https://doi.org/10.30764/1819-2785-2024-2-76-87

Искусственный интеллект и судебная компьютерно-техническая экспертиза

Ю.С. Руденкова[1,2,3], **Ш.Н. Хазиев**[1], **А.И. Усов**[1,2,4]

[1] Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы имени профессора А.Р. Шляхова при Министерстве юстиции Российской Федерации, Москва 109028, Россия

[2] ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана», Москва 105005, Россия

[3] ФГБОУ ВО «Национальный исследовательский университет "МЭИ"», Москва 111250, Россия

[4] ФГБОУ ВО «Всероссийский государственный университет юстиции» (РПА Минюста России), Москва 117638, Россия

Аннотация. В связи с масштабной цифровизацией современного общества и быстрого внедрения технологий искусственного интеллекта (ИИ) возникла потребность криминалистического и судебно-экспертного обеспечения судопроизводства по делам, в которых фигурирует ИИ. Наиболее актуальными задачами, решаемыми судебными компьютерно-техническими экспертными подразделениями, являются исследование фактов неправомерного (главным образом криминального) использования искусственного интеллекта, использование ИИ для создания новых и совершенствования существующих методик компьютерно-технической экспертизы, судебно-экспертное исследование продуктов, использующих технологии ИИ с целью установления соответствия готового продукта техническому заданию на его создание, а также комплексное судебно-экспертное исследование с целью определения стоимости IT-продукта.

В зависимости от свойств подлежащего исследованию объекта экспертиза проводится либо в рамках судебной компьютерно-технической экспертизы, либо комплексно, с привлечением специалистов в области судебной лингвистической, судебной фоноскопической и других видов судебных экспертиз. Показательным примером совершенствования судебно-экспертных методик анализа цифровых изображений является выявление искажений в метаданных.

Ключевые слова: *автоматизация, безопасность, дипфейк, искусственный интеллект, кибератаки, мошеннические услуги, определение стоимости IT-продукта, судебная компьютерно-техническая экспертиза*

Для цитирования: Руденкова Ю.С., Хазиев Ш.Н., Усов А.И. Искусственный интеллект и судебная компьютерно-техническая экспертиза // Теория и практика судебной экспертизы. 2024. Т. 19. № 2. С. 76–87. https://doi.org/10.30764/1819-2785-2024-2-76-87

Artificial Intelligence and Computer Forensics

Yulia S. Rudenkova[1,2,3], **Shamil N. Khaziev**[1], **Alexandr I. Usov**[1,2,4]

[1] The Russian Federal Centre of Forensic Science named after professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation, Moscow 109028, Russia

[2] Bauman Moscow State Technical University, Moscow 105005, Russia

[3] National Research University "Moscow Power Engineering Institute", Moscow 111250, Russia

[4] The All-Russian State University of Justice, Moscow 117638, Russia

Abstract. As a result of large-scale digitalization of all spheres of human activity and the rapid introduction of artificial intelligence technologies, the need has arisen for forensic support for legal proceedings in cases in which artificial intelligence has a role. The most pressing tasks solved by forensic computer expert units are the study of the facts of unlawful (mainly criminal) use of artificial intelligence, the use of artificial intelligence to create new and improve existing methods of computer forensics, forensic analysis of products using artificial intelligence technologies in order to establish compliance of the final product with the technical specifications for its creation, as well as a comprehensive forensic study to determine the cost of an IT product. Depending on the properties of the object to be examined,

the analysis is carried out either within a forensic computer examination, or comprehensively, with the involvement of specialists in the field of forensic linguistics, forensic phonoscopic and other types of examinations. Identifying distortions in metadata is an illustrative example of improving forensic methods for analyzing digital images using artificial intelligence technology.

Keywords: *automation, security, deepfake, artificial intelligence, cyberattacks, fraudulent services, determining the cost of an IT product, forensic computer analysis*

For citation: Rudenkova Yu.S., Khaziev Sh.N. Usov A.I. Artificial Intelligence and Computer Forensics. *Theory and Practice of Forensic Science.* 2024. Vol. 19. No. 2. P. 76–87. (In Russ.).
https://doi.org/10.30764/1819-2785-2024-2-76-87

Введение

Судебная компьютерно-техническая экспертиза (СКТЭ) является самостоятельным родом судебной экспертизы. Она включает в себя исследования компьютерных средств, в том числе электронных носителей информации, и систем, обеспечивающих реализацию информационных процессов, для установления фактических данных, имеющих доказательственное значение в процессе судопроизводства[1].

Активное внедрение технологий, основанных на использовании ИИ, неизбежно порождает необходимость изучения его свойств, признаков и их отображений специалистами в области СКТЭ.

Алгоритмы искусственного интеллекта могут анализировать большие объемы мультимедийного контента – быстро идентифицировать людей по лицам, объекты или текст на изображениях и видео, тем самым значительно ускоряя процесс поиска и извлечения важных данных, необходимых для решения задач экспертизы. Перечень областей потенциального применения ИИ в криминалистике будет расширяться с появлением новых возможностей искусственного интеллекта в области анализа данных, распознавания образов и обнаружения аномалий.

В настоящий момент для СКТЭ большой интерес представляют объекты IoT – Интернета вещей (разного рода «умная» техника промышленного и бытового применения), облачные сервисы хранения информации, 3D-принтеры и некоторые другие технологии производства и обработки информации, в том числе с применением ИИ [1].

Развитие судебной компьютерно-технической экспертизы тесно связано с развитием современных цифровых технологий и в значительной степени определяется им. Однако судебно-экспертные исследования технологий искусственного интеллекта в системе Минюста России сейчас ограничиваются решением вопросов определения стоимости программных продуктов, основанных на нейросетях и ИИ, которые возникают по уголовным делам о хищении бюджетных средств, направляемых на развитие и внедрение IT-технологий.

В судебной компьютерно-технической экспертизе существуют четыре направления, связанных с большими данными и искусственным интеллектом.

