DOI: 10.18137/RNU.V9276.25.03.P.085 УДК 347

Шайдуллин Римнур Марсович
аспирант кафедры гражданского и предпринимательского права, Университет управления «ТИСБИ», город Казань.
Электронный адрес: rimnurs@inbox.ru
Rimnur M. Shaidullin
Postgraduate at the Department of civil and business law, University of Management "TISBI", Kazan.
E-mail address: rimnurs@inbox.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДИПФЕЙК-ТЕХНОЛОГИЙ В СТРАНАХ АЗИИ И ЕГО ЗНАЧЕНИЕ ДЛЯ ВЛАДЕЛЬЦЕВ САЙТОВ (СТРАНИЦ САЙТА) В СЕТИ ИНТЕРНЕТ: ПУТИ СОВЕРШЕНСТВОВАНИЯ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА

Аннотация. *Актуальность* исследования обусловлена стремительным развитием технологий искусственного интеллекта, в частности дипфейков, которые создают серьезные вызовы для современной правовой системы. *Целью* работы является проведение сравнительного анализа правовых подходов к регулированию указанных технологий в зарубежных государствах и разработка научно обоснованных предложений по совершенствованию российского законодательства. В ходе исследования применялся сравнительно-правовой метод, позволивший выявить особенности национальных моделей регулирования, формально-юридический анализ нормативных актов, а также системный подход к оценке эффективности правовых механизмов. В результате установлено, что наиболее эффективными являются модели, сочетающие превентивные меры (обязательная маркировка контента, процедуры верификации) с балансом между необходимостью регулирования и стимулированием технологического развития. Научная *новизна* исследования заключается в разработке классификации правовых подходов к регулированию дипфейк-технологий и формулировании конкретных рекомендаций по совершенствованию российского законодательства, включая введение механизмов оперативного удаления противоправного контента. *Практическая значимость* работы состоит в возможности использования ее результатов законодательными органами при разработке нормативных актов, правоохранительными органами в правоприменительной деятельности, а также технологическими компаниями при создании систем саморегулирования.

Ключевые слова: правовое регулирование, дипфейк-технологии, генеративный ИИ, маркировка дипфейков, защита персональных данных, владельцы сайтов, ответственность владельцев сайтов.

Для цитирования: *Шайдуллин Р.М.* Правовое регулирование дипфейк-технологий в странах Азии и его значение для владельцев сайтов (страниц сайта) в сети Интернет: пути совершенствования российского законодательства // Вестник Российского нового университета. Серия: Человек и общество. 2025. № 3. С. 85–97. DOI: 10.18137/RNU.V9276.25.03.P.085

LEGAL REGULATION OF DEEPFAKE TECHNOLOGIES IN ASIAN COUNTRIES AND ITS SIGNIFICANCE FOR WEBSITE OWNERS (SITE PAGES) ON THE INTERNET: WAYS TO IMPROVE RUSSIAN LEGISLATION

Abstract. The article addresses the topical issues of the legal regulation of deepfake technologies. The *relevance* of the research is due to the rapid development of artificial intelligence technologies, in particular deepfakes, which pose serious challenges to the modern legal system and public safety. The *purpose* of the study is a comparative analysis of legal approaches to regulating these technologies in foreign coun-

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

tries and develop scientifically sound proposals for improving Russian legislation. In the course of the study, a comparative legal method was used, which made it possible to identify the features of national regulatory models, a formal legal analysis of regulations, as well as a systematic approach to assessing the effectiveness of legal mechanisms. As a result, it was found that the most effective models are those that combine preventive measures (mandatory labeling of content, verification procedures) with a balance between the need for regulation and stimulating technological development. The *scientific novelty* of the study is the development of a classification of legal approaches to regulating deepfake technologies and the formulation of specific recommendations for improving Russian legislation, including the introduction of mechanisms for the prompt removal of illegal content. The *practical significance* of the work consists in the possibility of using its results by legislative bodies in the development of regulations, law enforcement agencies in law enforcement activities, as well as technology companies in the creation of self-regulation systems.

Keywords: legal regulation, deepfake technologies, generative AI, deepfake labeling, personal data protection, website owners, responsibility of website owners.

For citation: Shaidullin R.M. (2025) Legal regulation of deepfake technologies in Asian countries and its significance for owners of websites (site pages) on the Internet: Ways to improve Russian legislation. *Vestnik of Russian New University. Series: Man and Society.* No. 3. Pp. 85–97. DOI: 10.18137/RNU.V9276.25.03.P.085 (In Russian).

