ISSN 2949-1150 (online)
2071-8284 (print)

Научная статья
УДК 343.85
https://doi.org/10.35750/2071-8284-2025-2-159-169

Обеспечение защищенности биометрических персональных данных от использования в криминальных целях

Михаил Александрович Желудков[1, 2], доктор юридических наук, доцент
Анна Павловна Алексеева[3], доктор юридических наук, профессор

[1] Юридический институт Тамбовского государственного технического университета
Тамбов (392000, ул. Советская, д. 106/5), Российская Федерация
[2] Юго-Западный государственный университет
Курск (305040, ул. 50 лет Октября, д. 94), Российская Федерация
[3] Калининградский филиал Санкт-Петербургского университета МВД России
Калининград (236006, ул. Генерала Галицкого, д. 30), Российская Федерация

[1] kandydat1@yandex.ru, [3] alexeeva.klg-mvd@yandex.ru
[1] https://orcid.org/0000-0003-4482-125X, [3] https://orcid.org/0000-0002-4569-7564

Аннотация:
Введение. *Проблема создания с помощью нейросети и технологии «Дипфейк» поддельных образов человека на основе незаконно полученных достоверных биометрических персональных данных для последующего совершения с их помощью преступления остается в настоящее время нерешенной. В эпоху всеобщей цифровизации обеспечение безопасности персональных данных, включая биометрические, часто зависит не столько от самой потенциальной жертвы, чьи данные могут быть незаконно использованы, сколько от третьих лиц, которые их собирают и хранят, что способствует созданию криминальных ситуаций. При разработке современных программ предупреждения преступности, внедрении новых правил использования цифровых устройств и программного обеспечения необходимо учитывать, что последние достижения науки и техники значительно изменили формы общения людей, перевели многие процессы и документооборот в виртуальное пространство, в то время как пути обеспечения безопасности биометрических персональных данных, которые могут быть подделаны и использованы для последующего совершения преступлений, в современной практике проработаны недостаточно.*
Методы. *При написании статьи были использованы различные методы познания: диалектический, статистический, метод анализа, изучения документальных фактов. Материалом исследования послужили нормативные правовые акты, статистические сведения, а также научные работы авторов, изучающих проблемы использования поддельных биометрических персональных данных при создании аудиозаписей и видеоизображений в целях последующего совершения преступлений.*
Результаты. *В ходе исследования были выявлены проблемы нормативного, организационного и другого характера в сфере контроля за сбором, обработкой и хранением биометрических персональных данных, а также доступа к ним при генерации поддельных аудиозаписей и видеоизображений. Предложено дополнить Уголовный кодекс Российской Федерации новой нормой, предусматривающей уголовную ответственность за создание и распространение заведомо поддельных аудиозаписей и видеоизображений, созданных с применением нейросети и технологии «Дипфейк» на основе полученных незаконным путем биометрических персональных данных.*

Ключевые слова:
биометрические персональные данные, незаконный доступ, нейронная сеть, Дипфейк, спуфинг, видеоизображение человека, аудиозапись голоса

Для цитирования:
Желудков М. А., Алексеева А. П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. 2025. № 2 (106). С. 159–169. https://doi.org/10.35750/2071-8284-2025-2-159-169.

Статья поступила в редакцию 23.02.2025;
одобрена после рецензирования 09.04.2025;
принята к публикации 20.06.2025.

Original article

Ensuring the security of biometric personal data against the use for criminal purposes

Mikhail A. Zheludkov[1, 2], Doc. Sci. (Jurid.), Docent
Anna P. Alekseeva[3], Doc. Sci. (Jurid.), Professor

[1] Law Institute of Tambov State Technical University
106/5 Sovetskaya str., Tambov, 392000, Russian Federation
[2] Southwest State University
94, 50 let Oktyabrya str., Kursk, 305040, Russian Federation
[3] Kaliningrad Branch of the Saint Petersburg University of the MIA of Russia
30, Generala Galitskogo str., Kaliningrad, 236006, Russian Federation
[1] kandydat1@yandex.ru, [3] alexeeva.klg-mvd@yandex.ru
[1] https://orcid.org/0000-0003-4482-125X, [3] https://orcid.org/0000-0002-4569-7564

Abstract:
Introduction. *Creating synthetic human images by neural networks and Deepfake technology, based on illicitly obtained authentic biometric personal data for the subsequent commission of an offence using them, remains a significant and unresolved problem. In the age of digital transformation, the security of personal data, particularly biometric data, often depends not so much on the potential victim, whose data may be unlawfully misappropriated, but on third parties that collect and keep it, thereby inadvertently facilitating the emergence of criminal scenarios.*
In the development of contemporary crime prevention programmes and the introduction of new regulations pertaining to the use of digital devices and software, it is necessary to acknowledge the profound impact of scientific and technological advancements on the evolution of human communication. These advancements have pushed many processes and document flow into the virtual space. Concurrently, the methods to ensure the security of biometric personal data, which can be falsified and used for the subsequent commission of offences, are not sufficiently developed in contemporary practice.
Methods. *In writing article, various methods of cognition were used: dialectical, statistical, analytical method and documentary analysis techniques. The material of the study encompasses normative legal acts, statistical data, as well as scientific publications of authors examining the issues of using of fake biometric personal data in the creation of audio and video recordings for the subsequent commission of crimes.*
Results. *The study revealed regulatory, organisational and other problems in controlling the collection, processing and storage of biometric personal data, as well as access to them during the creation of fake audio and video recordings. It is suggested that the Criminal Code of the Russian Federation be amended with a new provision stipulating criminal liability for the creation and distribution of fake audio and video recordings created by neural networks and Deepfake technology based on illicitly obtained biometric personal data.*

Keywords:
biometric personal data; illegal access; neural networks; Deepfake; spoofing; human video recording; audio recording

For citation:
Zheludkov M. A., Alekseeva A. P. Ensuring the security of biometric personal data against the use for criminal purposes // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 2 (106). P. 159–169.https://doi.org/10.35750/2071-8284-2025-2-159-169.

