

Викулова Ольга Сергеевна

канд. юрид. наук, доцент, начальник кафедры

Калининградский филиал

ФГКОУ ВО «Санкт-Петербургский университет МВД России»

г. Калининград, Калининградская область

**АКТУАЛЬНЫЕ ВОПРОСЫ ПРОВЕДЕНИЯ
СУДЕБНЫХ ЭКСПЕРТИЗ ПО ЦИФРОВЫМ АВАТАРАМ,
ИСПОЛЬЗУЕМЫМ В ПРЕСТУПНЫХ ЦЕЛЯХ**

***Аннотация:** статья посвящена проблемам судебного экспертного обеспечения расследования преступлений, совершённых с использованием цифровых аватаров. Рассматриваются виды экспертиз: компьютерно-техническая, судебная портретная, лингвистическая и психолого-лингвистическая, трасологическая цифровая. Предложена классификация аватаров по степени подобия реальному лицу, способу управления и функциональному назначению в криминальной среде. Обоснована необходимость создания реестра типовых экспертных методик и подготовки экспертов-криминалистов, владеющих технологиями ИИ и компьютерной графикой.*

***Ключевые слова:** судебная экспертиза, цифровой аватар, экспертиза по цифровым аватарам, компьютерно-техническая экспертиза.*

Проблемы судебно-экспертного обеспечения расследования преступлений, совершенных с использованием цифровых аватаров (включая дипфейки, виртуальных персонажей в игровых средах, анимированные 3D-модели, чат-боты и реалистичные CGI-изображения), выступают насущной юридической реальностью.

Цифровой аватар – виртуальное представление лица (либо вымышленного персонажа), способное к автономному или управляемому действию в цифровой среде.

Относительная доступность технологий искусственного интеллекта, генерации глубоких подделок (deepfake), а также развитие метавселенных и плат-

форм с пользовательскими аватарами создали благоприятные условия для использования указанных объектов в противоправных целях.

По данным экспертных сообществ, число преступлений, связанных с незаконным использованием deepfake и аватаров, в Российской Федерации за период 2023–2025 годов выросло более чем в четыре раза [1]. При этом существующие методики судебных экспертиз зачастую не успевают адаптироваться к новым вызовам, что порождает сложности в доказывании и установлении объективной истины.

Развитие судебной экспертизы в этой сфере требует создания реестра типовых экспертных методик по исследованию deepfake и аватаров; подготовки экспертов-криминалистов, владеющих технологиями искусственного интеллекта (далее – ИИ) и компьютерной графикой.

На сегодняшний день в практике российских судебно-экспертных учреждений можно назвать следующие виды экспертиз при расследовании деяний, совершенных с использованием цифровых аватаров:

- компьютерно-техническая экспертиза – является базовой. Эксперт исследует программный код или исполняемые файлы, которые управляли аватаром. При наличии исходных данных возможно определить алгоритм или версию генеративной модели (StyleGan, VAE, диффузионные модели), а также идентификацию «цифрового почерка» автора подделки, например, характерных для конкретного deepfake-инструмента. Компьютерно-техническая экспертиза также позволяет восстановить действия пользователя в метавселенной: перемещение, взаимодействия с другими аватарами, произносимые реплики;

- судебная портретная экспертиза. При исследовании deepfake она необходима в двух аспектах: для идентификации реального лица, чей образ скопирован; для установления признаков монтажа или синтеза. Новейшие методики используют анализ виртуальных аномалий на уровне частотных характеристик кадров, неравномерности моргания аватара, отсутствия реалистичного отражения в глазах. В отличие от классической портретной экспертизы здесь востребованы инструменты компьютерного зрения и ИИ-ассистенты. Как отмечают

М.А. Новоженина и Е.В. Горчинская [2, с. 1–5], deepfake-технологии подрывают базовый постулат криминалистической идентификации о стабильности идентифицируемых признаков.

– лингвистическая и психолого-лингвистическая экспертиза: если аватар ведёт диалог, например чат-бот, виртуальный собеседник, то текстовая или голосовая продукция подлежит анализу на предмет речевых стереотипов, синтаксических конструкций, характерных для конкретного лица. Исследование может установить: генерировался ли текст нейросетью – «парафразером» или непосредственно человеком-преступником. Применяются методы дистинктивного анализа и лингвостатистики.

