



УДК 343.98.065

ДИПФЕЙК-ТЕХНОЛОГИИ КАК ВЫЗОВ ИНСТИТУТУ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ В КРИМИНАЛИСТИКЕ

Новоженина Мария Андреевна

Горчинская Екатерина Владимировна

студенты 4 курса очной формы обучения

Федеральное государственное автономное образовательное учреждение высшего образования
«Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)»,
Россия, г.Оренбург

Аннотация. В данной статье исследуется влияние технологий глубокого синтеза (дипфейков) на классический институт криминалистической идентификации личности. Целью работы является анализ правовых и технических вызовов, возникающих в связи с возможностью фальсификации биометрических данных и аудиовизуальных доказательств. Авторы рассматривают современные меры государственного регулирования в России и за рубежом, включая вопросы криминализации создания синтетического контента и внедрения систем автоматизированной детекции. Практическая значимость исследования заключается в обосновании необходимости адаптации методик портретной экспертизы и процессуальных норм к условиям «синтетической реальности» для обеспечения достоверности судебных доказательств.

Ключевые слова: криминалистическая идентификация, дипфейк-технологии, габитоскопия, цифровая фальсификация, портретная экспертиза.

DEEPFAKE TECHNOLOGIES AS A CHALLENGE TO THE INSTITUTE OF PERSONAL IDENTIFICATION IN FORENSIC SCIENCE

Novozhenina Maria A.

Gorchinskaya Ekaterina V.

fourth-year full-time students

Federal State Autonomous Educational Institution of Higher Education "O.E. Kutafin Moscow State
Law University (MSAL)", Orenburg, Russia

Abstract. This article examines the impact of deep synthesis technologies (deepfakes) on the traditional forensic identification system. The aim of the work is to analyze the legal and technical challenges arising from the potential for falsification of biometric data and audiovisual evidence. The authors examine current government regulations in Russia and abroad, including the criminalization of synthetic content creation and the implementation of automated detection systems. The practical significance of

the study lies in its substantiation of the need to adapt forensic analysis methods and procedural norms to the conditions of "synthetic reality" to ensure the reliability of forensic evidence.

Keywords: forensic identification, deepfake technologies, habitoscopy, digital forgery, portrait examination.

Технологии глубокого синтеза (deepfake), основанные на использовании генеративно-состязательных нейронных сетей и вариационных автокодировщиков, создают принципиально новые угрозы для одного из фундаментальных институтов криминалистики — идентификации личности по признакам внешности. В отечественной криминалистической науке идентификация рассматривается как установление тождественности объекта самому себе, что позволяет выделить искомый объект из множества ему подобных [5]. Данное определение, восходящее к трудам Р.С. Белкина, А.И. Винберга и В.А. Снеткова, лежит в основе всей системы портретной экспертизы и габитоскопии как раздела криминалистической техники.

Исторически портретная экспертиза сформировалась в 1950-х годах благодаря работам А.И. Винберга, А.А. Гусева, В.А. Снеткова и Н.В. Терзиева, которые обосновали возможность экспертного отождествления личности по фотокарточкам на основе анатомических и антропологических признаков внешности [10]. Винберг А.И. в своей докторской диссертации «Основы советской криминалистической экспертизы» (1947) заложил теоретические основы идентификации, дополнив концепцию С.М. Потапова описанием стадий процесса экспертного исследования и логических оснований выводов эксперта-криминалиста [3]. Снетков В.А. в монографии «Экспертное отождествление личности по чертам внешности» (1959) разработал методику сравнительного исследования признаков внешности по фотоснимкам, включающую предварительное, раздельное и сравнительное исследование. Эти классические разработки основывались на постулате об индивидуальности внешности человека и возможности её объективного отображения на фото- и киноматериалах.

Современные дипфейк-технологии разрушают эту парадигму, создавая синтетические медиа, внешне неотличимые от оригинальных записей. Генеративно-состязательные сети (GAN) и вариационные автокодировщики позволяют заменять лица на видео, синтезировать речь и мимику реальных людей, создавая цифровые копии, которые визуально идентичны оригиналу [4]. Это приводит к кризису достоверности аудиовизуальных доказательств, которые традиционно являлись надёжным источником для портретной идентификации. Как отмечается в исследовании И.Н. Мосечкина, дипфейк-технологии обострили угрозу использования образа другого человека при совершении противоправных деяний, а первые случаи хищений с применением поддельных биометрических данных уже зафиксированы в Китае и ОАЭ [9].



