Тел.89178332511

Яна Александровна КЛИМОВА,

кандидат юридических наук, доцент, ORCID 0009-0008-7226-4925

Волгоградская академия МВД России

профессор кафедры криминалистики

учебно-научного комплекса по предварительному следствию в ОВД

aya3008@yandex.ru

Научная статья

УДК 343.985.7

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ДИПФЕЙК

КЛЮЧЕВЫЕ СЛОВА: Дипфейк, искусственный интеллект, расследование преступлений, цифровизация, методика расследования, IT-технологии, цифровая криминалистика, технико-криминалистическое обеспечение расследования, специальные знания.

АННОТАЦИЯ. ***Введение.*** Современная криминалистическая наука претерпевает существенную трансформацию в результате стремительной цифровизации, коснувшейся всех сфер жизни общества. Вследствие чего в последнее время в фокус внимания ученых-криминалистов все чаще попадают технологии искусственного интеллекта. При этом затрагиваются как их позитивные стороны, например, реализация прогностической функции, использование искусственного интеллекта при получении и анализе оперативно-разыскной и криминалистически значимой информации, так и негативные, связанные с противодействием потенциальным угрозами, поскольку современные технологии помогают не только раскрывать преступления, но и совершать их. Актуальность исследования обусловлена необходимостью использования возможностей цифровой криминалистики

при разработке криминалистических рекомендаций, способствующих эффективному и качественному расследованию высокотехнологичных преступлений. ***Методы.*** Исследование опиралось на универсальный диалектический метод, общенаучные методы познания (наблюдение, анализ, синтез, дедукция и др.) и специальные методы научного исследования (формально-юридический, сравнительно-правовой, статистический анализ, метод криминалистического прогнозирования и др.). Научная новизна исследования определяется кругом исследуемых проблем, носящих комплексный характер для криминалистической деятельности. ***Результаты.*** Автором рассмотрены понятие и сущность технологии дипфейка, проведен анализ статистических данных по данной категории преступлений. Делается вывод о стремительном росте указанных преступлений во всех странах. Выявленная проблема свидетельствует о необходимости изучения механизма совершения преступлений. Отсутствие судебно-следственной практики предопределило необходимость криминалистического анализа таких правонарушений. В результате автором выделяются отдельные способы совершения преступлений с использованием технологии дипфейк. В заключении формулируются перспективные направления, позволяющие эффективно расследовать и предупреждать преступления, совершенные с использованием технологии дипфейк.

ВВЕДЕНИЕ

Активное внедрение информационных технологий в повседневную жизнь способствовали кардинальному изменению архитектуры преступного мира и, как следствие, появлению разнообразных высокотехнологичных способов совершения преступлений.

Полагаем, что если рассматривать криминалистическую деятельность как определенный процесс и учитывать основные тенденций развития современного научного криминалистического знания, то очевидно, что

стремительная цифровизация послужила толчком к смене парадигмы расследования преступлений.

В последнее время все большую популярность в преступном мире набирает «тренд», связанный с использованием в преступных целях технологии искусственного интеллекта.

По всему миру фантастическими темпами растёт количество случаев мошенничества с использованием искусственного интеллекта. Страны накрывает эпидемия высокотехнологического обмана, проникающего во все сферы цифрового пространства. В течение последних двух лет дополнительную сложность стало представлять распространение такого вида преступления, совершенного с использованием искусственного интеллекта, как мошенничество с применением технологии DEEPFAKE (далее – дипфейк).

Об актуальности исследуемой проблемы свидетельствует внимание к ней самом высшем государственном уровне. Так, 14 декабря 2023 г. в рамках мероприятия «Итоги года с Владимиром Путиным – 2023» в ходе прямой линии к Президенту России Владимиру Путину обратился с вопросом «цифровой двойник», созданный с использованием технологии дипфейк. После этого российский лидер подчеркнул, что предотвратить развитие искусственного интеллекта невозможно, а значит, нужно стремиться быть лидерами в этом направлении.[1]

МЕТОДЫ

Методологической основой исследования являются универсальный диалектический метод, рассматривающий предмет исследования с точки зрения его непрерывного развития, изменения и взаимосвязи с другими явлениями, а также общие и частные методы научного познания правовых явлений: сравнительно-правовой метод, способствовавший выявлению сходства состояния преступности в России и зарубежных странах; методы

[1]Итоги года с Владимиром Путиным – 2023 // URL: https://www.pnp.ru/story/itogi-goda-s-vladimirom-putinym-2023/ (дата обращения: 29.04.2024).

