Забродина Валерия Витальевна

Преподаватель кафедры уголовного права имени М. И. Ковалева
Уральского государственного юридического университета
имени В. Ф. Яковлева
leran.00@mail.ru

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ DEEPFAKE В ПРЕСТУПНЫХ ЦЕЛЯХ: ОТЕЧЕСТВЕННЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

Аннотация. В современных условиях цифровизации и информатизации общества все более быстрыми темпами развиваются технологии искусственного интеллекта, одной из которых является технология дипфейк. Безусловно, новые возможности имеют положительный эффект, но, как и всё новое и полезное могут использоваться и в преступных целях, что заставляет законодателя серьезно подходить к вопросу уголовно-правовой оценки новых явлений. В статье автором приводятся различные примеры совершения преступлений при помощи дипфейков, выявляются преимущества и недостатки нового законопроекта, внесенного в Государственную Думу РФ, предусматривающего ужесточение уголовной ответственности за совершение преступлений с использованием дипфейков, анализируется зарубежный опыт в сфере уголовно-правового регулирования технологии дипфейк. В результате проведенного исследования автор приходит к выводу о необходимости внесения изменений в российское законодательство.

Ключевые слова: цифровизация, искусственный интеллект, дипфейк, преступление, уголовный закон.

Zabrodina Valeria Vitalevna

Lecturer of the Department of Criminal Law
V. F. Yakovlev Ural State Law University

USING DEEPFAKE TECHNOLOGY FOR CRIMINAL PURPOSES: DOMESTIC AND FOREIGN EXPERIENCE

Abstract. In modern conditions of digitalization and informatization of society, artificial intelligence technologies are developing at an increasingly rapid pace, one of which is deepfake technology. Of course, new opportunities have a positive effect, but, like everything new and useful, they can also be used for criminal purposes, which forces the legislator to take a serious approach to the issue of criminal legal assessment of new phenomena. In the article, the author provides various examples of crimes committed with the help of deepfakes, identifies the advantages and disadvantages of a new draft law submitted to the State Duma of the Russian Federation providing for stricter criminal liability for crimes committed using deepfakes, analyzes foreign experience in the field of criminal law regulation of deepfake technology. As a result of the conducted research, the author comes to the conclusion that it is necessary to amend Russian legislation.

Key words: digitalization, artificial intelligence, deepfake, crime, criminal law.

Ни для кого ни секрет, что искусственный интеллект стал неотъемлемой частью современного общества, оказывая значительное влияние на различные сферы жизни. Одной из технологий, использующих искусственный интеллект является технология deepfake (deep learning — глубокое обучение и fake — подделка). Технологии дипфейк могут быть использованы для различных целей: развлечение, образование, искусство. Между тем, несмотря на потенциальные положительные применения, дипфейки несут значительные риски для общества, включая возможность их использования в преступных целях. Злоумышленники могут использовать технологии искусственного интеллекта для совершения мошенничества, шантажа, нанесения вреда репутации, распространения порнографических материалов и т.п.

Известным инцидентом мошенничества с использованием технологии дипфейков является случай в Гонконге, где сотрудник финансового отдела крупной международной компании получил сообщение, якобы от финансового директора, с просьбой провести несколько денежных переводов. Несмотря на возникшие сомнения злоумышленники пригласили сотрудника на групповую видеоконференцию, где, как он думал, присутствовали его руководители и коллеги, между

тем, все участники видеозвонка были дипфейками, созданными на основе общедоступных видео и аудио. В результате чего компания потеряла около 25,6 миллионов долларов[1].

Похожая ситуация произошла и с руководителем британской компании, который был уверен, что в телефонном разговоре общается со своим немецким коллегой, поскольку преступнику удалось в точности повторить интонацию и акцент другого человека с помощью технологии дипфейк. В результате противоправных действий компания лишилась крупной суммы денег[2].

В Российской Федерации такие ситуации не являются исключениями, преступники все чаще и чаще используют нейросети для получения материальной выгоды, об этом, в том числе предупреждает Банк России[3]. Так, жертвами дипфейков стали преподаватель московского вуза и бывший командующий сухопутными войсками, преступники действовали по одной и той же схеме. Преподавательница МГОУ получила звонок якобы из мэрии Москвы, где ей сообщили, что состоится видеоконференция с Сергеем Собяниным и замминистром МВД России, конференция действительно состоялась, но только со злоумышленниками с лицами мэра и министра, которые и убедили жертву перевести денежные средства в размере 2 миллионов рублей якобы на безопасный счет[4]. Аналогичная ситуация произошла и с военным в отставке[5].