Введение

Современные цифровые технологии стремительно трансформируют информационное пространство, создавая не только новые возможности, но и значительные правовые вызовы. Одним из наиболее дискуссионных явлений последних лет стало распространение *дипфейков* (англ. ‘deepfake”) – синтетических медиа, созданных с использованием искусственного интеллекта (далее – ИИ) и методов глубокого обучения. Эти технологии позволяют с высокой точностью манипулировать аудио- и видеоконтентом, подменяя личность и речь реальных людей.

Особый интерес в этом контексте представляет опыт стран Азии: Китая (КНР), Сингапура, Южной Кореи, – где активно развивается законодательство, направленное на контроль над созданием и распространением синтетического контента. Эти юрисдикции демонстрируют различные подходы правового регулирования дипфейк-технологий, что при помощи сравнительно-правового подхода может помочь выявить наилучшую модель в целях совершенствования российского законодательства в данной сфере.

Для России, где правовое регулирование дипфейков находится на стадии формирования, изучение азиатского опыта имеет особое значение. Владельцы сайтов и онлайн-платформ сталкиваются с неочевидными рисками, связанными с размещением пользовательского контента, включая возможные претензии со стороны правообладателей и пострадавших от манипуляций с дипфейками. Вопросы ответственности интернет-ресурсов, процедуры удаления противоправного контента и превентивные меры требуют четкой законодательной регламентации.

Несмотря на растущую озабоченность со стороны государства, бизнеса и гражданского общества, правовое регулирование дипфейк-технологий остается фрагментарным и не успевает за динамикой технологического развития. Отсутствие унифицированных подходов к квалификации подобного контента, а также механизмов его обнаружения и блокировки создает правовые про-

белы, которые могут быть использованы в противоправных целях [1, с. 114].

В вопросе правового регулирования ИИ важно также и соблюсти баланс между урегулированием данной области и предоставлением свободы, «пространства» для стабильного развития различных технологий ИИ. Ведь в случае с «переурегулированностью» данной области может возникнуть ситуация, при которой излишнее правовое регулирование может оказаться препятствием для планомерного развития ИИ-технологий. Данная позиция озвучивалась Президентом Российской Федерации В.В. Путиным на встрече с руководителями парламентов стран Организации Договора о коллективной безопасности 9 декабря 2024 года[1].

Сами по себе дипфейк-технологии не являются чем-то отрицательным, напротив, они могут положительно применяться в различных сферах жизни [2, с. 217].

Стремление найти баланс между регулированием и свободой развития технологий прослеживается в законодательных подходах разных стран, однако степень его соблюдения варьируется в зависимости от правовых традиций и приоритетов государства. В то время как одни юрисдикции делают акцент на жестком контроле над распространением дипфейков, другие ограничиваются точечными мерами, оставляя пространство для технологических инноваций.

Китай

Китай, будучи одним из лидеров в сфере развития ИИ, обладает наиболее детализированным законодательством в сфере правового регулирования генеративного ИИ, и, в частности, дипфейк-технологий.

Первым специальным нормативно-правовым актом в сфере регулирования дипфейк-технологий в Китае стали Положения об управлении глубоким синтезом информационных услуг Интернета от 25.11.2022 г.[2], вступившие в силу 10.01.2023 г. (далее – Положение).

Под дипфейк-технологиями в Положении понимается «технология глубокого синтеза». «Технология глубокого синтеза» определяется в статье 23 Положения как использование алгоритмов глубокого обучения, виртуальной реальности и иных методов для генерации или модификации: текстов (создание, стилизация, диалоги), аудио (синтез речи, изменение голоса), музыки и звуковых эффектов, изображений и видео (генерация/замена лиц, изменение поз, атрибутов), цифровых персонажей и 3D-сцен (моделирование, реконструкция).

Субъектами, на которые распространяется Положение, определены Поставщики услуг глубокого синтеза – организации, предоставляющие услуги глубокого синтеза, и организации технической поддержки, а также пользователи услуг глубокого синтеза – юридические и физические лица, которые используют сервисы глубокого синтеза для создания, копирования, публикации или передачи информации.

Положением определяются следующие требования к поставщикам услуг:

• маркировка контента: весь синтетический контент (например, дипфейки или AI-голоса) должен иметь четкую пометку (Статьи 16, 17);

[1] Путин выступил за баланс при регулировании интернета и ИИ // ТАСС. 09.12.2024. URL: https://tass.ru/ekonomika/22620997 (дата обращения: 12.05.2025).

[2] Положения об управлении глубоким синтезом информационных услуг Интернета // Cyberspace Administration of China. URL: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата обращения: 01.06.2025).

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

• верификация пользователей: платформы обязаны проверять личность пользователей, создающих синтетический контент (Статья 9);
• контроль безопасности: регулярные проверки алгоритмов, особенно если они затрагивают биометрические данные (лица, голос) (Статья 15);
• борьба с фейками: удаление ложной информации и уведомление регуляторов (например, CAC – Cyberspace Administration of China) (Статьи 10, 11).