анализа и синтеза для изучения позиций ученых по ключевым аспектам темы, при осуществлении исследования нормативных актов различного уровня, анализе материалов практики; системно-структурного анализа, использованный при изучении механизма совершения данных преступлений; формально-юридический, позволивший выявить различные способы совершения преступления с использованием технологии дипфейк, а также толковать нормы действующего законодательства; статистического анализа, позволивший исследовать статистические данные, практику и выявить существующие проблемы; метод криминалистического прогнозирования, использованный для обоснования необходимости разработки частной криминалистической теории расследования преступлений в условиях цифровизации.

ОБСУЖДЕНИЕ

Отсутствие легитимной дефиниции и законодательной регламентации дипфейков предопределяет их преступный потенциал. На устранение лакун в нормативном регулировании дипфейков направлена законодательная инициатива о введении ответственности за несанкционированное использование голоса и изображений человека в целях мошенничества[2].

Кроме того, на заседании Правительственной комиссии по профилактике правонарушений, состоявшейся 20 декабря 2023 года, было принято решение, согласно которому до ноября 2024 года в результате совместной работы МВД, Минцифры и Роскомнадзора должен быть разработан алгоритм правового регулирования «цифровых портретов» в целях недопущения их противоправного использования[3].

[2]В Госдуме работают над законопроектом о запрете дипфейков// URL: https://pravo.ru/news/251111/(дата обращения: 09.05.2024).

[3] Владимир Колокольцев провел заседание Правительственной комиссии по профилактике правонарушений // URL:https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedfanie-pravitelstvennoy-komissii-po-profilaktike-pravonarusheniy/ (дата обращения: 06.05.2024).

Исследованию проблем законодательной регламентации и противодействия технологии дипфейков посвящены работы многих ученых: Е. Ю. Антоновой, В. Б. Батоева, А. В. Пучнина, Е. С. Лариной, В. С. Овчинского, С. В. Лемайкиной, О.В. Расторопова и др. [1-5].

Криминалистические аспекты расследования преступлений и использования искусственного интеллекта в противоправной деятельности исследовались А. А. Бессоновым, Д. В. Бахтеевым, О. Б. Дроновой, Д. С. Клюевым, А. Б. Смушкиным, Ю. В. Соколовой, С. Е. Платоновым, Е. Л. Лужинской, В. А. Чванкиным и др. [6-10].

Согласно статистическим данным платформы Statista[4]за 2022-2023 г. проанализировано два миллиона случаев из 124 стран, в результате в мире зафиксирован взрывной рост мошенничеств, связанных с использованием технологии дипфейк (см. иллюстрацию 1). Эти преступления буквально охватывают весь мир вне зависимости от социально-экономического развития, политического режима и иных различий государств.

Так, в 2023 году на Филиппинах число случаев мошенничества с использованием дипфейков выросло на 4500% по сравнению с 2022 годом. Во Вьетнаме рост составил больше 3000%, в Японии - 2800%. Четырёхзначные цифры темпов роста зафиксированы и в США, ОАЭ, ЮАР и многих странах Европы.

[4]Statista — международная глобальная платформа данных с обширной коллекцией статистических данных, отчетов и аналитической информации // URL: https://www.statista.com/aboutus/ (дата обращения: 02.05.2024).

Иллюстрация 1. Стремительный рост мошенничества, с использованиемтехнологии дипфейк (указаны страны с наибольшим ростом таких случаев), за период с 2022 по 2023 год (в %).

Согласно отчету Onfido (компании, разрабатывающей платформы безопасной цифровой идентификации личности) на основе анализа мошеннических схем с личными данными в 2024 году прогнозируется увеличение на 3000% количества цифровых атак[5].

Считаем правильным присоединиться к мнению В. Б. Батоева и А. В. Пучнина, считающих, что дипфейки находятся в прямой зависимости от уровня развития информационных технологий [2; с. 166]. Если раньше дипфейки встречались относительно редко из-за их технологической сложности, то сейчас наблюдается тенденция к упрощению и общедоступности технологии. Широко применяется «цифровая ретушь» и «цифровой монтаж» [11; с. 279].

