УДК 343.4

СИНТЕТИЧЕСКИЕ МЕДИА КАК СРЕДСТВА "КРАЖИ ЛИЧНОСТИ"

Я.А. КУРТО
(Представлено: канд. ист. наук, доц. А.Л. РАДЮК)

Данная статья посвящена анализу синтетических медиа и их разновидностей. Автор статьи рассматривает синтетические медиа с точки зрения "кражи личности" – кражи личных данных, используемых в противоправных целях – и последствий, возникающих после.

Видео- и аудиоконтент постепенно становятся одними из самых влиятельных способов коммуникации в сети Интернет. Они достаточно легко передают сведения, эмоции, и являются неотъемлемой частью средств массовой информации. Однако по мере того, как СМИ, заполняющиеся искусственно созданными продуктами виртуальной реальности, становятся повсеместными, мы должны быть готовы к миру, в котором видеть и слышать правду станет редкостью. В таком случае, так называемые синтетические медиа приобретут массовый характер. Под синтетическими медиа понимают контент, созданный компьютером с помощью технологий искусственного интеллекта (ИИ).

Синтетические медиа включают в себя модифицированные видео, голоса и изображения. Сам по себе синтез изображений, видео или аудио может не иметь очевидных социально-опасных целей, однако манипулирование средствами массовой информации с использованием изображений, видео или голосов реальных людей создает целый комплекс моральных, юридических и управленческих проблем [1].

Материалы, созданные с помощью технологий искусственного интеллекта, можно отличить от оригинальных по нескольким параметрам. Во-первых, синтезированные видео, как правило, отличаются характеризуются признаками роботизированности. Моргание, движения тела и губ лишены естественности и синхронизации, такие видео примечательны необычным темпом речи и резким изменением освещения и тона кожи. Во-вторых, модифицированное аудио характеризуется ненатуральным ритмом голоса и низким качеством звука. Внедрение искусственного интеллекта в такие программы только улучшит качество таких медиа.

Первый тип синтетических медиа является, пожалуй, самым известным в виртуальном мире средством введения в заблуждение. Дипфейк – это форма синтеза изображения человека, когда существующая фотография или изображение накладывается на видео, чтобы изменить идентичность того, кто изображен в видео [2]. Нина Шик, непало-немецкий автор, консультант и спикер, определяет дипфейк как тип "синтетических медиа", то есть медиа (включая изображения, аудио и видео), которые либо частично, либо полностью генерирует ИИ [3]. С английского языка deepfake дословно переводится как "глубокая подделка", что соответствует сущности самого явления. В большинстве случаев, они создаются для развлекательных, и, в целом, безобидных целей. Однако использование персональных данных человека (лицо, голос) с целями введения в заблуждение принимает криминальный характер. В таком ключе такое правонарушение подходит под параметры "кражи личности" – преступления с использованием чьей-либо персональной информации с целью выдать себя за иного человека и получить деньги или товары на его имя [4].

В большинстве случаев такие видео остаются в Сети в течение длительного времени и могут быть перенесены на другие интернет-источники после удаления. Эти порочащие материалы могут быть использованы в целях мести, запугивания, политического саботажа, пропаганды, шантажа и даже в качестве фальшивых новостей, которые состоят из дезинформации и пропаганды, искажающей реальные новости и факты, заменяя действительность ложными изображениями и информацией [5].

С этим же мотивом могут использоваться и биометрические данные человека. Синтезированная речь может использоваться в мошеннических схемах, включая махинации с банковскими счетами [1]. Рассмотрим использование голоса для совершения кражи личности на практическом примере. Первым широко известным в Европе случаем использования биометрических данных человека в мошеннических целях стало использование голоса Генерального директора энергетической фирмы, базирующейся в Великобритании (название компании не приводится). Думая, что он разговаривает по телефону со своим боссом, исполнительным директором немецкой материнской компании, без лишних вопросов перевел 243,000 долларов "венгерскому поставщику". Генеральный директор принял синтезированный голос за подлинный, и деньги были переведены на счет в течение часа, согласно данным страховой фирмы Euler Hermes Group SA. К сожалению, неизвестно, существовали ли прецеденты к такому случаю, однако предполагается, что хакеры будут использовать технологии ИИ повсеместно, если таковые сделают киберпреступления более успешными и смогут приносить реальный доход [6].

Синтезированные медиа могут стать основным источником дохода для преступных организаций и виртуальных мошенников. Одна из главных опасностей, связанных с синтетическими медиа, заключается в том, что они могут демонстрировать события или намеки на поведение, которых никогда не было, с целью разрушить репутацию личности. Такие поддельные материалы также потенциально могут быть использованы для шантажа и вымогательства, либо ради финансовой выгоды, либо для манипулирования лицами [7].

