

DOI: <http://dx.doi.org/10.21686/2411-118X-2026-2-134-142>

## **Теоретические основания доверия к цифровым доказательствам в условиях развития технологий искусственного интеллекта**

**П. С. Шевчук**

Доктор технических наук, профессор, профессор кафедры «Информатика»  
Ростовского государственного университета путей сообщения;  
Профессор кафедры «Информационная безопасность в вычислительных системах и сетях»  
Донского государственного технического университета  
Адрес: ФГБОУ ВО «Ростовский государственный университет путей сообщения»,  
344038, г. Ростов-на-Дону, площадь Ростовского стрелкового полка народного ополчения, 2;  
ФГБОУ ВО «Донской государственный технический университет»,  
344003, г. Ростов-на-Дону, площадь Гагарина, 1  
E-mail: petr.shevchuk@mail.ru

**И. П. Напханенко**

кандидат юридических наук, доцент,  
заведующий кафедрой «Административное право и уголовно-правовые дисциплины»  
Ростовского государственного университета путей сообщения.  
Адрес: ФГБОУ ВО «Ростовский государственный университет путей сообщения»,  
344038, г. Ростов-на-Дону, площадь Ростовского стрелкового полка народного ополчения, 2.  
E-mail: Nip1966@yandex.ru

**О. О. Корытько,**

директор НП РПО «Белые паруса»  
Адрес: НП РПО «Белые паруса»,  
350053, г. Краснодар, ул. Средняя, 53  
E-mail: korutko@bk.ru

## **Theoretical foundations of trust in digital evidence in the context of the development of artificial intelligence technologies**

**P. S. Shevchuk**

Doctor of Technical Sciences, Professor, Professor of the Department "Computer Science" of the  
Rostov State Transport University,  
Professor of the Department "Information Security in Computing Systems and Networks" of the Don  
State Technical University  
Address: Rostov State Transport University,  
2 Rostov Rifle Regiment of the People's Militia Square,  
Rostov-on-Don, 344038, Russian Federation  
Don State Technical University, 1 Gagarin Square,  
Rostov-on-Don, 344003, Russian Federation  
E-mail: petr.shevchuk@mail.ru

**I. P. Napkhanenko**

PhD in Law, Associate Professor,  
Head of the Department of Administrative Law and Criminal Law Disciplines of the  
Rostov State Transport University.  
Address: Rostov State Transport University,  
2 Rostov Rifle Regiment of the People's Militia Square,  
Rostov-on-Don, 344038, Russian Federation  
E-mail: Nip1966@yandex.ru

**O. O. Koritko**

Director of the NP RPO "White Sails"  
Address: NP RPO "White Sails", 53 Srednyaya str.  
Krasnodar, 350053, Russian Federation  
E-mail: korutko@bk.ru

*Поступила 26.02.2026 Принята к печати 15.03.2026*

## Аннотация

В статье исследуется проблема обеспечения доверия к цифровым доказательствам в условиях стремительного развития технологий искусственного интеллекта и генеративных нейросетевых моделей. Предметом исследования являются теоретические основания такого доверия, а также фундаментальные ограничения современных экспертных методик верификации электронных файлов, применяемых в уголовном и гражданском судопроизводстве. Методологическую основу исследования составляет междисциплинарный подход, интегрирующий методы системного анализа, цифровой форензики и сравнительно-правового исследования. Проведен структурный анализ четырех групп методов верификации цифровых файлов: анализа метаданных EXIF, исследования структуры файла, проверки системных журналов и идентификации устройства. Для каждой группы выявлены конкретные уязвимости, возникающие при применении генеративных состязательных сетей (GAN), специализированных инструментов манипуляции метаданными и методов обхода системных ограничений мобильных устройств.

Научная новизна работы заключается в формализации модели многоэтапной фальсификации цифрового объекта, включающей три последовательных этапа: генеративный синтез изображений с имитацией характеристик конкретного устройства, глубокую манипуляцию метаданными EXIF с полной перезаписью временных, геолокационных и аппаратных атрибутов, а также внедрение файла на целевое устройство с использованием привилегированного доступа и синхронизацией системных временных меток. Впервые проведен комплексный анализ технологической асимметрии между средствами фальсификации и верификации цифровых доказательств, демонстрирующий, что каждому методу экспертизы может быть противопоставлена доступная контрмера, нейтрализующая его эффективность.

