

Аналитический обзор



О ФОРМИРОВАНИИ СТАНДАРТОВ РЕГУЛИРОВАНИЯ ГЕНЕРАТИВНОГО ИИ В КИТАЕ



Центр глобальной ИТ-кооперации
Москва 2026

Цитирование:

О формировании стандартов регулирования генеративного ИИ в Китае, Аналитический обзор, Центр глобальной ИТ-кооперации, авторы: Курбатова Т.А., Шамраев Р.А., под редакцией Игнатьева А.Г., 35 С, 2026

Citation:

Development of Standards for Regulating Generative AI in China, Analytical Report, Center for Global IT Cooperation, authors: Kurbatova T.A., Shamraev R.A., edited by Ignatiev A.G., 35 p., 2026

Краткая аннотация: в обзоре представлены общие подходы Китая к созданию правовой базы в области регулирования продуктов глубокого синтеза с использованием технологий ИИ с акцентом на законодательные рамки для обязательной и технически отслеживаемой маркировки ИИ-контента. Обзор не претендует на полную ревизию и детальное отражение регуляторных положений, а отражает лишь наиболее значимые регуляторные новеллы и правоприменительные практики.

Материал может быть полезен в качестве справочного материала профильным организациям, научно-исследовательским центрам, учебно-образовательным заведениям и различным площадкам развития в области цифровых технологий.

Ключевые слова: Китай, искусственный интеллект (ИИ), регулирование в области ИИ, дипфейки, генеративный ИИ, маркировка ИИ-контента, нормативно-правовые акты, законы, инструменты, стандарты, техническая стандартизация в области ИИ.

АНО «Центр компетенций по глобальной ИТ-кооперации» (<https://cgitc.ru/>) создан в 2020 году для экспертного изучения вопросов международного сотрудничества в сфере информационных технологий (ИТ), укрепления позиций России в глобальной ИТ-кооперации, в частности, продвижения новых подходов к многостороннему и равноправному управлению Интернетом на основе обеспечения безопасности и уважения национального суверенитета.

CGITC является членом Сектора развития электросвязи (ITU-D) Международного союза электросвязи, начиная с 2021 года Центр ежегодно представляет Россию на международном Форуме ООН по управлению Интернетом (IGF).

Центр проводит исследования и реализует проекты в области международного сотрудничества в сфере цифровой экономики, выпускает аналитические обзоры по развитию всего стека цифровых технологий (<https://cgitc.ru/research/>), помогает молодым исследовательским командам и начинающим разработчикам по продвижению инноваций и научных работ, в т. ч. ежегодно публикует [Сборник авторских статей](#) по развитию цифровой среды.

CGITC оказывает содействие продвижению экспорта продуктов и услуг в сфере ИКТ, организует деловые миссии за рубеж (календарь миссий – <https://cgitc.ru/export/>), предоставляет консалтинговые услуги и GR-поддержку по выводу российских ИТ-компаний на зарубежные рынки, имеет собственный маркетплейс продуктов и услуг (<https://itrussia.global/>).

Во взаимодействии с российским и международным сообществом CGITC на регулярной основе проводит ряд научных и экспертных круглых столов, конференций и вебинаров (<https://cgitc.ru/events/>).

CGITC является соорганизатором ежегодного Российского форума по управлению Интернетом (<https://rigf.ru>), ключевым организатором Молодежного российского форума по управлению Интернетом (<https://youth.rigf.ru>), в 2022 и 2023 годах - участник проекта Think20 исследовательской сети G20. В 2025 году Центр глобальной ИТ-кооперации выступал соорганизатором первого Глобального Цифрового Форума (<https://gdfconf.com>).

Правила использования Обзора

Настоящий аналитический обзор «**О формировании стандартов регулирования генеративного ИИ в Китае**» (далее – «Обзор») подготовлен специалистами АНО «Центр глобальной ИТ-кооперации».

Информация, приведенная в Обзоре, подпадает под действие законодательства об авторских правах Российской Федерации. Исключительные права на Обзор принадлежат АНО «Центр глобальной ИТ-кооперации» (далее – «Правообладатель»).

Обзор может использоваться в целях ознакомления. Допускается размещение активных ссылок на Обзор в других информационных источниках без непосредственного копирования его содержания. При любом использовании Обзора активная ссылка на источник обязательна.

Частичное или полное воспроизведение и распространение, а также любое коммерческое использование Обзора запрещено без письменного разрешения правообладателя, а также без ссылки на авторов Обзора.

Приступая к ознакомлению с Обзором, вы подтверждаете свое согласие с изложенными ниже условиями:

- Правообладатель не принимает на себя обязательств или ответственности за использование информации, содержащейся в Обзоре.
- Обзор носит исключительно информационный характер и составлен на основе публичных (открытых) источников, признанных надежными, однако правообладатель не несет ответственности за точность приведенных данных.
- Выводы, представленные в Обзоре, носят исключительно информационный характер и основаны на информации, полученной из открытых источников, указанных в соответствующем разделе Обзора.
- Обзор не является юридическим заключением по вопросам, рассмотренным в нем. Правообладатель не несет ответственности за решения, принятые на основании представленных в Обзоре данных.
- Обзор включает в себя ссылки на сторонние веб-сайты, находящиеся вне контроля правообладателя. Правообладатель не несет ответственности за содержание этих ссылок; такая ответственность во всех случаях возлагается на соответствующего провайдера, либо оператора этих сторонних веб-сайтов. Правообладатель не несет ответственности за доступ к этим веб-сайтам и их содержанию.

