оригинальная статья / original paper

специальность: 5.5.3, 5.1.5

EDN: XCYAWK

Проблема недостаточности нормативной регламентации использования в медиаиндустрии изображений, созданных с использованием технологий искусственного интеллекта

Качук В. Н.[1], **Коростелев С. В.**[2,] ***, **Соколов Д. А.**[1], **Студеновский В. В.**[1]

[1] Санкт-Петербургский государственный институт кино и телевидения, Санкт-Петербург, Российская Федерация

[2] Государственный научно-исследовательский навигационно-гидрографический институт, Санкт-Петербург, Российская Федерация

* e-mail: stakor@mail.ru

ORCID: 0000-0003-2650-1826

РЕФЕРАТ

В статье рассматриваются проблемы и риски, связанные с быстрым развитием и усовершенствованием технологии дипфейков, которые становятся все более доступными и трудно отличимыми от настоящего контента. Приводятся примеры технологических достижений и их применение. **Цель.** Обоснование необходимости правового регулирования использования изображений, синтезированных с помощью искусственного интеллекта, в медиаиндустрии, важности международного диалога по вопросам законодательства, кодификации запретов на использование изображений должностных лиц и распространение дипфейков, а также установления ответственности за их создание и распространение. **Задачи**. Выделить и сформулировать направления концентрации усилий органов публичной власти при движении к обеспечению защиты прав и свобод личности в условиях цифровизации, а также защиты медиаконтента, исходящего от органов публичной власти и их должностных лиц. **Методология**. Рассматриваются формы ответственности за противоправное использование дипфейков и средства противодействия этому явлению, в том числе через введение обязательной маркировки официальных фото- и видеоматериалов с использованием стеганографических методов для их идентификации и верификации, создание правовых механизмов для защиты авторских прав и предотвращения незаконного использования и распространения поддельных материалов. **Результаты и выводы**. Действия органов публичной власти должны быть направлены на согласование воль государств с целью разработки соответствующей международной конвенции и интеграции ключевых принципов борьбы с дипфейками в национальные законодательные системы.

Ключевые слова: искусственный интеллект, генеративно-состязательные сети, синтезированные изображения, цифровая подделка, ответственность за дипфейки, стеганографические методы

Для цитирования: Качук В. Н., Коростелев С. В., Соколов Д. А., Студеновский В. В. Проблема недостаточности нормативной регламентации использования в медиаиндустрии изображений, созданных с использованием технологий искусственного интеллекта // Евразийская интеграция: экономика, право, политика. 2026. Т. 20, № 1. С. 187–195. EDN: XCYAWK

The Problem of Insufficient Regulatory Framework for the Use of Images Created Using Artificial Intelligence Technologies in the Media Industry

Veronika N. Kachuk[a], **Stanislav V. Korostelev**[b,] ***, **Denis A. Sokolov**[a], **Victor V. Studenovsky**[a]

[a] State University of Film and Television, Saint Petersburg, Russian Federation

[b] State Research Navigation-Hydrographic Institute, Saint Petersburg, Russian Federation
* e-mail: stakor@mail.ru
ORCID: 0000-0003-2650-1826

ABSTRACT

This article examines the challenges and risks associated with the rapid development and improvement of deepfake technology, which is becoming increasingly accessible and difficult to distinguish from genuine content. Examples of technological advances and their applications are provided. **Aim**. To substantiate the need for legal regulation of the use of images synthesized using artificial intelligence in the media industry, the importance of international dialogue on legislation, the codification of prohibitions on the use of images of officials and the dissemination of deepfakes, and the establishment of liability for their creation and dissemination. **Tasks**. To identify and formulate areas for public authorities to focus their efforts in ensuring the protection of individual rights and freedoms in the context of digitalization, as well as the protection of media content emanating from public authorities and their officials. **Methods**. The challenge lies in determining the areas of public authorities' efforts and coordinating their international efforts in the area of information protection (media content emanating from them), which manifests itself in the distortion of the state's true intentions in the implementation of foreign policy. The article examines the forms of liability for the illegal use of deepfakes and measures to combat this phenomenon, including the introduction of mandatory labeling of official photos and videos using steganographic methods for identification and verification, and the creation of legal mechanisms to protect copyright and prevent the illegal use and distribution of counterfeit materials. **Results and conclusions.** Public authorities should work to align the wills of states with the goal of developing an appropriate international convention and integrating key principles for combating deepfakes into national legislation.

