Яна Александровна КЛИМОВА,
кандидат юридических наук, доцент, ORCID 0009-0008-7226-4925
Волгоградская академия МВД России (г. Волгоград)
профессор кафедры криминалистики учебно-научного комплекса
по предварительному следствию в органах внутренних дел
aya3008@yandex.ru

Научная статья
УДК 343.985.7

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ, СОВЕРШЁННЫХ С ИСПОЛЬЗОВАНИЕМ ДИПФЕЙК-ТЕХНОЛОГИИ

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 этого 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 угрозам, 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, криминалистического прогнозирования и др.). Научная новизна исследования определяется кругом изучаемых проблем, носящих в рамках криминалистической деятельности комплексный характер.* ***Результаты.*** *Автором рассмотрены понятие и сущность дипфейк-технологии, проведен анализ статистических данных по соответствующей категории преступлений. Делается вывод о стремительном росте количества преступлений, совершенных с использованием дипфейк-технологии, во всех странах. Выявленная проблема свидетельствует о необходимости изучения механизма совершения таких преступлений. Отсутствие судебно-следственной практики предопределило проведение криминалистического анализа преступлений, совершаемых с использованием дипфейк-технологии. Автором установлены некоторые способы совершения преступлений данного вида. Формулируются предложения по повышению эффективности расследования и предупреждения преступлений, совершенных с использованием дипфейк-технологии.*

ВВЕДЕНИЕ

Активное внедрение информационных технологий в повседневную жизнь способствовало кардинальному изменению архитектуры преступного мира и, в частности, появлению разнообразных высокотехнологичных способов совершения преступлений. С другой стороны, если рассматривать криминалистическую деятельность как процесс и учитывать основные тенденций развития современного научного криминалистического знания, то становится очевидным, что бурная 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 технологий

Yana A.KLIMOVA,
Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0009-0008-7226-4925
Volgograd Academy of the Ministry of Interior of Russia (Volgograd, Russia)
Professor of the Department of Criminalistics of the Educational and Scientific Complex for Preliminary Investigation in the Internal Affairs Bodies
aya3008@yandex.ru

FORENSIC ANALYSIS OF CRIMES COMMITTED USING DEEPFAKE TECHNOLOGY

KEYWORDS. 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 to commit their. 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, etc.). The scientific novelty of the research is determined by the range of problems being studied, which are complex in nature within the framework of forensic activity.* ***Results.*** *The author examined the concept and essence of deepfake technology and analyzed statistical data on the corresponding category of crimes. It is concluded that the number of crimes committed using deepfake technology is rapidly growing in all countries. The identified problem indicates the need to study the mechanism for committing such crimes. The lack of forensic investigative practice predetermined the conduct of a forensic analysis of crimes committed using deepfake technology. The author has established some methods of committing crimes of this type. In conclusion, proposals are formulated to improve the efficiency of investigation and prevention of crimes committed using deepfake technology.*

искусственного интеллекта. По всему миру стремительными темпами растет количество случаев мошенничества, осуществляемого с использованием этих технологий. Образно говоря, планету накрывает эпидемия высокотехнологического обмана, проникающего во все сферы цифрового пространства. В течение последних двух лет особую опасность стало представлять распространение такого вида преступлений, совершаемых с использованием возможностей искусственного интеллекта, как мошенничество с применением технологии «deepfake» (далее – дипфейк).