На основании полученных результатов обосновывается необходимость введения в судебную практику принципа презумпции сомнительности цифровых доказательств, предполагающего обязательное комплексное исследование электронных файлов с указанием границ применимости экспертных методик. Сформулированы практические рекомендации по совершенствованию нормативно-правовой базы, разработке мультидисциплинарных программ детектирования фальсификаций и модернизации экспертных стандартов оценки подлинности электронных доказательств.

**Ключевые слова:** цифровые доказательства, искусственный интеллект, генеративные состязательные сети, цифровая криминалистика, метаданные EXIF, фальсификация, допустимость доказательств, нейросетевой синтез, презумпция сомнительности, информационной безопасности, цифровые данные, идентификация, верификации, подделка, искажение, целостность.

## Abstract

The article examines the problem of ensuring trust in digital evidence in the context of the rapid development of artificial intelligence technologies and generative neural network models. The subject of the research is the theoretical foundations of such trust, as well as the fundamental limitations of modern expert methods for verifying electronic files used in criminal and civil proceedings. The methodological basis of the research is an interdisciplinary approach that integrates methods of system analysis, digital forensics and comparative legal research. A structural analysis of four groups of digital file verification methods has been performed: EXIF metadata analysis, file structure research, system log verification, and device identification. Specific vulnerabilities have been identified for each group that arise when using generative adversarial networks (GANS), specialized metadata manipulation tools, and methods to circumvent system limitations of mobile devices.

The scientific novelty of the work lies in the formalization of a model of multi-stage falsification of a digital object, which includes three successive stages: generative image synthesis with imitation of the characteristics of a specific device, deep manipulation of EXIF metadata with complete overwriting of time, geolocation and hardware attributes, as well as file embedding on the target device using privileged access and synchronization of system timestamps. For the first time, a comprehensive analysis of the technological asymmetry between the means of falsification and verification of digital evidence has been conducted, demonstrating that each examination method can be countered by an available countermeasure that neutralizes its effectiveness.

Based on the results obtained, the necessity of introducing into judicial practice the principle of the presumption of the dubiousness of digital evidence, which implies a mandatory comprehensive study of electronic files indicating the limits of applicability of expert methods. Practical recommendations are formulated

to improve the regulatory framework, develop multidisciplinary fraud detection programs, and modernize expert standards for assessing the authenticity of electronic evidence.

**Keywords:** digital evidence, artificial intelligence, generative adversarial networks, digital forensics, EXIF metadata, falsification, admissibility of evidence, neural network synthesis, presumption of doubt, information security, digital data, identification, verification, forgery, distortion, integrity.

## Введение

Современные реалии цифрового пространства характеризуются стремительным развитием технологий хранения, обработки и масштабной фальсификации цифровых данных. Смещение цифровых доказательств в центр юридических процессов и судебных разбирательств сопряжено с расширением арсенала средств для модификации, подделки и искажения исходной информации [1, 2]. Под сомнение ставятся не только технические методы верификации, но и сам принцип достоверности электронных источников.

В условиях динамичных изменений в области искусственного интеллекта (далее – ИИ), нейросетевых алгоритмов и цифровой криминалистики, вопрос происхождения цифрового файла приобретает фундаментальное значение для судебной экспертизы [3]. Ключевая проблема заключается в принципиальной невозможности эмпирически обоснованного заключения о подлинности файла на основании используемых методик, программного обеспечения и инструментов. Констатация отсутствия признаков монтажа в настоящее время свидетельствует лишь о пределах применяемых экспертных технологий, но не об отсутствии факта подделки как такового [4].

С правовой точки зрения рассматриваемая проблема ставит под угрозу поддержание таких принципов доказательства в уголовном судопроизводстве, как относимость, допустимость и достоверность. В частности, достоверность полученного доказательства не может быть полноценно проверена экспериментальным путем, несмотря на формальное соответствие процессуальным критериям, вследствие чего ставится под сомнение законность приобщения материалов к судопроизводству [5].

Авторы, исследующие вопрос информационной безопасности как криминологической проблемы, указывают на необходимость применения мер криминологической профилактики, связанных с устранением причин и условий, способствующих реализации деструктивного воздействия на электронную информацию,

а также обуславливающих ее восприятие различными субъектами [6]. Помимо профилактики, необходима предварительная проверка информации путем использования усовершенствованных методов криминалистической техники.

