Дата поступления рукописи в редакцию: 15.01.2026 г.
Дата принятия рукописи в печать: 16.02.2026 г.
DOI: 10.24412/2076-1503-2026-1-699-704

СОВИНА Анна Рудольфовна,
ассистент кафедры гражданского права
Санкт-Петербургского государственного университета
аэрокосмического приборостроения,
e-mail: rudolfovna15@mail.ru

ДРАГАНЧУК Александр Васильевич,
студент кафедры публичного права
Санкт-Петербургский государственный университет
аэрокосмического приборостроения,
Санкт-Петербург, Российская Федерация,
e-mail: alekdraganchuk@yandex.ru

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОСУЩЕСТВЛЕНИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

Аннотация. *Актуальность темы обусловлена активным развитием искусственного интеллекта и его внедрения в различные сферы, включая правоохранительные органы. В настоящее время применение ИИ в оперативно-розыскной деятельности ограничено, что не соответствует современным вызовам. В статье рассматриваются возможности использования ИИ и больших данных для повышения эффективности борьбы с киберпреступностью. Особое внимание уделяется «электронно-цифровым следам» как важной информации для криминалистики. Авторами предлагается создать программное обеспечение для непрерывного мониторинга преступной активности в Интернете, что позволит оперативно выявлять значимую информацию. Это повысит качество планирования и проведения операций в киберпространстве.*

Ключевые слова: *оперативно-розыскная деятельность, искусственный интеллект, киберпространство, цифровой след, преступность, большие данные.*

SOVINA Anna Rudolfovna,
Assistant of the Department of Civil Law
of Saint Petersburg State University
of Aerospace Instrumentation

DRAGANCHUK Aleksandr Vasilyevich
student of Department Public Law
Saint-Petersburg State University
of Aerospace Instrumentation
Saint-Petersburg

PROSPECTS FOR THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE IMPLEMENTATION OF OPERATIONAL INVESTIGATIVE ACTIVITIES ON THE INTERNET

Annotation. *The relevance of the topic is due to the active development of artificial intelligence (AI) and its implementation in various fields, including law enforcement agencies. Currently, the use of AI in operational investigative activities is limited, which does not meet modern challenges. The article discusses the possibilities of using AI and big data to increase the effectiveness of combating cybercrime. Special attention is paid to "digital footprints" as important information for criminology. The authors propose to create software for continuous monitoring of criminal activity on the Internet, which will quickly identify relevant information. This will improve the quality of planning and conducting operations in cyberspace.*

Key words: *operational investigative activities, artificial intelligence, cyberspace, digital footprint, crime, big data.*

Введение

Преступность, как социальное и правовое явление, обладает изменчивой природой, в результате которой совершенствуются методы совершения преступлений, а также появляются новые виды общественно-опасных деяний. Ответ государства в таком случае должен быть незамедлительным и беспощадным. Для ведения эффективной борьбы органам государственной власти сперва необходимо достичь качественно нового уровня своего технологического, кадрового и правового оснащений.

В настоящий момент технологией, от освоения которой зависит успешная деятельность в последующие десятилетия как отдельных сфер государства (например, правоохранительной), так и всей страны и общества, является технология искусственного интеллекта (далее - ИИ). Важность её отмечалась Президентом РФ: «Значение прорывов в сфере искусственного интеллекта колоссально. От того, каких результатов мы добьёмся, зависит место России в мире, наш суверенитет, безопасность и состоятельность нашей страны, наши возможности на качественно новом уровне решать задачи экономического, промышленного, социального развития, создавать широкие условия для самореализации граждан, для запуска общественных инициатив» [1].

Общий план и цели развития ИИ в России нашли свое отражение в Национальной стратегии развития ИИ на период до 2030 года. В ней ИИ описывают как комплекс технологий, имитирующих когнитивные функции человека и включающих инфраструктуру, программное обеспечение и обработку данных. [2].

