Дата поступления рукописи в редакцию: 15.07.2026 г.
Дата принятия рукописи в печать: 07.08.2026 г.
DOI: 10.24412/2076-1503-2026-8-745-750

ГУБКО Алексей Александрович,
доцент кафедры публичного права Санкт-Петербургского государственного университета аэрокосмического приборостроения,
e-mail: gubko.60@mail.ru

КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. *В статье рассматривается содержание криминалистического обеспечения расследования преступлений, совершаемых с использованием технологий искусственного интеллекта. Проанализированы типичные способы применения данных технологий в преступной деятельности, включая создание синтезированных аудиовизуальных материалов, клонирование голоса, автоматизацию фишинговых рассылок и генерацию вредоносных программ. Раскрыты особенности механизма следообразования и охарактеризованы проблемы, возникающие при назначении и производстве судебных экспертиз синтезированного цифрового контента. Обоснованы направления совершенствования научного, технико-криминалистического, тактико-методического и кадрового обеспечения расследования рассматриваемой группы преступлений. Сформулирован вывод о необходимости разработки частной криминалистической методики расследования преступлений, совершаемых с использованием технологий искусственного интеллекта.*

Ключевые слова: *криминалистическое обеспечение; искусственный интеллект; цифровые следы; дипфейк; генеративные модели; компьютерно-техническая экспертиза; специальные знания; следственные действия; методика расследования; цифровизация.*

GUBKO Alexey Alexandrovich,
Associate Professor, Department of Public Law, Saint Petersburg State University of Aerospace Instrumentation

FORENSIC SUPPORT FOR THE INVESTIGATION OF CRIMES COMMITTED USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Annotation. *The article examines the content of the forensic support for the investigation of crimes committed with the use of artificial intelligence technologies. Typical ways of applying these technologies in criminal activity are analysed, including the creation of synthesised audiovisual materials, voice cloning, the automation of phishing campaigns and the generation of malicious software. The features of the trace formation mechanism are revealed, and the problems arising in the appointment and production of forensic examinations of synthesised digital content are characterised. The directions for improving the scientific, technical, tactical-methodological and personnel components of forensic support are substantiated. The conclusion is drawn about the need to develop a specific forensic methodology for investigating crimes committed with the use of artificial intelligence technologies.*

Key words: *forensic support; artificial intelligence; digital traces; deepfake; generative models; computer forensic examination; special knowledge; investigative actions; investigation methodology; digitalization.*

Введение

Современный этап общественного развития характеризуется ускоренным внедрением технологий искусственного интеллекта в экономику, государственное управление, социальную сферу и повседневную деятельность граждан. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10 октября 2019 г. № 490, определяет развитие данных

технологий в качестве одного из условий обеспечения технологического суверенитета страны [1]. Вместе с тем, доступность инструментов машинного обучения, генеративных нейронных сетей и больших языковых моделей закономерно повлекла их освоение преступной средой. Правоприменительная практика фиксирует устойчивый рост числа общественно опасных деяний, при подготовке, совершении и сокрытии которых применяются возможности искусственного интеллекта, что ставит перед криминалистической наукой задачу выработки адекватного научно-методического ответа на данный вызов.

Особенность рассматриваемой проблематики состоит в двойственной роли технологий искусственного интеллекта в сфере борьбы с преступностью. С одной стороны, данные технологии выступают орудием совершения преступлений, качественно изменяя способы преступной деятельности и механизм следообразования. С другой стороны, они образуют перспективный инструментарий самой криминалистики, позволяющий автоматизировать обработку значительных массивов криминалистически значимой информации. Полноценное криминалистическое обеспечение расследования преступлений, совершаемых с использованием технологий искусственного интеллекта, должно учитывать обе стороны данного явления. Цель настоящей работы состоит в определении содержания и направлений развития криминалистического обеспечения расследования преступлений рассматриваемой группы.

Методология исследования

В статье используются общенаучные методы (анализ, синтез, обобщение, системно-структурный метод) и частно-научные методы (формально-юридический, сравнительно-правовой, метод криминалистического моделирования).

