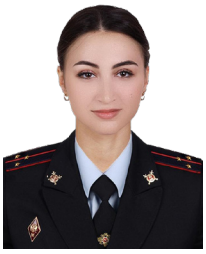
ДИСКУССИОННАЯ ТРИБУНА СОИСКАТЕЛЕЙ УЧЕНЫХ СТЕПЕНЕЙ И ЗВАНИЙ

УДК 343.985.7 DOI 10.51980/2542-1735_2023_2_187



Нина Игоревна СТАРОСТЕНКО,
адъюнкт Краснодарского университета
МВД России
nstarostenko1996@mail.ru

КРИМИНАЛИСТИЧЕСКОЕ ПРОГНОЗИРОВАНИЕ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ «DEEPFAKE»-ТЕХНОЛОГИЙ

CRIMINALISTIC FORECASTING OF THEFTS COMMITTED BY USING «DEEPFAKE»-TECHNOLOGIES

Статья посвящена изучению способа совершения мошеннических действий с использованием «deepfake»-технологий с позиции криминалистического прогнозирования. Выявлены основные направления использования «deepfake»-технологий при хищениях: создание видеофайлов, на которых лицо оригинального человека замещается лицом другого человека; создание видеофайлов путем считывания мимики одного человека и последующего ее синтеза с лицом другого человека без соответствующей замены лиц, указанной в первом случае; создание синтезированного голоса из образцов аудиозаписей определенного человека. В заключение сделан вывод о необходимости использования прогностической информации для разработки рекомендации по совершенствованию проведения отдельных следственных действий в ходе расследования хищений, совершенных в сфере информационно-телекоммуникационных технологий.

The article is devoted to the study of the method of committing fraudulent actions using «deepfake» technologies from the perspective of criminalistic forecasting. The main directions of using «deepfake» technologies for thefts are revealed: the creation of video files in which the face of the original person is replaced by the face of another person; creation of video files by reading the facial expression of one person, and then synthesizing it with the face of another person, without the corresponding replacement of faces indicated in the first case; creating a synthesized voice from sample audio recordings of a particular person. At the end, the conclusion is made about the necessity of using the predictive information in order to develop recommendations for improvement of conducting certain investigative actions when investigating thefts committed in the sphere of information and telecommunication technologies..

Ключевые слова: криминалистика, расследование преступлений, криминалистическое прогнозирование, хищения, социальная инженерия, deepfake.

Keywords: *forensics, crime investigation, criminalistic forecasting, thefts, social engineering, deepfake.*

В настоящее время проблемы, связанные с ростом преступности в сфере информационно-телекоммуникационных технологий, приобретают все большую актуальность. Основную часть среди указанных преступлений составляют хищения. Так, в 2019 г. зарегистрированы 294 409 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в 2020 г.– 510 396, в 2021 г. – 517 722. При этом восемь таких преступлений из десяти совершаются путем кражи (98 798 – 2019 г., 173 416 – 2020 г., 156 792 – 2021 г.) или мошенничеств (136 709 тыс. – 2019 г., 237 074 – 2020 г., 249 249 – 2021 г.), что составляет 79,9% в 2019 г., 80,4 % в 2020 г. и 8,4 % в 2021 г.[1]

Это обусловлено, прежде всего, широким распространением технологий дистанционного банковского обслуживания, увеличением количества транзакций, совершаемых клиентами банков дистанционно через удаленные каналы связи, с одной стороны, а с другой – появлением технологий, позволяющих осуществлять преступную деятельность анонимно, используя при этом компьютерную технику, различные программные средства, средства мобильной связи, сеть Интернет. Данные условия стали благодатной почвой для эволюции способов совершения преступных действий против собственности. Вместе с тем преступники, совершающие хищения в сфере информационно-телекоммуникационных технологий, постоянно совершенствуют преступные навыки, применяя в своей деятельности не только современные программные средства, но и так называемые методы социальной инженерии, в результате использования которых владелец счета либо самостоятельно переводит свои денежные средства на счет преступников, либо передает конфиденциальную информацию (например, персональные данные, данные платежных карт, контрольную информацию, пароли), необходимую для получения доступа к счету[2].

