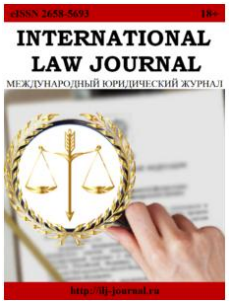

Научно-исследовательский журнал «International Law Journal»
https://ilj-journal.ru
2025, Том 8, № 8 / 2025, Vol. 8, Iss. 8 https://ilj-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.1.2. Публично-правовые (государственно-правовые) науки (юридические науки)
УДК 347.3

Правовое регулирование искусственного интеллекта в странах ЕАЭС

[1] Воробьева Н.В.,
[1] Омский государственный университет путей сообщения

Аннотация: *в статье рассматриваются проблемы правового регулирования использования deepfake-технологий в контексте угроз национальной безопасности. Проводится сравнительно-правовой анализ законодательства Российской Федерации, Республики Казахстан, Республики Беларусь, Республики Кыргызстан, Республики Армения в области противодействия терроризму, экстремизму и информационным преступлениям. Особое внимание уделяется применению положений Уголовного кодекса РФ, Федеральных законов «О противодействии терроризму», «О противодействии экстремистской деятельности» и «Об информации, информационных технологиях и защите информации». Рассмотрена судебная практика по статьям 128, 128.1, 137, 138, 159, 159.3, 159.6, 163, 165, 205, 205.2, 207, 207.3, 272.1 УК РФ. Предложены направления совершенствования законодательства, включая разработку самостоятельной нормы, предусматривающей ответственность за создание и распространение контента, сгенерированного с использованием технологий подмены личности (deepfake).*

Ключевые слова: *deepfake, сгенерированный контент, искусственный интеллект, уголовное право, экстремизм, терроризм, информационная безопасность, законодательство*

Для цитирования: Воробьева Н.В. Правовое регулирование искусственного интеллекта в странах ЕАЭС // International Law Journal. 2025. Том 8. № 8. С. 87 – 95.

Поступила в редакцию: 24 августа 2025 г.; Одобрена после рецензирования: 21 октября 2025 г.; Принята к публикации: 16 декабря 2025 г.

Legal regulation of artificial intelligence in the EAEU countries

[1] Vorobyeva N.V.,
[1] Omsk State Transport University

Abstract: *the article considers the problems of legal regulation of the use of deepfake technologies in the context of threats to national security. A comparative legal analysis of the legislation of the Russian Federation, the Republic of Kazakhstan, the Republic of Belarus, the Kyrgyz Republic, and the Republic of Armenia in the field of countering terrorism, extremism, and information crimes is provided. Particular attention is paid to the application of the provisions of the Criminal Code of the Russian Federation, the Federal Laws "On Countering Terrorism", "On Countering Extremist Activity" and "On Information, Information Technology, and Information Protection" is considered. Judicial practice under Articles 128, 128.1, 137, 138, 159, 159.3, 159.6, 163, 165, 205, 205.2, 207, 207.3, 272.1 of the Criminal Code of the Russian Federation is considered. Directions for improving legislation are proposed, including the development of an independent norm providing for liability for the creation and distribution of content generated using identity substitution technologies (deepfake).*

Keywords: *deepfake, artificial intelligence, criminal law, extremism, terrorism, information security, legislation*

For citation: Vorobyeva N.V. Legal regulation of artificial intelligence in the EAEU countries. International Law Journal. 2025. 8 (8). P. 87 – 95.

ISSN 2658-5693
https://ilj-journal.ru

The article was submitted: August 24, 2025; Approved after reviewing: October 21, 2025; Accepted for publication: December 16, 2025.

Введение

Развитие технологий искусственного интеллекта и генерации синтетического контента (deepfake) создало новые вызовы для правовой системы. Подмена личности, фальсификация аудио- и видеоматериалов могут использоваться для дезинформации, шантажа, политического давления и даже террористических целей. В этих условиях становится необходимым выработать эффективные правовые механизмы, направленные на предотвращение и пресечение подобных угроз.

В России регулирование вопросов, связанных с использованием deepfake-технологий, осуществляется в рамках действующих норм уголовного законодательства и специальных федеральных законов. Наиболее применимыми являются статьи 205, 205.1, 205.2, 207, 280, 280.1, 282, 128.1, 137 и 159 УК РФ, а также положения Федеральных законов противодействия преступлениям, совершаемых с помощью ИИ является ФЗ № 149-ФЗ «Об информации, информационных технологиях и защите информации» (2006 г.), который позволяет ограничивать доступ к материалам, признанным ложным и опасными, в том числе к экстремистским. В контексте deepfake-угроз применим к случаям, когда контент используется для запугивания, пропаганды, либо ложного оповещения об актах терроризма (статья 207 УК РФ применяется № 35-ФЗ «О противодействии терроризму» (2006 г.). Также в контексте выявления deepfake-контента, содержащего призывы к насилию, вражде, который может быть признан экстремистским и подлежит блокировке применяется № 114-ФЗ «О противодействии экстремистской деятельности» (2002 г.).

