Научная статья
УДК 343.98
EDN PWAZVK
DOI 10.17150/2411-6122.2026.3.45-55

Проблемы доказывания по делам о высокотехнологичных преступлениях: от цифрового следа к синтетическому доказательству

А.Ф. Реховский

Владивостокский государственный университет, г. Владивосток, Российская Федерация, a.rekhovskiy@vvsu.ru

Аннотация. Анализируются криминалистические и уголовно-процессуальные проблемы доказывания по делам о высокотехнологичных преступлениях в условиях распространения технологий генеративного искусственного интеллекта. Ставится задача выявления пробелов правового регулирования цифровых доказательств и обоснования необходимости нормативного закрепления категории «синтетическое доказательство». Методологическую основу составили сравнительно-правовой анализ, изучение материалов правоприменительной практики и обобщение зарубежных стандартов цифровой форензики. Рассмотрена природа цифрового следа, специфика синтетического контента как нового объекта доказывания, проблема процессуальной оценки вероятностных результатов автоматизированной детекции, а также трансграничный фактор и значение специальных знаний. Сделан вывод о необходимости дополнения процессуального законодательства самостоятельным понятием электронного доказательства, разработки экспертной методики оценки синтетического контента и синхронной подготовки частных криминалистических методик расследования. Предложен переход от реактивной к проактивной модели противодействия, сочетающей совершенствование законодательства, развитие института специальных знаний и превентивную работу с населением.

Ключевые слова: высокотехнологичные преступления, цифровой след, электронное доказательство, синтетическое доказательство, дипфейк, цифровая форензика, специальные знания.

Конфликт интересов. Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

Для цитирования: Реховский А.Ф. Проблемы доказывания по делам о высокотехнологичных преступлениях: от цифрового следа к синтетическому доказательству / А.Ф. Реховский. — DOI 10.17150/2411-6122.2026.3.45-55. — EDN PWAZVK // Сибирские уголовно-процессуальные и криминалистические чтения. — 2026. — № 3. — С. 45–55.

Original article

Problems of Proof in High-Tech Crime Cases: From Digital Traces to Synthetic Evidence

A.F. Rekhovskiy

Vladivostok State University, Vladivostok, the Russian Federation, a.rekhovskiy@vvsu.ru

Abstract. The author examines criminalistic and criminal procedure problems of proof in high-tech crime cases in the conditions of increasing use of generative artificial intelligence. The aim of the study is to identify gaps in the legal regula-

© Реховский А.Ф., 2026

tion of digital evidence and to demonstrate the necessity of including the category of "synthetic evidence" into law. Its methodological basis combines comparative-legal analysis, a review of the materials of law enforcement practice and a summary of international digital forensics standards. The article covers the nature of a digital trace, specifics of synthetic content as a new object of proof, the problem of procedural assessment of probabilistic automated detection results, as well as the trans-border factor and the significance of specialized knowledge. It concludes that there is a necessity to supplement procedural legislation with a concept of electronic evidence, to develop an expert methodology for evaluating synthetic content, and, simultaneously, to work out special criminalistic methods of investigation. The author proposes a transition from a reactive to a proactive model of counteraction, combining the improvement of legislation, the development special knowledge, and preventive public outreach.

Keywords: high-tech crimes, digital trace, electronic evidence, synthetic evidence, deepfake, digital forensics, special knowledge.

Conflict of interest. The author declares the absence of obvious and potential conflicts of interest related to the publication of this article.

For citation: Rekhovskiy A.F. Problems of Proof in High-Tech Crime Cases: From Digital Traces to Synthetic Evidence. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2026, no 3, pp. 45–55. (In Russian). EDN: PWAZVK. DOI: 10.17150/2411-6122.2026.3.45-55.

1. Постановка проблемы

Рост киберпреступности в 2019–2024 гг. осложняли прежде всего латентность и трансграничность; с 2024–2025 гг. к ним добавился новый вызов — массовое использование генеративного ИИ, в первую очередь дипфейков, для мошенничеств и хищений[1]. При этом средний ущерб на жертву продолжает расти, а синтетический (искусственно сгенерированный) контент образует новый класс доказательств, правовой статус которого в УПК РФ не определен.

Масштаб явления впечатляет: совокупный ущерб от киберпреступности исчисляется триллионами долларов в год, а сама киберпреступность по обороту сопоставима с экономикой крупного государства[2]. Традиционная криминалистика, ориентированная на материальные следы и линейную реконструкцию события, здесь не справляется: цифровая среда порождает следы иной природы — изменчивые, легко уничтожаемые, рассредоточенные между носителями и юрисдикциями, — что требует пересмотра и теории следа, и практического инструментария.