1. Исследование фактов неправомерного (главным образом криминального) использования ИИ.
2. Использование ИИ для создания новых и совершенствования существующих методик судебной компьютерно-технической экспертизы.
3. Судебно-экспертное исследование продуктов, использующих технологии ИИ, с целью установления соответствия готового продукта техническому заданию на его создание.
4. Комплексное судебно-экспертное исследование с целью определения стоимости IT-продукта.

В зависимости от свойств подлежащего исследованию объекта экспертиза проводится либо в рамках СКТЭ, либо комплексно, с привлечением специалистов в области судебной лингвистической, судебной фоноскопической и других видов судебных экспертиз (портретной, трасологической, экономической, почерковедческой и др.).

Общая характеристика способов неправомерного (главным образом криминального) использования ИИ

При расследовании любого преступления или административного правонару-

[1] ГОСТ Р 71232-2024. Национальный стандарт Российской Федерации. Роды судебных экспертиз. Термины и определения (утв. и введен в действие Приказом Росстандарта от 05.02.2024 № 193-ст) // КонсультантПлюс.

шения, совершенного с использованием искусственного интеллекта, может потребоваться проведение СКТЭ. В литературе по цифровой криминалистике приведено более двадцати способов совершения преступлений или административных правонарушений с использованием возможностей ИИ [2], перечислим некоторые из них.

Аудио/визуальная выдача себя (или иного лица) за другое лицо. Преступники выдают себя за отдельных лиц посредством убедительных аудио- или видеоманипуляций, что потенциально может привести к финансовому мошенничеству или манипулированию общественным мнением, опасным провокациям. Такие действия называют «пранк» (от англ. *prank* – «шалость, выходка, розыгрыш, шутка, проказа»), а их авторов – пранкерами.

Розыгрыши провокационного характера часто записывают и размещают в интернете. Аудио- или видео- манипуляции, созданные с применением этой технологии для целей мошенничества, иногда записываются жертвами преступлений и тогда они могут стать объектом судебно-экспертного исследования, главным образом комплексного компьютерно-технического и фоновидеоскопического или лингвистического, иногда с включением в комиссию судебного эксперта-психолога.

Использование беспилотных транспортных средств в качестве оружия или орудия совершения различных видов преступлений. Автономные дроны, управляемые ИИ, облегчают преступную деятельность, позволяя злоумышленнику находиться на недосягаемом расстоянии. Беспилотники используются для противозаконного негласного наблюдения за потенциальной жертвой, для доставки запрещенных предметов и веществ в места лишения свободы и даже для контрабандных поставок за границу.

Появление автономных транспортных средств позволяет террористам осуществлять скоординированные атаки без участия человека. Примером применения дронов-убийц с искусственным интеллектом является турецкая разработка Kargu-2. Квадрокоптер Kargu-2 может автономно отслеживать и уничтожать человеческие цели на основе распознавания лиц. Это большой технологический скачок по сравнению с парками дронов, требующих дистанционного управления со стороны людей-операторов.

В докладе Совета Безопасности ООН утверждается, что Kargu-2 использовался в Ливии для организации автономных атак: Kargu-2 выслеживал отступающие логистические и военные конвои, «атакуя цели, не требуя передачи данных и связи между оператором и боеприпасом»[2].

В онлайн-базе данных IMDb[3] размещен сериал «Дроны-убийцы»[4] с ограничением по возрасту 12+.

В случаях беспилотных транспортных средств объектами СКТЭ являются используемые в них компьютерные технические средства и программы, в том числе технологии искусственного интеллекта.

Специализированный фишинг. Фишинговые атаки, управляемые искусственным интеллектом, способны создавать крайне убедительные сообщения, что затрудняет обнаружение различий между подлинными и ложными, часто вредоносными, сообщениями.

Генеративный ИИ позволяет сделать традиционные фишинговые атаки (через электронную почту, прямые сообщения и поддельные веб-сайты) более реалистичными, устраняя орфографические и грамматические ошибки и убедительно применяя профессиональные стили письма. Большие языковые модели (англ. *large language models, LLM*) поглощают информацию в режиме реального времени из новостных агентств, корпоративных веб-сайтов и других источников. Включение актуальных подробностей в фишинговые электронные письма делает сообщения более правдоподобными и создает ощущение срочности, заставляя жертв действовать.

Чат-боты с искусственным интеллектом могут создавать и распространять компрометацию деловой электронной почты и другие фишинговые кампании гораздо быстрее правонарушителей-одиночек, что

[2] Заключительный доклад Группы экспертов по Ливии, учрежденной резолюцией Совета Безопасности. Документ Совета Безопасности ООН S/2021/229 от 08.03.2021.

[3] *Internet Movie Database (IMDb)* – веб-сайт со свободно редактируемой и крупнейшей в мире базой данных о кинематографе.

[4] «Дро́ны-Уби́йцы» (от англ. *Murder Drones*) – австралийско-американо-канадский компьютерно-анимационный веб-сериал в жанре комедийного хоррора. Премьера пилотного эпизода состоялась на YouTube-канале GLITCH 29.10.2021. Сериал рассчитан на сезон из 8 серий, который официально начался 18.11.2022.

увеличивает зону воздействия атак. Генеративный ИИ способен за считанные секунды собирать и обрабатывать конфиденциальную информацию об организации или человеке для создания целенаправленных и убедительных сообщений и даже фейковых телефонных звонков и видео.

Нарушение систем, контролируемых искусственным интеллектом. Поскольку системы ИИ становятся неотъемлемой частью значимых для общества секторов, злоумышленники атакуют их, вызывая хаос, сбои в электроснабжении или финансовые потрясения. Тогда задачей судебной компьютерно-технической экспертизы является выявление и исследование способов противоправного воздействия на интеллектуальную составляющую пострадавшей системы, использованных для этого программных и технических средств.

Масштабный шантаж. Искусственный интеллект может облегчить сбор данных и выявление уязвимостей личности, что делает шантаж более масштабным и высокотехнологичным.

