

ГОНЫШЕВ Максим Алексеевич,
аспирант кафедры гражданского
права и процесса юридического факультета
ФГБОУ ВО «Оренбургский государственный университет»,
г. Оренбург,
e-mail: maximu13@mail.ru

ПРАВОВАЯ ОТВЕТСТВЕННОСТЬ ЗА СОЗДАНИЕ, РАСПРОСТРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ДИПФЕЙКОВ И СИНТЕТИЧЕСКИХ ГОЛОСОВ В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье рассматриваются проблемы правовой ответственности за создание, распространение и использование синтетических медиа – дипфейков (deepfakes) и искусственно сгенерированных (клонированных) голосов в условиях активного развития технологий искусственного интеллекта. Актуальность темы обусловлена ростом числа дипфейков в интернете и связанными с ними рисками нарушения прав граждан, дезинформации и мошенничества. Проанализировано современное состояние правового регулирования в России и за рубежом (ЕС, США, Китай), выявлены пробелы в законодательстве и правоприменении. На основе исследований ведущих ученых и зарубежного опыта предлагаются меры по совершенствованию российского законодательства, в том числе введение юридического определения дипфейка, обязанностей по маркировке синтетического контента и установление ответственности за его намеренное использование.

Ключевые слова: дипфейк, синтетический голос, искусственный интеллект, правовое регулирование, ответственность, дезинформация, законодательство России, зарубежный опыт.

GONYSHEV Maxim Alekseevich,
is a postgraduate student at the Department
of Civil Law and Process, Faculty of Law,
Orenburg State University, Orenburg

LEGAL RESPONSIBILITY FOR THE CREATION, DISTRIBUTION AND USE OF DEEPFAKES AND SYNTHETIC VOICES IN THE CONTEXT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Annotation. The article examines issues of legal liability for the creation, dissemination and use of synthetic media – deepfakes and artificially generated (cloned) voices in the context of rapid development of artificial intelligence technologies. The relevance of the topic is driven by the growth of deepfakes online and the associated risks of citizens' rights violations, disinformation and fraud. The current state of legal regulation in Russia and abroad (EU, USA, China) is analyzed, gaps in legislation and law enforcement are identified. Based on leading scholars' research and foreign experience, measures are proposed to improve Russian legislation – including introducing a legal definition of deepfake, obligations to label synthetic content, and establishing liability for its malicious use.

Key words: deepfake, synthetic voice, artificial intelligence, legal regulation, liability, disinformation, Russian legislation, foreign experience.

Широкое распространение технологий «глубоких фейков» (от англ. deepfake – медиаконтента, созданного нейросетями для правдоподобной имитации реальных людей) стало одним из серьёзных вызовов цифровой

эпохи. Возможность достоверно подделывать облик и голос человека несёт существенные угрозы для прав личности, общественной безопасности и информационного пространства. Уже сегодня фиксируется стремительный рост числа

таких подделок: например, в 2023 году в интернете обнаружено втрое больше видеодипфейков и в восемь раз больше аудиодипфейков по сравнению с предыдущим годом[1]. Дипфейки используются злоумышленниками для клеветы, мошенничества, манипулирования общественным мнением и иных противоправных целей. Вместе с тем они находят и легитимное применение (например, в киноиндустрии для воссоздания образов актёров или в создании персональных цифровых аватаров), что серьёзно осложняет задачу правового регулирования.

Актуальность проблемы подтверждается повышенным вниманием учёных и законодателей. В зарубежной литературе указывается на «распад правды»[2] в информационной среде и появление новых угроз правам человека, порожаемых дипфейками[3]. В России также появились исследования (Н. В. Архиреев, В. В. Виноградов, Д. Ю. Трофимов и др.), посвящённые правовым аспектам технологии *deepfake*, однако законодательная реакция пока отстаёт от технологического прогресса. Широко дискутируется, как противодействовать злоупотреблениям дипфейком, не нарушая при этом фундаментальные права – свободу слова, неприкосновенность частной жизни, интеллектуальную собственность и т.д. Для выработки адекватного правового ответа следует сначала определить, что представляет собой эта технология и какие угрозы она несёт.