Статистика киберпреступности уже достаточно полно представлена в отраслевых отчетах, поэтому задача статьи иная — сформулировать конкретную проблему: отсутствие нормативно закрепленной категории «синтетическое доказательство» и связанные с этим процессуальные риски при использовании детекторов дипфейков. Для этого последовательно рассматриваются природа цифрового следа, специфика синтетического контента, оценка результатов его детекции, а также трансграничные, законодательные и кадровые факторы.

[1] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2025 года. URL: https://xn--b1aew.xn--p1ai/reports/item/77848182/ (дата обращения: 16.06.2026).

[2] Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. — Hague: Europol, 2024. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (дата обращения: 16.06.2026).

2. Теоретическое обоснование: цифровой след и его процессуальный статус

УПК РФ не содержит понятия «электронное» доказательство, довольствуясь термином «электронные носители информации»[3], из-за чего цифровые объекты — журналы, метаданные, переписку — искусственно относят к «иным документам» либо «вещественным доказательствам» [1, с. 15]. Приказ СК РФ № 62 (2024 г.) частично восполнил пробел[4]. Цифровые следы значимы не только по киберделам, но и по коррупции, убийствам, наркопреступлениям [2, с. 489]; в доктрине компьютерная информация уже рассматривается как самостоятельный вид доказательств [3]. Такой разрыв между практикой и нормой создает риск не единообразного применения.

Цифровой след неоднороден: на устройстве пользователя он выражается в файлах и кэше приложений, в сети — в журналах соединений и IP-адресах, в облаке — в резервных копиях и журналах доступа, отдельно стоят следы в распределенных реестрах и платежных системах. У каждой группы свой режим хранения, поэтому единого алгоритма собирания не существует. Главная особенность цифрового следа — волатильность: данные нередко перезаписываются или удаляются автоматически в течение часов. Отсюда вывод: специалист должен подключаться уже на стадии осмотра.

Уязвимость цифровых следов — их родовая черта: неосторожное действие способно необратимо изменить или уничтожить данные на носителе [4]. При этом доказательственную ценность имеет не только сама информация, но и метаданные — время, источник, условия создания файла, — которые следует рассматривать как самостоятельную разновидность цифрового следа [5, с. 76].

Ориентиром служит американское руководство NIST SP 800-86[5], которое выделяет четыре этапа работы с цифровыми доказательствами и пять атрибутов их допустимости: подлинность, точность, полноту, убедительность, допустимость. Модель нужно увязать с принципом допустимости доказательств (ст. 75 УПК РФ) и идеей непрерывности цепочки хранения (chain of custody), которая у нас как институт пока не оформлена [6, с. 260]. На практике целостность обеспечивается косвенно — протоколированием, хэшированием, — но без прямого требования документировать весь путь объекта остаются основания для сомнений в его неизменности.

3. Синтетический контент как новый объект доказывания

Дипфейк[6] сместил объект атаки с технической инфраструктуры на «человеческую архитектуру доверия». Три кейса 2024 г. показывают эволюцию схемы: хищение 25,6 млн долл. у Arup Group (Гонконг) через дипфейк-видеоконференцию; сорванная атака на руководителя WPP plc с клонированным голосом; провалившаяся атака на топ-менеджера Ferrari, разоблаченная

[3] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в ред. от 2025 г.) // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.

[4] О порядке работы с цифровыми доказательствами: приказ Следственного комитета Российской Федерации от 2024 г. № 62.

[5] Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response / National Institute of Standards and Technology. URL: https://csrc.nist.gov/pubs/sp/800/86/final (дата обращения: 16.06.2026).

[6] Термин «дипфейк» происходит от первого слова технологии глубокого машинного обучения ИИ («deep learning») и «fake» — «подделка». Дипфейк — это метод создания синтетического контента (аудио, изображения, видео, текста) с помощью различных моделей глубокого обучения.

контрольным вопросом — практическая реализация внеполосной верификации (out-of-band verification)[7], позже закрепленной в NIST Cybersecurity Framework 2.0[8]. В 2025 г. в России зафиксирован кратный рост дипфейков с образами должностных лиц.

Эти кейсы складываются в общую схему: сбор открытых данных о жертве, генерация убедительного синтетического образа, искусственная срочность, исключающая перепроверку, и само действие. Дипфейки выглядят гиперреалистично [7, с. 139], и эта схема формирует ядро криминалистической характеристики преступлений данного вида. Показательно: успех атаки определяет не качество подделки, а навык внеполосной верификации у жертвы[9].