Простыми словами технология дипфейк позволяет создавать поддельные фото, видео и аудио, заменяя голоса и лица людей. Впервые данное явление появилось в 2017 году и существует уже достаточно продолжительное время, но несмотря на это в России на данный момент отсутствует специальное законодательство, регулирующее создание и распространение дипфейков, в том числе при совершении преступления. 16 сентября 2024 года в Государственную Думу РФ был внесен законопроект, который вводит в ряд статей УК РФ дополнительный квалифицирующий признак, а именно совершение преступления с использованием технологии «дипфейк». Речь идет о таких преступлениях, как клевета, кража, мошенничество, вымогательство и причинение имущественного ущерба путем обмана или злоупотребления доверием[6]. При этом, Правительство и Верховный суд РФ выразили сомнения относительно необходимости и целесообразности данного законопроекта, в частности, отметив, что для начала необходимо урегулировать вопросы использования технологии подмены личности в отраслевом законодательстве, а уже потом вносить изменения в Уголовный кодекс Российской Федерации[7].

Безусловно, законопроект об усилении уголовной ответственности за совершение преступлений с использованием дипфейков поднимает важные вопросы о правовом регулировании новых технологий и их влиянии на общество, но не всегда внесение изменений в уголовное законодательство решает возникающие проблемы. С этой целью необходимо обратиться к опыту зарубежного законодательства.

Одной из стран, которая активно регулирует использование технологий дипфейков через ряд законов и правил, является Китай. С 1 января 2020 года в стране действует специальный Закон о дипфейках, который вводит строгие требования к производству и распространению контента, созданного с использованием таких технологий. Все видео и аудиозаписи должны быть промаркированы, а от лиц, изображенных на таких записях, обязательно должно быть получено согласие.

---

[1] «Everyone looked real»: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting. URL: https://www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage (дата обращения: 08.10.2024).

[2] Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (дата обращения: 08.10.2024).

[3] Мошенники обманывают людей с помощью дипфейков. URL: https://cbr.ru/information_security/pmp/15082024/ (дата обращения: 08.10.2024).

[4] Вам звонит Сергей Собянин: преподавателя Университета просвещения обманули на 2 млн рублей. URL: https://regions.ru/mytischi/proisshestviya/vam-zvonit-sergey-sobyanin-prepodavatelya-universiteta-prosvescheniya-obmanuli-na-2-mln-rubley (дата обращения: 08.10.2024).

[5] Новая жертва дипфейк мэра Москвы: на этот раз обманули экс-замминистра обороны РФ. URL: https://arbatmedia.kz/exo-moskvy/novaya-zertva-dipfeik-mera-moskvy-na-etot-raz-obmanuli-eks-zamministra-oborony-rf-7004 (дата обращения: 08.10.2024).

[6] Законопроект № 718538–8 «О внесении изменений в Уголовный кодекс Российской Федерации». URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 08.10.2024).

[7] Официальный отзыв Правительства РФ, официальный отзыв Верховного суда РФ. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 08.10.2024).

Так, использование технологий дипфейков стало уголовным преступлением с 1 января 2020 года[1]. Но несмотря на наличие законодательства, в практической реализации возникает немало сложностей. Новые правила возлагают ответственность за контент именно на разработчиков технологий, а не на пользователей, что может негативно сказаться на деятельности самих компаний в сфере искусственного интеллекта, за рамками остаются действия самих злоумышленников, которые будут нести ответственность за использование дипфейков в преступных целях на общих основаниях. При этом, безусловно, принятые меры имеют преимущества. Так, В.А. Виноградов полагает, что обязательная маркировка позволит отличать поддельные аудио- и видеозаписи, что существенно снизит риски введения в заблуждение и манипулирования граждан[2]. Подход законодателя в Китае импонирует и другим авторам, которые считают его логичным, прагматичным и целесообразным[3].

Еще одной азиатской страной, которая планирует установление уголовной ответственности за использование технологии дипфейк, выступает Южная Корея. 26 сентября 2024 года южнокорейским парламентом был принят законопроект, который вводит уголовную ответственность за создание, хранение или просмотр фейковых изображений и видео сексуального характера. Нарушителям грозит до трех лет тюремного заключения или штраф до 33 млн вон[4]. Принятие законопроекта было обусловлено ростом групповых чатов, в которых распространялись дипфейки сексуального характера. В отличие от Китая южнокорейский подход обусловлен именно борьбой с сексуальными преступлениями, оставляя за рамками использование искусственного интеллекта в иных преступных целях, что видится не совсем обоснованным.