Термин «дипфейк» обозначает методику создания сфальсифицированных изображений или видео с использованием алгоритмов глубокого обучения. По сути, нейросеть, обученная на большом массиве фотографий или видеозаписей человека, способна синтезировать чрезвычайно правдоподобное изображение его лица либо имитацию речи. Обычно для генерации дипфейков применяются генеративно-состязательные нейросети (GAN), где две модели – генератор и дискриминатор тренируются в соревновании: генератор создаёт фальшивый контент, а дискриминатор пытается отличить его от подлинного. Итогом такого обучения становятся фото, видеоролики или аудиозаписи, практически неотличимые от настоящих.

Синтетический (клонированный) голос является частным случаем дипфейка, когда на основе образцов речи реального человека создаётся искусственная запись, имитирующая его голос для произнесения заданного текста. Юридически такие имитации голоса порождают те же вопросы, что и визуальные дипфейки. Как отмечает Н. В. Архиреев, с правовой точки зрения имитация голоса человека практически не отличается от имитации его внешнего облика[4]. Тем не менее, в российском законодательстве пока нет нормы,

прямо регулирующей копирование голоса, и остаётся открытым вопрос, считать ли голос охраняемыми персональными данными либо нематериальным благом гражданина[4]. В отсутствие прямого регулирования несанкционированное использование чужого образа или голоса без согласия затрагивает конституционное право каждого свободно распоряжаться своей личностью и создаёт предпосылки для злоупотреблений.

Дипфейк-технологии затрагивают сразу несколько отраслей права – уголовное, гражданское, информационное, законодательство о персональных данных, избирательное и др. Соответственно, если вводить в правовое поле определение дипфейка, оно должно быть достаточно широким и технически выверенным, чтобы охватить различные формы синтезированного медиа, одновременно разграничивая правомерные случаи использования (пародии, творчество, эксперименты) и неправомерные (клевета, мошенничество и т.д.).

Риски, связанные с применением дипфейков, чрезвычайно разнообразны по природе и тяжести последствий. Прежде всего это угрозы правам и свободам личности. Правдоподобные поддельные видео- и аудиозаписи способны нанести серьёзный урон чести, достоинству и деловой репутации граждан. Например, с помощью дипфейка злоумышленники могут вложить в уста человека ложные оскорбительные либо порочащие высказывания или сгенерировать компрометирующее видео, по сути, новую форму клеветы, усиленную тем, что визуальный образ жертвы делает ложь более убедительной. Отмечены также случаи телефонного мошенничества с использованием клонированного голоса руководителя, когда у сотрудников выманивались крупные суммы денег. Кроме того, дипфейки позволяют обходить биометрическую аутентификацию, что приводит к прямому имущественному ущербу и подрывает доверие к цифровым системам безопасности.

Существенные риски связаны и с угрозами публичным интересам, зависящим от достоверности информации. Дипфейки становятся инструментом массовой дезинформации и манипуляции общественным мнением. Фальшивые заявления от лица политиков или знаменитостей способны влиять на электоральные настроения, разжигать рознь либо провоцировать панику. Эксперты предупреждают о «дивиденде лжеца»: осознание того, что любое медиа может быть сфальсифицировано, подрывает доверие общества даже к реальным новостям.

Отдельную тревогу вызывают риски киберпреступности. Злоумышленники применяют синтетический медиаконтент для новых схем мошен-

ничества и вымогательства, нарушения приватности, нелегитимного сбора данных и шантажа. Кроме того, распространение дипфейков затрудняет работу правоохранительных органов и судов, если аудио- и видеодоказательства перестают восприниматься как достоверные из-за риска их подделки. Подрыв информационной достоверности представляет опасность для национальной безопасности.

Подводя итог, дипфейки и клонированные голоса обладают двоякой природой. С одной стороны, эти технологии открывают новые полезные возможности (в медицине, образовании, творчестве и т.д.), но с другой порождают качественно новые угрозы неправомерного вмешательства в частную жизнь, распространения недостоверных сведений и совершения преступлений. Эти угрозы уже проявились на практике и будут расти по мере совершенствования технологий, что создаёт настоятельную необходимость адекватного правового ответа как со стороны национального законодательства, так и посредством международных усилий.