Преступники в процессе подготовки, непосредственного совершения и сокрытия преступных действий используют специальные программы для изменения голоса, подмены номера телефона, удаленного доступа к компьютерному устройству, сокрытия IP-адреса и др. Данные инструменты помогают скрытно и дистанционно оказывать психологическое воздействие на жертв в целях побуждения у них желания в предоставлении конфиденциальной информации, способствующей неправомерному доступу к банковскому счету (карте), осуществления ими денежных переводов на банковские счета сторонних лиц или убеждения в необходимости выполнения иных действий, создающих благоприятные условия для последующего завладения чужим имуществом [подр.: 12].

Так, инструментами, работа которых основана на технологиях искусственного интеллекта, являются программы по созданию «deepfake»-файлов: «FaceSwap», «DeepFaceLab», «Avatarity», «Doublicat», «Deepfakes web» и др. Указанные инструменты могут преобразовывать аудио-, фото- и видеоматериалы с заменой лиц или голоса любого человека. Широкое использование данных «продуктов» стало возможным благодаря распространению программных интерфейсов для редактирования медиафайлов. Дистрибутивы программного обеспечения для персональных компьютеров, предоставляющие возможность осуществлять манипуляции с аудио-, фото- и видеоматериалами, доступны неограниченному кругу лиц. Открывающая принципиально новые возможности для целого ряда индустрий (рекламы и медиа, индустрии развлечений и игр, киноиндустрии, медицины и т.д.) эта технология также может быть использована злоумышленниками в преступных целях [8, с. 90-101]. Данные программы стали использоваться для манипуляций и нанесения вреда третьим лицам [11, с. 103-105].

По мнению исследователей, «deepfake»-технологии могут использоваться для

1 Официальный сайт МВД России. Краткая характеристика состояния преступности в Российской Федерации за 2019-2021 гг. URL: https://мвд.рф/reports (дата обращения: 19.01.2022).

2 Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств) URL: https://sozd.duma.gov.ru/bill/186266-7 (дата обращения: 10.11.2021).

кражи личных данных для совершения мошеннических действий, в случаях, когда злоумышленник выдает себя за государственных служащих или членов семьи жертвы, реализуя корыстный интерес, при совершении хищений с переводом денежных средств путем выдачи себя за сотрудника кредитно-финансовой организации и др. [4].

Анализ судебно-следственной практики в России не выявил фактов многократного использования технологий «deepfake» при совершении хищений, но их существование, активная разработка и внедрение позволяют сделать вывод об их соответствии потребностям злоумышленников, совершающих мошеннические действия, а также прогнозировать их широкое применение в корыстных целях на ближайшую перспективу. В этой связи возрастает потребность в изучении новых способов совершения преступлений с позиции криминалистического прогнозирования, что позволит определить дальнейшее направление прогноза – его реализацию в виде разработки рекомендаций, повышающих уровень подготовленности сотрудников правоохранительных органов к противодействию мошенническим действиям, совершенным с применением «deepfake»-технологий.

Рассмотрим основные понятия криминалистического прогнозирования, имеющиеся в специальной литературе.

Криминалистическое прогнозирование представляет собой основанное на анализе действия объективных закономерностей развития криминалистически значимых явлений, событий и процессов и использовании положений теории прогностики предвидение направлений дальнейшего развития криминалистики как науки, целесообразного корректирования всех видов практической криминалистической деятельности (ее методов и средств) в условиях предполагаемого изменения и появления новых видов преступной деятельности, способов ее совершения и т.д. [7, с. 148]. Это процесс, результатом которого является составление прогноза как формы научного предвидения, как системы аргументированных представлений о будущем, как характеристики вероятных направлений развития. Результатом этого процесса служит прогноз – вывод о возможном наступлении явлений, процессов, событий, основанный на анализе соответствующих данных. Содержание прогноза составляет прогностическая информация, т.е. информация о будущем [6, с. 143-144].