Традиционный шантаж предполагает вымогательство под угрозой раскрытия доказательств преступного или иного противоправного, аморального деяния или компрометирующей личной информации. Ограничивающим фактором при этом является стоимость получения таких доказательств: преступление оправдано только в случае, если жертва заплатит за сокрытие доказательств больше, чем стоит их приобретение.

ИИ делает возможным масштабный сбор информации (которая сама по себе не обязательно должна представлять собой убедительные доказательства) из социальных сетей или больших наборов личных данных, таких как журналы электронной почты, из истории браузеров, содержимого жестких дисков или телефонов, а затем выявление конкретных уязвимостей для большого количества потенциальных целей и адаптацию сообщений об угрозах для каждой.

ИИ может быть использован и для создания фальшивых доказательств, например, когда обнаруженная информация предполагает наличие уязвимости без предоставления достаточных доказательств [3].

Подобный шантаж высоко прибылен: как и в случае с фишингом, экономия на масштабе означает, что для прибыльной атаки достаточно низкого процента попаданий.

Создание сфальсифицированных материалов (фейков, дипфейков и т. п.). Искусственный интеллект используется злоумышленниками для создания фальшивых (фейковых) новостей [4], дипфейков (синтезированных поддельных изображений, поддельных голосов), фейковых аукционов [5], фальшивых географических карт[5].

Новости, созданные с помощью искусственного интеллекта, позволяют манипулировать общественным восприятием, хотя и не всегда напрямую приносят финансовую прибыль. В то же время известны случаи, когда фейковые новости о предстоящих банкротствах или акциях в отношении финансовых структур приводили к значительным негативным экономическим последствиям для потерпевших с одновременной выгодой для организовавших данные фейки криминальных структур.

Дезинформаторы используют генеративный ИИ для создания недорогого фейкового контента, и эксперты полагают, что это позволяет вводить общественность в заблуждение лучше контента, созданного людьми.

В рамках судебной компьютерно-технической экспертизы могут решаться вопросы о создании фейков: что фотографии, аудиозаписи, видеозаписи были изготовлены, либо в их оригиналы были внесены изменения с использованием технологий ИИ.

По данным А.А. Бессонова методы установления следов некоторых из информационных технологий, которые использовались при изготовлении фальсифицированных объектов, уже разработаны [6].

Неправомерное использование военных роботов. Использование военного оборудования с искусственным интеллектом преступными или террористическими организациями представляет серьезную угрозу, хотя ее масштабы пока остаются неопределенными.

«Змеиное масло». В настоящее время различные компании часто рекламируют решения, принятые на основе ИИ. При этом возникают вопросы относительно того, действительно ли эти решения используют

[5] Вопросы выявления методами СКТЭ карт, созданных с помощью ИИ, были детально рассмотрены группой американских исследователей [7].

искусственный интеллект, и если да, то полезно ли это на самом деле.

Мошеннические услуги, маскирующиеся под решения на основе применения ИИ, могут обмануть организации, но осведомленность об истинных возможностях и характеристиках искусственного интеллекта позволяет смягчить эту угрозу[6]. Свое название этот вид мошенничества получил благодаря появившемуся в 19 веке и до сих пор распространенному обману покупателей лекарственных средств. Им предлагались средства, якобы содержащие змеиное масло (жир), в то время как такого продукта в большинстве рекламируемых товаров не содержалось. Обман о наличии в составе лекарства змеиного масла позволял существенно увеличить цену товара.

Авторы книги «AI Snake Oil» («Змеиное масло искусственного интеллекта»), ученые-компьютерщики Арвинд Нараянан и Саяш Капур, анализируют многочисленные способы введения потребителей ИИ в заблуждение, показывая, как действительно работает искусственный интеллект. Они объясняют, где он может быть полезен, а где – вреден, и когда следует подозревать, что компании используют шумиху вокруг ИИ для продажи своих товаров, которые на самом деле не приносят пользу потребителям.

Признавая потенциал некоторых моделей искусственного интеллекта, таких как ChatGPT, авторы разоблачают утверждения о возможностях ИИ и описывают вред, который искусственный интеллект уже наносит в образовании, медицине, найме, банковском деле, страховании и уголовном правосудии. В книге объясняются принципиальные различия между типами ИИ, причины любви организаций к ИИ, почему ИИ не может исправить социальные сети, почему он не представляет экзистенциального риска и почему мы должны гораздо больше беспокоиться о том, что будут делать люди с ИИ, чем что-либо, что искусственный интеллект будет делать сам по себе. Книга также предупреждает об опасностях мира, в котором ИИ продолжает контролироваться по большей части неподотчетными государству и обществу крупными технологическими компаниями [8].

Аромат «змеиного масла» чаще всего возникает при использовании программного обеспечения (ПО) для автоматизации, поэтому устранение ошибочного представления о том, что программное обеспечение для автоматизации – это ИИ, может помочь снизить распространенность данного явления. Автоматизация бизнес-процессов – система, основанная на правилах, существующая уже около десяти лет. ПО работает по правилам, которые вы должны ему сообщить, при этом правила имеют тенденцию принимать форму утверждений «если это, то – то». После настройки ПО для автоматизации может показаться интеллектуальным, однако оно не изучает и не понимает данные; оно всегда делает только то, что ему поручено (что заложено в нем изначально).

Между тем, искусственный интеллект является родственником автоматизации, но его внедрение обходится гораздо дороже. Подобно автоматизаци ИИ выполняет задачи без вмешательства человека. Но если автоматизация отлично подходит для администрирования и простых процессов, искусственный интеллект полезен для важных задач, требующих принятия решений.

Искусственный интеллект не полагается на правила, которые ему указывают, скорее он использует машинное обучение для обработки и своего дальнейшего совершенствования на массивах данных, которые ему предоставляют. Идея состоит в том, что ИИ имитирует человеческий мозг, таким образом, он решает задачи приблизительно на том же уровне, что и человек.