Результаты и обсуждение

Несомненно, одна из перспективных сфер применения технологий ИИ в рамках борьбы с преступностью – оперативно-розыскная деятельность (далее – ОРД). Уже сейчас некоторые из таких технологий применяются для решения оперативных задач. Среди них: алгоритмы ИИ, способные распознавать и выявлять в транспортном потоке подозрительные или украденные транспортные средства (отчасти благодаря этому в 2022 году в Санкт-Петербурге на 12,3% повысилась раскрываемость краж транспортных средств, а число таких преступлений планомерно сокращается с 2016 года) [3, с. 51]; программы машинного распознавания образов, способные выявлять и распознавать как неодушевленные объекты, так и лиц находящихся в розыске или представляющих оперативный интерес; программы на основе технологий ИИ, нацеленные на эффективную и не требующую труда человека обработку больших объемов данных, документной информации и т.д. с последующей систематизацией; и др. Однако, применение программ, основанных на технологии ИИ, в ОРД на данный момент носит фрагментарный и эпизодический характер, что не в полной мере отвечает современным вызовам, с которыми сталкиваются правоохранительные органы. Стоит обозначить, что во всех вышеперечисленных случаях речь идет о применении технологий так называемого «слабого ИИ» (также называемого прикладным или узким), предназначенного для какой-либо одной интеллектуальной задачи или их небольшого множества, которые не подразумевают наличия у компьютера подлинного сознания [4, с. 130].

Интерес пользователей Интернета к применению ИИ для предотвращения и раскрытия преступлений растет. Цифровая преступность стала обычным явлением, с увеличением новых видов противоправных действий. Интернет служит площадкой для разнообразной активности человека и общества, а также катализатором общественных отношений. Анонимность в Сети позволяет людям делиться информацией, включая планы преступлений, что подтверждается случаями, когда пользователи обсуждали свои намерения в социальных сетях перед совершением деяний. Искренность, с которой люди могут делиться различной информацией, в том числе своими помыслами, в Интернете, при наличии некоторой (зачастую мнимой) анонимности, поражает воображение. Наглядный пример этого явления – неоднократные случаи освещения субъектами своих планов по совершению преступлений на своих страницах в социальных сетях и т.п. непосредственно перед совершением такого деяния.

В частности, подобные действия были совершены: устроившим стрельбу в школе № 175 в Казани – он упомянул о своих планах в созданном для этого Telegram-канале непосредственно перед нападением [5]; напавшим на школу № 4 в посёлке Большевик в Вольске – накануне нападения он опубликовал соответствующий манифест на своей странице Вконтакте [6], устроившим настоящую резню в своей школе девятиклассником в подмосковных Горках-2, аналогично разославшим подобный манифест своим одноклассникам перед нападением [7]; совершившим самоподрыв в здании регионального управления ФСБ в Архангельске – перед терактом он разместил в

чате соцсети Telegram послание, в котором брал на себя ответственность за готовящееся преступление [8].

Уникальность сети Интернет заключается в том, что практически любое действие, совершенное в ней, оставляет электронно-цифровой след, который был определен В. Б. Веховым как «любая криминалистически значимая компьютерная информация, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий, либо передающиеся по каналам связи посредством электромагнитных сигналов» [9, с. 90]. В случае, если такое действие как-либо связано с готовящимся или уже совершенным преступлением, информация, содержащаяся в подобных следах, может оказаться критически важной, решающей для успешного раскрытия этого преступления. И именно задачи по сбору, проверке, оценке и систематизации такой информации представляются работой, идеально подходящей для выполнения программами, основанными на технологиях ИИ.