**The article was submitted February 23, 2025;
pproved after reviewing April 9, 2025;
accepted for publication June 20, 2025.**

Введение

Обеспечение защиты биометрических персональных данных с учетом возможности их незаконного использования в ходе генерации поддельных аудиозаписей и видеоизображений для совершения преступлений является актуальной задачей государства. В разные периоды технологические и экономические преобразования в стране влияли на показатели преступности, основанной на применении информационно-телекоммуникационных технологий. Так, если в 2020 году таких деяний было зарегистрировано 510 396, то в 2021 – 517 722 (+ 1,4 %), в 2022 – 522 065 (+ 0,8 %), в 2023 – 676 951 (+ 29,7 %), в 2024 – 765 365 (+ 13,1 %)[1]. Это неудивительно, поскольку, анализируя причины и условия преступности, ученые и практики неизбежно приходят к выводу о сочетании внешних и внутренних факторов, воздействующих на личность преступника, формирующих ее структуру и механизм преступного поведения. Согласимся с тем, что «изучение преступности и ее причин, а также организация противодействия ей в первую

[1] Статистика и аналитика // Министерство внутренних дел Российской Федерации : [официальный сайт]. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 09.01.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

очередь определяются пониманием той опасности, которую она представляет на данном этапе развития общества. Это понимание требует устранения негативных явлений, порождающих тот или иной вид преступности, и разработки соответствующих профилактических мер для решения этой проблемы»[2]. Придерживаясь такого криминологического подхода к разработке специальных профилактических мер, мы должны не только изучать количественные и качественные характеристики преступности, но и с учетом выявленных тенденций ее изменения, закономерностей существования и прогнозов развития своевременно корректировать систему мер безопасности, способную защитить граждан от потенциальных опасностей, постоянно повышая ее эффективность. Это в свою очередь невозможно сделать, если не учитывать стремительно развивающиеся технологии, которые, с одной стороны, призваны облегчить труд человека, но с другой – представляют потенциальную угрозу в случае их применения в криминальных целях [1, с. 69]. В противном случае можно недооценить способности преступников и переоценить возможности правоохранительных органов по борьбе с преступностью. Нужно понимать, что преступники, использующие неправомерно полученные персональные данные в криминальных целях, разрабатывают все новые способы совершения преступлений. Правоохранительные органы всегда отстают в этом направлении, реагируя лишь на новые появившиеся угрозы. Безусловно, в последнее время наметился некоторый прогресс в области защиты персональных данных, но современные технологии, такие как «Дипфейк», открывают все новые возможности для обмана граждан, позволяя генерировать аудиозаписи и видеоизображения, которые очень сложно отличить от реальных.

Слово «Дипфейк» было заимствовано из английского языка, оно объединило в себе значение двух слов: «глубинное обучение» (англ. *deep learning*) и «подделка» (англ. *fake*)[3]. Изначально данная технология позволяла вносить изменения в подлинные фотографии, записанные видеоизображения и голосовые треки, искажая после обработки их содержание и смысл. Разработчики придумали это ради развлечения, шутки. Однако с развитием генеративно-состязательных нейросетей (GAN) появилась возможность вносить сознательные изменения не только в материалы, ранее записанные на электронные носители, но и генерировать новые цифровые образы конкретных людей, которые стали подменять реальность, имитируя их поведение, разговоры, манеры общения, жесты и т. д. Технологии «Дипфейк» позволяют создавать поддельные фотографии, аудиозаписи и видеоизображения с участием людей, к чьим биометрическим персональным данным был получен доступ, причем генерируемые таким способом материалы являются лишь реализацией выдуманного сценария, тогда как в реальности воспроизводимые события могли никогда не происходить. Технологии «Дипфейк» базируются на методике компьютерного синтеза, которая использует искусственный интеллект для переноса с высокой степенью достоверности черт лица, голоса одного человека на подставное изображение или голосовой файл [2, с. 113]. Таким образом сегодня технология «Дипфейк» перешла из развлекательной и технической сферы в область, представляющую серьезную угрозу для личности, общества и государства. Она представляет собой процесс создания поддельного образа человека, сгенерированного на основе имеющейся о нем информации, которую нейросеть может собирать из социальных сетей, различных открытых ресурсов, куда пользователи часто сами размещают свои изображения, видеозаписи, описания вариантов своей трудовой занятости и свободного времяпрепровождения.