Об актуальности проблемы свидетельствует внимание к ней на самом высоком государственном уровне. 14 декабря 2023 года в ходе общения Президента России с гражданами и журналистами на прямой линии, проводившейся в рамках проекта «Итоги года с Владимиром Путиным», к нему обратился с вопросом его «цифровой двойник», созданный с использованием дипфейк-технологии. После этого российский лидер подчеркнул, что предотвратить развитие искусственного интеллекта, в том числе сверхинтеллекта, который начинает чувствовать, который различает запахи, у которого появляются когнитивные возможности, который сам себя развивает, невозможно. «А значит, нужно возглавить. Во всяком случае, нужно сделать все, чтобы мы могли быть одними из лидеров в этом направлении», – заявил он[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 способствовал выявлению сходства состояния преступности в России и зарубежных странах; методы анализа и синтеза использовались для изучения позиций ученых по ключевым аспектам темы, нормативных актов, материалов практики. Метод системно-структурного анализа был необходим при исследовании механизма совершения преступлений рассматриваемого вида. Формально-юридический метод позволил выявить различные способы совершения преступления с использованием дипфейк-технологии, а также толковать нормы действующего законодательства. При помощи метода статистического анализа изучались статистические данные, практика правоприменения, выявлялись наиболее актуальные проблемы. Метод криминалистического прогнозирования использовался 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 пробелов в нормативном регулировании дипфейков направлена законодательная инициатива о введении ответственности за несанкцио-

[1] Путин: лидеры в сфере ИИ вряд ли начнут договариваться об ограничениях до появления угроз // Интернет-сайт ТАСС. 14.12.2023 // URL: https://tass.ru/obschestvo/19538893 (дата обращения: 29.04.2024).

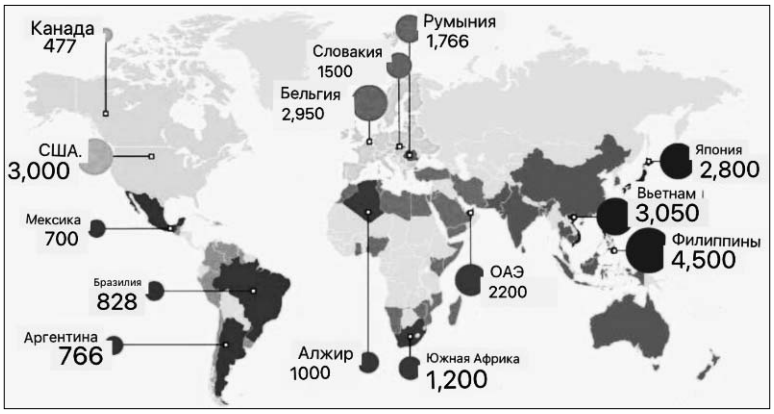

Иллюстрация 1. Стремительный рост показателей совершения мошеннических действий с использованием дипфейк-технологии (данные по странам с наибольшим увеличением числа таких случаев), 2022-2023 гг. (в %).

нированное использование голоса и изображений человека в целях мошенничества[1]. Кроме того, на заседании Правительственной комиссии по профилактике правонарушений, состоявшемся 20 декабря 2023 года, было принято решение о совместной разработке МВД России, Минцифры и Роскомнадзором до ноября 2024 года алгоритма правового регулирования «цифровых портретов» для недопущения их противоправного использования[2].

Исследованию проблем законодательной регламентации дипфейков и противодействия криминальному использованию этой технологии посвящены работы многих ученых: Е.Ю. Антоновой, В.Б. Батоева, А.В. Пучнина, Е.С. Лариной, В.С. Овчинского, С.В. Лемайкиной, О.В. Расстороповой и др. [1-5]. Криминалистические аспекты расследования преступлений рассматриваемого вида и особенности использования искусственного интеллекта в противоправной деятельности изучались 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 интернет-платформы «Statista»[3], в 2022-2023 годах зафиксирован взрывной рост мошенничеств, связанных с использованием дипфейк-технологии (см. иллюстрацию 1), за это время собрана информация о двух миллионах подобных случаев, имевших место в 124 странах. Такие преступления происходят по всему миру вне зависимости от социально-экономического развития и политического режима государств. Так, например, в 2023 году на Филиппинах число случаев мошенничества с использованием дипфейков выросло на 4500% по сравнению с показателем 2022 года, во Вьетнаме рост составил больше 3000%, в Японии – 2800%. Четырехзначными числами выражаются темпы роста количества таких преступлений в США, Объединенных Арабских Эмиратах, ЮАР и многих странах Европы. В отчете «Onfido» (компании, разрабатывающей платформы для безопасной цифровой идентификации личности) на основе результатов анализа мошеннических схем с использованием персональных данных в 2024 году прогнозируется увеличение на 3000% количества цифровых атак[4].