Для раскрытия содержания проводимых в сети Интернет оперативно-розыскных мероприятий (далее - ОРМ) важно обозначить подход к пониманию этой среды, которую стоит рассматривать не только с технологической точки зрения, то есть как информационно-телекоммуникационное средство обеспечивающего передачу, обработку и хранение информации, но и с социальной – как сложный социокультурный феномен, образующий особую среду реализации определенных видов деятельности и проявления специфических общественных отношений – киберпространство [10, с. 222]. В связи с этим можно говорить о многообразии проводимых в Сети ОРМ, которые выходят за рамки очевидного «снятия информации с технических каналов связи». Среди них: наблюдение, опрос, отождествление личности, получение компьютерной информации, наведение справок, проверочная закупка, а в некоторых случаях даже оперативное внедрение. Список ОРМ в Интернете не статичен и расширяется с появлением новых преступлений и методов противодействия им. Правовая основа мероприятий остается такой же, как и в материальном мире, не требуя существенных уточнений.

В целях решения задач по эффективному выявлению оперативно значимой информации из общего гигантского объема различных видов данных, содержащихся в Интернете, органы, осуществляющие ОРД, неизбежно обращаются к технологии Big Data (большие данные) – структурированным или неструктурированным массивам данных большого объема, обрабатываемых при помощи специальных автоматизированных инструментов. Она позволяет агрегировать, а затем подробно анализировать петабайты существующих и генерирующихся в Интернете данных для последующей их классификации, кластеризации, для выявления отклонений и закономерностей, а также прогнозирования. Результатом применения этой технологии в процессе ОРД может стать: формирование «электронного досье» на лиц, представляющих оперативный интерес; слежка за активностью в Интернете определенных лиц в режиме реального времени; выявление цифровых следов по заданным свойствам и признакам; план осуществления ОРД с учетом сложной совокупности множества факторов, оказывающих на неё воздействие и т.д.

Использование технологий ИИ в обработке больших данных значительно повысит эффективность анализа. ИИ сократит время обработки, увеличит точность результатов и сможет работать с неограниченными объемами данных. Это приведет к оптимизации работы с Big Data в ОРД и правоохранительной деятельности. ИИ сможет синтезировать и оценивать разнообразные данные, выделяя информацию, интересующую органы ОРД. Со временем он научится обнаруживать неявные связи в данных и составлять точные прогнозы [11, с. 64]. ИИ, анализируя множество «электронных досье», сможет выявить тонкие закономерности, связывающие активность людей в Сети с их намерениями и действиями. Это позволит эффективно раскрывать преступления и предотвращать множество противоправных деяний на стадии подготовки, значительно повысив уровень работы ОРД.

Внедрение столь многоаспектных технологий в повседневную деятельность правоохранительных органов, потребует, кроме прочего, большого штата квалифицированных специалистов, особенно на начальных этапах. Осуществимость этой задачи не вызывает сомнений – такая же нужда возникла у МВД при резком скачке роста Интернет-преступности в 2020 году, вследствие чего ряды подразделения по борьбе с киберпреступностью пополнили 3000 сотрудников [12].

Для реализации возможностей технологий ИИ и Big Data необходимо сотрудничество правоохранительных органов с научным сообществом и специалистами в программировании и ИИ. Также требуется создание независимого отечественного программного обеспечения, защищенного от внешнего вмешательства, включающего системы обработки информации и сопутствующие документы [13].

В настоящее время в данном направлении ведется активная работа. Так, с 2019 года МВД России разрабатывает программу на основе тех-

нологий ИИ, нацеленную на поиск серийных преступников и определение индивидуальных анатомических признаков человека, полученных из биологического материала с мест совершения преступлений. В текущий момент проект находится на этапе создания и тестирования конкретных функций ПО [14, с. 153]. В современных международных отношениях использование иностранного ПО в ключевых для государства сферах может угрожать национальной безопасности, поэтому от этого стоит отказаться. Критически важно обеспечить правоохранительные органы средствами для получения, обработки и передачи информации, а также защищенными хранилищами данных. Без этого реализация исследования невозможна. Объемы анализируемых данных потребуют новейшего оборудования, обслуживание которого станет приоритетом в системе ОРД. Необходим быстрый и защищенный доступ к базам данных, поскольку скорость работы ИИ зависит от качества технической оснащенности.

