Секция «44.41 LegalTech. Цифровая криминалистика»

Применение технологий искусственного интеллекта в цифровой криминалистике

Научный руководитель – Яковлев Алексей Николаевич

Василенко Юрий Андреевич
Студент (специалист)
Национальный исследовательский университет «МИЭТ», Москва, Россия
E-mail: vasilenkoyra06@gmail.com

Применение технологий искусственного интеллекта в цифровой криминалистике обусловлено ростом объёма и разнородности цифровых данных (переписка, журналы событий, файлы и метаданные, аудио- и видеозаписи, сведения мобильных устройств и облачных сервисов), подлежащих выявлению, фиксации и последующему исследованию, что при отсутствии специализированных средств автоматизации затрудняет своевременное обнаружение сведений, имеющих значение для дела, и ведёт к нерациональным затратам времени. В научной литературе отмечается, что такие технологии способны повысить эффективность аналитического обеспечения расследования, однако не должны подменять принятие процессуальных решений и юридически значимую оценку доказательств [6; 7]. В этой связи технологии искусственного интеллекта целесообразно использовать как инструмент поддержки при выявлении, фиксации и анализе цифровых следов при сохранении ответственности уполномоченных должностных лиц, принимающих процессуальные решения, и роли эксперта в интерпретации результатов в пределах специальных знаний [1; 4; 7]. Возможным направлением применения является перевод материалов в машиночитаемый вид и формирование единого массива для поиска и анализа: распознавание текста и речи позволяет индексировать сканы и аудиозаписи, а методы обработки естественного языка — извлекать ключевые элементы ситуации (временные ориентиры, участников и их роли, используемые учётные записи и сервисы) и формировать структурированную «карту артефактов» со ссылками на первоисточники [6]. По мере накопления материалов линейный просмотр становится менее эффективным; семантический поиск по смыслу обеспечивает оперативное выявление значимых фрагментов и устойчивых связей (контакты, платёжные реквизиты, домены, IP-адреса, идентификаторы устройств, адреса криптокошельков) [6]. Важным направлением является автоматизированная реконструкция хронологии и корреляция разнородных источников (журналы ОС и приложений, сетевые события, облачные логи, метаданные файлов и медиаконтента): построение временных линий позволяет выявлять противоречия и пробелы журналирования, которые служат основанием для проверяемых версий, при условии технической интерпретации с учётом часовых поясов, синхронизации времени и особенностей регистрации событий [6]. Приоритизация объектов исследования (устройства, учётные записи, каталоги, массивы сообщений) по формализованным признакам вероятной относимости оптимизирует объём осмотра и экспертизы без подмены полноты исследования механическим фильтром [6]. Модели выявления аномалий применимы для обнаружения признаков шифрования, стирания следов, обфускации, нетипичных цепочек процессов и сетевых соединений; результаты корректно использовать как основание для постановки частных вопросов эксперту, а не как самостоятельное доказательство умысла [6; 7]. Проверка подлинности медиаматериалов должна сочетать анализ содержательных признаков с анализом метаданных, параметров кодирования и цепочки происхождения; вывод формулируется как вероятностная оценка с указанием условий применимости и ограничений используемых методов [6]. При формулировании результатов важно избегать психологизирующих выводов и

ограничиваться фиксацией объективных признаков с последующей проверкой контекста. Доказательственная пригодность результатов обеспечивается воспроизводимостью и трассируемостью: работа ведётся на неизменяемых исходниках и судебно-пригодных копиях, фиксируются контрольные суммы исходных данных и ключевых производных результатов, сохраняются производные артефакты, ведётся журнал операций (инструмент, версия, параметры, условия получения результата), обеспечивается цепочка хранения и доступа [5; 4]. В случаях, когда побитовое копирование невозможно либо неприменимо (облачные сервисы, распределённые хранилища, волатильные данные), используется сопоставимый по проверяемости порядок: формализованные выгрузки штатными средствами, экспорт журналов и метаданных, документирование критериев отбора и происхождения данных, контроль целостности полученных наборов и проверка по альтернативным источникам [5; 6]. Существенное значение имеют конфиденциальность и защита информации: локальное размещение компонентов, содержащих охраняемую законом информацию, шифрование каналов передачи, разграничение доступа и протоколирование обращений, а также соблюдение требований законодательства об информации и персональных данных [2; 3]. Таким образом, применение технологий искусственного интеллекта в цифровой криминалистике повышает эффективность выявления, фиксации и анализа цифровых следов и способствует формированию проверяемых версий при обработке существенных объёмов разнородной цифровой информации при условии приоритета процессуальной формы, документированной проверки результатов и обязательной экспертной верификации юридически значимых выводов.

Источники и литература

1) Уголовно-процессуальный кодекс Российской Федерации (Федеральный закон от 18.12.2001 № 174-ФЗ).
2) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4) Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».
5) ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме».
6) Цифровая криминалистика: учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. М.: Юрайт, 2021.
7) Постановление Пленума Верховного Суда РФ от 21.12.2010 № 28 (ред. от 29.06.2021) «О судебной экспертизе по уголовным делам».