Научная статья
УДК: 343.3/.7
DOI: 10.17323/tis.2024.21708

Original article

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ОБРАЗОВ И СМЫСЛА В СИСТЕМЕ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ

INTELLIGENT SYSTEMS FOR RECOGNIZING IMAGES AND MEANING IN THE CRIME PREVENTION SYSTEM

Анна Константиновна ЖАРОВА
Институт государства и права РАН, Москва, Россия,
anna_jarova@mail.ru,
ORCID: 0000-0002-2981-3369

Информация об авторе
А.К. Жарова — ведущий научный сотрудник Института государства и права РАН, доктор юридических наук, доцент, ассоциированный член Кафедры ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам

Аннотация. Интеллектуальные системы (ИС) являются наиболее перспективным направлением развития информационных технологий, важность применения технологических решений ИС в экономике и общественных отношениях заявлена в правовых актах. Однако мы сталкиваемся с ситуацией, когда информация, например, размещенная в интернете и содержащая намерение совершить преступление, не выявляется, что приводит к реализации преступником своих преступных умыслов. А ведь возможности некоторых алгоритмов искусственного интеллекта вполне могут быть использованы уполномоченными органами обеспечения безопасности в системе предупреждения преступлений. Это, к примеру, алгоритмы глубокого обучения, предиктивной аналитики больших данных, распознавания смысла и образов и другие.
К сожалению, в открытом доступе отсутствуют отчеты о результатах применения методов предиктивной аналитики больших данных в системе предупреждения преступлений на территории Российской Федерации. Однако есть много зарубежных отчетов о применении алгоритмов искусственного интеллекта (ИИ) в целях предотвращения преступных действий. Возможно, такая ситуация связана с различными подходами к пониманию понятия «преступление». В связи с этим в статье изучены аналитические материалы, в которых отражен опыт применения алгоритмов ИИ в целях определения вероятности отнесения выявленных противоправных действий к преступным на основе соотнесения признаков преступления; осуществления преступления конкретным человеком на основе анализа его криминогенных качеств, а также в целях выявления преступного умысла и оценки вероятности его перехода в преступные действия.

Ключевые слова: интеллектуальные системы, признаки преступлений, стадии преступлений, преступный умысел

Для цитирования: *Жарова А.К.* Интеллектуальные системы распознавания образов и смысла в системе предупреждения преступлений // Труды по интеллектуальной собственности (Works on Intellectual Property). 2024. Т. 49, № 2. С. 16–23; DOI: 10.17323/tis.2024.21708

Anna K. ZHAROVA
Russian Academy of Sciences, Institute of State and Law, Moscow, Russia,
anna_jarova@mail.ru,
ORCID: 0000-0002-2981-3369

Information about the author
A.K. Zharova — leading researcher of the Institute of State and Law of the Russian Academy of Sciences, Doctor of Law, Associate Professor, Associate Fellow of the UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights

Abstract. Intelligent systems (IS) are the most promising area of information technology development, the importance of using AI technological solutions in economics and public

relations is stated in legal acts. However, we are faced with a situation where information, for example, posted on the Internet, containing the intention to commit a crime is not revealed, which eventually leads to the realization of the criminal's criminal intentions. Although the capabilities of AI could well be used by authorized security agencies in the crime prevention system.
But, unfortunately, we were unable to find reports on the results of using predictive big data analytics methods in the crime prevention system on the territory of the Russian Federation. However, there are many foreign reports on the use of AI systems in order to prevent criminal acts. Perhaps this situation is related to different approaches to understanding the concept of "crime".
In this regard, the article examines the possibilities of AI in order to determine the probability of: attributing the identified illegal actions to criminal ones based on correlating the signs of a crime; committing a crime by a specific person based on an analysis of his criminogenic qualities, as well as identifying criminal intent and assessing the probability of its transition to criminal actions.