Считаем правильным присоединиться к мнению В.Б. Батоева и А.В. Пучнина, полагающих, что опасность дипфейков 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 их производства. Широко применяется «цифровая ретушь» и «цифровой монтаж» [11, с. 279]. Сегодня существует множество онлайн-сервисов, приложений, ботов, позволяющих создавать дипфейки (например «DeepFaceLab», «Zao», «FaceSwap», «Neuman», «Deepfakesweb» и т.д.). Как только технология стала более доступна, ее стали активно использовать и мошенники.

Здесь целесообразно обратить внимание на точку зрения М.А. Желудкова, согласно которой необходимо видеть общую картину киберпреступности и анализировать способы совершения преступлений с использованием программ искусственного интеллекта [12, с. 68]. В связи с этим требуется более подробное рассмотрение дипфейк-технологии.

Дипфейк (англ. Deepfake, от deeplearning – глубокое обучение и fake – подделка) – технология на базе искусственного интеллекта, позволяющая создавать ложные изображения и видео на основе реальных кадров[5]. Компьютерный алгоритм анализирует большое количество снимков, аудио-, видеозаписей и изучает, как может выглядеть, говорить и двигаться тот или иной конкретный

[1] В Госдуме работают над законопроектом о запрете дипфейков // Интернет-сайт «Право.Ru». 23.01.2024 // URL: https://pravo.ru/news/251111/ (дата обращения: 09.05.2024).
[2] Владимир Колокольцев провел заседание Правительственной комиссии по профилактике правонарушений // Интернет-сайт «МВД Медиа». 20.12.2023 // URL: https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedfanie-pravitelstvennoy-komissii-po-profilaktike-pravonarusheniy/ (дата обращения: 06.05.2024).
[3] «Statista» – международная глобальная информационная интернет-платформа с обширной базой статистических данных, отчетов и аналитических сведений // URL: https://www.statista.com/aboutus/ (дата обращения: 02.05.2024).
[4] Отчет о мошенничестве с личными данными, 2024 г. // Интернет-сайт «Onfido» // URL: https://onfido.com/landing/identity-fraud-report/ (дата обращения: 07.05.2024).
[5] Дипфейк // Официальный сайт Большой российской энциклопедии // URL: http://bigenc.ru/c/dipfeik-f9f89b (дата обращения: 03.05.2024).

Иллюстрация 2.
Примеры изображений, сгенерированных нейросетями.

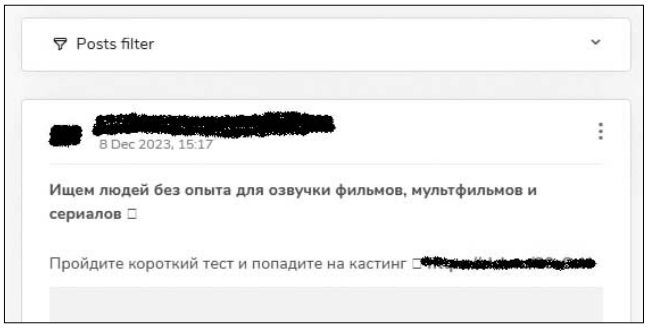

Иллюстрация 3.
Объявление в мессенджере.

Иллюстрация 4.
Пример дипфейка, с помощью которого мошенники вымогают деньги в «Telegram» (видео – по QR-коду).

человек. Нейросеть собирает из Интернета, в том числе из открытых источников в социальных сетях, файлы, содержащие изображения человека (в разных ракурсах, с разными выражениями лица), записи его голоса, обрабатывает их и создает на этой основе новое изображение, новую аудиозапись или новый видеоролик. Дипфейки выглядят гиперреалистично, поскольку инструменты искусственного интеллекта были обучены на десятках тысяч изображений реальных людей (см. иллюстрацию 2).