Рядом ученых понятие «криминалистического прогнозирования» рассматривается в двух аспектах:

в качестве частного криминалистического учения, содержанием которого является теория криминалистического прогнозирования (предсказания) неизвестных событий;

в качестве разновидности отраслевого прогнозирования, процесса, результатом которого является прогноз практического характера, сущность которого заключается в научном предсказании криминалистических аспектов развития преступности определенного вида, способов совершения преступлений и т.д. [10, с. 95-96]

Следовательно, осознание возможности применения инструментов «deepfake» в корыстных целях в будущем помогает прогнозировать способ совершения хищения, выявить его особенности, формы использования современных технологий искусственного интеллекта, что позволит скорректировать существующие и разработать новые рекомендации по проведению отдельных следственных действий, таких как осмотр аудио- и видеоматериалов, предположительно созданных с применением указанных инструментов.

На сегодняшний день существуют несколько разновидностей «deepfake»: звуковые, фото- и видео «дипфейки» (сочетающие комбинацию динамического изображения и голоса человека). Одна из самых популярных программ – «DeepFaceLab», открытое программное обеспечение от российского разработчика, называющего себя «Iperov», позволяет не только вставлять лицо в видео, но и менять движения губ говорящего, т.е. подделывать содержание речи [5].

В основе технологии создания реалистичных аудиовизуальных материалов «deepfake» лежит один из подвидов искусственного интеллекта – генеративно-состязательные нейронные сети (GAN). Посредством машинного обучения искусственные нейронные

сети на реальном наборе аудио-, видео- и фотоматериала учатся генерировать реалистичный поддельный контент [2].

Рассмотрим основные понятия «deepfake»-технологий.

«Deepfake»-технологии – технологии, основанные на применении искусственного интеллекта, которые позволяют преступникам искажать реалистичные фото, аудио, видео и иные носители информации о лицах, местах, предметах, событиях, обстоятельствах и т.п. и тем самым создавать качественную подделку, путем кибератаки на нейронные сети через введение данных [4, с. 191-194].

«Deepfake»-технологии – вид технологий, использующих искусственный интеллект, а именно – технологию «машинного обучения» для создания «синтетического контента» [4].

С точки зрения экспертно-криминалистических исследований под «deepfake»-технологиями понимается внутрикадровый монтаж с направленным на искажение сути изначальной сцены видеоизображения [9].

Основные направления использования «deepfake»-технологий:

1) создание видеофайлов, на которых лицо оригинального человека замещается лицом другого человека. Так, в сентябре 2021 г. в социальных сетях распространилось мошенническое видео, на котором было наложено лицо российского предпринимателя (основателя «Тинькофф банка»). Человек с лицом предпринимателя предлагал людям внести сумму на определенный сайт, а взамен получить выгоду, в полуторном размере превышающую сумму вклада. При переходе по ссылке рядом с видео пользователь попадал на лендинг с логотипом банка и инвестиционного сервиса. Ему предлагали ответить на несколько общих вопросов и оставить имя, телефон и email. Сгенерированное видео было не самого хорошего качества: движения губ и речь рассинхронизированы, голос не похож на оригинал. Но этого хватило, чтобы обмануть пользователей, которые пролистывают ленту в социальных сетях[1];

2) создание видеофайлов путем считывания мимики одного человека и последующего ее синтеза с лицом другого человека без соответствующей замены лиц, указанной в первом случае. Примерами этого направления применения «deepfake»-технологий могут послужить случаи, когда злоумышленники используют видеоматериалы, на которых имеется запись с участием известных людей. Так, считывая их мимику мошенники синтезируют ее с лицом другого человека и далее создают видеофайлы, распространяют их в социальных сетях с содержанием просьб «перевести деньги на благотворительность», «поучаствовать в розыгрыше призов или денежных средств» и др. [1];

