

Статья посвящена значимости успешного выявления, раскрытия и расследования правоохрнительными органами при помощи компьютерной информации преступлений любого вида. Отмечено, что в условиях современности возникла стройная система научно-технических средств, приспособленных и специально созданных для раскрытия, расследования и предупреждения преступных посягательств. Не менее интересным является вопрос о перспективах развития и совершенствования данного направления, изучение опыта зарубежных государств.

В процессе исследования показаны значения терминов: искусственный интеллект, цифровые следы преступлений. Рассмотрены и проанализированы мнения ученых, изучающих специфику применения представленных феноменов, а также российскую и зарубежную практику. Приведен опыт крупных IT-компаний, занимающихся развитием направления цифровизации.

Предложено разработать на основе зарубежных информационных систем и адаптировать под российскую действительность специализированные базы данных, содержание которых, помимо основной стандартизированной информации о гражданине, включало бы информацию об IP, MAC-адресе, ID и ник-неймах пользователя в социальных сетях за весь период их использования, адреса электронной почты, доменные адреса и т.п.

Ключевые слова: базы данных; выявление преступлений; информационно-телекоммуникационные технологии; искусственный интеллект; компьютерные исследования; компьютерные технологии; правоохрнительные органы; раскрытие преступлений; расследование преступлений; цифровизация; цифровые следы преступлений; IT-индустрия; IT-технологии.

Денис Валентинович Теткин, канд. юрид. наук, подполковник полиции, доцент, кафедра уголовного процесса, Рязанский филиал ФГКОУ ФО «Московский университет МВД России имени В. Я. Кикотя», Рязань, Россия; tyotkinden@mail.ru

Ирина Сергеевна Воронина, младший лейтенант полиции, секретарь научного общества курсантов и слушателей, Рязанский филиал «ФГКОУ ФО Московского университета МВД России имени В. Я. Кикотя», Рязань, Россия; irinasvoronina@yandex.ru

СОВРЕМЕННАЯ ПЕРСПЕКТИВА ПРИМЕНЕНИЯ НОВЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ПРИ ВЫЯВЛЕНИИ, РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Введение

С уверенностью можно отметить, что данные компьютерных исследований в настоящее время представляют собой хороший источник информации, существенно оказывающий помощь сотрудникам подразделе-

ний следствия, дознания, аппарата оперативных служб органов внутренних дел в процессе выявления, раскрытия и расследования преступлений. Результаты таких исследований могут способствовать не только точному изобличению виновных в преступлении лиц, но и выбрать направление их работы в борьбе с преступностью. В МВД РФ на сегодняшний день существует немало сервисов, баз данных, которые фактически по одному электронному запросу предоставляют нужный объем необходимых сведений, что заметно ускоряет работу правоохранителей. Однако деятельность по улучшению и разработке новых программ компьютерно-информационного толка не прекращается, и это правильно, учитывая ежедневное развитие информационно-телекоммуникационных технологий в XXI веке.

Основная часть

В сегодняшней действительности ни для кого не секрет, что высокие технологии последние несколько десятков лет развиваются очень стремительно. Ежегодно IT-компании представляют вниманию общественности новейшие разработки компьютерных специалистов и инженеров-конструкторов. Сенсорные экраны, система бесконтактной оплаты, сканеры отпечатка пальца и лица, высокоскоростные сети четвертого и пятого поколения (4G и 5G); голосовые ассистенты, встроенные в смартфон, распознающие голос владельца, технологии виртуальной реальности и многое другое – все было изобретено сравнительно недавно. Огромное количество информации ежедневно поступает в базы данных системы МВД России, и еще больший информационный объем уже содержится в них.

Правоохранительные органы уже имеют в своем арсенале массив биометрических данных о правонарушителях, основой которого являются дактилоскопические карты с отпечатками пальцев рук, а также фотографии в различных ракурсах. Базы МВД России обладают данными о зарегистрированных в государстве гражданах. Информация о фамилии, имени, отчестве, месте регистрации, дате рождения, фотографии гражданина, составе семьи, отношении к воинской обязанности – все эти данные можно получить только лишь из одного документа. Все чаще в научно-публицистической литературе встречаются идеи о применении в деятельности правоохранительных органов такого достижения мировой компьютерной индустрии, как искусственный интеллект.

Что же из себя представляет искусственный интеллект, когда он появился, в чем его сущность, какая у него функция – и это только некоторые вопросы, которые интересуют людей, сталкивающихся с термином «искусственный интеллект» на просторах сети Интернет.