**Целью настоящего исследования** является системный анализ теоретических оснований доверия к цифровым доказательствам и выявление фундаментальных ограничений современных экспертных методик в условиях применения технологий искусственного интеллекта для фальсификации цифровых объектов.

### Задачи исследования:

- 1) Систематизация существующих методов верификации цифровых файлов и выявление их уязвимостей;
- 2) формализация модели многоэтапной фальсификации цифрового объекта с применением генеративных нейросетей;
- 3) правовой анализ проблемы допустимости цифровых доказательств;
- 4) разработка рекомендаций по совершенствованию подходов к оценке подлинности электронных доказательств.

### 1. Анализ современных методов верификации цифровых файлов

Основу экспертного анализа подлинности цифрового объекта составляют структурированные критерии оценки, включающие несколько взаимодополняющих направлений проверки. Фазовая дифференциация верификации предполагает следующие категории:

- сопоставление временных меток в файловой системе и в EXIF-структуре файла;
- идентификация технических параметров устройства на основании встроенных метаданных;
- проверка целостности структуры JPEG-файла, проведение Error Level Analysis (ELA);
- анализ журналов событий устройства и сверка наличия программ-редакторов среди установленных приложений.

Все более масштабное распространение генеративных моделей ИИ приводит к появлению изображений, файлов и документов, полностью синтезированных нейросетевыми алгоритмами,

без характерных артефактов редактирования и следов вмешательства. Судебная система оказывается перед необходимостью работы с информацией, не имеющей прямого отношения к действительности, что негативно влияет на осуществление правосудия.

В силу универсального доступа к инструментам фальсификации сложность подмены мета-

данных и имитации условий создания файла более не является исключением, а становится стандартной практикой злоумышленников. Для систематизации существующих подходов к верификации и их ограничений нами разработана классификационная схема методов экспертизы цифровых файлов, представленная на рис. 1.



Рис. 1. Классификация методов верификации цифровых файлов и их ограничения

## 2. Генеративные модели ИИ как инструмент фальсификации

Развитие генеративных моделей искусственного интеллекта обозначает качественно иной уровень угроз, связанных с фальсификацией цифровых артефактов. Современные нейросети, основанные на архитектуре генеративных состязательных сетей (Generative Adversarial Networks, GAN) и глубоких трансформеров, интегрируют методы стилистического переноса (style transfer), семантической рекомпозиции изображения, имитации параметров устройства, экстраполяции условий освещения, добавления шумов и артефактов, характерных для конкретных устройств и временных периодов их функционирования [7].

Принципиальное отличие нейросетевого синтеза от традиционных методов редактирования (Adobe Photoshop и др.) заключается

в том, что генеративные алгоритмы перерабатывают изображение на семантическом уровне, создавая полностью новый, целостный файл с сохранением визуальной правдоподобности. Классические признаки вмешательства – слои, резкие границы пикселей, структурные артефакты при этом отсутствуют.

Помимо синтеза изображения, ключевым этапом фальсификации является тотальная переработка метаданных. С помощью специализированного программного обеспечения (ExifTool и аналоги) осуществляется полная очистка исходных данных и моделирование новых EXIF-полей:

- DateTimeOriginal и CreateDate с установкой необходимой даты;
- Make и Model с подменой на распространенное устройство заданного периода;

- GPS-координаты с коррекцией на требуемую геолокацию;
- параметры прошивки, линзы, выдержки и фокусного расстояния, скопированные с подлинных снимков аналогичного устройства [8].

Для наглядной демонстрации технологической асимметрии между средствами фальсификации и верификации нами составлена сводная сравнительная таблица, представленная в табл. 1.