В российском законодательстве на сегодняшний день нет специальной нормы, напрямую предусматривающей ответственность за создание или распространение дипфейков. Тем не менее, определённые правовые положения могут применяться к отдельным аспектам использования этой технологии – по аналогии, в рамках общих составов правонарушений.

С уголовно-правовой точки зрения, отсутствие прямой статьи о «дипфейках» в УК РФ не означает безнаказанности злоумышленников. Их действия подпадают под традиционные составы преступлений в зависимости от намерений и последствий. Например, распространение компрометирующего дипфейк-видео о человеке при умысле его опорочить квалифицируется как клевета (ст. 128.1 УК РФ), а применение дипфейка для обмана с целью хищения имущества – как мошенничество (ст. 159 УК РФ). Обман остаётся обманом независимо от способа его совершения. Многие специалисты отмечают, что нет нужды специально перечислять в законе каждый новый технический способ обмана, а уголовно-правовые нормы сформулированы достаточно широко[6]. Так, адвокат Д. И. Загайнов критически относится к идее введения отдельной уголовной статьи за дипфейки, считая существующие положения достаточными[6].

Предпринимались и попытки учесть специфику дипфейков в уголовном законе. В 2023 году в Государственную Думу был внесён законопроект, предусматривающий ответственность за распространение заведомо недостоверных видеоматериалов, созданных с помощью ИИ (т.е. дипфейков). Однако Правительство РФ не поддержало

эту инициативу, указав, что сам по себе факт создания дипфейка без цели его распространения не обладает достаточной общественной опасностью[5]. В своём заключении Правительство также напомнило, что если посредством дипфейка незаконно разглашены персональные данные или частная информация о лице, уже действуют статьи УК (например, ст. 137 о нарушении неприкосновенности частной жизни) [5], а терминология проекта оказалась неясной. В итоге специальная статья принята не была.

Дискуссия, однако, продолжилась. В 2024 году появилась инициатива внести поправки в УК РФ, предлагающие учитывать использование «поддельного или искусственно созданного изображения или голоса» потерпевшего какотягчающее обстоятельство ряда преступлений[6]. Предлагалось дополнить квалифицирующие признаки в составах мошенничества, вымогательства, неправомерного доступа к компьютерной информации и др., если деяние совершено с применением дипфейка, а также уточнить ст. 128.1 УК («Клевета»), добавив указание на сфальсифицированный образ или голос потерпевшего[6]. Эта инициатива вызвала неоднозначные оценки: сторонники подчёркивали повышенную общественную опасность таких деяний, противники (включая того же Д. Загайнова) указывали, что существующих норм достаточно.

В гражданско-правовом порядке пострадавшие от дипфейка могут защищать свои права на основании норм о нематериальных благах. Российское законодательство охраняет облик (изображение) гражданина: ст. 152.1 ГК РФ запрещает использование изображения человека без его согласия (за исключением отдельных случаев, предусмотренных законом). Соответственно, лицо, чей образ (фотография, видео) сгенерирован и распространён без согласия, вправе требовать удаления такого контента и компенсации морального вреда. Уже есть прецеденты: в 2023 году российский суд впервые рассмотрел дипфейк-видео как объект смежных прав, указав, что применение технологии deepfake не лишает полученный продукт статуса аудиовизуального произведения для целей авторско-правовой охраны. Иными словами, использование нейросети не исключает охраноспособности результата.

Прямой нормы, аналогичной ст. 152.1 ГК РФ в отношении голоса, пока нет. Однако голос человека традиционно рассматривается в доктрине как часть его образа, его индивидуального облика, а значит как нематериальное благо, принадлежащее гражданину от рождения[4]. Следовательно, неправомерное создание и использование клонированного голоса без согласия можно расценивать как посягательство на нема-

териальное благо (нарушение ст. 150 ГК РФ, защищающей честь, достоинство и частную жизнь). Кроме того, элементы дипфейка могут подпадать под понятия персональных данных (если позволяют идентифицировать лицо) и биометрических персональных данных (изображение лица, голосовой слепок) в смысле закона «О персональных данных». Незаконный сбор, использование или распространение таких данных влечёт гражданско-правовую и административную ответственность (штрафы для нарушителей).