– трасологическая цифровая экспертиза: относительно новый вид, разрабатываемый в экспертных подразделениях МВД РФ. Изучаются трассы – следы идентификационного характера, оставляемые программным обеспечением: уникальные паттерны сжатия видео, характерные ошибки округления в числовых параметрах 3D-модели аватара, специфические серийные номера библиотек рендеринга.

Комплексное применение перечисленных экспертиз позволяет ответить на ключевые вопросы следствия и суда: является ли видеозапись с лицом подозреваемого deepfake; кому принадлежит аккаунт, с которого управлялся аватар; какие действия фактически совершены реальным человеком, а какие – автоматикой.

Традиционная криминалистика оперирует материальными и идеальными следами. В случае использования цифровых аватаров основными становятся компьютерно-технические следы, имеющие двоякую природу: с одной стороны, это объективные данные, фиксируемые на серверах и устройствах; с другой – они подвержены лёгкой модификации.

Наиболее значимыми для экспертизы являются: блокчейн-записи транзакций при покупке и кастомизации аватара или внутриигровых активов – помогают установить кошелёк, а через него – лицо; журналы сессий и IP-адреса входа в аккаунт, управляющий аватаром; артефакты генерации deepfake – несогласо-

ванность движения глаз, пульсация кожи, несоответствие гистограмм яркости; поведенческие цифровые следы – индивидуальные особенности нажатия на клавиши, стилистика текста и пр.

С криминалистической точки зрения аватары, используемые в преступных целях, могут быть классифицированы по ряду оснований:

- по степени подобия реальному лицу: аватары-deepfake (фото-, видео- и аудиосимуляция конкретного человека без его согласия); синтетические аватары (персонажи, не имеющие прямого прототипа, но обладающие правдоподобными человеческими чертами); абстрактные или игровые аватары (анимированные объекты, не претендующие на реалистичность, но используемые для коммуникации, например в компьютерных играх);

- по способу управления: прямое (ручное управление пользователем в режиме реального времени); автоматизированное (действия прописаны заданным алгоритмом или сценарием); гибридное (частичное управление человеком, частичное – искусственным интеллектом);

- по функциональному назначению в криминальной среде: аватары – средства сокрытия личности (подмена лица в видеозвонках, фейковых аккаунтах); аватары – орудия воздействия (чат-боты для фишинга, виртуальные собеседники для склонения к преступлению); аватары – элементы инсценировки (создание ложных цифровых алиби).

Классификация важна для выбора конкретной судебно-экспертной методики. Так, при исследовании аватаров, созданных с использованием технологии deepfake, приоритетной должна выступать видео- и компьютерно-техническая экспертиза, тогда как для выявления преступных действий через игрового аватара в метавселенной требуется комплексная цифровая трасология и анализ метаданных [3].

Проведение судебной экспертизы по цифровым аватарам требует фиксации не только конечного продукта – готового deepfake-видео, но и промежуточных артефактов, таких как лог-файлы нейросети, чекпоинты моделей, метаданные исходных изображений. Отсутствие методики изъятия таких данных, аналогич-

ной правилам работы с вещественными доказательствами, создаёт риск утраты или фальсификации следов.

Цифровые аватары превратились в новый инструмент преступной деятельности, требующий радикального пересмотра подхода к судебной экспертизе.

Список литературы

1. Судебная и независимая экспертиза дипфейков: правовые основания, методология и актуальные вызовы // Центр инженерных экспертиз. – 2026. – URL: <https://komprexp.ru> (дата обращения: 24.04.2026).

2. Новожеина М.А. Дипфейк-технологии как вызов институту идентификации личности в криминалистике / М.А. Новожеина, Е.В. Горчинская // Наука через призму времени. – 2026. – №04(109). – С. 1–5.

3. Шайдуллин Р.Р. О совершенствовании методического обеспечения применения технологий искусственного интеллекта в судебно-экспертной деятельности в условиях цифровизации / Р.Р. Шайдуллин // Вестник Института права Башкирского государственного университета. – 2026.