3) создание синтезированного голоса из образцов аудиозаписей определенного человека. Злоумышленники, получив образец голоса, с помощью искусственного интеллекта могут проводить анализ аудиозаписи и на ее основе осуществлять моделирование синтетического профиля определенного человека для введения в заблуждение потенциальной жертвы. Так, одним из примеров совершения хищения с применением «deepfake»-технологий является случай, произошедший в Великобритании. Преступники с помощью манипуляции с аудиозаписью голоса генерального директора британской энергетической компании убедили сотрудника корпорации перечислить им €220 тыс. Для усиления убеждения преступники смогли повторить не только сам голос директора, но и особенности его речи, акцент[2].

Таким образом, при совершении хищений злоумышленники могут использовать специальные программные средства «deepfake», работа которых основана на технологиях машинного обучения, создающих «синтетический контент» и содержащих специальные инструменты, с помощью которых может моделироваться человеческий образ путем осуществления вмешательства в структурную целостность аудио- или фотоматериалов, выполняться внутрикадровый монтаж видеома-

1 Мошенники впервые создали дипфейк Олега Тинькова для поддельной рекламы. URL: https://www.rbc.ru/finances/06/09/2021/6135fce99a794722f3400ff7 (дата обращения: 05.02.2021).

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: 20.10.2022).

териалов. Указанные инструменты «в руках» злоумышленника могут использоваться им в целях оказания психологического воздействия на жертву и убеждения ее в выполнении перевода денежных средств на счет преступников либо в передаче конфиденциальной информации (например, персональных данных, данных платежных карт, контрольной информации, паролей), необходимой для получения доступа к банковскому счету.

Вместе с тем в связи с предложенными данными можно констатировать, что возможности «deepfake»-технологий, которые могут применяться в корыстных целях, следует считать криминалистически значимыми явлениями, поскольку рассмотренные направления и закономерности их использования имеют значение для формирования научных предсказаний криминалистических аспектов развития преступности анализируемого вида.

На наш взгляд, представляется важным предвидеть развитие преступности анализируемого вида и предложить некоторые варианты решения данных проблем.

Во-первых, необходимо разработать криминалистические рекомендации, содержащие совокупность средств и методов обнаружения признаков использования злоумышленниками «deepfake»-технологий, которые могут применяться сотрудниками органов предварительного расследования в ходе проведения отдельных следственных действий, например при осмотре видео- и аудиофайлов.

Во-вторых, требуется создание и внедрение в деятельность экспертных учреждений специальных программных средств для проведения исследований, устанавливающих монтаж аудиозаписей, а также внутрикадровый монтаж видеозаписей, созданных при помощи нейронных сетей («deepfake»-технологий). Данная рекомендация существенна при проведении судебной фоноскопической и судебной видеотехнической экспертиз. Здесь важно подчеркнуть, что такие программы действительно находятся в разработке, например «Зеркало (Верблюд)»[1]. Данное программное средство разрабатывается в рамках проведения научно-исследовательской работы «Исследование возможных способов выявления признаков внутрикадрового монтажа видеоизображений, выполненного с помощью нейронных сетей». Указанная программа, на наш взгляд, может повысить уровень научно-технического обеспечения деятельности экспертно-криминалистических подразделений МВД России по линии производства видеотехнических экспертиз и исследований в современных условиях.