Таблица 1

| Сравнительный анализ средств фальсификации и верификации цифровых файлов |                                                               |                                                        |
|--------------------------------------------------------------------------|---------------------------------------------------------------|--------------------------------------------------------|
| Аспект проверки                                                          | Средство фальсификации                                        | Средство верификации и его ограничение                 |
| Визуальная целостность изображения                                       | GAN, Style Transfer - генерация без артефактов монтажа        | ELA - неэффективен при целостно сгенерированном файле  |
| Метаданные файла (EXIF, XMP, IPTC)                                       | ExifTool - полная перезапись всех полей с нуля                | Анализ EXIF - все поля согласованы, противоречий нет   |
| Системные журналы и логи ОС                                              | Root-доступ + ADB Shell – очистка всех записей                | Проверка логов - журналы пусты или очищены             |
| Временные метки файловой системы                                         | touch -t - принудительная подмена дат создания/модификации    | Сверка дат - все метки синхронизированы с EXIF         |
| Идентификация устройства                                                 | Копирование параметров с реального устройства того же периода | Make/Model/Firmware - совпадают с реальным устройством |
| Следы ПО для редактирования                                              | Виртуальная машина - все манипуляции вне целевого устройства  | Поиск редакторов - на устройстве не установлены        |

### 3. Формализованная модель многоэтапной фальсификации

На основании проведенного анализа нами разработана формализованная модель много-

этапной фальсификации цифрового объекта, представленная в виде последовательности трех ключевых этапов, представленная на рис. 2.