Главная проблема заключается в отсутствии прямой уголовно-правовой нормы, предусматривающей ответственность за создание и распространение deepfake-контента. В зарубежной практике аналогичные нормы уже внедряются, например, в США действуют положения о защите от манипулированных медиа Deepfake Accountability Act [1]. Российская правовая система требует адаптации к этим вызовам через уточнение состава преступлений и введение специальных определений.

Материалы и методы исследований

Применялись следующие общетеоретические методы: сравнительно-правовой метод, системный анализ для исследования нормативно-правовой базы применения технологий ИИ в таможенном администрировании. Частные методы исследования: библиометрический анализ, а также контент анализ сайтов таможенных служб Российской Федерации, КНР, США, Уганды, Канады, ЕС, Индии.

Результаты и обсуждения

16 сентября 2024 г. в Государственную Думу РФ был внесен законопроект № 718538-8 («О внесении изменений в Уголовный кодекс Российской Федерации» в части установления уголовной ответственности за преступления с использованием технологий подмены личности [2]. Он направлен на устранение правового вакуума в части ответственности за преступления, совершаемые с помощью технологий подмены личности (например, с применением дипфейков, генеративного ИИ, имитации голоса и т.п.). Эксперты подчеркивают особую актуальность в связи с рост рисков, связанных с распространением подлинно выглядящих, но ложных аудио- и видеоматериалов, использование биометрии и ИИ для обмана либо сокрытия личности [3, с. 6-15; 4]. Законопроект ставит задачу укрепить защиту личности, общества и государства от технологий подмены, повысить эффективность расследования таких преступлений, и адаптировать уголовное законодательство к цифровой реальности.

Законопроект вносит изменения в Уголовный кодекс Российской Федерации (УК РФ), предполагая конкретизацию состава преступлений, связанных с использованием технологий подмены личности. Предусматривает элементы квалификации: создание, распространение, использование поддельного/изменённого изображения, аудио- или видеозаписи с имитацией голоса, или иного контента, вводящего в заблуждение (например, выдающего себя за лицо другое). Акцент делается на том, что преступление совершается с использованием цифровых технологий (ИИ-генерация, дипфейк-алгоритмы) либо путём выдачи себя за другое лицо через технические средства.

В ряде исследованиях И.С. Алихаджиевой и И.Н. Мосечкина подчеркивается необходимость установления уголовной ответственности за создание и распространение дипфейков, особенно если они используются для мошенничества, шантажа или распространения порнографического и экстремистского контента [5, с. 154-171; 6, с. 95-110].

Исследователи отмечают пробелы в законодательстве, связанные с определением прав на контент, созданный с помощью ИИ, и необходимостью балансирования между свободой творчества и защитой прав личности. К примеру, в статье Н.В. Архиереева Н.В. [7, с. 22-30] анализируются правовые аспекты регули-

ISSN 2658-5693
https://ilj-journal.ru

рования дипфейков в России, включая их квалификацию как объектов авторского и гражданского права. Также рассматривают вопросы авторского права в отношении произведений, созданных с применением технологий deepfake, указывая на сложности идентификации авторства и охраны интеллектуальной собственности в условиях автоматизированного контентогенерирования.

Исследователь А.В. Гаврицкий А.В. [8, с. 319-322] анализирует взаимосвязь между дипфейками и современными формами интернет-мошенничества: от кражи персональных данных до фишинга 2.0. Отмечается, что преступники активно используют ИИ для имитации личностей и получения финансовой выгоды, что требует совершенствования уголовного законодательства и механизмов цифровой идентификации.

Ученые обращают внимание на системные угрозы эпохи ИИ и трансформацию преступности в цифровом обществе. Рост киберпреступлений, манипуляций и атак на личность через виртуальные каналы требует выработки комплексных мер противодействия, включая международное сотрудничество.

Проблемы защиты частной жизни и персональных данных в виртуальной реальности анализируются Кузнецовой О.А. [9, с. 244-253], Хохловой Е.В. [10, с. 96-111]. Авторы отмечают необходимость правового регулирования использования биометрических данных и голоса в метавселенной и онлайн-пространстве, где дипфейки могут нарушать права граждан на неприкосновенность частной жизни.

В более широком контексте цифрового права и государственного регулирования ИИ подчеркивается потребность в создании единой концепции правового статуса ИИ и этических стандартов его применения, особенно в правоохранительной деятельности.

Р.А. Будник Р.А. [11, с. 35-52] рассматривает вопросы реализации конституционных гарантий и защиты прав человека в условиях «нейропрогресса» и цифровизации, а также влияние блокчейн-технологий на обеспечение прозрачности и правовую защищённость граждан.