Появившаяся новинка по вполне понятным причинам всерьез заинтересовала криминальные структуры, которые начали использовать технологию «Дипфейк» в преступных целях. Сгенерированные таким способом поддельные образы реально существующих людей преступники стали использовать для атаки на конкретную жертву, а само явление получило название «спуфинг» (англ. *spoofing* – подделка). В отличие от технологии «Дипфейк» «спуфинг» – это собирательный термин, используемый для обозначения кибератак, при которых преступник выдает себя за доверенное лицо или организацию, чтобы получить выгоду или причинить вред пользователю. Основные элементы, задействуемые во время спуфинг-атаки, – это подменный адрес электронной почты, сайт или другие фальшивые ресурсы. Для спуфинг-атаки также необходим сценарий, основанный на принципах социальной инженерии, который побуждает жертву к нужным преступнику действиям. Успешная спуфинг-атака может привести к серьезным негативным последствиям: к распространению вредоносного программного обеспечения; к получению

[2] Серебрякова В. А., Зырянов В. Н. Корыстные преступления, совершаемые женщинами : методическое пособие. Москва : ВНИИ проблем укрепления законности и правопорядка. 1990. С. 24.

[3] Brandon J. Terrifying high-tech porn: Creepy «deepfake» videos are on the rise (February 16, 2018) // Fox News : [сайт]. URL: https://web.archive.org/web/20180615160819/http://www.foxnews.com/tech/2018/02/16/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-rise.html (дата обращения: 09.01.2025).

неправомерного доступа к личной или корпоративной информации; к взлому аккаунтов и неправомерному завладению учетными данными для дальнейших атак; к получению несанкционированного доступа к сети, а также расширенных прав такого доступа. Для организаций это может закончиться сбоем в доступе к компьютерной информации, обусловленным шифрованием файлов или другими причинами, с последующим шантажом, требованием выкупа, а в случае отказа – потерей данных, которая причинит серьезный материальный вред.

В настоящее время пока нет механизмов, позволяющих не просто отслеживать случаи применения информационно-телекоммуникационных технологий для совершения преступлений, а иметь достоверную информацию об использовании технологий «Дипфейк» в криминальных целях. Это было бы возможно в случае внесения изменений в документы статистического учета преступлений, которые бы позволили видеть все подобные эпизоды в отчетности. Тем не менее специально организованные наблюдения позволили экспертам отобрать некоторые сведения, характеризующие современную ситуацию в этой сфере. Так, на заседании Общественного совета при МВД России в 2024 году была представлена информация, из которой следует, что «удельный вес киберпреступлений в общем массиве за год составил около 40 % от всех зарегистрированных посягательств, причем практически в каждом втором преступлении фигурировали какие-либо электронные средства или устройства, а по тяжким и особо тяжким составам этот показатель приблизился к 60 %. С начала 2024 года общая сумма ущерба по данной категории дел превысила 116 миллиардов рублей. Способы совершения преступлений стали более изощренными, активно использовалась технология «Дипфейк». Особенно часто это происходило при совершении мошенничеств, когда преступники действовали от имени руководителей различных ведомств, в том числе МВД России, генерируя с помощью нейросетей их изображения и голоса»[4]. Из этого можно сделать вывод о стремительном развитии технологии «Дипфейк», с помощью которой создается заведомо поддельный контент, применяемый к потенциальным жертвам. По мнению экспертов, в 2024 году в интернет-пространстве было выявлено более 12 миллионов сообщений с ложной информацией, распространяемой под видом достоверной, которые набрали несколько миллиардов просмотров[5]. Потенциальная жертва может долгое время даже не осознавать, что имеет дело с обманом. Такая отсрочка обращения в правоохранительные органы позволяет преступникам скрыть следы преступления, значительно затрудняет быстрое выявление этих преступлений, их пресечение, а также полное, всестороннее и объективное расследование.

Особенно актуальна описанная ситуация для дистанционных хищений, число которых значительно выросло в последние годы. Так, если в 2020 году в России доля мошенничеств в общей структуре преступности составляла 16,4 %, то в 2024 году она выросла до 23,3 %[6]. По мнению многих экспертов, такой значительный рост обусловлен именно применением методов социальной инженерии в совокупности с технологиями, позволяющими подменять аудиовизуальное восприятие происходящих событий.

Со стороны органов государственной власти сегодня предпринимаются значительные усилия, направленные на защиту потенциальных жертв от возможных мошеннических действий. Так, в соответствии с достигнутыми договоренностями банки стали добровольно возмещать материальный ущерб, причиненный их клиентам в результате совершенного хищения. Однако это правило действует только в том случае, если хищение произошло без непосредственного участия жертвы: пострадавший не сообщал сведения о банковской карте, не передавал коды из СМС, логин или пароль, не предоставлял преступникам доступ к своим средствам. Как показывает практика, таких случаев в общей массе хищений насчитывается сравнительно немного. В основном жертвы, будучи обманутыми, добровольно переводят свои сбережения злоумышленникам, либо способствуют этому, что исключает применение механизма банковских компенсаций[7].

Осенью 2024 года группа компаний Б1 совместно с *MTS AI* провели опрос представителей бизнеса из различных отраслей, чтобы оценить угрозы, исходящие от использования технологии «Дипфейк» и других подобных разработок. При этом более 60 % респондентов были руководителями высшего и среднего звена, остальные представляли компании со штатом более 1 000 человек. В ходе исследования 21 % респондентов сообщили, что уже сталкивались с технологиями «Дип-

[4] Серков Д. Колокольцев заявил об ущербе в более 100 млрд от киберпреступлений // РБК : сетевое издание : [сайт]. URL: https://www.rbc.ru/politics/25/09/2024/66f3cda19a79477a70eff34f?from=from_main_6 (дата обращения: 09.01.2025).