«Отравление данных». Речь идет о преднамеренном манипулировании данными, предназначенными для машинного обучения ИИ. Это состязательная атака, заключающаяся в использовании серии приемов, призванных нарушить работу моделей машинного и глубокого обучения.

При умелом использовании метод предоставляет злоумышленнику своеобразный бэкдор[7] к моделям машинного обучения,

[6] «Змеиное масло» – термин, используемый для описания вводящего в заблуждение маркетинга, мошенничества в сфере здравоохранения или жульничества. Аналогично, «продавец змеиного масла» – это распространенное выражение, используемое для обозначения того, кто продает, продвигает или является сторонником какого-либо бесполезного или мошеннического лекарства, средства или решения.

[7] Бэкдор, тайный вход (от англ. *back door* – «черный ход», «лазейка», букв. «задняя дверь») – дефект алгоритма, который намеренно встраивается в него разработчиком/злоумышленником и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.

через который можно обойти защиту систем, управляемых алгоритмами ИИ [9].

Кибератаки, основанные на обучении (разработка продвинутого вредоносного программного обеспечения). ИИ позволяет осуществление конкретных и масштабных кибератак с одновременной проверкой на уязвимость не одной, а нескольких систем.

Злоумышленники используют ИИ для создания более совершенных вредоносных программ, которые труднее обнаружить. Так, они могут использовать алгоритмы машинного обучения для создания вредоносного программного обеспечения, которое самооптимизируется в зависимости от реакции среды, которую оно пытается заразить, таким образом уклоняясь от систем, обычно используемых для его обнаружения (антивирусов).

Выселение через Интернет (онлайн-выселение). Отказ в доступе к основным онлайн-услугам (к компьютерным/онлайн-ресурсам, например, банкам, кредитным картам, коммунальным услугам) может быть использован для вымогательства или создания хаоса.

Обман распознавания лиц. Чтобы избежать обнаружения или обойти системы безопасности, преступники используют системы распознавания лиц, управляемые ИИ, применяя такие методы, как морфинг[8].

Рыночная бомбардировка. Манипулирование финансовыми рынками с помощью ИИ является сложным и дорогостоящим занятием, что делает его проблемой средней степени важности.

Использование предвзятости. Имеется в виду использование ИИ существующих предвзятостей в различных алгоритмах.

Боты-взломщики. Небольшие автономные роботы, используемые для краж со взломом.

Уклонение от обнаружения искусственным интеллектом. Подрыв систем ИИ, используемых правоохранительными органами или службами безопасности.

Поддельные обзоры, созданные ИИ. Создание поддельного контента для манипулирования оценками отзывов.

Преследование с помощью искусственного интеллекта (***AI-assisted stalking***)**.** Это мониторинг местонахождения и активности людей. В качестве инструмента наблюдения ИИ может позволить правонарушителям отслеживать и контролировать потенциальных жертв с большей легкостью и точностью.

Алгоритмы на базе искусственного интеллекта позволяют, например, анализировать и прогнозировать передвижения человека, собирая данные из множества источников: сообщений в социальных сетях, фотографий с геотегами и т. д., чтобы в нужный момент знать о местоположении жертвы и ее наиболее вероятных маршрутах.

Усовершенствованная технология распознавания лиц, основанная на ИИ, гораздо эффективнее человека проводит идентификацию по изображениям или видео; даже если качество низкое, или человек частично скрыт.

Сталкеры могут отслеживать жертв в режиме реального времени с помощью камер наблюдения, социальных сетей и других онлайн-источников. Известны случаи, когда они использовали услуги нечистоплоных сотрудников правоохранительных органов, имевших доступ к соответствующим базам данных.

Программное обеспечение на базе ИИ анализирует огромные объемы данных в считанные секунды, позволяя сталкерам следить и за онлайн-деятельностью своих жертв. Отслеживая цифровой след людей, от истории просмотров до электронных писем и загрузок, злоумышленники получают представление об их повседневной жизни и используют эту информацию для манипулирования, контроля, принуждения или шантажа.

Искусственный интеллект может быть направлен даже на автоматизацию и масштабирование процессов манипулирования, отслеживая взаимодействия, выявляя закономерности в публикациях и даже анализируя настроение и эмоции жертвы. Это может быть использовано злоумышленни-

[8] Морфинг (от англ. *morphing* – «трансформация») – технология в компьютерной анимации, визуальный эффект, создающий впечатление плавной трансформации одного объекта в другой. Используется в кино и рекламе. Реализуется трех- и двухмерной (как растровой, так и векторной) графикой.

ками или даже мошенниками для поиска подходящих жертв [10].

Наблюдение за местом совершения террористического акта. Для планирования и подготовки террористического акта требуются длительные периоды наблюдения, особенно в случае крупномасштабных атак. Террористические группы ведут наблюдение как за конкретными площадками, так и за людьми, посещающими их, чтобы определить пригодность цели для атаки, выявить слабые стороны, которые можно использовать для ее облегчения. Традиционно это делается в ходе пеших наблюдений, съемки из припаркованной машины, онлайн – через социальные сети, и может занимать недели, месяцы и даже годы.

Развитие возможностей наблюдения и целенаправленного сбора информации с помощью ИИ позволяет сократить значительную часть трудоемких аспектов наблюдения. С помощью искусственного интеллекта террористы могут, например, контролировать места и отслеживать перемещения людей, идентифицировать целевые лица и активы, а также автоматически и удаленно оценивать меры физической безопасности в целевом месте [11, с. 43].

Подделка произведений искусства и других культурных ценностей. Это создание с помощью искусственного интеллекта поддельного контента в изобразительном искусстве, музыке, литературе. Современные технологии позволяют изготавливать подделки работ известных мастеров путем обучения ИИ на базе большого количества подлинных произведений с последующей 3D-печатью с использованием подобранных материалов, соответствующих нужному периоду времени и предпочтениям копируемого автора.