Keywords: artificial intelligence, generative adversarial networks, synthesized images, digital forgery, liability for deepfakes, steganographic methods

For citation: Kachuk V. N., Korostelev S. V., Sokolov D. A., Studenovsky V. V. The Problem of Insufficient Regulatory Framework for the Use of Images Created Using Artificial Intelligence Technologies in the Media Industry // Eurasian Integration: Economics, Law, Politics. 2026. Vol. 20, No. 1. P. 187–195. (In Russ.) EDN: XCYAWK

Введение

В настоящее время развитие и внедрение технологий искусственного интеллекта (далее — ИИ) приобретает ключевое значение для многих сфер жизни общества, включая экономику, образование, медицину и правоохранительную систему. Российская Федерация активно участвует в этой глобальной тенденции, стремясь создать благоприятные условия для разработки и применения ИИ. В частности, были приняты важные нормативные документы, такие как Федеральный закон № 123-ФЗ[1], регулирующий эксперимент по специальному регулированию ИИ в Москве, и Указ Президента Российской Федерации № 490[2], определяющий стратегическое развитие ИИ в стране. В начале 2021 г. предполагалось внедрение «цифровых песочниц», позволяющих более гибкое регулирование и быструю адаптацию законодательства к новым вызовам, и в июле того же года в Москве был запущен такой эксперимент.

[1] Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» [Электронный ресурс] // СПС «Консультант Плюс Проф». URL: https://www.consultant.ru/document/cons_doc_LAW_351127/ (дата обращения: 21.11.2025).

[2] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс] // СПС «Консультант Плюс Проф». URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 21.11.2025).

Целью данной статьи является обоснование необходимости — в свете недавних событий, связанных с распространением дипфейков[1], — разработки новых правовых норм, которые бы регламентировали частное использование нейросетей и обеспечивали правовые основы для организации защиты информационного пространства от подобных угроз.

Дипфейковая технология, или «глубокие подделки», представляет собой сравнительно новую разработку в сфере компьютерных технологий, характеризующуюся использованием алгоритмов искусственного интеллекта для модификации аудиовизуальных данных с целью создания высококачественных иллюзорных репрезентаций. А инструменты для их создания становятся все более простыми и доступными, не требующими от пользователей глубоких специализированных знаний, что представляет серьезные угрозы для общества, так как поддельные материалы могут подрывать доверие к официальным источникам информации, вызывать социальные конфликты и даже влиять на политические процессы.

Модификации медиаконтента могут охватывать лицо, тембр голоса, элементы одежды и окружающую среду, что позволяет синтезировать цифровые конструкции, внешне неотличимые от реальности, которые могут использоваться для различных целей, включая политическую пропаганду, мошенничество и распространение дезинформации.

Применение дипфейков не ограничивается одним видом медиаконтента, оно распространяется на фотографии, видеопоследовательности, аудиозаписи и тексты, в то время как первичным объектом изменений являются фото- и видеоматериалы.

Результаты и обсуждение

Первое документированное использование подобных средств состоялось в 2017 г., когда участник платформы Reddit, известный как deepfakes, обнародовал видеоролики, созданные на основе искусственного интеллекта, в которых изображались известные личности в непристойном контексте [10].

В основе технологии дипфейков лежат генеративно-состязательные сети (GAN), представляющие собой класс нейронных сетей, обучающихся на создании правдоподобных имитаций данных, которые использовались в их тренировке [7]. На сегодняшний день GAN широко применяются для генерации фальсификаций, включая методы «замены лица», позволяющие менять анатомические черты лица субъекта или полностью замещать его, «замены выражений», которые воспроизводят слова и фразы с точным имитированием тембра голоса, и «синтеза изображений», способного создавать новые цифровые образы или модифицировать уже существующие.

Несмотря на то, что наиболее убедительные цифровые имитации создаются с помощью инструментов, доступ к которым пока что ограничен, даже применение некоммерческих программ позволяет производить фото- и видеоподделки достаточного качества, чтобы нанести значительный ущерб репутации индивидов и безопасности на государственном и международном уровне. Так, например, М. В. Федоров акцентирует внимание на двух ключевых аспектах, способствующих вирусной распространенности дипфейков среди пользователей интернета, политических технологов, а также мошенников и экстремистов: относительная простота процесса создания и мощный эмоциональный эффект, порождаемый подделками [8].