Сегодня существует множество онлайн сервисов, приложений, ботов, позволяющих их создавать (например, DeepFaceLab, Zao, FaceSwap, Neuman,

[5]Отчет о мошенничестве с личными данными, 2024 г. Onfido// URL: https://onfido.com/landing/identity-fraud-report/(дата обращения: 07.05.2024).

Deepfakesweb и т.д.). Как только технология стала доступна большинству, её начали активно использовать и мошенники.

Здесь целесообразно привести точку зрения, высказанную М.А. Желудковым, согласно которой необходимо видеть общую картину киберпреступности и анализировать способы совершения преступлений с использованием программ искусственного интеллекта [12; с. 68].

Сказанное обуславливает необходимость более подробного рассмотрения указанной технологии.

Дипфе́йк (англ. Deepfake, от deeplearning – глубокое обучение и fake – подделка) - технология на базе искусственного интеллекта, позволяющая создавать ложные изображения и видео на основе реальных кадров.[6]

Алгоритм анализирует большое количество снимков, аудио, видео и учится тому, как может выглядеть, говорить и двигаться конкретный человек. Нейросеть собирает из интернета, в том числе из открытых источников в социальных сетях, аудио- и видеофайлы, фотографии человека с разными выражениями лица и создает из них новое изображение, аудио или видео. Дипфейки выглядят гиперреалистично, поскольку инструменты искусственного интеллекта были обучены на десятках тысяч изображений реальных людей (см. иллюстрацию 2).

[6] Большая российская энциклопедия (Официальный сайт) // URL: http://bigenc.ru/c/dipfeik-f9f89b (дата обращения: 03.05.2024).

Иллюстрация 2. Примеры изображений, сгенерированных нейросетями.

Следует согласиться с мнением В.Г. Иванова и В.Р. Игнатовского, которые считают, что возможно более серьезной проблемой, чем манипуляции с изображениями и видео, является способность технологии имитировать акцент, интонацию и речевые паттерны с недоступной прежде точностью [13; с. 67].

Кроме того, мошенники с целью получения образцов голосов стали размещать в интернете объявления с предложением о платной озвучке рекламы и фильмов (см. иллюстрацию 3). Целью является обучение нейросетей и последующая генерация аудиосообщений для вымогательства денег у родственников и друзей.

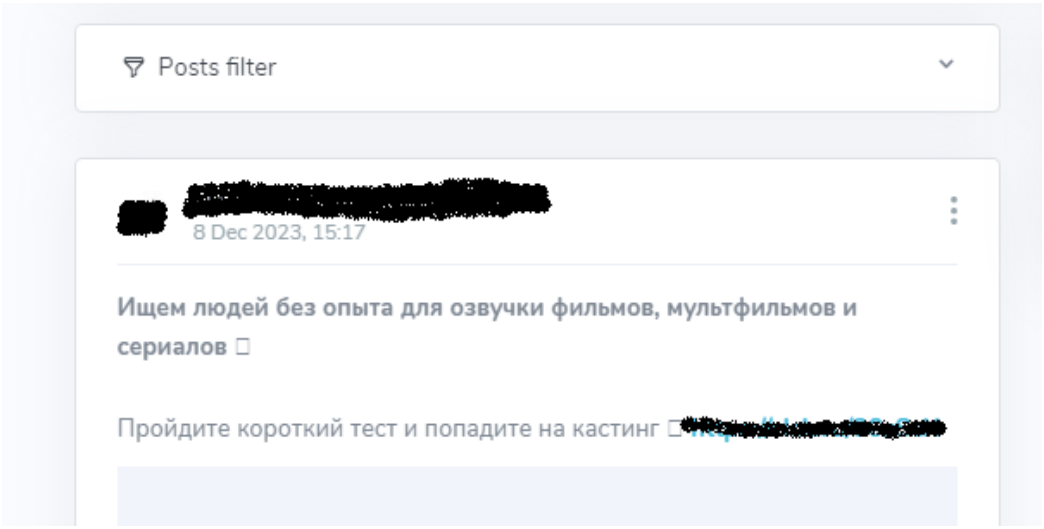


Иллюстрация 3. Объявление в мессенджере.

Таким образом, нейросети научились создавать «цифрового двойника» практически любого человека. Они могут подделывать не только внешность, но и голос.

РЕЗУЛЬТАТЫ

Дипфейки становятся все более реалистичными и убедительными. Такая трансформация способствует появлению все новых мошеннических схем. Рассмотрим некоторые способы совершения таких преступлений.

