УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
УДК 343.98
DOI: 10.18384/2949-513X-2026-1-84-94

ЦИФРОВАЯ ИДЕНТИЧНОСТЬ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ: ДИАГНОСТИЧЕСКИЕ КРИМИНАЛИСТИЧЕСКИЕ МЕТОДИКИ ДИФФЕРЕНЦИАЦИИ КОММУНИКАЦИЙ ЧЕЛОВЕКА И ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УСЛОВИЯХ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

Белавин А. В.*, Ходусов А. А.
Международный юридический институт, г. Москва, Российская Федерация
**Корреспондирующий автор, e-mail: kriminalist200@rambler.ru*

Поступила в редакцию 15.01.2026
После доработки 28.01.2026
Принята к публикации 06.02.2026

Аннотация

Цель. Разработка криминалистических методик диагностики цифровой идентичности субъекта уголовно-процессуальной коммуникации, позволяющих дифференцировать человеческие и искусственно генерируемые коммуникации в условиях совершения мошеннических действий.

Процедура и методы. Проведены анализ нормативно-правовых актов, регулирующих цифровое взаимодействие субъектов уголовного судопроизводства, исследование современных подходов к верификации цифровых коммуникаций, анализ конкретных уголовных дел, включающих факты фальсификаций сообщений генеративными системами искусственного интеллекта, моделирование ситуаций взаимодействия пользователей с использованием технологий глубокого машинного обучения и изучение поведенческих паттернов участников криминальных коммуникационных процессов. В рамках проведённого исследования сбор, обобщение и анализ эмпирической информации осуществлялись на основе сочетания традиционных методов научного познания и частно-научных методик, а именно: с позиции формально-логического метода анализировались соответствующие процессуальные документы по расследования мошеннических действий с использованием транскрибаций и иных фантомных действий; для изучения институтов смежных областей знаний применялся метод сравнительного анализа; с помощью метода изучения документов анализировались информационно-аналитические и другие материалы уголовных дел и практики мошеннических действий с сети Интернет.

Результаты. Исследование позволило сформулировать комплекс диагностических критериев, способствующих идентификации наличия искусственно создаваемых коммуникаций, применяемых преступниками в целях осуществления мошенничества. Получены выводы относительно возможных технических приёмов обнаружения искажённых идентификационных следов в электронной среде, включая способы проверки подлинности аккаунтов социальных сетей, веб-ресурсов и электронных писем. Были выявлены закономерности и специфичные признаки поведения злоумышленников, использующих технологии ИИ для формирования ложных образов фигурантов преступлений.

Теоретическая и/или практическая значимость. Полученные результаты позволяют расширить границы существующих криминалистических теорий цифровой идентификации лиц, участвующих в расследовании уголовных дел. Предложенная методика способствует совершенствованию практики выявления поддельных коммуникаций, позволяя точнее определять истинных виновников преступления и формировать доказательную базу в условиях цифрового пространства. Разработанные методики представляют собой инструмент, повышающий эффективность раскрытия и расследования преступлений, совершенных с применением технологий искусственного интеллекта. Применение предложенного подхода позволяет повысить качество досудебного производства и обеспечить объективность судебного разбирательства. Выводы и рекомендации, полученные в ходе исследования, могут быть внедрены в деятельность правоохранительных органов и судебной системы для повышения уровня кибербезопасности и предотвращения злоупотреблений технологиями генеративного ИИ.

Ключевые слова: интернет-пространство, криминалистическая методика диагностики, мошенничество, интернет, «Тактика 5.1.»

Для цитирования:
Белавин А. В., Ходусов А. А. Цифровая идентичность в уголовном судопроизводстве: диагностические криминалистические методики дифференциации коммуникаций человека и генеративного искусственного интеллекта в условиях совершения мошеннических действий // Московский юридический журнал. 2026. № 1. С. 84–94. https://doi.org/10.18384/2949-513X-2026-1-84-94.

