Алексей Александрович Бессонов,
доктор юридических наук, доцент,
ректор
Московская академия Следственного комитета
Российской Федерации
E-mail: bestallv@mail.ru

Искусственный интеллект как орудие преступлений и средство их расследования

Аннотация

Стремительно распространяющиеся сегодня преступления, совершаемые с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, обусловливают необходимость изучения их криминалистических особенностей и формирования криминалистических учетов цифровых следов. Одновременно с этим требуется проведение исследований о применимости технологий искусственного интеллекта в деятельности по расследованию преступлений, поскольку они имеют не только преимущества, но и ограничения. В связи с этим важнейшим направлением государственной научно-технической политики в сфере криминалистического обеспечения правоохранительной деятельности должно стать изучение роли в ней современных технологий искусственного интеллекта.

Ключевые слова и словосочетания: *искусственный интеллект; расследование преступлений; цифровая криминалистическая модель преступлений.*

Созданный еще в прошлом веке образ восстания машин против человечества вновь будоражит умы людей. Пресловутые нейронные сети проникают буквально во все сферы нашей жизни: смартфоны, бытовые приборы, автомобили, умные дома, города и органы государственного управления. Использование искусственного интеллекта с целью посягательства на безопасность отдельных государств и народов начинают сравнивать с последствиями применения ядерного оружия. Весь нюанс в том, что у технологий искусственного интеллекта, как и у ядерного синтеза, имеются две стороны медали – несомненно, прогрессивная и одновременно разрушительная.

На круглом столе «Военные конфликты будущего» в рамках научно-деловой программы Международного военно-технического форума «АРМИЯ-2022» было сакцентировано внимание на серьезном влиянии технологии искусственного интеллекта на развитие подходов к применению оружия в ходе современных и будущих вооруженных конфликтов [10, с. 81–82].

Агенством Европейского Союза по кибербезопасности (ENISA) злоупотребление технологиями искусственного интеллекта включено в топ-10 ключевых угроз кибербезопасности [12], которые могут возникнуть к 2030 г., что является вполне обоснованным, поскольку цифровые технологии становятся распространенным орудием совершения преступлений. При этом искусственный интеллект составляет наиболее прогрессивный инструментарий этих технологий, что, конечно же, не осталось вне поля зрения криминалитета. Ярким подтверждением тому выступают выявленные специалистами факты использования популярной сегодня нейронной сети ChatGPT для написания вредоносного компьютерного кода («компьютерных вирусов») [8].

Согласно статистическим сведениям МВД России, на протяжении последних трех лет ежегодно регистрируется свыше полумиллиона криминальных деяний, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Их удельный вес в общей преступности составляет не менее четверти, а свыше 70 % остаются нераскрытыми. Например, за 2022 г. зарегистрировано 522 065 таких преступлений, что составило 27 % от общей преступности, не раскрыт 71 % из них [9]. Если экстраполировать количество обвиняемых по оконченным производством уголовным делам о таких деяниях на нераскрытые преступления, то получится, что за последние три года уголовной ответственности избежали более 1,5 млн совершивших их лиц. Представляется, что это достаточно существенный показатель, требующий самого глубокого осмысления.

Одновременно технологии искусственного интеллекта рассматриваются в качестве средства расследования преступлений, в первую очередь, с их же помощью и совершенных. Все активнее становится дискурс относительно возможностей и границ внедрения этих технологий в уголовное судопроизводство. Звучат разные точки зрения, среди которых самые антагонистические – человек в сфере судопроизводства может быть практически полностью заменен искусственным интеллектом и категорическое нет.

В связи с этим уместно упомянуть научные изыскания, предшествовавшие принятию на 31-м пленарном заседании Европейской

комиссии по эффективности правосудия, состоявшемся 3–4 декабря 2018 г. в Страсбурге, Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Согласно данным изысканиям, на настоящий момент и в обозримом будущем не стоит торопиться с заменой судьи искусственным интеллектом в части оценки доказательств при рассмотрении дел и вынесении по ним итоговых решений[1]. Этот вывод хорошо дополняет мнение председателя Совета судей Российской Федерации В. В. Момотова, который по отношению к судье как правоприменителю, не отрицая необходимости использования в его работе алгоритмов искусственного интеллекта, отметил, что «говорить о замене судьи искусственным интеллектом как минимум преждевременно, а скорее всего невозможно» [5]. Также он указывает на то, что процесс принятия судебных решений включает в себя: внутреннее убеждение, сформировавшееся под воздействием индивидуальных особенностей рассматриваемого дела; учет ряда оценочных и ценностных критериев и принципов, закрепленных в законе; применение аналогии закона и права при наличии законодательных пробелов. Все перечисленное, по его мнению, пока не под силу искусственному интеллекту [5]. На наш взгляд, сказанное справедливо относится и к досудебной стадии производства, где ключевым правоприменителем выступают следователь и дознаватель.