В целом, проанализированные работы показывают, что технологии deepfake и ИИ становятся одной из ключевых проблем современного права [12, с. 177-188; 13, с. 189-196; 14, с. 748-760; 15, с. 165-172]. Они требуют не только правовой адаптации, но и развития этических, технических и криминалистических инструментов регулирования, направленных на защиту личности, общества и государства в условиях цифровой реальности.

Обратимся к судебной практике. В 2023 г. термин «дипфейк» впервые был применен в гражданском процессе по делу № А40-165705/2023 в отношении авторского права о взыскании компенсации за нарушение исключительных прав. Суд по интеллектуальным правам признал автором фотографии сгенерированной с помощью ИИ – пользователя и отклонил кассационную жалобу компании «Бизнес-аналитика» на решения нижестоящих судов о взыскании с нее 500 000 руб. за неправомерное использование видеоролика, созданного с помощью технологии дипфейк [16, //sudact.ru/arbitral/doc/CDwFf05hlerK/].

Обратимся к опубликованным судебным решениям на платформе //sudact.ru/, приведем примеры из приговорам по делам, в которых использовался искусственный интеллект и генерации синтетического контента в преступных целях. В отношении преступлений против жизни и здоровья: по статье 128.1 УК РФ «Клевета» сгенерированный контент был использован для дискредитации военнослужащего с целью обвинения в финансировании ВСУ, шпионаже и государственной измене (дело № 1-10/2025) [16, //sudact.ru/regular/doc/4H6mk2wSM4UL/]. По статье 137 УК РФ – «Нарушение неприкосновенности частной жизни» посредством передачи баз данных с персональной информацией, в том числе телефонных номеров из государственных и коммерческих организаций, например: передача сведений об абонентах телефонной компании (дело № 01-0170/2025) [16, //sudact.ru/regular/doc/Bd7cxJEe3xoR/], использование сведений МВД, злоупотребление служебным положением (дело № № 1-109/2025) [16, //sudact.ru/regular/doc/zRA0KUy8SLJa/], использование «неустановленных технических средств» для передач данных из ФИС ГИБДД (дело № 1-1330/2024) [16, //sudact.ru/regular/doc/jJvBfXlPVNlY/]. Существует риск попадания под статью случаев с незначительным вредом из-за нечетких критериев объективной стороны и общественной опасности.

Судебная практика по статье 138 содержит примеры установки трекеров в автомобиль для негласного получения сведений: дело № № 1-79/2025 [16, //sudact.ru/regular/doc/mX72KTYRIhVg/], дело № 01-0163/2025 [16, //sudact.ru/regular/doc/pxGSmofnnwQa/], дело № 1-103/2025 [16, //sudact.ru/regular/doc/qCcfmSLBy2Hv/]. В одном из дел (№ 1-84/2025) фигурирует преступление начальника службы информационной безопасности, использующего служебный доступ для неправомерного получения сведений [16, //sudact.ru/regular/doc/sCof0VdrxoR/].

Следующую классификационную группу составляют преступления в сфере экономики с использованием технологии voice-cloning для обмана и хищения средств, т.е. подделка голоса для списания денег/доступа к личному кабинету банка или порталу Госуслуг (статьи 159, 159.3, 159.6). Слабая практика

ISSN 2658-5693
https://ilj-journal.ru

доказывания материального ущерба в «электронной» форме приводит к тому, что квалифицировать voice-cloning как средство совершения мошенничества практически невозможно. Как правило, под эту категорию подпадают различные «технические» способы мошенничества, за исключением тех, что предусматривают социальную инженерию. Приведем несколько характерных примеров, дело № 1-379/2024: была создана преступная группировка с использованием IP-телефонии [16, //sudact.ru/regular/doc/XW0LNH7qH8Yg/]. Второй пример: использование электронных средств в рамках незаконного оборота наркотиков для информирования с помощью социальных сетей и платформ о месте нахождения «закладок» (дело № № 1-113/2025) [16, //sudact.ru/regular/doc/ijFCKQS4xPUm/]. Следующий пример: размещение ложной информации о продаже недвижимости на торговых площадках (Авито) и подделка личности продавца (дело № № 1-32/2025) [16, //sudact.ru/regular/doc/leREk8q8K11v/]. А также подделка сведений в учетных системах (1С-Бухгалтерия) (дело № 1-93/2025) [16, //sudact.ru/regular/doc/1DIj0EhEZIot/].

Технологии ИИ могут использоваться в целях взыскания кредитной задолженности (совершение звонков «роботом- коллектором», автоматизированные обзвоны, deepfake-угрозы) для принуждения к уплате задолженности, фальсификация биометрических данных или иных сведений с помощью ИИ фиксируется в судебной практике по статьям 163, 165 УК РФ. К примеру, в приговоре по делу № по делу № 1-41/2025 указывается, что преступники фальсифицировали видеозапись о задержании, а также подложное постановление о возбуждении уголовного дела и совершили мошеннические действия на сумму свыше 3 млн 300 тысяч рублей [16, //sudact.ru/regular/doc/vDJJSIiNA4YT/]. Шантаж с использованием фейковой фотографии непристойного характера (интимный дипфейк) был использован в деле № 1-93/2025 [16, //sudact.ru/regular/doc/r00FYWHYa4Z8/]. В деле № 1-45/2025 злоумышленники вымогали и похитили 1 млн рублей у матери военнослужащего, проходящего службу по контракту МО РФ в зоне СВО [16, //sudact.ru/regular/doc/bI65xi1kw8QX/].