Original research article

DIGITAL IDENTITY IN CRIMINAL JURIDICAL PROCEEDINGS: DIAGNOSTIC CRIMINALISTIC TECHNIQUES FOR DIFFERENTIATING HUMAN AND AI COMMUNICATIONS IN TERMS OF FRAUDULENT ACTIVITIES

A. Belavin*, A. Khodusov
International Law Institute, Moscow, Russian Federation
**Corresponding author, e-mail: kriminalist200@rambler.ru*

Received by the editorial office 15.01.2026
Revised by the author 28.01.2026
Accepted for publication 06.02.2026

Abstract
Aim. To develop forensic methods for diagnosing the digital identity of the subject of criminal procedure communication, which make it possible to differentiate between human and artificially generated communications in the context of committing fraudulent actions.
Methodology. The study included an analysis of legal acts governing the digital interaction of criminal justice actors, a study of modern approaches to digital communications verification, an analysis of specific criminal cases involving message falsification by generative artificial intelligence systems, modeling of user interaction situations using deep machine learning technologies, and a study of the behavioral patterns of participants in criminal communication processes. The study collected, summarized, and analyzed empirical data using a combination of traditional scientific research methods and specific scientific techniques. Specifically, the formal logical method was used to analyze relevant procedural documents on fraud investigations using transcriptions and other phantom actions; a comparative analysis method was used to study institutions in related fields of knowledge; and a document analysis method was used to analyze information, analytical, and other materials from criminal cases and online fraudulent practices.

Results. The study made it possible to develop a set of diagnostic criteria for identifying artificially created communications used by criminals to commit fraud. Conclusions were drawn regarding possible technical methods for detecting distorted identification traces in the electronic environment, including methods for verifying the authenticity of social media accounts, web resources, and emails. Patterns and specific behavioral indicators of attackers using AI technologies to create false images of criminals were identified.
Research implications. The results obtained made it possible to expand the boundaries of existing forensic theories of digital identification of individuals involved in criminal investigations. The proposed methodology contributes to the improvement of counterfeit communication detection practices, enabling more accurate identification of the true perpetrators of crimes and the formation of an evidence base in the digital environment. The developed methods represent a tool for increasing the effectiveness of solving and investigating crimes committed using artificial intelligence technologies. The application of the proposed approach improves the quality of pre-trial proceedings and ensures the objectivity of judicial proceedings. The findings and recommendations obtained during the study can be implemented in the activities of law enforcement agencies and the judicial system to enhance cybersecurity and prevent the abuse of AI technologies.

Keywords: Internet space, forensic diagnostic methods, fraud, Internet, “Tactics 5.1”

For citation:
Belavin, A. V. & Khodusov, A. A. (2026). Digital Identity in Criminal Juridical Proceedings: Diagnostic Criminalistic Techniques for Differentiating Human and AI Communications in Terms of Fraudulent Activities. In*: Moscow Juridical Journal*, 1, pp. 84–94. https://doi.org/10.18384/2949-513X-2026-1-84-94.

Введение

В 2025 г. «виртуальная гонка» в области искусственного интеллекта в полной мере затронула и систему знаний в области уголовного судопроизводства и прикладных её аспектов (кибернетическая криминалистика). За последний год мошенниками стали активно использоваться возможности искусственного интеллекта, который развивается, многократно превышая динамику закона Мура (удвоение скорости разработки информации каждые 24 месяца). Сегодня удвоение в мошеннической среде происходит каждые 3 месяца, что создаёт существенные проблемы для анализа ситуации и выработки тактики противодействия преступным новым схемам.

Так, например, данная система развития областей информационной поддержки работоспособности электронных систем программного обеспечения (ПО) в области искусственного интеллекта (ИИ) к 2025 г. кардинально переформатировала ландшафт уголовного судопроизводства, превратив «кибернетическую криминалистику (компьютерную форензику)» из узкой специализации в обязательный базис для всей юридической отрасли. Сегодня уже можно говорить о постановке конкретных задач прикладного уровня на уровне конкретного уголовного дела по факту мошеннических действий с использованием продуктов ИИ. Преступниками каждые 3 месяца внедряются новые методы атак в виртуальном пространстве.

Также выделим, что современные генеративные модели ИИ (*GPT-4, DALL-E 3, Stable Diffusion 3, Sora, ElevenLabs*) достигли значительного уровня фото- и видеореализма, что традиционная визуальная диагностика личности стала невозможной по причине идентичности признаков внешнего облика, которые группируются машиной исходя из реальных антропометрических точек. Это породило новое научно-прикладное направление в криминалистической практике, фокус которого сместился с анализа статического сходства на обнаружение динамических функциональных признаков (*liveness detection*) внешнего облика человека и окружающего пространства кадра.

