[4] Губулов А.К. Проблемы защиты персональных данных в системе электронного правосудия // Закон и право. № 8. 2019. С. 148-149.

[5] Денисов И.С. Развитие электронного правосудия в России // Вестник Санкт-Петербургского университета МВД России. № 1 (77). 2018. С. 101-104.

[6] Кондюрина Ю.А. Реализация принципов арбитражного процесса в системе электронного правосудия // Вестник Омского университета. № 1 (34). 2013. С. 157-161.

IMPLEMENTATION OF THE PRINCIPLES OF ARBITRATION PROCESS IN THE E-JUSTICE MODEL

© 2019 Churakova Ekaterina Nikolaevna,
PhD, Associate Professor
Samara State University of Economics
E-mail: katek_07@mail.ru
© 2019 Mikhaylova Marina Sergeevna
Student
Samara State University of Economics
E-mail: marina-marinka-mixajlova@mail.ru

The article discusses the relationship between the principles of arbitration procedural law and technical means of organizing proceedings, combined in the concept of «electronic justice».

Keywords: electronic justice, arbitration process, legal proceedings.

УДК 343.7

DEEPFAKE: ПРАВОВЫЕ ПРОБЛЕМЫ И ИХ РЕШЕНИЕ

© 2019 Яворский Максим Александрович
Кандидат юридических наук, доцент
Самарский государственный экономический университет
E-mail: yavorm@mail.ru
© 2019 Мавринская Татьяна Владимировна
Студент
Самарский государственный экономический университет
E-mail: mavrinskaya1998@mail.ru

В статье рассматривается вопрос об использовании современных технологий, таких как искусственный интеллект и нейросети, в целях подделки изображений, голоса людей для совершения незаконных действий. Показана актуальность угрозы таких правонарушений, приведены примеры мошенничеств. Авторами дается ряд предложений для снижения угрозы использования сфальсифицированных биометрических данных людей.

Ключевые слова: дипфейк; искусственный интеллект; нейросеть; биометрические данные; технологии; мошенничество.

Современные информационные технологии развиваются стремительными темпами, и порой то, что несколько лет назад было невозможно представить, сегодня мы можем увидеть во многих сферах деятельности человека. Одним из самых быстро развивающихся направлений развития технологий является искусственный интеллект. Данные технологии не только могут анализировать значительные объемы информации, но и делать какие-либо «самостоятельные» выводы по результатам анализа. Искусственный интеллект используется в разных сферах: медицина, промышленность, телекоммуникации, наука, финансы, киноиндустрия и иные сферы. Так, нейросети (одна из форм реализации искусственного интеллекта) используются в искусстве. Например, нейросеть может самостоятельно создать картину, проанализировав перед этим большое количество произведений живописи. Или, изучив значительный объем фотографий, может создать новое лицо, либо заменить одно лицо другим. Так, в 2014 году студент Стэнфордского университета Ян Гудфеллоу создал генеративно-состязательную нейросеть (GAN), один алгоритм которой обучается на фотографиях человека и создает на основе их анализа изображения, а второй - «противодействует ему», пока первый алгоритм не начинает понимать, где копия, а где оригинал. Такая реализация нейросети и позволяет создавать дипфейки (deepfake - deep learning - «глубинное обучение» и fake - «подделка»)[1]. Современные нейросети создают очень качественные фотографии, видеоизображения и голоса людей, в которых практически невозможно определить фальсификацию.