Keywords: Intelligent systems, signs of crimes, stages of crimes, criminal intent

For citation: *Zharova A.K.* Intelligent Systems for Recognizing Images and Meaning in the Crime Prevention System // Trudi po Intellectualnoy Sobstvennosti (Works on Intellectual Property). 2024. Vol. 49 (2). P. 16–23; DOI: 10.17323/tis.2024.21708

Мы все чаще встречаем примеры использования систем искусственного интеллекта (ИИ) в различных областях экономики и общественных отношений. В Указе Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» определена одна из целей развития искусственного интеллекта в нашей стране — это «обеспечение национальной безопасности и правопорядка» (п. 23) [1].

Под искусственным интеллектом понимают «моделируемую (искусственно-воспроизводимую) интеллектуальную деятельность мышления человека» [2]. К интеллектуальным системам (ИС) относят программно-аппаратные решения, созданные на основе различных алгоритмов ИИ [3]. Так, ИС, основанные на генетических алгоритмах, «конструируют роботов, которые могут быть изготовлены на автоматизированных заводах без участия человека» [3].

Термин «алгоритм» связывают с именем математика, философа, историка Аль-Хорезми, который сформулировал правила вычислений. В дальнейшем этот термин стал определять понятие «алгоритм». Под алгоритмом понимают «инструкцию, точное описание способа действия с использованием простых, общепонятных элементов (например, операций). В математике понятие алгоритма сужается до последовательности переходов от одного состояния вычисления к другому» [4].

Например, такие алгоритмы ИИ, как глубокое обучение, предиктивная аналитика больших данных, распознавание смысла и образов, и другие могут выявлять точки социальной напряженности в процессе анализа текста, видео и фотоматериалов.

Возможности алгоритмов ИИ могли бы выявлять точки напряженности в Сети, а объединение алгоритмов ИИ и уполномоченных органов в области обеспечения общественной безопасности как комбинация взаимодействия позволило бы не только получить смысловой анализ таких признаков преступного деяния, как противоправность, общественная опасность содержащаяся в размещенной информации [5], оценить реальность намерений человека совершить противоправные действия, но и вовремя отреагировать уполномоченным органам в области обеспечения

общественной безопасности и тем самым предотвратить преступные действия.

Статистика непредотвращенных преступлений, информация о намерении совершения которых была размещена в интернете за некоторое время до реализации преступного умысла, позволяет предположить, что интеллектуальные системы распознавания образов и смысла информации в Сети малоэффективны в системе предупреждения преступлений. Для подтверждения или опровержения данной гипотезы в статье дан ответ на вопрос о том, могут ли алгоритмы ИИ прогнозировать преступление, анализируя признаки преступного деяния, а также оценивать вероятность перехода стадий преступлений.

ПРОГНОЗИРОВАНИЕ ПОЛОЖЕНИЯ ДЕЛ В ОБЛАСТИ ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Большая часть уголовно-правовых отношений возникает в связи с совершением преступлений, т.е. тогда, когда правоохраняемым ценностям уже нанесен определенный вред, хотя обществу «выгоднее» предотвратить преступления, чем потом их расследовать и наказывать преступников. В связи с этим большое значение приобретает вторая задача уголовного преследования — предупреждение преступлений [6, 7]. В решении этой задачи мог бы помочь ИИ как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека». В комплекс технологических решений входят информационно-коммуникационная инфраструктура, программное обеспечение (в том числе то, в котором используются методы машинного обучения), процессы и сервисы по обработке больших данных и поиску решений (п. 5 подп. «а») [1].

Таким образом, используя разные алгоритмы ИИ, комбинируя их, можно создавать ИС. Алгоритмы ИИ с высокой точностью могут определить смысл текста или изображений, размещенных в Сети, построить причинно-следственные связи развития событий. Например, такая область ИИ, как NLP, отвечает за аналитику контента, понимание и обработку естественного языка, извлечение из него ключевых идей или тем.

Таким образом, ИИ мог бы стать эффективным инструментом в руках уполномоченных органов в области обеспечения общественной безопасности для реализации одной из их основных задач — предотвращение противоправных действий.