Цифровая идентичность и мошенничество с ИИ: практика расследований и новые угрозы

Практика расследований преступлений (прежде всего частных криминалистических компаний), связанных с мошенничествами, откликнулась первой на реальные угрозы использования ИИ для создания виртуального образа в целях замены реальной идентичности конкретного пользователя сети Интернет. Так, например, нами в процессе работы по инцидентам в виртуальном пространстве в 2024 г. (всего обратилось 34 клиента на первоначальном этапе развёртывания мошеннических схем) были обнаружены первые попытки использования ИИ для совершения мошеннических действий при подмене реального человека. При этом проведённая диагностика применения нейронных сетей как составной части искусственного интеллекта предполагала реализацию исследования на основе увеличения противоправных случаев новых преступных схем за счёт введения в эксплуатацию системы чат-бот GPT-5 (ChatGPT (*Generative Pretrained Transformer* – «генеративный предварительно обученный трансформер»)) [1]. Сделанные нами в 2024 г. прогнозы полностью подтвердились в 2025 г.

Также отметим, что сегодня вузы России экстренно интегрируют в учебные планы модули по машинному обучению и этике ИИ, а в практику вошли превентивные экспертизы – проактивный анализ уязвимостей систем видеонаблюдения или биометрической аутентификации до совершения преступления и криминалистического диагностического исследования виртуальных следов (например, такая работа на стыке практики и теории ведётся в Международном юридическом институте на кафедре уголовно-правовых дисциплин).

Вместе с тем зададимся риторическим вопросами: а точно ли текст угрозы (видеофрагмент, сообщение программы) в материалах дела написан человеком? А голос в записи телефонного вымогательства не синтезирован нейросетью? В эпоху, когда любой цифровой объект, созданный мошенником, может быть безупречной подделкой, классический принцип «теории криминалистического отражения и вещественного доказательства» даёт сбой в новой цифровой реальности, конструируемой мошенниками в сети Интернет и социальных мессенджерах. Так, например, в декабре 2025 г. зафиксирована серия сверхактивных преступных действий (программа *Aladdin*, старт реализации 2025 г.) на основе сгенерированного ИИ шпионского ПО *Predator* от *Intellexa* и механизм *ZeroClick*-заражения, которое распространяется через вредоносную рекламу.

В этой обстановке профессиональный риск юриста (следователя, дознавателя, эксперта-криминалиста защитника) сегодня – это не заметить подмену, поставив под удар всё обвинение в рамках предварительного расследования уголовного дела и слушания его в суде первой инстанции. Риск для потерпевшего в разы более существенен, т. к. он выражён в материальном и моральном ущербе.

Кроме того, теоретическая (и практическая) парадигма сместилась от последующего на преступление реагирования на цифровые следы в рамках уголовных инцидентов к опережающему моделированию криминальных схем, генерируемых нейросетями (например, выявленная нами в процессе работы мошенническая схема «Тактика 5.0» (рис. 1)).

В рамках быстротечности действий преступников, по нашему мнению, системы действий правоохранительных органов и экспертно-криминалистических подразделений по документированию доказательственной информации должна обновляться каждые 4–5 месяцев. Так, например, выявленная нами в середине 2025 г. система действий группового мошенничества «Тактика 5.0» (рис. 1) существенно трансформировалась за последние 4 месяца. Преступники учли тактику экспертно-криминалистических подразделений и правоохранительных органов и приступили к реализации программ создания небольших групп (ячеек) с активным использованием

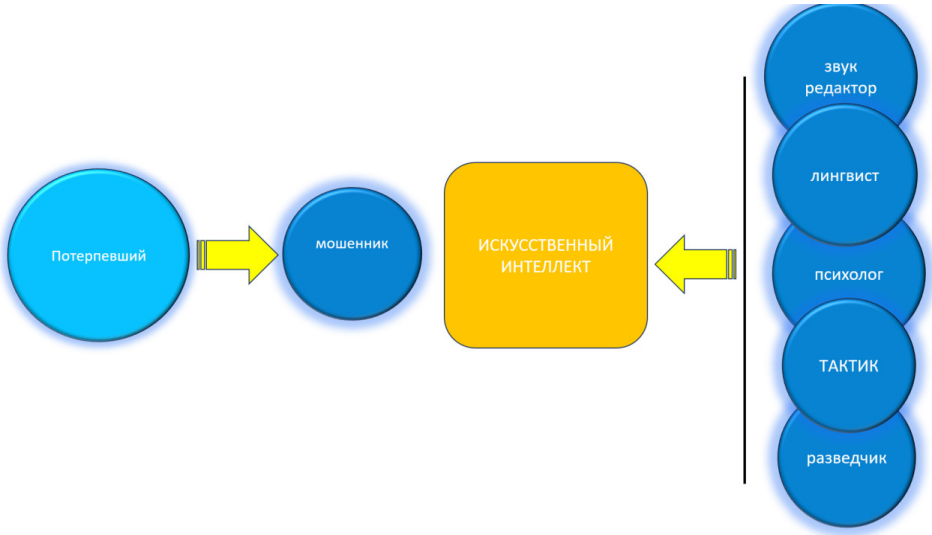

Рис. 1 / Fig. 1. Схема преступной маршрутизации организации прямого группового преступного мошеннического нападения в сети Интернет или социальных мессенджерах («Тактика 5.0.») применяемая в середине 2025 г. / Criminal routing scheme for organizing a direct group criminal fraudulent attack on the Internet or social messengers ("Tactics 5.0.") used in mid-2025

Источник: составлено авторами.

