Голятина Светлана Михайловна
канд. юрид. наук, старший преподаватель
ФГКОУ ВО «Волгоградская академия МВД России»
г. Волгоград, Волгоградская область

ОРУЖИЕ МОШЕННИКОВ – ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫЕ СЕТИ (GAN)

Аннотация*: в статье приводится статистика киберпреступлений, совершенных в России в 2020–2023 гг. Рассматриваются понятие генеративно-состязательных сетей, способы их использования мошенниками в преступных целях, даются некоторые рекомендации по распознаванию дипфейков.*

Ключевые слова*: кибермошенничество, искусственный интеллект, генеративно-состязательная сеть, нейросеть, дипфейк.*

В России печальной тенденцией последних нескольких лет является увеличение количества преступлений, совершаемых с использованием информационно-телекоммуникационной сети Интернет. Так, в 2020 г. было зарегистрировано 510 400 таких уголовно наказуемых деяний, в 2021 г. – 517 700, в 2022 г. – 522 100, в 2023 г. – 677 000. При этом значительную часть (примерно две трети) названных преступлений составляют кражи и мошенничества [1]. В 2023 г. злоумышленники провели 1,17 млн успешных операций, ущерб от их действий оценивается в 15,8 млрд руб. Согласно данным Центробанка России, причина сложившейся ситуации состоит в адресных и подготовленных атаках [2].

Стоит признать тот факт, что с каждым годом мошенники становятся изобретательнее и совершают преступления все более изощренными способами. Заместитель председателя правления Сбербанка С. Кузнецов отмечает: «Есть ощущение, что мы все время находимся в состоянии догоняющих. Мы научились управлять рисками по традиционным направлениям, но появились новые» [3]. В числе таких новых вызовов необходимо назвать мошенничество с использованием генеративно-состязательных сетей (GAN) – нейронных сетей, которые умеют генерировать изображения, музыку, речь и тексты. Злоумыш-

ленники применяют данную технологию для имитации чужой личности (чаще всего голоса и внешности).

Один из первых случаев совершения мошенничества с использованием генеративно-состязательных сетей произошел в январе 2020 г. в Дубае (ОАЭ), когда управляющему банком позвонил якобы директор. Последний предупредил сотрудника финансово-кредитной организации о том, что в почте его ожидает запрос на перевод $ 35 000 000, который необходимо осуществить как можно скорее, что и было сделано. До этого инцидента управляющий банком неоднократно разговаривал с директором и, естественно, сразу узнал его по голосу, однако, как стало известно позднее, никаких распоряжений руководитель не давал, а его голос был имитирован нейросетью [4]. Аналогичным образом были похищены денежные средства в сумме € 220 000 у генерального директора британской энергетической компании [5].

Если раньше такие случаи были единичными, то сегодня они становятся повсеместными. Дипфейковая (от англ. deep learning – глубинное обучение и fake – подделка) имитация голоса применяется мошенниками в атаках не только на крупные корпорации и финансовые организации, но и на простых граждан. В январе 2024 г. Центробанк России предостерег клиентов: «Чтобы вынудить человека сообщить необходимые сведения или совершить денежный перевод, злоумышленники могут выходить на контакт с человеком от имени знакомых, родных или коллег, имитируя их голоса с помощью специальных программ» [6]. Однако, несмотря на предупреждения, россияне по-прежнему демонстрируют беспечность и попадаются на удочку преступников. Так, в феврале 2024 г. жительнице Иркутска поступило несколько голосовых сообщений якобы от подруги, которая просила одолжить ей 40 000 руб. Сибирячка осуществила перевод денежных средств, но, как оказалось, вовсе не своей знакомой, а мошенникам, сымитировавшим ее голос [7].

Чтобы подделка голоса была качественной, аферисты используют записи, размещенные в социальных сетях (видеоролики со звучащей речью), или «указывают, что голоса им нужны для озвучивания игры, кино, для социального

эксперимента. Размещают объявление, где предлагают приобрести запись голоса. У человека просят прочитать абзац текста. Записи с большим количеством словесных паттернов загоняют в программы, после чего они достаточно быстро могут вести диалог от любого индивидуума. Зачастую люди, чтобы заработать 200–500 руб., не будут пытаться найти какие-то подводные камни, и предоставят такую услугу» [8]. Специалисты в сфере информационных технологий отмечают, что преступники воруют наши голоса, чтобы воровать наши деньги. Задержать их крайне сложно, если вообще возможно [9].