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]. Мошенники с целью получения образцов голоса стали размещать в Интернете объявления с предложением принять участие в оплачиваемой озвучке рекламы и фильмов (см. иллюстрацию 3). Их целью в данном случае является сбор материала для обучения нейросетей и последующей генерации аудиосообщений, предназначенных для вымогательства денег от имени человека, образцы голоса которого были использованы при создании дипфейка, у его родственников и друзей.

Таким образом, можно констатировать, что 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 подобного рода преступлений.

В настоящее время широкое распространение получила схема «FakeBoss» (ложный начальник), предполагающая направление распоряжения якобы от лица руководителя. Жертве мошенничества поступает текстовое или голосовое сообщение, сгенерированное при помощи дипфейк-технологии, в котором под предлогом возникновения форс-мажорных обстоятельств предлагается срочно перевести деньги на «безопасный счет».

Другим способом мошенничества является использование образа узнаваемой популярной личности. Так, в конце ноября 2023 года в сети появилось видео, в котором известный комик и киноактер Нурлан Сабуров рекламирует приложение онлайн-казино. На самом деле это дипфейк – так мошенники завлекают пользователей на фишинговый сайт[1]. Ключевая идея всех дипфейков заключается в достижении максимальной реалистичности и правдоподобности, и уже сегодня можно наблюдать лавинообразный рост объемов модифицированного интернет-контента, созданного с целью манипуляции сознанием и поведением человека.

Обратим внимание еще на один новый вид мошенничества – хищение средств с использованием технологии «Voicedeepfake», основанной на обработке голоса для создания ложных звуковых сообщений. Суть данного способа точно сформулировал Р.Н. Малышкин: хищение с помощью голосовых клонов [14, с. 332]. Преступники посредством возможностей нейросети генерируют голосовые обращения якобы от имени владельца того или иного аккаунта и вымогают деньги у тех, с кем тот поддерживает связи, для убедительности прикрепляя фотографию банковской карты с именем и фамилией. На первом этапе они взламывают аккаунты в мессенджерах, например «Telegram» или «WhatsApp», с помощью фейковых голосований. Затем скачивают сохраненные голосовые сообще-

[1] Фейковая реклама казино от имени стендап-комика Нурлана Сабурова распространяется в Сети // Интернет-сайт «StopFake». 07.06.2024 // URL: https://stopfake.kz/ru/archives/21066 (дата обращения: 30.04.2024).

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

ния и создают на их основе новые – с нужным им содержанием, например с просьбой об одолжении большой суммы денег. Такие сгенерированные сообщения рассылают в личные и групповые чаты, к ним, как правило, прикрепляются изображения банковских карт с поддельными именами получателей (см. иллюстрацию 4).

Другим распространенным и при этом легким дипфейк-способом хищения денег является использование реального голоса жертвы, записанного, например, посредством спам-звонка. Задача мошенников состоит в том, чтобы добиться произнесения ключевых слов, на основе которых генерируется типовая звуковая дорожка для «общения» с роботом службы поддержки банка. Грамотно синтезированная из фрагментов речи жертвы запись позволяет «достоверно» ответить на все вопросы робота и добиться осуществления перевода средств на счета, к которым у преступников имеется доступ.

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

В теневом сегменте Интернета – даркнете набирают популярность услуги по созданию фейковых видео для криптостримов на платформах популярных социальных сетей и фальшивых розыгрышей криптовалют, в рамках которых мошенники побуждают зрителей переводить им деньги.

Главная особенность всех описанных выше способов мошенничества заключается в том, что выявить подделку может только специалист с помощью специализированного программного обеспечения. Так, например, В.Б. Батоев и Р.С. Юможапов приходят к выводу о том, что по видеозаписям, созданным с помощью нейронных сетей и представленным при отсутствии информации об обстоятельствах их получения, возможно проводить экспертное исследование [15, с. 79].