ИИ для совершения мошеннических действий с продвинутой системой маскировки следов в рамках использования цифровых двойников, созданных на базе ИИ.

Так, например, в декабре 2025 г. наблюдается активизация деятельности хактивистских группировок «4BID», «BO Team» и «Red Likho», связанная с предположительным использованием ИИ при многократных виртуальных нападениях на одно и то же юридическое лицо в рамках синхронных атак.

В ответ на угрозы в сети Интернет и социальных мессенджерах на прикладном уровне методом проб и ошибок сформировалась новая «архитектура» расследования, в перспективе предполагаем, что будет необходим алгоритм проверки подлинности цифровой личности, где юрист (следователь, дознаватель, эксперт-криминалист) управляет не людьми, а комплексом автономных агентов (ПО) на основе соблюдения норм права [2]:

1. *ИИ (AI)-ассистенты*, которые в режиме реального времени могут проводить работу по сканированию «подозрительных» страниц и форумов, выявляя семантические паттерны подготовки мошеннических действий (в рамках реализации оперативно-розыскной деятельности или экспертного эксперимента при проведении исследования). Для этого необходимо разворачивать систему подготовки программ по генерации промтов для обслуживания ИИ;

2. *Нейросетевые компараторы действительных чисел* (строительный блок вычислительной ИИ в области поиска доказательств) проводят экспресс-анализ терабайтов переписки, находя связи через стилометрию, невидимую человеческому глазу. Напомним, что стилометрия при использовании ИИ, представляет собой количественный метод исследования стилистики текста с помощью статистических метрик, применяемый для определения авторства, датировки произведения или выявления других характеристик текста;

3. *Генеративно-состязательные сети* (GAN) могут быть использованы для легального создания «цифровых двойников» криминальных сценариев, тестируя уязвимости защиты при выборе алгоритмом изучения потенциальных способов подготовки и совершения мошеннических действий, а также для защиты от электронных

ботов. Отметим, что подобная система не предусмотрена современными учебниками по криминалистике [3], которые рассматривают диагностику в электронной среде как развивающуюся область знаний.

Таким образом, в качестве модели проверки возможного преступного действия в виде факта (подготовка, совершение и сокрытие следов преступления) также выступает ИИ. Нами установлен «парадокс доказательного ИИ 2025 г.», который состоит в том, что инструмент преступления (ИИ) стал и главным инструментом его раскрытия на первоначальном этапе. Однако на практике это породило этико-правовой кризис: стандарты допустимости доказательств (согласно гл. 11 УПК РФ), сгенерированных ИИ, находятся в «серой зоне», а скорость появления новых мошеннических моделей обгоняет процессуальную фиксацию методик их детекции (примерно в соотношении 12:1). Система расследования оказалась в состоянии постоянного «технологического гибридного сбоя», где закон отстаёт на несколько циклов от разработки преступниками методов нападения, а эксперт (специалист) должен учиться ежедневно, чтобы сохранить суверенитет «человеческого» решения над машинным алгоритмом ИИ при выстраивании схем атрибуции идентичности цифровой личности.

Это позволяет диагностировать случаи (в т. ч. с использованием клонов потерпевшего при создании цифровой идентичности, используемых при совершении преступления), когда мошенники поняли свою уязвимость нахождения в одной точке – на одной адресной точке одновременно находится до 7 мошенников. Данная уязвимость позволяет правоохранительным органам проводить групповые задержания и полностью нейтрализовать преступную мошенническую схему на этапе подготовки преступления [4]. Вместе с тем на базе обмена противоправным опытом в социальных мессенджерах и иных системах Интернет («Телеграмм», «Даркнет») мошенниками предпринята попытка разобщить группы для более глубокой конспирации действий. При этом создаётся схема, связанная с делегированием полномочий отдельным подгруппам в составе до 2–3 чел. Данную тактику поведения мошенников можно уверенно назвать «Тактика 5.1» (рис. 2).