Из этого следует криминалистически значимый вывод: дипфейк-атака не оставляет традиционных следов компрометации систем и потому невидима для классических средств защиты. При этом возникает вопрос о доказательственном статусе самой записи и записи, фиксирующей факт атаки: одна и та же видеозапись может одновременно быть орудием преступления (синтетический образ, обманувший жертву) и носителем доказательственной информации. Действующая классификация доказательств для такой двойственности готового решения не предлагает.

Сложен и вопрос квалификации: содеянное обычно охватывается составами мошенничества, но использование дипфейка как средства обмана влияет на оценку способа и степени общественной опасности деяния [8, с. 109–110]. Отдельная проблема — ответственность за изготовление и распространение синтетического контента как такового, для которой специальной нормы нет. Это утяжеляет доказывание: правоприменителю приходится устанавливать не только факт обмана, но и техническую природу примененного средства, а значит — вновь привлекать специальные знания и экспертизу.

4. Процессуальная оценка результатов детекции дипфейков

Синтетический контент сегодня выявляют детекторы на основе машинного обучения и анализ метаданных[10], но их результат — не категоричное заключение, а вероятностная оценка («98 % вероятности синтетической генерации»). Теория доказательств строится на бинарной логике допустимости, поэтому для вероятностного заключения нужны: методика экспертной оценки достоверности детекции (по аналогии с почерковедческой или фоноскопической экспертизой); законодательный порог вероятности, при котором заключение может лечь в основу обвинения; и само нормативное определение «синтетического доказательства», отграничивающее его от обычных аудио- и видеозаписей.

Осложняет дело «гонка вооружений» генеративных и детектирующих алгоритмов: модель, вчера уверенно находившая подделку, завтра бессильна перед новой версией генератора. В литературе это называют «постоянным противоборством генеративных моделей и дискриминато-

[7] РБК. «Драконы», «муравьи», ИИ и дипфейки: как мошенники используют новые технологии. 2025. 26 окт.

[8] Cybersecurity Framework 2.0 / National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата обращения: 16.06.2026).

[9] ИИ против Ferrari: разбор изощрённой атаки с применением deepfake. URL: https://www.securitylab.ru/news/550579.php (дата обращения: 16.06.2026).

[10] ИИ против хакеров: новая эра форензики в 2025 году / Forensicanvil. 2025. URL: https://forensicanvil.ru/blog/ai-vs-hackers-forensics/ (дата обращения: 16.06.2026).

ров» («the ongoing arms race between generative models and discriminators») [9] — замкнутым циклом, где усложняются и генерация дипфейков, и их выявление. В итоге цифровая криминалистика все больше автоматизируется, но задача обеспечить достоверность результатов только усложняется.

Следовательно, заключение о синтетическом происхождении записи имеет ограниченный срок годности и должно сопровождаться указанием методики, версии инструмента и условий исследования. Оно не обладает заранее установленной силой и подлежит проверке в совокупности с другими доказательствами (ст. 17, 88 УПК РФ) — на легкую изменяемость электронных доказательств уже не раз обращали внимание [4].

Отсутствие нормативного определения создает два противоположных риска: необоснованное исключение записей, ставших объектом манипуляции, хотя сама запись может фиксировать факт преступления, а не быть его инструментом; и, наоборот, неконтролируемое использование вероятностных заключений как единственного основания решения. Баланс — статус одного из доказательств, требующего проверки, но не отвергаемого «априори» только из-за вероятностной формы вывода.

5. Трансграничный фактор и сроки сохранности цифровых следов

Осложняет дело и трансграничность: по данным Европола, более 60 % расследованных трансграничных киберпреступлений требовали не менее двух запросов о правовой помощи со средним сроком исполнения 6–14 месяцев[11] — намного дольше типичного срока хранения журналов и метаданных у операторов связи. Международная правовая помощь систематически отстает от волатильности цифровых следов, обесценивая доказательства еще до их истребования [10, с. 391].

Цифровая среда снимает территориальные ограничения: этапы преступления могут быть разнесены между странами, а инфраструктура атаки — размещена там, где сотрудничество затруднено. Это порождает проблему разграничения компетенции, и коллизия между быстрым доступом к данным и защитой персональных данных. Решение — прямой трансграничный запрос данных у провайдеров [10], уже действующий по Второму протоколу к Будапештской конвенции[12] и в виде европейских ордеров e-Evidence[13].