О ФОРМИРОВАНИИ СТАНДАРТОВ РЕГУЛИРОВАНИЯ ГЕНЕРАТИВНОГО ИИ В КИТАЕ

Оглавление

ВВЕДЕНИЕ	6
I. ЭТАПЫ ФОРМИРОВАНИЯ КИТАЙСКОЙ МОДЕЛИ РЕГУЛИРОВАНИЯ ИИ ..	6
II. ОСНОВНЫЕ ИНСТРУМЕНТЫ РЕГУЛИРОВАНИЯ	11
2.1 Правила управления сервисами (2019 г.)	12
2.2 Меры в отношении рекомендательных алгоритмов (2021г.).....	13
2.3 Положение о глубоком синтезе (2022 г.)	14
2.4 Временные меры по управлению генеративным ИИ (2023 г.).....	15
2.5 Меры по маркировке ИИ-контента (2025 г.) и система NET ID	17
2.6 Система верификации пользователей Net ID.....	18
2.7 Поддержка технических стандартов и рекомендаций	19
2.7.1 Стандарт по идентификация синтетического контента	20
2.7.2 Требования по безопасности сервисов (2024 г.)	20
III. ПРАВОПРИМЕНИТЕЛЬНЫЕ ПРАКТИКИ	21
3.1 Общая структура органов регулирования ИИ в КНР.....	21
3.2 Актуализация мер по регулированию дипфейков со стороны государства.....	22
3.3 Некоторые кейсы государственного регулирования дипфейк-технологий в КНР ..	24
3.3.1 Общенациональная кампания по борьбе с немаркированным и вводящим в заблуждение контентом с использованием ИИ.....	24
3.3.2 Кампания NRTA по борьбе с культурным вандализмом	25
3.3.3 Административное задержание за дезинформацию о дорожно-транспортном коллапса в Шанхае	25
3.3.4 Противоправное использование дипфейков для финансовых преступлений..	26
3.3.5 «Дело Тодда»: судебный процесс о замене лица иностранным ИИ	26
3.4 Меры саморегулирования со стороны крупных компаний	27
IV ОСНОВНЫЕ ВЫВОДЫ	29
БИБЛИОГРАФИЯ	34

ВВЕДЕНИЕ

В условиях, когда темпы развития искусственного интеллекта опережают законотворческие процессы, Китайская Народная Республика становится уникальной нормативной лабораторией мирового масштаба. Страна разработала один из наиболее комплексных и структурированных регуляторных режимов в сфере ИИ, охватывающий ключевые и наиболее чувствительные области применения технологий. Пекин не только тестирует, но и активно внедряет правовые акты, регулирующие дипфейки, генеративные модели и рекомендательные алгоритмы.

В основе китайского подхода лежат принципы прозрачности, подотчетности и защиты прав пользователей. Особое внимание уделяется биометрической идентификации: использование распознавания лиц в системах наблюдения и безопасности жестко регламентировано. Кроме того, Китай ввел строгие требования к маркировке синтетического контента, включая обязательное внедрение водяных знаков и метаданных. Это обеспечивает сквозную прослеживаемость происхождения цифрового контента и устанавливает контроль еще на этапе его генерации.

Это означает не только необходимость работы китайского бизнеса в жестких нормативных рамках, но и понимание того, что китайская модель может стать ориентиром для других юрисдикций. Страна стремится занять позицию мирового лидера в сфере ИИ, сочетая технологический прогресс с защитой социального порядка и национальной безопасности.

I. ЭТАПЫ ФОРМИРОВАНИЯ КИТАЙСКОЙ МОДЕЛИ РЕГУЛИРОВАНИЯ ИИ

Ключевая особенность подхода Китая — это поэтапное внедрение норм, которое прошло три стадии эволюции:¹

1. **Стратегическое планирование и отраслевая саморегуляция (2017–2020).** На этом этапе власти предоставили отрасли свободу для ускоренного развития инноваций, закладывая основы будущего регулирования.
2. **Введение добровольных стандартов (2020–2022).** По мере выявления потенциальных рисков начался переход к более жесткому контролю. Этот этап стал подготовительным перед введением обязательных требований.
3. **Прямой нормативный надзор (с 2022 года по настоящее время).** Заключительная фаза, связанная с амбициозной целью Китая достичь глобального лидерства в индустрии ИИ к 2030 году. Сегодня регуляторика

¹ <https://data-privacy-office.com/regulation-of-artificial-intelligence-in-china/>

направлена на создание среды, где инновации и контроль существуют в симбиозе, дополняя друг друга.

Китай не существует в вакууме, страна тщательно анализирует международный переговорный процесс в сфере ИИ и международный опыт, адаптируя лучшие практики ЕС и США под свои национальные задачи. Это позволяет внедрять не только технологические, но и регуляторные инновации, усиливая долгосрочную стратегию развития.

В глобальном масштабе подход КНР отличается приоритетом государственного надзора. Для сравнения²:

- **ЕС** требует маркировки синтетического контента, но предусматривает исключения.
- **США** делают ставку на добровольное использование водяных знаков.
- **Великобритания** рассматривает законопроект, обязывающий предупреждать пользователей о взаимодействии с ИИ.

Несмотря на то, что ЕС был первопроходцем, системный подход Китая выглядит сегодня более строгим. Оба региона преследуют общую цель — сохранение общественного доверия к технологиям. Однако Китай идет дальше, внедряя обязательную и технически отслеживаемую маркировку, что делает его систему уникальной на фоне западных аналогов, сталкивающихся, например, с ограничениями Первой поправки в США.³

Таким образом, китайская модель регулирования ИИ представляет собой симбиоз инновационной политики и жесткого надзора, направленный на укрепление международного влияния страны и защиту национальных интересов.

Определение «Глубокий синтез»

В Китае «технологии глубокого синтеза» (*deep synthesis*, данный термин используется далее в Обзоре) определяются⁴ (источник - см. также п. 2.3) как «технологии, использующие алгоритмы генеративного секвенирования, такие как глубокое обучение и виртуальная реальность, для создания текста, изображений, аудио, видео, виртуальных сцен или другой информации» (перевод с китайского на английский может допускать некоторые лексические несоответствия).