Результаты

В криминалистической доктрине под криминалистическим обеспечением традиционно понимается система криминалистических знаний и основанных на них навыков и умений сотрудников правоохранительных органов использовать научные криминалистические рекомендации, применять криминалистические средства, методы и технологии в целях предотвращения, выявления, раскрытия и расследования преступлений [2, с. 207]. Применительно к рассматриваемой группе деяний, содержание криминалистического обеспечения образуют несколько взаимосвязанных элементов: научное обеспечение, предполагающее формирование криминалистической характеристики и частной методики расследования; технико-криминалистическое обеспечение, охватывающее средства обнаружения, фиксации и исследования цифровых следов; тактико-методическое обеспечение, включающее рекомендации по производству отдельных следственных действий; кадровое обеспечение, связанное с подготовкой субъектов расследования. Данный подход согласуется с разработанной Е.Р. Россинской теорией информационно-компьютерного обеспечения криминалистической деятельности, в рамках которой закономерности возникновения, движения, собирания и исследования компьютерной информации рассматриваются в качестве самостоятельного элемента предмета современной криминалистики [3, с. 195].

Для целей построения криминалистических рекомендаций преступления, совершаемые с использованием технологий искусственного интеллекта, целесообразно классифицировать в зависимости от функциональной роли соответствующих технологий в механизме преступной деятельности. К первой группе относятся деяния, в которых системы искусственного интеллекта выступают средством совершения преступления: создание синтезированных аудиовизуальных материалов (дипфейков) в целях хищения чужого имущества путем обмана, вымогательства, клеветы или незаконного распространения сведений о частной жизни; автоматизированная генерация фишинговых сообщений; создание вредоносных компьютерных программ. Ко второй группе следует отнести деяния, при совершении которых системы искусственного интеллекта и их компоненты выступают предметом посягательства: неправомерное воздействие на обучающие данные, несанкционированная модификация моделей, хищение результатов интеллектуальной деятельности в данной сфере. Третью группу образуют случаи применения рассматриваемых технологий для сокрытия преступлений и противодействия расследованию, в том числе для генерации ложных цифровых следов и маскировки сетевой активности.

Наибольшее практическое распространение получили способы, относящиеся к первой группе. Типичным примером выступает хищение денежных средств путем обмана с использованием синтезированной аудиозаписи или видеозаписи, имитирующей голос и внешность руководителя организации, родственника потерпевшего либо должностного лица. Современные генеративные модели позволяют получить убедительную имитацию голоса конкретного человека на основе короткого образца речи, размещенного в открытом доступе, что существенно повышает результативность приемов социальной инженерии. Подобные деяния квалифицируются по статьям 159, 128.1, 137 Уголовного кодекса Российской Федерации [4] в зависимости от направленности умысла. Отдельного

внимания заслуживает законопроект № 718538-8, предусматривающий дополнение ряда статей уголовного закона квалифицирующим признаком, связанным с использованием изображения или голоса потерпевшего либо иного лица, в том числе сформированных с применением специальных технологий [5]. Реализация данной законодательной инициативы потребует от криминалистической науки опережающей разработки средств и методов доказывания соответствующего признака.

Криминалистически значимыми являются и иные способы применения генеративных технологий: массовое создание персонализированных фишинговых сообщений, учитывающих сведения о потерпевшем из открытых источников; генерация фрагментов вредоносного кода лицами, не обладающими глубокими познаниями в программировании; обход систем биометрической аутентификации при дистанционном получении финансовых услуг. Общей тенденцией выступает снижение порога технической подготовки, необходимой для совершения высокотехнологичных преступлений, что влечет расширение круга потенциальных субъектов преступной деятельности и рост числа посягательств.

Ключевое значение для организации расследования имеет понимание особенностей механизма следообразования. Преступления рассматриваемой группы отражаются преимущественно в цифровой среде. В криминалистической литературе для обозначения соответствующих отражений используются категории «виртуальные следы», под которыми В.А. Мещеряков понимал изменения состояния автоматизированной информационной системы, связанные с событием преступления и зафиксированные на машинном носителе [6], а также «электронные доказательства», исследованные в работах В.Б. Вехова [7]. А.Б. Смушкин обоснованно рассматривает работу с цифровыми следами в качестве ядра формирующейся концепции цифровой криминалистики [8]. Цифровым следам присущи такие свойства, как опосредованный характер восприятия, отсутствие неразделимой связи с конкретным материальным носителем, легкость копирования, модификации и уничтожения, а также территориальная распределенность, поскольку значимая информация может находиться на серверах, расположенных в различных государствах.