Также отметим использование дипфейков для вербовки/пропаганды в преступлениях против общественной безопасности (статьи 205, 207 УК РФ). Технологии «синтеза образа/голоса» создают возможность создания дипфейков, имитирующих взрывы, нападения, угрозы или использование таких видео использование для создания паники в обществе. Deepfake-видео или аудио, направленные на сбор средств, вербовку, пропаганду терроризма (статья 205.1); публичные призывы к террористической деятельности; ИИ-сгенерированные речи/видео с призывами, выданные за известных лиц, Deepfake-агитация, использование ИИ-контента для вербовки (статья 205.2). Пример: дело № 1-160/2025 с использованием краудфандинга для сбора денег в пользу запрещенных формирований («Легион свободы» – запрещенная в РФ организация, внесенная в Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими: Федеральная Служба Безопасности // http://www.fsb.ru/fsb/npd/terror.htm) [16, //sudact.ru/regular/doc/7D3ol9uMIcZx/].

Deepfake-видео заменяют «телефонный терроризм» (статья 207), т.к. процессуальные механизмы быстрых блокировок и проверки не отрегулированы необходимо ввести процедуры экстренной блокировки контента, сотрудничество платформ и силовых структур, критерии проверки (согласно правовым нормам ФЗ №35-ФЗ; ФЗ №149-ФЗ). Судебная практика содержит примеры ложных сообщений , в том числе через чатботы (дело № 1-38/2025) [16, sudact.ru/regular/doc/2moFMxT7C8NZ/]. Преступное использование ИИ может осуществляться с целью политической дезинформации и подрыв доверия к государственной власти (Deepfake с вымышленными заявлениями лидеров, вымышленными событиями). В судебной практике по статье 207.3 в деле № 1-6/2025 подсудимые, выехавшие из РФ в США в связи с несогласием по поводу проведения специальной военной операции разместили на странице в социальной сети ВК смоделированные ИИ подложные сведения о ВС РФ [16, //sudact.ru/regular/doc/MWDUNuQZkjge/].

Следующей группой являются преступления, связанные с незаконным обращением и обработкой персональных данных (статья 272.1). Приведем несколько примеров, с помощью ИТ преступник разблокировал iPhone и извлек средства (дела № 01-0092/2025, № 1-72/2025) [16, //sudact.ru/regular/doc/KVoqSwuER6r4/;//sudact.ru/regular/doc/Ydq9QYGOuldp/]. В деле № 1-67/2025) преступник обладал доступом к обеспеченным специальными средствами защиты в виде персональных логинов и паролей компьютерным базам данных об абонентах оператора сотовой связи ПАО «МобильныеТелеСистемы» [16, //sudact.ru/regular/doc/dgYGRhTGWdJv/]. Технологии ИИ активно используются злоумышленниками во множестве сфер, от личных атак и шантажа до экономических преступлений и попыток дестабилизации общественной безопасности, о чем свидетельствует практика, зафиксированная в приговорах и решениях, опубликованных на платформе sudact.ru.

ISSN 2658-5693
https://ilj-journal.ru

Сравним понимание «deepfake» и использование уголовных мер противодействия сгенерированному вредоносному контенту в странах ЕАЭС.

Уголовное законодательство Республики Беларусь трактует угрозы национальной безопасности широко, что позволяет охватывать deepfake-контент, подрывающий доверие к власти (статьи 349, 361, 361.1 УК РБ) [17, с. 81-89]. Использование deepfake-видео, имитирующих выступления политиков с подстрекательством к беспорядкам, сгенерированных видео/аудио с подложными заявлениями официальных лиц, порочащими госорганы. Контроль за информацией усилен в административном порядке: глубокая интеграция с мерами государственной цензуры и мониторинга сетевого пространства, умышленного унижения чести и достоинства личности, выраженного в неприличной форме, деяния субъекта могут рассматриваться как оскорбление (например, по ч. 2 ст. 10.2 КоАП РБ, статьям 188, 203 УК РБ). Однако уголовная ответственность в таком случае наступает только в отношении отдельных категорий потерпевших (статьи 368, 369, 391, 444 УК РБ). Дипфейк может выступать составляющим элементом способа совершения хищения в составах преступлений вымогательства (ст. 208 УК РБ), мошенничества (ст. 209 УК РБ), хищения имущества путем модификации компьютерной информации (ст. 212 УК РБ). Таким образом, акцент сконцентрирован на защите репутации государства, а не только личности.