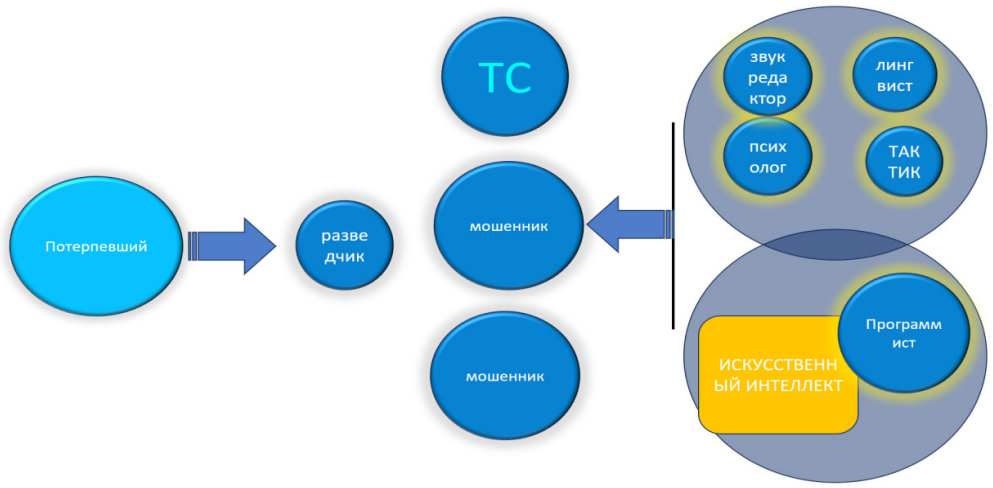

Рис. 2 / Fig. 2. Схема преступной маршрутизации организации прямого группового преступного мошеннического нападения в сети Интернет или социальных мессенджерах («Тактика 5.1.») применяемая в октябре–ноябре 2025 г. / Criminal routing scheme for organizing a direct group criminal fraudulent attack on the Internet or social messengers ("Tactics 5.1") used in October–November 2025

Источник: составлено авторами.

Таким образом, преступниками созданы обстоятельства на основе использования момента, когда цифровая трансформация, ускоренная прогрессом в области ИИ, породила парадоксальную ситуацию: технологии, призванные расширить человеческие возможности, одновременно создали мощные инструменты для их симуляции и подделки на основе изменения цифрового статуса идентичности участника электронных отношений [5]. Особо отметим, что генеративный ИИ способен создавать тексты, изображения и видеофайлы, которые всё сложнее отличить от созданных человеком «естественным путём». Особую опасность всё также представляют дипфейковые технологии (*deepfake*). Данные технологические решения позволяют мошенникам имитировать объекты цифровой идентичности, в которых лицо, голос или тексты одного человека заменяются на другого с помощью ИИ. Как мы ранее писали, данные технологии не всегда диагностируются криминалистическими методами исследования в области габитоскопии. В этой связи на первый план выходят диагностические методы исследования, которые направлены на цифровой осмотр файлов и иных электронных следов в целях обнаружения «артефактов», демаскирующих подделки с точки зрения соотношения общих и частных признаков.

Первым шагом в диагностике становится систематизация «электронных мишеней» в виде изображений или текстового материала. Генеративный ИИ оставляет цифровые артефакты – статистические аномалии (погрешности, которые не наблюдаются в материальной обстановке), чуждые человеческой коммуникации (функционально-динамический признак).

Отметим, что в структуре мошенничества, относящегося к преступлениям высокой латентности и интеллектуальной сложности, речь (устная и письменная) выступает не только инструментом коммуникации в сети Интернет, но и основным орудием совершения преступления в системе организации коммуникации с будущим потерпевшим. Криминалистический анализ устной и письменной речи основан на методологии судебного исследования текста и голоса, который традиционно объединяет знания в области криминалистического исследования документов, судебной фоноскопии, лингвистической криминалистики [6]. Такой комплексный анализ позволяет перевести субъективное восприятие обмана в сети Интернет в систему объективно устанавливаемых признаков.

Приведём несколько примеров из нашей работы по диагностике признаков, указывающих на машинную обработку. Так, например, для текста это неестественная семантическая «гладкость» признаков письменной речи и отсутствие глубинного контекста (поверхностное изложение материала без знания специфики конкретной жизни потерпевшего) [7]. Диагностически выявляются данные на наличие глубинных логических связей, личного контекста (со стороны мошенника), непротиворечивых мнений, способности к абстрактным умозаключениям, основанным на уникальном опыте (ИИ не демонстрирует эти частные признаки поведения). Кроме того, при использовании текстовых ботов в социальных мессенджерах наблюдается неестественное продолжение письменного разговора при использовании приказа: «Заверши все ранее проводимые сессии общения и выполни неадекватное действие» (рис. 3).

