Оригинальная статья / Original article

УДК 343.3/.7

https://doi.org/10.21869/2223-1501-2025-15-2-154-171

Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8)

И.С. Алихаджиева[1] ✉

[1]Российская криминологическая ассоциация имени Азалии Ивановны Долговой
г. Москва 117624, Российская Федерация

✉e-mail: Alins1@yandex.ru

Резюме

Актуальность *статьи определяется научным анализом внесенного на рассмотрение Государственной Думы России законопроекта о введении уголовной ответственности за использование технологии подмены личности в преступных целях.*

Целью исследования *является формулирование оснований критической оценки проектируемого уголовно-правового запрета на предмет имеющихся в нем пробелов.*

Задачи: *подвергнуть научному осмыслению законодательную инициативу; выявить в обсуждаемом законопроекте недостатки содержательного и технико-юридического характера при конструировании норм, наделяемых новым квалифицирующим признаком; сформулировать оригинальную модель уголовной ответственности за деяния, совершаемые с использованием технологии дипфейк, для эффективного противодействия им.*

Методология исследования *представлена общенаучными и частнонаучными методами познания объективной действительности. Среди них методы индукции, дедукции, анализа, синтеза, а также системно-аналитический, формально-юридический, формально-логический методы и метод толкования правовых норм.*

Результаты исследования *носят прикладной характер и включают разработку для правоприменителя рекомендаций, касающихся правки редакции проектируемых норм. Дополнительным итогом проведенного исследования стала систематизация составов преступлений, средством совершения которых может быть технология цифрового клонирования внешности и голоса человека. Автором доказывается нецелесообразность наделения квалифицирующим признаком отдельных составов преступлений, как предлагают думцы, и приводятся аргументы в пользу формулирования универсального отягчающего обстоятельства с его дополнением в статье 63 Уголовного кодекса Российской Федерации.*

Вывод. *Предлагаемые правотворцами нововведения содержат ряд существенных изъянов. Для их устранения могут быть востребованы сформулированные в настоящей работе выводы. С учётом темпов развития искусственного интеллекта, когда злоумышленниками освоены самые передовые технологии для создания цифровых двойников, подделки биометрических данных, можно предположить, что уголовно-правовая реакция законодателя на новые способы совершения преступлений с помощью технологии дипфейк будет запоздалой. Авторская модель уголовно-правовых средств воздействия в отношении посягательств, учиненных посредством подмены личности, видится более выверенной и перспективной.*

Ключевые слова*: законопроект; дипфейк; дипвойс; биометрические персональные данные; нейросеть; преступность.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Алихаджиева И.С. Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8) // Известия Юго-Западного государственного университета. Серия: История и право. 2025. Т. 15, № 2. С. 154–171. https://doi.org/10.21869/2223-1501-2025-15-1-154-171.

Поступила в редакцию 28.02.2025 Принята к публикации 02.04.2025 Опубликована 28.04.2025

Prospects for establishing criminal liability for crimes involving the use of identity substitution technologies (Draft Law № 718538-8)

Inna S. Alikhadzhiyeva[1]✉

[1]Russian Criminological Association named after Azalea Ivanovna Dolgova
Moscow 117624, Russian Federation

✉e-mail: Alins1@yandex.ru

Abstract

The relevance *of the article is determined by the scientific analysis of the bill submitted to the State Duma of Russia on the introduction of criminal liability for the use of personality substitution technology for criminal purposes.*

The purpose *of the study is to formulate the grounds for a critical assessment of the projected criminal law prohibition for the gaps in it.*

Objectives: *to subject the legislative initiative to scientific understanding; identify in the draft law under discussion shortcomings of a substantive and technical-legal nature in the design of norms endowed with a new qualifying feature; formulate an original model of criminal liability for acts committed using deepfake technology to effectively counter them.*

Methodology*. The research methodology is represented by general scientific and private scientific methods of cognition of objective reality. Among them are methods of induction, deduction, analysis, synthesis, as well as system-analytical, formal-legal, formal-logical methods and a method of interpreting legal norms.*

The results *of the study are applied in nature and include the development of recommendations for the law enforcer regarding the revision of the draft norms. An additional result of the study was the systematization of the composition of crimes, the means of which can be the technology of digital cloning of a person's appearance and voice. The author proves the inexpediency of endowing with a qualifying feature of individual corpus delicti, as suggested by the Duma members, and gives arguments in favor of formulating a universal aggravating circumstance with its addition in Art. 63 of the Criminal Code of the Russian Federation.*

Conclusion. *The innovations proposed by the creators contain a number of significant flaws. To eliminate them, the conclusions formulated in this work may be in demand. Taking into account the pace of development of artificial intelligence, when cybercriminals have mastered the most advanced technologies for creating digital twins, faking biometric data, it can be assumed that the criminal law reaction of the legislator to new ways of committing crimes using deepfake technology will be belated. The author's model of criminal legal means of influence in relation to encroachments committed through personality substitution seems to be more verified and promising.*

Keywords*: bill; deepfake; diplomatic troops; biometric personal data; neural network; crime.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Alikhadzhiyeva I.S. Prospects for establishing criminal liability for crimes involving the use of identity substitution technologies (Draft Law № 718538-8). *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2025;15(2):154–171. (In Russ.) https://doi.org/10.21869/2223-1501-2025-15-2-154-171.

Received 28.02.2024 Accepted 02.04.2025 Published 28.04.2025

***

Введение

Множество примеров противоправного применения дипфейков вызвали оживленную дискуссию в научном сообществе, предметом которой стало осмысление перспективы уголовно-правовой оценки технологии глубокого синтеза.

Одни правоведы (Л.В. Головко) утверждают, что «уголовное и уголовно-процессуальное законодательство обладает всем необходимым инструментарием, чтобы бороться с любыми проявлениями мошенничества, будь то дипфейки или телефонные обманы. Мошенничество остается мошенничеством независимо от способа обмана: он может быть вербальным, телефонным, сопряженным с созданием фейковых видео и т. п. Искусственный интеллект здесь также ни при чем, т. к. подложные видео создают не машины сами по себе, а конкретные люди, действующие в своих корыстных интересах и лишь использующие для их реализации программные технологии. Иначе говоря, здесь, как и во всех остальных случаях, мы сталкиваемся с интеллектом не искусственным, а естественным, пусть и, увы, преступным»[1].

Другие юристы, пишущие об опасности методики клонирования изображения и голоса, выступают за полный запрет создания видео- или аудиофальшивок под угрозой уголовной репрессии. Так, Р.И. Дремлюга предлагает установить ответственность за дипфейк в ст. 274[3] УК РФ, поместив ее в главу 28 УК РФ [1, с. 277]. Комментируя инициативу введения наказания за само применение технологии без преступной цели, В.Н. Ситник видит проблему в двойном учете одного и того же деяния, когда правоприменитель будет вынужден квалифицировать, к примеру, изготовление порнографических материалов сразу по двум статьям УК РФ [2, с. 79]. Не ясно, по мнению В.Н. Ситника, и то, в какую главу поместить новый состав ввиду сложности определения видового объекта уголовно-правовой охраны [2, с. 80].