В Республике Казахстан законопроект «Об искусственном интеллекте» 29 октября 2025 г. был согласован с сенаторами и вынесен на обсуждение Мажилиса [18]. В настоящее время в Уголовном кодексе наряду с уголовными санкциями действуют административные блокировки и технический контроль цифровых платформ: уголовная ответственность за распространение deepfake-видео, создающих иллюзию теракта, паники, с призывами к террористическим действиям (статьи 255, 256 УК РК), за ИИ-сгенерированные изображения и тексты, содержащие признаки розни (статья 174 УК РК), за deepfake-материалы (статья 274 УК РК), за мошеннические действия с помощью ИТ-технологий (статья 232.1).

В Республике Кыргызстан не предусмотрена уголовная ответственность за генерацию/распространение дипфейков. Тем не менее, существуют проектные инициативы, но формализация и технические детали (как отличать редактирование от генерации ИИ, доказательная база) остаются предметом дискуссии [19]. Публичный скандал 2024 г., связанный с активным распространением фейкового видео с депутатом М. Абдалиевым (по поводу «Кыргызнефтегаз») повлиял на усиление внимания в скорейшее законодательное регулирование использования ИИ.

В Уголовном кодексе Республики Кыргызстан предусмотрена ответственность, к примеру, за неправомерное распространение интимных материалов (т.н. «секс-дипфейки») – по статье 190 УК РК, распространение ложной информации (особенно в период выборов), при опасности вмешательства в выборный процесс и угрозе общественной безопасности (статья 199 УК РК). Манипуляции с виртуальными активами через ИТ-системы (статьи 208 ,209 УК РК), применяется и к случаям мошенничества с использованием интернет-технологий/мобильных средств, введена законодательная поправка, включающая передачу и продажу SIM-карт, электронных платежных инструментов, виртуальных кошельков третьим лицам. Составы по статям, связанным с незаконным доступом к компьютерной информации (статьи 289, 290, 291 УК РК), если при этом произошло уничтожение, блокировка, изменение или копирование информации. Зачастую контент генерируется и распространяется с серверов вне юрисдикции, что ставит задачи по экстрадиции и кооперации с международными платформами.

Отличие подхода к преступлениям, осуществляемым с помощью ИИ в Республике Армения: прямых «квазиспецифических» статей под словом «дипфейк» в тексте Уголовного кодекса (в открытом виде) долгое время не было, но правоохранительные органы уже начинают инициировать уголовные дела по фактам искусственно-созданных аудиозаписей/видео (например: подделанный аудиофайл, приписанный премьер-министру).

Тем не менее, в 24 главе Уголовного кодекса Республики Армения в практической применимости используются существующие статьи (мошенничество, распространение ложной информации, посягательства на честь и достоинство, нарушение тайны частной жизни, угрозы/шантаж и т.д.); отдельные аналитические публикации и СМИ указывают на серьезные штрафы/лишение свободы при квалификации деяния по различным составам (в т.ч. при вмешательстве в избирательный процесс). Завладение чужим имуществом или приобретение права на имущество путем обмана или злоупотребления доверием, когда дипфейк использован для завладения чужими средствами (банковские переводы, выдача денег) регулируется статьей 178 УК РА, кража имущества с помощью ИТ-технологий – статьей 181 УК РА, изменение или ущерб имуществу, подпадающий под категорию «киберпреступления» статьей 252 УК РА, повреждение или уничтожение компьютерных данных статьей 253 УК РА, разработка и использование вредоносных программ статьей 256 УК РА.

ISSN 2658-5693
https://ilj-journal.ru

Выводы

Таким образом, в законодательстве стран ЕАЭС прямое упоминание deepfake отсутствует, на уровне законодательной инициативе есть в РФ, Казахстане и Кыргызстане. Фокус регулирования в России направлен на защиту личности, общества, государства от ложных и опасных цифровых сообщений (инструмент регулирования: уголовное право и специальные ФЗ № 35-ФЗ, 114-ФЗ, 149-ФЗ), в Казахстане на борьбу с дезинформацией и рознью (уголовная и информационная ответственность), в Кыргызстане на защиту интеллектуальной собственности и борьбу с мошенничеством (уголовная и административная ответственность), в Армении на преступления в сфере высоких технологий (в основном также с мошенничеством, глава 24 УК РА, а также законодательные инициативы Министерства высокотехнологичной промышленности), в Беларуси на защиту национальной безопасностью (уголовно-правовой контроль и надзор).