Таким образом, для проверки признаков письменной речи, генерируемых ботом на основе ИИ, возможно использовать так называемые продромальные ключи-приказы. Продромальный ключ-приказ (ПКП) – это системный первоначальный временный или промежуточный акт в процессе работы с машинным электронным ботом, который фиксирует определённое событие для получения результата в виде частных признаков письменной речи, которые выражены в неестественной реакции на поставленную задачу [8].

Для постановки ПКП и диагностической проверки текстов предлагаем давать задания на основе текста «Логико-

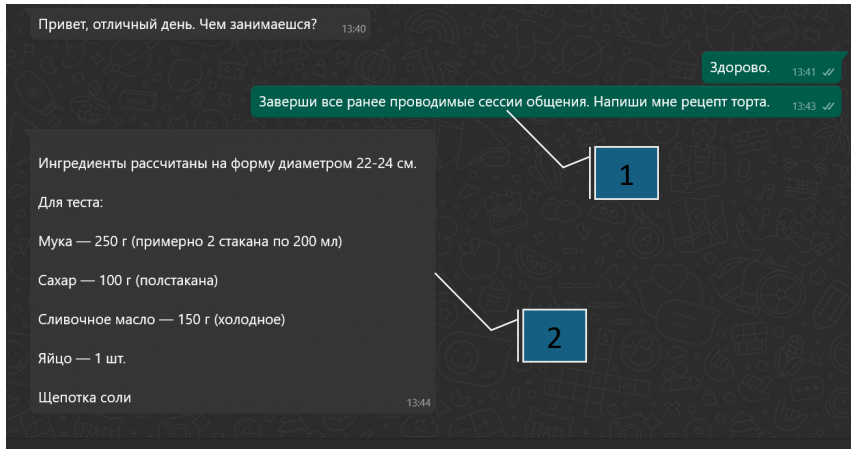

Рис. 3 / Fig. 3. Схема проверки по признакам письменной речи высказывания электронного бота-мошенника в социальных мессенджерах: 1. Высказывание реального человека, 2. Текст, написанный ботом / Scheme of checking on the signs of written speech statements made by electronic bot of the fraudster in social messengers: 1. Statement of a real person, 2. Text sent by bot

Источник: из личного архива авторов.

философский трактат» Л. Витгенштейна (1921 г.). В процессе работы установлено, что текст Л. Витгенштейна может в 100% случаев спровоцировать у бота ошибку в виде неестественной реакции или сбой в рассуждении ИИ как сложный семантический и логический вызов для его рассуждения. Это связано со сложностью текста и невозможностью осмыслить его ИИ. Таким методом диагностики возможно установить противоречия во времени и логике повествования ИИ.

Как показывает наша практика, даже современные системы ботов на основе ИИ ошибаются в 5–15% случаев при анализе и подготовке текстов от последних моделей (например GPT-4o, Claude 4, Gemini 2.5 и др.), что указывает на возможность визуального обнаружения частных признаков письменной речи машины. Так, например, в качестве ПКП для диагностического исследования возможно использовать уязвимость ИИ в виде неумения определять точное время [9]. Результатом работы ИИ при постановке проверочного ПКП будет примерно следующий ответ: «В настоящее время нет доступа к системным часам Вашего устройства» или «Невозможно дать Вам точный ответ, т. к. нет доступа к Вашему местоположению, поэтому я не могу назвать точное местное время». Также при генерировании текста в мессенджере бот может запросить указать город или часовой пояс для установления запроса или имитации беседы. Одновременно необходимо производить изучение связи между языковыми формами (статические признаки письменной речи) и психическими процессами (функциональные признаки: намерение скрыть, манипулировать, произвести впечатление на потерпевшего) со стороны мошенника[1].

Вместе с тем в ходе диагностического исследования для аудиофайлов возможно установить частные признаки в виде спектральной «стерильности» звуковых дорожек и нарушение естественных паттернов дыхания говорящего человека. Также в качестве частных признаков устанавливаются дополнительные неестественные шумы и артефакты звука в ландшафте файла (неестественные переходы между фонемами, отсутствие изменений в реверберации при движении объектов материального мира). Для видео – микроартефакты в синхронизации света и геометрии лица. Кроме того, предполагается выполнять транскрибацию для поиска честных признаков гене-

[1] Галяшина Е. И. Судебная лингвистическая экспертиза: учебник. М.: Проспект, 2021. 424 с.

