МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ДИПФЕЙКОВ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПО СТ. 159 УК РФ И ПЕРСПЕКТИВЫ ЗАКОНОДАТЕЛЬНОГО РЕГУЛИРОВАНИЯ

Р.Р. Зямилева, *студент*
А.О. Мартынова, *студент*
Научный руководитель: *Г.З. Ситдикова, д-р юрид. наук, доцент*
Уфимский университет науки и технологий
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2026-5-2-203-207

Аннотация. *В работе рассматриваются особенности квалификации мошеннических действий, совершаемых с применением технологий дипфейков, в контексте статьи 159 Уголовного кодекса Российской Федерации. Анализируются сложности правоприменительной практики, связанные с определением признаков обмана, установлением субъективной стороны преступления, а также выбором способа его совершения. Обосновывается необходимость дальнейшего развития уголовного законодательства, включая возможное закрепление специальных квалифицирующих признаков, учитывающих использование технологий искусственного интеллекта.*

Ключевые слова: *мошенничество; дипфейк; искусственный интеллект; уголовное право; квалификация преступлений; цифровые технологии.*

Стремительное развитие технологий искусственного интеллекта, особенно генеративных моделей, обусловило появление такого явления, как дипфейки – высокореалистичные аудио- и видеоматериалы, имитирующие внешность и голос конкретного человека. Подобные технологии находят применение не только в сфере развлечений, но и используются в противоправной деятельности, в том числе при совершении мошенничества.

В связи с этим возрастает значимость уголовно-правовой оценки таких деяний. Несмотря на технологическую специфику, указанные действия посягают на традиционный объект уголовно-правовой охраны – общественные отношения, связанные с защитой права собственности, что позволяет квалифицировать их по статье 159 Уголовного кодекса Российской Федерации.

Согласно части 1 статьи 159 Уголовного кодекса Российской Федерации Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [1].

Ключевыми признаками состава являются:

1) непосредственный объект – общественные отношения по защите права собственности;

2) объективная сторона – хищение или приобретение права на чужое имущество, путем обмана или злоупотребление доверием;

3) субъект – вменяемое лицо, достигшее возраста уголовной ответственности, в данном случае достигшее 16 лет;

4) субъективная сторона – прямой умысел и корыстная цель, здесь прямой умысел выражается в осознании виновным, что он похищает чужое имущество путем обмана или злоупотребления доверия, предвидит, что его действия неизбежно приведут к нарушению права собственности и причинят материальный ущерб и желает наступления указанных последствий и целенаправленно стремится к противоправному обогащению за счёт другого лица.

Мошенничество характеризуется тем, что потерпевший самостоятельно передает имущество, находясь под воздействием введения в заблуждение.

Дипфейки являются разновидностью синтетического медиаконтента, формируемого с применением нейросетевых технологий. Их отличительной чертой выступает высокий уровень реалистичности, который существенно осложняет распознавание поддельного характера таких материалов.

Термин «дипфейк» был введен в 2017 г. на платформе Reddit и первоначально обозначал

подмену изображения лица с применением алгоритмов искусственного интеллекта (ИИ) для генерации новых, реалистично выглядящих изображений. Развитие технологий привело к выходу за рамки статичных визуальных манипуляций: современные алгоритмы синтезируют не только изображение, но и голос, создавая аудио- и видеоконтент с использованием внешности или тембра иного лица. Для этого не требуется глубоких технических знаний или дорогостоящего оборудования: ряд мобильных приложений позволяет сформировать дипфейк-ролик за считанные минуты [2].

Дипфейк-мошенничество – это форма хищения, при которой злоумышленники используют технологии синтеза изображения или голоса (так называемые дипфейки), чтобы ввести человека в заблуждение относительно личности говорящего или реальности происходящего.

Жертва убеждается, что взаимодействует с реальным знакомым, родственником или официальным лицом, тогда как на самом деле имеет дело с подделкой. В такой ситуации легко поддаться обману: современные дипфейки очень качественно имитируют не только голос, но и внешность близкого человека.

Очень часто злоумышленники совмещают использование дипфейков со взломом аккаунта в социальных сетях – это делает обман особенно трудно распознаваемым. Кажется, что вам пишет знакомый или даже очень близкий человек, но в итоге оказывается, что это мошенник, который завладел не только аккаунтом, но и, по сути, цифровой «личностью» этого человека.