На мировом уровне предлагается относить к сферам высокого риска использование систем искусственного интеллекта в деятельности правоохранительных органов по профилированию физических лиц в контексте выявления и расследования преступных деяний (прил. 3, ст. 6 п. «f») и анализа больших данных с целью выявления неизвестных закономерностей или обнаружения скрытых взаимосвязей в них при расследовании преступлений против личности (прил. 3, ст. 6 п. «g») [13].

Сказанное хорошо дополняет выраженный в отечественной Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники[2] принцип, согласно которому законодательно следует допускать лишь точечное

[1] Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях: принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3–4 декабря 2018 г.) // СПС КонсультантПлюс (дата обращения: 21.02.2023).

[2] Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : распоряжение Правительства Рос. Федерации от 19 авг. 2020 г. № 2129-р // СПС КонсультантПлюс (дата обращения: 21.02.2023).

«делегирование» определенных решений системам искусственного интеллекта, где это объективно целесообразно и не несет угрозы основополагающим правам и свободам человека, обороне страны и безопасности государства.

В связи с этим следует согласиться с мнением профессора Ю. В. Гаврилина об обусловленности необходимости формирования государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) цифровой трансформацией механизма большинства преступлений и совершенствованием в этой связи криминалистической техники [6, с. 100].

Таким образом, сквозь призму актуальности проблемы активного внедрения в преступную деятельность цифровых технологий, основу которых сегодня составляет в первую очередь искусственный интеллект, представляется возможным определить следующие важные для криминалистической теории и практики направления:

1) изучение криминалистических особенностей преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, с объединением для этого усилий ученых-криминалистов и специалистов в сфере таких технологий;

2) исследования в сфере криминалистической техники, предназначенной для поиска, фиксации и изъятия цифровых следов;

3) научно-исследовательские работы о применимости цифровых технологий, прежде всего искусственного интеллекта, в деятельности по выявлению, раскрытию, расследованию и предупреждению преступлений.

При этом отправной точкой первых двух направлений должны стать цифровые криминалистические модели рассматриваемого вида преступлений, что мы уже ранее предлагали в ходе 61-х криминалистических чтений [3]. Обратим внимание на то, что такие модели будут полезны и в расследовании любых других видов преступных деяний. Например, проведенное нами исследование об использовании искусственного интеллекта в расследовании серийных преступлений, совершаемых из сексуальных побуждений, позволило предложить технологии построения портрета серийного преступника, выявления в массиве нераскрытых деяний тех, которые наиболее вероятно составляют серию, и приоритезацию подозреваемого из числа лиц, ранее привлеченных к уголовной ответственности [1; 2].

Следующее, на чем следует сакцентировать внимание, – это то, что в современной медиасфере значительный сегмент занимают

фейковые фотографии, аудио- и видеозаписи, нередко влекущие повышенный общественный резонанс, а в последнее время все чаще на уровне угрозы национальной безопасности. Нужно отметить, что уже несколько лет как зафиксировано превышение количества недостоверных информационных публикаций над числом достоверных [4, с. 165–166]. Согласно мнению тайваньского предпринимателя в области разработок программного обеспечения и искусственного интеллекта Ли Кайфу, сегодня «мир стоит на краю пропасти, с которого мы полетим в пучину неконтролируемой лжи», по причине всепоглощающего распространения дипфейков, созданных с помощью нейронных сетей [8].

Многие действия, связанные с созданием и распространением такой информации сегодня в правовой системе нашего государства, влекут наступление уголовной ответственности. К числу таких деяний, например, относятся: публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1 УК РФ); публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2 УК РФ); публичное распространение заведомо ложной информации об использовании Вооруженных сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий (ст. 207.3 УК РФ). К тому же никем уже не оспаривается тот факт, что фейковая информация в сегодняшнем мире является одним из средств ведения гибридных войн, посягающих на безопасность суверенных государств.

Для изготовления такой фейковой аудиовизуальной информации преступники активно используют новейшие цифровые технологии, в том числе искусственный интеллект, среди которых особо следует выделить нейронные сети. В частности, появились методы получения видеозаписей на основе одной единственной фотографии, генерации изображения людей, которых в реальности не существует, добавления небольшого шума в фейковые объекты, препятствующие их анализу, и т. д. [4, с. 174]. На наш взгляд, близок тот день, когда при производстве по уголовным делам возникнет вопрос проверки фото-, аудио- и видеодоказательств на предмет относимости к дипфейкам. Поэтому этот вопрос следует изучать уже сейчас, чтобы разработать эффективные меры профилактики и своевременного выявления и пресечения таких случаев.

Назрела необходимость формирования криминалистических учетов цифровых следов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или

в сфере компьютерной информации – IP-адресов, адресов электронной почты, индивидуальных особенностей написания компьютерного кода и т. п. Здесь нужны исследования относительно того, какие именно следы должны составить содержание этих учетов и какие технологии работы с ними будут наиболее эффективны.

Следовательно, также требует поддержки и развития предложение о формировании, ведении и использовании федерального банка оперативно-розыскных данных, содержащих сведения о лицах, предметах и фактах, представляющих оперативный интерес по такого рода преступным деяниям [7, с. 90].