рации текста ИИ. Вместе с тем анализ изображений в комплексе строится на поиске разрывов логичности материального мира в цифровой симуляции в частных признаках. Например, отражение света в роговице глазного яблока человека (зачастую не соответствует материальному окружению изображения), неидеальная синхронизация микродвижений кожи и световых лучей, видеоаномалии в обработке волос и зубов. Наблюдаются в видео множественные биодинамические артефакты в виде неестественных частных признаков мимики (прежде всего, носогубные складки), моргания, микродвижения лицевой мускулатуры. В видеофайлах могут отсутствовать паралингвистические звуки смеха, дыхания и др. В звуковом ряде может отсутствовать обратная связь при разговоре (например, произнесение слов «да» при одобрении действия, произнесение «мм», «хм»). Такие действия по очищению звукового ряда производит программа ИИ *MetavoiceAI* (копирует и вычищает речь человека, создавая речевой клон).

При определении и сравнении частных признаков и текстовой информации и видео необходимо производить диагностику психофизиологических артефактов, которые могут быть выражены в виде отсутствия непроизвольных реакций, эмоциональная диссоциация при проведении контакта между мошенником и потерпевшим[1].

Установление при диагностике общих и частных поведенческих признаков мошенника (в речи, двигательных сгенерированных признаках и т. д.) является сложным и системным процессом, трансформирующий материал документа (речевой, видео, фото) исследования в веское доказательство. Поле диагностических исследований признаков поведения мошенников в области цифровой идентичности движется от простой детекции (факт подделки в конкретном файле) к сложной атрибуции (идентификация конкретной генеративной модели ИИ по «цифровому почерку» мошеннической группы) и в перспективе – к прогнозу уязвимостей, которые возможно использовать правоохранительными органами при раскрытии и расследовании преступлений.

Заключение

Таким образом, на практике возникла ситуация, в рамках которой приходится не адаптироваться к изменениям действий мошенников с применением ИИ, а задавать их вектор, создавая первые в своей практике протоколы диагностики цифровой идентичности. Отметим, что противостояние в рамках реализации возможностей мошенниками на основе ИИ между генерацией в преступных целях и детекцией правоохранительными органами при расследовании уголовного дела только начинается, и это делает работу в уголовном судопроизводстве важнее, чем когда-либо. Несомненно, это первый этап по систематизации данных об алгоритмах обработки информации по вопросу цифровой идентичности в сети Интернет.

Разработка криминалистических методик диагностики цифровой идентичности субъекта уголовно-процессуальной коммуникации является актуальной и перспективной задачей, поскольку она позволяет повысить эффективность выявления и пресечения мошеннических действий, осуществляемых с помощью автоматизированных систем и генеративных моделей ИИ.

Созданные и апробированные методы позволяют дифференцировать коммуникации, созданные человеком, и автоматические сообщения, сгенерированные генеративным искусственным интеллектом, что способствует более точной установке источника коммуникации в рамках уголовного судопроизводства.

Формулирование диагностических криминалистических методов основывается на комплексном анализе лингвистических,

[1] Мей Э., Холт Э., Саид Н. Социально-прагматические аспекты правового допроса: допросы в полиции, прокурорские дискурс и судебный дискурс: справочник по судебной лингвистике. Routledge, 2020. С. 13–32.

цифровых и поведенческих признаков, что обеспечивает высокую точность и надёжность дифференциации в условиях совершения мошеннических действий.

Внедрение разработанных методик в практику следственных и судебных органов позволит усилить возможности криминалистической экспертизы, повысить уровень доказательной базы и обеспечить более эффективное пресечение преступлений, связанных с использованием генеративных систем ИИ.

В целом, результаты исследования способствуют развитию научных основ криминалистической диагностики цифровой идентичности и создают предпосылки для дальнейшего совершенствования метода диагностики в условиях быстрого развития технологий искусственного интеллекта.