² <https://www.ddg.fr/actualite/transparency-of-ai-generated-content-china-goes-further-than-europe>

³ <https://eurasia.today/actual/opyt-kitaya-v-regulirovanii-iskusstvennogo-intellekta/>

⁴ Положение Китая о глубоком синтезе в информационных услугах на основе Интернета, статья 23 (Положения о глубоком синтезе), <https://perma.cc/MV6Z-5BGB>, перевод с английского

К таким технологиям относятся, помимо прочего, технологии для генерации или редактирования различного контента (массивов данных):

- (1) Текстовое содержимое: например, генерация текста, преобразование стиля текста и генерация вопросов и ответов.
- (2) Речевое содержание: например, преобразование текста в речь, преобразование голоса и редактирование атрибутов голоса.
- (3) Неречевой контент: например, создание музыки и редактирование фонового звука.
- (4) Биометрические признаки в изображениях или видеоконтенте: например, генерация лица, замена лица, редактирование личных атрибутов, манипулирование лицом и манипулирование жестами.
- (5) Небиометрические признаки в изображениях или видеоконтенте: такие как генерация изображений, улучшение изображений и восстановление изображений.
- (6) Цифровые персонажи или виртуальные сцены: например, 3D-реконструкция и цифровое моделирование.

Таким образом в китайском подходе намеренно используется термин "глубокий синтез", как более широкое и технически нейтральное понятие, которое охватывает любые результаты работы генеративных алгоритмов, включая полезные и творческие – то есть написание текстов, создание музыки, оказание помощи в программировании. Это обеспечивает регулирование этих процессов, основанных на технологии ИИ в едином правовом поле.

«Сгенерированный и синтезированный с использованием ИИ контент» в соответствии с принятыми в 2025 году Мерами по маркировке контента, сгенерированного и синтезированного с использованием ИИ (*Measures for Labeling of AI-Generated Synthetic Content*)⁵ служит общим термином для всей информации, созданной или измененной с помощью этих технологий (см. далее п. 2.5).

Понятие «дипфейк» в КНР не является строго определенным юридическим термином, а скорее описывает вредоносное приложение или вводящий в заблуждение выходной продукт на основе глубокого синтеза.

Ниже приведена краткая панорама значимых шагов Китая по формированию нормативно-правовых инструментов в области ИИ.

Страна последовательно выстраивает одну из самых структурированных и амбициозных систем регулирования искусственного интеллекта в мире. Этот процесс, начавшийся с

⁵ <https://www.chinalawtranslate.com/en/ai-labeling/>

формулирования этических норм, к 2025–2026 годам привел к созданию комплексной правовой базы, охватывающей как национальные интересы, так и международное сотрудничество.

Формирование этического фундамента, 2018–2019 гг.

Отправной точкой нормативной деятельности стала разработка этических ориентиров для сферы ИИ. В 2018 году Правительство КНР делегировало Китайской ассоциации искусственного интеллекта (Chinese Association for Artificial Intelligence - CAAI) задачу по созданию свода профессиональных норм. Результатом этой работы стала публикация в 2019 году **«Пекинских принципов искусственного интеллекта»**. Документ заложил мировоззренческую базу для дальнейшего законотворчества, провозгласив ключевые ценности: защиту приватности, уважение человеческого достоинства, обеспечение безопасности систем ИИ, открытость к инновациям и приверженность международному сотрудничеству в сочетании с долгосрочным стратегическим планированием.⁶

Первый комплексный Закон об ИИ (2024 - 2025 г.г.)

Ключевым этапом институционализации отрасли стало принятие **«Закона об искусственном интеллекте»** в 2024 году. Документ, вступивший в законную силу 1 июля 2025 года, представляет собой первый в истории Китая всеобъемлющий нормативный акт, систематизирующий разрозненные ранее инициативы. Его главные новации включают три фундаментальных блока:⁷

1. Градация рисков.

Все ИИ-приложения классифицируются по четырем уровням опасности: минимальный, ограниченный, высокий и неприемлемый. К категории высокого риска отнесены системы, задействованные в критической инфраструктуре, правоохранительной деятельности, судопроизводстве, а также технологии для сканирования эмоций в реальном времени. Для таких решений введены обязательные процедуры: независимый аудит, стресс-тестирование и государственная сертификация.

2. Принцип алгоритмического суверенитета.

Закон вводит требование локализации алгоритмов для стратегических отраслей (финансовые технологии, логистика, здравоохранение). Компании, обрабатывающие данные китайских граждан в этих сферах, обязаны применять

⁶ <https://data-privacy-office.com/regulation-of-artificial-intelligence-in-china/>

⁷ <https://hbh.ru/biznes/tehnologii-i-innovatsii/iskusstvennyy-intellekt/2025/09/29/10288/regulirovanie-iskusstvennogo-intellekta-v-kitae>

алгоритмы, разработанные и зарегистрированные на территории КНР. Данная мера стала мощным катализатором для роста национальных стартапов и развития фундаментальных исследований в области ИИ.

3. Прозрачная цепочка ответственности.

Впервые законодательно закреплена сквозная ответственность всех участников жизненного цикла ИИ-продукта: от сборщика данных и разработчика модели до системного интегратора и конечного оператора. Это устраняет правовые коллизии и стимулирует бизнес к созданию более объяснимых и контролируемых алгоритмов.

Международная экспансия и отраслевая интеграция (2025 г.)

Летом 2025 года Китай вышел на международную арену с собственной нормативной повесткой. 26 июля 2025 года на Всемирной конференции по искусственному интеллекту Министерство иностранных дел КНР представило **«Глобальный план действий по управлению ИИ»** (*Global AI Governance Action Plan*). Документ, состоящий из 13 пунктов, предлагает мировому сообществу основу для сотрудничества в области безопасности ИИ, развития инфраструктуры и унификации стандартов данных. Основная цель инициативы — «полное раскрытие потенциала ИИ при гарантиях его безопасности, надежности, управляемости и справедливости». В плане подчеркивается необходимость глобальной солидарности перед лицом как беспрецедентных возможностей, так и новых вызовов эпохи искусственного интеллекта.⁸

Параллельно с внешнеполитическими инициативами внутри страны было опубликовано Руководство по реализации **программы «AI Plus»**. Этот документ нацелен на ускорение глубинной интеграции искусственного интеллекта во все сферы экономики и общественной жизни для формирования так называемых «новых качественных производительных сил».⁹

Усиление кибербезопасности и борьба с deepfakes (2026 г.)