Как правило, такое мошенничество осуществляется дистанционно: злоумышленник связывается с потерпевшим по телефону или через интернет, нередко имитируя голос близкого человека (например, родственника, якобы попавшего в беду). Под предлогом срочной ситуации он требует перевести деньги или передать их иным способом. При этом потерпевшего обычно не побуждают к личной встрече или перемещению – вся коммуникация происходит удалённо. В контексте мошенничества можно выделить следующие типичные схемы:

1. Имитация голоса руководителя – распоряжение о переводе средств сотруднику бухгалтерии;

2. Подделка видеозвонка – убеждение жертвы в подлинности личности злоумышленника;

3. Фальсификация личности в социальных сетях – создание доверительных отношений и последующее хищение средств.

Рассматривая реальную практику в Ново-Савиновский суд Казани поступило дело курьера кибермошенника. Пожилая жительница Казани рассказала, что мошенникам удалось по телефону подделать голос ее подруги, которую она знает уже больше 60 лет. Женщина, чтобы помочь подруге, отдала курьеру полмиллиона, которые получила от продажи дачи [3, с. 403].

Согласно открытым статистическим данным, около 80% россиян опасаются возможных злоупотреблений технологиями deep fake и краж биометрических данных [4, с. 108].

Несмотря на то, что дипфейк объективно является формой обмана, возникает вопрос: является ли он новым способом или лишь разновидностью уже известных форм введения в заблуждение. Традиционно обман трактуется как сообщение ложных сведений или сокрытие истины. Однако дипфейки создают иллюзию реальности, что затрудняет разграничение:

1) обмана как интеллектуального воздействия;

2) технической подделки как способа воздействия.

Возникает вопрос: следует ли квалифицировать такие действия как обычное мошенничество или как особую форму, требующую отдельного регулирования.

По мнению директора Центра цифровой экономики и финансовых инноваций профессора Ж.Л. Сидоренко, предложение о дополнении уголовного законодательства квалифицированном составом об использовании дипфейков, является обоснованным, но скорее будет логичным использовать термин не «дипфейки», а «цифровые технологии» применительно к мошенничеству, дабы не ограничивать только «дипфейками» сферу применения особо квалифицированного мошенничества [5, с. 30].

Для квалификации мошенничества необходимо доказать прямой умысел и корыстную цель. В случаях с дипфейками усложняется установление:

1) личности виновного (анонимность цифровой среды);

2) осознания потерпевшим факта обмана;

3) связи между созданием дипфейка и наступившими последствиями.

Действующая редакция ст. 159 УК РФ не учитывает использование высокотехнологичных средств как обстоятельство, повышающее общественную опасность деяния. Представляется целесообразным дополнить ст. 159 УК РФ указанием на совершение мошенничества с использованием технологий искусственного интеллекта или цифровой имитации личности.

Стремительное развитие технологий искусственного интеллекта и их внедрение в повседневную коммуникацию обуславливают необходимость не точечных, а системных изменений в уголовном законодательстве. Использование дипфейков в мошеннических схемах демонстрирует, что традиционные конструкции уголовного права, сформированные в доцифровую эпоху, требуют модернизации. Наиболее эволюционным и практически реализуемым подходом является дополнение действующей редакции нормы о мошенничестве новым квалифицирующим признаком – совершение преступления с использованием технологий искусственного интеллекта, включая дипфейки.

Во-первых, использование дипфейков существенно повышает степень общественной опасности деяния. В отличие от традиционного обмана, здесь задействуются высокотехнологичные средства, создающие практически неотличимую от реальности иллюзию. Это снижает критическое восприятие информации потерпевшим и увеличивает вероятность причинения ущерба.

Во-вторых, подобный способ совершения преступления усложняет его раскрытие и расследование. Следовательно, он должен учитываться при дифференциации уголовной ответственности.

Возможная формулировка: «…совершенное с использованием технологий искусственного интеллекта, направленных на имитацию личности (в том числе с применением дипфейков)…».

Помимо вышеуказанного, альтернативной, более радикальной моделью является введение в УК РФ отдельной нормы, предусматривающей ответственность за незаконное создание и использование дипфейков. Аргументы в пользу введения отдельной нормы:

1. Самостоятельная общественная опасность. Дипфейк может причинять вред не только в рамках мошенничества, но и, например, при дискредитации личности, распространении ложной информации, шантаже.

2. Превентивная функция. Криминализация самого факта создания вредоносного дипфейка (при наличии цели причинения вреда) позволит пресекать преступление на ранней стадии.

3. Гибкость регулирования. Возможность дифференцировать ответственность в зависимости от последствий (имущественный ущерб, вред репутации, угрозы безопасности).