В зарубежной научной литературе обсуждается возможность использования алгоритмов ИИ для прогнозирования преступлений [1, 8]. В российском научном пространстве исследований, посвященных этой тематике, меньше [9, 10, 11]. Кроме того, в основном в зарубежных отчетах публикуются результаты применения ИИ в целях проведения предиктивной аналитики преступности и предотвращения преступлений на основе полученного анализа. В отечественных отчетах и литературе в большинстве случаев речь идет об интеллектуальных технологиях, применяемых на этапе расследования преступления [12], таких, например, как программа «Конструктор места происшествия», системы моделирования различных следственных действий [13] и др. [14]. Но эти отечественные системы не решают проблему прогнозирования преступлений, хотя еще в 2008 г. предлагалось использовать методы предиктивной аналитики в целях принятия обоснованных управленческих решений [15].

Актуальность данной проблемы подтверждает поставленная в Ведомственной программе цифровой трансформации МВД России на 2022–2024 гг. [16] задача ликвидации имеющегося отставания по вопросам применения технологий искусственного интеллекта.

Однако, несмотря на имеющиеся зарубежные отчеты о прогнозировании преступлений, закономерен вопрос: можно ли прогнозировать совершение преступлений, иными словами — имеются ли у преступления те параметры или признаки, которые подлежат вероятностной оценке?

ПРЕСТУПЛЕНИЕ ИЛИ НЕ ПРЕСТУПЛЕНИЕ?

К полномочиям МВД России отнесено в том числе «формирование основных направлений государственной политики в сфере внутренних дел на основе анализа и прогнозирования: состояния преступности; положения дел в области охраны общественного порядка и собственности, обеспечения общественной безопасности; миграционных процессов» (п. 11) [17].

Необходимо подчеркнуть, что в данном случае речь идет о прогнозировании преступности, но не о прогнозировании преступления. Преступление является конкретным юридическим фактом, обладающим определенными признаками, а преступность — явлением социальным, обобщенным и статистически измеряемым.

Прогнозирование таких социальных явлений, как «преступность, личность преступника, факторы (причины и условия) преступности, последствия пре-

ступности, меры борьбы с преступностью» [16], отнесено к задачам криминологического прогнозирования. Причем преступность рассматривается на трех уровнях интерпретации: свойства преступности как массового явления, свойства преступника, признаки преступного деяния.

Прогнозирование преступности как социального явления связано с предвидением, вычислением вероятностных изменений, тенденций и закономерностей преступности в будущем и является одной из задач криминологического прогнозирования.

Однако если подходить к оценке преступления как преступного деяния, то построение системы установленных причинно-следственных связей и закономерностей, сопровождающих преступные деяния, позволит дать оценку состояния и его вероятного направления развития. Но для прогнозирования вероятности совершения преступления как уголовно-наказуемого деяния необходимо оценить его признаки.

Т.Н. Долгих считает, что в теории уголовного права, несмотря на сформулированное понятие преступления, вопрос о перечне признаков преступления является дискуссионным, поскольку УК РФ не определяет понятие и виды признаков преступления [18]. С учетом анализа определения, сформулированного в ч. 1 ст. 14 УК РФ, выделяются следующие признаки преступления как деяния: общественная опасность, противоправность, виновность, наказуемость. Однако эти признаки присущи уже совершенному деянию, у которого в связи с реальностью его существования можно оценить такие признаки.

Отмечу, что среди обозначенных признаков преступления алгоритмами ИИ, например алгоритмом глубокого обучения, может быть дана оценка только двум признакам — общественной опасности и противоправности, а два других признака — наказуемость и виновность — должны быть оценены только человеком. Оценка интеллектуальной системой двух других признаков преступления — виновности и наказуемости — должна носить рекомендательный характер, окончательное решение необходимо принимать уполномоченному лицу.