[5] Терещенко М. Эксперт сообщил, что в сети выявили 12 млн копий фейков // ТАСС : [сайт]. URL: https://tass.ru/obschestvo/21868693 (дата обращения: 09.01.2025).

[6] URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 09.01.2025).

[7] Ильина Н. Банки отбили более 20 млн попыток похитить деньги клиентов // Известия : [сайт]. URL: https://iz.ru/1642179/natalia-ilina/banki-otbili-bolee-20-mln-popytok-pokhitit-dengi-klientov (дата обращения: 09.01.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

фейк», но ущерб от их использования был незначительным. При этом 92 % респондентов выразили уверенность в том, что целенаправленные спуфинг-атаки представляют реальную угрозу для бизнеса и граждан. Только 3 % респондентов выразили полную уверенность в собственной защищенности и защищенности своей компании от угроз, связанных с применением технологий, работающих на основе искусственного интеллекта, и спуфинг-атаками. Остальные опрошенные в той или иной степени обозначили обеспокоенность существованием потенциальных угроз. Результаты исследования показывают, что технологии «Дипфейк» становятся серьезной угрозой как для бизнеса, так и для всех россиян. Отечественные компании оказались пока не готовы эффективно защищаться от нее, хотя все понимают, что количество спуфинг-атак будет только увеличиваться[8]. Все это наглядно демонстрирует актуальность существующей проблемы, которая требует комплексного подхода с использованием правовых, технологических механизмов, а также других форм регулирования.

Цель исследования – показать специфику неправомерного использования биометрических персональных данных для генерации поддельных аудиозаписей и видеоизображений в целях последующего совершения с их помощью преступлений и, как следствие, целесообразность усовершенствования уголовного законодательства для достижения его адекватности современному состоянию киберпреступности, усиления его ориентированности на борьбу с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий.

Задачи исследования: проанализировать способы применения технологии «Дипфейк» для совершения преступлений; сформулировать системные решения, направленные на защиту биометрических персональных данных от преступных посягательств.

Методы

При написании статьи были использованы различные методы исследования: диалектический – для познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними; статистический – для извлечения полезной информации из собранных сведений о киберпреступности, выявления закономерностей и зависимостей; метод анализа – для изучения признаков и свойств процесса применения нейросети и технологии «Дипфейк» в криминальных целях; документального изучения фактов – обобщения судебной практики рассмотрения уголовных дел о преступлениях, основанных на спуфинг-атаках. Материалом исследования послужили нормативные правовые акты, статистические сведения, а также научные работы авторов, изучающих проблемы использования поддельных биометрических персональных данных при генерации аудиозаписей и видеоизображений в целях последующего совершения преступлений.

Результаты

Сегодня каждый человек стал частью цифрового мира: в повседневной жизни он сталкивается с тем, что его регулярно фотографируют, снимают на видео, записывают его голос. Прогрессивные технологии часто служат на благо общества, например, когда позволяют реализовать алгоритмы распознавания лиц, которые могут помочь не только в раскрытии преступлений, но и в их своевременном предотвращении, пресечении. Вместе с тем социальные сети переполнены изображениями, размещенными самими гражданами, которые не всегда задумываются о том, кто и как может воспользоваться этими данными в деструктивных целях, реализуемых с помощью технологии «Дипфейк».

Криминальное использование цифровых технологий, нарушающее безопасность людей, может не только ограничить их дальнейшее развитие, но и создать в обществе атмосферу страха, снижая уровень защищенности персональных данных, формируя недоверие ко всем телефонным звонкам, фото- и видеоконтенту в интернете. Ситуация осложняется тем, что «на человеческий голос не распространяется право собственности. В России использование чужой речи для создания похожего голоса прямо не запрещено законодательством. Имитация голоса, например, телефонными пранкерами, также не является нарушением и зависит скорее от содержания сказанного, которое может повлечь за собой уголовную ответственность» [2, с. 116].

Развитие технологии «Дипфейк» привело к тому, что даже профессиональные программы не всегда могут отличить поддельное видео от подлинного. Так, «в период с 3 марта по 12 июня

[8] Спуфинг и дипфейки: бизнес под прицелом : Исследование MTS AI и Группы компаний Б1 // Б1 – Консалт : [сайт]. URL: https://b1.ru/analytics/b1-mts-ai-deepfake-and-spoofing-threats-for-business-survey-2025/ (дата обращения: 27.01.2025).

2020 года компании «Майкрософт», «Фейсбук» и «Амазон» провели конкурс *Deepfake Detection Challenge* (DFDC) для демонстрации возможностей генерации поддельных видео, созданных с помощью голосовых или лицевых манипуляций, и их идентификации. В конкурсе приняли участие 2 114 экспертов, которые представили более 35 000 моделей для определения подделок. В результате были объявлены победители, однако выяснилось, что многие сгенерированные видео так и не удалось идентифицировать как поддельные»9.

Мы изучили экспертные мнения и научные разработки в этой области и пришли к обоснованному выводу о том, что технологии «Дипфейк» постоянно совершенствуются. Алгоритм подмены истинных данных на ложные постоянно улучшается, и существует риск, что в будущем новая версия такой технологии сможет в случае необходимости по заказу разработчика полностью скорректировать «нужным» образом все аудиозаписи и видеоизображения, размещенные в интернете. И здесь возникает угроза массовой манипуляции сознанием людей с помощью поддельных изображений, видеозаписей или голосов реальных людей, которая требует незамедлительного реагирования путем решения массы юридических, управленческих и моральных вопросов [3, с. 267; 4, с. 381]. В научной литературе в связи с этим высказываются мнения об опасности технологии «Дипфейк» для интересов государства в целом [5].