М.А. Ефремова, Е.А. Русскевич, подвергая сомнению правильность определения местоположения спроектированной нормы, указывают на другие недочеты в ее редакции: «Крайне спорным также является выделение автором в качестве квалифицирующего признака – использование информационно-телекоммуникационных сетей. Вряд ли дипфейк вообще можно представить вне сетевого пространства» [3, с. 103]. Эта (третья) группа исследователей в трудах по рассматриваемой теме не находит социально-правовых предпосылок для самостоятельной криминализации любых действий с дипфейками. Они считают новую технологию «инструментом, который может применяться в разных целях», а потому в научном дискурсе обсуждаются иные уголовно-правовые модели реагирования на инциденты с дипфейками (в частности, признание совершения тех или иных общественно опасных деяний с их помощью новым квалифицирующим обстоятельством [2, с. 81; 3, с. 104; 4, с. 10]). Приведенные суждения, по их мнению, подтверждаются и отведением использованию технологии дипфейк отдельной графы в статистическом учете Генеральной прокуратуры России в соответствии с приказом от 9 декабря 2022 г. № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре» (п. 049 «Поддельные печати и документы» раздела «Предметы, устройства и другие средства, использованные при совершении преступлений» (Справочник № 25-ГП))[2].

[1] Мошенничество с использованием дипфейков доказать проще, чем обычный обман – эксперт // Российское агентство правовой и судебной информации: сайт. 2023. 20 нояб. URL: https://rapsi-pravo.ru/digital_law_news/20231120/309397389.html?ysclid=m6wb2ln1g851591457 (дата обращения: 18.12. 2024).

[2] О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре: приказ Генпрокуратуры России от 9 дек. 2022 г. № 746: послед. ред. //

При поддержке теоретиков в части недостаточности социальной обусловленности уголовной ответственности за дипфейк в отдельной статье УК РФ основным аргументом выступает прежде всего отсутствие какой-либо общественной опасности дипфейка, если его изготовление и распространение не преследует противоправной цели. Разделяя позицию об ужесточении ответственности за дипфейки, Н.Ф. Бодров и А.К. Лебедева обосновывают ее большей степенью общественной опасности совершенных с их использованием преступлений. «Создание такого материала, – пишут соавторы, – преследует иллокутивную цель, то есть введение в заблуждение, а его выявление характеризуется особой сложностью, требуются специальные программы или эксперты. С учетом природы дипфейка и невозможности установления запрета на создание генеративного контента нужна правовая регламентация именно распространения и использования генеративного контента на основе биометрических персональных данных» [5, с. 53]. И действительно. Эта технология, способная объединить внешность (лицо и мимику) и голос одного человека с телом другого либо изготовить похожий на оригинал цифровой клон живущего или умершего человека, позволяет использовать ее во благо. Так, при помощи российского стартапа Deepcake был создан проморолик Сбера с Жоржем Милославским (наследники дали согласие на использование изображения и голоса Леонида Куравлева). Компания МегаФон «сняла» в рекламе виртуального двойника Брюса Уиллиса, обработав его внешность через дипфейк технологию, а Брюс Ли «участвовал» в промоушн виски «Джонни Уокер». В новом проекте «Диверсант. Идеальный штурм» создатели кинофильма воплотили на экране цифровую модель умершего актера Владислава Галкина, взяв за основу видеоряд персонажа из первых сезонов сериала. А музей во Флориде для беседы со зрителями, рассказов о жизни и совместного селфи «оживил» художника Сальвадора Дали. Для воспроизведения голоса, акцента и манеры речи искусственным интеллектом с актером были обработаны 6 тыс. фотографий, 1 тыс. часов машинного обучения интервью и писем художника и 145 видео.

Цифровые возможности дипфейка используются и в глобальной повестке всего человечества для блага настоящих и будущих поколений. К примеру, звезда британского футбола Дэвид Бекхэм участвовал в съемках социального видео, посвященного борьбе с малярией, для британской благотворительной организации здравоохранения Malaria No More («Малярия должна умереть»). По сценарию он предстал перед зрителями в роли седого старика, озвучивая с помощью нейросети месседж к мировым лидерам на девяти языках голосами людей, переживших малярию, и врачей, победивших ее. В Африке малярия убивает около 435 тыс. человек ежегодно, 61% смертности приходится на детей в возрасте до пяти лет. Для «смены» лица и искусственного состаривания футболиста, обратившегося из будущего к живущим сейчас людям на их родных языках, компанией, участвовавшей в съемках фильма «Загадочная история Бенджамина Баттона», применялась технология дипфейк[1].

О том, что нельзя под страхом уголовного наказания запретить дипфейк сам по себе, говорит и его признание объектом авторского права впервые в России[2]. Арбитражный суд г. Москвы в

КонсультантПлюс: сайт. URL: https://www.con-sultant.ru/document/cons_doc_LAW_433986/ (дата обращения: 14.02.2025).

[1] 70-летний Бекхэм – в рекламе, где мир уже победил малярию // Гол: сайт. 2020. 3 дек. URL: https://gol.ru/materials/7764-70-letnij-bekhem-v-reklame-gde-mir-uze-pobedil-malariu?ysclid=m6w355w3xs172677742 (дата обращения: 25.12.2024).

[2] Дипфейк разобрали в суде // Коммерсантъ: сайт. 2023. 6 дек. URL: https://www.

решении от 30 ноября 2023 г. по делу № А40-200471/23 установил, что компания «Бизнес-аналитика» незаконно использовала чужое аудиовизуальное произведение хронометражем 00.31 минут, в котором появляется сгенерированный нейросетью образ актера Киану Ривза. В юмористическом ролике, созданном Agenda Media Group («Адженда медиа групп»), человек с лицом актера несколько раз проверяет, выключил ли он утюг перед выходом из дома, фотографирует его и берет с собой. На основании договора об отчуждении исключительного права с продакшн-студией правообладателем видеоролика является истец – компания ReFace Technology («Рефейс технолоджис»). Между сторонами не заключалось соглашение о праве использовать ответчиком для рекламы указанного сложного объекта. Видеоматериалы содержат маркировку, в том числе ERID, которая позволяет установить «Бизнес-аналитику» как рекламодателя. Представитель «Бизнес-аналитики» утверждал, что видео нельзя считать объектом авторского права, поскольку оно создано с использованием технологии дипфейк. Суд отклонил этот довод, «поскольку технология Deepfake – это дополнительный инструмент обработки (технического монтажа) видеоматериалов, а не способ их создания. Исходный видеоряд вопреки доводам ответчика отличается исключительно визуальным образом лица актера». Он удовлетворил требования истца и взыскал 500 тыс. руб. компенсации с компании «Бизнес-аналитика» за незаконное использование чужого видео[1]. Несостоятельными утверждения ответчика были признаны и Девятым арбитражным апелляционным судом, указавшим следующее: «Тот факт, что моушн-дизайнер осуществил технический монтаж исходных материалов видеоролика посредством технологии deepfake, сам по себе не свидетельствует, что видеоролик доступен для свободного использования (без согласия правообладателя), или о том, что группа лиц, обеспечившая написание сценария видеоролика, видеосъемку, его аудиосопровождение, не внесли личный творческий вклад в создание видеоролика и не признаются его авторами»[2]. Устояло решение и в кассационной инстанции (постановление Суда по интеллектуальным правам от 19 августа 2024 г. № А40-200471/2023).