Сейчас наибольшее распространение получила схема «fakeboss» - указания от фейкового руководителя. Сначала в мессенджер (чаще всего, Telegram или WhatsApp) приходит текстовое сообщение о том, что сотруднику будет звонить начальник (представитель государственных органов) или голосовое сообщение аналогичного содержания. Затем, используя методы социальной инженерии, под видом форс-мажора, мошенники заставляют потерпевшего перевести деньги на «безопасный счет».

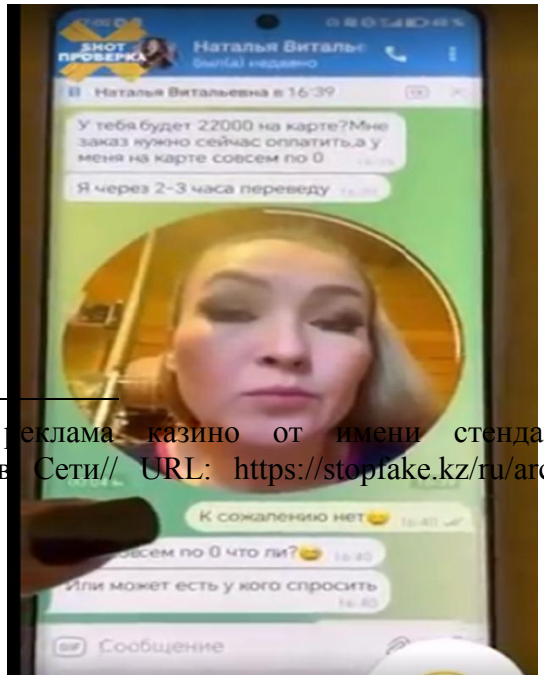
Другим способом является использование образа узнаваемой популярной личности. Так, в конце ноября 2023 г. в сети появилось видео, где известный комик и киноактер Нурлан Сабуров рекламирует приложение

онлайн-казино. На самом деле это дипфейк—так мошенники завлекают пользователей на фишинговый сайт[7].

Поскольку генеральная идея любых дипфейков — максимальная реалистичность и правдоподобность, то уже сегодня можно наблюдать лавинообразный рост модифицированного контента, созданного с целью манипуляции сознанием отдельно взятого человека.

Еще один новый вид мошенничества заключается в хищении средств с использованием Voicedeepfake. Суть данного способа точно сформулировал Р. Н. Малышкин: хищение с помощью голосовых клонов [14; с. 332].

Преступники с помощью нейросети генерируют голосовые обращения владельцев аккаунта и вымогают деньги у его контактов, прикрепляя фото банковской карты с именем и фамилией. На первом этапе преступники взламывают аккаунты в мессенджерах, например, Telegram или WhatsApp, с помощью фейковых голосований. Затем они скачивают сохраненные голосовые сообщения и создают новые сообщения с нужным контекстом. В конечном итоге они рассылают эти сообщения в личные и групповые чаты с просьбой об одолжении большой суммы денег, подкрепляя их сгенерированными голосовыми сообщениями и отфотошопленными банковскими картами с поддельными именами получателей (см. иллюстрацию 4).



[7]Фейковая реклама: казино от имени стендап-комика Нурлана Сабурова распространяется в Сети// URL: https://stopfake.kz/ru/archives/21066 (дата обращения: 30.04.2024).

Иллюстрация 4. Пример дипфейка, с помощью которого мошенники получают деньги в телеграмме (видео по QR-коду).

Другим распространенным и при этом легким дипфейк-способом изъятия денежных средств у населения является запись мошенниками голоса жертвы, например, при спам-звонках.

Главная задача состоит в том, чтобы добиться произнесения ключевых слов, например, таких как «да», на основе которых генерируется типовая звуковая дорожка для «общения» с роботом службы поддержки банка. Грамотно синтезированная на базе ключевых фрагментов запись позволяет «достоверно» ответить на все вопросы робота для перевода средств на нужный мошенникам счет.

В начале 2024 года в России уже зафиксированы попытки использования еще одного способа мошенничества: преступники, используя технологию дипфейка для подтверждения по видеозвонку личности владельца аккаунта, обращаются в банк с просьбой привязать личный кабинет к новому номеру телефона. После указанных действий мошенники получают полный доступ к личному кабинету потерпевшего и ко всем денежным средствам (см. иллюстрацию 5).