В иных сферах также отсутствуют специальные положения о дипфейках. Тем не менее, общие запреты на распространение заведомо ложной информации могут применяться. Например, закон о выборах запрещает предвыборную агитацию с использованием заведомо недостоверных сведений, а так называемый закон о «фейк-ньюс» (Федеральный закон №31-ФЗ от 18.03.2019 г.) предусматривает блокировку Роскомнадзором общественно значимой информации, распространяемой под видом достоверных сообщений и вводящей в заблуждение. Под это определение может подпасть и дипфейк-новость, если она угрожает общественному порядку. Однако отличить глубокую фальшивку от иных фейков порой непросто, требуется техническая экспертиза происхождения контента.

В зарубежной практике выработаны различные модели регулирования дипфейков[7]. Так, в США отсутствует единое федеральное регулирование из-за принципа свободы слова. Борьба с вредоносными дипфейками ведётся точечно на уровне штатов (приняты законы против порно-дипфейков, манипуляций на выборах и т.д.), плюс применяется широкий набор имеющихся правовых механизмов. Интернет-платформы при этом практически не несут ответственности за контент пользователей благодаря действующему иммунитету (Section 230 Закона США о приличиях)[8]. В Европейском союзе проблема решается преимущественно через призму регулирования деятельности онлайн-платформ и прозрачности ИИ. Принят закон о цифровых услугах и всеобъемлющий Акт об искусственном интеллекте, которые обязывают крупные платформы оценивать и снижать риски распространения дезинформации, а разработчиков и пользователей ИИ явно маркировать сгенерированный контент[9]. Иными словами, в ЕС введена обязательная маркировка всех AI-сгенерированных изображений, видео и аудио (за исключением случаев пародии, исследований и иных законных целей), а за нарушение этих требований грозят многомиллионные штрафы.

В Китае реализован один из самых жёстких подходов к проблеме дипфейков. С 2020 года там

фактически запрещена публикация непомеченных дипфейков: уголовно наказуемо распространение в сети видео- и аудиоконтента, созданного с помощью ИИ или VR-технологий, если такой контент вводит пользователей в заблуждение относительно реальности событий. Одновременно Администрация киберпространства Китая обязала все сервисы «глубокого синтеза» снабжать сгенерированные изображения и ролики явной маркировкой, а также запретила использовать дипфейки для создания фейковых новостей. Нарушение этих правил влечёт для платформ блокировку ресурса и другие суровые санкции. Таким образом, китайский подход сочетает тотальный контроль и превентивные меры: государство требует обязательной прозрачности (маркировки) и строго наказывает за злоупотребления. Некоторые специалисты называют китайское регулирование дипфейков «самым всеобъемлющим на сегодняшний день»[10].

Несмотря на предпринимаемые шаги, существующие правовые механизмы лишь частично отвечают на новые вызовы, связанные с дипфейками. Назрела необходимость восполнить ряд пробелов и усовершенствовать законодательство. Прежде всего требуется разработать и закрепить легальное определение «дипфейка» и его разновидностей. Отсутствие чёткого терминологического аппарата приводит к разночтениям: что считать дипфейком и какие случаи подпадают под действие норм. Следует внести в законодательство (например, в закон «Об информации») определение дипфейка как созданного с использованием технологий ИИ изображения, видео или аудиозаписи, имитирующих реального человека для правдоподобной передачи контента, не соответствующего действительности. Одновременно целесообразно закрепить термин «синтетический голос», указав, что искусственно сгенерированный голос, воспроизводящий идентифицируемое лицо, признаётся элементом биометрических персональных данных. Это устраним правовой пробел и создаст базис для дальнейшего регулирования ответственности.