Кроме того, Положением прямо запрещается (Статья 6) создавать, тиражировать, публиковать или распространять с помощью технологий глубокого синтеза информацию, противоречащую нормам действующего законодательства, применять данные технологии для осуществления противоправной деятельности.

Положение предусматривает ответственность за нарушение требований, установленных Положением, для поставщиков услуг в виде штрафов, приостановки деятельности, уголовной ответственности в случае, если нарушения повлекли тяжкие последствия. Для пользователей предусмотрены блокировка аккаунтов, административные наказания.

После вступления в силу указанного Положения в Китае были приняты Временные меры по администрированию услуг генеративного искусственного интеллекта от 10.07.2023 г.[1], вступившие в силу 15.08.2023 г.

Временные меры по администрированию услуг генеративного ИИ от 10 июля 2023 г. представляют собой логическое продолжение и развитие нормативной базы, заложенной в Положениях об управлении глубоким синтезом информационных услуг Интернета от 25 ноября 2022 г. Новый документ конкретизирует положения предыдущего регулирования применительно к быстроразвивающемуся сегменту генеративных ИИ-технологий.

Важным нововведением стало уточнение понятийного аппарата. Термин «глубокий синтез», использовавшийся в Положениях 2022 года, дополнен более специализированным понятием «генеративный искусственный интеллект», что отражает эволюцию технологического ландшафта.

Продолжая линию последовательного развития нормативной базы в сфере регулирования технологий искусственного интеллекта, китайские законодатели в 2025 году приняли дополнительные меры по усилению контроля за распространением синтетического контента. В развитие Положения от 25.11.2022 г. и Временных мер 10.07.2023 г. были утверждены «Меры по маркировке контента, созданного искусственным интеллектом» от 07.03.2025 г.[2] и национальный стандарт GB 45438-2025 «Технологии кибербезопасности. Метод маркировки контента, созданного искусственным интеллектом» от 15.03.2025 г.[3]

[1] Временные меры по администрированию услуг генеративного искусственного интеллекта // Cyberspace Administration of China. URL: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 01.06.2025).

[2] Меры по маркировке контента, созданного искусственным интеллектом // Cyberspace Administration of China. URL: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm (дата обращения: 01.06.2025).

[3] Обязательный национальный стандарт GB 45438-2025 «Метод идентификации синтетического контента, созданного на основе искусственного интеллекта в технологиях сетевой безопасности» // National Committee 260 on Cybersecurity of Standardization Administration of China. URL: https://www.tc260.org.cn/front/postDetail.html?id=20250315113048 (дата обращения: 01.06.2025).

(далее – правила маркировки), которые вступят в силу 1 сентября 2025 года.

Особенностью новых правил стало введение двухуровневой системы маркировки, включающей как явные, так и неявные метки. Явные метки представляют собой визуально или аудиально распознаваемые индикаторы, однозначно указывающие на искусственное происхождение контента. Неявные метки включают скрытые метаданные, содержащие информацию о происхождении контента и обеспечивающие его прослеживаемость.

Значительное внимание в новых правилах уделяется обязанностям платформ распространения контента, которые должны внедрить механизмы автоматического обнаружения и классификации ИИ-генерируемых материалов. В зависимости от степени подтвержденности происхождения контента он подразделяется на три категории: подтвержденный, возможный и предполагаемый контент, созданный ИИ, для каждой из которых установлены особые требования к маркировке.

Сингапур

В отличие от Китая, где принято специализированное законодательство об искусственном интеллекте, в Сингапуре в настоящее время отсутствует отдельный нормативный акт, посвященный исключительно регулированию ИИ-технологий, и не планируется его разработка в ближайшей перспективе. Данная позиция находит свое отражение в Национальной стратегии искусственного интеллекта (NAIS 2.0)[1], где подчеркивается приверженность правительства гибкому подходу к регулированию, предполагающему своевременное внесение изменений в нормативно-правовую базу с учетом трансграничной природы технологий искусственного интеллекта и необходимости применения дифференцированных мер управления рисками – от императивных норм до рекомендательных положений.