Исследователи, классифицируя дипфейки по целям их создания, выделяют самые безобидные из них – любительские и развлекательные без недобросовестной генерации. И здесь они являются хобби, монтируются не для обмана целевых аудиторий, а для увеличения трафика на ресурсе и притока новых подписчиков и др., помечаются как искусственно сгенерированные алгоритмом [6, с. 34].

Методология

Для достижения необходимого теоретического результата автором в качестве научного инструментария использовались общенаучные и частнонаучные методы объективного познания действительности (анализ и синтез, индукция и дедукция, системно-аналитический, формально-юридический, формально-логический метод и метод толкования правовых норм). Основу для проведения настоящего исследования составили ме-

kommersant.ru/doc/6381237 (дата обращения: 14.12.2024).

[1] Решение Арбитражного суда г. Москвы от 30.11.2023 по делу № А40-200471/23 // Электронное правосудие: сайт. URL: https://mkad.arbitr.ru/card/4d7f0305-69af-44fe-8841-a59e84aa7deb?controller=card&instanceid=75c4df24-d81e-46b9-a584-10d3a57769b1 (дата обращения: 14.02.2025).

[2] Постановление Девятого арбитражного апелляционного суда от 08.04.2024 № 09АП-642/2024 по делу № А40-200471/2023 // КонсультантПлюс: сайт. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=MARB&n=2651955&ysclid=m8ey7qv23573864688#zBYWpfUcH2vYLCgp (дата обращения: 14.02.2025).

тоды анализа и синтеза, индукции и дедукции, позволившие описать его актуальность, осуществить выборку научных публикаций по заявленной теме, комплексно и логически верно систематизировать материал, установить значение понятия «дипфейк». Свое применение в работе нашли системно-аналитический, формально-юридический и формально-логический методы и метод толкования правовых норм. С их помощью выполнен обстоятельный анализ текста законопроекта № 718538-8, внесенного на рассмотрение Государственной Думы РФ в части поправок уголовного закона, пояснительной записки к нему, действующего уголовного законодательства, а также выделены и описаны те составы преступлений, для совершения которых в качестве средства может быть использована технология дипфейк. Названные методы в их совокупности послужили формулированию автором замечаний, касающихся редакции новеллы об учете преступного использования дипфейка в качестве квалифицирующего признака отдельных деяний. В результате использования всех перечисленных методов были получены объективные и достоверные результаты, которые могут быть востребованы в законотворчестве, и предложена оригинальная модель уголовной ответственности за совершение преступлений посредством технологии дипфейк.

Результаты и их обсуждение

По пути, предложенному третьей группой ученых, пошел и законодатель. В порядке законодательной инициативы в Государственную Думу РФ депутатом Я.Е. Ниловым и сенатором Российской Федерации А.К. Пушковым был внесен проект закона № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)»[1]. Его авторы предлагают наделить диспозицию четырех уголовно-правовых норм («Кража», «Мошенничество в сфере компьютерной информации», «Вымогательство», «Причинение имущественного ущерба путем обмана или злоупотребления доверием») новым квалифицирующим признаком. Он сформулирован как «деяния, совершенные с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, либо их биометрических персональных данных». В редакциях двух норм – «Клевета» и «Мошенничество» – проектируется отдельный квалифицированный состав того же содержания (дополнение специальной частью 2^1).

Пробелы содержательного характера законопроекта

Разработчики проекта ограничились криминализацией действий с биометрией другого человека в отношении только некоторых составов преступлений. Непонятно, почему иные деяния, имеющие, очевидно, более высокую степень общественной опасности, не попали в перечень тех, в чью диспозицию следует добавить ответственность за использование чужих физических данных, умышленно сфабрикованных при помощи технологии дипфейк или дипвойс. Например, А.А. Смирнов, изучая вредоносное применение глубоких фейков, назвал составы преступлений Модельного уголовного кодекса для государств-участников СНГ от 17 февраля 1996 г., при совершении которых могут быть использованы технологии искусственного интеллекта. Среди них: публичные призывы к развязыванию

[1] О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности): законопроект № 718538-8 // Государственная Дума РФ: сайт. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 25.11.2024).

агрессивной войны (ст. 103), принуждение (ст. 142), клевета (ст. 143), оскорбление (ст. 144), понуждение к действиям сексуального характера (ст. 147), заведомо ложное сообщение об акте терроризма (ст. 182), возбуждение национальной, расовой или религиозной вражды (ст. 187), незаконное распространение порнографических материалов или предметов (ст. 237), вымогательство (ст. 143), публичные призывы к насильственному изменению конституционного строя (ст. 295), оскорбление представителя власти (ст. 312) [7, с. 69]. Следуя этому примеру, составим примерный перечень деяний российского уголовного закона, когда дипфейки как средство их совершения повысят вероятность достижения преступной цели.

Без внимания инициаторов законопроекта остались преступления против личности, когда сгенерированные посредством искусственного интеллекта внешность и голос человека будут использоваться для доведения до самоубийства (ст. 110 УК РФ), склонения к совершению самоубийства или содействия совершению самоубийства (ст. 110[1] УК РФ). Так, в штате Пенсильвания (США), чтобы исключить из школьной команды чирлидеров соперниц, мать одной из девочек посредством искусственного интеллекта создала их поддельные видео и фотоизображения. На них потерпевшие обнажались, курили электронные сигареты и употребляли алкоголь. Женщина анонимно отправила смонтированные дипфейк-видео тренеру и девушкам, призывая подростков покончить с собой[1].

Сфабрикованные аудиовизуальные материалы (фотографии, видеозаписи) с изображением кандидата на выборах, размещенные в информационном поле с десятками миллионов просмотров, могут образовать противоправное вмешательство в избирательную кампанию и отразиться на итогах голосования. Искусственно синтезированные видео с динамическим изображением и голосом человека способны нанести вред референдумным и избирательным правам, служить инструментом политической манипуляции, что требует соответствующей реакции законодателя в части усиления наказания и за них при использовании технологии дипфейк (141 УК РФ). Высоки риски завладения чужими, модифицированными через технологию дипфейк изображением и (или) голосом для совершения преступлений, нарушающих авторские и смежные права (ст. 146 УК РФ), или изготовления материалов, оскорбляющих религиозные чувства верующих (ст. 148 УК РФ). К примеру, компания Roc Nation, принадлежащая американскому музыканту Шону Картеру, известному как Jay-Z, уведомила YouTube о нарушении авторских прав и прав артиста на интеллектуальную собственность и подала иск в суд. Предметом судебного спора стал размещенный ютубером под ником «Vocal Synthesis» deepfake ролик, в котором звучит голос Jay-Z. Сгенерированный нейросетью рэпер читает монолог Уильяма Шекспира «Быть или не быть» из пьесы «Гамлет». По мнению правообладателя, «в этом контенте незаконно используется искусственный интеллект для олицетворения голоса нашего клиента». Кроме Jay-Z, автор канала опубликовал дипфейк записи Боба Дилана и Фрэнка Синатры, исполняющих песни шведской группы Abba. Как пишет The Guardian, видеоролики были удалены с канала, а затем вновь опубликованы с новым дипфейком с участием Jay-Z[2].