Применение генеративных моделей порождает и специфические следы, ранее не известные криминалистической практике. К ним относятся артефакты синтеза изображения: нарушения анатомической достоверности, несогласованность освещения и теней, аномалии мимики и морганий, дефекты отображения фона. Синтезированная речь характеризуется особыми спектральными и интонационными закономерностями, отличающими ее от естественной. Следовую картину дополняют метаданные файлов, идентификаторы генеративных сервисов, сведения о сетевых соединениях, записи в журналах доступа, а также следы оплаты подписок на соответствующие сервисы. Выявление и интерпретация перечисленных следов требуют применения специальных знаний и постоянно обновляемых программных средств.

Существенные трудности связаны с установлением лица, применившего технологии искусственного интеллекта. Использование зарубежных сервисов, средств анонимизации сетевого трафика, подменных абонентских номеров и криптовалютных расчетов затрудняет ретроспективное восстановление цепочки действий преступника. В ходе расследования подлежит проверке версия о том, применялся ли общедоступный онлайн-сервис либо модель, развернутая на вычислительных мощностях самого субъекта, поскольку от данного обстоятельства зависят направления поиска следов и содержание запросов, направляемых операторам связи и администраторам информационных ресурсов.

Центральным элементом технико-криминалистического обеспечения выступает судебно-экспертное исследование цифрового контента. Методические основы судебной компьютерно-технической экспертизы, заложенные Е.Р. Россинской и А.И. Усовым [9], нуждаются в развитии применительно к задаче диагностики синтезированных материалов. Традиционные методики экспертного исследования видеозаписей и фонограмм ориентированы на выявление признаков монтажа, то есть механического соединения фрагментов. Однако синтезированный контент создается генеративной моделью целиком и не содержит монтажных переходов в привычном понимании, вследствие чего сложившиеся методические подходы оказываются недостаточными. Возникает потребность в разработке и валидации методик, основанных на анализе статистических закономерностей, присущих продукции генеративных моделей.

Дополнительную сложность создает состязательный характер развития рассматриваемых технологий: совершенствование генеративных моделей направлено в том числе на устранение распознаваемых артефактов, вследствие чего программные детекторы синтезированного контента быстро утрачивают достоверность и нуждаются в постоянной актуализации. Поскольку многие детекторы сами основаны на нейросетевых алгоритмах, функционирующих по принципу «черного ящика», возникает вопрос о соответствии их применения требованиям объективности, все-

сторонности и полноты исследований, а также научной обоснованности используемых методов, закрепленным в статье 8 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» [10]. Заключение эксперта должно быть проверяемым, что предполагает раскрытие в исследовательской части признаков, положенных в основу вывода, а не ограничение итоговой вероятностной оценкой, выданной алгоритмом. Перспективным направлением является сертификация и государственная валидация программных средств выявления синтезированного контента, а также производство подобных исследований с участием экспертов различных специальностей: в области компьютерной техники, видеотехники, фоноскопии и лингвистики.

Тактико-методическое обеспечение расследования рассматриваемых преступлений определяется неотложным характером работы с цифровыми следами. На первоначальном этапе подлежат производству осмотр места происшествия и осмотр электронных носителей информации, изъятие которых в ходе следственных действий осуществляется по правилам статьи 164.1 Уголовно-процессуального кодекса Российской Федерации с участием специалиста [11]. Значимым источником информации выступают результаты осмотра интернет-страниц, содержащих распространенный синтезированный контент, с подробной фиксацией адресов ресурсов, дат размещения и идентификаторов учетных записей. Промедление с фиксацией влечет риск утраты доказательственной информации вследствие удаления материалов правонарушителем или администрацией ресурса.