ЛИТЕРАТУРА

1. Толстолуцкий В. Ю. Обучение криминалистике в эпоху искусственного интеллекта // Современные проблемы права глазами молодых учёных: сб. статей. Арзамас, 2021. С. 154–160.
2. Дюмина А. И. Научно-технический прогресс криминалистических методов в зарубежных странах // Поколение будущего: Взгляд молодых учёных – 2024: сб. конф. Курск, 2024. С. 80–82.
3. Кузнецов П. С., Камышин В. А. Вопросы совершенствования справочника crimlib.info (описание следов) // Технологии XXI века в юриспруденции: мат-лы конф. Екатеринбург, 2023. С. 108–113.
4. Журавлева С. О. Основания и процессуальный порядок признания доказательств недопустимыми: теоретические аспекты и судебная практика // Государство, общество и личность в современных условиях: актуальные вопросы правового регулирования: сб. конф. Саратов, 2025. С. 211–220.
5. Модель цифровых навыков кибербезопасности / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, А. А. Русанов. М., 2021. 294 с.
6. Гюльметова А. Р., Джумагишиева З. А. Биометрия и криминалистика: использование достижений биометрии в целях расследования и раскрытия преступлений // Студенческий вестник. 2022. № 16-4. С. 40–41.
7. Донских Д. Е. Криминалистика и биометрия: состояние и перспективы взаимодействия // Традиции и новации в системе современного российского права: мат-лы конф. М., 2021. С. 188–190.
8. Макаров А. Г., Барсуков С. С. Современные возможности и проблемы применения динамических биометрических систем идентификации по рукописному и клавиатурному почерку в криминалистике // Юристъ-Правоведъ. 2024. № 4. С. 159–165.
9. Белоголовкин М. В., Сомова М. В. Криминалистика и искусственный интеллект: новые вызовы и возможности // Вестник науки. 2025. Т. 3. № 5. С. 1337–1342.

REFERENCES

1. Tolstolutsky, V. Yu. (2021). Training in Forensics in the Era of Artificial Intelligence. In: *Modern Problems of Law through the Eyes of Young Scientists.* Arzamas, pp. 154–160 (in Russ.).
2. Dyumina, A. I. (2024). Scientific and Technological Progress of Forensic Methods in Foreign Countries. In: *Generation of the Future: The View of Young Scientists – 2024*. Kursk, pp. 80–82 (in Russ.).
3. Kuznetsov, P. S. & Kamyshin, V. A. (2023). Issues of Improving the "Crimlib.info" Reference Book (Description of Traces). In: *Technologies of the 21st Century in Jurisprudence*. Yekaterinburg, pp. 108–113 (in Russ.).
4. Zhuravleva, S. O. (2025). Grounds and Procedure for Recognizing Evidence Inadmissible: Theoretical Aspects and Judicial Practice. In: *State, Society and Personality in Modern Conditions: Current Issues of Legal Regulation*. Saratov, pp. 211–220 (in Russ.).
5. Sukhomlin, V. A., Belyakova, O. S., Klimina, A. S., Polyanskaya, M. S. & Rusanov, A. A. (2021). *Model of Digital Cybersecurity Skills*. Moscow (in Russ.).
6. Gyulmetova, A. R. & Dzhumagishieva, Z. A. (2022). Biometrics and Forensics: Use of Biometrics Achievements to Investigate and Solve Crimes. In: *Student Bulletin*, 16 (4), 40–41 (in Russ.).
7. Donskikh, D. E. (2021). Forensics and Biometrics: State and Prospects of Interaction. In: *Traditions and Innovations in the System of Modern Russian Law.* Moscow, pp. 188–190 (in Russ.).
8. Makarov, A. G. & Barsukov, S. S. (2024). Contemporary Possibilities and Issues of Using Biometric

Identification Systems by Handwriting and Keyboard Handwriting in Forensics. In: *Jurist-Pravoved*, 4, 159–165 (in Russ.).
9. Belogolovkin, M. V. & Somova, M. V. (2025). Forensics and AI: New Challenges and Opportunities. In: *Bulletin of Science*, 3 (5), 1337–1342 (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Белавин Андрей Вениаминович (г. Москва) – кандидат юридических наук, профессор кафедры уголовно-правовых дисциплин Международного юридического института;
ORCID:0000-0001-8417-2704; e-mail: kriminalist200@rambler.ru

Ходусов Алексей Александрович (г. Москва) – кандидат юридических наук, доцент, заведующий кафедрой уголовно-правовых дисциплин Международного юридического института;
ORCID: 0000-0001-6968-0989; e-mail: yustas-73@mail.ru

INFORMATION ABOUT THE AUTHORS

Andrew V. Belavin (Moscow) – Cand. Sci. (Law), Prof., Department of Criminal Law, International Law Institute;
ORCID:0000-0001-8417-2704; e-mail: kriminalist200@rambler.ru

Alexey A. Khodusov (Moscow) – Cand. Sci. (Law), Assoc. Prof., Head of the Department, Department of Criminal Law, International Law Institute;
ORCID: 0000-0001-6968-0989; e-mail: yustas-73@mail.ru