Итак, новая технология основана на современных алгоритмах искусственного интеллекта, таких как сеть кодер-декодер (*Encoder-Decoder*); конволюционная нейронная сеть (*Convolutional neural network*); генеративная состязательная сеть (*Generative adversarial network*); архитектура *Pix2Pix*; циклическая генеративная состязательная сеть (*CycleGAN*); рекуррентная нейронная сеть (*Recurrent neural network*) [6, с. 22]. Если раньше для того, чтобы скопировать голос человека, требовалось 20 минут записанной речи, то сегодня появилась методика, которая позволяет изменить речь, используя всего несколько произнесенных им слов. «Все более совершенный алгоритм GANS способен полностью автоматизировать процесс синтеза и подделки изображений, аудио и видео. Индивидуальные особенности голоса, мимики, движений тела и другие биологические маркеры, поведенческие черты могут быть успешно перенесены, создавая иллюзию подлинности», – утверждают специалисты [7, с. 119].

Преступления, связанные с незаконным использованием биометрических персональных данных, в отличие, например, от бытовых, не происходят спонтанно, они тщательно планируются и подготавливаются. Алгоритм действий потенциальных преступников при совершении самого распространенного «Дипфейк»-посягательства – мошенничества – сводится к реализации следующих этапов.

1. На первом этапе злоумышленники изучают цифровой профиль потенциальной жертвы, включая его фотографии, видеоизображения в социальных сетях, круг общения – по работе, дружбе или в микрогруппах, а также материальные возможности, основываясь на информации о путешествиях и покупках. Они оценивают кредитную историю потенциальной жертвы и вероятность одобрения банком кредита на большую сумму. Важно отметить, что эту информацию потенциальная жертва может неосознанно предоставить преступникам самостоятельно, совершая какие-либо операции в интернете. Кроме того, персональные данные могут быть скомпрометированы в органах и организациях, которые их собирают и хранят [8, с. 75].

2. На втором этапе с помощью искусственного интеллекта и психологических алгоритмов создается индивидуальный сценарий обмана потенциальной жертвы. В основе обмана лежит разработка вариантов эффективной коммуникации с потенциальной жертвы с применением технологии «Дипфейк». Для этого изучаются аккаунты руководителей, начальников, друзей и знакомых. Некоторые голосовые сообщения создаются заранее по сведениям, собранным о потенциальной жертве [9, с. 238].

3. Завершающим этапом является прямой контакт с потенциальной жертвой по телефону или видеосвязи, в ходе которого используются различные приемы психологической обработки. Для имитации в режиме реального времени голоса и изображения известного жертве человека применяются нейросети и технологии «Дипфейк». Схемы таких преступлений в целом схожи, их цель – получить доступ к денежным средствам жертвы [10, с. 379]. Тенденцией последнего времени стало использование хищения у жертвы денег в качестве преступления, обеспечивающего совершение другого преступления: жертву обманным путем заставляют совершить какие-либо преступные деяния в обмен на обещание вернуть похищенные деньги [11, с. 10].

Для определения характерных способов применения технологии «Дипфейк» в совершении преступлений с использованием подложных биометрических персональных данных нами было

[9] Deepfake Detection Challenge (DFDC) // Deepfake Detection Challenge : [сайт]. URL: https://web.archive.org/web/20200112102819/https://deepfakedetectionchallenge.ai/ (дата обращения: 09.01.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

предпринято эмпирическое исследование (изучение приговоров судов общей юрисдикции[10]), которое позволило сформулировать наиболее типичные варианты действий с участием цифровых клонов физического лица.

1. Просьба о финансовой помощи. Преступники с помощью нейросети синтезируют голос члена семьи, родственника или коллеги, а затем по телефону передают просьбу о финансовой помощи в сложной жизненной ситуации (такой как болезнь, привлечение к ответственности, пожар или другая трагедия) [12, с. 34]. Особенно часто подобные провокации осуществляются в ночное время, когда люди, по большей части пожилые, наиболее уязвимы, что создает «благоприятные» условия для хищения их денежных средств.

2. Фальшивый видеоконтент. Преступники с помощью нейросети и технологии «Дипфейк» синтезируют голос, создаются поддельное фото или видеоизображение, на которых потенциальная жертва якобы совершает аморальные или даже преступные деяния. Затем с потенциальной жертвой связываются преступники, предлагающие «уничтожить» эту информацию за определенную плату. Подобный контент может использоваться не только для получения денег, но и для последующей дискредитации человека [13, с. 76]. Например, в ходе предвыборной агитации опубликованное в социальных сетях аморальное видео может опорочить любого кандидата или создать условия для манипулирования действиями жертвы под угрозой его распространения.

3. Обман в предпринимательской сфере. Преступники с помощью нейросети и технологии «Дипфейк» синтезируют голос и видеоизображение руководителя, который якобы дает подчиненному поручение о переводе денежных средств на определенный счет [14, с. 189]. При этом все поручения выдаются только в дистанционном формате, исключающем непосредственный контакт с подчиненным, производящим перевод денег.