Конвенция ООН против киберпреступности[14], подписанная в октябре 2025 г. 72 государствами, включая Россию, закладывает основу для взаимодействия с частным сектором почти в реальном времени. Но ее эффективность будет зависеть от скорости имплементации национальных процедур, а не от самого факта подписания — это стоит учесть уже на стадии подготовки к ратификации. По состоянию на май 2026 г. договор подписали 74 страны, но ратифицировали его только Катар, Азербайджан и Вьетнам.

[11] Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. Hague: Europol, 2024. P. 28–32. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (дата обращения: 16.06.2026).

[12] Second Additional Protocol supplementing the Convention on Cybercrime (CETS No. 185). Section 2 — Procedures enhancing direct cooperation with providers and entities in other Parties / Council of Europe.

[13] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 28 June 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings («e-Evidence Regulation»).

[14] Конвенция Организации Объединённых Наций против киберпреступности (принята Генеральной Ассамблеей ООН 24 дек. 2024 г., открыта для подписания 25 окт. 2025 г., г. Ханой).

 DOI 10.17150/2411-6122.2026.3.45-55 ISSN 2411-6122

6. Обновление законодательства и его связь с криминалистической методикой

Статья 272.1 УК РФ[15] криминализировала незаконный оборот персональных данных, а ст. 274.3–274.5[16] — использование SIM-боксов, виртуальных АТС и оборот учетных записей. Эти новеллы расширяют предмет доказывания, но не решают методическую проблему: частных криминалистических методик расследования по новым составам пока нет, хотя общие методические основы уже разработаны и могут стать отправной точкой [7].

Системным документом стала Концепция государственной системы противодействия ИКТ-преступлениям[17], задающая ориентиры для законодательства, техники и цифровой грамотности населения. Но между принятием нормы и рабочей методикой ее применения неизбежен временной разрыв, который практика заполняет эмпирически.

Такую ситуацию можно охарактеризовать как методический вакуум: криминализация опережает разработку алгоритмов расследования, и следователь остается один на один с преступлением, для которого еще нет методики [11, с. 14–28]. Пробел закрывают ведомственные акты — прежде всего Приказ СК РФ № 62, — но полноценной заменой частной методике они не служат, а сам разрыв ощутимее тем, чем быстрее растет Особенная часть УК [12, с. 2–6]. Устранить его способна только синхронная подготовка методик уже на стадии законопроекта, в тесной связке с криминалистами.

7. Роль специальных знаний и судебной экспертизы

Институт специальных знаний по делам о высокотехнологичных преступлениях становится системообразующим. Е.Р. Россинская отмечает: такие знания «перешли из разряда факультативных в категорию обязательных», поскольку цифровой след неотделим от программно-аппаратной среды [13, с. 173–178]. Чем раньше на месте происшествия появляется специалист, тем полнее доказательственная база; сама фиксация электронно-цифровых следов остается предметом споров [14, с. 30–33].

Э. Кейси формулирует это ясно: цифровое доказательство легко изменить, повредить или уничтожить — случайно или намеренно [15]. Поэтому специалист нужен с первых минут расследования. Ошибка первичной фиксации — некорректное отключение устройства, нарушение целостности данных, отсутствие хэширования — почти всегда необратима [16, с. 44–51].

Синтетический контент требует нового вида судебной экспертизы — установления факта искусственной генерации медиаматериалов [17, с. 152–156]. Направление уже складывается, хотя методически отстает от практики [18, с. 68–80]. Ключевое условие — воспроизводимость результата, проверяемая другим экспертом. Автоматизированные системы форензик-анализа находят закономерности, недоступные при руч-

[15] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30 нояб. 2024 г. № 421-ФЗ // Официальный интернет-портал правовой информации. URL: http://www.kremlin.ru/acts/bank/51382 (дата обращения: 16.06.2026).

[16] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 31 июля 2025 г. № 282-ФЗ.

[17] Об утверждении Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации от 30 дек. 2024 г. № 4154-р. URL: http://government.ru/docs/53922/ (дата обращения: 16.06.2026).

ном просмотре, но заменить экспертную интерпретацию не могут.

Кадровый вопрос стоит отдельно: следователь должен обладать не только процессуальной, но и устойчивой цифровой компетенцией [19]. Это обусловливает необходимость повышать цифровую квалификацию сотрудников и выстраивать каналы связи с экспертными учреждениями. Без решения кадрового вопроса предупреждают Ю.В. Гаврилин и Ю.Е. Салеева, любые новеллы рискуют остаться на бумаге [20, с. 54–63].

