Ткаченко Д. Г.

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ

Общество с ограниченной ответственностью «Союз электронной торговли», ул. Корнейчука, 48,127543, г. Москва, Россия,
tkachenko.dmitriy1@yandex.ru

Исследуются особенности внедрения цифровых технологий, включая искусственный интеллект, блокчейн. Качество цифровых технологий в криминалистике и организация цифровой криминалистической экспертизы определяют результаты установления объектов и субъектов правонарушения. Необходимость обрабатывать огромные объемы данных приводит к машинному обучению искусственного интеллекта и целенаправленному совершенствованию криминалистических программ искусственного интеллекта. Практическое применение в качестве инновации в криминалистике искусственного интеллекта подразумевает быструю и эффективную работу с большими данными, проработку огромных массивов информации. Блокчейн-криминалистика будет способствовать установлению финансовой дисциплины в транзакциях. Благодаря блокчейн-криминалистике повысится раскрываемость финансовых правонарушений.

Ключевые слова: криминалистика; уголовное право; искусственный интеллект; цифровые технологии; блокчейн; цифровая криминалистика.

Влияние искусственного интеллекта на многочисленные секторы нашего общества и его успехи на протяжении многих лет указывают на то, что он может помочь в решении множества сложных проблем расследования цифровой криминалистики [1, с. 565]. Анализ криминалистики может использовать возможности обнаружения и распознавания образов моделей машинного обучения для обнаружения скрытых доказательств в цифровых артефактах, которые были бы пропущены, если бы проводились вручную. Многочисленные работы предлагали способы применения искусственного интеллекта в цифровой криминалистике. Тем не менее, скептицизм относительно непрозрачности искусственного интеллекта препятствовал адекватной формализации и стандартизации этой области.

Развитие исследований и разработок методологий для интеллектуального анализа больших данных на основе искусственного интеллекта (ИИ), который стремится обнаружить значимые и поддающиеся исследованию закономерности в данных, сделало возможным, мотивировало его применение в расследовании цифровой криминалистики (ЦК). Цифровые артефакты представляют собой наборы цифровых данных,

которые часто являются большими, сложными и неоднородными. Несмотря на опасения относительно способности моделей «черного ящика» искусственного интеллекта генерировать надежные и проверяемые цифровые доказательства, предположение о том, что когнитивные методологии, используемые в анализе больших данных, будут успешными при применении к анализу цифровой криминалистики, подпитывало десятилетний всплеск исследований в области применения искусственного интеллекта в цифровой криминалистике.

Для начала существует недопонимание относительно разговорного использования терминов «Forensics AI» и «AI Forensics» в сообществе криминалистов (и за его пределами). При этом некоторые используют эти фразы взаимозаменяемо, как относящиеся к применению искусственного интеллекта в цифровой криминалистике. Хотя обе фразы не требуют пояснений, крайне важно прояснить распространенные заблуждения и различать эти два понятия. С одной стороны, согласно, слово, предшествующее «forensics» в домене DF (цифровая криминалистика), обозначает цель (инструмент или устройство), подлежащую анализу (например, облачная криминалистика, сетевая криминалистика, криминалистика памяти и т. д.). В результате автор называет «AI Forensics» криминалистическим анализом инструментов или методов искусственного интеллекта, а не криминалистическим расследованием с применением методов искусственного интеллекта. В том же ключе авторы называют AI Forensics «научными и юридическими инструментами, методами и протоколами для извлечения, сбора, анализа и представления цифровых доказательств, относящихся к сбоям в системах с поддержкой искусственного интеллекта». Подводя итог их определения, можно сказать, что криминалистика искусственного интеллекта – это анализ последовательности событий и обстоятельств, которые привели к сбою интеллектуальной системы, включая оценку того, был ли сбой вызван вредоносной деятельностью, и выявление ответственных лиц в таком сценарии.