Тактика допроса потерпевшего по делам о хищениях, совершенных с применением синтезированных аудиовизуальных материалов, должна предусматривать детализацию обстоятельств восприятия: канала связи, качества изображения и звука, особенностей речи и поведения мнимого собеседника, содержания высказанных требований. Полученные сведения позволяют выдвинуть версию о применении генеративных технологий и определить предмет последующих экспертных исследований. Судебные экспертизы по данной категории дел целесообразно назначать на первоначальном этапе расследования, формулируя перед экспертом вопросы о наличии признаков синтеза, использованных технологиях и возможной принадлежности исходных образцов голоса или внешности конкретному лицу. Версия о синтезированном происхождении аудиовизуальных материалов подлежит проверке во всех случаях, когда подобные материалы имеют доказательственное значение, поскольку игнорирование данной версии создает риск судебной ошибки.

Результативность расследования во многом определяется организацией взаимодействия следователя со специализированными подразделениями органов внутренних дел, осуществляющими противодействие противоправному использованию информационно-коммуникационных технологий, с операторами связи, кредитными организациями и владельцами цифровых платформ. Трансграничный характер преступной деятельности обусловливает востребованность механизмов международного сотрудничества, включая направление запросов о правовой помощи и обмен сведениями по каналам международных полицейских организаций. Своевременное получение сведений от зарубежных провайдеров генеративных сервисов нередко имеет решающее значение для установления причастных лиц.

Вторая сторона рассматриваемой проблематики связана с применением технологий искусственного интеллекта в интересах самого расследования. Необходимость активного освоения криминалистикой новых информационных технологий последовательно обосновывалась Е.П. Ищенко [12]. Этико-правовые условия применения систем искусственного интеллекта в юридической деятельности исследованы Д.В. Бахтеевым [13]. А.А. Бессоновым разработаны подходы к использованию алгоритмов машинного обучения и математической статистики для криминалистического изучения преступлений, построения вероятностных моделей и выдвижения версий [14]. Практическое применение находят системы распознавания лиц и речи, средства автоматизированного анализа больших массивов данных о соединениях и транзакциях, инструменты выявления связей между эпизодами серийной преступной деятельности.

Вместе с тем применение алгоритмических средств в доказывании должно оставаться вспомогательным. Результаты работы систем искусственного интеллекта представляют собой ориентирующую информацию, подлежащую проверке процессуальными средствами, а ответственность за принимаемые процессуальные решения сохраняется за следователем и судом. Недопустимо перекладывание оценки доказательств на алгоритм, выводы которого не могут быть содержательно объяснены. Соблюдение принципа объяснимости выступает условием допустимости внедрения подобных систем в уголовное судопроизводство.

Самостоятельным элементом криминалистического обеспечения является кадровая составляющая. Расследование преступлений рассматриваемой группы требует от следователей и экспертов устойчивых представлений о прин-

ципах функционирования генеративных моделей, типичных способах их преступного применения и особенностях образуемых следов. Данное обстоятельство обусловливает потребность в обновлении программ высшего юридического образования и дополнительного профессионального образования, включении в курс криминалистики разделов, посвященных цифровым следам и синтезированному контенту, а также в создании специализированных учебных полигонов, моделирующих типичные следственные ситуации.

Заключение

Проведенное исследование позволяет сформулировать следующие выводы. Во-первых, преступления, совершаемые с использованием технологий искусственного интеллекта, образуют криминалистически однородную группу, объединенную общностью механизма следообразования и применяемых специальных знаний, что создает предпосылки для разработки соответствующей частной криминалистической методики. Во-вторых, приоритетным направлением технико-криминалистического обеспечения выступает создание и валидация экспертных методик диагностики синтезированного цифрового контента, отвечающих требованиям научной обоснованности и проверяемости. В-третьих, тактические рекомендации по производству следственных действий должны учитывать неотложный характер фиксации цифровых следов, необходимость участия специалиста и обязательность проверки версии о синтезированном происхождении аудиовизуальных материалов. В-четвертых, внедрение технологий искусственного интеллекта в деятельность органов расследования допустимо при сохранении вспомогательной роли алгоритмических средств и соблюдении принципа объяснимости их результатов.