Законодательство Сингапура содержит ряд нормативных актов, которые, не будучи специально ориентированными на регулирование ИИ, тем не менее устанавливают правовые рамки для противодействия связанным с ним рискам [3]. Например, Закон о неправомерном использовании компьютеров 1993 года (Computer Misuse Act)[2], являясь технологически нейтральным актом, криминализирует широкий спектр противоправных действий в цифровой сфере, включая потенциальные злоупотребления технологиями генеративного ИИ. В частности, раздел 3 указанного Закона квалифицирует как преступление несанкционированный доступ к компьютерным данным, что может включать фишинговые атаки с использованием технологий искусственного интеллекта, санкционируя за такие деяния наложение штрафа до 5000 сингапурских долларов и/или лишение свободы на срок до двух лет. Раздел 4 Закона специально предусматривает ответственность за использование дипфейк-технологий для обхода систем биометрической аутентификации или совершения мошеннических действий, устанавливая более строгие санкции – штраф до 50000 сингапурских долларов и/или лишение свободы на срок до десяти лет.

[1] National AI Strategy (NAIS 2.0) // Smart Nation. URL: https://www.smartnation.gov.sg/initiatives/national-ai-strategy (дата обращения: 01.06.2025).

[2] Computer Misuse Act 1993// Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/CMA1993 (дата обращения: 01.06.2025).

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

Принятый в 2023 году Закон о противодействии преступному вреду в Интернете (Online Criminal Harms Act)[1] предоставляет компетентным органам дополнительные инструменты для противодействия противоправной деятельности в цифровом пространстве. В соответствии с его положениями уполномоченные органы могут направлять предписания поставщикам онлайн-услуг о прекращении взаимодействия с аккаунтами, используемыми для противоправной деятельности, и об ограничении доступа к соответствующим интернет-ресурсам, что особенно актуально для случаев использования технологий генеративного ИИ в мошеннических схемах или распространения вредоносного контента.

Закон о защите от онлайн-лжи и манипуляций 2019 года (Protection from Online Falsehoods and Manipulation Act)[2] устанавливает запрет на распространение заведомо ложных утверждений фактологического характера, предоставляя правительству широкие полномочия по противодействию подобным нарушениям, включая возможность выдачи предписаний об удалении контента, размещении корректирующей информации и ограничении доступа к ресурсам, распространяющим ложные сведения. Данные положения могут распространяются и на контент, созданный с использованием технологий искусственного интеллекта.

9 сентября 2024 года Министерством цифрового развития и информации был внесен в парламент законопроект (принят 15.10.2024 г.)[3], вносящий поправки в законодательство о выборах и направленный на обеспечение достоверности онлайн-рекламы в избирательный период. Данная инициатива обусловлена необходимостью создания специальных правовых механизмов для борьбы с манипулятивным контентом, поскольку существующий Закон о защите от онлайн-лжи и манипуляций не в полной мере охватывает все аспекты распространения дипфейков в политическом контексте.

Проект поправок устанавливает запрет на публикацию и распространение цифрового контента, созданного или измененного с использованием современных технологий, который реалистично изображает кандидатов совершающими действия или произносящими слова, не соответствующие действительности, при условии, что такой контент может быть расценен как предвыборная агитация.

Особенностью предлагаемого регулирования является дифференцированный подход к установлению ответственности: для социальных сетей предусмотрены значительные административные штрафы, достигающие одного миллиона сингапурских долларов, в то время как для физических лиц и иных субъектов может наступать как административная, так и уголовная ответственность с возможным лишением свободы на срок до одного года. Важно отметить, что особый правовой режим будет действовать исключительно в период избирательных кампаний, что отражает

[1] Online Criminal Harms Act // Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/OCHA2023 (дата обращения: 01.06.2025).

[2] Protection from Online Falsehoods and Manipulation Act // Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/POFMA2019 (дата обращения: 01.06.2025).

[3] Elections (Integrity of Online Advertising) (Amendment) Bill // Parliament of Singapore (PARL). URL: https://www.parliament.gov.sg/docs/default-source/bills-introduced/elections-(integrity-of-online-advertising)-(amendment)-bill-29-2024.pdf (дата обращения: 01.06.2025).

стремление законодателей найти баланс между защитой демократических процессов и соблюдением принципов свободы информации. При этом сохраняется возможность применения других нормативных актов, таких как POFMA или Закон о компьютерных злоупотреблениях, в случаях, когда распространение дипфейков сопряжено с совершением иных правонарушений.

Закон о защите персональных данных 2012 года (Personal Data Protection Act)[1], регулируя обработку персональных данных частными организациями, устанавливает требования по обеспечению их безопасности, что приобретает особую актуальность в контексте использования больших объемов данных для обучения ИИ-систем.

Южная Корея

Южнокорейская модель по сравнению с китайской и сингапурской моделями правового регулирования дипфейк-технологий занимает промежуточное положение, сочетая избирательные уголовно-правовые запреты с элементами технологического регулирования, что позволяет провести ее содержательное сравнение как с всеобъемлющей китайской системой контроля, так и с либеральной сингапурской практикой адаптации существующих правовых норм.