Мошеннические схемы также могут использовать персональные данные как умерших людей, так и людей несуществующих. "Кража личности" с использованием синтезированных личностей – это более сложный вид мошенничества, который, как правило, труднее обнаружить. Преступники объединяют персональные данные нескольких человек с целью использования этих сведений для генерирования нового несуществующего человека. Далее, мошенники совершают основное преступление. Вместо того чтобы использовать украденную личность одного человека, преступники добывают информацию и сведения по нескольким людям, чтобы синтезировать нового «человека», которого на самом деле не существует. Затем эти данные используются для крупных финансовых транзакций или получения новых кредитов. Обобщая, следует отметить, что ИИ может похитить личность абсолютно любого человека, но не без помощи человека, осуществляющего задуманный преступный план.

Вопросом времени является введение в действие законов, запрещающих определенный неправомерный контент deepfake. Разработка проектов таких законов уже идет в ряде стран мира [1]. 20 декабря 2019 г., первый в стране закон, криминализирующий создание и распространение видео-дипфейков, не отмеченных соответствующим образом, был подписан Президентом США. Законодательное закрепление дипфейков стало частью Закона о национальной обороне на 2020 финансовый год. Помимо вышеперечисленных нововведений, закон включил в себя разработку плана дальнейших исследований и создания инструментов обнаружения дипфейков [8]. В Китае с 1 января 2020 года действуют новые правила, регулирующие видео-и аудиоконтент в Интернете. Он включает запрет на публикацию и распространение “фальшивых новостей”, созданных с помощью ИИ. Отмечается, что любое использование искусственного интеллекта должно быть четко обозначено, и несоблюдение данных правил может рассматриваться как уголовное преступление, которое может “поставить под угрозу национальную безопасность и ущемить законные права и интересы других лиц” [9].

Алгоритмы, позволяющие манипулировать личными данными субъекта, постоянно совершенствуются. Необходимо подчеркнуть, что искусственный интеллект может использоваться не только для создания синтетических медиа, которые позволяют совершать киберпреступления с их использованием, но и для их идентификации и предупреждения мошенничества. На сегодняшний день специалисты многих компаний занимаются созданием программ, которые смогут определять следы цифрового манипулирования. Предположим, что число «краж личности» с использованием синтетических медиа будет увеличиваться, если не принимать должных мер. По нашему мнению, в них входят криминализация самого явления кражи персональных данных, разработка программ по противодействию кибермошенникам и информирование населения об угрозах в Сети.

ЛИТЕРАТУРА

1. Иванов, В.Г., Игнатовский Я.Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности / В.Г. Иванов, Я.Р. Игнатовский // Вестник российского университета дружы народов. Серия Государственное и муниципальное управление. – 2020. – Том 7. – С. 379–386.
2. Kirchengast, T. Deepfakes and image manipulation: criminalisation and control / T.Kirchengast // Information & Communications Technology Law – 2020. –Vol. 29, Issue 3. – P. 308–323.
3. Schick, Nina deepfakes: The Coming Infocalypse / Nina Schick. – Grand Central Publishing, 2020. – P. 3.
4. Cambridge Dictionary [Электронный ресурс]. – Режим доступа: https://dictionary.cambridge.org/ru/ – Дата доступа: 11.04.2021.
5. Maras, Marie-Helen, Alexandrou, A. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos / Marie-Helen Maras, A. Alexandrou // The International Journal of Evidence & Proof [Electronic resource]. – 28.10.2018. – Mode of access: https://journals.sagepub.com/doi/10.1177/1365712718807226 – Date of access: 19.09.2021.
6. Stupp, C. Fraudsters Used AI to mimic CEO’s Voice in unusual Cybercrime Case / C. Stupp // The Wall Street Journal [Electronic resource]. – 30.08.2019. – Mode of access: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 – Date of access: 22.09.2021.
7. Kalpokas, I. Problematising reality: the promises and perils of synthetic media / I. Kalpokas // SN Soc Sci [Electronic resource]. – 2021. – 1,1 – Mode of access: https://doi.org/10.1007/s43545-020-00010-8 – Date of access: 22.09.2021.
8. Chipman, J., Ferraro, M., Preston, S. First Federal Legislation on Deepfakes Signed Into Law / J. Chipman, M. Ferraro, S. Preston // JDSUPRA [Electronic resource]. – 24.12.2019. – Mode of access: https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/ – Date of access: 22.09.2021.
9. Yang, Y., Goh, B., Gibbs, E. China seeks to root out fake news and deepfakes with new online content rules / Y. Yang, B. Goh, E. Gibbs // Reuters [Electronic resource]. – 29.11.2019. – Mode of access: https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU – Date of access: 23.09.2021.