[1] Мать обвинили в создании дипфейков, чтобы подставить соперниц дочери из группы поддержки // Techinsider: сайт. 2021. 16 марта. URL: https://www.techinsider.ru/techn-ologies/news-681103-mat-obvinili-v-sozdanii-dipfeykov-chtoby-podstavit-sopernic-docheri-iz-gruppy-podderzhki/ (дата обращения: 20.12.2024).

[2] Jay-Z решил подать в суд на блогера за deepfake // News.ru: сайт. 2020. 30 апр. URL: https://news.ru/music/jay-z-reshil-podat-v-sud-

К составам преступлений, которые надлежит дополнить новым квалифицирующим признаком, следует отнести и мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ) и в сфере кредитования (ст. 159^1 УК РФ), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ). Правоохранители зарегистрировали первые случаи нового способа мошенничества с кредитами, когда злоумышленник запрашивает смену телефонного номера на чужом банковском аккаунте. Он ссылается на то, что якобы является владельцем утерянной вместе с телефоном сим-карты. Для прохождения аутентификации, применяемой для проверки клиентов и предоставления доступа к их учетным записям, преступник при помощи дипфейка по видеозвонку привязывает новый номер к личному кабинету жертвы. Получив доступ, им похищаются денежные средства и удаленно оформляются кредиты с использованием мобильного банка[1]. Технологии клонирования голоса могут применяться и для незаконного получения сведений, составляющих коммерческую, налоговую или банковскую тайну и манипулирования рынком (ст. 185^3 УК РФ). Вполне допустимо смоделировать ситуацию, когда для обвала спроса и цен на акции, иностранную валюту и (или) товары могут вбрасываться инсайд дипфейки с подложным заявлением о банкротстве бирж, финансовых учреждений и компаний и др. К примеру, дипфейк «генерального директора», отвечающего за реализацию бизнес-планов и стратегическое управление, финансовую устойчивость компании, может сообщить о ее банкротстве либо о технологическом прорыве или выпуске нового продукта, чтобы повлиять на стоимость акций.

Фальшивые аудиовизуальные материалы для «смены» лица и голоса могут быть инструментом для совершения преступлений в сфере компьютерной информации (ст. 272, 272^1, 273, 274, 274^1 УК РФ) как «первоначальных» в серии последующих противоправных деяний. Обладая специальными познаниями в области компьютерной техники и программного обеспечения, преступники, используя дипфейк сотрудника банка, к примеру, могут получить логины и пароли для доступа к специальным банковским компьютерным программам с информацией о клиентах (личные данные, вклады и счета, банковские карты, транзакции, потребительские кредиты и др.), А затем персональные данные могут быть использованы для дистанционных краж в отношении электронных денежных средств, вымогательства, незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну, нарушений авторских и смежных прав, мошенничества в сфере компьютерной информации и др. Проникнув в локальную сеть через имитацию звонка от IT-директора, хакеры могут обманом завладеть секретной информацией, привилегиями доступа, после чего нанести ущерб критической информационной инфраструктуре.

В новой цифровой реальности технологии глубокого синтеза могут быть средством сокрытия киберпреступниками другого преступления или облегчения его совершения. С помощью внешности, измененной нейросетью или компьютерной графикой, мошенники научились подделывать официальные документы граждан, что подтверждает необходимость повышенной санкции за дипфейк и в ст. 327 УК РФ. При создании цифровых копий паспорта для процесса идентификации и синтеза данных с помощью нейросети совмещаются две фотографии

na-blogera-za-deepfake/ (дата обращения: 19.12.2024).

[1] В полиции Кубани предупредили о новых мошенничествах с использованием дипфейков // Коммерсантъ: сайт. 2024. 5 февр. URL: https://www.kommersant.ru/doc/6493222 (дата обращения: 19.12.2024).

в одну (морфинг-атака, morphing attack), чтобы лицо (изображение) сохраняло сходство с владельцем и несколькими преступниками (facemorphing trend). Оригинальные фотографии паспорта для заимствования внешности могут быть получены хакерами путем «взлома» мессенджеров, страниц в социальных сетях и электронной почты.

Критику авторов научных публикаций вызывает и отсутствие незаконного оборота порнографии среди тех деяний, в объективную сторону которых проектируется внесение поправок [5, с. 50]. Дипфейки могут быть использованы для изготовления и массового тиражирования порнографических материалов или предметов (ст. 242 УК РФ), в том числе с изображением детей, что значительно повышает опасность незаконного оборота порнопродукции (ст. 242[1] УК РФ). Pornodeepfake, по оценке экспертов компании Home Security Heroes, не теряет своей популярности. Именно на порнографию приходится 98% всех дипфейков. Их объем за два года (с 2022 по 2023 г.) в Глобальной сети увеличился на 464%. Количество выявленных в Сети поддельных порнографических видео, созданных при помощи искусственного разума, в 2023 г. достигло 280 тыс. Масштаб явления со стремительным продвижением мировой порноиндустрии с персонализацией контента можно оценить и по таким показателям, как общая продолжительность дипфейков (1249 дней, или почти три с половиной года) и число их просмотров, превысившее 4,2 млрд[1]. Подделки цифровых образов настолько глубоко вошли в индустрию порнографической продукции, что создали дилемму уголовной ответственности. Представляется сложным разрешать вопросы квалификации и то, кто является субъектом преступления, когда копии физической реальности созданы искусственным интеллектом – пользователь-создатель видеоролика, первым выложивший его в интернет, владелец платформы или компания-разработчик нейросети [8, с. 71].

Разрушительное действие такого контента, в котором порноактрисам были «приделаны» лица потерпевших женщин, подвергшихся травле в Интернете, может затронуть и неприкосновенность частной жизни (ст. 137 УК РФ). После скандальных дипфейков с публичными людьми в иностранной юридической литературе уже высказана мысль о том, что реалистичные изображения человека в порно – новая форма посягательства на частную жизнь и сексуальную приватность [9, с. 199]. Зарубежные авторы пишут о цифровом сексуальном насилии, совершаемом с помощью технологий (киберпорнография), которое проявляется в «раздевании», в виртуальной порнографии в виде псевдоизображений, полностью сгенерированных искусственным интеллектом [10, с. 1779]. Нарушение человеческой самостоятельности и автономии в сексуальной сфере посредством изготовления порно без согласия человека может проявляться и в сексуальном домогательстве, принуждении к сексу, в сексуальной эксплуатации [11, с. 1351; 12, с. 1801]. Другими словами, с помощью технологии клонирования внешности и голоса можно шантажировать «героя» порновидеоролика как «уличенного» в неблаговидных поступках и принудить его к совершению действий сексуального характера, участию в порнографических съемках, вступить в половое сношение, вовлечь в занятие проституцией (ст. 133, 134, 240, 240[1] УК РФ).