В сентябре 2024 года Национальное собрание Южной Кореи приняло масштабные поправки к Закону о специальных случаях наказания за сексуальные преступления (Act on Special Cases Concerning the Punishment of Sexual Crimes)[2]. Эти изменения существенно расширили сферу ответственности за использование дипфейков. Впервые в мировой практике был криминализован просмотр и хранение дипфейков, установлено наказание не только за создание и распространение, но и за просмотр или хранение дипфейков сексуального характера без согласия изображенных лиц. Санкции предусматривают до трех лет лишения свободы или штраф до 30 млн вон (~22,600 USD). Также ужесточилось наказание за создание контента подобного рода. Для лиц, создающих или редактирующих дипфейк-материалы сексуального характера, максимальное наказание увеличено с пяти до семи лет лишения свободы. Расширился круг потерпевших: ранее нормы защищали преимущественно несовершеннолетних, теперь они распространяются на всех граждан независимо от возраста.

Центральное место в системе правового регулирования дипфейк-технологий занимает Закон о содействии использованию информационно-коммуникационных сетей и защите информации[3], который был существенно дополнен новыми положениями, направленными на противодействие

[1] Personal Data Protection Act (PDPA) // Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/PDPA2012 (дата обращения: 01.06.2025).

[2] Act on Special Cases Concerning the Punishment of Sexual Crimes. Enforcement Date 18. Dec, 2018. Act No. 15977, 18. Dec, 2018, Partial Amendment // Ministry of State Legislation of Korea. URL: https://law.go.kr/LSW/lsInfoP.do?lsiSeq=205815&viewCls=engLsInfoR&urlMode=engLsInfoR#0000 (дата обращения: 01.06.2025).

[3] Act on promotion of information and communications network utilization and information protection. Act No. 14080, Mar. 22, 2016 // Korea legislation research institute URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG (дата обращения: 01.06.2025).

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

незаконному использованию синтетического контента. Например, в указанный закон была внесена поправка от 03.12.2024 г. в части его дополнения статьей 4-2: Министерство науки и ИКТ и Корейская Комиссия по коммуникациям должны разработать меры предотвращению преступлений сексуального характера, клеветы и мошенничества с использованием сгенерированного контента без согласия лица, чьи биометрические данные использовались при создании такого контента. Указанная поправка вступила в силу 04.06.2025 г. Кроме того, в соответствии с поправками к данному закону цифровые платформы обязаны удалять дипфейк-материалы в течение 24 часов с момента получения официального уведомления от Корейской комиссии по коммуникациям (KCC)[1].

Наиболее важным шагом к регулированию дипфейк-технологий в Южной Корее стало принятие Основного закона об искусственном интеллекте от 21.01.2025 г.[2], который вступит в силу 22.01.2026 г. Указанный закон, хотя и является рамочным, но содержит положения, напрямую регулирующие распространение контента, сгенерированного с использованием возможностей дипфейк-технологий.

Указанным Законом также вводится обязательная маркировка продуктов и услуг с использованием генеративного ИИ, в частности дипфейк-технологий (п. 3 ст. 31), за нарушение указанной статьи вводится административная ответственность в виде штрафа (ст. 43).

Южнокорейская правовая система в сфере регулирования дипфейк-технологий демонстрирует точечный подход, криминализуя лишь отдельные виды дипфейков и на данный момент не отличается комплексным подходом. В отличие от китайской модели, предусматривающей всеобъемлющее регулирование, южнокорейский законодатель избрал путь выборочного запрета, сосредоточив внимание на наиболее социально опасных проявлениях данной технологии. В частности, уголовной ответственности подлежит создание и распространение дипфейков сексуального характера без согласия изображенного лица, что закреплено в Законе о специальных положениях относительно наказания за сексуальные преступления. Однако другие потенциально опасные виды синтетического контента, такие как политические дипфейки или фейковые новости, остаются за рамками специального регулирования. Подобная избирательность правового реагирования объясняется стремлением сохранить баланс между защитой прав граждан и недопущением избыточного ограничения свободы творчества и технологического развития.

Россия

На данный момент в России отсутствует специальное законодательство, регулирующее правоотношения в сфере генеративного ИИ и, в частности, дипфейк-технологий [4–11].

[1] Korean Communications Commission (KCC) // Korean Communications Commission. URL: https://www.kcc.go.kr (дата обращения: 01.06.2025).

[2] Basic Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust // Ministry of State Legislation of Korea. URL: https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%9D%B8%EA%B3%B5+%EC%A7%80%EB%8A%A5%EC%97%90+%EA%B4%80%ED%95%9C+%EA%B8%B0%EB%B3%B8%EB%B2%95#J42:0 (дата обращения: 01.06.2025).