С 1 января 2026 года вступили в силу масштабные **поправки к Закону о кибербезопасности** (*Cybersecurity Law, CSL*), которые кодифицируют правила работы с генеративным ИИ и технологиями глубокого синтеза (*deep synthesis*). Ключевым

⁸ <https://ppc.land/china-unveils-global-ai-governance-action-plan-framework/>

⁹ <https://russian.shanghai.gov.cn/ru-PolicyInsights/20250908/b5eae96c1e6d45dfbe86ff52f784e164.html>

нововведением стала отдельная **статья 20**, реализующая двухвекторный подход к регулированию¹⁰:

- **Вектор развития:** государство берет на себя обязательства по поддержке фундаментальных исследований, разработке алгоритмов и созданию инфраструктуры (вычислительные мощности и ресурсы обучающих данных).

- **Вектор безопасности:** одновременно формализуются этические нормы, вводится усиленный мониторинг и оценка рисков. Закон также поощряет использование самих технологий ИИ для повышения уровня кибербезопасности («борьба с ИИ при помощи ИИ»).

Поправки прямо нацелены на противодействие дезинформации и мошенничеству с использованием дипфейков. Регуляторы наделены полномочиями для оперативного реагирования на нарушения, а провайдеры сервисов несут прямую ответственность за распространение нелегального контента¹¹, что может повлечь за собой гражданско-правовые, административные или уголовные санкции.¹²

Таким образом, пройдя путь от общих этических деклараций до жестких законодательных норм и международных инициатив, Китай к 2026 году сформировал целостную экосистему регулирования ИИ, основанную на балансе технологического суверенитета, инновационного развития и национальной безопасности.

II. ОСНОВНЫЕ ИНСТРУМЕНТЫ РЕГУЛИРОВАНИЯ

Китайская система регулирования искусственного интеллекта строится по модульному принципу: для каждой технологической сферы. Для генеративных моделей, дипфейков и рекомендательных сервисов разработаны отдельные нормативные акты. При этом все они базируются на единых принципах прозрачности, подотчетности и защиты прав пользователей, а также опираются на фундаментальные законы страны:

- Закон о кибербезопасности;
- Закон о безопасности данных;

¹⁰ "China's 2025 Cybersecurity Law amendments: Enhanced penalties, expanded extraterritorial application, and AI governance," Linklaters Tech Insights, November 3, 2025, <https://techinsights.linklaters.com/post/102lrz5/chinas-2025-cybersecurity-law-amendments-enhanced-penalties-expanded-extraterr>

¹¹ "China's 2025 Cybersecurity Law amendments," Linklaters.

¹² Zhang Xu, "China enforces AI labeling rules as deepfakes proliferate," Interface News, September 5, 2025, <https://www.163.com/dy/article/K8NK80GC0534A4SC.html>.

- Закон о защите персональной информации и профильные административные регламенты в сфере интернет-услуг.¹³

Для компаний, ведущих деятельность в области ИИ в Китае, ключевое значение имеют несколько специализированных инструментов, формирующих архитектуру *compliance* (соответствия требованиям).

2.1 Правила управления сервисами (2019 г.)

Нормативная база Китая в сфере глубокого синтеза прошла путь от общих запретов до детализированного регулирования деятельности провайдеров.

Правила управления онлайн-аудио- и видеoinформационными сервисами (*Regulations on Administration of Online Audio and Video Information Services 2020*), принятые в 2019 году и вступившие в силу 1 января 2020 года, ввели универсальный запрет на применение технологий компьютерной графики, аудио- и видеомонтажа для производства и распространения недостоверной информации.

В этом документе регуляторы продемонстрировали понимание специфических рисков, связанных с развивающимися технологиями. Правила 2019 года стали первым нормативным актом в Китае, связанным с проблемой глубокого синтеза. Они установили ключевые требования, которые были развиты в последующих актах.

Развитие технологий требовало более тонкой настройки законодательства. Новый блок нормативных актов сместил фокус с конечного продукта (в том числе фейковых новостей) непосредственно на самих создателей технологий — поставщиков услуг глубокого синтеза. Современные требования концентрируются вокруг трех ключевых аспектов:

- управление данными;
- обеспечение кибербезопасности;
- обязательная верификация пользователей.

Кроме того, вводится обязанность маркировать синтетический контент, предупреждая аудиторию об его искусственном происхождении.

Такой подход преследует стратегическую цель: создать условия для устойчивого развития индустрии при одновременном снижении системных рисков. Речь идет о платформах, которые используют технологии глубокого обучения или виртуальной реальности для модификации любых типов онлайн-материалов.

¹³ <https://hbh.ru/biznes/tehnologii-i-innovatsii/iskusstvennyy-intellekt/2025/09/29/10288/regulirovanie-iskusstvennogo-intellekta-v-kitae/>

При этом сфера действия наложенных ограничений не исчерпывается дипфейками. Китайское регулирование распространяется на значительно более широкий спектр явлений: автоматически сгенерированные тексты, отредактированные с помощью ИИ изображения и даже синтезированные виртуальные ландшафты. Такой всеобъемлющий подход демонстрирует, что власти страны оценивают технологическое развитие не только с точки зрения локальных рисков (например, мошенничества), но и через призму влияния новых технологий на стабильность общественной системы в целом. Контроль над инструментами синтеза контента рассматривается как один из ключевых элементов поддержания информационной безопасности и социальной гармонии.

2.2 Меры в отношении рекомендательных алгоритмов (2021г.)