Статистические данные, обнародованные на платформах, таких как Всемирный экономический форум, демонстрируют экспоненциальный рост количества дипфейков в интернете, которое, согласно исследованиям, увеличивается примерно на 900% ежегодно[2]. В течение первых четырех месяцев 2023 г. наблюдалось трехкратное возрастание визуальных дипфейков и восьмикратное — аудиодипфейков в сравнении с аналогичным периодом предыдущего года.

В нашей стране ситуация также имеет сложную негативную динамику: «Согласно информации АНО “Диалог Регионы” с января по сентябрь 2025 года в Рунете выявлено 342 уникальных дипфейка. Этот

[1] Термин «дипфейк» не закреплен в технической или юридической документации и употребляется в публичном дискурсе как слияние терминов «глубокое обучение» (deep learning) и «подделка» (fake).

[2] ВЭФ назвал дипфейки и ИИ главными угрозами для выборов в разных странах [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/11/01/2024/659fe9ff9a79475f70435f09?from=copy (дата обращения: 21.11.2025).

показатель в 4,1 раза превышает общее число подобных фальсификаций за весь 2024 год — тогда было зарегистрировано 84 случая… За неполный 2025 год обнаружено в 5,9 раза больше копий фейковых видео, чем за весь предыдущий год: 55 тысяч против 9,3 тысячи. Суммарное число просмотров достигло 122,5 млн, что в 3,1 раза выше результата за весь 2024 год»[1].

С ростом распространения контента, сгенерированного с использованием технологии deepfake, усугубляются проблемы манипулирования общественным мнением, нарушения как имущественных, так и личных неимущественных прав индивидуумов, а также проблемы, связанные с обработкой персональных данных. Технологии deepfake, оставаясь вне полного правового регулирования, представляют собой инструмент для распространения дезинформации и манипуляции общественным сознанием, что создает потенциальную угрозу не только для личных прав, но и для общественной безопасности в широком смысле. Они могут привести к массовой панике и подорвать доверие как к традиционным информационным каналам, так и к фундаментальным принципам демократического государственного устройства.

Например, в июне 2023 г. жители нескольких регионов России столкнулись с трансляцией поддельного обращения, фальсифицированного от имени Президента страны Владимира Путина, в котором говорилось о введении военного положения и начале полной мобилизации. Это обращение транслировалось как по телевидению, так и по радио, однако позже было установлено, что данное сообщение является дипфейком[2].

В декабре 2019 г. Всемирная организация интеллектуальной собственности начала рассматривать вопросы, связанные с нарушением прав индивидов, вызванным использованием технологии deepfake. В «Проекте концептуального документа по вопросам интеллектуальной собственности и искусственного интеллекта»[3] подчеркивается важность регулирования вопросов нарушения авторских прав на оригинальные изображения, прав на созданный с их помощью контент и необходимость обеспечения компенсации людям, чьи внешность и голос используются для создания deepfake-материалов. Также в источниках отмечается, что deepfake-технологии могут нарушать и иные личные права и свободы[4].

А. И. Овчинников отмечает, что цифровизация может влиять на человеческую индивидуальность. По его словам, современный человек, внося свои данные в всевозможные цифровые системы, становится лишь частью этой цифровой среды, теряя уникальность и даже собственное имя, которое заменяется логинами и паролями. Это создает впечатление, будто цифровая среда стала более важной, чем человек, для которого она изначально была создана. Указывается на необходимость умения использовать современные технологии и соглашаться с условиями обработки личных данных для получения преимуществ цифрового мира. Граждане испытывают опасения по поводу кражи личной информации и несовершенства защиты своих устройств, включая угрозу безопасности мобильных устройств, содержащих доступ к личным и банковским данным. Несмотря на развитие биометрических систем защиты, проблемы с доступом и ошибочная авторизация по-прежнему вызывают беспокойство среди пользователей. Такое состояние информационного элемента общественной безопасности ставит перед органами публичной власти задачи по выделению и формулированию направлений концентрации своих усилий при движении к обеспечению защиты прав и свобод личности в условиях цифровизации, а также защиты медиаконтента, исходящего от органов публичной власти и их должностных лиц.