Что касается третьего направления, то важно учитывать не только положительный эффект от внедрения цифровых технологий на досудебной стадии уголовного судопроизводства, но и риски, обусловленные ограничениями этих же технологий.

В первую очередь обозначим преимущества технологий искусственного интеллекта и систем, в которые они интегрированы:

– возможность обработки больших объемов информации (big data);

– высокая вычислительная скорость в совокупности с быстродействием современных компьютеров;

– способность выявления как явных, так и неочевидных закономерностей в данных, представляющих различные явления окружающего мира [11, с. 27–37; 14, с. 1–34].

Укажем и основные их ограничения, имеющие место в настоящий момент:

– отсутствие полной прозрачности процесса получения конкретных выводов;

– невозможность обеспечения надлежащего уровня безопасности, однозначно исключающего возможность вмешательства в работу технологий искусственного интеллекта кого бы то ни было;

– большое количество правоприменительных неординарных ситуаций, которые невозможно заранее предусмотреть и описать математическими алгоритмами;

– определенная доля субъективности и неполноты, детерминированные участием человека в разработке данных технологий и эмпирическим материалом, использующимся для их обучения, который также сформирован человеком, и нередко не исключающим той или иной степени тенденциозности.

Проводимое нами уже на протяжении нескольких лет исследование о применимости искусственного интеллекта в деятельности по расследованию преступлений позволяет сделать ряд следующих актуальных на настоящий момент выводов:

– во-первых, возможно и необходимо использовать методы математической статистики и искусственного интеллекта в криминалистическом изучении преступлений в научных и практических целях в качестве инструмента получения новых знаний и для их расследования;

– во-вторых, системы, имеющие своим базисом искусственный интеллект, в уголовном судопроизводстве при расследовании криминальных деяний следует рассматривать исключительно как комплексы поддержки принятия решений и инструмент собирания доказательственной информации при сохранении ключевой роли следователя и дознавателя;

– в-третьих, важнейшим направлением государственной научно-технической политики в сфере криминалистического обеспечения правоохранительной деятельности должно стать изучение роли в ней именно современных технологий искусственного интеллекта;

– в-четвертых, реалии сегодняшнего дня указывают на то, что значение изучения использования искусственного интеллекта в преступной деятельности и ее раскрытии, расследовании и предупреждении выходит за рамки государственной политики противодействия преступности, поднимаясь на уровень обеспечения национальной безопасности не только от внутренних, но и внешних угроз.

Список литературы:

1. *Бессонов А. А.* Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений) // Вестник Университета имени О. Е. Кутафина (МГЮА). 2021. № 2.

2. *Бессонов А. А.* Перспективы использования искусственного интеллекта в раскрытии серийных преступлений // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации : сб. науч. ст. по материалам Междунар. науч.-практ. конф. «62-е криминалистические чтения» / под ред. Ю. В. Гаврилина, Ю. В. Шпагиной. М., 2021.

3. *Бессонов А. А.* Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13).

4. *Бирин Д. А.* Проблемы исследования фейковой информации // Современное состояние и перспективы развития технико-криминалистического и экспертного сопровождения расследования преступлений, сопряженных с использованием средств вычисли-

тельной техники. Цифровые технологии современной криминалистики. М., 2022.

5. Выступление председателя Совета судей РФ В. В. Момотова на пленарном заседании VI Московского юридического форума по теме «Судебная власть в условиях современных цифровых технологий» (МГЮА(У), 4 апреля 2019 г.) // Совет судей Российской Федерации : сайт. URL: http://www.ssrf.ru/news/vystuplieniia-intierv-iu-publikatsii/32548 (дата обращения: 25.02.2023).

6. *Гаврилин Ю. В.* О понятии и содержании государственной научно-технической политики в области криминалистического обеспечения правоохранительной деятельности (криминалистической политики) // Труды Академии управления МВД России. 2022. № 2 (62).

7. *Иванов П. И.* Оперативно-розыскное противодействие киберпреступлениям (проблемы и пути их решения) // Труды Академии управления МВД России. 2022. № 4 (64).

8. Искусственный мир победил: информация, сфабрикованная нейросетями, неотличима от правдивой // Московский комсомолец : сайт. URL: https://www.mk.ru/science/2023/02/05/iskusstvennyy-mir-pobedil-informaciya-sfabrikovannaya-neyrosetyami-neotlichima-ot-pravdivoy.html?ysclid=lewgo2238m909097103 (дата обращения: 25.02.2023).

9. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года // М-во внутренних дел Рос. Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 15.02.2023).

10. *Смоловый А. В.* Военные конфликты будущего: современный взгляд // Вестник Академии военных наук. 2022. № 3 (80).

11. *Шолле Ф.* Глубокое обучение на R. СПб., 2018.

12. Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! // enisa. European Union Agency for Cybersecurity : сайт. URL: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 (дата обращения: 21.02.2023).

13. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts // EUR-Lex : сайт. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (дата обращения: 25.02.2023).

14. *Russell S., Norvig P.* Artificial Intelligence: A Modern Approach, 4th US ed. // aima : сайт. URL: https://aima.cs.berkeley.edu/ (дата обращения: 26.02.2023).