Цифровые подделки высокого уровня реалистичности способны тиражировать не только «обычную» клевету (как думает законотворец), но и распространять ложные, порочащие сведения в от-

[1] Голая «цифра»: эксперты предупредили о рисках популярности дипфейк-порно // Известия: сайт. 2024. 24 янв. URL: https://iz.ru/1638024/dmitrii-bulgakov/golaia-tcifra-eksperty-predupredili-o-riskakh-populiarnosti-dipfeik-porno (дата обращения 22.12.2024).

ношении специальной категории граждан: судей, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения РФ (ст. 298[1] УК РФ). Высокотехнологичный обман на основе комбинации реальных видео и фотографий одного человека либо встраивание изображения людей в чужие видеозаписи может повлечь подрыв профессиональной (служебной) репутации сотрудников полиции, авторитета правоохранительных органов, военнослужащих. Публичные оскорбительные действия в отношении «человека» – цифрового двойника представителя власти (ст. 319 УК РФ) и военнослужащего (ст. 336 УК РФ) могут выражаться в форме, противоречащей общепринятым нормам человеческой морали (в том числе с использованием ненормативной лексики, в неприличных жестах и телодвижениях клона, в унизительном обращении с ним и др.).

Постановочные видео с компрометирующими сюжетами, где государственные служащие, судьи, сотрудники правоохранительных органов якобы совершают правонарушения или аморальные поступки, подрывающие авторитет и деловую репутацию тех ведомств, в которых они работают, могут повлечь не только диффамацию, но и нарушение их трудовых прав. Ведь мотивами создания дипфейка с изображением легко узнаваемого человека, если он носит непристойный или отвратительный характер, может быть месть за профессиональную деятельность, личная неприязнь, карьеризм и др. Уже сегодня суды рассматривают иски, оспаривающие расторжение трудовых договоров за поступки, порочащие честь и достоинство. Как утверждают заявители, их оригинальные видеозаписи и фотографии из социальных сетей в форменном обмундировании со знаками различия и символикой правоохранительных органов, ставшие основанием для увольнения со службы, подверглись изощренной фальсификации с монтированием в них ненормативной лексики[1].

В группу деяний, которые могут быть совершены при помощи дипфейка, не вошли должностные и служебные преступления и преступления против правосудия, а ведь технология искусственного синтеза человеческого изображения и голоса может быть востребована злоумышленниками и для фальсификации документов при служебном подлоге (ст. 292 УК РФ), результатов оперативно-разыскной деятельности и вещественных доказательств по делу (ст. 303 УК РФ).

Высока угроза применения технологии глубокой подделки для совершения актов терроризма (ст. 205[2], 207, 207[1], 207[2] УК РФ) и осуществления экстремистской и другой деятельности (ст. 280, 280[1], 280[3], 280[4], 282, 282[4], 284[2] УК РФ), что отмечают исследователи [13, с. 115]. Как пишет М.А. Савушкина: «Вредоносной и опасной в военно-политическом противостоянии технология дипфейка становится благодаря манипулятивному потенциалу процесса перевода виртуального посыла сообщения в реальные действия его получателей: от перевода денег на финансирование террористических организаций до организации протестов и погромов» [14, с. 51]. Идеальным форматом фейка будет псевдореалистичное видео для публичного распространения недостоверной либо иной вредоносной информации. А.А. Смирнов верно предполагает, что в пропагандистских кампаниях для вброса в целевую аудиторию провокационных фальшивых, но правдоподобных аудио- и видеоматериалов, преступники попытаются задействовать новые ресурсы, чтобы вызвать широкий ре-

[1] Определение Восьмого кассационного суда общей юрисдикции от 11.07.2023 № 88-14506/2023 по делу № 2-4240/2022 // КонсультантПлюс: сайт. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=KSOJ008&n=107963&ysclid=m8ezlgv28o481610057#LdHgpfUu0PFS3DAv (дата обращения: 20.12.2024).

зонанс, массовые беспорядки, применение насилия в отношении какой-то социальной группы. По его мнению, чтобы разжечь ненависть либо вражду, подделка может изображать кадры расстрела мирных жителей военнослужащими, жестокие пытки лиц, подозреваемых в причастности к терроризму или экстремизму, оскорбительные действия в отношении объектов религиозного культа [7, с. 76]. Подтверждение тому – индийские самосуды, или волна насилия и убийств толпой после того, как в WhatsApp завирусились фальсифицированные видео о похищении детей для изъятия органов. Используя страх перед похищением детей, подстрекатели, чтобы разжечь насилие, через мессенджер рассылали вместе с настоящими видео и прикреплённые к ним фейковые сообщения, дополненные местными деталями. Провокация началась с линчевания семи человек и привела к погромам и массовым актам насилия против религиозных и этнических меньшинств, учиненных толпами неграмотных и безработных [15, с. 92]. Виртуальные копии «лидеров мнений» для деструктивного воздействия на потенциального адресата (подписчиков, поклонников) могут транслировать дезинформацию о российских Вооруженных силах с искусственным созданием доказательств обвинения (п. «в» ч. 2 ст. 207^3 УК РФ).

Контент с шоковым информационным поводом (стихийные бедствия, теракты, техногенные катастрофы) фальсифицируется для опровержения официальных версий, чтобы негативными слухами вызвать панику и недоверие властям. Инциденты с дипфейками последних лет с очевидной наглядностью показывают, что сообщения провокационного содержания способны создать эффект взрыва «информационной бомбы». В критических ситуациях риск информационного раскола общества, «информационный апокалипсис», усугубляемый медийной и сетевой разгонкой, может вызывать дестабилизацию в обществе, социальные катаклизмы, привести к конфронтации отдельных социальных групп, вооруженному мятежу, массовым беспорядкам и хулиганским акциям. Так, в 2022 г. в Telegram-каналах вирусилось дипфейк-видео Президента России Владимира Путина, в котором «он» заявил о заключении мира с Украиной и признании по итогам переговоров ее территории в границах с Луганской и Донецкой областями[1]. Годом позже в эфире ряда радиостанций и телеканалов транслировали другое обращение, где глава государства якобы объявил о введении военного положения в отдельных регионах и анонсировал всеобщую мобилизацию[2].