Например, для получения ответа на вопросы, является ли смысловая конструкция в интернете общественно опасной и содержит ли она признаки противоправности, интеллектуальной системе необходимо оценить не только смысл текста, но и все связанные с размещением этого текста события — например, провести анализ всей информации, которая размещена на странице социальной сети предполагаемого преступника, его социальных связей. Одна и та же информация может носить различную окраску в зависимости от контекста — например, словосочетание «я тебя убью» может быть как фигурой речи, так и угрозой убийства. Для оценки реальности угрозы интеллектуальные системы должны проанализировать множество данных, оставленных человеком, который разместил текст, — его цифровые следы и цифровые тени [19]. В этом случае результат работы интеллектуальной системы будет отвечать требованию смыслового толкования обстоятельств криминальной ситуации в неразрывной связи со всеми сведениями по делу [20].

Хотя объективности ради необходимо отметить, что не существует абсолютно точных технологий и возможны ошибки в оценке данных. Но ошибки могут быть минимизированы в случае, если интеллектуальные системы не будут принимать решение за уполномоченные органы охраны общественной безопасности, а будут служить лишь инструментом анализа большого объема данных, передавая результат своей работы — вероятностную оценку опасности, противоправности и реальности намерений человека, полученную на основе совокупности цифровых данных, — уполномоченным органам в области охраны безопасности.

Таким образом, оценка ИИ признаков преступления возможна в случае существующего события. Фактически данная оценка признаков деяния позволит понять, можно ли отнести это деяние к преступлению.

ОЦЕНКА ИИ СТАДИЙ ПРЕСТУПЛЕНИЯ

Возможным этапом оценки преступных деяний является оценка стадий совершения преступлений. С.В. Расторопов считает, что «преступные действия достаточно предсказуемы и прогнозируемы, необходимо лишь правоохранительным органам найти в больших объемах данных эти закономерности» [21].

Действительно, анализ больших данных может позволить оценить преступные действия на предмет их соответствия стадиям преступления — приготовление, покушение и оконченное действие. В этом случае ИИ должен оценить вероятность перерастания одной стадии преступления в другую, выявить сопровождающие преступные действия события и явления, распознать их, сравнить полученные данные с другими данными, построить причинно-следственную связь и предотвратить переход преступления в последующие стадии [22].

Однако оценка стадий возможна не для любых преступлений. Специалисты в области уголовного права считают, что выделение стадий преступления возможно только в отношении умышленных преступлений [23]. В таком случае закономерен вопрос: могут ли алгоритмы ИИ выявить преступный умысел в размещенной информации? Иными словами: может

ли ИИ построить вероятностную модель перерастания преступного умысла в совершение преступных действий определенным человеком? Преступный умысел как отражение преступных намерений может быть выражен посредством телодвижения, слов, символов, фото- или видеоматериалов. Современные возможности ИИ позволяют оценить всю связанную с человеком информацию и выявить, например, в Сети предварительную преступную деятельность.

Необходимо оговориться, что, хотя большинство российских специалистов по уголовному праву не относят формирование преступного умысла к стадиям преступления [24], есть и те, кто считают это нулевой стадией подготовки преступления [25, 26].

В зарубежной научной литературе ученые представляют результаты своих работ, связанные с выявлением преступных намерений, умысла по результатам проведенного ИИ анализа пользовательского контента на платформах социальных сетей [27]. В проведенном эксперименте использование алгоритмов машинного обучения позволило понять и проанализировать настроения пользователей социальной сети, связанные с возможными преступными действиями. ИИ достаточно точно определил преступные намерения, отраженные в пользовательском контенте, что позволило правоохранительным органам усилить свои упреждающие меры [27].

Кроме того, существуют технологические решения, направленные на прогнозирование вероятности совершения преступления конкретным человеком по результатам оценки его криминогенных качеств [28, 29]. В этом случае алгоритм ИИ анализирует существующие отношения, действия, совершаемые человеком, например, в Сети. Результаты работы таких математических моделей уже представлены на обсуждение общественности [30, 31].

Обсуждая возможность предотвращения преступлений, мы должны исходить из того, что распознание ИИ преступного умысла, выраженного в размещенной в Сети информации, позволит оценить вероятность перерастания умысла в реальные преступные действия и заблаговременно отправить эту информацию уполномоченным органам в области обеспечения безопасности. Тем самым риск развития преступных действий будет минимизирован, а правоохранительные органы примут соответствующие профилактические меры [32].