Ориентиром развития искусственного интеллекта в России до недавнего времени являлась Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, утвержденная распоряжением Правительства РФ от 19.08.2020 г. № 2129-р.[1] В Концепции особо отмечается, что внедрение и использование ИИ должно достаточным образом обеспечивать защиту прав и свобод человека, а также отвечать интересам общества и государства.

Кроме того, внимание уделяется и вопросу юридической ответственности за вред, причиненный использованием ИИ. В частности отмечается, что с появлением новых правоотношений в сфере применения искусственного интеллекта не предполагается кардинального изменения института юридической ответственности. Однако темпы развития ИИ требуют точечных изменений в части гражданско-правовой, административной и уголовной ответственности. Также поднимается вопрос о необходимости проработки механизмов возмещения вреда, причиненного ИИ (страхование ответственности, компенсационные фонды и т. д.)

Важным документом в сфере развития искусственного интеллекта является и Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»)[2].

Содержательно Национальная стратегия развития ИИ базируется на принципе баланса между стимулированием технологического прогресса и обеспечением безопасности, что отражает глобальную тенденцию поиска оптимальной модели регулирования прорывных технологий. Документ выделяет семь приоритетных направлений развития ИИ, среди которых особое внимание уделяется фундаментальным и прикладным исследованиям, подготовке кадров и созданию инфраструктуры. Анализ редакций документа показывает эволюцию подходов к регулированию: если первоначальная версия делала акцент преимущественно на экономических аспектах, то изменения 2024 года усиливают компоненты, связанные с национальной безопасностью и технологическим суверенитетом, что отражает изменившуюся геополитическую и технологическую реальность.

Сравнительно-правовой анализ показывает, что российская Стратегия развития ИИ, с одной стороны, учитывает международный опыт (в частности, элементы китайской модели), с другой – предлагает оригинальный подход, сочетающий централизованное управление с поддержкой частной инициативы. В отличие от ЕС, где доминирует регуляторная логика, российский документ делает акцент на развитии технологического потенциала, что отражает специфику национальных приоритетов.

[1] Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года : утв. распоряжением Правительства РФ от 19.08.2020 № 2129-р // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_360681/7f2affb15ff9b9d6f75a9aa566d1b0646b3d2e94/ (дата обращения: 01.06.2025).

[2] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.06.2025).

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

Обозреваемые выше документы являются рамочными, определяющими концептуальные направления развития ИИ в РФ. Но стремительное развитие ИИ требует своевременного реагирования на новые вызовы с точки зрения охраны прав и свобод человека. Таким вызовом могут являться многократно участившиеся случаи мошенничества, клеветы и причинения ущерба репутации лиц с применением технологии дипфейк[1].

16 сентября 2024 года в Государственную Думу РФ был внесен законопроект № 718834-8[2]. Указанным законопроектом предлагается ввести в ГК РФ новую статью «Охрана голоса гражданина». Предполагается законодательно защитить голос гражданина по аналогии с уже существующей статьей об охране изображения гражданина (ст. 152.1 ГК РФ). Однако различие между текстом предлагаемой ко введению и существующей статьями все же есть, оно заключается в указании в п. 1 ст. 152.3 (предлагаемой ко введению) о защите голоса, воссозданного с помощью специальных технологий, что фактически защищает голос гражданина от несанкционированного его использования в том числе при помощи дипфейк-технологий.

Также 16. сентября 2024 года в Государственную Думу РФ был внесен законопроект № 718538-8[3], который предлагает ввести квалифицирующий признак ряда преступлений, в последнее время наиболее часто совершающихся с использованием дипфейк-технологий (клевета, кража, мошенничество, мошенничество в сфере компьютерной информации, вымогательство, причинение имущественного ущерба путем обмана или злоупотребления доверием).

Анализ текущего состояния правового регулирования в сфере дипфейк-технологий в Российской Федерации свидетельствует о наличии нормативного пробела. Несмотря на предпринимаемые законодательные инициативы, существующая правовая база остается фрагментарной и не обеспечивает комплексной защиты от потенциальных рисков, связанных с использованием технологий глубокого синтеза. Предлагаемые изменения в Гражданский кодекс РФ (проект № 718834-8) и Уголовный кодекс РФ (проект № 718538-8), безусловно, представляют собой шаг вперед, однако носят точечный характер и не охватывают весь спектр возможных злоупотреблений. Особое значение имеет отсутствие четкого законодательного определения дипфейк-технологий, что создает правовую неопределенность и затрудняет правоприменительную практику.