В конце 2023 года «Сбер» запатентовал технологию распознавания дипфейков, предназначенную для повышения точности и эффективности обнаружения синтетического изменения изображений лиц людей в видео[1]. Основу технологии составляет ряд ансамблей нейросетевых моделей класса «EfficientNet» (патент № 2768797) и метод амплификации и анализа средствами искусственного интеллекта микроизменений в цветах объектов на кадрах (патент № 2774624). Все это, объединенное в одной системе, позволяет с высокой точностью определить наличие на видео синтетически измененных изображений лиц. Отличительной особенностью системы является возможность обработки видеоконтента с несколькими лицами в кадре. В этом случае анализу на достоверность подвергается отдельно изображение каждого лица, созданное синтетическим образом.

Отметим также потенциал эффективности еще одной системы мониторинга дипфейков – «Зефир», которая предназначена для выявления сгенерированных нейросетями элементов аудио- и видеозаписей. Эта и подобные ей технологии предназначены прежде всего для использования в целях обеспечения защиты граждан от мошеннических действий.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что появляются программные продукты, ориентированные на распознавание дипфейков, сегодня специалисты все еще фактически выявляют их «вручную». Для исследования объектов, содержащих признаки дипфейков, целесообразно назначать компьютерную, видеотехническую и фоносокопическую экспертизы. Полагаем, что на разрешение экспертов необходимо 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 изображения на другое), излишняя пикселизация, дефекты, нечеткое или смазанное изображение, дрожание или запаздывание речи, неестественное лицо, неестественные движения и

[1] Сбер создал одну из лучших в мире технологий распознавания дипфейков // Интернет-сайт «Ferra.ru». 09.02.2023 // 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).

мимика человека, отсутствие моргания, нарушения потоков аудиозаписи, различие в освещенности и тенях, нарушение детализации, понижение качества видео как попытка скрыть факт использования дипфейка и др.

Результаты проведенного исследования позволяют сформулировать ряд предложений, реализация которых, по нашему мнению, будет способствовать повышению эффективности расследования и предупреждения преступлений рассматриваемого вида:

1. Необходимы уголовно-правовая регламентация дипфейка и закрепление дефиниции в законодательстве России с целью выработки единообразия правоприменения. Соответствующий законопроект активно обсуждается, но, судя по всему, до его принятия еще далеко, хотя очевидно, что существуют правовые коллизии и пробелы в данной сфере.

2. Видится актуальным внедрение системы распознания компьютерного (клавиатурного) почерка на основе интеллектуального анализа времени удержания объектов на экране, то есть того, как именно пользователь набирает текст и с какой скоростью. У каждого человека эти параметры уникальны, что и позволяет идентифицировать пользователя[1].

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 задней стенке глаза. «Центр биометрических технологий» изучает возможность такой идентификации с конца 2023 года[2].

4. Перспективной представляется разработка специальных программ, позволяющих автоматизировать выявление дипфейков. Такие программы необходимо внедрять в экспертную деятельность.

5. Требует глубокого изучения механизм совершения преступлений рассматриваемого нами вида, на основе полученных результатов возможна разработка частной криминалистической методики их расследования.

Таким образом, полагаем, что к решению проблем, связанных с использованием дипфейк-технологии для совершения преступлений, необходим комплексный подход – как на законодательном, так и на технологическом уровне. Дальнейшее исследование механизмов совершения преступлений данного вида будет способствовать обеспечению эффективности их 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). С. 31-39.

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

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

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

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 возможностях современной криминалистики в работе с электронными следами // Вестник университета имени 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 Международной научно-практической конференции. Волгоград, 2022. С. 189-194.

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

10. Лужинская Е.Л., В.А. Чванкин Особенности исследования изображений внешнего облика человека, измененного при помощи программных средств // 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: Международная научно-практическая конференция. 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.

[1] В РФ разработали систему идентификации пользователя по клавиатурному почерку // Интернет-сайт «Москва 24». 15.03.2024 // URL: https://www.m24.ru/news/nauka/15032024/674543?utm_source=CopyBuf (дата обращения: 09.05.2024).

[2] ЦБТ изучает возможность идентификации по сетчатке глаза // Интернет-сайт РИА «Новости». 09.11.2023 // URL: https://ria.ru/20231109/identifikatsiya-1908290911.html (дата обращения: 07.05.2024).

