты на основе международных этических кодексов и рекомендаций.

Список источников

1. Агеев В.В Большие данные и искусственный интеллект на службе полиции / Сб. стат. Международной научно-практической конференции «Стратегическое развитие системы МВД России: Состояние, тенденции, перспективы»: [сайт]. URL: https://www.elibrary.ru/item.asp?id=41722065 (дата обращения 23.07.2021).
2. Овчинский.В.С. Искусственный интеллект для полиции: [сайт]. URL: https://izborsk-club/ru/17797 (дата обращения 26.07.2021).

УДК: 343.98

ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ОБЪЕКТОВ НАТУРНЫХ КОЛЛЕКЦИЙ В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

***И. В. Рыжков**, преподаватель кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности Волгоградской академии МВД России*

Статья посвящена проблеме легитимности использования при производстве экспертных исследований натурных объектов, являющихся частью справочно-информационных фондов и дислоцирующихся