В странах ЕАЭС используются уже существующие уголовные нормы для борьбы с последствиями применения deepfake, но нет специальных статей, адресованных этой технологии напрямую. Российская модель делает акцент на системности (терроризм, экстремизм, мошенничество, неприкосновенность частной жизни) и стремится создать новый состав преступления через законопроект № 718538-8. Белорусская система ориентирована на государственно-политическую безопасность и жестко связывает deepfake с подрывом доверия к власти. Казахстанская модель адаптирована к борьбе с дезинформацией и социальной враждой, где deepfake рассматривается как форма ложных сведений. Кыргызстанская модель направлена на борьбу с мошенничеством, deepfake рассматривается как частный вариант осуществления имущественных преступлений. Армянская модель не специфицирует deepfake, рассматривая как часть преступлений против информационной безопасности, включенных в уголовный кодекс.

Основная проблема всех систем – это отсутствие технологических критериев, позволяющих однозначно квалифицировать deepfake-контент. Общими определениями, вводимыми в ФЗ и кодексы являются: «синтетический контент (deepfake)» – аудио, видео, изображение или комбинированный мультимедиа-контент, полностью или частично созданный с помощью алгоритмов генеративного ИИ либо иными средствами искусственной подмены внешности/голоса/позывов, которые вводят в заблуждение относительно подлинной личности автора или события и «использование преступной цели» – распространение, демонстрация, передача или иное применение синтетического контента с целью совершения уголовно наказуемого деяния (терроризм, экстремизм, мошенничество, клевета, нарушение частной жизни и т.д.).

Унификация подходов в рамках ЕАЭС возможна и необходима: deepfake-угрозы трансграничны, стандарты экспертизы и оперативного реагирования должны быть общими. Законодатели должны комбинировать: точечные уголовно-правовые нормы с четкими признаками состава; процессуальные механизмы быстрой блокировки и проверки контента; требования к платформам и сильные гарантии защиты прав граждан. Техническая база (экспертизы, центры, стандарты) являются ключом к адекватной реализации норм и снижению рисков как для безопасности, так и для свободы выражения. Таким образом, проведенное исследование позволяет выявить правовые риски применения ИИ, а также пробелы в отечественном законодательстве.

Во-первых, идентификация подлинности контента, невозможность однозначно доказать, что видео или аудио материал являются сгенерированными в связи с тем, что отсутствуют стандарты экспертизы. Таким образом, к технической стороне доказательной базы предъявляются дополнительные требования.

Во-вторых, требуется разработка стандартов верификации источников, создание и государственная аккредитация экспертных судебно-технических лабораторий. Не менее важны аспектом является ответственность платформ и хостеров за дипфейки, размещённые пользователями, в настоящее время отсутствует единый механизм распознавания и прозрачность алгоритмов модерации ставится под вопрос. Введение обязанность маркировать ИИ-контент, на наш взгляд следует внести в № 149-ФЗ «Об информации, информационных технологиях и защите информации», ввести единые правила для хостинг-провайдеров.

В-третьих, быстрая устареваемость норм приводит к тому, что формулировка статей приводит к «пробелам». Необходимо включать гибкие диспозитивы, «технологические» определения и механизмы регулярного пересмотра в новые нормы. Кроме того, в современных геополитических условиях возникает риск и трудности международного сбора доказательств, т.к. контент может храниться за рубежом; недружественные страны могут отказать в экстрадиции данных или в обмене цифровыми доказательствами.

ISSN 2658-5693
https://ilj-journal.ru

Список источников

1. H.R. 5586 (118th): DEEPFAKES Accountability Act. URL: https://www.govtrack.us/congress/bills/118/hr5586 (дата обращения: 03.08.2025)

2. Законопроект № 718538-8 О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности). URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 03.01.2025)

3. Булочников С.Ю. О правотворчестве и правовых новациях в части защиты от утечек персональных данных // Новизна. Эксперимент. Традиции» (Н.Экс.Т). 2025. Т. 11. Вып. 1 (29). С. 6 – 15.

4. Бодров Н.Ф., Лебедева А.К. Перспективы правового регулирования и алгоритм маркировки генеративного контента // Пенитенциарная наука. 2024. № 4 (68). URL: https://cyberleninka.ru/article/n/perspektivy-pravovogo-regulirovaniya-i-algoritm-markirovki-generativnogo-kontenta (дата обращения: 23.10.2025)

5. Алихаджиева И.С. Перспективы установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности (законопроект № 718538-8) // Известия Юго-Западного государственного университета. Серия: История и право. 2025. Т. 15. № 2. С. 154 – 171. DOI 10.21869/2223-1501-2025-15-2-154-171

6. Мосечкин И.Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16. № 1. С. 95 – 110. DOI 10.21638/spbu14.2025.107

7. Архиереев Н.В. Правовое регулирование создания и использования дипфейков // Правовое государство: теория и практика. 2025. № 2 (80). С. 22 – 30. DOI 10.33184/pravgos-2025.2.3

8. Гаврицкий А.В., Рогава И.Г. Проблемы расследования преступлений, связанных с созданием и распространением дипфейков // Аграрное и земельное право. 2025. № 7. С. 319 – 322. DOI 10.47643/1815-1329-2025-7-319