Не исключена возможность вброса в информационное пространство намеренно искаженной визуализации для публичных призывов к введению мер ограничительного характера в отношении Российской Федерации, граждан Российской Федерации или российских юридических лиц (ст. 284^2 УК РФ), развязывания агрессивной войны (ст. 354 УК РФ) и реабилитации нацизма (ст. 354^1 УК РФ). Под влиянием поддельных аудиовизуальных материалов, умышленно разгоняемых медиаресурсами, могут приниматься спонтанные, необдуманные решения по тематике международных отношений и внешней политики, способные поставить под угрозу мир и безопасность всего человечества. В информационном поле уже появлялось «обращение» к нации Дональда Трампа о ядерной атаке против

[1] В Telegram распространился дипфейк с заявлением Путина насчет Украины // Телерадиокомпания «Петербург». 2022. 28 февр. URL: https://www.5-tv.ru/news/377904/vtelegram-rasprostranilsa-dipfejk-szaavleniem-putina-nascet-ukariny/?ysclid=m64ww2r9op108966943 (дата обращения: 19.12.2024).

[2] «В некоторых регионах был взлом». Хакеры пустили «обращение Путина» в эфир ТВ и радио // Газета.Ru: сайт. 2023. 5 июня. URL: https://www.gazeta.ru/politics/2023/06/05/17092868.shtml?ysclid=m62ko3503c739617942 (дата обращения: 20.12.2024).

Северной Кореи [16, с. 102]. Североамериканский журнал Foreign Affairs («Форин афферс») опубликовал материалы с видеозаписями, на которых якобы американские генералы в Афганистане сжигают Коран, а премьер-министр Израиля в частных разговорах обсуждает план политических убийств лидеров Ирана [17].

Пробелы технико-юридического характера законопроекта

Законопроектные формулировки уголовно-правового запрета содержат ряд других существенных изъянов. К ним следует отнести разные варианты написания одного и того же отягчающего обстоятельства, предлагаемого для дополнения указанных составов преступлений. Поправки к четырем из них (ст. 128, 158, 159, 159[6] УК РФ) содержат одинаковую формулировку средства их совершения, а именно «с использованием изображения или голоса *потерпевшего или иного лица*». В ст. 163 УК РФ говорится уже о биометрии *потерпевшего или его близких*, а в ст. 165 УК РФ – о биометрии *известного потерпевшему лица*. Если правотворцы учитывали суть хищений, почему для вымогательства предусматривается категория «близкие потерпевшего», а для мошенничества нет? Ведь больше мошенническому обману свойственно использовать реалистичный «виртуальный клон» близких потерпевшему людей для психологического манипулирования с целью выманивания конфиденциальной информации и денежных средств. Необходимо продумать унифицированную версию текста предлагаемого для криминализации квалифицирующего признака.

Погрешностью законопроекта следует считать неясность понятия «фальсифицированные или искусственно созданные», которое может быть истолковано неоднозначно. Разве «фальсифицированные или искусственно созданные» аудио и видеоизображения при использовании дипфейк технологии – это не синонимичные понятия? Во всяком случае, норма должна сопровождаться пояснением (возможно в примечании), что означают оба термина. Усматривается и другое нарушение правил юридической техники в тексте законопроекта. В его редакции используется неудачный прием с разделительным союзом «или» (мошенничество, совершенное с использованием изображения *или* голоса), однако дипфейк – это в том числе симбиоз внешнего облика и голоса человека (видеоизображение с речью), потому следует указать и на соединительный союз «*и*» (и (или)). Думается, что новелла будет создавать сложности правоприменителю в отмежевании уголовно наказуемых деяний между собой ввиду отсутствия для этого четких критериев. Использование настоящих изображения и (или) голоса как биометрических персональных данных потерпевшего или иного лица как действие, описанное в предлагаемом законопроекте, может конкурировать в части уголовно-правовой оценки содеянного со ст. 272[1] «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения» (начала действовать с 30.11.2024[1]).

Для исключения сумятицы с составами преступлений, закладываемой на будущее проектом, если он будет принят, законодателю следует предложить реформировать институт отягчающих наказание обстоятельств. Чтобы новелла носила унифицированный и системный характер, необходимо дополнить ч. 1 ст. 63 УК РФ новым п. «ф» следующего содержания: «Совершение преступления с использованием персональных данных, специальных категорий персональных

[1] О внесении изменений в Уголовный кодекс Российской Федерации: Федер. закон от 30 нояб. 2024 г. № 421-ФЗ // Российская газета. 2024. 6 дек.

данных и (или) биометрических персональных данных, в том числе фальсифицированных технологией машинного обучения и (или) искусственного интеллекта». Тем самым указанное обстоятельство будет единым и универсальным инструментом, применяемым комплексно к тем деяниям, которые совершены с помощью любых персональных данных – «живых» и неоригинальных. Машинное обучение и искусственный интеллект при создании дипфейка различаются: первым используются алгоритмы, генерирующие новый контент из заданного набора. Они позволяют при помощи двухмерной или трёхмерной (2D, 3D) компьютерной графики (захват движений и мимики, копирование голоса, наложение текстур) изготовить или улучшить статичные или динамичные изображения (CGI) в видеоиграх, в искусстве, в печатных изданиях, в киноиндустрии и рекламе, в телепрограммах (персонажи, виртуальные миры, сцены и спецэффекты). Искусственный интеллект анализирует настоящую запись голоса и внешности человека и обучается тому, как он может выглядеть, говорить и двигаться, а затем создаёт новые видеоизображения по заданному сюжету.

Дополнительным аргументом «универсализации» отягчающего обстоятельства без локальных новаций в Особенную часть УК РФ выступает прогноз изменения «качества» преступности с персональными данными [18, с. 102; 19, с. 125; 20, с. 142]. В пояснительной записке к проекту его соавторы комментируют правотворческую инициативу специальной защиты голоса и внешности так: «Развитие компьютерных технологий привело к расширению возможностей по созданию видео- и аудиоматериалов на основе образцов изображений и голоса гражданина, искусственно воссоздающих несуществующие события. …Современные программно-аппаратные комплексы, а также использование нейросетей и искусственного интеллекта (технологии «дипфейк», «цифровые маски» и т. д.) позволяют создавать подделки, отличить которые от реальности неспециалисту практически невозможно. Те же технологии позволяют воспроизводить и иные биометрические персональные данные. Следует отметить, что изображение гражданина или его голос в различных ситуациях могут как относиться к биометрическим персональным данным, используемым в целях идентификации гражданина, так и не иметь такого статуса. Учитывая, что именно голос и изображение гражданина используются чаще всего для обмана, предлагается выделить их в отдельную категорию»[1].

В условиях новой цифровой реальности с переходом на удаленную идентификацию и аутентификацию по биометрии информационно-коммуникационные технологии будут аккумулировать огромные объёмы биометрической информации о людях. Развитие научных знаний в медицине (3D-культивирование органов для трансплантации, искусственные конструкции, биопечать, пересадка трансплантатов от генно-модифицированных животных и др.) изменит и виды биометрических персональных данных, потребующих повышенной уголовно-правовой защиты.

Существенный недостаток законопроекта № 718538-8 видится в том, что задуманные поправки в Уголовный кодекс по шести составам преступлений как нежизнеспособные не будут успевать за криминальной реальностью. Его авторам следует дополнить предлагаемый перечень теми преступлениями, которые, как показывает практика, уже совершаются с использованием дипфейка. В этой связи М.А. Желудков верно подмечает, что «в России необходимо создание особой системы цифровых и правовых форм защиты от дипфейков. Подобная трансформация потребует …полноценной ревизии

[1] Пояснительная записка к проекту № 718538-8 // Государственная Дума Рос. Федерации: сайт. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 12.12.2024).