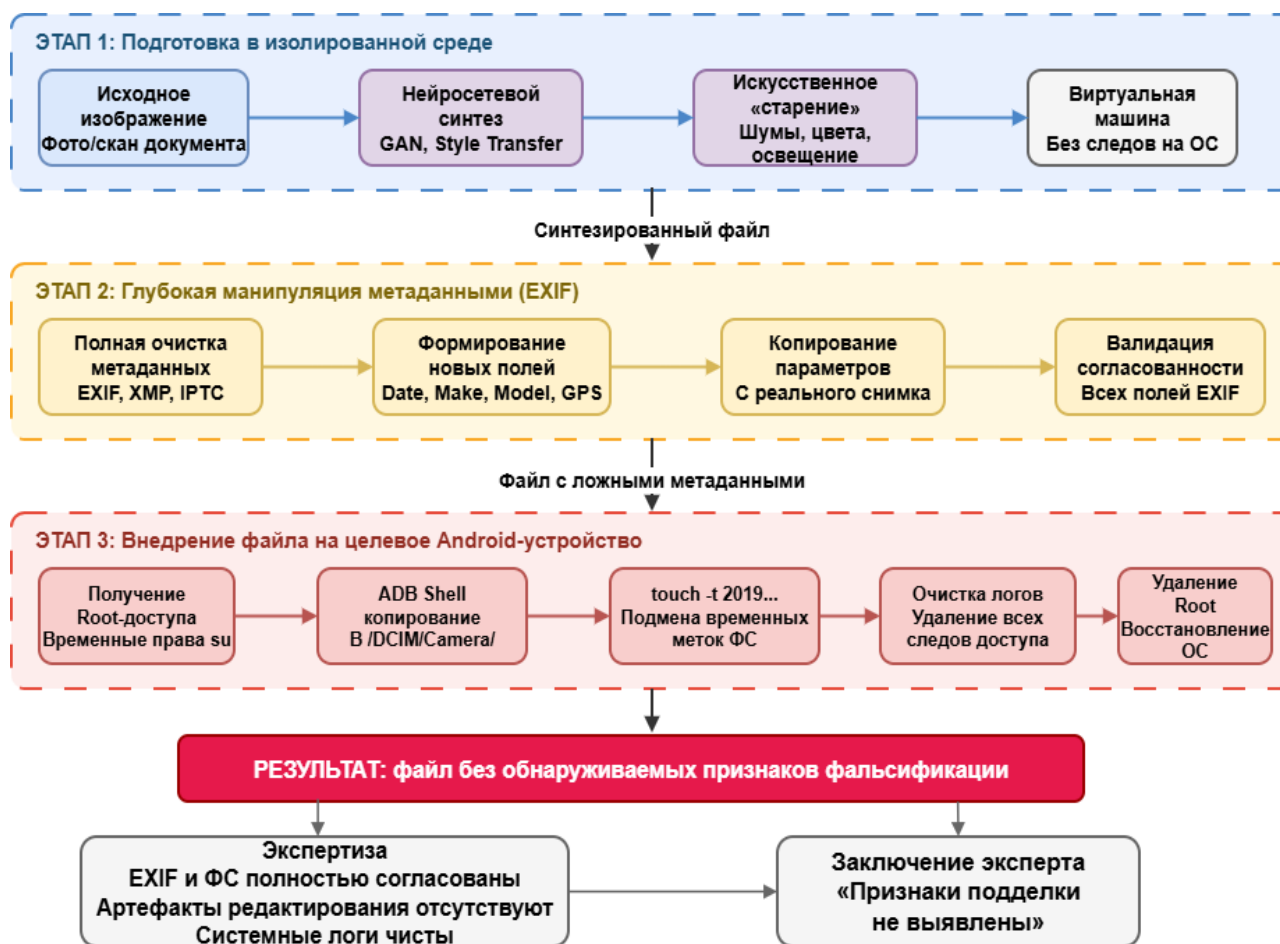


Рис. 2. Модель многоэтапной фальсификации цифрового объекта

### Этап 1. Подготовительный – работа в изолированной среде.

Злоумышленник создает исходное изображение (фотография документа на любое современное устройство или сканирование) с максимальной четкостью и детализацией. Все последующие манипуляции производятся на отдельном компьютере, предпочтительно в виртуальной машине, что минимизирует вероятность сохранения следов активности на устройствах, подлежащих потенциальному криминалистическому анализу. Далее с применением генеративных нейросетевых моделей (GAN, style transfer) изображение подвергается искусственному «старению» с имитацией характеристик камеры конкретного устройства заданного периода.

### Этап 2. Глубокая манипуляция метаданными (EXIF).

Посредством ExifTool осуществляется полное удаление всех исходных метаданных из цифрового файла, включая структуры EXIF, XMP, IPTC. После очищения формируются новые метаданные, точно соответствующие заданным параметрам:

дата и время создания, модель устройства, GPS-координаты, технические параметры камеры. Применение пакетной обработки и кастомизированных тегов обеспечивает высокий уровень контроля над конечным результатом и исключает сохранение следов предыдущих метаданных.

### Этап 3. Внедрение файла на целевое устройство.

Данный этап является критически важным, поскольку стандартное копирование оставляет характерные цифровые следы. Злоумышленник получает кратковременный физический доступ к целевому устройству и применяет программные средства для получения временных прав суперпользователя (root). Через интерфейс командной строки (ADB Shell с правами su) файл копируется непосредственно в системный каталог для фотографий (/sdcard/DCIM/Camera/). Критическим действием является принудительное изменение системных временных меток файла командой touch с указанием необходимой даты, обеспечивающее полную согласованность всех временных данных.

Результатом описанной процедуры является файл, у которого внутренние метаданные EXIF и внешние атрибуты файловой системы строго соответствуют заданному периоду, при полном отсутствии признаков использования стандартных процедур копирования.

#### 4. Неэффективность традиционных экспертных методик

Проверочные протоколы эксперта-криминалиста строятся на сравнении метаданных, анализе структуры файла, поиске следов вмешательства и сверке системных журналов. Однако перечисленные методы оказываются неэффективными в условиях применения описанной модели фальсификации.

Проверка согласованности данных EXIF и файловой системы не выявляет противоречий,

так как все атрибуты были изменены синхронно. Поиск следов графических редакторов не приносит результата, поскольку нейросетевые алгоритмы, в отличие от Adobe Photoshop, не оставляют характерных границ монтажных слоев. Методики Error Level Analysis и иные способы выявления JPEG-нарушений неэффективны перед целостно сгенерированным файлом. Отсутствие записей в журналах событий устройства (или их полная очистка при root-доступе) исключает возможность вывода о манипуляциях с файлами.

Для наглядного представления взаимосвязи между технологиями фальсификации и возможностями их обнаружения разработана концептуальная модель противостояния средств фальсификации и верификации, представленная на рис. 3.