В современном мире использование роботов и ИИ для охраны правопорядка стало реальностью. Например, полиция Сингапура применяет беспилотные летательные аппараты с ИИ для мониторинга улиц и сбора видеоданных, что повышает эффективность работы ОВД без значительного увеличения численности сотрудников [15, с. 93-101]. Важно учитывать как положительный, так и отрицательный опыт других стран в применении ИИ в правоохранительной сфере. Полное копирование практики не представляется возможным ввиду большого числа существенных различий правовых систем, однако в нем нет необходимости, но российским правоохранительным органам следует разработать уникальный подход к внедрению ИИ и больших данных, чтобы избежать конфликтов в правовой системе и практике ОРД.

Заключение и выводы

Применение технологий ИИ и больших данных в ОРД имеет большой потенциал, особенно для оперативно-розыскных мероприятий в киберпространстве. Скорость и точность обработки больших объемов данных позволят сотрудникам ОВД преодолеть ограничения ручной работы и сосредоточиться на более сложных задачах, требующих человеческой интуиции и опыта, что значительно повысит производительность труда. В первую очередь это касается использования ИИ для рутинных действий, требующих точного анализа и систематизации информации.

Среди таких задач, например, анализ видеозаписей из Интернета, включая распознавание статичных образов с помощью машинного зрения и оценку сложных действий на основе видеоданных [16, с. 329]. Подобный подход применяется во время футбольных матчей – система-анализатор имела своей целью, исходя из базового набора данных, осуществлять потоковую передачу сводок игр в реальном времени [17, с. 806]. ИИ способен обрабатывать огромное количество материала, не упуская деталей, анализировать звуковые дорожки и выявлять скрытые связи, объединяя результаты в удобный отчет с ценными сведениями для органов ОРД.

Важно отметить, что в данном исследовании речь идет о применении особого ПО для анализа информации, находящейся в открытом доступе. Сбор и обработка таких данных не нарушает конституционные права граждан, поэтому ОРД с применением этих технологий возможен без предварительного судебного решения. Нет необходимости в создании отдельной правовой базы для ОРМ с ИИ, так как эта технология является одним из средств правоохранительных органов и может регулироваться внутренними уставами. Однако ИИ как наука и технология должен быть закреплен в федеральном законодательстве России, например, в виде закона, который станет основой для применения ИИ в различных сферах.

Совместное использование технологий ИИ и больших данных – будущее борьбы с преступностью. Оптимизация аналитико-информационного обеспечения ОРД позволит создать систему непрерывного контроля в киберпространстве, где любой цифровой след будет выявлен и проанализирован с помощью ИИ. Это приведет к значительному повышению эффективности планирования и проведения ОРМ в Сети.

Повысится не только реальная раскрываемость преступлений, но и многократно увеличится количество «несостоявшихся» правонарушений, то есть пресеченных на ранних стадиях. Скорость ИИ совместно с высокой подготовкой сотрудников правоохранительных органов, как осуществляющих ОРД, так и отвечающих за техническое обеспечение и обслуживание технических средств, приведет к значительному повышению скорости оперативного реагирования. Данные показатели не просто найдут свое отражение в статистических отчетах, но и позволят спасти жизни и здоровье многих людей, не допустить потенциальных трагедий, защитить государство от враждебных проявлений и т.д. Внедрение таких технологий в правоохранительную деятельность – объективная необходимость нашего времени. Использование ИИ злоумышленниками в противоправных целях может быть крайне опасно как для личности, так и для государства. А потому органы власти должны обратить свое пристальное внимание на обсуждаемые в данном исследовании технологии и без промедлений подготовить базу для внедрения их в свою деятельность, а далее – перейти к непо-

средственному их использованию. Скорость выполнения данных задач позволит пресечь большой объем потенциальных преступлений, совершенных с прямым или косвенным использованием ИИ.

