**МОРОЗОВ ВИКТОР ИВАНОВИЧ**

*Профессор кафедры уголовно-правовых дисциплин*
*Тюменского государственного университета*
*v.i.morozov@utmn.ru*

**ЛОСЕВ СЕРГЕЙ ГЕННАДЬЕВИЧ**

*Доцент кафедры уголовно-правовых дисциплин*
*Тюменского государственного университета*
*s.g.losev@utmn.ru*

# УГОЛОВНО-ПРАВОВАЯ ОЦЕНКА ИСПОЛЬЗОВАНИЯ «ДИПФЕЙКА» ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ

**Аннотация.** В настоящий момент в России наблюдается взрывной рост хищений, совершаемых путем мошенничества с использованием информационно-коммуникационных технологий. Всего рост с начала 2020 года дошел до троекратной разницы. Одним из способов совершения данный преступлений в последнее время все более становится использование достижений цифровых технологий — возможность редактирования видеоизображений и звука с целью ввести в заблуждение потерпевших. Данный способ уже вызвал реакцию законодателей — сенатором А.К. Пушковым был внесен законопроект, который предусматривает внесение в статьи 128.1, 159, 159.3, 163 и 165 УК РФ нового квалифицирующего признака — с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием биометрических персональных данных потерпевшего или иного лица. Однако, как представляется, проблема использования «дипфейков» в преступных целях стоит гораздо шире, чему посвящена настоящая статья.

**Ключевые слова:** дипфейк, преступления в цифровом пространстве, кибермошенничество.

**MOROZOV VIKTOR IVANOVICH**

*Professor of the Department of Criminal Law Disciplines*
*University of Tyumen*

**LOSEV SERGEY GENNADIEVICH**

*Associate Professor of the Department of Criminal Law Disciplines*
*University of Tyumen*

# CRIMINAL-LEGAL ASSESSMENT OF THE USE OF “DEEPFAKE” IN COMMITTING CRIMES

**Abstract.** At the moment in Russia there is an explosive growth of thefts committed by fraud using information and communication technologies. The total growth since the beginning of 2020 has reached a threefold difference. One of the ways of committing this crime in recent times is increasingly becoming the use of advances in digital technology — the ability to edit video images and sound in order to mislead victims. This method has already provoked the reaction of legislators — Senator A.K. Pushkov introduced a bill that provides for the introduction of a new qualifying feature in Articles 128.1, 159, 159.3, 163 and 165 of the Criminal Code of the Russian Federation — using the image or voice (including falsified or artificially created) of the victim or another person, as well as using biometric personal data of the victim or another person. However, it seems that the problem of using “deepfakes” for criminal purposes is much wider, which is the subject of this article.

**Key words:** deepfake, crimes in digital space, cyberfraud.

Преступность всегда отличалась способностью адаптироваться к условиям окружающего мира в целях наиболее эффективной «эксплуатации» общества. Одним из способов совершения преступлений стала трансформация изображения

Термин дипфейк (Deepfake) (от словосочетания deep learning (глубинное обучение) и fake (фейк, подделка). Глубинное обучение — это метод на базе т.н. «искусственного интеллекта», который использует многоуровневые алгоритмы для осуществления все более сложных преобразований данных. Один из примеров дипфейка с участием знаменитостей — видео, выложенное актером Д. Пилом, который записал небольшую речь голосом Барака Обамы, совмещенную с видеосъемкой выступления этого политика.

В настоящее время подобные редактированные записи используются для совершения самых разнообразных преступлений. По мнению российских экспертов, данную схему уместно назвать «ложные боссы», потому что объектом подделки выступают руководитель потерпевших.

Например, у директора британской энергетической компании мошенники смогли выманить 220 000 евро с помощью имитации голоса руководителя головной компании, якобы запросившего срочно перевести указанную сумму — подмена была настолько похожей, что обманутый директор не стал перепроверять информацию[1].

Известной атакой с использованием дипфейка стал инцидент в банке в Гонконге в 2020 году: менеджеру позвонил «директор компании» с просьбой об авторизации перевода, так как компания собирается совершить поглощение. Дополнительно он получил электронное письмо, подписанное директором и юристом, которое выглядело как настоящее. Менеджер осуществил перевод. Следователи смогли отследить украденные средства и выяснили, что в мошенничестве было задействовано 17 человек[2].

Необходимо отметить, что примеры использования сгенерированных сообщений отмечаются и в России.

Так, глава г. Березовского Свердловской области Е. Писцов сообщил, что мошенники стали писать и звонить от его имени. С помощью «искусственного интеллекта» преступникам удалось сымитировать его голос[3].