4. Взлом платежных систем. Преступники с помощью технологий 3D-печати и 3D-масок, которые открывают абсолютно новые возможности для взлома платежных систем, подделывают реалистичное биометрическое изображение лица жертвы в реальном времени. Поскольку в современных платежных системах активно внедряются инструменты из разряда «Плати улыбкой», лицо каждого гражданина, подключившего эту функцию, становится ключом к его счету в платежных приложениях. «Бесконечные атаки на платформы онлайн-кредитования, супермаркеты, мобильные телефоны, которые имеют низкий коэффициент информационной безопасности, наносят всем субъектам значительный материальный ущерб» [8, с. 76]. В связи с этим особого внимания заслуживает нововведение, привнесенное Федеральным законом от 28 декабря 2024 г. № 521-ФЗ[11], в соответствии с которым в России до 15 июля 2025 г. должны быть реализованы меры, направленные на обеспечение в рамках экспериментального правового режима возможности банков проводить удаленную идентификацию клиентов, в т. ч. с использованием видео-конференц-связи [9, с. 216]. Однако пока остается неясным, будет ли эта идентификация учитывать возможность криминального участия в видеоконференции цифрового двойника реального человека.

5. Ложные конкурсы и розыгрыши. Преступники с помощью нейросети и технологии «Дипфейк» синтезируют голос и создаются поддельное видеоизображение с участием известных людей (политиков, артистов), которые заманивают пользователей на фишинговый сайт, обещая выигрыши или призы за участие в какой-либо акции. Перед этим формируется множество ложных комментариев и аккаунтов, которые создают видимость независимого или альтернативного мнения, но на самом деле побуждают людей присоединиться к акции или поучаствовать в конкурсе. Как только пользователь переходит на фишинговый сайт, ему на устройство скачивается вредоносное программное обеспечение, открывающее преступникам доступ ко всем установленным на нем приложениям [15, с. 121].

Таким образом, создание с помощью нейросетей и технологии «Дипфейк» цифровых клонов физического лица может нести в себе серьезные риски. В первую очередь они касаются всех традиционных киберугроз: преступники могут использовать цифровую копию для мошенничества; шантажа; создания контента, дискредитирующего оригинал; звонков подчиненным от имени руководителей; взлома приложений финансово-кредитных организаций и т. д. Приведенные примеры позволяют сделать однозначный вывод о том, что условия, способствующие совершению преступлений, заключаются в несогласованности нормативного регулирования

[10] Всего было изучено 300 приговоров судов общей юрисдикции, вынесенных в 2024 году, опубликованных на сайте «Судебные и нормативные акты РФ (СудАкт)» (URL: https://sudact.ru/regular/).

[11] О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 28 декабря 2024 г. № 521-ФЗ // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2024. № 53 (ч. I). Ст. 8531.

использования и защиты биометрических персональных данных человека. Утрата или подделка таких данных может привести к необратимым последствиям.

Для исправления ситуации для начала требуется проработать вопрос нормативно-правового регулирования оборота биометрических персональных данных физического лица. Область их применения охватывает множество важных сфер: финансы, здравоохранение, образование, ретейл, электронную коммерцию и государственные услуги. Вместе с тем должен быть обеспечен высокий уровень защиты такой информации. Однако в настоящее время даже сам термин «биометрические персональные данные физического лица» не имеет четкого законодательного закрепления. В Федеральном законе от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» п. 4 ст. 3 изложен следующим образом: «В единой биометрической системе размещаются и обрабатываются биометрические персональные данные следующих видов:

1) изображение лица человека, полученное с помощью фото- и видеоустройств;

2) запись голоса человека, полученная с помощью звукозаписывающих устройств»[12].

Соответственно, в качестве биометрических персональных данных в приоритете рассматриваются только голос и изображение лица, которые, как мы выяснили, при современном уровне развития технологий, позволяющем их копировать, не являются уникальными идентификаторами личности. Равно как и другие, не вошедшие в этот список биометрические характеристики (отпечатки пальцев, сетчатки глаза, биологические или поведенческие особенности), которые, как известно, можно подделать. На данный момент современные технологии пока не могут повторить лишь такие уникальные черты человека, как генетический код и рисунок вен, которые также не входят в список законодательно определенных биометрических персональных данных, позволяющих достоверно идентифицировать личность.

Кроме того, в законодательстве нет единого подхода к характеристикам голоса и изображения лица человека, пригодным для его идентификации. В январе 2025 года был опубликован проект приказа о внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 453 от 12 мая 2023 г. В этом документе ранее уже были изменены правила обработки биометрических персональных данных и введены новые технические параметры: увеличена неравномерность яркости изображения лица в области щек и носа с 0,3 до 0,6 единиц измерения; переработаны требования к детализации черт лица, длине чистой речи голоса и содержанию произносимых сообщений. Причем п. 11, 12 и 13, которые уже подвергались коррекции, сейчас содержат достаточно строгие требования к параметрам биометрических персональных данных для размещения и хранения их в Единой биометрической системе. В этих пунктах присутствуют слова «должен» и «должно», что указывает на то, что несоответствие перечисленным параметрам может привести к отклонению системой собранных биометрических данных. Работу по ужесточению правил сбора и обработки биометрических персональных данных планируется продолжить. Нормативное регулирование работы Единой биометрической системы осуществляется на основании Указа Президента Российской Федерации от 30 сентября 2022 г. № 693[13] и постановления Правительства Российской Федерации от 16 декабря 2022 г. № 2326[14], функции единого оператора Единой биометрической системы выполняет АО «Центр биометрических технологий», в качестве партнеров в этой системе выступают ПАО «Ростелеком», Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) и Центральный банк Российской Федерации.