Соединенные Штаты Америки, как один из лидеров цифровой сферы, считают технологию дипфейк одной из актуальных тем в контексте обеспечения национальной безопасности, что связано с ростом количества использования такой технологии в преступных целях. Ввиду этого на уровне штатов разработаны свои законы для борьбы с дипфейками, так в штате Массачусетс, создание и распространение дипфейков с целью обмана рассматривается как преступление подделки личности[5]. В штате Вирджиния предусмотрена уголовная ответственность за использование дипфейков в целях принуждения, преследования или запугивания граждан[6]. Несмотря на быстрое реагирование законодателя, многие аспекты остаются нерегулируемыми, что означает необходимость дальнейшего развития законодательства для защиты от использования технологий дипфейков в преступных целях.

В странах Европы также активно обсуждается вопросы введения уголовной ответственности за использование дипфейков в преступных целях. В Австрии несмотря на отсутствие специальных законов о дипфейках, их использование подпадает под существующие правила защиты персональных данных, уголовного и административного законодательства. При этом властями поднимается проблема регулирования технологии дипфейк посредством внесения конкретных изменений в действующее законодательство, в частности, еще в 2022 году правительство страны опубликовало План действий по борьбе с дипфейками, и до настоящего времени властями ведется активная работа по противодействию дипфейкам[7]. Франция придерживается аналогичной позиции, пытаясь регулировать использование технологии дипфейк в неправомерных целях в рамках действующего

[1] China makes it a criminal offense to publish deepfakes or fake news without disclosure. URL: https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality (дата обращения: 08.10.2024).

[2] Виноградов В. А., Кузнецова Д. В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. Т. 17, № 2. С. 230.

[3] Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (Deepfake): опыт Китая / Р. И. Дремлюга, В. В. Моисейцев, Д. В. Парин, Л. И. Романова // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 4.

[4] South Korea to criminalize watching or possessing sexually explicit deepfakes. URL: https://edition.cnn.com/2024/09/26/asia/south-korea-deepfake-bill-passed-intl-hnk/index.html (дата обращения: 08.10.2024).

[5] Дремлюга Р. И., Коробеев А. И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (Deepfake): уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. 2021. № 3.

[6] Свиридова Е. А. Правила использования технологий дипфейк в праве США и КНР: адаптация зарубежного опыта правового регулирования // Современное право. 2024. № 3. С. 119-123.

[7] Parlamentskorrespondenz Nr. 1005 vom 23.09.2022. URL: https://www.parlament.gv.at/aktuelles/pk/jahr_2022/pk1005 (дата обращения: 12.10.2024).

законодательства и ожидая принятия новых рамочных документов на уровне Европейского Союза, посвященных регулированию искусственного интеллекта[1].

Анализ зарубежного законодательства позволяет прийти к выводу об активной законодательной инициативе различных стран в сфере использования технологии дипфейков. В некоторых странах уже приняты законы, которые предусматривают уголовную ответственность за использование дипфейков в преступных целях. В российском законодательстве до настоящего времени данный вопрос не урегулирован, но уже делаются первые шаги на пути к установлению уголовной ответственности, что видится вполне обоснованным. Применение технологии дипфейков в преступных целях значительно повышает общественную опасность, поскольку оказывает очень серьезное воздействие на потерпевшего и практически лишает его возможности распознать обман. Опасности, связанные с дипфейками, достаточно многообразны и требуют комплексного подхода к их правовому регулированию, что, в том числе, показывает и зарубежный опыт. Российскому законодателю следует более тщательно подойти к вопросу установления уголовной ответственности за использование дипфейков при совершении преступления.

СПИСОК ЛИТЕРАТУРЫ

1. Виноградов, В. А. Зарубежный опыт правового регулирования технологии «дипфейк» / В. А. Виноградов, Д. В. Кузнецова // Право. Журнал Высшей школы экономики. 2024. — Т. 17, № 2. — С. 215-240.
2. Дремлюга, Р. И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (Deepfake): уголовно-правовые и криминологические аспекты / Р. И. Дремлюга, А. И. Коробеев // Всероссийский криминологический журнал. — 2021. — № 3.
3. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (Deepfake): опыт Китая / Р. И. Дремлюга, В. В. Моисейцев, Д. В. Парин, Л. И. Романова // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2022. — № 4.
4. Дюфло, А. Искусственный интеллект во Французском праве / А. Дюфло // Вестник Университета имени О. Е. Кутафина. — 2021. — № 1 (77).
5. Свиридова, Е. А. Правила использования технологий дипфейк в праве США и КНР: адаптация зарубежного опыта правового регулирования / Е. А. Свиридова // Современное право. — 2024. — № 3. — С. 119-123.

[1] Дюфло А. «Искусственный интеллект во Французском праве» // Вестник Университета имени О. Е. Кутафина. 2021. № 1 (77).