В Китае 4 января 2022 г. вступил в силу важный нормативный акт, определяющий правила работы рекомендательных сервисов, — **Положения по управлению алгоритмическими рекомендациями в информационных службах Интернета**¹⁴ (*China Provisions on the Management of Algorithmic Recommendations in Internet Information Services*), принятый в 2021 году. Документ регулирует деятельность платформ, которые используют алгоритмы для продвижения контента, формирования пользовательских лент или выдачи персонализированных рекомендаций.¹⁵

Главная задача Положений — предотвращение злоупотреблений рыночной властью со стороны цифровых платформ, работающих на базе искусственного интеллекта. Документ вводит ряд существенных ограничений:

1. **Антимонопольная защита.** Регламент прямо запрещает использование алгоритмов для осуществления монополистических действий или участия в схемах недобросовестной конкуренции. Это направлено на обеспечение равных условий для всех игроков рынка.

2. **Социальная защита уязвимых групп.** Особое внимание уделяется безопасности пожилых пользователей. Платформы обязаны проявлять повышенную осторожность при взаимодействии с этой аудиторией, в том числе для предотвращения мошеннических схем, которые могут эксплуатировать алгоритмические системы.

¹⁴ <https://www.chinajusticeobserver.com/law/x/regulations-on-the-administration-of-algorithm-recommendation-of-internet-information-services-20220104>

¹⁵ https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

3. **Информационная безопасность.** Положения запрещают использование алгоритмов для генерации и распространения недостоверной информации (фейковых новостей).

4. **Недопустимость дискриминации.** Под запрет попадает применение дискриминационных или предвзятых тегов в пользовательских профилях, которые могут влиять на работу рекомендательных алгоритмов.

Таким образом, китайский подход к регулированию алгоритмических рекомендаций демонстрирует стремление властей контролировать не только экономические последствия работы ИИ (монополизация), но и социальные эффекты, включая защиту прав потребителей и информационную безопасность.

2.3 Положение о глубоком синтезе (2022 г.)

В ноябре 2022 года китайские регулирующие органы представили важный нормативный акт в сфере искусственного интеллекта — **Положения об администрировании интернет-информационных сервисов, использующих технологии глубокого синтеза**^{16, 17} (*Provisions on the Administration of Deep Synthesis of Internet-based Information Service 2022*, далее - *Положения о глубоком синтезе*). Документ был опубликован 25 ноября 2022 года и вступил в законную силу 10 января 2023 года.

Положения состоят из 25 статей и регулирует применение технологий глубокого синтеза (*deep synthesis*) при оказании интернет-услуг на территории КНР. Под действие документа подпадают сервисы, генерирующие или модифицирующие изображения, видео, аудиоматериалы и тексты с использованием алгоритмов ИИ.¹⁸

Нормативный акт устанавливает многоуровневую систему контроля, включающую следующие обязательные элементы:

1. **Идентификация синтетического контента.** Все материалы, созданные с помощью ИИ, подлежат обязательной маркировке, указывающей на их искусственное происхождение. Публикация немаркированного синтетического контента запрещена.

2. **Регистрация алгоритмов.** Провайдеры услуг глубокого синтеза обязаны депонировать свои алгоритмы в уполномоченных органах.

¹⁶ <https://www.chinajusticeobserver.com/law/x/provisions-on-the-administration-of-deep-synthesis-of-internet-based-information-service-20221125>

¹⁷ https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm

¹⁸ <https://www.chinajusticeobserver.com/a/chinese-government-to-regulate-deepfake-technology>

3. **Верификация пользователей.** Для доступа к сервисам глубокого синтеза введено требование обязательной аутентификации пользователей на основе реальных идентификационных данных.

Положение вводит исчерпывающий перечень запрещенной деятельности:

- Запрет на использование технологий глубокого синтеза для создания, копирования или распространения информации, противоречащей законодательству КНР.
- Недопустимость применения сервисов в целях, наносящих ущерб национальной безопасности, государственному имиджу, общественным интересам, экономическому и социальному порядку, а также законным правам третьих лиц.
- Специальный запрет на генерацию и распространение ложной новостной информации с использованием технологий глубокого синтеза.

Обязанности платформ по борьбе с дезинформацией

На поставщиков услуг возлагается активная роль в противодействии фейкам. Положение обязывает провайдеров создавать и поддерживать механизмы опровержения слухов. В случае обнаружения фактов использования их сервисов для распространения недостоверной информации компании обязаны незамедлительно принимать меры по опровержению, фиксировать соответствующие данные и уведомлять регулирующие органы.

Особый контроль над биометрическими данными

Отдельное регулирование введено в отношении инструментов, работающих с биометрической информацией. Если провайдеры услуг глубокого синтеза или их технологические партнеры предоставляют средства для генерации или редактирования изображений лиц и голосов, они обязаны проходить процедуру оценки безопасности. Это требование направлено на предотвращение злоупотреблений в сфере дипфейков и защиты персональных биометрических данных граждан.

2.4 Временные меры по управлению генеративным ИИ (2023 г.)

В Китае 15 августа 2023 г. вступил в силу основополагающий нормативный акт, определяющий правила работы с генеративным ИИ, — **Временные меры по**

управлению сервисами генеративного искусственного интеллекта ^{19, 20} (*Interim Measures for the Administration of Artificial Intelligence Generated Content*, далее - *Меры по генеративному ИИ 2023*). Документ устанавливает комплексные обязательства для поставщиков соответствующих услуг и, в определенной степени, для их пользователей, формируя базовые требования в сферах безопасности, контент-политики и управления сервисами.

Действие документа распространяется на сервисы, способные автономно создавать контент, неотличимый от созданного человеком: тексты, изображения, аудио- и видеоматериалы. Документ развивает и конкретизирует нормы, ранее закрепленные в Положении о глубоком синтезе 2022 года, адаптируя их под специфику генеративных моделей.

Ключевые новеллы регулирования²¹:

1. Ответственность провайдера.