Не менее важно законодательно отграничить допустимое использование технологии от злоупотреблений. Сейчас нормы не делают различий между легитимным применением дипфейка (например, пародийным или исследовательским) и неправомерным (клеветническим, мошенническим и т. п.). Нельзя идти по пути тотального запрета технологии, ограничивать следует лишь негативные последствия её недобросовестного применения, не подавляя развитие самой технологии. Стоит установить принцип, согласно которому создание и использование дипфейк-технологий допускается, если при этом не нарушаются права и законные интересы других лиц и зрите-

лям очевидно искусственное происхождение контента. Напротив, умышленное немаркированное и вводящее в заблуждение использование чужого образа или голоса должно прямо признаваться противоправным. Такая норма позволила бы отделить допустимые пародии, сатиру, творческие приёмы (где публика осознаёт условность происходящего) от тайных фальсификаций реальности с преступными целями.

Ключевым профилактическим шагом является введение обязательной маркировки («лейблов») сгенерированного медиа-контента. Опыт ЕС и Китая демонстрирует, что требование чётко помечать дипфейк-материалы значительно повышает их распознаваемость и сдерживает злоупотребления. В российских реалиях необходимо законодательно обязать при публичном распространении материалов, созданных путём «глубокого синтеза», явно указывать их искусственное происхождение, будь то текстовая пометка, специальный визуальный знак или звуковое предупреждение в начале записи. Также следует возложить на крупные онлайн-платформы обязанность выявлять и помечать немаркированные дипфейки. За несоблюдение этих требований должны быть предусмотрены санкции (штрафы для юридических лиц, вплоть до ощутимого процента от оборота компании). Эта мера является одним из ключевых элементов минимизации вреда от дипфейков. Разумеется, её реализация потребует развития технологий автоматического обнаружения фейкового контента, государству следует стимулировать создание эффективных средств обнаружения, например посредством грантов и программ поддержки.

Нужно также усилить защиту прав жертв дипфейков. На данный момент потерпевшие могут предъявлять иски по общим основаниям о клевете, о защите изображения, о компенсации морального вреда, но эти средства не учитывают специфики проблемы (скорости и анонимности распространения фальшивок, глобального характера, сложностей идентификации виновных). Следует прямо закрепить право гражданина на защиту от фальсификации его образа и голоса. В ГК РФ можно указать, что распространение изображения или аудиозаписи, созданных с помощью дипфейка без согласия, приравнивается к использованию изображения или голоса без согласия. Это поможет судам правильно квалифицировать такие случаи и взыскивать компенсацию вреда. Также целесообразно ввести ускоренные судебные процедуры (обеспечительные меры) для оперативной блокировки очевидно ложных дипфейк-материалов по заявлению заинтересованного лица, не дожидаясь окончательного решения, иначе к моменту суда ущерб от вирусного фейка может стать невосполнимым.

Отдельно стоит рассмотреть установление уголовной ответственности за наиболее опасные злоупотребления, например, за создание и распространение порнографических дипфейков без согласия изображённого лица (по аналогии с законодательством некоторых стран). В существующий УК РФ это могло бы быть внедрено через дополнение ст. 137 или 242 квалифицирующим признаком «совершено с использованием технологий дипфейк».

С учётом глобального характера проблемы необходимо укреплять международное сотрудничество. Следует поддерживать инициативы на площадках ООН, Совета Европы, ШОС, направленные на выработку единых принципов обращения с синтетическим контентом. На национальном уровне имеет смысл предусмотреть возможность привлечения к ответственности иностранцев, если их дипфейки нанесли ущерб правам граждан РФ или безопасности государства (в том числе заочно), хотя такая норма во многом носила бы декларативный характер, она создала бы юридическую базу для санкций против зарубежных источников деструктивных фейков.