Таким образом, осуществлен криминалистический прогноз возможных направлений и форм использования искусственного интеллекта при совершении хищений в сфере информационно-телекоммуникационных технологий. Определено, что наиболее вероятными направлениями использования таких технологий в корыстных целях являются инструменты «deepfake», работа которых основана на технологиях машинного обучения, создающих «синтетический контент», а также содержащих специальные инструменты, с помощью которых может моделироваться человеческий образ путем осуществления вмешательства в структурную целостность аудио-, фотоматериалов, выполняться внутрикадровый монтаж видеоматериалов, в целях оказания психологического воздействия на жертву и убеждения ее в разглашении конфиденциальных данных (персональных или банковских) или совершения финансовых операций по банковскому счету. Полученная в ходе исследования прогностическая информация может позволить эффективно скорректировать существующие и разработать новые рекомендации по совершенствованию проведения отдельных следственных действий в ходе расследования хищений, совершенных в сфере информационно-телекоммуникационных технологий (например, в ходе осмотра аудио- и видеоматериалов, которые предположительно созданы при помощи технологий «deepfake»).

1 Официальный сайт Единой информационной системы в сфере закупок https://zakupki.gov.ru/epz/order/notice/ok504/view/common-info.html?regNumber=0173100013920000080# (дата обращения: 18.11.2022).

Библиографический список

1. Девяткин, Г.С. Особенности организации допроса потерпевшего с использованием высоких технологий по уголовным делам, связанным с совершением киберпреступлений / Г.С. Девяткин // Вестник военного права. – 2021. – N 1. – С. 17-23.

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. – Т. 15. – N 3. – С. 372-379. – DOI 10.17150/2500-4255.2021.15(3).372-379.

3. Зоз, В.А. Использование технологий искусственного интеллекта в правоохранительных органах / В.А. Зоз, А.Р. Шроль // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. – 2021. – Т. 7. – N 2. – С. 191-194. – DOI 10.37279/2413-1733-2021-7-2-191-194.

4. Карпика, А.Г. Проблемы эффективного противодействия преступлениям, совершаемым с использованием технологии машинного обучения / А.Г. Карпика // Философия права. – 2021. – N 4 (99). – С. 80-83.

5. Киселев, А.С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности / А.С. Киселев // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2021. – N 3. – С. 54-64. – DOI 10.18384/2310-6794-2021-3-54-64.

6. Криминалистика : учебник для вузов / под ред. Р.С. Белкина. – М.: Издательство НОРМА, 2000. – 990 с.

7. Криминалистика : учебник / отв. ред. Н.П. Яблоков. – 3-е изд., перераб. и доп. – М.: Юристъ, 2005. – 781 с.

8. Лексютина, Я.В. Злонамеренное использование дипфейков: риски информационно-психологической безопасности Японии / Я.В. Лексютина // Японские исследования. – 2021. – N 3. – С. 90-101. – DOI 10.24412/2500-2872-2021-3-90-101.

9. Проценко, Д.Е. Диагностические признаки внутрикадрового монтажа видеоизображений, выполненного с помощью нейронных сетей / Д.Е. Проценко, Д.Н. Жидков // Судебная экспертиза: прошлое, настоящее и взгляд в будущее : материалы международной научно-практической конференции, Санкт-Петербург, 13 мая 2021 года. – СПб.: Санкт-Петербургский университет МВД России, 2021. – С. 277-281.

10. Савельева, М.В. Криминалистика : учебник / М.В. Савельева, А.Б. Смушкин. – М.: Издательство Издательский дом «Дашков и К», 2009. – 608 с.

11. Соколова, А.С. Феномен дипфейка: существующие угрозы и проблемы правового регулирования / А.С. Соколова // Актуальные научные исследования в современном мире. – 2021. – N 11-5(79). – С. 103-105.

12. Старостенко, Н.И. Выявление методов социальной инженерии при совершении хищений с использованием информационно-телекоммуникационных технологий / Н.И. Старостенко // Вестник Академии Следственного комитета Российской Федерации. – 2022. – N 1 (31). – С. 172-181. – DOI 10.54217/2588-0136.2022.31.1.023.

13. Westerlund, M. The emergence of deepfake technology: A review / M. Westerlund // Technology Innovation Management Review. – 2019. – Т. 9. – N. 11. – P. 39-52.