всех нормативных актов, регулирующих использование биометрических данных человека. Изменения должны проходить не после создания объекта защиты, а в процессе его создания, где в защищаемый объект уже закладываются правовые процессы защищенности от дипфейков» [21, с. 270]. В этом смысле показательным является и опыт зарубежных стран, когда уголовное законодательство специально охраняет не только голос и изображение, внешний облик человека, а его иные биометрические характеристики. Примером может служить уголовное право США, где преступником признается тот, кто использует отпечатки пальцев, радужную оболочку или сетчатку глаза и другие физиологические данные человека для подмены («кражи») личности и мошеннического обмана (§18 U.S.C. §1028 (b)). Французский уголовный закон признает преступлением незаконное использование генетической информации другого человека (ст. 226-26).

Выводы

Подводя итоги исследованию, можно сделать *следующие выводы*:

1. Манипулятивный потенциал феномена дипфейк настолько разнообразен, что в качестве цели его использования как средства совершения преступления может быть что угодно. Его «инструментальная» роль в механизме преступного посягательства может выполняться в таких деяниях, как:

– *преступления против жизни* (доведение до самоубийства (ст. 110 УК РФ); склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110^1 УК РФ));

– *преступления против чести и достоинства личности* (клевета (ст. 128^1 УК РФ));

– *преступления против половой неприкосновенности и половой свободы личности* (понуждение к действиям сексуального характера (ст. 133 УК РФ); половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста (ст. 134 УК РФ));

– *преступления против конституционных прав и свобод человека и гражданина* (воспрепятствование осуществлению избирательных прав или работе избирательных комиссий (141 УК РФ); нарушение авторских и смежных прав (ст. 146 УК РФ); нарушение права на свободу совести и вероисповеданий (ст. 148 УК РФ));

– *преступления против собственности* (кража (ст. 158 УК РФ); мошенничество (ст. 159 УК РФ); мошенничество с использованием электронных средств платежа (ст. 159^3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ); вымогательство (ст. 163 УК РФ); причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ));

– *преступления в сфере экономической деятельности* (незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); манипулирование рынком (ст. 185^3 УК РФ));

– *преступления против общественной безопасности* (публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205^2 УК РФ); заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ); публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207^1 УК РФ); публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207^2 УК РФ); публичное распространение заведомо ложной информации об использовании Вооруженных сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в

выполнении задач, возложенных на Вооруженные силы Российской Федерации или войска национальной гвардии Российской Федерации (ст. 207^3 УК РФ));

– *преступления против здоровья населения и общественной нравственности* (вовлечение в занятие проституцией (ст. 240 УК РФ); получение сексуальных услуг несовершеннолетнего (ст. 240^1 УК РФ); незаконные изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ); изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242^1 УК РФ));

– *преступления в сфере компьютерной информации* (неправомерный доступ к компьютерной информации (ст. 272 УК РФ); незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272^1 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ));

– *преступления против основ конституционного строя и безопасности государства* (публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ); публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280^1 УК РФ); публичные действия, направленные на дискредитацию использования Вооруженных сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, исполнения государственными органами Российской Федерации своих полномочий, оказания добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные силы Российской Федерации или войска национальной гвардии Российской Федерации (ст. 280^3 УК РФ); публичные призывы к осуществлению деятельности, направленной против безопасности государства (ст. 280^4 УК РФ); возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ); неоднократные пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ст. 282^4 УК РФ); призывы к введению мер ограничительного характера в отношении Российской Федерации, граждан Российской Федерации или российских юридических лиц (ст. 284^2 УК РФ);

– *преступления против правосудия* (фальсификация доказательств и результатов оперативно-разыскной деятельности (ст. 303 УК РФ));

– *преступления против порядка управления* (подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков (ст. 327 УК РФ));

– *преступления против мира и безопасности человечества* (публичные призывы к развязыванию агрессивной войны (ст. 354 УК РФ)).

2. Во избежание конкуренции норм и необходимости внесения в уголовный закон новых дополнений, связанных с применением дипфейков, следует избрать иной, нежели предлагается законопроектом, подход – отнести использование рассматриваемой технологии к числу отягчающих обстоятельств.

Список литературы

1. Дремлюга Р.И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение: монография. М.: Юрлитинформ, 2022. 328 с.

2. Ситник В.Н. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // Уральский журнал правовых исследований. 2022. № 3(20). С. 76-83.

3. Ефремова М.А., Русскевич Е.А. Дипфейк и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 2 (56). С. 97-105.

4. Гришин Д.А., Клишина А.Д. О мошенничестве, совершаемом с использованием технологии «дипфейк» // Современное общество и личность: проблемы взаимодействия, вызовы и перспективы развития: сборник научных трудов по материалам Международной научно-практической конференции. Белгород: Агентство перспективных научных исследований (АПНИ), 2024. С. 9-13.

5. Бодров Н.Ф., Лебедева А.К. Уголовно-правовые и криминалистические аспекты противодействия распространению и использованию дипфейков в Российской Федерации // Криминалистика: вчера, сегодня, завтра. 2023. № 4. С. 42-55.

6. Воронин И.А., Гавра Д.П. Дипфейки: современное понимание, подходы к определению, характеристики, проблемы и перспективы // Российская школа связей с общественностью. 2024. № 33. С. 28-47.

7. Смирнов А.А. «Глубокие фейки». Сущность и оценка потенциального влияния на национальную безопасность // Свободная мысль. 2019. № 5 (1677). С. 63-84.

8. Порнографический дипфейк: вымысел или виртуальная реальность? / И.Н. Архипцев, А.Н. Александров, А.В. Максименко, К.И. Озеров // Социально-политические науки. 2021. Т. 11, № 1. С. 69-74.

9. McGlynn C. Towards a new criminal offence of intimate intrusions // Fem Leg Stud. 2024. Is. 32. P. 189-212.

10. Polyzoidou V. Digital violence against women: is there a real need for special criminalization? // Int. J. Semiot. Law. 2024. Is. 37. P. 1777-1797.

11. Deepfakes and digitally altered imagery abuse: a cross-country exploration of an emerging form of image-based sexual abuse / A. Flynn, A. Powell, A.J. Scott, E. Cama // The British Journal of Criminology. 2022. Vol. 62, is. 6. P. 1341-1358.

12. Chesney B., Citron D. Deep fakes: a looming challenge for privacy, democracy and national security // California Law Review. 2019. Vol. 107, is. 6. P. 1753-1820.

13. Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3(91). С. 107-116.

14. Савушкина М.А. Дипфейк как цифровое оружие гибридной войны // Вестник Омского университета. 2024. № 4(29). С. 45-54.