Так, термин «искусственный интеллект» (*англ.* – artificial intelligence) был предложен в 1956 г. в Соединенных Штатах Америки в Дартмутском колледже. Основная цель технологии искусственного интеллекта была выдвинута в тезисе: «Каждый аспект обучения или любая другая особенность интеллекта могут быть в принципе так точно описаны, что машина сможет симитировать их» [1, с. 753 – 766]. Главная сформулированная мысль – машины получают данные, на основе которых они обучаются, и в дальнейшем, на основе имеющегося у них накопленного опыта, про-

граммно-системных знаний, могут принимать самостоятельные решения. Такая база данных позволила ученым создать мощные нейрокомпьютеры и программы, с помощью которых машина распознает изображения, образы, выявляет и переводит текст на разные языки, обнаруживает спам и мошенничество, создает чат-боты и многое др.

Далее попытаемся поразмышлять о современной перспективе применения технологии искусственного интеллекта правоохранными органами для выявления, раскрытия и расследования преступлений.

В крупных городах нашей страны активно и вполне успешно реализуется автоматизированная комплексная программа «Безопасный город», сутью которой является накопление, систематизация, мониторинг, прогнозирование, оповещение и другие широкие возможности для анализа материалов, поступающих с диспетчерских служб различных направлений, а также видеокамер, установленных по городу. На практике мы видим, что компьютерные технологии в части видеонаблюдения уже активно способствуют пресечению нарушений правовых норм, связанных с правилами дорожного движения и не только. Компьютеры анализируют данные, получаемые с камер видеонаблюдения для определения нарушений скоростного режима: данные об автомобиле, его государственном номере, марке, модели, помогают найти владельца транспортного средства, определить, на сколько реальная скорость движения отличается от максимально разрешенной. На основе этих данных компьютеры определяют пункт, часть, и статью законодательства, и на ее основе избирают санкционную меру – административный штраф за превышение скорости. И это только одно из направлений программы «Безопасный город».

При создании представленных выше информационно-телекоммуникационных систем у сотрудников правоохранительных органов появится больше возможностей для детального исследования информации о цифровых следах преступлений. Однако важно понимать, что в юридическом смысле представляет собой термин «цифровой след преступления». В нашем понимании, это, прежде всего, уникальное закономерное отображение в современном цифровом информационном пространстве (Интернет) данных, которые остаются при использовании в преступных целях информационно-телекоммуникационных технологий, проявляемых в пассивной форме путем непредумышленно оставления IP-адреса устройства или истории посещений.

Не менее интересна и точка зрения, которая в науке сформировала понимание цифрового следа как криминалистически значимой компьютерной информации о событиях или действиях, отраженной в материальной среде, в процессе ее возникновения, обработки, хранения и передачи [2, с. 6 – 9]. Цифровой след в понимании авторов [3] – материальный невидимый след, в механизме образования которого лежат электромагнитные взаимодействия двух и более материальных объектов, сведения и данные, представленные в форме электрических сигналов, независимо от средств их обработки, передачи и хранения.

К примерам цифровых следов преступления следует отнести сведения о банковских картах, электронных кошельках и платежных системах, аобо-

ментских номерах и SIM-картах мобильной связи, IMEI-номерах сотовых телефонов и др.

На сегодняшний день можно уверенно сказать, что правоохранительные органы Российской Федерации располагают огромными объемами информации, собранными в различных форматах и из самых различных источников. Век новейших компьютерных технологий оказывает свою положительную динамику на развитие и совершенствование деятельности правоохранительных органов. Появляются новые технические средства расследования преступлений, обнаружения и собирания доказательств. В зарубежной практике также имеется ряд положительных примеров, связанных с использованием в деятельности правоохранительных органов искусственного интеллекта. Успешная работа компьютерных программ зафиксирована в США, например, программа компании DOIL COGNITIVE COMPUTING применяется правоохранительными органами США для распознавания по фотографиям и видеозаписям людей, осуществивших пластические операции, и выдачи вариантов их первоначальной внешности. Безусловно, такая программа заслуживает внимания, поскольку практике известны случаи, когда после совершенного преступления злоумышленники изменяли свою внешность и могли без труда скрыться от полиции, не говоря уже о побеге из страны. В результате программа успешно распознала по фотографиям разыскиваемых лиц факт пластической операции в 97 % случаев, в видеоматериалах – 90 %. В более чем 80 % случаев успешного распознавания программа позволяла восстановить первоначальную внешность [5].

Нельзя не рассмотреть опыт крупных IT-компаний, занимающихся развитием направления цифровизации. Так, китайская компания Hikvision является крупнейшим производителем камер безопасности. Компания сообщила, что новые камеры смогут лучше сканировать номерные знаки на автомобилях, запускать распознавание лиц для поиска потенциальных преступников или пропавших без вести людей и автоматически обнаруживать подозрительные аномалии, такие как бесхозные сумки в переполненных местах [4, с. 108].