Указанные дипфейки использовались для совершения корыстных преступлений, однако с помощью фальсифицированных файлов совершались посягательства и на иные объекты уголовно-правовой охраны: так, директор департамента информации и печати МИД России Мария Захарова в свое время стала невольной героиней подобного ролика, в котором «заявляла» о готовности России передать Запорожскую АЭС Украине в обмен на уход ВСУ из Курской области.

А в преддверии 1 сентября в сети появился новый дипфейк с врио губернатора Курской области Алексеем Смирновым, в котором он якобы сообщил жителям региона об отмене начала учебного года и призвал их покинуть регион[4].

Как представляется, указанные действия должны квалифицироваться как посягательства на конституционный строй и безопасности государства, так как целю совершения данных «публикаций», на наш взгляд, было причинение ущерба обороноспособности страны.

Также дипфейки могут использоваться для посягательств на личность. Одним из видов таких преступлений можно назвать создание эротических и порнографических изображений или клипов. Дипфейк-порно — это форма порнографического контента, создаваемая с помощью дипфейков. Дипфейк-технология используется для замены лиц или тел людей в видеозаписях с другими людьми[5].

Возникает резонный вопрос — может ли отечественный законодатель игнорировать отмеченные тенденции в криминальной активности?

Как представляется, ответ должен быть отрицательным. Игнорирование прогресса информационных технологий только облегчит совершение преступлений различным видам преступников, в том числе организованным.

Рассматривая создание дипфейка с позиции уголовного права, можно указать, что результаты его создания являются предметом преступления либо орудием его совершения. В первом случае речь идет, например, о ст. 128.1 УК РФ, а во втором случае — о преступлении, предусмотренном ст. 159 УК РФ.

---

[1]Мошенники массово дурят россиян с помощью нейросетей. Разбираемся, как защититься. URL: https://74.ru/text/criminal/2024/02/11/73213283/ (дата обращения:19.10.2024).

[2] В ногу с дипфейками: применение технологии и этические аспекты. URL: https://habr.com/ru/companies/sberbank/articles/848772/(дата обращения:19.10.2024).

[3] «Меня сейчас вызывают на ковер»: мошенники атаковали подписчиков и коллег уральского мэра. URL: https://www.e1.ru/text/incidents/2024/01/31/73179164/?ysclid=m3lmfddby1880361727 (дата обращения: 19.10.2024).

[4] Смотри в оба: как не стать жертвой дезинформации и уметь определять дипфейки. URL: https://tass.ru/obschestvo/22060857 (дата обращения: 19.10.2024).

[5] В сети участились случаи кражи данных с сайтов по созданию эротических дипфейков. URL: https://klops.ru/other/2024-10-08/305842-v-seti-uchastilis-sluchai-krazhi-dannyh-s-saytov-po-sozdaniyu-eroticheskih-dipfeykov?ysclid=m20l2ghpz4708157810.(дата обращения: 19.10.2024).

14 сентября 2024 года сенатором Пушковым А.К. был внесен законопроект, который предусматривает внесение в статьи 128.1, 159, 159.3, 163 и 165 УК РФ нового квалифицирующего признака — с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием биометрических персональных данных потерпевшего или иного лица. В пояснительной записке указывалось, 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[1].

В отзыве на законопроект, который дал Верховный суд РФ, указывается, что автор законопроекта не обосновал общественную опасность нового квалифицирующего признака, вследствие чего отзыв на законопроект был отрицательным.

Однако, как представляется, в пояснительной записке недвусмысленно описывалась главная характеристика «дипфейка» — сложность его распознавания даже лицу, обладающему специальными знаниями, особенно когда речь идет о редактировании записей, сделанных в плохом качестве.

Как можно учитывать данный способ совершения преступления в тексте уголовного закона?

Первый путь — криминализация в целом создания дипфейков в целях совершения преступлений. Таким образом, можно говорить о введении в состав УК РФ ст. 272.1 УК РФ — «Неправомерное модифицирование цифровой (компьютерной) информации». Однако, как представляется, такой способ усиления ответственности плохо учитывает специфику каждого преступления, которое совершается с помощью дипфейка. Также недостатком указанной статьи можно назвать то обстоятельство, что её будет сложно отграничить от состава ст. 272 УК РФ, что приведет к ситуации т.н. «сцепленной совокупности»[2], когда вменять в вину сразу совокупность преступлений, независимо от числа совершенных деяний.

Во-вторых, данный прием совершения преступления можно учесть в качестве признака основного состава. Так в ст. 281 УК РФ уместно указать в качестве способов совершения преступления распространение сообщений с целью дезинформировать или запугать население.

В-третьих, можно рассматривать использование дипфейка как способ совершения преступления, который отягчает ответственность. Так, в качестве квалифицирующего признака мошенничества можно указать использование сгенерированной цифровой (компьютерной) информации.