8. Латентность и превентивное противодействие

Латентность высокотехнологичных преступлений остается главным препятствием борьбы с новыми проявлениями кибепреступности: по оценке И.А. Ефремовой, она достигает 80–90 % [21, с. 122–131]. Причины понятны — низкая цифровая грамотность потерпевших, социальная инженерия, маскировка следов. К. Хаднаги отмечает: социальная инженерия бьет по «уязвимостям человеческой психологии», а не программ, и потому обходит даже совершенную техническую защиту [22].

Многие потерпевшие либо вовсе не обращаются в полицию, либо делают это с таким опозданием, что цифровые следы уже потеряны. Европол приводит по IOCTA 2024 неутешительную цифру: в правоохранительные органы обращается около 13 % жертв кибермошенничества, а средний срок обращения превышает 30 суток[18]. Отраслевая статистика говорит о том же: до 70 % инцидентов с использованием социальной инженерии так и остаются вне поля зрения правоохранителей[19].

Раз большинство атак реализуется через манипуляцию доверием, акцент смещается на превентивную модель. А.К. Жарова считает цифровую грамотность ключевым фактором виктимизации [23, с. 45–56]. В.А. Гусев формулирует цифровую гигиену как устойчивую систему индивидуальных мер защиты, а не разовую рекомендацию [24, с. 102–108]. NIST SP 800-161 Rev. 2[20] подтверждает то же: эффективнее всего сочетание технических средств защиты с ростом осведомленности пользователей.

Превентивная стратегия должна сочетать организационно-технические меры — многофакторную аутентификацию, независимую верификацию финансовых операций — с систематическим просвещением. Проактивная модель предполагает не только реагирование на уже совершенные деяния, но и профилактику, снижающую саму вероятность виктимизации.

9. Выводы

Проведенное исследование позволяет сформулировать следующие выводы и предложения.

[18] Internet Organised Crime Threat Assessment (IOCTA) 2024 / Europol. Hague: Europol, 2024. P. 28–32. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report (дата обращения: 16.06.2026).

[19] Positive Technologies. Киберпреступность и защита бизнеса: отчёт за 2024 год. М.: Positive Technologies, 2025. С. 14–17. URL: https://www.ptsecurity.com/ww-ru/analytics/cybersecurity-threats-2025 (дата обращения: 16.06.2026).; Positive Technologies. Актуальные киберугрозы: IV квартал 2024 года — I квартал 2025 года. URL: https://ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 04.07.2026).

[20] NIST SP 800-161 Rev. 2. Developing Trust Frameworks for Securing Critical Infrastructure Using Artificial Intelligence. Gaithersburg: NIST, 2025. URL: https://csrc.nist.gov/pubs/sp/800/161/r2/final (дата обращения: 16.06.2026).

1. Дополнить УПК РФ нормой об электронных (цифровых) доказательствах как самостоятельном виде с признаками допустимости (подлинность, целостность, полнота, цепочка хранения), адаптированными к ст. 74 УПК РФ.

2. Разработать экспертную методику оценки автоматизированной детекции синтетического контента со шкалой вероятностных значений и закрепить понятие «синтетическое доказательство» постановлением Пленума ВС РФ либо ведомственным актом.

3. Заключение о синтетическом происхождении записи не имеет заранее установленной силы и проверяется в совокупности с другими доказательствами; обязательны указание методики, версии инструмента и условий исследования.

4. Введение новых составов о высокотехнологичных преступлениях целесообразно сопровождать обязательным заключением НИИ криминалистики соответствующих ведомств о готовности методического обеспечения на стадии законопроекта, а не постфактум.

5. Своевременное привлечение специалиста на стадии осмотра и изъятия носителей сохраняет доказательственное значение цифровых следов; ошибки первичной фиксации обычно неустранимы.

6. Подписание Конвенции ООН против киберпреступности необходимо, но недостаточно; ключевой фактор — сокращение сроков исполнения запросов о правовой помощи до сроков технической сохранности следов.

Системное решение этих проблем позволит перейти от фрагментарного реагирования к проактивной криминалистической модели, сочетающей развитие законодательства, специальных знаний и превентивную работу с населением.

Список использованной литературы

1. Поляков В.В. Структура и содержание криминалистической характеристики высокотехнологичных преступлений / В.В. Поляков. — DOI 10.17803/1994-1471.2024.164.7.147-159. — EDN MCYWBH // Актуальные проблемы российского права. — 2024. — Т. 19, № 7. — С. 147–159.

2. Кашапова А.И. Цифровой след как инструмент раскрытия преступлений в условиях киберреальности / А.И. Кашапова, А.Г. Маркелов. — EDN IYIVDJ // Вестник науки. — 2025. — Т. 2, № 12 (93). — С. 486–493.

