УДК 343

ТЕХНОЛОГИЯ ДИПФЕЙК КАК ЦИФРОВАЯ УГРОЗА В СОВРЕМЕННОМ МИРЕ

А. В. ЩЕРБИНИНА
(Представлено: К. Ю. Мельнова)

В статье рассматривается понятие технологии дипфейк и их развитие в современном мире. Автор статьи делает акцент на исследовании вопросов использования дипфейков в противоправных целях и предлагает пути распознавания сгенерированных материалов с помощью судебных экспертиз. Анализируются понятия судебных экспертиз и способы их применения в сфере использования дипфейков.

С развитием цифровых технологий появляются новые риски, связанные с использованием искусственного интеллекта, нейросетей, с помощью которых создаются фото, видео- и аудиоматериалы. Получила свое распространение технология «дипфейк», которая подразумевает под собой копирование мимики человека, его голоса, внешности и иное, а также замена фото и иных материалов (аудио- /видео), которые вводят в заблуждение людей, нарушают конституционные права граждан, причиняют вред государственным и общественным интересам. Как отмечается в научной литературе, Т. И. Дудко «с учетом динамичного развития информационных технологий дипфейки могут быть представлены в различных формах: фото-, видео- и аудиоматериалы» [1, с. 62].

Понятие «дипфейк» более точно определяет Г. К. Игнатенков, отмечая, что «дипфейки – это преднамеренно искаженные аудио, видео или иные файлы с использованием технологий глубокого изучения, которые изображают что-то вымышленное или ложное, что позволяет злоумышленникам использовать новый и сложны инструмент социальной инженерии» [2, с. 74].

Так, в конце 1990-х годов стали развиваться технологии автоматизированной анимации лица на основе аудио. Одним из ярких примеров становится программа Video Rewrite, которая позволила с помощью специального оборудования скопировать движение губ с лица человека, заставляя изображение, сгенерированное нейросетью, произносить слова, записанные отдельно на аудиодорожку [1, с. 58–59].

На данном этапе нейросети не прекратили свое развитие, а, наоборот, прогрессировали, создавая совершенно новые изображения, копирующие мимику, черты лица, а также голос человека. И уже в 2017 году был придуман термин «дипфейк», который происходит от слов подделка и глубокое обучение, который полностью характеризовал созданные искусственным интеллектом видеозаписи, изображение, копирование голоса и т.д. Г. К. Игнатенков выделял 3 вида дипфейков на основе анализа их использования: текстовый (технология автоматического написания текста машиной, обученной на большом массиве текстовых документов), аудио (клонирование голоса человека) и визуальные (создание поддельных фотографий и видео) [2, с. 75–76].

В современном мире дипфейк становится оружием злоумышленников по совершению противоправных деяний. Как отмечал И. Н. Поздняк, «применяя данную технологию, злоумышленники используют нейросеть, накладывая фрагменты контента на исходное изображение или видео. Происходит подмена изображения лица, мимики человека, его жестов и голоса в видеоряде или звуковой дорожке» [5, с. 72]. Злоумышленники используют поддельные голоса и видео, представляясь руководителями предприятий, близких родственников или представителей государственных органов, чтобы заполучить денежные средства или данные, которые не подлежат разглашению. Вышеуказанные противоправные действия могут происходить в различных формах, например, по видеозвонку или аудиовызову, по переписке в социальных сетях и другими способами.

Как отмечает И. Н. Поздняк, «ярким примером применения мошенниками технологии дипфейк в феврале 2024 года прокатился по всем информационным платформам». В данном примере говорилось о том, что газета South China Morning Post сообщила о финансовых потерях на сумму 25,6 млн долларов США из-за мошенничества с использованием технологии дипфейк. Сначала им приходили фишинговые сообщения от финансового директора компании Великобритании о проведении секретной транзакции, затем поступило приглашение на групповую видеоконференцию. Во время данного мероприятия злоумышленники не вступали в беседу со жертвой, а давали указания [5, с. 73].

Вышеуказанный пример помогает нам определить, что дипфейк в настоящем времени используется не только в добрых побуждениях и намерениях, но и в противоправных целях, становясь в руках злоумышленников оружием против людей, которых они вводят в заблуждение, нарушают их конституционные права.

В связи с чем, важное значение имеют вопросы использования специальных знаний посредством назначения и проведения экспертиз в целях идентификации человека по голосу и речи, исследования данных о свойствах и признаках голоса, устной и письменной речи, выявления признаков внесения изменений в фото, видео и аудиоматериалы и др. по различным категориям дел, включая мошенничества, вербальное оскорбление, клевета, призывы, угрозы применения насилия, причинения вреда, преступления экстремисткой направленности и др.