В России вопросы использования и защиты биометрических данных обрели особую актуальность, когда в 2019 г. была введена программа создания единой системы биометрических данных, к которой подключились основные банки страны, включая Сбербанк, который стал пионером в сборе биометрических данных. Сбербанк пообещал и в целом добился того, что к концу 2021 г. многие его услуги стали доступны с использованием биометрии. Система СберID, позволяющая распознавать людей по их физи-

---

[1] В России зафиксирован рекордный рост числа дипфейков [Электронный ресурс]. URL: https://kolymaplus.ru/news/v-rossii-zafiksirovan-rekordnyj-rost-chisla-dipfejkov/ (дата обращения: 10.01.2026).

[2] «Обращение» Путина о мобилизации и военном положении оказалось дипфейком [Электронный ресурс]. URL: https://lenta.ru/news/2023/06/05/fake_radio/ (дата обращения: 21.11.2025).

[3] Проект концептуального документа по вопросам, касающимся политики в области интеллектуальной собственности и искусственного интеллекта [Электронный ресурс]. URL: https://www.wipo.int/meetings/ru/doc_details.jsp?doc_id=470053 (дата обращения: 11.01.2026).

[4] The deepfake dilemma: Detection and decree [Электронный ресурс]. URL: https://www.barandbench.com/columns/deepfake-dilemma-detection-and-desirability (дата обращения: 21.11.2025).

ческим характеристикам, упростила такие задачи, как оплата коммунальных услуг, совершение платежей, получение кредитов и другие операции [1].

Возникают резонные сомнения: реально ли подделать биометрические данные? Специалисты отдела безопасности Сбербанка уверены, что «в практике не было обнаружено полных совпадений голосовых отпечатков. Все попытки обмануть систему путем модификации голоса без применения электронных устройств оказались неудачными». С юридической точки зрения финансовые учреждения имеют полномочия самостоятельно регулировать уровень защиты клиентов, не нарушая их личные права.

В то же время Р. Б. Гасанова высказывает противоположное мнение, заявляя, что «несмотря на прогресс в изучении голосовых данных, нельзя говорить о стопроцентной точности» [3]. Ошибки в голосовой идентификации не исключены, они не гарантируют полную защиту финансов. Например, представители банков не упоминают о возможности записи голоса клиента и его последующего воспроизведения для незаконного доступа к банковским услугам.

В связи с этим в России в рамках Единой биометрической системы (далее — ЕБС) применяется усиленный уровень защиты данных. Стимулом к созданию данной системы послужила национальная программа «Цифровая экономика Российской Федерации». Основной принцип ЕБС — многоступенчатая аутентификация: помимо голоса, используется лицевое распознавание, а специфическое программное обеспечение анализирует уникальные черты лица: форму носа, подбородка, скул, контур губ, разрез глаз, расстояние между ними. Для удаленной верификации требуется совокупность голосовых и визуальных параметров, а используемые механизмы защиты исключают возможность подмены фотографий [6].

Казалось бы, с внедрением таких технологий опасения за безопасность банковских счетов могли бы исчезнуть, однако такое утверждение было бы слишком упрощенным, учитывая существующие угрозы, например, дипфейки.

Следующим шагом становится необходимость детального изучения концепции «искусственной нейронной сети», выступающей в роли фундаментального инструмента для создания дипфейков. Подобные компьютерные модели, базирующиеся на принципах, заимствованных из организации и функционирования биологических нейронных структур живых организмов, осуществляют сложнейшие вычислительные операции и имитируют процессы, присущие человеческому обучению [2].

В современном мире мы сталкиваемся с многообразием типов дипфейков — аудиальных, визуальных, а также гибридных, объединяющих видеоизображение и голос для формирования чрезвычайно реалистичных подделок. Яркой иллюстрацией служит DeepFaceLab — программный комплекс с открытым исходным кодом, созданный российским разработчиком под псевдонимом iperov. Данный инструмент предоставляет возможность не просто подменять лица в видеофайлах, но и корректировать артикуляцию губ, что влечет за собой трансформацию смысла произносимой речи. Корпорация Vera Voice демонстрирует иной вектор развития в сфере создания аудиодипфейков, генерируя голоса с такой степенью достоверности, что отличить сгенерированную речь от подлинной без применения специализированного софта практически нереально. Специалисты компании воспроизводят голоса ушедших деятелей искусства, опираясь на сохранившиеся фонограммы, как это было проделано с голосом Владимира Высоцкого.