3. Зигура Н.А. Компьютерная информация как вид доказательства в уголовном процессе России / Н.А. Зигура. — Москва : Юрлитинформ, 2011. — 176 с.

4. Жужлов И.С. Цифровые следы: понятие, роль и значение в современной криминалистике / И.С. Жужлов. — DOI 10.25136/2409-7136.2026.2.78312. — EDN LCLUPQ // Юридические исследования. — 2026. — № 2. — С. 167–183.

5. Хомяков Э.Г. О сущности цифровых следов в криминалистике и их фиксации / Э.Г. Хомяков. — EDN ENYUWP // Общество, право, государственность: ретроспектива и перспектива. — 2025. — № 1 (21). — С. 71–82.

6. Шимон Д.В. Проблемы использования цифровых доказательств в уголовном судопроизводстве / Д.В. Шимон, А.А. Теучеж. — DOI 10.24412/2073-3313-2026-5-259-264. — EDN ZDHPCV // Закон и право. — 2026. — № 5. — С. 259–264.

7. Климова Я.А. Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия / Я.А. Климова. — DOI 10.17803/1994-1471.2025.179.10.133-143. — EDN TBAUNR // Актуальные проблемы российского права. — 2025. — Т. 20, № 10. — С. 133–143.

8. Долгиева М.М. Квалификация дипфейк-мошенничества и киберпохищения человека / М.М. Долгиева. — DOI 10.17803/1994-1471.2024.168.11.106-113. — EDN GDLNXP // Актуальные проблемы российского права. — 2024. — Т. 19, № 11. — С. 106–113.

9. The Unwinnable Arms Race of AI Image Detection / T. Aczel, L. Vettor, A. Plesner, R. Wattenhofer. — Switzerland : ETH Zürich, 2025. — URL: https://openreview.net/pdf?id=atCFKHOV17.

10. Реховский А.Ф. Новое законодательство ЕС о цифровых доказательствах: преобразование процедур трансграничного доступа и вызовы судебных гарантий / А.Ф. Реховский. — DOI 10.34670/AR.2026.18.55.037. — EDN WBANYQ // Вопросы российского и международного права. — 2025. — Т. 15, № 12А. — С. 390–396.

11. Иванов В.И. Темная сторона цифровизации российского общества: киберпреступность и ее вызовы / В.И. Иванов. — DOI 10.25136/2409-7543.2025.2.74155. — EDN NWBTNJ // Вопросы безопасности. — 2025. — № 2. — С. 14–26.

12. Халиков А.Н. Применение общих положений методики расследования в отношении новых составов преступлений, криминализованных уголовным законом / А.Н. Халиков. — DOI 10.18572/1812-3783-2023-6-2-6. — EDN JRGYSB // Российский следователь. — 2023. — № 6. — С. 2–6.

13. Россинская Е.Р. Концепция частной теории цифровизации судебно-экспертной деятельности / Е.Р. Россинская. — DOI 10.24412/2414-3995-2022-5-173-178. — EDN EFXBZH // Вестник экономической безопасности. — 2022. — № 5. — С. 173–178.

14. Ткачев А.В. К вопросу о придании особого процессуального и криминалистического статуса компьютерной (цифровой) информации / А.В. Ткачев. — DOI 10.18572/2072-442X-2022-2-30-33. — EDN ELEIJX // Эксперт-криминалист. — 2022. — № 2. — С. 30–33.

15. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet / E. Casey. — 3rd ed. — Academic Press, 2011. — 807 p.

16. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами / А.А. Бессонов. — DOI 10.17803/2311-5998.2019.55.3.046-052. — EDN IHORPB // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 3 (55). — С. 44–51.

17. Пшава В.В. Некоторые аспекты использования возможностей искусственного интеллекта в процессе доказывания в уголовном судопроизводстве / В.В. Пшава, В.В. Плетнев, Е.А. Стешина. — DOI 10.24412/2411-2275-2025-2-152-156. — EDN NAULWC // Право и практика. — 2025. — № 2. — С. 152–156.

18. Россинская Е.Р. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») / Е.Р. Россинская, А.И. Семикаленова. — DOI 10.17223/22253513/42/5. — EDN DLEOHJ // Вестник Томского государственного университета. Право. — 2021. — № 42. — С. 68–80.

19. Овчинский В.С. Криминология цифрового мира : учебник / В.С. Овчинский. — Москва : Норма, 2024. — 352 с.

20. Гаврилин Ю.В. Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности / Ю.В. Гаврилин, Ю.Е. Салеева. — DOI 10.24412/2072-9391-2023-266-99-105. — EDN LONKER // Труды Академии управления МВД России. — 2023. — № 2 (66). — С. 54–63.