Однако имитациями голосов мошенники не ограничились. Сегодня они активно используют в преступных целях и дипфейк-видео, генерируемые нейросетями, которые собирают в Интернете фотографии человека с разными выражениями лица и создают из них новое изображение. Так, жительница г. Зуевки Кировской области перевела на счет злоумышленников 300 000 руб. По ее словам, по видеосвязи ей позвонил сотрудник спецслужб, за его спиной висел портрет Президента Российской Федерации В.В. Путина, данный факт натолкнул женщину на мысль о том, что она разговаривает с настоящим силовиком. Позже этот же преступник, который выглядел как актер Роберт Дауни-младший и представился полицейским, попытался выманить деньги у мужчины, но потерпел неудачу [10]. Отметим, что мошенники используют не только изображения известных людей, но и обычных граждан, поэтому совершенно правы те, кто утверждает, что в происходящем «есть доля и нашей с вами вины. Мы уж слишком выставляем себя напоказ, снимаем сторис, выкладываем фотографии, рассказываем о себе и своих увлечениях и, как следствие, получаем реальные оплеухи из мира виртуального, лишь в этот момент понимая, что попали в глобальную сеть. И она не умеет хранить секреты» [9].

Технологии создания дипфейков пока несовершенны, поэтому вывести мошенников на чистую воду можно с помощью наблюдения за видеоизображением (движениями (человек на видео не моргает или моргает редко, движения губ плохо синхронизируются со звучащей речью), цветом кожи, глаз). Кроме того, чтобы уберечь свои денежные средства от преступников, необходимо

прислушиваться к речи (особенностям артикуляции, построения фраз, использования слов), пользоваться антивирусным программным обеспечением, перезванивать родственникам и знакомым, попросившим одолжить денег, не отвечать на видеозвонки с неизвестных номеров, наконец, не отключать критическое мышление, ибо мы живем в то время, когда уже не приходится верить даже собственным глазам и ушам.

Список литературы

1. Состояние преступности в России за январь-декабрь 2020 года. Состояние преступности в России за январь-декабрь 2021 года. Состояние преступности в России за январь-декабрь 2022 года. Состояние преступности в России за январь-декабрь 2023 года [Электронный ресурс]. – Режим доступа: https://portal.tpu.ru (дата обращения: 21.03.2024).

2. Корочкина А. Кибермошенники украли почти 16 млрд руб. у россиян в 2023 году / А. Корочкина [Электронный ресурс]. – Режим доступа: https://clck.ru/3AJsDQ (дата обращения: 21.03.2024).

3. За 2023 год мошенники похитили со счетов граждан 15,8 млрд руб. Почему им это удалось? [Электронный ресурс]. – Режим доступа: https://www.dk.ru/news/237198415 (дата обращения: 21.03.2024).

4. Как нейросети-мошенники имитируют чужие личности [Электронный ресурс]. – Режим доступа: https://dzen.ru/a/Yg0nLAbNy0uEFgjW (дата обращения: 21.03.2024).

5. Дипфейки и другие поддельные видео – как защитить себя? [Электронный ресурс]. – Режим доступа: https://clck.ru/3AJsFW (дата обращения: 21.03.2024).

6. В ЦБ предупредили о мошенниках, подделывающих голоса для обмана россиян [Электронный ресурс]. – Режим доступа: https://clck.ru/3AJsGu (дата обращения: 21.03.2024).

7. Рахимова Р. «Один в один, отличить невозможно!»: аферисты выманили у блогера деньги, подделав голос ее подруги с помощью нейросетей / Р. Рахимова [Электронный ресурс]. – Режим доступа: https://clck.ru/3AJsJk (дата обращения: 21.03.2024).

8. Охотники за голосами. Как и зачем злоумышленники создают дипфейки [Электронный ресурс]. – Режим доступа: https://www.kommersant.ru/doc/6608487 (дата обращения: 21.03.2024).

9. Не верьте глазам своим: мошенники взяли на вооружение возможности дипфейков [Электронный ресурс]. – Режим доступа: https://clck.ru/3AJsLf (дата обращения: 21.03.2024).

10. Джабборов Д. Мошенник с лицом Роберта Дауни-младшего попытался украсть деньги кировчанина / Д. Джабборов [Электронный ресурс]. – Режим доступа: https://www.gazeta.ru/tech/news/2024/03/22/22608199.shtml (дата обращения: 22.03.2024).