ЗАКЛЮЧЕНИЕ

Поскольку в российских открытых источниках отсутствует информация о российских ИС в области предиктивной аналитики преступлений, было сделано предположение, что алгоритмы ИИ неэффективны для предупреждения преступности и преступлений. Однако анализ опубликованных за рубежом научных отчетов, российских и зарубежных научных работ, посвященных разработанным ИС в правоохранительной сфере, позволили сделать вывод, что ИС позволяют достичь результата — прогнозирования возможных преступлений.

Применение ИС уполномоченными органами охраны правопорядка, как показывают аналитические материалы, позволяет не только выявить противоправный и общественно-опасный контент, но и оценить вероятность совершения преступления конкретным человеком. Такие ИС разрабатываются на основе алгоритмов ИИ, например глубокого обучения, предиктивной аналитики, анализа больших данных и других, которые могут распознать преступление еще на стадии формирования преступного умысла, выраженного в размещенной информации, и тем самым минимизировать возможность перерастания умысла в реальные преступные действия.

СПИСОК ИСТОЧНИКОВ

1. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 г.») // СЗ РФ. 2019. № 41. ст. 5700.
2. ГОСТ Р 43.0.8-2017. Национальный стандарт Российской Федерации. Информационное обеспечение техники и операторской деятельности. Искусственно-интеллектуализированное человеко-информационное взаимодействие. Общие положения (утв. и введен в действие Приказом Росстандарта от 27.07.2017 № 757-ст). М.: Стандартинформ, 2018.
3. *Коровин А.М.* Интеллектуальные системы: текст лекций. Челябинск: ИЦ ЮУрГУ, 2015. 60 с. — URL:https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000539905&dtype=F&etype=.pdf
4. Большая российская энциклопедия. — URL: https://bigenc.ru/c/algoritm-ee5b00
5. *Жарова А.К.* Искусственный интеллект — средство или способ совершения мошенничества в сфере компьютерной информации? // Государство и право. 2023. № 2. С. 54–61. DOI 10.31857/S102694520021177-5. EDN PESJQJ.
6. Уголовное право Российской Федерации. Общая часть: уч. для вузов / под ред. В.С. Комиссарова, Н.Е. Крыловой, И.М. Тяжковой. М: Статут, 2012.
7. Полный курс уголовного права / под ред. А.И. Коробеева. Т. I: Преступление и наказание. СПб.: Юр. центр Пресс, 2008. С. 77–78.