Всесторонний анализ активности пользователей Сети, не ограничивающий при этом их конституционных прав, не принесет каких-либо негативных последствий для законопослушных граждан. На современном этапе развития цифровых технологий всякая анонимность в киберпространстве фактически отсутствует, а потому, вопреки возможным опасениям о потенциальной тоталитарности рассматриваемого ПО на основе ИИ, аналитическая деятельность программы с машинным интеллектом не вызовет в данном отношении каких-либо существенных отрицательных изменений, так как она будет работать с общедоступной информацией, изучить которую может любой пользователь Сети. Реализация на практике результатов исследования позволит достичь нового, высочайшего, уровня законности в цифровом пространстве, где будет прекращена всякая анархия. В Интернете не останется мест, где злоумышленники могли бы скрыться «в тени», а противоправные деяния станут безнадежной авантюрой, неизменно ведущей лишь к одному итогу – к неотвратимому наказанию.

Список литературы:

[1] Конференция по искусственному интеллекту. URL: https://clck.ru/36qVVf. (дата обращения: 22.12.2025).

[2] Национальная стратегия развития искусственного интеллекта на период до 2030 года: утв. Указом Президента РФ В.В. Путина от 10 октября 2019 г. № 490 // Официальный сайт Президента России. – URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 22.12.2025).

[3] Состояние преступности в Санкт-Петербурге. Криминологический мониторинг и прогноз: научно-практическое пособие // СПб.: Изд-во СПб ГУП «СПб ИАЦ». – 2023. – 302 с.

[4] Маковкин, А. С. Этические проблемы применения искусственного интеллекта // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: Грамота. – 2015. – № 2 (52). – С. 130-132.

[5] Дуров: стрелявший в Казани сделал канал в Telegram публичным за 15 минут до трагедии. URL: https://tass.ru/proisshestviya/11356769 (дата обращения: 22.12.2022)

[6] В Вольске подросток пытался совершить массовое убийство в школе. URL: https://clck.ru/36gDpr (дата обращения: 22.12.2025)

[7] Урок ужаса. URL: https://www.kommersant.ru/doc/8293546 (дата обращения: 22.12.2025)

[8] Студент взорвал себя в здании ФСБ. URL: https://www.kommersant.ru/doc/3786845 (дата обращения: 22.12.2025)

[9] Вехов, В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография // Волгоград: ВА МВД России. – 2008. – 401 с.

[10] Теория оперативно-розыскной деятельности. Учебник; издание пятое, испр. и доп. / под ред. д.ю.н., проф. К.К. Горяинова, д.ю.н. В.С. Овчинского. М. // «Норма: ИНФРА-М». – 2021. – 795 с.

[11] Frawley, W., Piatetsky-Shapiro, G., Matheus, C. Knowledge Discovery in Databases: An Overview // AI Magazine. – 1992. – № 3. – pp. 57-70.

[12] МВД ввело программу опознания серийных кибермошенников. URL: https://pravo.ru/news/229899/ (дата обращения: 25.12.2025)

[13] Национальный стандарт РФ ГОСТ Р 54593-2011 «Информационные технологии. Свободное программное обеспечение. Общие положения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 декабря 2011 г. N 718-ст)

[14] Ковтун, Ю. А., Лагуточкина, А. С. О применении правоохранительными органами специализированного программного обеспечения в организации использования искусственного интеллекта // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2021. – Т. 7 (73), № 3, ч. 2. – С. 148-154.

[15] Daswani, R., Tan, J. Artificial Intelligence: Impact on Public Safety & Security // ETHOS. Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative. – 2019. – № 21. – pp. 93-101.