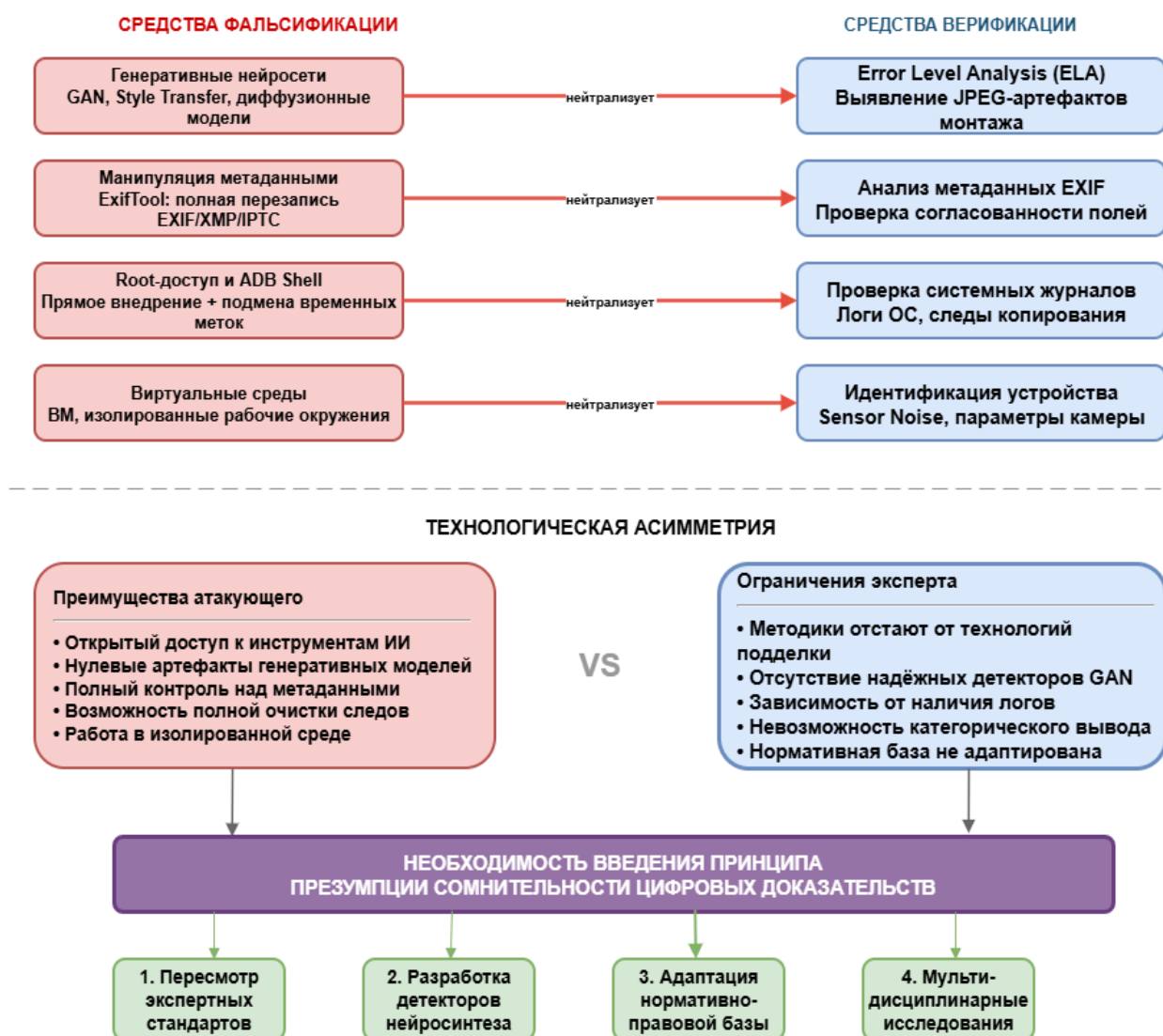


Рис. 3. Концептуальная модель противостояния средств фальсификации и верификации цифровых доказательств

Совокупность рассмотренных факторов позволяет сделать вывод о фундаментальном ограничении современных средств цифровой криминалистики: невозможности однозначного и беспристрастного установления подлинности исследуемого электронного файла. Технологическая доступность инструментов фальсификации создает условия, при которых копия, идентичная оригиналу, может быть создана и внедрена без надежных следов, фиксируемых традиционными методами анализа.

### **5. Правовые аспекты и направления совершенствования**

Законодатель предпринимает определенные меры для актуализации правовых норм. Статья 164.1 Уголовно-процессуальный кодекс Российской Федерации учитывает особенности изъятия электронных носителей информации и копирования с них информации [9]. Однако данная норма устраняет проблемы лишь частично, оставляя нерешенными масштабные вопросы допустимости и проверки цифровых доказательств.