В контексте криминалистической идентификации дипфейки создают две принципиальные проблемы. Первая связана с возможностью фальсификации видеодоказательств, которые используются для установления личности лица, совершившего преступление. Исследование, посвящённое противодействию фальсификации доказательств с применением дипфейк-технологий, указывает, что данная технология стремительно развивается, становится легкодоступной и недорогой, что увеличивает риски для правосудия [8]. Программы типа Reface, DeepFaceLab, Faceswar доступны без специальных технических познаний, что демократизирует возможности создания синтетических медиа. Батоев В.Б. отмечает, "анализ практической деятельности показывает, что оперативно-розыскных, следственных и судебных органах отсутствуют какие-либо стандарты, процедуры, алгоритмы или правила для выхода из сложившейся ситуации, что непременно создает ряд проблем в вопросах установления достоверности оперативно значимой информации и цифровых доказательств" [1].

Вторая проблема заключается в подрыве доверия к традиционным методам портретной экспертизы: если эксперт не может с уверенностью отличить реальное видео от синтетического, теряется объективная основа для идентификационных выводов.

Осознавая масштаб угроз, которые технологии глубокого синтеза несут для правопорядка и института идентификации личности, российское государство в последние годы перешло к активному формированию комплексной системы противодействия. Данные меры реализуются параллельно в трех плоскостях: судебном толковании существующих норм, точечном ужесточении уголовного законодательства и разработке рамочного регулирования всей отрасли искусственного интеллекта.

Важным этапом в адаптации правовой системы стало Постановление Пленума Верховного Суда РФ от 25 июня 2024 г. № 17. В нем высшая судебная инстанция прямо указала на недопустимость использования технологий манипуляции образом (дипфейков) в ходе избирательных кампаний. Суд разъяснил, что искажение внешности или речи кандидата с помощью нейросетей для дезинформации избирателей должно квалифицироваться как нарушение порядка информационного обеспечения выборов. Это решение заложило фундамент для признания дипфейков юридически значимым инструментом совершения правонарушений.

На законодательном уровне ответом на вызовы цифровой мимикрии стал Законопроект о дополнении ст. 272.1 УК РФ. Инициатива вводит ответственность за «автоматизированную обработку» персональных данных, целью которой является создание биометрических подделок (дипфейков). С точки зрения криминалистики это означает переход от преследования за последствия (например, мошенничество) к криминализации самого процесса создания фальсифицированного цифрового образа, что значительно расширяет возможности для оперативно-розыскной деятельности и фиксации доказательств на ранних стадиях [7].

Логическим завершением этой архитектуры безопасности призван стать Проект федерального закона о государственном регулировании применения искусственного интеллекта в РФ. Документ направлен на создание прозрачной среды использования генеративных моделей. Предполагается введение обязательной маркировки контента, созданного ИИ, и установление стандартов ответственности для разработчиков. Для криминалистической идентификации принятие этого закона создаст необходимую нормативную базу, позволяющую отличать законную цифровую модификацию от преступной фальсификации отображения личности.

Анализ судебной практики показывает, что российские суды уже сталкиваются с проблемами, связанными с дипфейками.

Так, Арбитражный суд города Москвы в 2023 году рассмотрел дело о неправомерном использовании дипфейк-видео с изображением актёра Киану Ривза, созданного компанией AMG и использованного ответчиком без разрешения [11]. Суд отметил, что технология deepfake является инструментом обработки видеоматериалов, а не способом их создания, однако это решение касалось авторских прав, а не уголовно-процессуальных аспектов идентификации.

В уголовном процессе ситуация осложняется тем, что ст. 69 УПК РФ требует, чтобы доказательство было относимым, допустимым и достоверным, а синтетические медиа ставят под сомнение последнее требование.

Важным направлением является разработка автоматизированных систем детекции дипфейков на основе машинного обучения. Предлагается создание централизованной платформы мониторинга, интегрированной с базами данных правоохранительных органов, и разработка адаптивных алгоритмов, способных противостоять новым методам генерации синтетических медиа [6]. Однако здесь возникает процессуальная проблема: результаты автоматического анализа должны иметь статус средства доказывания, что требует законодательного закрепления порядка их использования и требований к защите персональных данных.

