Секция «Уголовное право и криминология»

Дипфейк как способ совершения мошенничества

Научный руководитель – Кисляков Антон Валерьевич

Гаранина Екатерина Дмитриевна

Студент (специалист)

Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Юридический институт, Владимир, Россия

E-mail: ekaterina.garanina05@mail.ru

С развитием возможностей цифровых технологий и искусственного интеллекта (далее – ИИ) все больше людей становятся жертвами интернет-мошенничества, ставят под угрозу свои деньги и персональные данные [6]. Используя современные технологии, злоумышленники успешно манипулируют эмоциями жертвы, вводя её в состояние шока. Такой механизм совершения преступлений стал сегодня особенно распространен благодаря развитию технологий ИИ, которые в последние годы достигли значительных успехов.

Одна из новых ИИ технологий, известная как deepfake, может создавать новые гиперреалистичные поддельные материалы. Термин Deepfake объединяет концепции "deeplearning" (глубокого обучения) и "fake" (подделки). Данный метод синтеза мультимедийного контента основан на применении алгоритмов машинного обучения, способных создавать новые данные на основе ранее предоставленных параметров [3]. В частности он позволяет генерировать видеоматериалы, в которых лица выполняют действия или произносят фразы, отсутствующие в действительности.

В рамках уголовного права дипфейк может использоваться как инструмент осуществления широкого спектра преступлений. Наибольшее применение данная технология находит в области мошеннических действий. Злоумышленники применяют различные методы для достижения своих целей, среди которых можно выделить:

1. Использование технологий синтеза речи на основе нейронных сетей. Например, deepfakeaudio позволяет создавать аудиофальсификации, имитирующие голос конкретного лица, в том числе для осуществления мошеннических действий посредством звонков и сообщений, содержащих инструкции о переводе денежных средств на счета злоумышленников.

2. Манипуляция визуальными данными (фото и видео), осуществляемая с целью компрометации личности, и шантажа. В случае отказа от выполнения различных требований, фальсифицированные материалы распространяются среди ближайшего окружения потерпевшего.

3. Применение нейросетевых языковых моделей для генерации текста, имитирующего человеческую речь для создания фишинговых сообщений и рассылок.

Использование дипфейка как способа совершения мошенничества может квалифицироваться: в сфере компьютерной информации (хищение путем вмешательства в функционирование информационно телекоммуникационных сетей; хищение чужого имущества путем обмана или злоупотребления доверием [5]. При этом п. 21 ПП ВС РФ от 30.11.2017 № 48 устанавливает, что в случаях, когда хищение совершается путем использования учетных данных собственника независимо от способа их получения, действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение. А изменение данных о состоянии банковского счета или о движении денежных средств, происшедшее в результате использования виновным данных потерпевшего, не признается таким воздействием [2]. Но если хищение чужого имущества осуществляется

путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть "Интернет", то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ [1]. Вместе с тем, согласно п. 2 указанного Постановления обман как способ совершения хищения может состоять в умышленных действиях, направленных на введение владельца имущества в заблуждение, а сообщаемые при мошенничестве ложные сведения могут относиться к любым обстоятельствам, юридическим фактам, стоимости имущества, личности виновного, его полномочиям, намерениям.

Сложившаяся практика привлечения к уголовной ответственности за хищение чужого имущества посредством использования дипфейков, только начинает складывается. Можно предположить, что использование преступниками фейк технологий будут являться для правоохранительных структур примерным шаблоном того, как именно нужно квалифицировать противоправные деяния в таких случаях.

При анализе криминальных схем с применением дипфейков необходимо подчеркнуть, что их финальной целью часто является незаконное завладение имуществом. В этом контексте представляется целесообразным рассматривать подобные деяния с точки зрения положений статьи 159 УК РФ («Мошенничество»), поскольку использование дипфейков представляет собой способ достижения противоправного результата.

Стоит отметить, что и в российском обществе остро стоит проблема мошенничества, а схемы, используемые злоумышленниками, принимают новые формы и становятся все более ухищренными. Правоохранительным органам необходимо разрабатывать методики выявления дипфейка для предотвращения преступного использования этой технологии. В качестве примера таких контрмер предлагается использование технологии блокчейн в целях создания защищенных от несанкционированного доступа цифровых материалов. Блокчейн может быть использован для создания безопасного цифрового реестра, который может отслеживать происхождение информации, что затруднит производство неотслеживаемых дипфейков [4].

Вместе с тем важным шагом в этом направлении видится подготовка специалистов, обладающих дополнительными компетенциями в области цифровых технологий. По нашему мнению, представители всех правоохранительных органов должны обладать указанными компетенциями, в связи с чем целесообразно обеспечить возможность получить дополнительное профессиональное образование.

Источники и литература

1) Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024) (с изм. и доп., вступ. в силу с 01.03.2025) // "Собрание законодательства РФ". 17.06.1996. № 25. ст. 2954.

2) Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) "О судебной практике по делам о мошенничестве, присвоении и растрате" // "Российская газета". № 280. 11.12.2017.

3) Бодров Н.Ф., Лебедева А.К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. №11. С. 26-41.

4) Михалев Д.Д. Правовое регулирование дипфейков // Цифровые технологии и право: Сборник научных трудов II Международной научно-практической конференции: в 6 т. Казань. 2023. С. 267-272.

5) Сидельникова Э. Преступления в компьютерной сфере (мошенничество) и их правовая оценка // Вопросы российской юстиции. 2024. №33. С. 615-620.

6) Шепель Н.В. Использование дипфейков как современный способ совершения преступлений // Проблемы правовой и технической защиты информации. 2024. № 12. С. 103-106.