УДК 004.032.26

ДИПФЕЙК И ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ

Андрей Алексеевич Хохлов
студент
garlic142@gmail.com
Алла Борисовна Лыкова
студент
lukovaalla3@gmail.com
Лариса Ивановна Никонорова
кандидат сельскохозяйственных наук, доцент
lenaniknrva@rambler.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматривается развитие технологии Deep Fake, угрозы безопасности, способы защиты от дипфейков.

Ключевые слова: дипфейк, искусственный интеллект (ИИ), безопасность, мошенничество.

Прогресс не стоит на месте и с развитием искусственного интеллекта стали развиваться системы с максимальной фотореалистичностью, одной из которых стала технология замены лиц, голоса и мимики лица – «дипфейк».

Приложения по созданию поддельных видео и аудио материалов в большей степени бесплатны и легкодоступны. Так за последние 6 лет в сети интернет появилась масса поддельных видео. Одни из них несут исключительно развлекательный контент, другие являются плохой составляющей этой системы – обманные операции.

Риски злонамеренного использования дипфейков являются не менее реальными, чем польза от их применения. Во многих странах технология «дипфейк» уже рассматривается как потенциально опасная, способная нанести ущерб как национальной, так и информационно-психологической безопасности [4].

Технология изучает манеры речи и жестов человека, обучая нейронную сеть, которая и используется для создания «фейковых» видео.

Используя множество реальных примеров речи и движущихся изображений, обучается так называемая нейронная сеть. В зависимости от поставленных целей использование дипфейков в негативном плане условно разделяют на три уровня[1,2].

Первый уровень – это мелкое хулиганство, большей частью представляющей собой лишь демонстрацию своих способностей без намеренного получения материальной выгоды.

Второй уровень предусматривает извлечение злоумышленниками материальной выгоды. Это могут быть - валюты разных стран, акции, либо снижение репутации других компаний или людей высокого ранга. Так в 2019 году директор британской энергетической компании перевел преступникам более 240 тысяч долларов не распознав речь главы материнской компании в Германии.

Третий и самый высокий уровень использования дипфейков – это использование их для нанесения вреда политической власти, партии или

членам, работающим в политической сфере. Единственным, что руководит людьми в данной ситуации - это снижение репутационной статистики политических деятелей, (в предвыборной компании), что является очень актуальной проблемой всех современных государств. Злоумышленники могут нанести большой урон экономической и политической сфере и даже межгосударственным отношениям [3,4].

Помимо перечисленных проблем есть также проблемы, связанные с: распространения дезинформации; манипулирования общественным мнением; разжигания социальных волнений; некорректные высказывания в сторону национальных меньшинств; шантажированные состоятельных личностей.

В настоящий момент уже были случаи дипфейков с использованием образов правителей стран. Основа практически всех приложений подобного плана заключается в том, что снимки накладываются друга на друга и их соединении образуют фото или видеопоток. Чем больше программа анализирует поток информации, тем легче ей строить образы. Человеку крайне сложно обработать такой объемданных, но не для машины, из-за чего возникают серьезные проблемы, которые влекут угрозы политической и общественной жизни.

Решение, которые направлены на выявление поддельного видео контента уже предпринимаются. В России была создана программа разработанная специалистами ДГТУ, которая позволяет выявить неточности в видео с помощью алгоритма Generative Adversarial Network (GAN). Программа написана на языке программирования Python 3.11. Работает этот алгоритм, обнаруживая на видеокадрах признаки, сгенерированной нейросетью, синтеза лица или голоса. В основном главными признаками подделки являются: расхождение мимики лица и произношения слов, неточность в расположении пикселей или кривое натяжение и движение губ при разговоре.

Министерство внутренних дел использует программу «Зеркало» или «Верблюд», способную распознавать видео с подменёнными лицами.

Помимо перечисленного также существуют технологии блокчейн. Блокчейн – это способ защиты информации при передаче и хранении в виде цепочки блоков, что видно из названия. Они связаны друг с другом и в каждом из них содержаться данные о предыдущем [5].

Стержневая основа дипфейка является его несравнимая точность передачи образов.

На сегодняшний день проблема дипфейков остается до конца неизученной и сложной, так как технология непрерывно и стремительно развивается, а способы противостояния ей растут несколько медленнее.

За содержание дипфейком персональных данных любого человека, без согласия его, предусмотрена статья 137 УК РФ «Нарушение неприкосновенности частной жизни», поэтому отдельная статья не нужна [6].

Список литературы:

1. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия «Государственное и муниципальное управление». 2020. № 4. 379-386с.

2. Киселев А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник МГОУ. 2021. № 3.

3. 6 лучших Deepfake приложений и инструментов. / Новая Наука. - URL: https:// new-science.ru/6-luchshih-deepfake-prilozheniji-instrumentov-v-2020-godu/

4. Аферы с дипфейками: какие угрозы скрываются за искусственными лицами? / SecurityLab.ru. - URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351217

5. В России готовят закон против дипфейков: «Могут поставить под удар даже жизнь». / ФедералПресс. - URL: https://fedpress.ru/%20article/2951342

6. Могут ли быть обнаружены дипфейки в видео: как опознать подделку лица. / WebZnam. - URL: https://webznam.ru/blog/dipfejki_v_video/2020-10-20-1601

UDC 004.032.26

THE BENEFITS OF DIPFAKE AND WHAT THREAT DOES IT PRESENT TO POLITICAL AND PUBLIC SECURITY

Andrey Al. Khokhlov
student
garlic142@gmail.com
Alla Borisovna Lykova
student
lukovaalla3@gmail.com
Larisa Iv. Nikonorova
Candidate of Agricultural Sciences, Associate Professor of the Department
lenaniknrva@rambler.ru.
Michurinsk State Agrarian University
Michurinsk, Russian

Annotation. The article examines the rapid development of Deep Face technology, how it works, what threats to political security this technology carries and ways to protect against deepfakes.

Keywords: deepfake, artificial intelligence (AI), political security, malicious use, deception, technology, fraud.

Статья поступила в редакцию 03.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 27.06.2024.

The article was submitted 03.05.2024; approved after reviewing 13.06.2024; accepted for publication 27.06.2024.