8. Artificial Intelligence in the Context of Crime and Criminal Justice. — URL: https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf
9. *Umadevi V Navalgund, Priyadharshini K.* Crime Intention Detection System Using Deep Learning, December 2018, Conference: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)DOI: 10.1109/ICCSDET.2018.8821168
10. *Сретенцев Д.Н., Волкова В.Р.* Перспективы внедрения систем искусственного интеллекта в сферу расследования преступлений // Российский следователь. 2021. № 11. С. 38-42. DOI 10.18572/1812-3783-2021-11-38-42. EDN HLNQDU.
11. *Расторопов С.В.* Использование искусственного интеллекта для предупреждения и выявления преступлений (мировой опыт) // Международное публичное и частное право. 2020. № 5. С. 40–43. DOI 10.18572/1812-3910-2020-5-40-43. EDN QPDQHX.
12. *Sukhodolov A.P., Bychkova A.M.* Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution // Russian Journal of Criminology. 2018. Vol. 12, No 6. P. 753–766. DOI 10.17150/2500-4255.2018.12(6).753-766. EDN YYSTVR.
13. *Смушкин А.Б.* Экосистема предварительного расследования // Актуальные проблемы российского права. 2023. № 7. С. 143–158.
14. *Яшин А.А.* Виртуальные технологии в расследовании преступлений: перспективные направления и возможности использования // Адвокатская практика. 2022. № 6. С. 23–26.
15. *Горбенко А.О., Мамасуев А.В.* Применение аналитических систем при принятии управленческих решений в органах внутренних дел (аналитические системы OLAP) // Вестник Академии экономической безопасности МВД России. 2008. № 4. С. 96–99. EDN NEFKRP.
16. Распоряжение МВД России от 11 января 2022 г. № 1/37 «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2022–2024 гг.». Документ опубликован не был // СПС «КонсультантПлюс».
17. Указ Президента РФ от 21 декабря 2016 г. № 699 «Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации» // СЗ РФ. 2016. № 52 (Ч. V.). Ст. 7614.
18. *Долгих Т.Н.* Признаки преступления в теории уголовного права. 2023 // СПС «КонсультантПлюс».
19. *Жарова А.К., Елин В.М., Минбалеев А.В.* Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления. М.: Русайнс, 2022. 240 с. ISBN 978-5-466-00766-4. EDN DNKVPR.
20. *Халиков А.Н.* Герменевтические проблемы истолкования криминалистической информации при расследовании уголовных дел // Российский следователь. 2021. № 2. С. 19–23.
21. *Расторопов С.В.* Использование искусственного интеллекта для предупреждения и выявления преступлений (мировой опыт) // Международное публичное и частное право. 2020. № 5. С. 40–43.
22. *Жарова А.К.* Необходимо ли ужесточение требований об обязательном общем мониторинге информации провайдерами хостинга? // Труды по интеллектуальной собственности. 2022. Т. 41, № 2. С. 21–29. DOI 10.17323/tis.2022.14439. EDN LXKDRR.
23. Комментарий к Уголовному кодексу Российской Федерации» (постатейный). 7-е изд., перераб. и доп. / отв. ред. А.И. Рарог). М.: Проспект, 2011.
24. *Андрусенко С.П., Голованова Н.А., Гравина А.А.* Международно-правовые стандарты в уголовной юстиции Российской Федерации: научно-практическое пособие / отв. ред. В.П. Кашепов. М.: ИЗиСП, Анкил, 2012. 312 с.
25. *Баев О.Я.* Криминалистические методики в реализации доказывания по уголовным делам и совершенствование основ их конструирования // Законы России: опыт, анализ, практика. 2017. № 5. С. 21–29.
26. *Ситникова А.И.* Глава «Неоконченное преступление» УК РФ и ее законодательно-текстологическое обоснование // Lex russica. 2015. № 11. С. 83–95.
27. Leveraging Machine Learning for Crime Intent Detection in Social Media Posts / B.G. Bokolo, P. Onyehanere, E. Ogegbene-Ise et al. F. Zhao, D. Miao (eds) AI-generated Content. AIGC 2023 // Communications in Computer and Information Science. 2024. Vol. 1946. Springer, Singapore. — URL: https://doi.org/10.1007/978-981-99-7587-7_19
28. *Антонян Е.А., Аминов И.И.* Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6. С. 167–177.
29. Криминология: уч. для вузов. 2-е изд., перераб. и доп. / под ред. В.Д. Малкова. М.: Юстицинформ, 2006.
30. *Завьялов И.А.* Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений // Вестник Моск. ун-та МВД России. 2021. № 3. С. 228–236. DOI 10.24412/2073-0454-2021-3-228-236. EDN MWOJZD.
31. Cisco Secure Endpoint (AMP for Endpoints). — URL: https://www.cisco.com/c/en_hk/products/security/amp-for-endpoints/index.html
32. *Хисамова З.И., Бегишев И.Р.* Цифровая преступность в условиях пандемии: основные тренды //

Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 185–198. DOI 10.17150/2500-4255.2022.16(2).185-198. EDN GNPYZX.