---

[1] Сбербанк выявил случаи мошенничества с использованием дипфейков // РИА Новости. 11.12.2024. URL: https://ria.ru/20241211/moshennichestvo-1988701707.html (дата обращения: 01.06.2025); МВД предупредило о новой схеме мошенничества // РИА Новости. 17.01.2025. URL: https://ria.ru/20250117/mvd-1994199451.html (дата обращения: 01.06.2025); В России активизировались мошенники в дейтинг-сервисах и соцсетях // РИА Новости. 28.04.2025. URL: https://ria.ru/20250428/moshenniki-2013758448.html (дата обращения: 01.06.2025).

[2] Законопроект № 718834-8 «О внесении изменений в часть первую Гражданского кодекса Российской Федерации (об охране голоса)» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/718834-8 (дата обращения: 01.06.2025).

[3] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)» // Система обеспечения законодательной деятельности. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 01.06.2025).

Выводы

Современное правовое регулирование дипфейк-технологий демонстрирует существенные различия в подходах различных юрисдикций, что обусловлено как особенностями национальных правовых систем, так и приоритетами государственной политики в сфере цифровых технологий. Китайская модель, характеризующаяся жестким централизованным контролем, представляет собой наиболее детализированную систему регулирования, основанную на последовательном принятии специализированных нормативных актов. Особенностью китайского подхода является установление императивных требований к маркировке синтетического контента, верификации пользователей и созданию специализированных реестров, что обеспечивает высокий уровень контроля за оборотом дипфейк-технологий, но одновременно создает значительную регуляторную нагрузку на субъектов цифровой экономики.

В отличие от Китая, Южная Корея избрала более дифференцированный/точечный подход, сочетающий жесткие запретительные меры в отношении противоправного использования определенных дипфейков (включая криминализацию не только создания и распространения, но и потребления контента сексуального характера без согласия изображенных лиц) с сохранением возможностей для легитимного использования технологий синтеза в исследовательских и творческих целях. Однако реализация такого подхода сопряжена с существенными правоприменительными сложностями, особенно в части доказывания фактов потребления дипфейк-контента.

Сингапурская модель регулирования демонстрирует более гибкий подход, предполагающий адаптацию традиционных правовых институтов к новым технологическим вызовам. Особого внимания заслуживают поправки 2024 года к законодательству о выборах, направленные на противодействие использованию дипфейков в политическом контексте, что отражает стремление законодателя обеспечить баланс между защитой демократических процессов и сохранением свободы цифровых коммуникаций.

Российская правовая система в настоящее время находится на начальном этапе формирования специализированного регулирования дипфейк-технологий. Несмотря на наличие концептуальных документов, действующее законодательство не содержит комплексного регулирования вопросов создания и распространения синтетического контента. Законопроекты № 718834-8 и № 718538-8, предусматривающие введение гражданско-правовой защиты голоса гражданина и установление квалифицирующих признаков для преступлений, совершаемых с использованием дипфейк-технологий, представляют собой важный, но недостаточный шаг в направлении формирования целостной системы правового регулирования.

Сравнительный анализ выявляет ряд ключевых проблем российского регулирования:

- отсутствие четкого законодательного определения дипфейк-технологий;
- фрагментарность мер ответственности;
- недостаточная проработка механизмов превентивного контроля за распространением синтетического контента.

В этой связи представляется целесообразным заимствование отдельных элементов зарубежного опыта, таких как

- введение обязательной маркировки дипфейк-контента (по аналогии с китайской и южнокорейской моделями);

Вестник Российского нового университета
Серия: Человек и общество. 2025. № 3.

• установление специальных составов административных правонарушений за распространение немаркированного синтетического контента;
• создание механизма оперативного удаления противоправного контента с возложением соответствующих обязанностей на информационных посредников;
• разработка специализированных технологических стандартов верификации оригинального контента.

При этом необходимо сохранить баланс между защитой прав граждан и интересов государства, с одной стороны, и созданием благоприятных условий для развития перспективных технологий – с другой, избегая избыточного регулирования, характерного для китайской модели. Особого внимания заслуживает вопрос гармонизации национального регулирования с международными стандартами, что приобретает особую актуальность в условиях трансграничного характера цифровых технологий.