Анализ зарубежного законодательства демонстрирует переход от общих этических рекомендаций к жесткому правовому регулированию синтетического контента. Так, в Европейском союзе в рамках «Акта об искусственном интеллекте» (EU AI Act) внедряются обязательные требования к прозрачности: создатели дипфейков обязаны маркировать контент как искусственно сгенерированный, что упрощает задачу предварительной верификации доказательств.

Теоретически развитие идентификации в условиях дипфейков требует пересмотра некоторых положений криминалистической теории отражения. Если традиционно считалось, что фото- и видеоизображение объективно отражает внешность человека, то сейчас необходимо учитывать возможность цифровой модификации этого отражения. Белкин Р.С. определял

информацию как сведения об объектах и процессах материального мира, их параметрах, свойствах и состоянии, передаваемые через пространство и время [2]. Дипфейки создают искусственную информацию, имитирующую объективное отражение, что требует от эксперта не только анализа самого изображения, но и проверки его происхождения и целостности.

Таким образом, дипфейк-технологии представляют собой серьёзный вызов классическому институту идентификации личности в криминалистике. Они требуют развития методики портретной экспертизы, включая новые способы выявления признаков синтетической генерации, совершенствования процессуального регулирования допустимости аудиовизуальных доказательств и создания автоматизированных систем детекции. При этом фундаментальные положения теории криминалистической идентификации, разработанные Белкиным, Винбергом и их последователями, сохраняют своё значение, но требуют адаптации к условиям цифровой реальности, где объективное отражение может быть искусственно сконструировано. Криминалистика должна развиваться в направлении криминалистики синтетической реальности, сохраняя научные основы идентификации, но приобретая новые инструменты проверки достоверности отображений внешности человека.

Список литературы:

1. Батоев В.Б. О детекции дипфейков, используемых в преступной деятельности / В.Б. Батоев, А.В. Руденко // ЮП. — 2025. — № 1 (112). — URL: <https://cyberleninka.ru/article/n/o-detektsii-dipfeykov-ispolzuemyh-v-prestupnoy-deyatelnosti> (дата обращения: 22.03.2026).
2. Белкин, Р.С. Курс криминалистики : в 3 т. Т. 2 : Особенная часть / Р.С. Белкин. — М. : НОРМА : ИНФРА-М, 1997. — 391 с.
3. Винберг А.И. Основные принципы криминалистической экспертизы / А.И. Винберг. — М. : Госюриздат, 1949. — 132 с.
4. Verdoliva L. Media forensics and deepfakes: an overview / L. Verdoliva // IEEE Journal of Selected Topics in Signal Processing. — 2020. — Vol. 14, № 5. — P. 910–932.
5. Степаненко Д.А. Проблемы теории и практики криминалистической идентификации : дис. ... д-ра юрид. наук / Д.А. Степаненко. — М., 2009. — 495 с.
6. Голубева И.В., Мельников, В.Ю. Использование цифровых доказательств в уголовном судопроизводстве / И.В. Голубева, В.Ю. Мельников // Юридическая наука и практика. — 2024. — № 1. — С. 45–52.
7. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // Правовые вопросы в современном обществе. — 2025. — № 4. — С. 112–118.



8. Применение цифровых технологий в криминалистике / scilead.ru. — 2025. — URL: <https://scilead.ru/article/8905-primenenie-tsifrovikh-tekhnologij-v-kriminali> (дата обращения: 24.03.2026).
9. Жумаева А.Ш. Применение биометрических технологий в идентификации личности: ДНК, лицо, голос, поведенческие характеристики / А.Ш. Жумаева // Интеллект, инновации, инвестиции. — 2024. — № 2. — С. 89–95.
10. Леонов С.В. и др. Современные аспекты идентификации личности в судебной медицине и криминалистике / С.В. Леонов, Ю.П. Шакирьянова, А.И. Авдеев [и др.] // Дальневосточный медицинский журнал. — 2022. — № 3. — С. 104–110.
11. Цифровой обман: какие права нарушают дипфейки и как за это можно наказать // Право.ру. — 2024. — 31 октября. — URL: <https://pravo.ru/story/249733/> (дата обращения: 24.03.2026).