Описанные технологии не всегда могут использоваться в благих целях. Так, например, современные банковские системы позволяют совершать финансовые операции, для подтверждения которых могут использоваться биометрические персональные данные человека: изображение и голос. Так, например, технология MasterCard Identity Check (комплекс решений для подтверждения личности покупателей и упрощения онлайн-шопинга) позволяет совершать онлайн покупки с помощью фотографии, чем могут воспользоваться злоумышленники, создав дипфейк жертвы[2]. Подобные технологии открывают для мошенников новые возможности, а известные «традиционные» механизмы совершения хищений уходят на второй план. И это только один из возможных вариантов неправомерного использования таких технологий, вариантов мошенничества может быть очень много. Так, по данным Wall Street Journal, в марте 2019 года у управляющего директора энергетической компании из Британии было похищено 220 000 евро. Потерпевший совершил банковскую операцию по переводу денежных средств компании из Венгрии. Этот перевод был осуществлен на основании того, что его руководитель, глава материнской компании в Германии, несколько раз подтвердил ему данное действие по видеосвязи. Однако на самом деле это оказался не его руководитель, а мошенник, который использовал нейросеть для фальсификации в режиме реального времени видеоизображения и голоса руководителя фирмы. Нейросеть, которую использовал злоумышленник,

смогла полностью подделать голос руководителя: пунктуацию, тон и даже немецкий акцент[3].

В современном мире возникла ситуация, при которой технологии развиваются намного стремительнее нормативно-правовой базы, которая регулирует эти технологии. И если не контролировать эту сферу, общество придет к глобальной проблеме, когда любая информация может быть сфальсифицирована. Не будет доверия даже к самым правдоподобным видеозаписям или изображениям, ведь все это может оказаться результатом работы нейросети, управляемой неизвестными личностями. Качественные дипфейки станут удобными инструментами не только для мошенничества, вымогательства, но и для манипуляции общественным сознанием.

При этом некоторые иностранные государственные структуры обеспокоены нарастающей угрозой использования дипфейков. Израильское национальное управление защиты от киберугроз (INCD) в июле 2019 года выпустило предупреждение о возможных мошеннических действиях с использованием фальсифицированного голоса в отношении руководителей компании и высокопоставленных чиновников[4]. Управление перспективных исследовательских проектов Министерства обороны США (DARPA) в августе 2019 года проводило набор специалистов в программу Semantic Forensics, которая разрабатывается для быстрого обнаружения дипфейков[5]. Некоторые законодатели уже отреагировали на растущую угрозу неправомерного использования дипфейков: законодательное собрание штата Виргиния (США) ввело уголовную ответственность за распространение дипфейк-материалов без согласия объекта[6]. В Великобритании аналогичный закон действует с 2015 года, и подразумевает санкции к правонарушителям в виде лишение свободы до 2 лет.

Не только государственные органы заинтересованы в борьбе с дипфейками. Так, компания Facebook совместно с Microsoft и коалицией «Партнёрства по искусственному интеллекту во благо людей и общества» (PAI), а также научными сотрудниками из ряда университетов анонсировала конкурс на разработку технологии распознавания дипфейков. Конкурс стартовал осенью 2019 года, призовой фонд конкурса - 10 миллионов долларов[7].

Вышеописанные примеры наглядно показывают, что угроза фальсификации изображения и голоса воспринимается очень серьезно, и, хотя мошеннические действия с использованием дипфейков, по сравнению с иными видами мошенничества, пока не носят массовый характер, но в скором будущем, благодаря стремительному развитию нейросетей и беспрепятственному доступу к ним, будут представлять серьезную проблему.

Мы предлагаем реализовать несколько важных шагов для снижения распространения дипфейков:

1. Внесение изменений в законодательство Российской Федерации в части обязательной электронной и визуальной маркировки фото и видеоматериалов, содержащих дипфейки. Данная маркировка должна явно указывать на то, что материал является подделкой, а также содержать информацию об изготовителе. Помимо этого, если в дипфейке используется биометрические данные граждан РФ, то создатель

дипфейка обязан получить согласие на обработку персональных данных в соответствии с ст. 9 152-ФЗ «О персональных данных»[8]. Внесение данных изменений в законодательство не позволит полностью исключить противоправных действий с помощью дипфейков, однако позволит привлекать к ответственности лиц, использующих дипфейки для этих целей.