В судах уже рассматриваются споры, связанные с незаконным использованием манеры и сюжетов, созданных искусственным интеллектом на основе произведений современных наиболее востребованных художников и дизайнеров.

Использование ИИ для создания новых и совершенствования существующих методик судебной компьютерно-технической экспертизы

С развитием информационных технологий для расследования, судебно-экспертной деятельности и судебного разбирательства велика вероятность, что в рамках СКТЭ вскоре потребуются отдельные методические разработки, основанные на технологиях ИИ.

С помощью алгоритмов машинного обучения искусственный интеллект может в процессе проведения судебной компьютерно-технической экспертизы распознавать незаметные для человеческого глаза закономерности и аномалии в огромных наборах данных. При этом предполагается, что интеграция ИИ в экспертные технологии способна не только повысить эффективность и скорость производства судебной экспертизы, но также минимизировать человеческие ошибки и предвзятости при проведении исследования и формулировании выводов.

Эта трансформация, по мнению многих исследователей, приведет к более точным и надежным выводам и, следовательно, к обеспечению более справедливого судебного разбирательства. Однако не все так однозначно.

Несмотря на большой потенциал, использование моделей искусственного интеллекта в СКТЭ сопряжено с различными рисками. Например, некоторые риски использования LLM включают в себя предвзятость или ошибки обучающих данных, галлюцинации, юридические и этические проблемы, затруднения в обеспечении объяснимости полученных результатов, определения степени достоверности выводов и технические ограничения.

Проблема использования ИИ в судебной компьютерно-технической экспертизе заключается в отсутствии прозрачности, которая положила начало обсуждению «объяснимого интеллекта» [12]. Решение этой проблемы важно, поскольку прозрачность и, что более важно, цепочка сохранности имеют решающее значение для определения допустимости доказательств в суде.

Технологии искусственного интеллекта, предназначенные для обработки естественного языка (NLP), позволяют анализировать соответствующую информацию из больших объемов текстовых данных. Например, текстовые данные, включая электронные письма, журналы чатов и документы, часто содержат ценные доказательства. Использование экстрактивных[9] функций ИИ может быть более эффективным и точным для вы-

[9] Суммаризация – это процесс получения резюме на основе данного текста. Экстрактивная суммаризация использует только предложения из текста.

явления взаимосвязей, установления закономерностей и идентификации ключевых лиц во время исследований объектов содержащих большие объемы текстовых материалов [13].

Методики и программное обеспечение исследования больших данных в цифровой криминалистике детально рассмотрены авторами получившей большую популярность двухтомной книги, австралийскими специалистами Дарреном Квиком и Ким-Кван Рэймондом Чу [14, 15].

Другим показательным примером совершенствования судебно-экспертных методик анализа цифровых изображений является выявление искажений в метаданных (атрибутах файла). ИИ может анализировать метаданные изображения, такие как информацию о камере, дате и времени съемки, а также истории изменений файла.

Анализ цифрового следа позволяет обнаруживать историю и метаданные изображений для выявления возможности манипуляций. Когда выполняется съемка, цифровая камера сохраняет информацию о настройках, таких как модель камеры, фокусное расстояние, выдержка, диафрагма и ISO. Эта информация называется EXIF-данными (*Exchangeable Image File Format*), которая также содержит данные о дате и времени съемки и создании фотография.

Если метаданные указывают на то, что изображение было изменено после фиксации его камерой, это может быть признаком монтажа.

Помимо EXIF-данных, анализ цифрового следа также может включать рассмотрение других метаданных, таких как GPS-координаты (указывает на местоположение съемки) или информацию о хранении файла (указывает на историю изменений и редактирования). Несоответствия и противоречия в метаданных или некорректная информация могут быть признаками возможных манипуляций. Кроме того, изображения, измененные с помощью различных редакторов, могут иметь аномалии в форме и перспективе.

ИИ позволяет анализировать геометрические детали изображения, такие как искажения в перспективе, аномалии в пропорциях объектов или несоответствия в линейных структурах.

Таким образом, можно выделить следующие возможности ИИ по экспертному анализу изображений и их метаданных:

1. Определение перспективы: искусственный интеллект может использовать методы, такие как восстановление глубины сцены или анализ соотношения сторон объектов для определения соблюдения перспективы в редактированном изображении. Любое несоответствие в перспективе может указывать на то, что изображение было изменено.

2. Обнаружение аномалий в форме: методы компьютерного зрения могут анализировать форму объектов на изображении, сравнивая их с заранее заданными моделями или с примерами из обучающей выборки. Если форма объекта не выглядит натуральной или пропорции выглядят неправильными, это может быть признаком того, что изображение было отредактировано.

3. Детектирование несоответствий в линейных структурах: если два объекта, которые должны быть параллельными или перпендикулярными в реальном мире, не сохраняют эту свойственность на изображении, это может указывать на искажение.

С помощью таких технологий как GAN (генеративно-состязательные сети) искусственный интеллект может «воспроизвести» те участки изображения, которые были искажены или удалены, что делает его важным инструментом для распознавания и восстановления искаженных изображений. Редакторы могут использоваться для изменения освещения и добавления или удаления теней на изображении. ИИ анализирует различные уровни яркости, консистентность освещения и наличие артефактов вокруг объектов, которые могут указывать на редактирование изображения.

Кроме того, искусственный интеллект может распознавать признаки редактирования изображения путем анализа уровня освещения и тени. ИИ анализирует различные уровни яркости, консистентность освещения и наличие признаков вокруг объектов, которые указывают на вероятность изменения изображения с помощью определенного инструмента для редактирования изображений.

При сохранении изображения после редактирования могут возникать признаки сжатия, такие как блокирование или неравномерности в качестве изображения. Для обнаружения признаков сжатия, ИИ использует различные методы машинного обучения и компьютерного зрения. Например, алгоритмы глубокого обучения могут быть использованы на большом наборе данных с

известными артефактами сжатия для распознавания их с высокой точностью.