REFERENCES

1. Ukaz Prezidenta RF ot 10 oktyabrya 2019 g. № 490 "O razvitii iskusstvennogo intellekta v Rossijskoj Federacii" (vmeste s "Nacional'noj strategiej razvitiya iskusstvennogo intellekta na period do 2030 g.") // SZ RF. 2019. No 41. St. 5700.
2. GOST R 43.0.8-2017. Nacional'nyj standart Rossijskoj Federacii. Informacionnoe obespechenie tekhniki i operatorskoj deyatel'nosti. Iskusstvenno-intellektualizirovannoe cheloveko-informacionnoe vzaimodejstvie. Obshchie polozheniya (utv. i vveden v dejstvie Prikazom Rosstandarta ot 27.07.2017 NoNº 757-st). M.: Standartinform, 2018.
3. *Korovin A.M.* Intellektual'nye sistemy: tekst lekcij. Chelyabinsk: Izdatel'skij centr YuUrGU, 2015. 60 s. URL: https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000539905&dtype=F&etype=.pdf
4. Bol'shaya rossijskaya enciklopediya. — URL: https://bigenc.ru/c/algoritm-ee5b00
5. *Zharova A.K.* Iskusstvennyj intellekt–sredstvo ili sposob soversheniya moshennichestva v sfere komp'yuternoj informacii? // Gosudarstvo i pravo. 2023. № 2. S. 54–61. DOI 10.31857/S102694520021177-5. EDN PESJQJ.
6. Ugolovnoe pravo Rossijskoj Federacii. Obshchaya chast': uch. dlya vuzov / pod red. V.S. Komissarova, N.E. Krylovoj, I.M. Tyazhkovoj. M.: Statut, 2012.
7. Polnyj kurs ugolovnogo prava / pod red. A.I. Korobeeva. T. I: Prestuplenie i nakazanie. SPb.: Ur. tsentr Press, 2008. S. 77–78.
8. Artificial Intelligence in the Context of Crime and Criminal Justice. — URL: https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf
9. *Umadevi V Navalgund, Priyadharshini K.* Crime Intention Detection System Using Deep Learning, December 2018, Conference: 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET). DOI: 10.1109/ICCSDET.2018.8821168
10. *Sretencev D.N.* Perspektivy vnedreniya sistem iskusstvennogo intellekta v sferu rassledovaniya prestuplenij / D. N. Sretencev, V. R. Volkova // Rossijskij sledovatel'. 2021. No 11. S. 38-42. DOI 10.18572/1812-3783-2021-11-38-42. EDN HLNQDU.
11. *Rastoropov S.V.* Ispol'zovanie iskusstvennogo intellekta dlya preduprezhdeniya i vyyavleniya prestuplenij (mirovoj opyt) // Mezhdunarodnoe publichnoe i chastnoe pravo. 2020. No 5. S. 40–43. DOI 10.18572/1812-3910-2020-5-40-43. EDN QPDQHX.
12. *Sukhodolov A.P, Bychkova A.M., Sukhodolov A.P.* Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution // Russian Journal of Criminology. 2018. Vol. 12, No 6. P. 753–766. DOI 10.17150/2500-4255.2018.12(6).753-766. EDN YYSTVR.
13. *Smushkin A.B.* Ekosistema predvaritel'nogo rassledovaniya // Aktual'nye problemy rossijskogo prava. 2023. No 7. S. 143–158.
14. *Yashin A.A.* Virtual'nye tekhnologii v rassledovanii prestuplenij: perspektivnye napravleniya i vozmozhnosti ispol'zovaniya // Advokatskaya praktika. 2022. No 6. S. 23–26.
15. *Gorbenko A.O., Mamasuev A.V.* Primenenie analiticheskih sistem pri prinyatii upravlencheskih reshenij v organah vnutrennih del (analiticheskie sistemy OLAP) // Vestnik Akademii ekonomicheskoj bezopasnosti MVD Rossii. 2008. No 4. S. 96–99. EDN NEFKRP.
16. Rasporyazhenie MVD Rossii ot 11 yanvarya 2022 g. No 1/37 "Ob utverzhdenii Vedomstvennoj programmy cifrovoj transformacii MVD Rossii na 2022–2024 gg." Dokument opublikovan ne byl // SPS "Konsul'tantPlyus".
17. Ukaz Prezidenta RF ot 21 dekabrya 2016 g. No 699 "Ob utverzhdenii Polozheniya o Ministerstve vnutrennih del Rossijskoj Federacii i Tipovogo polozheniya o territorial'nom organe Ministerstva vnutrennih del Rossijskoj Federacii po sub"ektu Rossijskoj Federacii" // SZ RF. 2016. No 52 (Ch. V). St. 7614.
18. *Dolgih T.N.* Priznaki prestupleniya v teorii ugolovnogo prava // SPS "Konsul'tantPlyus", 2023.
19. *Zharova A.K., Elin V.M., Minbaleev A.V.* Paradigma cifrovogo profilirovaniya deyatel'nosti cheloveka: riski, ugrozy, prestupleniya. M.: Rusajns, 2022. 240 s. ISBN 978-5-466-00766-4. EDN DNKVPR.
20. *Halikov A.N.* Germenevticheskie problemy istolkovaniya kriminalisticheskoj informacii pri rassledovanii ugolovnyh del // Rossijskij sledovatel'. 2021. No 2. S. 19–23.
21. *Rastoropov S.V.* Ispol'zovanie iskusstvennogo intellekta dlya preduprezhdeniya i vyyavleniya prestuplenij (mirovoj opyt) // Mezhdunarodnoe publichnoe i chastnoe pravo. 2020. No 5. S. 40–43.
22. *Zharova A.K.* Neobhodimo li uzhestochenie trebovanij ob obyazatel'nom obshchem monitoringe informacii provajderami hostinga? // Trudy po intellektual'noj sobstvennosti. 2022. T. 41, No 2. S. 21–29. DOI 10.17323/tis.2022.14439. EDN LXKDRR.
23. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii (postatejnyj). 7-e izd., pererab. i dop. / otv. red. A.I. Rarog). M.: Prospekt, 2011.