Пройдя этап обучения на аудиоматериалах с голосом определенной личности, искусственная нейросеть обретает способность с исключительной точностью генерировать речь этого человека, начитывая произвольный текст без ощутимых дефектов или неестественного акцента. Создатели технологии отмечают широкие перспективы внедрения этой разработки в таких областях, как озвучивание литературных произведений, видеоигр, кинопродукции, а также при разработке виртуальных ассистентов. Вместе с тем они отдают себе отчет в том, что технология Vera Voice может эксплуатироваться как в развлекательных целях, так и в мошеннических схемах, включая подделку голосов известных политиков и публичных персон, что способно повлечь крайне негативные последствия. Осознавая эти риски, разработчики ведут активный поиск легитимных и этичных путей применения своего продукта.

Искусственные нейронные сети также способны самостоятельно генерировать музыкальные произведения в классическом стиле, обучаясь на творениях знаменитых композиторов, хотя пока и не способны

создавать полностью оригинальные композиции; они могут воспроизводить стиль игры лучше, чем многие люди.

Чтобы копировать лица и голоса на видео, нейросетям требуется обучающий материал, и чем он обширнее, тем точнее будет итоговый результат. Генеративно-состязательные сети строят карту лица, используя десятки точек и соединяющих их линий, создавая цифровой аналог в кратчайшие сроки [9].

Искусственные интеллектуальные системы, включая нейронные сети, сегодня находят применение в многочисленных областях деятельности, в том числе и в юриспруденции. Эти технологии способны безошибочно интерпретировать рукописный текст и трансформировать его в цифровой формат, а также ассистировать в составлении электронных документов, включая резюме. Они также используются для предсказания будущих событий, ведения криминалистических экспертиз и оценки государственных закупок, расширяя возможности аналитической поддержки в различных отраслях.

В своем исследовании Л. М. Кирова и М. Л. Макаревич упоминают о том, как в России юридическая компания «Право.ру» интегрировала искусственный интеллект для прогнозирования продолжительности и исходов судебных дел. Система основывается на анализе предшествующих судебных решений, что позволяет ей делать точные предположения о результатах. К тому же компания разработала бота, который способен отвечать на юридические запросы в Telegram, обрабатывая как текст, так и голосовые сообщения. Также известно, что в одном из университетов создана система Dare, которая может выявлять ложь в показаниях, анализируя мимику, голос и жесты, при этом эффективность ее работы достигает 92% [4].

В своем исследовании В. А. Лаптев выражает обоснованную тревогу о том, что такие технологии могут использоваться для фальсификации финансовых операций или изменения доказательств в уголовных делах [5]. Со временем дипфейки станут главной угрозой в идентификации подлинности аудио и видео в интернете, увеличив риск мошенничества, например, когда от имени руководства компании будут исходить ложные финансовые указания. Несмотря на это, искусственный интеллект может помочь в борьбе с преступностью.

На сегодняшний день понятия «дипфейк» и «нейросеть» юридически не закреплены, хотя они уже вошли в нашу жизнь. Применение этих технологий может нести как пользу, так и вред. Полностью запретить или контролировать использование нейросетей не представляется возможным, так как любой пользователь может установить соответствующее ПО или создать его самостоятельно. Следует сосредоточить усилия на разработке законодательных мер, направленных на привлечение к ответственности за злоупотребление нейросетями.

Необходимо принятие нового законодательства, так как вышеприведенный Федеральный закон № 123-ФЗ, регламентирующий в порядке эксперимента использование искусственного интеллекта в одном из субъектов Российской Федерации (Москве) и изменения, касающиеся персональных данных, не охватывает частное использование нейросетей. Также в приведенном Указе Президента № 490 определены лишь стратегические цели развития ИИ, заявлена возможность его применения в экономике для повышения эффективности бизнеса.