В настоящее время американская компания PredPol использует большие объемы данных и машинное обучение, чтобы предупредить возможные преступления, а также определить, когда и где произойдет преступление. Система обнаружит, есть ли какие-либо подозрительные изменения в поведении или необычных движениях, действиях. Например, если человек ходит туда и обратно в определенном районе снова и снова, то это считается, что он может быть карманником или изучать условия для будущего преступления. В связи с чем он будет отслеживаться системой в дальнейшем [4].

Алгоритм деятельности указанных систем основан на наблюдении и выявлении определенных закономерностей, в соответствии с которыми определенные типы преступлений, как правило, группируются во времени и пространстве. Используя имеющиеся данные и наблюдая, где были совершены последние преступления, они утверждают, что смогут определить, где будущее преступление, вероятнее всего, произойдет. Например,

серия краж в одном районе может коррелировать с большим числом краж в близлежащих районах в скором будущем [4].

Очевидно, что имеется перспектива для глобального скачка в вопросе обеспечения национальной безопасности правоохранными органами. Современные преступления, способы их сокрытия, изощренность злоумышленников побуждают правоохранные органы к соответствующему развитию, и это верное направление. По оценке Университета ФБР в Квонтико, в настоящее время правоохранные органы четырех стран мира уже обладают платформами интеллектуального анализа данных различного рода: фото и видеоматериалы, образцы подчёрка, документы, биометрические данные и т.д. Важно отметить, что университетом был подготовлен определенный рейтинг, отражающий практичность применения технологий искусственного интеллекта. Системная оценка была представлена миру следующим образом:

- первое место в рейтинге – США, полицейские управления 16 мегаполисов обладают и активно используют мощь искусственного интеллекта;
- второе место – Великобритания, новейшие технологии в полицейских отделах применяются в трех мегаполисах;
- третья позиция – полиция Иерусалима в Израиле;
- четвертая – полиция Германии, преимущественно в Берлине и Гамбурге.

Следует отметить, что в 2022 г. Турция разработала и запустила Asena – программу искусственного интеллекта, способную выявлять наркоторговцев, которая а 40 % случаев показала свою эффективность. Учитывая, что наркотические вещества являются одной из самых больших угроз для государства, это хороший результат.

Заключение

Представлена возможность сделать следующий вывод: развитие технологий искусственного интеллекта в порядке расследования преступлений в России – перспективное направление, которым в настоящее время занимаются ведущие IT-специалисты. Что касается непосредственно Министерства внутренних дел Российской Федерации, то обзором и расширением информационного функционала занимается Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации – самостоятельное структурное подразделение. При этом указом Президента РФ от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» закреплено создание структурного подразделения в системе МВД РФ, осуществляющего функции по обеспечению информационной безопасности, которое впоследствии получило название Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий.

Таким образом, исследовав подробно методы работы вышеуказанных информационных систем, акцентируем внимание на необходимости использования представленных информационно-коммуникационных техно-

логий для разработки и адаптирования под российскую действительность подобных специализированных баз данных, содержание которых, помимо основной стандартизированной информации о гражданине, включало бы в себя информацию об IP, MAC-адресе, ID и ник-неймах пользователя в социальных сетях за весь период их использования, адреса электронной почты, доменные адреса и т.п. Функционирование такой программы представляется на базе проекта Единой системы информационно-аналитического обеспечения деятельности МВД РФ, а названием для такого информационно-поискового сервиса может послужить наименование «ЦИФРА».

Российская Федерация в настоящее время имеет огромный потенциал развития в направлении внедрения в деятельность правоохранительных органов технологий искусственного интеллекта, технологий исследования цифровых следов, технологий доступа к информации. Именно поэтому останавливаться на достигнутых достижениях нельзя. Отметим, что Президент Российской Федерации В. В. Путин заявил о необходимости развития тенденции всеобщей цифровизации сфер общества: «Надо <...> подхватить эти тенденции перехода в цифру, брать пример с компаний – лидеров цифровизации»¹. Поскольку мы живем в век постиндустриального общества, где за компьютерными технологиями стоит будущее, то не стоит отрицать и обходить стороной новейшие достижения человечества. Следует использовать их, извлекая максимальную полезность и производительность.

В современном мире, где преступность видоизменяется, приобретая все новые и новые формы, органы правопорядка должны идти на несколько десятков шагов впереди злоумышленников, используя в своей деятельности знания об основополагающих началах выявления, раскрытия и расследования преступлений с соблюдением законодательства Российской Федерации, сочетая их с новейшими технологиями мировой IT-индустрии.