И, наконец, в-четвертых, целесообразно дополнить положения ч. 1 ст. 63 УК РФ пунктом, в который включить в качестве признака, отягчающего ответственность использование сгенерированной цифровой (компьютерной) информации.

Каким же образом можно использовать дипфейки в совершении разнообразных преступлений?

В случае посягательств на личность можно указать, на состав, предусмотренные ст. 128.1 УК РФ. Представляется, что в случае совершения клеветы общественная опасность данного преступления повышается в силу того, что «дипфейк» создает сильную эмоциональную вовлеченность, которая повышает восприимчивость к ложной информации. Следовательно, можно говорить о повышенной общественной опасности данного способа совершения преступления, что вызывает необходимость ввести новый квалифицированный состав. Также следует поступить и в отношении преступлений, предусмотренных ст. 298.1 (клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения). Аналогично и в случае вовлечения несовершеннолетнего в совершение преступлений дипфейк всего лишь способ психологического насилия и не повышает общественную опасность данного способа вовлечения.

В том случае, если речь о совершении посягательств против собственности, то содеянное можно квалифицировать либо по ст. 159.3 УК РФ, когда потерпевшего вводят в заблуждение относительно личности того, кто просит перевести деньги и в этом случае можно говорить о повышенной общественной опасности данных деяний, просто в силу того, что потерпевшему сложно

[1] URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 19.10.2024).

[2] Лопашенко Н. А. Преступления в сфере экономической деятельности: теоретический и прикладной анализ: монография: в 2 ч. М.: Юрлитинформ, 2015. Ч. 1. С. 27.

отличить признаки мошенничества без специальной подготовки. В случае же совершения вымогательства дипфейк-шантаж не отличается от обычного шантажа.

В случае совершения посягательств на общественную безопасность то к числу преступлений, которые могут быть совершены посредством дипфейков можно отнести реальную угрозу совершения террористических актов (ст. 205 УК РФ), 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 общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2 УК РФ), публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации (ст. 207.3 УК РФ). Как думается, использование дипфейка вряд ли повышает общественную опасность деяния и не требует введения квалифицированных составов в указанные статьи. Однако, в случае если в качестве личности для создания дипфейка используется какое-то известное лицо, то содеянное требует дополнительной квалификации по ст. 128.1 УК РФ.

Аналогично, в случае совершения какого из преступления, предусмотренного ч. 3 ст. 212 УК РФ или ст. 230 УК РФ. Однако, нужно учитывать направленность умысла лиц, создающих указные ролики, примером чему может служить ролик с участием известного актера В. Зеленского, в котором он, в результате искусного монтажа, признавался в систематическом употреблении кокаина.

Набольшее внимание заслуживают составы преступлений против государственной власти.

К таковым можно отнести 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 (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). В силу совершения данных преступлений способом распространения информации, то учитывать создание дипфейков следует аналогично преступлениям против общественной безопасности.

Таким образом, учет наших предложений позволит, на наш взгляд, повысит эффективность использования уголовно-правовых средств в противодействии использованию «дипфейков» при совершении преступлении.

**СПИСОК ЛИТЕРАТУРЫ**


1. В ногу с дипфейками: применение технологии и этические аспекты. — URL: https://habr.com/ru/companies/sberbank/articles/848772/ (дата обращения: 19.10.2024).
2. В сети участились случаи кражи данных с сайтов по созданию эротических дипфейков — URL: https://klops.ru/other/2024-10-08/305842-v-seti-uchastilis-sluchai-krazhi-dannyh-s-saytov-po-sozdaniyu-eroticheskih-dipfeykov?ysclid=m20l2ghpz4708157810 (дата обращения: 19.10.2024).
3. Лопашенко, Н. А. Преступления в сфере экономической деятельности: теоретический и прикладной анализ: монография: в 2 ч. / Н. А. Лопашенко. — Москва: Юрлитинформ, 2015. — Ч. 1. — 215 с.
4. «Меня сейчас вызывают на ковер»: мошенники атаковали подписчиков и коллег уральского мэра. — URL: https://www.e1.ru/text/incidents/2024/01/31/73179164/?ysclid=m3lmfddby1880361727 (дата обращения: 19.10.2024).
5. Мошенники массово дурят россиян с помощью нейросетей. Разбираемся, как защититься. — URL: https://74.ru/text/criminal/2024/02/11/73213283/ (дата обращения: 19.10.2024).
6. Смотри в оба: как не стать жертвой дезинформации и уметь определять дипфейки. — URL: https://tass.ru/obschestvo/22060857 (дата обращения: 19.10.2024).