Литература

1. *Добробаба М. Б.* Дипфейки как угроза правам человека // Lex Russica. 2022. Т. 75. № 11. С. 112–119. DOI: 10.17803/1729-5920.2022.192.11.112-119. EDN XMHEAJ.
2. *Виноградов В.А., Кузнецова Д.В.* Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. Т. 17. № 2. С. 215–240. DOI: 10.17323/2072-8166.2024.2.215.240. EDN ALACUF.
3. *Mason S., Seng D.* Artificial intelligence and Evidence // Singapore Academy of Law Journal. 2021. No. 33. P. 241–279. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3924762 (дата обращения: 01.06.2025).
4. *Данилова В.А., Левкин Д.М.* Правовые аспекты регулирования «deepfake» технологии в России // Право и государство: теория и практика. 2022. № 7 (211). С. 88–91. DOI: 10.47643/1815-1337.2022.7.88. EDN EUVFQP.
5. *Епифанова Т.В., Копейкин К.И.* Проблемы законодательного регулирования объектов, созданных с использованием дипфейк-технологии в России и за рубежом // Северо-Кавказский юридический вестник. 2024. № 3. С. 121–128. https://doi.org/10.22394/2074-7306-2024-1-3-121-128. EDN KMWGMQ
6. *Калятин В.О.* Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87–103. DOI: 10.37239/0869-4400-2022-19-7-87-103. EDN FENGGS.
7. *Токарев А.М.* Правовое регулирование дипфейк технологий в Российской Федерации // Евразийский юридический журнал. 2024. № 4 (191). С. 188–190. DOI: 10.46320/2073-4506-2024-4-191-188-190. EDN KTQEZL.
8. *Яткевич О.Г., Вершинина О.В.* Дипфейк: от пользы до угрозы неприкосновенности прав человека // Международный журнал конституционного и государственного права. 2023. № 1. С. 54–58. EDN VYOISS.
9. *Волкова Г.Е.* К вопросу о защите прав личности в условиях распространения дипфейк-технологий // Юристъ-Правоведъ. 2023. № 3(106). С. 15–22. EDN YYWIGR.
10. *Киселёв А.С.* О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64. DOI: 10.18384/2310-6794-2021-3-54-64. EDN AHJBNH.

11. *Ситник В.Н.* Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // Уральский журнал правовых исследований. 2022. № 3. С. 76–83. DOI: 10.34076/2658_512X_2022_3_76. EDN OUPAOB.

References

1. Dobrobaba M.B. (2022) Deepfakes as a threat to human rights. *Lex Russica*. Vol. 75. No. 11. Pp. 112–119. DOI: 10.17803/1729-5920.2022.192.11.112-119 (In Russian).
2. Vinogradov V.A., Kuznetsova D.V. (2024) Foreign experience in the legal regulation of deepfake technology. *Law. Journal of the Higher School of Economics*. Vol. 17. No. 2. Pp. 215–240. DOI: 10.17323/2072-8166.2024.2.215.240 (In Russian).
3. Mason S., Seng D. (2021) Artificial intelligence and Evidence. *Singapore Academy of Law Journal*. No. 33. Pp. 241–279. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3924762 (accessed 01.06.2025).
4. Danilova V.A., Levkin D.M. (2022) Legal aspects of regulation of "deepfake" technology in Russia. *Law and State: The Theory and Practice*. No. 7 (211). Pp. 88–91. DOI: 10.47643/1815-1337.2022.7.88 (In Russian).
5. Epifanova T.V., Kopeikin K.I. (2024) Problems of legislative regulation of facilities created using deepfake technology in Russia and abroad. North Caucasus Legal Vestnik. No. 3. Pp. 121–128. DOI: https://doi.org/10.22394/2074-7306-2024-1-3-121-128 (In Russian).
6. Kalyatin V.O. (2022) Deepfake as a legal problem: New threats or new opportunities? *Statute*. No. 7. Pp. 87–103. DOI: 10.37239/0869-4400-2022-19-7-87-103 (In Russian).
7. Tokarev A.M. () Legal regulation of deepfake technologies in the Russian Federation. *Eurasian Law Journal*. No. 4 (191). Pp. 188–190. DOI: 10.46320/2073-4506-2024-4-191-188-190 (In Russian).
8. Yatkevich O.G., Vershinina O.V. (2023) Deepfake: From benefits to threats to the inviolability of human rights. *International Journal of Constitutional and State Law*. No. 1. Pp. 54–58. (In Russian).
9. Volkova G.E. (2023) On the issue of protecting the rights of the individual in the context of the spread of deepfake technologies. *Yurist-Pravoved*. No. 3(106). Pp. 15–22. (In Russian).
10. Kiselev A.S. (2021) On the Expansion of Legal Regulation in the Field of Artificial Intelligence: Deepfake as a Threat to National Security. *Bulletin of Moscow Region State University. Series: Jurisprudence*. No. 3. Pp. 54–64. DOI: 10.18384/2310-6794-2021-3-54-6 (In Russian).
11. Sitnik V.N. (2022) Prospects for establishing criminal liability for crimes committed using deepfake technology. *Ural Journal of Legal Research*. No. 3. Pp. 76–83. DOI: 10.34076/2658_512X_2022_3_76 (In Russian).

Поступила в редакцию: 16.06.2025
Поступила после рецензирования: 30.06.2025
Принята к публикации: 12.07.2025

Received: 16.06.2025
Revised: 30.06.2025
Accepted: 12.07.2025