Меры вводят принцип прямой ответственности поставщика за контент, генерируемый его сервисами. Это правило распространяется в том числе на случаи предоставления доступа к моделям через программные интерфейсы (API). Таким образом, провайдер юридически приравнивается к производителю контента.²²

2. Требования к обучающим данным.

Установлены строгие критерии к источникам данных для предварительного обучения и дообучения (оптимизации) моделей. Провайдеры обязаны обеспечивать легальность происхождения данных, что подразумевает соблюдение законодательства об интеллектуальной собственности и защите персональной информации.²³

3. Запрет на дискриминацию.

При разработке алгоритмов, подборе обучающих выборок и оптимизации моделей необходимо принимать меры для предотвращения дискриминации. Под

¹⁹ https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

²⁰ Cyberspace Administration of China et al., "Interim Measures for the Management of Generative Artificial Intelligence Services," translated by China Law Translate, July 13, 2023, accessed February 18, 2026, <https://www.chinalawtranslate.com/en/generative-ai-interim/>. Original Chinese version: 国家互联网信息办公室等, "生成式人工智能服务管理暂行办法," 中华人民共和国中央人民政府, July 10, 2023, accessed February 18, 2026, https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm

²¹ "Key Points of the Interim Measures for the Administration of Artificial Intelligence Generated Content," JunHe, July 18, 2023, <https://junhe.com/legal-updates/2219?locale=en>.

²² «Меры по генеративному ИИ», ст. 9.

²³ Там же, ст. 7.

защиту попадают признаки расы, национальности, вероисповедания, пола, возраста, профессиональной принадлежности и состояния здоровья.²⁴

4. Гарантии прав пользователей.

На провайдеров возлагается обязанность по защите пользовательских данных, включая вводимую информацию и историю взаимодействия с сервисом. Запрещается проводить профилирование пользователей на основе этих данных без дополнительных оснований. Кроме того, провайдеры обязаны обеспечивать стабильное, безопасное и бесперебойное предоставление услуг.²⁵

Таким образом, Временные меры 2023 года формируют целостную систему регулирования, в которой технологическое развитие генеративного ИИ сочетается с жесткими требованиями к легальности данных, недискриминационности алгоритмов и защите прав конечных потребителей.

2.5 Меры по маркировке ИИ-контента (2025 г.) и система NET ID

Китай стал первым государством в мире, внедрившим обязательные и технически проработанные требования к маркировке контента, созданного или модифицированного с помощью искусственного интеллекта.²⁶ Основные цели этого регулирования — противодействие дезинформации (в рамках кампании «Цинлан» 2025 года было удалено 960 тыс. единиц нелегального ИИ-контента), защита прав граждан и формирование условий для ответственного внедрения технологий.²⁷

14 марта 2025 года четыре ведущих регулятора КНР — Управление по киберпространству Китая (САС), Министерство промышленности и информатизации (МИИТ), Министерство общественной безопасности (МПС) и Государственное управление радио и телевидения (НРТА) — совместно опубликовали **Меры по идентификации (маркировке) контента, созданного искусственным интеллектом, и синтетического контента** (*Measures for the Identification of Artificial Intelligence-generated Synthetic Content, далее – Меры по маркировке*).²⁸ Документ был подписан 7 марта и вступил в законную силу 1 сентября 2025 года.²⁹

²⁴ Там же, ст. 4.

²⁵ Там же, ст. 11, 13.

²⁶ "China implements mandatory AI content labeling," PPC Land.

²⁷ "China's new rule," GeoPolitechs; о количестве удаленного контента см. статью в блоге PPC Land.

²⁸ «Circular on Issuing the "Measures for Labeling Artificial Intelligence-Generated Contents"» (Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and National Radio and Television Administration, Notice No. 2025-2, March 7, 2025), цит. по "China implements mandatory AI content labeling standards effective September," PPC Land, September 2, 2025, <https://ppc.land/china-implements-mandatory-ai-content-labeling-standards-effective-september/>.

²⁹ Там же; "China's new rule requiring tech companies to label AI-generated content," GeoPolitechs, March 15, 2025, <https://www.geopolitechs.org/p/chinas-new-rule-requiring-tech-companies>.

Действие Мер по маркировке распространяется на три категории участников:

- поставщики сервисов генеративного ИИ;
- платформы-распространители (включая магазины приложений);
- конечные пользователи.

Поставщики должны раскрывать методы идентификации в пользовательских соглашениях.³⁰ Пользователям, в свою очередь, запрещено удалять, подделывать или скрывать маркеры, а также предоставлять инструменты для совершения таких действий.³¹ Важной особенностью является экстерриториальный принцип: иностранные компании, предоставляющие услуги на рынке КНР, обязаны соблюдать установленные требования независимо от места регистрации головного офиса.³²

Разбирая, например, требования к аудиоконтенту, можно отметить, что все аудиоматериалы, созданные с помощью ИИ, должны быть четко различимы (идентифицированы) с помощью как явной, так и скрытой маркировки.

Для явной маркировки аудио требуется, чтобы голосовые метки или метки звукового ритма добавлялись в начале, в конце или в соответствующих позициях аудиофайла.

Для скрытой маркировки поставщики услуг должны вставлять маркеры метаданных непосредственно в заголовки файлов, которые содержат техническую информацию (данные о производителе контента, коде поставщика услуг, идентификационные номера контента и т.п.).

В августе 2025 года Национальный технический комитет TC260 выпустил специальные технические рекомендации³³, в которых подробно описываются методы внедрения различных аудиоформатов, включая WAV, MP3, OGG (*Vorbis* и *Opus*), FLAC и M4A, устанавливающие стандартизированные подходы к внедрению и извлечению метаданных.

2.6 Система верификации пользователей Net ID

Параллельно с развитием маркировки контента в Китае совершенствуется система идентификации пользователей. Хотя законодательство о «реальном имени» действует с 2017 года, в июле 2025 года была запущена централизованная государственная система «Сетевой идентификатор» (Net ID / Cyberspace ID), регулируемая **Мерами по**

³⁰ Там же.