Таким образом, мошенничество с использованием дипфейков представляет собой качественно новый вызов для уголовного права, находящегося на стыке традиционных правовых конструкций и стремительно развивающихся технологий искусственного интеллекта.

В современном обществе искусственный интеллект активно проникает во все сферы жизни человека. Наряду с полезными функциями он может быть использован и в преступных целях. В связи с этим возникает необходимость совершенствования законодательства, регулирующего вопросы противодействия преступлениям с применением технологий на базе искусственного интеллекта.

Анализ диспозиции, указанной в статье 159 Уголовного Кодекса РФ на данный момент, относит действия подобного характера к мошенничеству. Но рассматриваемая статья не предусматривает всех особенностей, которые порождает использование искусственного интеллекта в сфере нарушения права собственности, путем хищения с помощью обмана. Это вызывает проблемы при сборе доказательств, их фиксации, а также сложность определении виновного лица. По данным деяниям нет единой практики, что вызывает сложности при их квалификации.

На наш взгляд необходимо усовершенствования законодательства в сфере мошенничества, поскольку наше общество стремительно развивается, законы тоже должны быть динамичными и соответствовать реалиям. Есть несколько решений:

1) Добавить в качестве квалифицирующего признака в состав ст. 159 УК РФ, часть, в которой будет указано применение технологий, позволяющих использовать чужой голос и внешность, то есть дипфейков

2) Введение в Уголовный Кодекс отдельной нормы, посвященной данному преступлению. То есть состава, который будет регулировать именно те преступления, которые связаны с применением технологий на базе искусственного интеллекта, в том числе и мошенничество с дипфейками.

Подводя итог, следует отметить, что такая разновидность мошенничества все чаще встречается в современном обществе. В интернете полно историй, где подобного рода мошенники обманывают население. И, к сожалению, наше законодательство пока не в полной мере отрегулировало данную проблему.

С каждым днем общественная опасность мошенничества с использованием технологий, позволяющих менять свою внешность и голос, возрастает. Основная проблема в том, что даже современная молодежь, разбирающаяся в технологиях и активно пользующаяся искусственным интеллектом, не всегда может распознать обман, а пожилое население страны, которое чаще всего и становится жертвой обмана и не разбирающееся в новых технологиях тем более. Поэтому необходимо усовершенствование норм уголовного права, с целью защиты имущественных прав граждан, а также снижение рисков для наиболее уязвимых категорий населения.

Таким образом, предлагаемые нами решения позволят сформировать более четкое регулирование в данной сфере и обеспечит быстрое реагирование на подобного рода преступления.

Библиографический список

1. Уголовный Кодекс Российской Федерации. – [Электронный ресурс]. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/.

2. Асадов Р.Б. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // Полицейская и следственная деятельность. – 2025. – № 4. – С. 16-36. – DOI: 10.25136/2409-7810.2025.4.75462 EDN: MFCNUV.

3. Талан М. В Уголовно-правовая охрана экономических интересов как основа функционирования семьи // Семья и традиционные семейные ценности как духовно-нравственная основа развития общества и государства: сб. материалов Междунар. науч. практ. конф., Чебоксары, 18-20 апреля 2024. – Чебоксары: Чувашский государственный университет имени И.Н. Ульянова, 2024. – С. 402-408.

4. Малышева Ю.Ю. Мошеннические проявления фейков и дипфейков: проблемы противодействия // Российско-азиатский правовой журнал. – 2025. – № 1.

5. Сидоренко Э.Л. Криптовалюта и будущее цифровых финансов. – М.: МГИМО МИД России, 2023. – 36 с. – EDN WDGHIN.

FRAUD USING DUPES: PROBLEMS OF QUALIFICATION UNDER ARTICLE 159 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION AND PROSPECTS FOR LEGISLATIVE REGULATION

R.R. Zyamileva, *Student*
A.O. Martynova, *Student*
Supervisor: *G.Z. Sitdikova, Doctor of Legal Sciences, Associate Professor*
Ufa University of Science and Technology
(Russia, Ufa)

Abstract. *The paper examines the features of the qualification of fraudulent actions committed using deepfake technologies in the context of Article 159 of the Criminal Code of the Russian Federation. The paper analyzes the difficulties of law enforcement practice related to the definition of the signs of deception, the establishment of the subjective aspect of the crime, and the choice of the method of committing the crime. The paper substantiates the need for further development of criminal legislation, including the possible establishment of special qualifying features.*

Keywords: *fraud; deepfake; artificial intelligence; criminal law; qualification of crimes; digital technologies.*