Предполагается очевидным, что цифровой образ личности схож с интеллектуальной собственностью, так как он является нематериальным правом. Однако он не является результатом творческой деятельности, поэтому должен регулироваться отдельными нормами.

Методология противодействия незаконному распространению дипфейков может использовать подход, аналогичный защите изображения гражданина по ст. 152.1 ГК РФ. Но правовые последствия обращения к дипфейкам имеют серьезные отличия от использования обычных изображений и видео — они, как показывает практика, могут нанести вред репутации человека, искажая историю его поведения. Существующие ст. 152.1 ГК РФ, ст. 5.61 КоАП РФ и ст. 128.1 УК РФ не учитывают особенностей таких деяний. Очевидно, что нужны новые организационно-технические решения, обоснованные нормами права.

Не вызывает также сомнения, что использование дипфейков может оказать влияние на историческую оценку фактов и событий. Поэтому авторы предполагают необходимым внести изменения в уголовное, административное и гражданское законодательство, предусмотрев особую ответственность за противоправное использование дипфейков, и предлагают средства противодействия этому явлению,

в том числе: введение обязательной маркировки официальных фото- и видеоматериалов с использованием стеганографических методов для их идентификации и верификации, создание институциональных механизмов для защиты авторских прав и предотвращения незаконного использования и распространения поддельных материалов, пропаганду знаний об ответственности за нарушение правил маркировки и распространение поддельных материалов.

Заключение

В заключение считаем необходимым отметить, что перед обществом стоят серьезные вызовы в связи с быстрым развитием технологий создания дипфейков, и это, в свою очередь, подтверждает необходимость системного подхода к правовому регулированию этой области. Наличие пробелов и недостаточность регулирования в существующем законодательстве как в России, так и на международном уровне, особенно в части регулирования частного использования нейросетей и синтезированных изображений, очевидны. Основываясь на анализе современных рисков и потенциальных последствий, рекомендуем разработку и принятие новых законодательных актов, которые включали бы четкие нормы относительно использования и распространения дипфейков, обеспечения защиты личности и общественного порядка, а также вводили ответственность за незаконное использование искусственного интеллекта для создания ложных изображений. Помимо этого, предполагаем целесообразным создание и внедрение международной конвенции в сфере унификации правовых механизмов противодействия проблеме дипфейков и облегчения межгосударственного сотрудничества. Считаем важным также акцентировать внимание на развитии и внедрении технологий искусственного интеллекта, направленных на распознавание и подтверждение аутентичности контента, что может стать важным инструментом в борьбе с информационным искажением и предотвратить множество негативных последствий, связанных с мошенничеством и подрывом доверия в обществе.

В результате анализа существующего политико-правового режима и международного опыта в данной очень важной сфере обеспечения информационной безопасности отмечаем, что ряд зарубежных государств предпринимают активные шаги по ограничению негативного влияния дипфейков. Однако системных нормативных решений, охватывающих одновременно вопросы маркировки, верификации и юридической ответственности за распространение подобного контента, на сегодняшний день не существует ни в одном государстве.

Предполагаем, что разработка проекта модельного закона Содружества Независимых Государств «О маркировке и обеспечении достоверности фото- и видеоматериалов, освещающих деятельность органов публичной власти и должностных лиц» (рабочее название) приобретает исключительную актуальность и своевременность. В ходе работы над проектом данного акта могут быть согласованы гармонизированные международные правовые основы для эффективного противодействия распространению недостоверной информации о деятельности органов публичной власти и должностных лиц посредством введения обязательных процедур маркировки официального контента и установления механизма его независимой верификации. А включение разработки проекта модельного закона в перечень приоритетных направлений деятельности Межпарламентской Ассамблеи государств — участников СНГ является необходимым и достаточно обоснованным.

Проект модельного закона СНГ должен, по нашему мнению, обязательно предполагать введение инновационных технических решений, таких как использование стеганографических методов встраивания метаданных в оригинальный контент, что сможет обеспечивать высокую степень защищенности и устойчивости к несанкционированному изменению или удалению общественно важной информации.

Кроме того, проект модельного закона СНГ должен предусмотреть создание специализированной системы верификации, доступной широкому кругу пользователей, а также закрепление мер административной и уголовной ответственности за нарушение предлагаемых норм маркировки и распространение заведомо недостоверного контента.