В отличие от ранее описанной концепции, всесторонний обзор исследовательских баз данных таки, как Google Scholar, IEEE Explore и Scopus, на предмет терминов «ИИ-криминалистика» или «ИИ-цифровая криминалистика» показывает, что большинство ресурсов основаны на методах анализа DF с использованием методов искусственного интеллекта.

Существует множество текущих следственных задач, которые с помощью изобретательности и применения можно решить с использованием искусственного интеллекта, особенно в сфере цифровой криминалистики и киберпреступности [2, с. 89]. За последнее десятилетие использование искусственного интеллекта стало обычным явлением во многих областях, и сейчас самое время рассмотреть различные способы

интеграции искусственного интеллекта в судебные, судебно-медицинские и уголовные дела для лучшего сбора и анализа доказательств, тем самым улучшая результаты.

При использовании искусственного интеллекта для борьбы с преступностью важно заботиться и уважать частную жизнь. Прогностическая аналитика на основе искусственного интеллекта может помочь правоохранительным органам эффективно распределять ресурсы, выявляя очаги преступности и прогнозируя закономерности преступлений. Только путем развития сотрудничества между заинтересованными сторонами, исследователями, политиками, разработчиками технологий, следственными органами и судебной системой мы сможем использовать положительный потенциал искусственного интеллекта, обеспечивая при этом его ответственное и этичное внедрение в целях обеспечения общественной безопасности.

От автоматизированного анализа журналов и обнаружения вредоносных программ до анализа сетевого трафика и судебной экспертизы, искусственный интеллект может играть решающую роль в нескольких видах цифровой криминалистики и оказывать преобразующее влияние на расследования [3, с. 104].

Вот шесть способов, которыми искусственный интеллект может произвести революцию в цифровой криминалистике.

1. Автоматизированный анализ журналов. Отделы безопасности часто имеют дело с огромным объемом файлов журналов, созданных различными системами, приложениями и сетевыми устройствами, но ручной анализ этих журналов может занять много времени и привести к ошибкам. Вот где вступает в дело автоматизированный анализ журналов.

Алгоритмы искусственного интеллекта отлично справляются с обработкой огромных объемов файлов журналов и их анализом на наличие шаблонов и аномалий. Благодаря анализу журналов на основе искусственного интеллекта следователи могут быстро выявлять подозрительные действия, потенциальные инциденты безопасности и области, требующие дальнейшего расследования. Искусственный интеллект повышает скорость и точность анализа журналов, позволяя следователям сосредоточить свои усилия на соответствующих областях интереса и избежать траты времени и ресурсов на ручную проверку.

2. Обнаружение вредоносных программ. Быстрая эволюция вредоносных программ требует передовых методов обнаружения. Системы обнаружения вредоносных программ на базе искусственного интеллекта используют машинное обучение для просмотра и сканирования кода и изучения моделей поведения пользователей, более эффективно обнаруживая вредоносное программное обеспечение и помогая

следователям удалять вредоносное программное обеспечение из скомпрометированных систем для защиты от дальнейших атак.

Например, компании по безопасности используют алгоритмы искусственного интеллекта для постоянного обучения на известных образцах вредоносного программного обеспечения и их характеристиках. Обучая эти алгоритмы на больших наборах данных, они могут обнаруживать и классифицировать новые и ранее неизвестные штаммы вредоносного программного обеспечения на основе сходства с ранее выявленными угрозами и отмечать потенциальную атаку до того, как она произойдет.

3. Анализ изображений и видео. Анализ цифровых изображений и видео является важнейшим компонентом цифровой криминалистики. Например, алгоритмы искусственного интеллекта могут просеивать большие объемы мультимедийного контента – быстро идентифицировать лица, объекты или текст на изображениях и видео, тем самым значительно ускоряя процесс поиска и извлечения важных доказательств – и поддерживать широкий спектр сценариев расследования.

Возможен случай, когда следователям необходимо идентифицировать подозреваемого, запечатленного на кадрах видеонаблюдения в многолюдном месте. Просмотр видеоматериалов часто утомителен и может занять несколько часов. Технология распознавания лиц на основе искусственного интеллекта может быстро сканировать огромные объемы видеоданных, выявляя интересующие лица и значительно сокращая требуемые ручные усилия. Эта технология ускоряет процесс идентификации, позволяя следователям сосредоточить свои усилия на наиболее важных зацепках и ускорить ход расследования.