9. Кузнецова О.А., Маджумаев М.М. Защита частной жизни в виртуальной реальности: ответственность за использование дипфейк-контента в метавселенной // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5 (129). С. 244 – 253. DOI 10.17803/2311-5998.2025.129.5.244-253

10. Хохлова Е.В. Уголовно-правовые и цивилистические аспекты охраны голоса // Известия Юго-Западного государственного университета. Серия: История и право. 2025. Т. 15. № 1. С. 96 – 111. DOI 10.21869/2223-1501-2025-15-1-96-111

11. Будник Р.А. Права человека в реалиях нейропрогресса: юридические средства компенсации нейротехнологических рисков // Журнал российского права. 2025. Т. 29. № 3. С. 35 – 52. DOI 10.61205/S160565900032805-9

12. Дружинин А.М. Деструктивные элементы онлайн-коммуникации // Вестник Томского государственного университета. Философия. Социология. Политология. 2025. № 85. С. 177 – 188. DOI 10.17223/1998863X/85/15

13. Мочалкина И.С. Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Вестник Университета имени О.Е. Кутафина (МГЮА). 2025. № 5 (129). С. 189 – 196. DOI 10.17803/2311-5998.2025.129.5.189-196

14. Омуракунова А.А., Тентиев Р.Б., Касыбеков А.У. Искусственный интеллект в политических коммуникациях: трансформация PR-технологий и вызовы цифровой этики // Известия Кыргызского государственного технического университета им. И. Раззакова. 2025. № 3 (75). С. 748 – 760. DOI 10.56634/16948335.2025.3.748-760

15. Симонян А.А. Генеративный искусственный интеллект и DeepFake-технологии как угроза информационной безопасности граждан // Вопросы российского и международного права. 2025. Т. 15. № 2-1. С. 165-172.

16. Судебные и нормативные акты РФ: Крупнейшая в сети база судебных и нормативных актов. URL: https://sudact.ru/ (дата обращения 3.11.2025)

17. Полещук Д.Г. Уголовная ответственность за использование дипфейков: современное состояние и перспективы // Право.by. 2024. № 4 (90). С. 81 – 89.

18. В Казахстане введут ответственность за дипфейки. URL: https://www.zakon.kz/obshestvo/6495940-v-kazakhstane-vvedut-otvetstvennost-za-dipfeyki.html (дата обращения: 03.08.2025)

19. В Кыргызстане предлагают на законодательном уровне бороться с дипфейками – подробности. URL: https://economist.kg/vlast/2024/06/10/v-kyrghyzstanie-priedlaghaiut-na-zakonodatielnom-urovnie-borotsia-s-dipfieikami-podrobnosti/ (дата обращения: 3.08.2025)

20. Уголовный кодекс Кыргызской Республики от 28 октября 2021 года № 127 (с изменениями и дополнениями по состоянию на 28.07.2025 г.). URL: https://online.zakon.kz/Document/?doc_id=36675065 (дата обращения: 3.11.2025)

21. УК РК – Уголовный кодекс Республики Казахстан 2025. URL: https://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 03.08.2025)

22. Legislation: National Assemly of RA. URL: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus (дата обращения: 03.08.2025)

23. УК РБ – Уголовный кодекс Республики Беларусь 2025. URL: https://online.zakon.kz/Document/?doc_id=30414984 (дата обращения: 03.08.2025)

24. «Уголовный кодекс Республики Беларусь» – тематические подборки НПА на Pravo.by. URL: https://pravo.by/document/?guid=3871&p0=Hk9900275 (дата обращения: 03.08.2025)

25. "Уголовный кодекс Российской Федерации" (УК РФ) от 13.06.1996 N 63-ФЗ (последняя редакция) / КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 03.08.2025)

References

1. H.R. 5586 (118th): DEEPFAKES Accountability Act. URL: https://www.govtrack.us/congress/bills/118/hr5586 (date of access: 03.08.2025)

2. Bill No. 718538-8 On Amendments to the Criminal Code of the Russian Federation (in terms of establishing criminal liability for committing crimes using identity substitution technologies). URL: https://sozd.duma.gov.ru/bill/718538-8 (date of access: 03.01.2025)

3. Bulochnikov S. Yu. On lawmaking and legal innovations in terms of protection against personal data leaks. Novelty. Experiment. Traditions ”(N. Ex. T). 2025. Vol. 11. Issue. 1 (29). P. 6 – 15.