21. Ефремова И.А. Особенности квалификации преступлений в сфере компьютерной информации и противодействия им / И.А. Ефремова. — DOI 10.52468/2542-1514.2025.9(1).122-131. — EDN MQUHVB // Правоприменение. — 2025. — Т. 9, № 1. — С. 122–131.

22. Hadnagy C. Social Engineering: the Science of Human Hacking / C. Hadnagy. — 2nd ed. — John Wiley & Sons, 2018. — 320 p.

23. Жарова А.К. Технологии дипфейк: социально-правовые риски нарушения частной жизни лица и правовые решения / А.К. Жарова. — DOI 10.47475/2311-696X-2025-45-2-63-68. — EDN NGILIG // Правопорядок: история, теория, практика. — 2025. — № 2 (45). — С. 63–68.

24. Гусев В.А. Цифровая гигиена vs. Киберпреступность / В.А. Гусев. — DOI 10.24412/1999-6241-2022-188-102-108. — EDN UIMYSU // Психопедагогика в правоохранительных органах. — 2022. — № 1 (88). — С. 102–108.

References

1. Polyakov V.V. Structure and Content of Forensic Characteristics of High-Tech Crimes. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2024, vol. 19, no. 7, pp. 147–159. (In Russian). EDN: MCYWBH. DOI: 10.17803/1994-1471.2024.164.7.147-159.

2. Kashapova A.I., Markelov A.G. Digital Footprint as a Tool for Solving Crimes in Context of Cyber Reality. *Vestnik nauki = Journal of Science*, 2025, no. 12, pp. 486–493. (In Russian). EDN: IYIVDJ.

3. Zigura N.A. *Computer Information as a Type of Evidence in Russian Criminal Process.* Moscow, Yurlitinform Publ., 2011. 176 p.

4. Zhuzhlov I.S. Digital Traces: Concept, Role, and Significance in Modern Forensic Science. *Yuridicheskie issledovaniya = Legal Studies*, 2026, no. 2, pp. 167–183. (In Russian). EDN: LCLUPQ. DOI: 10.25136/2409-7136.2026.2.78312.

5. Khomyakov Eh.G. On the Nature of Digital Traces in Forensics and their Fixation. *Obshchestvo, pravo, gosudarstvennost': retrospektiva i perspektiva = Society, Law, and the State: A Retrospective and Perspective*, 2025, no. 1, pp. 71–82. (In Russian). EDN: ENYUWP.

6. Shimon D.V., Teuchezh A.A. Problems of Using Digital Evidence in Criminal Proceedings. *Zakon i pravo = Law and Right*, 2026, no. 5, pp. 259–264. (In Russian). EDN: ZDHPCV. DOI: 10.24412/2073-3313-2026-5-259-264.

7. Klimova Ya.A. Core Principles of a Special Forensic Methodology for Investigating Crimes Committed Using Deepfake Technology: From Theory to Cyber-Investigation Practice. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2025, vol. 20, no. 10, pp. 133–143. (In Russian). EDN: TBAUNR. DOI: 10.17803/1994-1471.2025.179.10.133-143.

8. Dolgieva M.M. Classification of Deepfake Fraud and Cyber Kidnapping. *Aktual'nye problemy rossiiskogo prava = Topical Problems of Russian Law*, 2024, vol. 19, no. 11, pp. 106–113. (In Russian). EDN: GDLNXP. DOI: 10.17803/1994-1471.2024.168.11.106-113.

9. Aczel T., Vettor L., Plesner A., Wattenhofer R. *The Unwinnable Arms Race of AI Image Detection*. Switzerland, ETH Zürich, 2025. Available at: https://openreview.net/pdf?id=atCFKHOV17.

10. Rekhovskii A.F. New EU Legislation on Digital Evidence: Transforming Cross-Border Access Procedures and the Challenges to Judicial Guarantees. *Voprosy rossiiskogo i mezhdunarodnogo prava = Matters of Russian and International Law*, 2025, vol. 15, no. 12A, pp. 390–396. (In Russian). EDN: WBANYQ. DOI: 10.34670/AR.2026.18.55.037.

11. Ivanov V.I. The Dark Side of the Digitization of Russian Society: Cybercrime and its Challenges. *Voprosy bezopasnosti = Security Issues*, 2025, nol. 2, pp. 14–26. (In Russian). EDN: NWBTNJ. DOI: 10.25136/2409-7543.2025.2.74155.