Принятие указанного модельного акта позволит, во-первых, повысить уровень доверия в Содружестве Независимых Государств к официальной информации, укрепить основы информационной безопасности

и снизить риски, проистекающие из манипулирования общественным сознанием; во-вторых, данный модельный закон может послужить основой для согласования воль государств в процессе разработки соответствующей международной конвенции, как минимум, в Содружестве Независимых Государств.

Список литературы

1. *Берлин С. И., Батори Г. А., Копылова Д. В.* Биометрия в банковской сфере. Исследования вопроса безопасности хранения биометрических данных // Вестник Академии знаний. 2019. № 3 (32). С. 329–336. EDN: QRSWNV
2. *Вожегов А. В.* Понятие искусственных нейронных сетей // Актуальные современные проблемы и перспективные отрасли инновационного развития. Екатеринбург : Научно-исследовательский центр Technical Innovations, 2021. № 7. С. 256–259. EDN: KRLCXG
3. *Гасанова Р. Б.* Идентификационное значение голосовых сообщений при расследовании преступлений // Закон и власть. 2021. № 2. С. 43–46. EDN: JRFRYG
4. *Кирова Л. М., Макаревич М. Л.* Правовые аспекты использования нейронных сетей // Инновационная экономика: перспективы развития и совершенствования. 2018. № 1 (27). С. 58–63. EDN: YQCXYK
5. *Лаптев В. А.* Deepfake и иные продукты искусственного интеллекта на пути развития онлайн-правосудия // Актуальные проблемы российского права. 2021. № 11 (132). С. 180–186. EDN: HOMQCG. DOI: 10.17803/1994-1471.2021.132.11.180-186
6. *Маслова Е. В.* Российская Единая биометрическая система: насколько она безопасна для банковского сектора? // Современные проблемы и перспективы развития банковского сектора: Материалы IV Всероссийской научно-практической (заочной) конференции / отв. ред. Я. Ю. Радюкова. Тамбов : Тамбовский государственный университет имени Г. Р. Державина, 2019. С. 76–83. EDN: LXJEIJ
7. *Сухань А. А.* Генеративно-состязательные нейронные сети в задачах определения трендов // Московский экономический журнал. 2019. № 6. С. 32. EDN: BGTFHF. DOI: 10.24411/2413-046X-2019-16031
8. *Федоров М. В.* Социально-экономические аспекты внедрения технологий искусственного интеллекта // Исследования в цифровой экономике. 2023. Т. 1, № 1. С. 6–60. EDN: MGIURM. DOI: 10.24833/14511791-2023-1-6-60
9. *Халтурин Е. Д., Макарец А. Б.* Генеративно-состязательные сети: комбинирование нейронных сетей для стимулирования обучения и облегчения вычислительной нагрузки // Математика и математическое моделирование. Сборник материалов XIII Всероссийской молодежной научно-инновационной школы. Саров : Интерконтакт, 2019. С. 297–299. EDN: ZOFOXD
10. *Getman A. A., Ling Yilan.* The Deepfake Technology: Threats or Opportunities for Customs // Управленческое консультирование. 2023. № 4 (172). P. 30–36. EDN: TWWJO. DOI: 10.22394/1726-1139-2023-4-30-36

Об авторах:

Качук Вероника Николаевна, доцент кафедры проектной деятельности в медиаиндустрии, ученый секретарь Ученого совета, Санкт-Петербургский государственный институт кино и телевидения (Санкт-Петербург, Российская Федерация);
e-mail: kachuk-vn@spbgikit.ru;

Коростелев Станислав Валентинович, старший научный сотрудник, Государственный научно-исследовательский навигационно-гидрографический институт (Санкт-Петербург, Российская Федерация); SPIN-код 8294-5755;
e-mail: stakor@mail.ru; ORCID: 0000-0003-2650-1826

Соколов Денис Андреевич, доцент кафедры аудиовизуальных систем и технологий, Санкт-Петербургский государственный институт кино и телевидения (Санкт-Петербург, Российская Федерация)
e-mail: sokolov-da@gikit.ru; ORCID: 0009-0008-7282-2712