Итак, в соответствии с приказом Минцифры России № 453, «если в ходе контроля качества, проводимого банками, многофункциональными центрами и другими организациями,

---

[12] Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федеральный закон от 29 декабря 2022 г. № 572-ФЗ (ред. от 26.12.2024) // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

[13] Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации : Указ Президента Российской Федерации от 30 сентября 2022 г. № 693 // СЗ РФ. 2022. № 40. Ст. 6791.

[14] О возложении на акционерное общество «Центр Биометрических Технологий» функций оператора единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также о признании утратившими силу распоряжения Правительства Российской Федерации от 22 февраля 2018 г. № 293-р и пункта 4 изменений, которые вносятся в акты Правительства Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 24 июня 2021 г. № 982 : постановление Правительства Российской Федерации от 16 декабря 2022 г. № 2326 // СЗ РФ. 2022. № 52. Ст. 9598. Документ утратил силу.

ISSN 2949-1150 (online)
2071-8284 (print)

будет выявлено несоответствие параметров биометрических персональных данных требованиям, указанным в пунктах 11 и 13, такие биометрические персональные данные не будут переданы в Единую биометрическую систему»[15]. Получается, что биометрические персональные данные могут быть собраны, обработаны, но не приняты Центром биометрической технологии. При этом в приказе не прописан механизм их утилизации. Подобный пробел обладает серьезным криминогенным потенциалом, поскольку открывает широкие возможности для хищения или незаконного использования биометрических персональных данных, которые были отклонены Центром биометрической технологии и не вошли в Единую биометрическую систему.

Таким образом, несмотря на наличие множества нормативных правовых актов, посвященных защите персональных данных, а также технологических разработок, направленных на обеспечение их безопасности, проблему использования подложных биометрических персональных данных для совершения преступлений с применением нейросетей и технологии «Дипфейк» решить пока не удается. Поддельный контент не только вводит в заблуждение граждан, но и активно используется в различных преступлениях, что снижает уровень защиты биометрических персональных данных. При создании поддельных фотографий, аудиозаписей и видеоизображений потенциальные преступники не получают согласия на использование указанных биометрических персональных данных человека, следовательно, они фактически нарушают его личные неимущественные права. В связи с этим создание фальшивого контента и его последующее использование в криминальных целях должно быть законодательно запрещено, а за нарушение этого запрета должна наступать ответственность.

В целях обеспечения выполнения перечисленных требований, на наш взгляд, стоит внести изменения в действующую редакцию Уголовного кодекса Российской Федерации[16] (далее – УК РФ), дополнив ее новой нормой, предусматривающей уголовную ответственность за невыполнение установленных правил в этой сфере – ч. 61 ст. 272[1] УК РФ «Незаконные создание и (или) передача, использование аудио, видео, голосовых материалов, сгенерированных с помощью нейронной сети на основе биометрических персональных данных физического лица, полученных без его согласия». Подобные изменения не подменяют собой ч. 6 ст. 272[1] УК РФ, где объектом защиты выступает вся компьютерная информация, содержащая персональные данные. Они лишь создают новые профилактические возможности для защиты биометрических персональных данных на стадии подготовки к совершению другого более тяжкого преступления. Причем вопрос об уголовной ответственности за использование поддельных биометрических персональных данных неоднократно поднимался на уровне законопроектов. В частности, в законопроекте № 718538-9[17] было предложено сделать незаконную генерацию биометрических персональных данных физического лица с помощью нейронной сети квалифицирующим признаком нескольких составов преступлений, а в законопроекте № 718834-8[18] предлагалось закрепить правовой статус голоса и изображения человека в виде личного неимущественного права. Оба законопроекта находятся на стадии рассмотрения, но в заключениях правового управления Государственной Думы Федерального Собрания Российской Федерации уже имеются отрицательные аргументы, которые могут негативно сказаться на перспективе принятия данных документов.

В предлагаемой нами новой ч. 61 ст. 272[1] УК РФ компьютерная информация, сгенерированная с помощью нейронной сети на основе незаконного доступа к биометрическим персональным данным физического лица, может выступать только в качестве дополнительного объекта преступления, ведь подмена таких сведений о личности в качестве основного объекта подразумевает посягательство на права и свободы физического лица, а именно, его биометрические

[15] О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц : приказ Минцифры России от 12 мая 2023 г. № 453 (ред. от 29.11.2023) (зарег. в Минюсте России 30.05.2023, № 73620) // Официальный интернет-портал правовой информации (pravo.gov.ru) : [сайт]. URL: http://publication.pravo.gov.ru/document/0001202305310045 (дата обращения: 09.01.2025).

[16] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.12.2024) // СЗ РФ. 1996. № 25. Ст. 2954.

[17] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности) // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (далее – СОЗД ГАС «Законотворчество») : [официальный сайт]. URL : https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 09.01.2025).

[18] Законопроект № 718834-8 «О внесении изменений в часть первую Гражданского кодекса Российской Федерации» (об охране голоса) // СОЗД ГАС «Законотворчество» : [официальный сайт]. URL : https://sozd.duma.gov.ru/bill/718834-8 (дата обращения: 09.01.2025).