Согласно ст. 1 Закона Республики Беларусь от 18 декабря 2018 г. № 281-З «О судебно-экспертной деятельности» (далее – Закон «О судебно-экспертной деятельности»), судебная экспертиза – экспертиза, назначенная и проведенная в порядке, установленном процессуальным законодательством [4]. В основе определения необходимости назначения или проведения того или иного вида экспертизы лежит характер и природа исследуемых объектов, круг вопросов, которые требуют ответа, задачи, которые необходимо решить и др.

Так, с учетом объекта, задач и вопросов, которые необходимо решить в ходе проведения судебных экспертиз материалов, созданных с использованием технологии дипфейк, таковыми могут выступать портретные, компьютерно-технические, видеотехнические, фоноскопические, лингвистические, фототехнические и иные виды экспертиз. Их главными отличиями является то, что фоноскопическая экспертиза направлена на исследование звуковой и речевой информации на аудио- или видеозаписях; лингвистическая экспертиза направлена на исследование текста и воспроизведение его смыслового содержания; фототехническая экспертиза – исследование фотоснимков, видеозаписей и оборудования, с помощью которого они были получены; видеотехническая экспертиза – исследование видеозаписей, полученных с помощью средств видеофиксации [3]. Каждая из этих экспертиз будет выявлять определенные дефекты в видео или устной речи, например, видеотехническая, фототехническая и фоноскопическая экспертизы совместно смогут выявить явные противоречия, например, в чертах лица, в мимике человека, а также по иным признакам (цвет кожи, волос и т. п.), что позволит более углубленно проанализировать видеоматериалы с помощью методов одной и другой экспертиз для выявления дефектов.

Дипфейки, как говорилось ранее, создаются при копировании голоса, создавая аудио- или видеозапись самого начала с совершенно новыми словами и полностью скопированными чертами лица и мимики, которые в последующем будут использоваться в противоправных целях. Тем самым мы можем наблюдать, что могут возникать некоторые проблемы при проведении экспертных исследований для выявления следов нейросети, а именно: полностью сгенерированный голос или черты лица или мимики нейросетью не оставляет характерных следов для обнаружения искусственного интеллекта, появляются проблемы с использованием методов экспертиз, которые опираются на определенные материалы для анализа, т. е. одни опираются на аудио- или видеоматериалы, другие – на тексты (письменные или устные).

С учетом изложенного, стоит согласиться с подходом, согласно которому в целях решения вопроса о создании материалов с использованием технологии дипфейк необходимо применять комплексный подход с учетом необходимости использования знаний из различных отраслей.

Таким образом, дипфейк в современном мире зачастую используется в противоправных целях для введения в заблуждение людей, нарушая их конституционные права и свободы, а также причиняют вред государственным и общественным интересам. Данный термин представляет собой совершенно новый объект в сфере применения судебных экспертиз, что позволяет разработать новые методы для работы с нейросетью.

ЛИТЕРАТУРА

1. Дудко, Т. И. Дипфейк как объект криминалистического исследования / Т. И. Дудко // Вопросы криминологии, криминалистики и судебной экспертизы. – 2026. – № 1(59). – С. 57 – 63.
2. Игнатенков, Г. К. Технология дипфейк как угроза информационной безопасности / Г. К. Игнатенков // Наука. Исследования. Практика : Сборник избранных статей по материалам Междунар. научной конференции, Санкт-Петербург, 25 июня 2022 года. – Санкт-Петербург: Частное науч.-образоват. учрежд. доп. проф. образования Гуманитарный нац. исследоват. институт «НАЦРАЗВИТИЕ», 2022. – С. 74 – 77.
3. Научно-практический центр Государственного комитета судебных экспертиз Республики Беларусь : [сайт] – Мн., 2026. – URL: http://sudexpertiza.by/expertises/63 (дата обращения: 07.10.2026).
4. О судебно-экспертной деятельности : Закон Респ. Беларусь от 18 дек. 2019 г. № 281-З : в ред. от 16 марта 2026 г. № 134-З // ЭТАЛОН: информ.-поисковая система (дата обращения: 07.10.2026).
5. Поздняк, И. Н. Цифровые угрозы в современном мире: технология deepfake / И. Н. Поздняк // Экспертная практика. – 2024. – №2 (19). – С. 72 – 77.