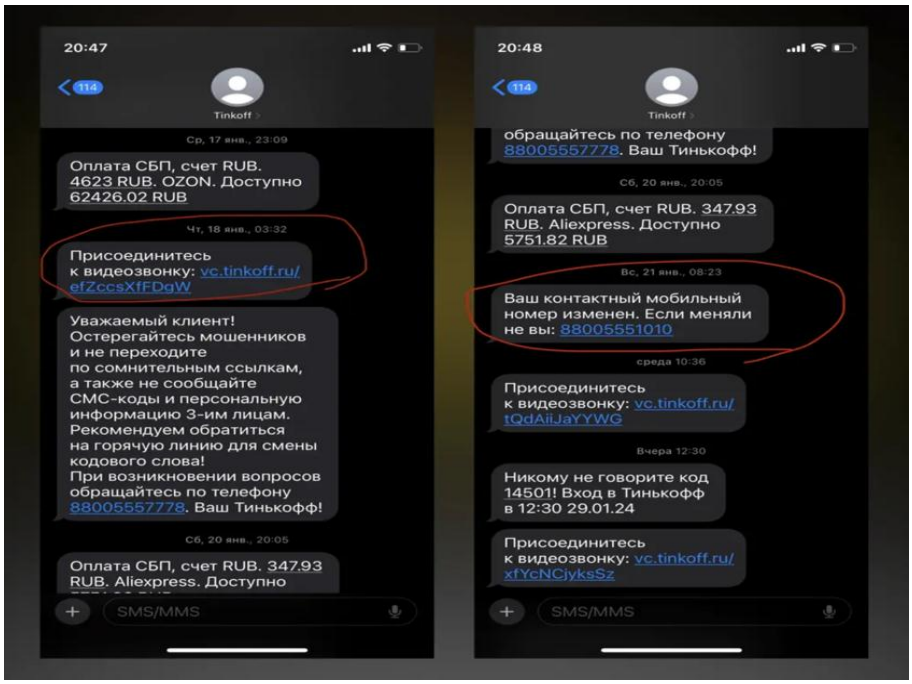


Иллюстрация 5. Переписка мошенника с сотрудником банка (январь 2024 г.).

В Даркнете набирают обороты услуги по созданию фейковых видео для криптостримов на платформах популярных социальных сетей и фальшивых розыгрышей криптовалют, в рамках которых мошенники побуждают зрителей переводить криптовалюту.

Главная особенность всех рассмотренных способов заключается в том, что выявить подделку может только специалист с помощью специальных программ. Наше мнение подтверждается результатами исследования В. Б. Батоева и Р. С. Юможапова, в котором они приходят к выводу, что по видеозаписям, созданных с помощью нейронных сетей, и представленных при отсутствии информации об обстоятельствах их получения, возможно проводить экспертное исследование [15; с. 79].

Так, в конце 2023 года СБЕР запатентовал технологию по распознаванию дипфейков, целью которой является повышение точности и эффективности обнаружения синтетического изменения изображений лиц

людей в видео[8]. Основу технологий составляет ряд ансамблей нейросетевых моделей класса EfficientNet (патент № 2768797) и метод амплификации и анализа средствами искусственного интеллектамикроизменений в цветах объектов на кадрах (патент № 2774624). Объединённые в одну систему, они позволяют с высокой точностью определить синтетически изменённые изображения лиц на видео.

Отличительной особенностью системы является возможность обработки видеоконтента с несколькими лицами в кадре. В этом случае система выявляет отдельное лицо, созданное синтетическим образом, и оценивает его достоверность, что позволяет противодействовать ряду методов обхода систем выявления дипфейков.

Кроме того, создана система мониторинга дипфейков «Зефир» — это информационная система выявления дипфейков в аудио и видео.

Разработанные технологии предназначены прежде всего для использования при обеспечении защиты граждан от мошеннических действий.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что программные продукты, направленные на распознавание дипфейков активно разрабатываются, сегодня специалисты фактически выявляют их «вручную».

Для исследования объектов, содержащих признаки дипфейков, целесообразно назначать компьютерную, видеотехническую и фоносокопическую экспертизы. Полагаем, что на разрешение экспертов нужно ставить вопрос: «Имеются ли в представленной записи признаки применения технологии дипфейка?»

