УЯЗВИМОСТИ ФОТО- И ВИДЕОМАТЕРИАЛОВ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ DEEPFAKE

И.И. Фролов

Технологии машинного обучения получили уже достаточно широкое распространение не только в научно-исследовательской среде, но также стали применяться во многих сферах реальной экономики: многие бизнесы используют нейронные сети для анализа исторических данных (например, данные о продажах) [1] и прогнозирования развития будущей деятельности, основываясь на результатах анализа. В последние годы в определенной степени снизился порог входа в область анализа данных и работы с нейронными сетями за счет создания и продвижения отдельных готовых высокоуровневых библиотек, реализующих сложные алгоритмы машинного обучения.

Получив широкое распространение среди пользователей, появились и новые области применения нейросетевых алгоритмов: стали популярными приложения по обработке и синтезу изображений, видеопотоков. Одним из популярных направлений стали приложения, позволяющие моделировать и заменять изображения лица человека не только на статичном фотоизображении, но и для видеопотока. Появился даже отдельный термин «DeepFake» [2] для описания такого рода технологий. Поначалу подобные эксперименты использовались в развлекательных целях большинством пользователей сети, а также открывали более широкие перспективы развития киноиндустрии. Однако вскоре стало понятно, что подобное программное обеспечение может использоваться и в целях дискредитации популярных личностей шоу-бизнеса и политики, подготовки видео- или аудиосообщений для оказания влияния как на отдельные процессы в бизнесе (например, телефонный звонок, имитирующий указание руководителя перевести денежные средства на указанный банковский счет), так и на финансовые рынки (например, смонтированное видео-сообщение крупных игроков о слиянии компаний). Несмотря на краткосрочность таких действий (реальные личности быстро опровергают подделки), эффект может быть использован в корыстных целях.

Кроме перечисленных уязвимостей в видео- и аудиосообщениях более простым вариантом использования технологии DeepFake может быть имитация/моделирование изображения лица для несанкционированного доступа к, например, мобильным устройствам, предоставляющим доступ по биометрическим параметрам владельца.

Таким образом, актуальными является не только разработка алгоритмов машинного обучения и обработки фото- и видеоизображений для построения качественных моделей, используемых для реализации технологии «DeepFake», но исследования в области распознавания результатов применения технологии «DeepFake».

Литература

1. Прогнозирование спроса с помощью автоматизированного машинного обучения без кода в студии машинного обучения Azure [Электронный ресурс] – Режим доступа: https://docs.microsoft.com/ru-ru/azure/machine-learning/tutorial-automated-ml-forecast. – Дата доступа: 02.05.2022.

2. What are deepfakes – and how can you spot them? [Электронный ресурс] – Режим доступа: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them. – Дата доступа: 02.05.2022.