³¹ Там же; "China's new rule," GeoPolitech.

³² "China implements mandatory AI content labeling," PPC Land.

³³ China: TC260 adopted Guidelines on Identification Methods for AI-Generated Synthetic Audio Content <https://digitalpolicyalert.org/event/33154-tc260-adopted-guidelines-on-identification-methods-for-ai-generated-synthetic-audio-content>

администрированию публичных сервисов для сетевой аутентификации личности (*Measures for the Administration of Public Services for Network Identity Authentication*).³⁴

Применение Net ID является правом, а не обязанностью граждан. Платформы обязаны предоставлять альтернативные способы верификации³⁵ (например, по номеру телефона).

Система генерирует для пользователя зашифрованный токен, связанный с его удостоверением личности. При регистрации платформа получает только подтверждение факта верификации, не имея доступа к оригинальным паспортным данным. Платформам запрещено требовать дополнительную информацию при авторизации через Net ID.³⁶

Требование к платформам интегрироваться с системами верификации пользователей (для привязки контента к создателю) было установлено еще **Положением о глубоком синтезе 2022 года** и **Временными мерами по управлению генеративным ИИ 2023 года**.

При этом нормы об обязательной биометрической верификации (например, распознавании лица) перед публикацией дипфейк-контента в данных документах отсутствуют. Этот вопрос регулируется общими требованиями к идентификации и отдельными актами, такими как **Меры по обеспечению безопасности применения технологии распознавания лиц** (вступили в силу 1 июня 2025 г.), которые предписывают не использовать биометрию как единственный метод там, где возможны альтернативы.³⁷

Меры по маркировке 2025 года работают в единой связке с другими ключевыми нормативными актами: Положениями о глубоком синтезе 2022; Положениями о рекомендательных алгоритмах 2021. В совокупности эти инструменты формируют целостную систему, направленную на минимизацию этических и социальных рисков, связанных с созданием, модификацией и распространением контента на основе технологий искусственного интеллекта.

2.7 Поддержка технических стандартов и рекомендаций

Помимо рамочных законов, Китай активно развивает систему узкоспециализированных технических регламентов. Эти нормативы задают конкретные параметры для разработчиков и операторов ИИ-систем и служат основным инструментом для

³⁴ О запуске Net ID в июле 2025 г. см. PPC Land; нормативная база — Государственный совет КНР, «Положение о государственной службе сетевой аутентификации личности», 2025,

http://big5.www.gov.cn/gate/big5/www.gov.cn/govweb/gongbao/2025/issue_12166/202507/content_7032498.html.

³⁵ Там же, ст. 4, 6; Coco Feng, "China Rolls Out 'Voluntary' Cyber ID System amid Concerns over Privacy, Censorship," South China Morning Post, July 15, 2025, <https://www.scmp.com/tech/tech-trends/article/3318302/china-rolls-out-voluntary-cyber-id-system-amid-concerns-over-privacy-censorship>.

³⁶ Там же, ст. 8.

³⁷ САС и MPS, «Меры по обеспечению безопасности применения технологии распознавания лиц», 2025, ст. 3, https://www.lexiscn.com/latest_message.php?id=481510.

регуляторов и участников рынка при проведении экспертиз и оценке соответствия продукции.

2.7.1 Стандарт по идентификация синтетического контента

Одновременно с Мерами по маркировке ИИ-контента (2025 г.) Государственное управление по регулированию рынка и Комитет по стандартизации КНР утвердили обязательный национальный стандарт **GB 45438-2025 Методы идентификации синтетического контента, созданного искусственным интеллектом, в технологиях кибербезопасности**, который устанавливает технические параметры реализации маркировки.

Данный стандарт носит обязательный характер и устанавливает унифицированные технические требования к маркировке материалов, сгенерированных нейросетями. Документ детализирует способы нанесения маркировки для различных типов данных (текст, изображение, видео, аудио), обеспечивая тем самым практическую реализацию законодательных норм о прослеживаемости контента.

Руководство Третьего научно-исследовательского института Министерства общественной безопасности КНР пояснило, что требование маркировки синтетического контента сегодня становится общепринятой международной практикой, поэтому при разработке GB 45438-2025 китайские специалисты учитывали глобальные тенденции, что позволило гармонизировать национальный подход с аналогичными нормами, действующими в Евросоюзе, США и других странах.³⁸

2.7.2 Требования по безопасности сервисов (2024 г.)

В развитие Временных мер по управлению сервисами генеративного ИИ (2025 г.) Национальный технический комитет по стандартизации кибербезопасности КНР представил дополнительный нормативно-технический документ — **Основные требования к безопасности для сервисов генеративного искусственного интеллекта 2024**³⁹ (*Basic Security Requirements for Generative Artificial Intelligence Service*, далее – *Требования к безопасности сервисов*). Стандарт вступил в силу 1 ноября 2025 г., он устанавливает требования к данным для обучения ИИ, а также к безопасности моделей и контента, содержит положения по обеспечению легитимности данных, фильтрации незаконного контента и предотвращению использования вредоносного контента в обучающих датасетах.

³⁸ "New Regulation on AI-generated Content," Science and Technology Daily, March 22, 2025, https://digitalpaper.stdaily.com/http_www.kjrb.com/ywtk/html/2025-03/22/content_586308.htm.

³⁹ <https://digitalpolicyalert.org/change/8857>

В отличие от рамочных Временных мер, данный стандарт устанавливает технические параметры и требования, которым должны следовать разработчики и операторы моделей при развертывании своих решений.