2. Необходимо исключить использование только лишь биометрических данных для подтверждения совершения банковских операций, а проводить такие операции в комплексе с иными методами идентификации личности. Так, например, вступившая в силу 14 сентября 2019 года платежная директива Евросоюза PSD2, обязывает банки использовать многофакторную идентификацию[9]. Такая идентификация подразумевает обязательное использование двух из трех компонентов:

a) *знания* - какой-то информации, известной только пользователю, например, пароля или контрольного вопроса.

b) *владения* - какого-то устройства, которое имеется только у пользователя, например, телефона или токена, содержащего электронную подпись.

c) *уникальности* - чего-то неотъемлемого, присущего пользователю и однозначно идентифицирующего личность, например, биометрических данных.

Эти три элемента должны быть независимыми друг от друга, чтобы компрометация одного элемента не влияла на надёжность других.

3. Увеличение в средствах массой информации количества социальной рекламы, направленной на повышение осведомленности граждан в вопросах кибербезопасности и формирования необходимых навыков в данной области.

---

[1] Goodfellow, Ian J.; Pouget-Abadie, Jean; Mirza, Mehdi; Xu, Bing; Warde-Farley, David; Ozair, Sherjil; Courville, Aaron & Bengio, Yoshua (2014), "Generative Adversarial Networks", arXiv:1406.2661 [stat.ML]. URL: https://arxiv.org/abs/1406.2661 (дата обращения: 14.10.2019).

[2] Иванов В.В., Черкасов Д.Ю., Любова Е.С. Биометрия: система идентификации личности при оплате // Вопросы науки и образования. 2017. С. 64.

[3] Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case // The Wall Street Journal. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (дата обращения: 14.10.2019).

[4] Israel warns of AI cyber-attacks by voice impersonating of senior executives // XINHUANET. URL: http://www.xinhuanet.com/english/2019-07/10/c_138212768.htm (дата обращения: 14.10.2019).

[5] Министерство обороны США попытается решить проблему deepfake // Habr.com. URL: https://habr.com/ru/news/t/463395 (дата обращения: 14.10.2019).

[6] Virginia's legislative information system // URL: http://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2678S1 (дата обращения: 14.10.2019).

[7] Facebook и Microsoft запускают конкурс по обнаружению deepfake // Habr.com. URL: https://habr.com/ru/news/t/466507 (дата обращения: 14.10.2019).

[8] Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СПС «Консультант плюс».

[9] Официальный сайт Европейского Союза // URL: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en (дата обращения: 14.10.2019).

DEEPFAKE: LEGAL PROBLEMS AND THEIR SOLUTION

© 2019 Maksim Alexandrovich Yavorsky
PhD, Associate Professor
Samara State University of Economics
E-mail: yavorm@mail.ru
© 2019 Tatiana Vladimirovna Mavrinskaya
Student
Samara State University of Economics
E-mail: mavrinskaya1998@mail.ru

The article discusses the use of modern technologies, such as artificial intelligence and neural networks, in order to fake images, people's voices for illegal actions. The urgency of the threat of such offenses is shown, examples of fraud are given. The authors give a number of proposals to reduce the threat of using falsified biometric data of people.

***Keywords*:** dipfake, artificial intelligence, neural network, biometric data, technology, fraud.

УДК 343.7

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ ЭКОНОМИЧЕСКОМУ ЭКСТРЕМИЗМУ

© 2019 Яворский Максим Александрович
Кандидат юридических наук, доцент
Самарский государственный экономический университет
E-mail: yavorm@mail.ru
© 2019 Милова Ирина Евгеньевна
Кандидат юридических наук, доцент
Самарский государственный экономический университет
E-mail: irina.milova@ro.ru

В статье акцентируется внимание на необходимости принятия комплексных мер по противодействию рейдерству как форме экономического экстремизма. Авторы полагают, что эффективно противодействовать проявлениям экономического экстремизма и его крайней форме - рейдерским захватам собственности возможно только при условии системного подхода, включающего в себя мероприятия организационно-правового, культурно-экономического, образовательного и пропагандистско-идеологического характера.

Ключевые слова: экономический экстремизм; деструктивная экономическая деятельность; рейдерство.

Следует констатировать, что в последние годы проблемы противодействия различным проявлениям экстремизма приобрели большую популярность в научных