Студеновский Виктор Владимирович, старший преподаватель кафедры проектной деятельности в медиаиндустрии, Санкт-Петербургский государственный институт кино и телевидения, IP/IT юрист, партнер Консалтинговой группы «О.С.В.» (Санкт-Петербург, Российская Федерация)
e-mail: victor_spbmk@mail.ru

References

1. Berlin, S. I., Bathory, G. A., Kopylova, D. V. Biometrics in the Banking Sector. Studying the Question of Security of the Storages of Biometrics Data // Bulletin of the Academy of Knowledge. 2019. No. 3 (32). (In Russ.) EDN: QRSWNV
2. Vozhegov, A. V. The Concept of Artificial Neural Networks // Actual Modern Problems and Promising Branches of Innovative Development. Ekaterinburg : Scientific Research Center Technical Innovations, 2021. No. 7. P. 256–259. (In Russ.) EDN: KRLCXG
3. Gasanova, R. B. Identification Value of Voice Messages for Investigation of Crimes // Law and Power. 2021. No. 2. P. 43–46. (In Russ.) EDN: JRFRYG
4. Kirova, L. M., Makarevich, M. L. Legal Aspects of the Use of Neural Networks // Innovative Economy: Prospects for Development and Improvement. 2018. No. 1 (27). P. 58–63. (In Russ.) EDN: YQCXYK
5. Laptev, V. A. Deepfake and Other Artificial Inntelligence Products on the Way to the Development of Online Justice // Actual Problems of Russian Law. 2021. No. 11 (132). P. 180–186. (In Russ.) EDN: HOMQCG. DOI: 10.17803/1994-1471.2021.132.11.180-186
6. Maslova, E. V. The Russian Unified Biometric System: How Safe Is It for the Banking Sector? // Modern Problems and Prospects for Development of the Banking Sector: Materials of the IV All-Russian Scientific and Practical (Correspondence) Conference / ed. by Y. Y. Radyukova. Tambov : Tambov State University named after G. R. Derzhavin, 2019. P. 76–83. (In Russ.) EDN: LXJEIJ
7. Sukhan, A. A. Generative Adversarial Neural Networks in Trend Determination Tasks // Moscow Economic Journal. 2019. No. 6. P. 32. (In Russ.) EDN: BGTFHF. DOI: 10.24411/2413-046X-2019-16031
8. Fedorov, M. V. Socio-economic aspects of the introduction of artificial intelligence technologies // Journal of Digital Economy Research. 2023. Vol. 1, No. 1. P. 6–60. (In Russ.) EDN: MGIURM. DOI: 10.24833/14511791-2023-1-6-60
9. Khalturin, E. D., Makarets, A. B. Generative Adversarial Networks: Combining Neural Networks to Stimulate Learning and Ease Computational Load // Mathematics and Mathematical Modeling: Collection of Materials of the XIII All-Russian Youth Scientific and Innovative School. Sarov : Intercontact, 2019. P. 297–299. (In Russ.) EDN: ZOFOXD
10. Getman, A. A., Ling Yilan. The Deepfake Technology: Threats or Opportunities for Customs // Administrative Consulting. 2023. No. 4 (172). P. 30–36. EDN: TWWJO. DOI: 10.22394/1726-1139-2023-4-30-36

About the authors:

Veronika N. Kachuk, Associate Professor of the Department of Project Activities in the Media Industry, Academic Secretary of the Academic Council, State University of Film and Television (Saint Petersburg, Russian Federation);
e-mail: kachuk-vn@spbgikit.ru

Stanislav V. Korostelev, Senior Researcher, State Research Navigation-Hydrographic Institute (Saint Petersburg, Russian Federation); SPIN 8294-5755;
e-mail: stakor@mail.ru; ORCID: 0000-0003-2650-1826

Denis A. Sokolov, Associate Professor of the Department of Audiovisual Systems and Technologies, State University of Film and Television (Saint Petersburg, Russian Federation);
e-mail: sokolov-da@gikit.ru; ORCID: 0009-0008-7282-2712

Victor V. Studenovsky, Senior Lecturer, Department of Project Activities in the Media Industry, State University of Film and Television (Saint Petersburg, Russian Federation), IP/IT Lawyer, Partner, O.S.V. Consulting Group (Saint Petersburg, Russian Federation);
e-mail: victor_spbmk@mail.ru

Авторы заявляют об отсутствии конфликта интересов.