Таким образом, криминалистическое обеспечение расследования преступлений, совершаемых с использованием технологий искусственного интеллекта, представляет собой развивающуюся систему научных положений, технических средств, тактических приемов и методических рекомендаций, формирование которой должно осуществляться с опережением динамики преступной деятельности. Согласованное развитие всех элементов данной системы, подкрепленное совершенствованием законодательства и подготовкой кадров, позволит обеспечить эффективное выявление, раскрытие и расследование преступлений данной группы в условиях продолжающейся цифровой трансформации общества.

Список литературы:

[1] Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (в редакции Указа Президента Российской Федерации от 15 февраля 2024 г. № 124) // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

[2] Белкин Р.С. Курс криминалистики: в 3 т. Т. 2: Частные криминалистические теории. М.: Юристъ, 1997. – 464 с.

[3] Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). – С. 193–202.

[4] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[5] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // СОЗД ГАС «Законотворчество». [Электронный ресурс]: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 05.07.2026).

[6] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Издательство Воронежского государственного университета, 2002. – 408 с.

[7] Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4 (11). – С. 46–50.

[8] Смушкин А.Б. Концепция цифровой криминалистики // Вестник Пермского университета. Юридические науки. 2021. Вып. 52. – С. 268–296.

[9] Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. – 416 с.

[10] Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // Собрание законодательства Российской Федерации. 2001. № 23. Ст. 2291.

[11] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. 2001. № 52 (часть I). Ст. 4921.

[12] Ищенко Е.П. Криминалистика и новые информационные технологии // Вестник криминалистики. 2009. Вып. 3 (31). – С. 6–15.

[13] Бахтеев Д.В. Искусственный интеллект: этико-правовые основы: монография. М.: Проспект, 2021. – 176 с.

[14] Бессонов А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. М.: Проспект, 2021. – 816 с.

References:

[1] Decree of the President of the Russian Federation of October 10, 2019 No. 490 "On the development of artificial intelligence in the Russian Federation" (as amended by Decree of the President of the Russian Federation of February 15, 2024 No. 124) // Collection of legislation of the Russian Federation. 2019. № 41. Art. 5700.

[2] Belkin R.S. Forensic course: in 3 vols. T. 2: Private forensic theories. M.: Lawyer, 1997. - 464 s.

[3] Rossinskaya E.R. Theory of information and computer support of forensic activities: concept, system, basic laws // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. № 2 (89). - S. 193-202.

[4] Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[5] Bill No. 718538-8 "On Amendments to the Criminal Code of the Russian Federation "// SOZD GAS" Lawmaking. "[Electronic resource]: https://sozd.duma.gov.ru/bill/718538-8 (access date: 05.07.2026).

[6] Meshcheryakov V.A. Crimes in the field of computer information: the foundations of the theory and practice of investigation. Voronezh: Voronezh State University Publishing House, 2002. - 408 s.

[7] Vekhov V.B. Electronic evidence: problems of theory and practice // Law and order: history, theory, practice. 2016. № 4 (11). - S. 46-50.

[8] Smushkin A.B. The concept of digital forensics // Bulletin of Perm University. Legal sciences. 2021. No. 52. - S. 268-296.

[9] Rossinskaya E.R., Usov A.I. Forensic computer-technical expertise. M.: Law and Law, 2001. - 416 s.

[10] Federal Law of May 31, 2001 No. 73-FZ "On State Forensic Activity in the Russian Federation "// Collection of Legislation of the Russian Federation. 2001. № 23. Art. 2291.

[11] Code of Criminal Procedure of the Russian Federation dated December 18, 2001 No. 174-FZ // Collection of Legislation of the Russian Federation. 2001. No. 52 (Part I). Art. 4921.

[12] Ishchenko E.P. Criminalistics and new information technologies // Bulletin of Criminalistics. 2009. No. 3 (31). - S. 6-15.

[13] Bakhteev D.V. Artificial intelligence: ethical and legal foundations: monograph. M.: Prospect, 2021. - 176 s.

[14] Bessonov A.A. Artificial intelligence and mathematical statistics in the forensic study of crimes: monograph. M.: Prospect, 2021. - 816 s.