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 // Научные исследования: фундаментальные и прикладные аспекты – 2021: Сборник научных трудов. Вып. 1. Казань: 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.

REFERENCES

1. Antonova Ye.Yu. Tekhnologii iskusstvennogo intellekta – sub"yekt prestupleniya ili orudiye / sredstvo soversheniya prestupleniya? // Yuridicheskiy vestnik Kubanskogo gosudarstvennogo universiteta. 2022. № 14 (1). S. 31-39.

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

3. Larina Ye.S., Ovchinskiy V.S. Kriminal'naya zhizn' dipfeykov // Informatsionnyye voyny. 2022. № 3 (63). S. 69-73.

4. Lemaykina S.V. Aktual'nyye voprosy protivodeystviya ispol'zovaniyu tekhnologii dipfeykov // Yurist"-Pravoved". 2022. № 3 (102). S. 175-178.

5. Rastoropova O.V. Protivodeystviye ispol'zovaniyu iskusstvennogo intellekta v prestupnykh tselyakh // Vestnik Universiteta prokuratury Rossiyskoy Federatsii. 2021. № 4 (84). S. 52-58.

6. Bessonov A.A. O nekotorykh vozmozhnostyakh sovremennoy kriminalistiki v rabote s elektronnymi sledami // Vestnik universiteta imeni O.Ye. Kutafina. 2019. № 3. S. 46-52.

7. Bakhteyev D.V. Iskusstvennyy intellekt v kriminalistike: sostoyaniye i perspektivy ispol'zovaniya // Ugolovnyy protsess i kriminalistika. 2018. № 2. S. 43-49.

8. Dronova O.B. Perspektiva sozdaniya sovremennykh tekhnicheskikh sredstv vyyavleniya dipfeykov // Sudebnaya ekspertiza: rossiyskiy i mezhdunarodnyy opyt. Materialy VI Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Volgograd, 2022. S. 189-194.

9. Klyuyev D.S., Smushkin A.B., Sokolova Yu.V., Platonov S.Ye. Analiz vozmozhnostey iskusstvennogo intellekta dlya rassledovaniya moshennichestva // Fizika volnovykh protsessov i radiotekhnicheskiye sistemy. 2023. T. 26. № 3. S. 116-122.

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

11. Luzhinskaya Ye.L. K voprosu o dostovernosti informatsii o vneshnem oblike cheloveka // Problemy bor'by s prestupnost'yu i podgotovki kadrov dlya pravookhranitel'nykh organov: Mezhdunarodnaya nauchno-prakticheskaya konferentsiya. Minsk, 2021. S. 279-280.

12. Zheludkov M.A. Obosnovaniye neobkhodimosti adaptatsii deyatel'nosti pravookhranitel'nykh organov k usloviyam tsifrovoy transformatsii prestupnoy sredy // Lex Russica (Russkiy zakon). 2021. T. 74. № 4 (173). S. 63-70.

13. Ivanov V.G., Ignatovskiy YA.R. Deepfakes: perspektivy primeneniya v politike i ugrozy dlya lichnosti i natsional'noy bezopasnosti // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Gosudarstvennoye i munitsipal'noye upravleniye. 2020. № 4. C. 379-386.

14. Malyshkin R.N. Moshennichestvo v informatsionnoy srede: ispol'zovaniye golosovykh feykov // Nauchnyye issledovaniya: fundamental'nyye i prikladnyye aspekty – 2021: Sbornik nauchnykh trudov. Vyp. 1. Kazan': Poznaniye, 2021. S. 330-334.

15. Batoyev V.B., Yumozhapov R.S. Ispol'zovaniye tekhnologiy iskusstvennogo intellekta v vyyavlenii videodipfeykov // Vestnik Krasnodarskogo universiteta MVD Rossii. 2023. № 3 (61). S. 76-81.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Климова Я.А. Криминалистический анализ преступлений, совершённых с использованием дипфейк-технологии // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 2 (76). С. 29-35.