При производстве экспертизы можно выявить следующие признаки подделки: муар (волнообразный узор, возникающий из-за наложения одного

[8]Сбер создал одну из лучших в мире технологий распознавания дипфейков // URL:https://www.ferra.ru/news/techlife/sber-sozdal-odnu-iz-luchshikh-v-mire-tekhnologii-raspoznavaniya-dipfeikov-09-02-2023.htm (дата обращения: 29.04.2024).

изображения на другое), излишняя пикселизация, дефекты, нечеткое или смазанное изображение, дрожание или запаздывание речи, неестественное лицо, неестественные движения и мимика человека, отсутствие моргания, нарушения потоков аудиозаписи, различие в освещенности и тенях, мелкие детали, низкое качество видео как попытка скрыть факт использования нейросетей и другие.

Сказанное, позволяет сформулировать перспективные направления, позволяющие эффективно расследовать и предупреждать такие преступления:

1. Необходимость уголовно-правовой регламентации и закрепление дефиниций в законодательстве России с целью единого правоприменения. Несмотря на то, что законопроект активно обсуждается, до настоящего времени все еще существуют правовые коллизии и лакуны в этой сфере.

2. Внедрение системы распознания компьютерного (клавиатурного) почерка стоится на основе интеллектуального анализа времени удержания объектов на экране, то есть того, как именно пользователь набирает текст и с какой скоростью — у каждого человека этот фактор уникален и может меняться в зависимости от психофизиологического состояния. При походке система анализирует положение гаджета в пространстве. За счет применения сверхточных нейронных сетей из динамики походки можно выделить те перемещения в пространстве, которые идентифицируют непосредственно пользователя. (15.03.2024 отечественные ученые представили разработку)[9].

3. Авторизация пользователя по сетчатке глаза. Данный метод в качестве идентификатора использует уникальный рисунок кровеносных сосудов глазного дна. Сканирование происходит с помощью инфракрасного излучения низкой интенсивности, которое направляется через зрачок к

[9]В РФ разработали систему идентификации пользователя по клавиатурному почерку// URL:https://www.m24.ru/news/nauka/15032024/674543?utm_source=CopyBuf(дата обращения: 09.05.2024).

задней стенке глаза. «Центр биометрических технологий» изучает возможность такой идентификации с конца 2023 г.[10]

4. Разработка и внедрение в экспертную деятельность специальных программ, позволяющих автоматизировать выявление дипфейков.

5. Изучение механизма совершения преступления и разработка частной криминалистической методики расследования.

Таким образом, полагаем, что проблема использования технологии дипфейка для совершения преступлений, требует комплексного решения, как на законодательном, так и на технологическом уровнях. При этом дальнейшее исследование механизмов совершения данного вида преступлений будет способствовать обеспечению эффективности предварительного расследования.

Библиографический список:

1. Антонова Е. Ю. Технологии искусственного интеллекта – субъект преступления или орудие / средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 14(1). 31–39.

2. Батоев В. Б. Использование технологии Deepfake в преступной деятельности: проблемы противодействия и пути их решения / В. Б. Батоев, А. В. Пучнин // Вестник Воронежского института МВД России. 2023. № 1. С. 165-169.

3. Ларина Е. С. Криминальная жизнь дипфейков / Е. С. Ларина, В. С. Овчинский // Информационные войны. 2022. № 3(63). С. 69-73.

4. Лемайкина С. В. Актуальные вопросы противодействия использованию технологии дипфейков / С. В. Лемайкина // Юристъ-Правоведъ. 2022. № 3(102). С. 175-178.

[10] ЦБТ изучает возможность идентификации по сетчатке глаза // URL:https://ria.ru/20231109/identifikatsiya-1908290911.html(дата обращения: 07.05.2024).

5. Расторопова О.В. Противодействие использованию искусственного интеллекта в преступных целях // Вестник Университета прокуратуры Российской Федерации. 2021. №4(84). С. 52–58.

6. Бессонов А.А. О некоторых возможностей современной криминалистики в работе с электронными следами // Вестник университета им. О.Е. Кутафина. 2019. № 3. С. 46-52.

7. Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49.

8. Дронова О. Б. Перспектива создания современных технических средств выявления дипфейков // Судебная экспертиза: российский и международный опыт: материалы VI Междунар. науч.-практ. конф. Волгоград, 2022. С. 189–194.

9. Анализ возможностей искусственного интеллекта для расследования мошенничества / Д. С. Клюев, А. Б. Смушкин, Ю. В. Соколова, С. Е. Платонов // Физика волновых процессов и радиотехнические системы. 2023. Т. 26, № 3. С. 116-122.