Наконец, необходимы меры, адресованные разработчикам и платформам, распространяющим технологии дипфейк. В настоящее время «информационные посредники» почти не несут специальных обязанностей за пользовательский контент, согласно действующим нормам (например, ст. 1253.1 ГК РФ и аналогичным положениям закона об информации) они освобождаются от ответственности при условии своевременного удаления незаконной информации по заявлению. Этот иммунитет (аналог американского §230 CDA) затрудняет борьбу с дипфейками, так как платформы не мотивированы фильтровать даже явно вредоносные фальшивки. Поэтому назрела необходимость возложить на крупные онлайн-платформы прямые обязанности по противодействию «цифровым имитациям личности». Например, законом можно обязать такие платформы разрабатывать и опубликовать политику модерации дипфейков (меры по их обнаружению, маркировке либо удалению) и установить штрафы за её неисполнение (вплоть до оборотных, по аналогии с европейской практикой)[8]. Разумеется, подобные рычаги должны применяться взвешенно, чтобы избежать цензурных злоупотреблений, например, только на основании судебного решения или заключения экспертной комиссии.

В заключение следует отметить, что дипфейки и технологии синтетического голоса являются сложными, многогранными явлениями, затрагивающее интересы личности, общества и государства. Их распространение порождает новые виды правонарушений, на которые существующие нормы реагируют не всегда эффек-

тивно. Зарубежный опыт варьируется от фрагментарных ограничений отдельных злоупотреблений (США) до платформенной ответственности и обязательной прозрачности ИИ-контента (ЕС) и тотального государственного контроля с маркировкой (Китай). Российское законодательство пока делает лишь первые шаги, применяя общие нормы (например, о клевете, защите приватности) к новым технологическим реалиям и не вводя специальных терминов или правил.

Предложенные в статье меры призваны сформировать проактивный и комплексный механизм ответственности за дипфейки, минимизировав риски и не препятствуя развитию полезных инноваций. Их реализация существенно повысила бы защищённость граждан и общества от вреда, причиняемого «глубокими фейками», при этом, не вводя неоправданных ограничений для добросовестного использования технологий ИИ. Задача законодателя найти баланс: не позволить злоумышленникам безнаказанно использовать достижения ИИ во вред людям, но и не тормозить прогресс и свободу творчества. Дипфейк-технологии уже стали постоянным явлением цифрового мира, и правовая система должна эволюционировать, чтобы отвечать на этот вызов. Внедрение предложенных шагов по совершенствованию законодательства укрепит информационную безопасность, защитит права граждан и позволит России занять достойное место среди стран, формирующих международные стандарты ответственного и этичного обращения с ИИ.

Список литературы:

[1] Газета.Ru. Эксперт рассказал россиянам о росте популярности нейросетей среди мошенников (новостная заметка). – 10.03.2024. – URL: <https://www.gazeta.ru/tech/news/2024/03/10/22517065.shtml> (дата обращения: 04.09.2025).

[2] Citron D.K., Chesney R. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // *California Law Review*. – 2019. – Vol. 107, No. 1753. – P. 1753–1819.

[3] Dobrobaba M.B. Deepfakes as a Threat to Human Rights // *Lex Russica*. – 2022. – Vol. 75, No. 11. – P. 112–119. DOI: 10.17803/1729-5920.2022.192.11.112-119.

[4] Архипереев Н.В. Правовое регулирование создания и использования дипфейков // *Правовое государство: теория и практика*. – 2025. – № 2 (80). – С. 22–30.

[5] Лента.ру. Правительство не поддержало введение уголовной ответственности за дипфейки // *Lenta.ru*. – 04.06.2023. – URL: <https://lenta.ru/news/2023/06/04/deepfake/> (дата обращения: 04.09.2025).

[6] Загайнов Д.И. Дипфейки: изменения в УК РФ // *ЭЖ-Юрист*. – 2024. – № 36 (1336). – С. 6–8.

[7] Виноградов В.В., Кузнецова Д.В. Зарубежный опыт правового регулирования технологий «дипфейк» // *Правовой журнал ВШЭ*. – 2024. – Т. 17, № 2. – С. 215–240. DOI: 10.17323/2072-8166.2024.2.215.240.

[8] Quinn Emanuel. Regulating Deepfakes: New Consequences for Platforms and Producers // *Artificial Intelligence Update*. – July 2022. – URL: <https://www.quinnemanuel.com/the-firm/news-events/regulating-deepfakes-new-consequences-for-platforms-and-producers-artificial-intelligence-update-july-2022/>.

[9] Fragale M., Grilli V. Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation // *Columbia Journal of European Law, Preliminary Reference* (online). – 11.11.2024. – URL: <https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/>.