[16] Буйко, А. Ю., Виноградов, А. Н. Выявление действий на видео с помощью рекуррентных нейронных сетей // Программные системы: теория и приложения. – 2017. – №4 (35). – С. 327–345.

[17] Ekin, A., Tekalp, A., Mehrotra, R. Automatic Soccer Video Analysis and Summarization // IEEE Transactions on Image Processing. – 2003. – № 12 (7). – pp. 796–807.

References:

[1] Artificial Intelligence Conference. URL: https://clck.ru/36qVVf. (accessed on: 22.12.2025).

[2] National Strategy for the Development of Artificial Intelligence for the Period up to 2030: approved. By decree of the President of the Russian Federation V.V. Putin dated October 10, 2019 No.

490//Official website of the President of Russia. - URL: http://www.kremlin.ru/acts/bank/44731 (access date: 22.12.2025).

[3] The state of crime in St. Petersburg. Criminological monitoring and forecast: scientific and practical guide//St. Petersburg: Publishing House of St. Petersburg State Unitary Enterprise "St. Petersburg IAC." – 2023. - 302 s.

[4] Makovkin, A. S. Ethical problems of the use of artificial intelligence//Historical, philosophical, political and legal sciences, cultural studies and art history. Questions of theory and practice. Tambov: Diploma. – 2015. – № 2 (52). - S. 130-132.

[5] Durov: the shooter in Kazan made the Telegram channel public 15 minutes before the tragedy. URL: https://tass.ru/proisshestviya/11356769 (accessed on: 22.12.2022)

[6] In Volsk, a teenager tried to commit a massacre at school. URL: https://clck.ru/36gDpr (accessed on: 22.12.2025)

[7] A lesson in horror. URL: https://www.kommersant.ru/doc/8293546 (accessed on: 22.12.2025)

[8] A student blew himself up in the FSB building. URL: https://www.kommersant.ru/doc/3786845 (accessed on: 22.12.2025)

[9] Vekhov, V. B. Fundamentals of the forensic doctrine of the study and use of computer information and the means of its processing: monograph//Volgograd: VA Ministry of Internal Affairs of Russia. – 2008. - 401 s.

[10] Operational-search activity theory. Textbook; fifth edition, rev. and additional/ed. Doctor of Legal Sciences, prof. K.K. Goryainova, Doctor of Law V.S. Ovchinsky. M.//" Norm: INFRA-M. " – 2021. - 795 s.

[11] Frawley, W., Piatetsky-Shapiro, G., Matheus, C. Knowledge Discovery in Databases: An Overview // AI Magazine. – 1992. – № 3. – pp. 57-70.

[12] The Ministry of Internal Affairs has introduced a program for identifying serial cyber fraudsters. URL: https://pravo.ru/news/229899/ (accessed on: 25.12.2025)

[13] National Standard of the Russian Federation GOST R 54593-2011 "Information Technologies. Free software. General provisions" (approved by Order of the Federal Agency on Technical Regulation and Metrology No. 718-st dated December 6, 2011)

[14] Kovtun, Yu. A., Lagutochkina, A. S. On the use of specialized software by law enforcement agencies in organizing the use of artificial intelligence//Scientific notes of the V. I. Vernadsky Crimean Federal University. Legal sciences. – 2021. - T. 7 (73), No. 3, part 2. - S. 148-154.

[15] Daswani, R., Tan, J. Artificial Intelligence: Impact on Public Safety & Security // ETHOS. Digital Government, Smart Nation: Pursuing Singapore's Tech Imperative. – 2019. – № 21. – pp. 93-101.

[16] Buiko, A. Yu., Vinogradov, A. N. Identification of actions on video using recurrent neural networks//Software systems: theory and applications. – 2017. – №4 (35). - S. 327-345.

[17] Ekin, A., Tekalp, A., Mehrotra, R. Automatic Soccer Video Analysis and Summarization // IEEE Transactions on Image Processing. – 2003. – № 12 (7). – pp. 796–807.