10. Лужинская, Е. Л. Особенности исследования изображений внешнего облика человека, измененного при помощи программных средств / Е. Л. Лужинская, В. А. Чванкин // Вопросы криминологии, криминалистики и судебной экспертизы. 2022. № 2(52). С. 116-121.

11. Лужинская Е.Л. К вопросу о достоверности информации о внешнем облике человека // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов : Междунар. науч.-практ. конф., Минск, 26 февр. 2021 г.: тез. докл. / Акад. МВД Респ. Беларусь ; редкол.: П.В. Гридюшко (отв. ред.) [и др.]. Минск, 2021. С. 279–280.

12. Желудков М. А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex Russica (Русский закон). 2021. Т. 74, № 4(173). С. 63-70.

13. 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. С. 379-386.

14. Малышкин Р. Н. Мошенничество в информационной среде: использование голосовых фейков / Р. Н. Малышкин // Научные исследования: фундаментальные и прикладные аспекты - 2021 : Сборник научных трудов, Набережные Челны, 01 января – 31 2021 года. Том Выпуск 1. Казань: Издательство "Познание", 2021. С. 330-334.

15. Батоев В. Б., Юможапов Р. С. Использование технологий искусственного интеллекта в выявлении видеодипфейков // Вестник Краснодарского университета МВД России. 2023. № 3(61). С. 76-81.

Bibliograficheskijspisok:

1. Antonova E. YU. Tekhnologii iskusstvennogo intellekta – sub"ekt prestupleniya ili orudie / sredstvo soversheniya prestupleniya? // Yuridicheskij vestnik Kubanskogo gosudarstvennogo universiteta. 2022. № 14(1). 31–39.

2. Batoev V. B. Ispol'zovanie tekhnologii Deepfake v prestupnoj deyatel'nosti: problemy protivodejstviya i puti ikh resheniya / V. B. Batoev, A. V. Puchnin // Vestnik Voronezhskogo instituta MVD Rossii. 2023. № 1. S. 165-169.

3. Larina E. S. Kriminal'naya zhizn' dipfejkov / E. S. Larina, V. S. Ovchinskij // Informacionnye vojny. 2022. № 3(63). S. 69-73.

4. Lemajkina S. V. Aktual'nye voprosy protivodejstviya ispol'zovaniyu tekhnologii dipfejkov / S. V. Lemajkina // Yurist"-Pravoved". 2022. № 3(102). S. 175-178.

5. Rastoropova O.V. Protivodejstvie ispol'zovaniyu iskusstvennogo intellekta v prestupnykh celyakh // Vestnik Universiteta prokuratury Rossijskoj Federacii. 2021. №4(84). S. 52–58.

6. Bessonov A.A. O nekotorykh vozmozhnostej sovremennoj kriminalistiki v rabote s ehlektronnymi sledami // Vestnik universiteta im. O.E. Kutafina. 2019. № 3. S. 46-52.

7. Bakhteev D. V. Iskusstvennyj intellekt v kriminalistike: sostoyanie i perspektivy ispol'zovaniya // Ugolovnyj process i kriminalistika. 2018. № 2. S. 43–49.

8. Dronova O. B. Perspektiva sozdaniya sovremennykh tekhnicheskikh sredstv vyyavleniya dipfejkov // Sudebnaya ehkspertiza: rossijskij i mezhdunarodnyj opyt: materialy VI Mezhdunar. nauch.-prakt. konf. Volgograd, 2022. S. 189–194.

9. Analiz vozmozhnostej iskusstvennogo intellekta dlya rassledovaniya moshennichestva / D. S. Klyuev, A. B. Smushkin, YU. V. Sokolova, S. E. Platonov // Fizika volnovykh processov i radiotekhnicheskie sistemy. 2023. T. 26, № 3. S. 116-122.

10. Luzhinskaya, E. L. Osobennosti issledovaniya izobrazhenij vneshnego oblika cheloveka, izmenennogo pri pomoshchi programmnykh sredstv / E. L. Luzhinskaya, V. A. Chvankin // Voprosy kriminologii, kriminalistiki i sudebnoj ehkspertizy. 2022. № 2(52). S. 116-121.