ИИ анализирует изображение пиксель за пикселем для поиска специфических структур и шаблонов, которые характеризуют признаки сжатия. Например, блокирование может проявляться в виде четко выделенных квадратных областей с нереалистичными переходами между цветами. ИИ позволяет анализировать такие области, применять статистические методы и сравнивать со знакомыми моделями блокирования для определения вероятности присутствия признака монтажа.

Для обучения нейросети распознавать характерные признаки монтажа необходимо подготовить достаточное количество обучающих изображений, которые включают как оригинальные, так и отредактированные фотографии. В процессе обучения, нейросеть будет настраивать свои веса таким образом, чтобы максимально точно предсказывать, отредактировано ли изображение или нет. После обучения, нейросеть может быть использована для классификации новых изображений на оригинальные и отредактированные.

Однако нейронные сети не всегда могут быть абсолютно надежными в распознавании изменений, связанных с редакторами изображений. Некоторые современные методы редактирования достаточно сложны для распознавания, и нейросеть может допускать ошибки. Поэтому, важно использовать несколько моделей и при необходимости проводить дополнительные проверки, чтобы добиться максимальной точности классификации.

Таким образом, выявление монтажа с помощью искусственного интеллекта является важным и необходимым шагом в борьбе с фальсификацией изображений. Благодаря развитию технологий машинного обучения и компьютерного зрения, ИИ может автоматически обнаруживать изменения и ретушировку на фотографиях, что позволяет сохранять достоверность и подлинность изображений. Это важно для всех пользователей социальных сетей, где распространение фейковых фотографий может привести к негативным последствиям.

Развитие судебно-экспертных технологий выявления монтажа искусственным интеллектом является важным шагом в повышении эффективности использования специальных знаний в защите от дезинформации и сохранении доверия к визуальным материалам, в том числе имеющим доказательственное значение.

Судебно-экспертное исследование продуктов, использующих технологии ИИ с целью установления соответствия готового продукта техническому заданию на его создание

Такая задача ставится перед экспертами по делам, связанным как с гражданско-правовыми спорами юридических лиц относительно соответствия программного продукта указанным в техническом задании требованиям, так и с обвинениями владельцев или руководителей организаций-разработчиков в совершении экономических преступлений или мошенничества. Определенные наработки в этом направлении и реальный практический опыт уже накоплен в отделе судебной компьютерно-технической экспертизы ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России.

Решение этой судебно-экспертной задачи является весьма трудоемкой и требует использования широкого спектра знаний и практического опыта. В результате накопления необходимых сведений, создания соответствующих справочно-информационных фондов, обобщения посвященных вопросам создания программных продуктов научных публикаций, появится возможность разработки и внедрения соответствующих алгоритмов и моделей машинного обучения и применения технологий ИИ.

Судебно-экспертное исследование IT-продукта с целью определения его стоимости

Практика применения технологий и инструментов, созданных на основе искусственного интеллекта, показывает их высокую эффективность. Это в свою очередь вызывает повышение спроса на такие инструменты в самых различных сферах – от медицины до журналистики и шоу-бизнеса.

Технологии ИИ – дорогостоящий продукт, требующий значительных финансовых инвестиций. Это касается как производства, так и платной подписки. Только крупные компании имеют возможности инвестирования в дорогостоящие технологии и разработки собственных алгоритмов.

Решение этой судебно-экспертной задачи требует знания технологий и экономики создания продуктов, содержащих искусственный интеллект. Поэтому такие экспертизы должны проводиться комплексно,

с привлечением специальных знаний в области экономики IT-отрасли.

Стоимость продукта складывается из нескольких основных составляющих:

Трудозатраты. Любая команда, занимающаяся разработкой искусственного интеллекта, будет включать в себя большое количество важных ролей, например, специалист по данным, инженер по машинному обучению, разработчик ИИ, разработчики программного обеспечения и руководитель проекта. Стоимость каждого участника варьируется в зависимости от навыков и опыта. И в зависимости от членов команды, привлеченных в проект, его общая стоимость также будет варьироваться. Даже в малом бизнесе стоимость команды разработчиков ИИ может достигать более 320 тыс. долларов в год.

Продолжительность проекта. Стоимость разработки искусственного интеллекта зависит от продолжительности создания программного обеспечения. Продолжительность будет зависеть от всех факторов, рассмотренных выше. Например, создание базовой версии ИИ обойдется дешевле и потребует меньше времени по сравнению с версией MVP[10].

Независимо от того, используется ли аутсорсинг или собственная команда, увеличение продолжительности означает, что участникам придется уделять больше времени и усилий, что приведет к увеличению конечной стоимости.

По данным американской компании RisingMax, приблизительная стоимость разработки ИИ в 2024 г. будет следующей:

Стоимость программного обеспечения 30–45 тыс. долларов США; стоимость трудозатрат 25–49 долларов в час; стоимость обучения и обслуживания 8 999–14 999 долларов США.

Расходы в зависимости от размера компании, нанимаемой для разработки ИИ:

– небольшая компания – от 20 до 45 тыс. долларов США;

– компания среднего размера – от 50 до 100 тыс. долларов США;

– крупная компания – от 100 до 150 тыс. долларов США.

Стоимость продукта в зависимости от уровня сложности:

– низкоуровневый сложный ИИ – 15–35 тыс. долларов США;

– сложный ИИ среднего уровня – 40–60 тыс. долларов США;

– сложный ИИ высокого уровня – 80–100 тыс. долларов США[11].

Данный пример расчета стоимости создания продукта на основе искусственного интеллекта является ориентировочным и может применяться лишь с учетом особенностей отечественной IT-индустрии и соответствующих экономических показателей.

Заключение

В настоящее время внедрение технологий ИИ в практику судебной компьютерно-технической экспертизы происходит достаточно быстро.