[10] Zhang L. China's Deepfake Regulations: navigating a new era of content authenticity // *Oxford Martin School* (blog). – 15.08.2023. – URL: <https://www.oxfordmartin.ox.ac.uk/blog/chinas-deepfake-regulations/>.

[11] Заключение Правительства РФ на проект фед. закона № 1172050-7 «О внесении изменений в Уголовный кодекс РФ (об установлении ответственности за незаконное создание и распространение дипфейков)». – 2023.

[12] Cyberspace Administration of China (CAC). Provisions on the Administration of Deep Synthesis Internet Information Services (effective 10.01.2023). – Translation // *Stanford DigiChina*. – 2022.

[13] Trofimov D.Yu. Legal aspects of regulating deepfake technology in Russia // *Advances in Social Science, Education and Humanities Research*. – 2022. – Vol. 640. – P. 281–287.

References:

[1] Gazeta.Ru. The expert told the Russians about the growing popularity of neural networks among scammers (news note). – 10.03.2024. – URL: <https://www.gazeta.ru/tech/news/2024/03/10/22517065.shtml> (access date: 04.09.2025).

[2] Citron D.K., Chesney R. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // *California Law Review*. – 2019. – Vol. 107, No. 1753. – P. 1753–1819.

[3] Dobrobaba M.B. Deepfakes as a Threat to Human Rights // *Lex Russica*. – 2022. – Vol. 75, No. 11. – P. 112–119. DOI: 10.17803/1729-5920.2022.192.11.112-119.

[4] Bishop N.V. Legal regulation of the creation and use of deepfakes//Legal state: theory and practice. – 2025. – № 2 (80). – S. 22-30.

[5] Лента.ру. The government did not support the introduction of criminal liability for deepfakes// Lenta.ru. – 04.06.2023. – URL: <https://lenta.ru/news/2023/06/04/deepfake/> (access date: 04.09.2025).

[6] Zagainov D.I. Deepfakes: changes in the Criminal Code of the Russian Federation//EZh-Lawyer. – 2024. – № 36 (1336). – S. 6-8.

[7] Vinogradov V.V., Kuznetsova D.V. Foreign experience in the legal regulation of deepfake technology//HSE Legal Journal. – 2024. – T. 17, NO. 2. – S. 215-240. DOI: 10.17323/2072-8166.2024.2.215.240.

[8] Quinn Emanuel. Regulating Deepfakes: New Consequences for Platforms and Producers // Artificial Intelligence Update. – July 2022. – URL: <https://www.quinnemanuel.com/the-firm/news-events/regulating-deepfakes-new-consequences-for-platforms-and-producers-artificial-intelligence-update-july-2022/>.

[9] Fragale M., Grilli V. Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Gener-

ated Misinformation // Columbia Journal of European Law, Preliminary Reference (online). – 11.11.2024. – URL: <https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/>.

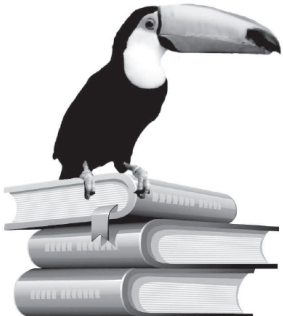
[10] Zhang L. China's Deepfake Regulations: navigating a new era of content authenticity // Oxford Martin School (blog). – 15.08.2023. – URL: <https://www.oxfordmartin.ox.ac.uk/blog/chinas-deepfake-regulations/>.

[11] Conclusion of the Government of the Russian Federation on the fed project. Law No. 1172050-7 "On Amendments to the Criminal Code of the Russian Federation (on establishing responsibility for the illegal creation and distribution of deepfakes)." – 2023.

[12] Cyberspace Administration of China (CAC). Provisions on the Administration of Deep Synthesis Internet Information Services (effective 10.01.2023). – Translation // Stanford DigiChina. – 2022.

[13] Trofimov D.Yu. Legal aspects of regulating deepfake technology in Russia // Advances in Social Science, Education and Humanities Research. – 2022. – Vol. 640. – P. 281-287.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.