12. Khalikov A.N. Application of General Provisions of the Investigation Methodology to New Constituent Elements of Offenses Criminalized by the Criminal Law. *Rossiiskii sledovatel' = Russian Investigator*, 2023, no. 6, pp. 2–6. (In Russian). EDN: JRGYSB. DOI: 10.18572/1812-3783-2023-6-2-6.

13. Rossinskaya E.R. The Concept of a Particular Theory of the Digitalization of Forensic Expert Activity. *Vestnik ekonomicheskoi bezopasnosti = Bulletin of Economic Security*, 2022, no. 5, pp. 173–178. (In Russian). EDN: EFXBZH. DOI: 10.24412/2414-3995-2022-5-173-178.

14. Tkachev A.V. On the Assignment of a Special Procedural and Criminalistic Status to Computer (Digital) Information. *Ekspert-kriminalist = Expert-Criminalist*, 2022, no. 2, pp. 30–33. (In Russian). EDN: ELEIJX. DOI: 10.18572/2072-442X-2022-2-30-33.

15. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Academic Press, 2011. 807 p.

16. Bessonov A.A. On Some Possibilities of Modern Forensic Science in Working with Electronic Traces. *Vestnik Universiteta imeni O.E. Kutafina = Courier of the Kutafin Moscow State Law University*, 2019, no. 3, pp. 44–51. (In Russian). EDN: IHORPB. DOI: 10.17803/2311-5998.2019.55.3.046-052.

17. Pshava V.V., Pletnev V.V., Steshina E.A. Some Aspects of Using Artificial Intelligence in the Process of Evidence in Criminal Proceedings. *Pravo i praktika = Law and Practice*, 2025, no. 2, pp. 152–156. (In Russian). EDN: NAULWC. DOI: 10.24412/2411-2275-2025-2-152-156.

18. Rossinskaya E.R., Semikalenova A.I. Information-Computer Forensic Models of Computer Crimes as the Elements of Forensic Techniques (Using the Example of "Cyber Blackmail"). *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo = Tomsk State University Journal of Law*, 2021, no. 42, pp. 68–80. (In Russian). EDN: DLEOHJ. DOI: 10.17223/22253513/42/5.

19. Ovchinskii V.S. *Criminology of the Digital World.* Moscow, Norma Publ., 2024. 352 p.

20. Gavrilin Yu.V., Saleeva Yu.E. Development of the Doctrine of Forensic Registration in the Context of Digital Transformation of Crime. *Trudy Akademii upravleniya MVD Rossii = Proceedings of the Management Academy of the Ministry of the Interior of Russia*, 2023, no. 2, pp. 54–63. (In Russian). EDN: LONKER. DOI: 10.24412/2072-9391-2023-266-99-105.

21. Efremova I.A. Peculiarities of Qualification of Crimes in the Field of Computer Information and Counteraction to them. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 1, pp. 122–131. (In Russian). EDN: MQUHVB. DOI: 10.52468/2542-1514.2025.9(1).122-131.

22. Hadnagy C. *Social Engineering: The Science of Human Hacking*. 2nd ed. John Wiley & Sons, 2018. 320 p.

23. Zharova A.K. Dipfake Technologies: Socio-Legal Risks of Violation of Individual's Privacy and Legal Solutions. *Pravoporyadok: istoriya, teoriya, praktika = The Rule of Law: History, Theory, Practice*, 2025, no. 2, pp. 63–68. (In Russian). EDN: NGILIG. DOI: 10.47475/2311-696X-2025-45-2-63-68.

24. Gusev V.A. Digital Hygiene vs. Cybercrime. *Psikhopedagogika v pravookhranitel'nykh organakh = Psycho-Pedagogics in Law Enforcement Agencies*, 2022, no. 1, pp. 102–108. (In Russian). EDN: UIMYSU. DOI: 10.24412/1999-6241-2022-188-102-108.

Информация об авторе

Реховский Александр Федорович — кандидат юридических наук, доцент, доцент кафедры уголовно-правовых дисциплин, Институт права, Владивостокский государственный университет, 690014, Российская Федерация, г. Владивосток, ул. Гоголя, 41.

Author Information

Rekhovsky, Aleksandr F. — Ph.D. in Law, Ass. Professor, Department of Criminal Law Disciplines, Institute of Law, Vladivostok State University, 41 Gogol Str., Vladivostok, 690014, the Russian Federation.

Поступила в редакцию / Received 05.07.26

Одобрена после рецензирования / Approved after reviewing 17.09.26

Принята к публикации / Accepted 15.10.26

Дата онлайн-размещения / Available online 09.11.26