4. Обработка естественного языка. Технологии искусственного интеллекта, такие как обработка 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 в цифровых расследованиях. Использование извлекающего искусственного интеллекта может быть более эффективным и точным для выявления связей, обнаружения закономерностей и идентификации ключевых лиц во время текстовых расследований.

Возможен сценарий, в котором следователи изучают огромную коллекцию журналов чатов, чтобы выявить потенциальных соучастников киберпреступления. Алгоритмы обработки естественного языка (NLP) на основе искусственного интеллекта могут быстро обрабатывать и анализировать текстовые данные, выявляя повторяющиеся фразы, подозрительные закономерности и связи между людьми. Это позволяет следователям точно определять ключевых лиц, представляющих интерес,

и раскрывать скрытые сети, ускоряя процесс расследования и обеспечивая своевременное вмешательство.

5. Анализ сетевого трафика. Мониторинг и анализ шаблонов сетевого трафика имеют важное значение для обнаружения и реагирования на кибератаки. Вместо того чтобы проводить ручной аудит и анализировать шаблоны сетевого трафика с заранее определенными интервалами, группы экспертов-криминалистов могут обучать алгоритмы искусственного интеллекта для автоматического анализа сетевых пакетов, выявления отклонений от обычных шаблонов трафика и выдачи оповещений, когда аномалия требует дальнейшего расследования. Искусственный интеллект также может помочь в сопоставлении сетевых событий с известными шаблонами атак, предоставляя ценную информацию группам реагирования на инциденты.

6. Криминалистическая сортировка. Цифровые расследования включают в себя огромные объемы данных, требующие от следователей быстрого просеивания и расстановки приоритетов соответствующих доказательств. Искусственный интеллект в криминалистической сортировке часто включает в себя использование алгоритмов машинного обучения для классификации и категоризации большого количества цифровых файлов на основе их релевантности расследованию. Эти инструменты анализируют метаданные файлов, содержимое и другие атрибуты, чтобы расставить приоритеты для более тщательного изучения файлов, постоянно «учась» идентифицировать соответствующий материал с возрастающей точностью по мере добавления новых данных в расследование. Команды криминалистов могут быстро идентифицировать и сосредоточиться на самых важных доказательствах раньше, что приводит к более быстрым и эффективным расследованиям при оптимизации распределения ресурсов.

Растущий уровень сложных преступлений увеличил возможности и потребность в судебной экспертизе в изучении различных новых технологий для противодействия преступникам, и искусственный интеллект не является исключением. Важно отметить, что, несмотря на точность и точность большинства алгоритмов искусственного интеллекта, из-за многочисленных исследовательских фокусов и ресурсов, посвященных им в последнее время, их применение в цифровой криминалистике требует значительной осторожности и учета специфических для данной области тонкостей. Очевидно, что результаты бизнес-ориентированной задачи искусственного интеллекта будут оцениваться иначе, чем результаты судебного расследования. Большая часть алгоритмов искусственного интеллекта основана на статистических вероятностях, что обычно приводит к недетерминированным результатам. Таким образом, задача будет заключаться в том, чтобы установить

правильность результатов и сообщить вероятностное заключение судебной экспертизы максимально простым и понятным способом, чтобы оно было допустимо в судебном разбирательстве.

Цифровая криминалистика включает в себя идентификацию, получение и анализ электронных доказательств, играя решающую роль в современных уголовных расследованиях. Она используется в судебных разбирательствах и помогает в изучении кибератак и реагировании на инциденты. Сбор электронных доказательств из различных источников, таких как компьютеры, мобильные устройства и т.д., является ключевым аспектом цифровой криминалистики.