Список литературы

1. **Суходолов А. П., Бычкова А. М.** Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753 – 766. DOI: 10.17150/2500-4255.2018.12(6)
2. **Россинская Е. Р., Рядовский И. А.** Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Междунар. науч.-практ. конф. (Алматы, 19 февраля 2019 г.). Алматы, 2019. С. 6 – 9.
3. **Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н.** Цифровые следы преступлений: монография. М.: Проспект, 2021. 168 с.
4. **Кравцов Д. А.** Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. № 3. С. 108 – 110.
5. **Тишунина И. В.** Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 4. С. 46 – 55.

¹ Путин заявил о необходимости развития тенденций к цифровизации. – Текст электронный. 10 июня 2020. 14:26. URL: <https://iz.ru/1022039/2020-06-10/putin-zaiavil-o-neobkhodimosti-razvitiia-tendencii-k-tcifrovizacii> (дата обращения: 01.09.2022).

References

1. **Sukhodolov A.P., Bychkova A.M.** [Artificial intelligence in combating crime, its prediction, prevention and evolution], *Vserossiyskiy kriminologicheskiy zhurnal* [All-Russian Criminological Journal], 2018, vol. 12, no. 6, pp. 753-766. DOI: 10.17150/2500-4255.2018.12(6) (In Russ., abstract in Eng.).
2. **Rossinskaya Ye.R., Ryadovskiy I.A.** [The concept of digital traces in criminalistics], *Aubakirovskiy chteniya: materialy Mezhdunar. nauch.-prakt. konf.* [Aubakirov readings: materials of the Intern. scientific-practical. conf.], Almaty, 19 Feb. 2019). Almaty, 2019, pp. 6-9. (In Russ.).
3. **Bagmet A.M., Bychkov V.V., Skobelin S.Yu., Il'in N.N.** *Tsifrovyye sledy prestupleniy: monografiya* [Digital traces of crimes: monograph], Moscow: Prospekt, 2021, 168 p. (In Russ.).
4. **Kravtsov D.A.** [Artificial intelligence: prevention and prediction of crime], *Vestnik Moskovskogo universiteta MVD Rossii* [Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia], 2018, no. 3, pp. 108-110. (In Russ., abstract in Eng.).
5. **Tishunina I.V.** [New opportunities for solving and investigating crimes in the context of global digitalization], *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskiye i yuridicheskiye nauki* [Bulletin of the Tula State University. Economic and legal sciences], 2019, no. 4, pp. 46-55. (In Russ., abstract in Eng.).

Modern Perspective for the Application of New Computer Technologies in the Detection, Disclaimer and Investigation of Crimes

D. V. Tetkin, *Cand. Sci. (Law), Police Lieutenant Colonel,
Associate Professor, Department of Criminal Procedure,
Ryazan Branch of Moscow University of the Ministry of Internal Affairs
of Russia named after V.Ya. Kikot', Ryazan, Russia;*
tyotkinden@mail.ru

I. S. Voronina, *Police Lieutenant,
secretary of the scientific society of cadets and students,
Ryazan Branch of Moscow University of the Ministry of Internal Affairs
of Russia named after V.Ya. Kikot', Ryazan, Russia;*
irinasvoronina@yandex.ru

The article is devoted to the importance of successful detection, disclosure and investigation by law enforcement agencies using computer information of crimes of any kind. The authors note that in modern conditions, a coherent system of scientific and technical means has arisen, adapted and specially created for the disclosure, investigation and prevention of criminal encroachments. According to the authors, of interest is the question of the prospects for the development and improvement of this direction, the study of the experience of foreign countries.

In the process of research, the authors revealed the meaning of the terms: artificial intelligence, digital traces of crimes. They also considered and analyzed the opinions of scientists studying the specifics of the application of the phenomena presented, as well as Russian and foreign practice. The paper also considers the experience of large IT companies involved in the development of digitalization.

The authors proposed to develop specialized databases based on foreign information systems and adapt them to Russian reality, the content of which, in addition to the basic standardized information about a citizen, included information about the IP, MAC address, ID and nicknames of the user in social networks for the entire period of their use, e-mail addresses, domain addresses, etc.

Keywords: computer technologies; computer research; information and telecommunication technologies; law enforcement agencies; crime detection; crime investigation; databases; IT-technologies; digital traces of crimes; artificial intelligence; IT industry; digitalization.

© Д. В. Теткин, 2023

© И. С. Воронина, 2023

Статья поступила в редакцию 04.10.2022

При цитировании использовать:

Теткин Д. В., Воронина И. С. Современная перспектива применения новых компьютерных технологий при выявлении, раскрытии и расследовании преступлений // *Право: история и современность*. 2023. Т. 7, № 1. С. 82 – 89. doi: 10.17277/pravo.2023.01.pp.082-089