Технологии искусственного интеллекта неизбежно завоевывают «территорию» судебных экспертиз и судебной компьютерно-технической экспертизы в частности. Помимо указанных и исследованных в данной статье направлений использования ИИ в судебной компьютерно-технической экспертизе закономерно возникнут и другие направления, обусловленные появлением новых актуальных задач судопроизводства [16].

Представляется важным и тот факт, что распространение технологий искусственного интеллекта в других родах и видах судебной экспертизы повлечет расширение спектра комплексных экспертиз и исследований с привлечением лиц, обладающих специальными знаниями в области СКТЭ.

В процессе апробации и внедрения технологий ИИ в судебно-экспертную деятельность следует критически относиться к многочисленным рекламным материалам производителей и распространителей соответствующих коммерческих продуктов, предназначенных для проведения экспертиз. Это обусловлено тем, что, во-первых, в значительном числе случаев возможности и достоверность получаемых с помощью таких технологий результатов существенно завышено, а во-вторых, пока не выработаны и не проверены методы и средства объективной оценки использованных при создании конечного продукта баз данных и алгоритмов машинного обучения.

[10] *Minimal Viable Product* (минимально жизнеспособный продукт) – тестовая версия товара, услуги или сервиса с минимальным набором функций (иногда даже одной), которая представляет ценность для конечного потребителя. MVP создают для тестирования гипотез и проверки жизнеспособности задуманного продукта, насколько он будет ценным и востребованным на рынке.

[11] How Much Does AI Cost In 2024 // RisingMax. 05.01.2024. https://risingmax.com/blog/how-much-does-artificial-intelligence-cost

СПИСОК ЛИТЕРАТУРЫ

1. Завьялова Д.В. Современные возможности судебной компьютерно-технической экспертизы при расследовании различных видов преступлений // Теория и практика судебной экспертизы. 2020. Т. 15. № 3. С. 89–97. https://doi.org/10.30764/1819-2785-2020-3-89-97
2. Miralis N.G. AI-enabled Future Crime: Study Reveals 20 Disturbing Possibilities // Lexology. 11.10.2023. https://www.lexology.com/library/detail.aspx?g=93ff642e-0026-4f99-ba79-0fae4114ded5
3. Peters K.M. 21st Century Crime: How Malicious Artificial Intelligence Will Impact Homeland Security. Monterey: Naval Postgraduate School (U.S.). Center for Homeland Defense and Security, 2019. 99 p.
4. Burkhardt J.M. Chapter 1. History of Fake News // Library Technology Reports. 2017. Vol. 53. № 8. P. 5–9.
5. Nabeth T. Virtual Online Social Environments, Real Digital Identities Issues // Identity in a Networked World: Use Cases and Scenarios. Bern: Computer Science Division, Berne University of Applied Sciences, 2006. P. 8–9.
6. Бессонов А.А. Перспективы использования технологии искусственного интеллекта в экспертно-криминалистической деятельности // Судебная экспертиза и исследования. 2022. № 1. С. 16–21.
7. Zhao B., Zhang Sh., Xu Ch., Sun Y., Deng Ch. Deep Fake Geography? When Geospatial Data Encounter Artificial Intelligence // Cartography and Geographic Information Science. 2021. Vol. 48. № 4. P. 1–15. https://doi.org/10.1080/15230406.2021.1910075
8. Narayanan A., Kapoor S. AI Snake Oil: What Artificial Intelligence Can Do, What It Can't, and How to Tell the Difference. Princeton: Princeton University Press, 2024. 360 p.
9. Caldwell M., Andrews J.T.A., Tanay T., Griffin L.D. AI-enabled Future Crime // Crime Science. 2020. Vol. 9. № 14. P. 1–13. https://doi.org/10.1186/s40163-020-00123-8
10. Goldberg C.A. AI in the Hands of Stalkers, Abusers and Traffickers: A New Frontier in Victims' Rights // C.A. Goldberg. Victims' Rights Law Firm. 22.04.2023. https://www.cagoldberglaw.com/ai/
11. Algorithms and Terrorism. The Malicious Use of Artificial Intelligence for Terrorist Purposes. A Joint Report by UNICRI and UNCCT. Turin: UNICRI, 2021. 57 p.
12. Kelly L., Sachan S., Ni L., Almaghrabi F., Allmendinger R., Chen Y.-W. Explainable Artificial Intelligence for Digital Forensics: Opportunities, Challenges and a Drug Testing Case Study // Digital Forensic Science. 2020. https://doi.org/10.5772/intechopen.93310
13. Азаренко Н.Ю. Экстрактивная суммаризация научных текстов // Актуальные вопросы техники, науки, технологии. Сборник научных трудов национальной конференции (Брянск, 08–12 февраля 2022 года) / Под общей ред. Т.Э. Сергутиной. Брянск: Брянский государ-