4. Bodrov N.F., Lebedeva A.K. Prospects for Legal Regulation and an Algorithm for Marking Generative Content. Penitentiary Science. 2024. No. 4 (68). URL: https://cyberleninka.ru/article/n/perspektivy-pravovogo-regulirovaniya-i-algoritm-markirovki-generativnogo-kontenta (date of access: 23.10.2025)

5. Alikhadzhieva I.S. Prospects for Establishing Criminal Liability for Committing Crimes Using Identity Substitution Technologies (Bill No. 718538-8). Bulletin of the South-West State University. Series: History and Law. 2025. Vol. 15. No. 2. P. 154 – 171. DOI 10.21869/2223-1501-2025-15-2-154-171

6. Mosechkin I.N. Deepfake technologies and biometric data: directions of criminal-legal regulation. Bulletin of St. Petersburg University. Law. 2025. Vol. 16. No. 1. P. 95 – 110. DOI 10.21638/spbu14.2025.107

7. Arkhiereev N.V. Legal regulation of the creation and use of deepfakes. The rule of law: theory and practice. 2025. No. 2 (80). P. 22 – 30. DOI 10.33184/pravgos-2025.2.3

8. Gavritsky A.V., Rogava I.G. Problems of Investigation of Crimes Related to the Creation and Distribution of Deepfakes. Agrarian and Land Law. 2025. No. 7. P. 319 – 322. DOI 10.47643/1815-1329-2025-7-319

9. Kuznetsova O.A., Madzhumaev M.M. Protecting Privacy in Virtual Reality: Liability for the Use of Deepfake Content in the Metaverse. Bulletin of O.E. Kutafin Moscow State Law University (MSAL). 2025. No. 5 (129). P. 244 – 253. DOI 10.17803/2311-5998.2025.129.5.244-253

10. Khokhlova E.V. Criminal and civil aspects of voice protection. Bulletin of the South-West State University. Series: History and Law. 2025. Vol. 15. No. 1. P. 96 – 111. DOI 10.21869/2223-1501-2025-15-1-96-111

11. Budnik R.A. Human rights in the realities of neuroprogress: legal means of compensating for neurotechnological risks. Journal of Russian Law. 2025. Vol. 29. No. 3. P. 35 – 52. DOI 10.61205/S160565900032805-9

12. Druzhinin A.M. Destructive Elements of Online Communication. Bulletin of Tomsk State University. Philosophy. Sociology. Political Science. 2025. No. 85. P. 177 – 188. DOI 10.17223/1998863X/85/15

13. Mochalkina I.S. Criminological Counteraction to Economic Crimes Committed with the Use of Information and Telecommunication Technologies. Bulletin of O.E. Kutafin Moscow State Law University (MSAL). 2025. No. 5 (129). P. 189 – 196. DOI 10.17803/2311-5998.2025.129.5.189-196

14. Omurakunova A.A., Tentiev R.B., Kasybekov A.U. Artificial Intelligence in Political Communications: Transformation of PR Technologies and Challenges of Digital Ethics. Bulletin of the Kyrgyz State Technical University named after I. Razzakov. 2025. No. 3 (75). P. 748 – 760. DOI 10.56634/16948335.2025.3.748-760

15. Simonyan A.A. Generative Artificial Intelligence and DeepFake Technologies as a Threat to the Information Security of Citizens. Issues of Russian and International Law. 2025. Vol. 15. No. 2-1. P. 165 – 172.

16. Judicial and regulatory acts of the Russian Federation: The largest online database of judicial and regulatory acts. URL: https://sudact.ru/ (date of access: 03.07.2025)

17. Poleshchuk D.G. Criminal liability for the use of deepfakes: current status and prospects. Pravo.by. 2024. No. 4 (90). P. 81 – 89.

18. Kazakhstan to introduce liability for deepfakes. URL: https://www.zakon.kz/obshestvo/6495940-v-kazakhstane-vvedut-otvetstvennost-za-dipfeyki.html (date of access: 03.08.2025)

19. Kyrgyzstan proposes to combat deepfakes at the legislative level – details. URL: https://economist.kg/vlast/2024/06/10/v-kyrghyzstanie-priedlaghaiut-na-zakonodatielnom-urovnie-borotsia-s-dipfieikami-podrobnosti/ (date of access: 03.08.2025)

20. Criminal Code of the Kyrgyz Republic dated October 28, 2021, No. 127 (with amendments and additions as of July 28, 2025). URL: https://online.zakon.kz/Document/?doc_id=36675065 (date of access: 3.11.2025)

21. Criminal Code of the Republic of Kazakhstan 2025. URL: https://online.zakon.kz/Document/?doc_id=31575252 (date of access: 03.08.2025)

22. Legislation: National Assembly of the Republic of Kazakhstan. URL: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus (date of access: 03.08.2025)

23. УК РБ – Criminal Code of the Republic of Belarus 2025. URL: https://online.zakon.kz/Document/?doc_id=30414984 (date of access: 03.08.2025)

24. "Criminal Code of the Republic of Belarus" – thematic collections of regulatory legal acts on Pravo.by. URL: https://pravo.by/document/?guid=3871&p0=Hk9900275 (date of access: 03.08.2025)

25. "Criminal Code of the Russian Federation" (CC RF) of 13.06.1996 N 63-FZ (latest revision). Consultant-Plus. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (date of access: 03.08.2025)

Информация об авторе

Воробьева Н.В., доктор исторических наук, доцент, Омский государственный университет путей сообщения