персональные данные. Нарушение личных неимущественных прав происходит здесь на стадии создания и последующего использования поддельных аудиозаписей и видеоизображений, что не охватывается ч. 6 ст. 272[1] УК РФ, в которой ответственность предусмотрена за «Создание и (или) обеспечение функционирования информационного ресурса (сайта в сети „Интернет" и (или) страницы сайта в сети „Интернет", информационной системы, программы для электронных вычислительных машин), заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем»[19]. Следовательно, в ч. 6 ст. 272[1] УК РФ речь идет только о подлинных персональных данных, а не о заведомо поддельных, сгенерированных с помощью нейронной сети.

Заключение

Для обеспечения безопасности биометрических персональных данных необходима надежная и достоверная система правовых и технических средств. Решить данную проблему, по мнению законодателей, можно, введя тотальную аутентификацию всех пользователей в цифровой среде, когда каждый компьютер и аккаунт будет зарегистрирован на конкретного человека, чья личность подтверждена двухфакторной системой. Подобный подход исключает анонимность, следовательно, гарантирует абсолютную прозрачность всех действий в интернете. Кроме этого необходимо законодательно регламентировать понятийный аппарат и прописать основные правила использования нейросетей и технологии «Дипфейк», в частности, определить, какие изображения граждан, созданные нейросетями, можно использовать без разрешения обладателя биометрических персональных данных, а какие – только с его согласия. Одновременно нужно полностью исключить использование цифровых клонов в новостных передачах и социальных сетях, где затрагиваются вопросы защиты личности, общества и государства, а также экономические интересы страны. Следует прописать правила использования таких технологий для обеспечения общественной безопасности (например, для распознавания лиц с использованием комплекса «Безопасный город»). В таких случаях контент должен быть промаркирован соответствующей меткой. Признавая неизбежность научно-технического прогресса и внедрения новых разработок в нашу жизнь, считаем, что лишь законодательными или техническими мерами обеспечить полную безопасность биометрических персональных данных вряд ли удастся. Необходимо в перспективе разработать концепцию эффективной защиты биометрических персональных данных, на основе которой будет осуществляться скоординированная деятельность всех заинтересованных лиц и организаций в этом направлении.

Список источников

1. *Миловановa М. М., Шурухнов В. А.* Кибермошенничество: взаимосвязь способа совершения преступления и личности преступника // Расследование преступлений: проблемы и пути их решения. 2024. № 2 (44). С. 63–71; https://doi.org/10.54217/2411-1627.2024.44.2.006.

2. *Добробаба М. Б.* Дипфейки как угроза правам человека // Lex Russica. 2022. Т. 75, № 11 (192). С. 112–119; https://doi.org/10.17803/1729-5920.2022.192.11.112-119.

3. *Желудков М. А.* Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология deepfake) / Развитие наук антикриминального цикла в свете глобальных вызовов обществу : сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием, г. Саратов, 16 октября 2020 г. Саратов : Саратовская государственная юридическая академия, 2021. С. 262–270.

4. *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. Т. 7, № 4. С. 379–386; https://doi.org/10.22363/2312-8313-2020-7-4-379-386.

5. *Киселев А. С.* О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64; https://doi.org/10.18384/2310-6794-2021-3-54-64.

6. *Ли Я.* Использование технологии «дипфейк» в Китае: проблемы правового регулирования и пути их решения // Lex Russica. 2024. Т. 77, № 11 (216). С. 21–31; https://doi.org/10.17803/1729-5920.2024.216.11.021-031.

7. *Свиридова Е. А.* Правила использования технологий дипфейк в праве США и КНР: адаптация зарубежного опыта правового регулирования // Современное право. 2024. № 3. С. 119–123; https://doi.org/10.25799/NI.2024.96.67.019.

8. *Поздняк И. Н.* Цифровые угрозы в современном мире: технология deepfake // Судебная экспертиза Беларуси. 2024. № 2 (19). С. 72–77.

9. *Виноградов В. А., Кузнецова Д. В.* Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. № 2. С. 215–240; https://doi.org/10.17323/2072-8166.2024.2.215.240.

10. *Купка И. П., Щербаков С. С.* Дипфейк как информационное оружие современности // Динамика медиасистем. 2023. Т. 3, № 1. С. 375–381.

[19] СЗ РФ. 1996. № 25. Ст. 2954.

ISSN 2949-1150 (online)
2071-8284 (print)

11. *Алексеева А. П., Белокобыльская О. И.* Виды преступности, обеспечивающие совершение других преступлений, и возможности их предупреждения // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 2 (76). С. 9–15.

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

13. *Голятина С. М.* Криминалистическое прогнозирование дистанционного мошенничества // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 4 (78). С. 75–80.

14. *Захаров Н. Д.* Правовые основы регулирования отношений в информационно-телекоммуникационных сетях в Российской Федерации в рамках противодействия преступности (часть 1) // Вестник Волгоградской академии МВД России. 2024. № 2 (69). С. 181–190.

15. *Захаров Н. Д.* Правовые основы регулирования отношений в информационно-телекоммуникационных сетях в Российской Федерации в рамках противодействия преступности (часть 2) // Вестник Волгоградской академии МВД России. 2024. № 3 (70). С. 119–127.

Авторами внесен равный вклад в написание статьи.
Авторы заявляют об отсутствии конфликта интересов.

The authors have made an equal contribution to the writing of the article.
The authors declare no conflicts of interests.