Категорическое утверждение эксперта о подлинности файла должно подвергаться критической оценке, основанной на знаниях о существующих и развивающихся технологиях цифровой фальсификации. Эксперт может лишь подтвердить, что методики и инструментарий, находящиеся в его распоряжении, не позволили обнаружить признаков подделки.

На основании проведенного исследования предлагаются следующие направления совершенствования:

- 1) Введение в судебную практику принципа презумпции сомнительности цифровых доказательств, предполагающего обязательное комплексное исследование электронных файлов, представляемых в качестве доказательств.

- 2) Разработка мультидисциплинарной программы по изучению, прогнозированию и детектированию новых сценариев фальсификации, интегрирующей достижения теории искусственного интеллекта, кибербезопасности и криминалистики.

- 3) Внесение изменений в нормативно-правовую базу, обеспечивающих регламентацию процедур верификации цифровых доказательств с учетом возможностей генеративных технологий ИИ.

- 4) Постоянный пересмотр и усиление методик цифровой экспертизы с учетом эволюции техно-

логий подделки, включая разработку детекторов нейросетевого синтеза и методов анализа статистических аномалий в структуре файлов.

### **Заключение**

Проведенное исследование демонстрирует, что современный цифровой объект представляет собой не столько отражение реальности, сколько конструкт, подчиненный законам стремительного развития технологий синтеза и подделки. Генеративные модели искусственного интеллекта, специализированные инструменты манипуляции метаданными и методы обхода системных ограничений устройств создают совокупность условий, при которых экспертное заключение о подлинности цифрового файла не может быть сформулировано в категорической форме.

Результаты исследования позволяют сформулировать следующие выводы:

Во-первых, масштабируемость и эффективность современных методов нейросетевого синтеза изображений создали условия, при которых подделка цифровых объектов достигает беспрецедентного уровня реалистичности. Технологии на основе GAN и методов стилистического переноса позволяют создавать изображения, полностью воспроизводящие специфические характеристики оборудования.

Во-вторых, инструментарий для работы с метаданными обеспечивает возможность полного удаления исходных метаданных с последующим формированием новых, статистически и семантически непротиворечивых наборов атрибутов, что сводит к минимуму вероятность обнаружения изменений.

В-третьих, возможность прямого внедрения файлов в файловую систему целевого устройства с подменой системных временных меток, минуя стандартные протоколы, исключает обнаружение следов цифровой деятельности.

Совокупность изложенных факторов обосновывает необходимость пересмотра не только экспертных стандартов, но и фундаментальных правовых подходов к цифровым доказательствам, что требует синергетического подхода, объединяющего технические, нормативно-правовые и организационные меры.

### Список литературы

1. Герасимчук М. Ю., Герасимчук Е. В. Недееспособность и ограниченная дееспособность лиц в рамках наследственных правоотношений // Наследственное право. – 2022. – № 1. – С. 12–15. – URL: <https://www.elibrary.ru/item.asp?id=48015787>
2. Карцхия А. А., Макаренко Г. И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. – 2024. – № 1. – С. 4–19.
3. Кондрашов П. Е., Петрунин Ю. Ю., Попова С. С. Регулирование разработки и применения искусственного интеллекта: проблемы и направления развития // Вестник Московского университета. Серия 21. Управление (государство и общество). – 2025. – № 1. – С. 3–19.
4. Кустова М. Н., Умарова А. А. Этика и инновации: исследование этических аспектов влияния инновационных технологий на современное общество // Региональная и отраслевая экономика. – 2025. – № 4. – С. 48–57.
5. Подузова Е. Б. Права на аккаунт при использовании технологий искусственного интеллекта: нотариальные и цивилистические аспекты защиты // Нотариальный вестник. – 2023. – № 6. – С. 30–37.
6. Репин Д. А. Технологии искусственного интеллекта как фактор совершенствования государственного управления: вызовы и угрозы. Экономика и управление. – 2025. – № 32(2). – С. 139–148.
7. Третьякова О. Ю. Применение технологий искусственного интеллекта в нотариальной деятельности: проблемы и перспективы // Нотариальный вестник. – 2023. – № 12. – С. 58–64.
8. Deng, P. Exploration of Scientific and Technological Ethics Governance in the Age of Artificial Intelligence, Journal of Electronic Research and Application. – 2025. – Vol. 9. Is. 4. – P. 97–103.