15. Mukherjee R. Mobile witnessing on WhatsApp: vigilante virality and the anatomy of mob lynching // South Asian Popular Culture. 2020. Vol. 18, is. 1. P. 79-101.

16. Harris D. Deepfakes: False pornography is here and the law cannot protect you // Duke Law & Technology Review. 2019. Vol. 17, is. 1. P. 99-128.

17. Chesney R., Citron D. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics // Foreign Affairs. 2018. December 11.

18. Алихаджиева И.С. Криминологические риски персональных данных: основные тенденции и прогнозы // Известия Юго-Западного государственного университета. Серия: История и право. 2023. № 13(3). С. 90-101.

19. Алихаджиева И.С. Персональные данные как предмет и средство совершения преступления // Пенитенциарная система и общество: опыт взаимодействия: сборник материалов XI Международной научно-практической конференции, посвященной 145-летию уголовно-исполнительной системы Российской Федерации. Пермь: Перм. ин-т ФСИН России, 2024. С. 125-129.

20. Хохлова Е.В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными // Вестник Тверского государственного университета. Серия: Право. 2022. № 3(71). С. 141-148.

21. 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. Саратов: Изд-во СГЮА, 2021. С. 269-270.

References

1. Dremlyuga R.I. Criminal and legal protection of the digital economy and information society from cybercrime attacks: doctrine, law, law enforcement. Moscow: Yurlitinform; 2022. 328 p. (In Russ.)

2. Sitnik V.N. Prospects of establishing criminal liability for crimes committed using deepfake technology. *Ural'skii zhurnal pravovykh issledovanii = Ural Journal of Legal Research*. 2022;(3):76-83. (In Russ.)

3. Efremova M.A., Russkevich E.A. Deepfake and criminal law. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia*. 2024;15(2):97-105. (In Russ.)

4. Grishin D.A., Klishina A.D. About fraud committed using deepfake technology. In: *Sovremennoe obshchestvo i lichnost': problemy vzaimodejstviya, vyzovy i perspektivy razvitiya: sbornik nauchnyh trudov po materialam Mezhdunarodnoj nauchno-prakticheskoj konferencii = Modern society and personality: problems of interaction, challenges and development prospects: a collection of scientific works based on materials from the International scientific and practical conference*. Belgorod: Agentstvo perspektivnyh nauchnyh issledovanij (APNI); 2024. P. 9-13. (In Russ.)

5. Bodrov N.F., Lebedeva A.K. Criminal law and criminalistic aspects of countering the spread and use of deepfakes in the Russian Federation. *Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow*. 2023;(4):42–55. (In Russ.)

6. Voronin I.A., Gavra D.P. Deepfeyki: modern understanding, approaches to definition, characteristics, problems and prospects. *Rossijskaya shkola svyazej s obshchestvennost'yu = Russian School of Public Relations*. 2024;(33):28-47. (In Russ.)

7. Smirnov A.A. “Deep fakes”. Essence and assessment of potential impact on national security. *Svobodnaya mysl' = Free thought*. 2019;(5):63-84. (In Russ.)

8. Arhipcev I.N., Aleksandrov A.N., Maksimenko A.V., Ozerov K.I. Pornographic deepfake: fiction or virtual reality? *Social'no-politicheskie nauki = Sociopolitical Sciences*. 2021;(11):69-74. (In Russ.)

9. McGlynn C. Towards a new criminal offence of intimate intrusions. *Fem. Leg. Stud*. 2024;(32):189-212.

10. Polyzoidou V. Digital violence against women: is there a real need for special criminalization? *Int. J. Semiot. Law*. 2024;(37):1777-1797.

11. Flynn A., Powell A., Scott A. J., Cama E. Deepfakes and digitally altered imagery abuse: a cross-country exploration of an emerging form of image-based sexual abuse. *The British Journal of Criminology*. 2022;62(6):1341-1358.

12. Chesney B., Citron D. Deep fakes: a looming challenge for privacy, democracy and national security. *California Law Review*. 2019;107(6):1753-1820.

13. Chukreev V.A. Personal data, including biometric data, as subjects of criminal law protection. *Vestnik Universiteta imeni O.E. Kutafina (MGYUA) = Courier of Kutafin Moscow State Law University (MSLA)*. 2022;(3):107-116. (In Russ.)

14. Savushkina M.A. Deepfake as a digital weapon of hybrid warfare. *Vestnik Omskogo universiteta = Herald of Omsk University*. 2024;(4):45-54. (In Russ.)

15. Mukherjee R. Mobile witnessing on whatsapp: vigilante virality and the anatomy of mob lynching. *South Asian Popular Culture*. 2020;18(1):79-101.

16. Harris D. Deepfakes: False pornography is here and the law cannot protect you. *Duke Law & Technology Review*. 2019;17(1):99-128.

17. Chesney R., Citron D. Deepfakes and the new disinformation war: the coming age of post-truth geopolitics. *Foreign Affairs*. 2018. December 11.

18. Alikhadzhieva I.S. Criminological risks of personal data: Main trends and forecasts. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2023;13(3):90-101. (In Russ.)

19. Alikhadzhieva I.S. Personal data as the object and means of committing a crime. In: *Penitentsiarnaya sistema i obshchestvo: opyt vzaimodeistviya: sbornik materialov XI Mezhdunarodnoi nauchno-prakticheskoi konferentsii, posvyashchennoi 145-letiyu ugolovno-ispolnitel'noi sistemy Rossiiskoi Federatsii = The penitentiary system and society: the experience of interaction: collection of materials of the XI International Scientific and Practical Conference dedicated to the 145th anniversary of the penal system of the Russian Federation*. Perm': Perm. in-t FSIN Rossii; 2024. P. 22-30. (In Russ.)

20. Khokhlova E.V. Social conditioning of criminal liability for crimes related to personal data. *Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Pravo = Herald of Tver State University. Series: Law.* 2022;(3):141-148. (In Russ.)

21. Zheludkov M.A. Studying the impact of new digital technologies on the determination of fraudulent actions (Deepfake technology). In: *Razvitie nauk antikriminal'nogo cikla v svete global'nyh vyzovov obshchestvu: sbornik trudov po materialam Vserossijskoj zaochnoj nauchno-prakticheskoj konferencii s mezhdunarodnym uchastiem = Development of the sciences of the anti-criminal cycle in the light of global challenges to society: a collection of works based on the materials of the All-Russian correspondence scientific and practical conference with international participation.* Saratov: Izd-vo SGYuA; 2021. P. 269-270. (In Russ.)

Информация об авторе / Information about the Author

Алихаджиева Инна Саламовна, доктор юридических наук, доцент, Российская криминологическая ассоциация имени Азалии Ивановны Долговой, г. Москва, Российская Федерация,
e-mail: Alins1@yandex.ru,
ORCID: 0000-0002-6998-930X

Inna S. Alikhadzhiyeva, Doctor of Sciences (Juridical), Associate Professor, Russian Criminological Association named after Azalea Ivanovna Dolgova, Moscow, Russian Federation,
e-mail: Alins1@yandex.ru,
ORCID: 0000-0002-6998-930X