В сложном и быстро меняющемся мире блокчейна и криптовалюты понимание деталей транзакций и движения цифровых активов может быть сложной задачей. Каждая транзакция оставляет цифровой след, и в этих следах лежат сложные детали, которые могут иметь решающее значение в юридических спорах, усилиях по возврату активов и расследованиях безопасности.

Неизменная и прозрачная природа блокчейна обеспечивает полную запись транзакций, но расшифровка этой информации требует специальных навыков и инструментов. Сложность возникает из-за децентрализованной структуры блокчейна, где транзакции являются псевдонимами и распространяются по сети узлов. Отслеживание потока активов, выявление мошеннических действий и связывание цифровых транзакций с реальными сущностями требуют сложного понимания различных протоколов блокчейна и криптографических принципов. Глобальный и безграничный характер блокчейна добавляет уровни юрисдикционных и нормативных проблем [4, с. 840].

Несмотря на эти сложности, криминалистика блокчейна жизненно важна для борьбы с незаконной деятельностью, такой как мошенничество, отмывание денег и киберпреступность.

Сегодня блокчейн-криминалистика так же сложна, как и транзакции, которые она отслеживает. Chainalysis и CipherTrace остаются лидерами отрасли. Но целый ряд интернет-сыщиков, небольших консалтинговых компаний и инструментов DIY доступен для помощи следователям в отслеживании цифровых денег. Финансовые следователи и блокчейн-криминалистика вскоре могут оказаться в таком же положении, как и другие следователи с цифровой криминалистикой.

Блокчейн продолжает развиваться. Криптовалюты, такие как Zcash и Monero, были созданы с приоритетом конфиденциальности. Другие формы доказательств с нулевым разглашением – проверка транзакций без раскрытия посторонней информации остальной части блокчейна – еще больше усложнят криминалистические усилия. Но многие вещи кажутся неотслеживаемыми, пока внезапно они таковыми не становятся.

Блокчейн-криминалистика будет играть все большее значение в противодействии отмыванию финансовых средств и финансирования терроризма, способствуя укреплению национальной безопасности. Блокчейн-криминалистика станет орудием для осуществления финансовой дисциплины. Поддержка финансовой дисциплины является важным условием для стабильности внутри государства как социальной организации [5, с. 479].

Вероятно, в будущем развитие цифровых технологий приведет к синтезу использования методов блокчейн-криминалистики и криминалистики искусственного интеллекта [6, с. 76]. Инновационные технологии искусственного интеллекта и блокчейна в криминалистике способствуют более оперативному раскрытию преступлений.

Библиографический список

1. Бабаханова, И. А. Искусственный интеллект в криминалистике / И. А. Бабаханова // Криминалистика наука без границ: традиции и новации: м-лы междунар. науч.-практ. конф. – СПб, 2024. –С. 564-568.

2. Бахтеев, Д. В. О связи криминалистики и технологии искусственного интеллекта / Д. В. Бахтеев // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 1 (35). – С. 88-93.

3. Неретина, Н. С. Искусственный интеллект в криминалистике и судебной экспертизе / Н. С. Неретина // Судебная экспертиза и исследования. – 2022. – № 1. – С. 103-106.

4. Скрыпникова, А. В. Применение искусственного интеллекта в криминалистике, возможности и перспективы / А. В. Скрыпникова, А. М. Яковенко // Криминалистика наука без границ: традиции и новации. Материалы междунар. науч.-практ. конф. – СПб, 2024. – С. 839-843.

5. Ткаченко, Д. Г. Совершенствование правового регулирования при внедрении технологи блокчейн для осуществления финансового контроля и надзора / Д. Г. Ткаченко // Трансформация национальной социально-экономической системы России. Материалы II Междунар. науч.-практ.конф. – Москва, 2020. – С. 478-482.

6. Тучков, Я. В. Искусственный интеллект: перспективы использования в криминалистике / Я. В. Тучков // Актуальные вопросы теории и практики в деятельности подразделений полиции по охране общественного порядка и иных служб ОВД. Материалы вузовской науч.-практ. конф. – Москва, 2022. – С. 75-78.