24. *Andrusenko S.P., Golovanova N.A., Gravina A.A.* Mezhdunarodno-pravovye standarty v ugolovnoj yusticii Rossijskoj Federacii: nauchno-prakticheskoe posobie / otv. red. V.P. Kashepov. M.: IZiSP, Ankil, 2012. 312 s.
25. *Baev O.Ya.* Kriminalisticheskie metodiki v realizacii dokazyvaniya po ugolovnym delam i sovershenstvovanie osnov ih konstruirovaniya // Zakony Rossii: opyt, analiz, praktika. 2017. No 5. S. 21–29.
26. *Sitnikova A.I.* Glava "Neokonchennoe prestuplenie" UK RF i ee zakonodatel'no-tekstologicheskoe obosnovanie // Lex russica. 2015. No 11. S. 83–95.
27. Leveraging Machine Learning for Crime Intent Detection / B.G. Bokolo, P. Onyehanere, E. Ogegbene-Ise et al. // Social Media Posts / F. Zhao, D. Miao (eds). AI-generated Content. AIGC 2023 // Communications in Computer and Information Science 2024. Vol. 1946. Springer, Singapore. — URL: https://doi.org/10.1007/978-981-99-7587-7_19
28. *Antonyan E.A., Aminov I.I.* Blokchejn-tekhnologii v protivodejstvii kiberterrorizmu // Aktual'nye problemy rossijskogo prava. 2019. No 6. S. 167–177.
29. Kriminologiya: uc. dlya vuzov. 2-e izd., pererab. i dop. / pod red. V.D. Malkova. M.: Yusticinform, 2006.
30. *Zav'yalov I.A.* Zarubezhnyj opyt ispol'zovaniya iskusstvennogo intellekta v raskrytii prestuplenij // Vestnik Moskovskogo universiteta MVD Rossii. 2021. No 3. S. 228–236. DOI 10.24412/2073-0454-2021-3-228-236. EDN MWOJZD.
31. Cisco Secure Endpoint (AMP for Endpoints). — URL: https://www.cisco.com/c/en_hk/products/security/amp-for-endpoints/index.html
32. *Hisamova Z.I., Begishev I.R.* Cifrovaya prestupnost' v usloviyah pandemii: osnovnye trendy // Vserossijskij kriminologicheskij zhurnal. 2022. T. 16, No 2. S. 185–198. DOI 10.17150/2500-4255.2022.16(2).185-198. EDN GNPYZX.