11. Luzhinskaya E.L. K voprosu o dostovernosti informacii o vneshnem oblike cheloveka // Problemy bor'by s prestupnost'yu i podgotovki kadrov dlya pravookhranitel'nykh organov : Mezhdunar. nauch.-prakt. konf., Minsk, 26 fevr. 2021 g.: tez. dokl. / Akad. MVD Resp. Belarus' ; redkol.: P.V. Gridyushko (otv. red.) [i dr.]. Minsk, 2021. S. 279–280.

12. Zheludkov M. A. Obosnovanie neobkhodimosti adaptacii deyatel'nosti pravookhranitel'nykh organov k usloviyam cifrovoj transformacii prestupnoj sredy // Lex Russica (Russkij zakon). 2021. T. 74, № 4(173). S. 63-70.

13. Ivanov V.G., Ignatovskij YA.R. Deepfakes: perspektivy primeneniya v politike i ugrozy dlya lichnosti i nacional'noj bezopasnosti // Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Gosudarstvennoe i municipal'noe upravlenie. 2020. №4. C. 379-386.

14. Malyshkin R. N. Moshennichestvo v informacionnoj srede: ispol'zovanie golosovykh fejkov / R. N. Malyshkin // Nauchnye issledovaniya: fundamental'nye i prikladnye aspekty - 2021 : Sbornik nauchnykh trudov, Naberezhnye Chelny, 01 yanvarya – 31 2021 goda. Tom Vypusk 1. Kazan': Izdatel'stvo "Poznanie", 2021. S. 330-334.

15. Batoev V. B., Yumozhapov R. S. Ispol'zovanie tekhnologij iskusstvennogo intellekta v vyyavlenii videodipfejkov // Vestnik Krasnodarskogo universiteta MVD Rossii. 2023. № 3(61). S. 76-81.

Klimova Yana Aleksandrovna,
candidate of juridical sciences, assistant professor
professorat the criminalistics department
of the educational and scientific complex for preliminary investigations
in the Internal Affairs Bodies
of the Volgograd Academy of the Ministry of the Interior of Russia,
aya3008@yandex.ru

FORENSIC ANALYSIS OF CRIMES COMMITTED USING DEEPFAKE TECHNOLOGY

KEY WORDS: Deepfake, artificial intelligence, crime investigation, digitalization, investigation techniques, IT technologies, digital forensics, technical and forensic support for investigations, special knowledge.

ANNOTATION. Introduction. Modern forensic science is undergoing a significant transformation as a result of rapid digitalization, which has affected all spheres of society. As a result, artificial intelligence technologies have increasingly become the focus of attention of forensic scientists. At the same time, both their positive aspects are touched upon, for example, the implementation of a predictive function, the use of artificial intelligence in obtaining and analyzing operational

investigative and forensically significant information, as well as the negative ones associated with countering potential threats, since modern technologies help not only to solve crimes, but also commit them. The relevance of the study is due to the need to use the capabilities of digital forensics in the development of forensic recommendations that contribute to the effective and high-quality investigation of high-tech crimes. ***Methods.*** The research was based on the universal dialectical method, general scientific methods of cognition (observation, analysis, synthesis, deduction, etc.) and special methods of scientific research (formal legal, comparative legal, statistical analysis, forensic forecasting method, etc.). The scientific novelty of the research is determined by the range of problems being studied, which are complex in nature for forensic activities. ***Results.*** The author examined the concept and essence of deepfake technology and analyzed statistical data on this category of crimes. The conclusion is drawn about the rapid growth of these crimes in all countries. The identified problem indicates the need to study the mechanism of committing crimes. The lack of judicial investigative practice predetermined the need for a forensic analysis of such offenses. As a result, the author identifies individual methods of committing crimes using deepfake technology. In conclusion, promising directions are formulated to effectively investigate and prevent crimes committed using deepfake technology.

«Представленный материал ранее нигде не публиковался и в настоящее время не находится на рассмотрении на предмет публикации в других изданиях. Заявляем об отсутствии конфликта интересов, связанного с публикацией данной статьи в журнале «Вестник Калининградского филиала Санкт-Петербургского университета МВД России». Разрешаем размещение полнотекстовой версии статьи, а также её частей в открытом доступе в сети Интернет, а также на официальных каналах журнала в социальных сетях. При создании статью и не использовались возможности искусственного интеллекта».

Профессор кафедры криминалистики УНК по ПС в ОВД
Волгоградской академии МВД России

к.ю.н., доцент, полковник полиции  Я.А. Климова