REFERENCES

1. Zav'yalova D.V. Current Capacities of Digital Forensics for Investigations of Different Types of Crimes. *Theory and Practice of Forensic Science.* 2020. Vol. 15. No. 3. P. 89–97. (In Russ.). https://doi.org/10.30764/1819-2785-2020-3-89-97
2. Miralis N.G. AI-enabled Future Crime: Study Reveals 20 Disturbing Possibilities. *Lexology.* 11.10.2023. https://www.lexology.com/library/detail.aspx?g=93ff642e-0026-4f99-ba79-0fae4114ded5
3. Peters K.M. *21st Century Crime: How Malicious Artificial Intelligence Will Impact Homeland Security.* Monterey: Naval Postgraduate School (U.S.). Center for Homeland Defense and Security, 2019. 99 p.
4. Burkhardt J.M. Chapter 1. History of Fake News. *Library Technology Reports.* 2017. Vol. 53. No. 8. P. 5–9.
5. Nabeth T. *Virtual Online Social Environments, Real Digital Identities Issues. Identity in a Networked World: Use Cases and Scenarios*. Bern: Computer Science Division, Berne University of Applied Sciences, 2006. P. 8–9.
6. Bessonov A.A. Prospects for the Use of Artificial Intelligence Technology in Forensic Activities. *Forensic science and research.* 2022. No. 1. P. 16–21. (In Russ.).
7. Zhao B., Zhang Sh., Xu Ch., Sun Y., Deng Ch. Deep Fake Geography? When Geospatial Data Encounter Artificial Intelligence. *Cartography and Geographic Information Science*. 2021. Vol. 48. No. 4. P. 1–15. https://doi.org/10.1080/15230406.2021.1910075
8. Narayanan A., Kapoor S. *AI Snake Oil: What Artificial Intelligence Can Do, What It Can't, and How to Tell the Difference*. Princeton: Princeton University Press, 2024. 360 p.
9. Caldwell M., Andrews J.T.A., Tanay T., Griffin L.D. AI-enabled Future Crime. *Crime Science.* 2020. Vol. 9. No. 14. P. 1–13. https://doi.org/10.1186/s40163-020-00123-8
10. Goldberg C.A. AI in the Hands of Stalkers, Abusers and Traffickers: A New Frontier in Victims' Rights // C.A. Goldberg. Victims' Rights Law Firm. 22.04.2023. https://www.cagoldberglaw.com/ai/
11. *Algorithms and Terrorism. The Malicious Use of Artificial Intelligence for Terrorist Purposes. A Joint Report by UNICRI and UNCCT.* Turin: UNICRI, 2021. 57 p.
12. Kelly L., Sachan S., Ni L., Almaghrabi F., Allmendinger R., Chen Y.-W. Explainable Artificial Intelligence for Digital Forensics: Opportunities, Challenges and a Drug Testing Case Study. *Digital Forensic Science.* 2020. https://doi.org/10.5772/intechopen.93310
13. Azarenko N.Yu. Extractive Summation of Scientific Texts. *Actual Issues of Technics, Science, Technology. Collection of Scientific Works of the National Conference (Bryansk, February 08–12, 2022)* / T.E. Sergutina (ed.). Bryansk: Bryanskii gosudarstvennyi inzhenerno-tekh-

ственный инженерно-технологический университет, 2022. С. 150–152.
14. Quick D., Choo K.-K.R. Big Digital Forensic Data. Volume 1: Data Reduction Framework and Selective Imaging. Singapore: Springer, 2018. 96 p. https://doi.org/10.1007/978-981-10-7763-0
15. Quick D., Choo K.-K.R. Big Digital Forensic Data. Volume 2: Quick Analysis for Evidence and Intelligence. Singapore: Springer, 2018. 86 p. https://doi.org/10.1007/978-981-13-0263-3
16. Чеснокова Е.В., Усов А.И., Омельянюк Г.Г., Никулина М.В. Искусственный интеллект в судебной экспертологии // Теория и практика судебной экспертизы. 2023. Т. 18. № 3. С. 60–77. https://doi.org/10.30764/1819-2785-2023-3-60-77

nologicheskii universitet, 2022. P. 150–152. (In Russ.).
14. Quick D., Choo K.-K.R. *Big Digital Forensic Data. Volume 1: Data Reduction Framework and Selective Imaging.* Singapore: Springer, 2018. 96 p. https://doi.org/10.1007/978-981-10-7763-0
15. Quick D., Choo K.-K.R. *Big Digital Forensic Data. Volume 2: Quick Analysis for Evidence and Intelligence*. Singapore: Springer, 2018. 86 p. https://doi.org/10.1007/978-981-13-0263-3
16. Chesnokova E.V., Usov A.I., Omel'yanyuk G.G., Nikulina M.V. Artificial Intelligence in Forensic Expertology. *Theory and Practice of Forensic Science.* 2023. Vol. 18. No. 3. P. 60–77. (In Russ.) https://doi.org/10.30764/1819-2785-2023-3-60-77

ИНФОРМАЦИЯ ОБ АВТОРАХ

Руденкова Юлия Сергеевна – государственный судебный эксперт отдела судебной компьютерно-технической экспертизы ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России; старший преподаватель МГТУ им. Н.Э. Баумана, кафедры: «Безопасность в цифровом мире», «Информационные системы и телекоммуникации»; старший преподаватель НИУ МЭИ, ИнЭИ, кафедра: «Безопасность и информационные технологии»;
e-mail: julia.rudenkova@gmail.com

Хазиев Шамиль Николаевич – д. юр. н., доцент, главный научный сотрудник отдела научно-методического обеспечения ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России;
e-mail: khaziev2@rambler.ru

Усов Александр Иванович – д. юр. н., профессор, заслуженный юрист Российской Федерации, первый заместитель директора ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России, профессор кафедры «Безопасность в цифровом мире» МГТУ имени Н.Э. Баумана, и.о. заведующего кафедрой судебной экспертологии РПА Минюста России;
e-mail: a.usov@sudexpert.ru

Статья поступила: 02.04.2024
После доработки: 25.05.2024
Принята к печати: 04.06.2024

ABOUT THE AUTHORS

Rudenkova Yulia Sergeevna – State Forensic expert of the Department of Shlyakhov RFCFS; Senior Lecturer at Bauman Moscow State Technical University, Departments: "Security in the digital world", "Information systems and Telecommunications"; Senior Lecturer at National Research University "Moscow Power Engineering Institute", Department: "Security and Information Technology"; e-mail: julia.rudenkova@gmail.com

Khaziev Shamil Nikolaevich – Doctor of Law, Associate Professor, Principal Researcher at the Forensic Research Methodology Department of Shlyakhov RFCFS; e-mail: khaziev2@rambler.ru

Usov Aleksandr Ivanovich – Doctor of Law, Full Professor, Distinguished Lawyer of the Russian Federation, the First Deputy Director of Shlyakhov RFCFS; Professor of the Security in the Digital World Department of the Bauman Moscow State Technical University; Acting Head of the Department of Forensic Expertology of the All-Russian State University of Justice; e-mail: a.usov@sudexpert.ru

Received: April 02, 2024
Revised: May 25, 2024
Accepted: June 04, 2024