III. ПРАВОПРИМЕНИТЕЛЬНЫЕ ПРАКТИКИ

3.1 Общая структура органов регулирования ИИ в КНР

За регулирование информационного поля и обеспечение соответствия национальному законодательству отвечает Администрация киберпространства Китая (САС).⁴⁰ Эта организация, также известная как Исполнительный орган Центральной комиссии по делам киберпространства Коммунистической партии Китая, подчиняется непосредственно Центральной комиссии, которая, в свою очередь, подотчетна ЦК КПК. САС является ключевым акционером и фактическим владельцем ведущих китайских технологических компаний, включая ByteDance (владелец TikTok, Xigua, Toutiao, BaBe, Helo), SenseTime (разработчик систем распознавания лиц на базе ИИ), Kuaishou (крупный разработчик мобильных приложений) и Weibo Corporation. Совокупно эти компании и их цифровые платформы формируют значительную часть китайского интернет-пространства под общим контролем САС.

В структуру САС входят такие подразделения, как Центр управления чрезвычайными ситуациями в области безопасности Интернета, Центр обслуживания и Центр сообщений о незаконной и вредной информации. Регулятор выполняет функции цензора, издавая директивы для всех средств массовой информации в стране. Его компетенция распространяется на регулирование в отношении имен пользователей, проверку пригодности онлайн-контента, установление правил использования VPN и мониторинг публикаций на интернет-ресурсах.

В соответствии с законом «О кибербезопасности», САС во взаимодействии с другими государственными службами формирует перечень «базового сетевого оборудования» и «особых продуктов кибербезопасности», подлежащих обязательному лицензированию. Кроме того, САС анализирует государственные закупки сетевых продуктов и сервисов с позиции обеспечения государственной безопасности. Информация, которую китайские компании хранят за пределами страны, также требует получения разрешения от Администрации киберпространства.

Наряду с САС, в своих соответствующих областях полномочия по надзору за дипфейк-технологиями осуществляют отраслевые управления, такие как Национальное

⁴⁰ 中央网络安全和信息化委员会办公室, URL: <https://www.cac.gov.cn/> (дата обращения: 12.02.2026).

управление радио и телевидения⁴¹ (в области вещания и культуры) и Государственное управление по регулированию рынка⁴² (в сфере финансовой безопасности). При этом сами онлайн-платформы также принимают активное участие в регулировании генеративного ИИ, усиливая процессы проверки контента, удаляя материалы, не соответствующие требованиям, и наказывая аккаунты-нарушители.

3.2 Актуализация мер по регулированию дипфейков со стороны государства

С 2020 года злонамеренное использование дипфейк-технологий становится всё более распространённым явлением, в т.ч. и в цифровом пространстве Китая. Согласно данным отчета о безопасности искусственного интеллекта за 2024 год, представленного компанией Qianxin, в 2023 году зафиксирован колоссальный рост мошеннических операций, связанных с применением дипфейк-технологий (увеличение почти в 30 раз⁴³). Эта динамика во многом предопределила сдвиг в подходе Китая к регулированию дипфейков в период 2024-2026 гг. - от формулирования основных принципов к их широкомасштабному и систематическому применению.

В июне 2024 года Управление интернет-безопасности при Министерстве общественной безопасности Китая обнародовало несколько распространенных сценариев применения дипфейк-технологий. В одном из приведенных примеров фигурирует злоумышленник, который с помощью программы на базе искусственного интеллекта осуществил «автоматическую генерацию компрометирующих изображений на основе фотографий потерпевших». В результате было создано порядка 7 тыс. порнографических снимков, которые затем реализовывались через интернет.⁴⁴


С января 2025 года пользователи могут создавать или размещать видеоматериалы, сгенерированные ИИ, только через интеграцию с национальной системой подтверждения подлинности «Real ID». Теперь, перед публикацией видео, созданного с использованием дипфейк-технологий, автору потребуется пройти процедуру распознавания лица. После успешной верификации система автоматически оформляет цифровой сертификат, который навсегда свяжет данный контент с его создателем.⁴⁵

⁴¹ 国家广播电视总局, URL: <https://www.nrta.gov.cn/> (дата обращения: 13.02.2026).

⁴² 国家金融监督管理总局, URL: <https://www.nfra.gov.cn> (дата обращения: 12.02.2026).

⁴³ 2024 人工智能安全报告-奇安信, URL: https://www.qianxin.com/threat/reportdetail?report_id=311 (дата обращения: 13.02.2024).

⁴⁴ Яо Ли Использование технологии «дипфейк» в Китае: проблемы правового регулирования и пути их решения // Lex Russica. 2024. №11 (216). URL: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-dipfeyk-v-kitae-problemy-pravovogo-regulirovaniya-i-puti-ih-resheniya> (дата обращения: 12.02.2026).

⁴⁵ Регулирование искусственного интеллекта в Китае  | Бизнес с Китаем сетевое издание, URL: <https://hbh.ru/biznes/tehnologii-i-innovatsii/iskusstvennyy-intellekt/2025/09/29/10288/regulirovanie-iskusstvennogo-intellekta-v-kitae/?ysclid=mls2tdxq7n704449924> (дата обращения: 14.02.2026).

К сентябрю 2025 года САС сформировал перечень из примерно 140 разработок в сфере генеративного ИИ, свободных для применения. Фокус сместился с количества параметров моделей на качество используемых данных, их энергоёмкость и узкую специализацию. Требование о 100% предварительной проверке обучающих данных осталось в силе, но методы его соблюдения усложнились. Компании теперь обязаны представлять САС не только детализацию датасетов, но и результаты работы «белых хакеров», которые стремятся спровоцировать модель на генерацию нежелательного контента. Модели, прошедшие проверку, получают «знак качества», который укрепит доверие пользователей к продукту.⁴⁶

Иностранные алгоритмы ИИ, поступающие на китайский рынок, в первую очередь подпадают под Требования о регистрации и подаче заявок в соответствии с Временными мерами по управлению службами генеративного ИИ (Interim Measures for the Management of Generative Artificial Intelligence Services).

Процесс, как правило, включает в себя двухэтапную процедуру:

- 1 этап: подача заявки на алгоритм в Администрацию киберпространства Китая (САС) в соответствии с рекомендациями по алгоритму и положениями о глубоком синтезе;
- 2 этап: прохождение проверки сетевой безопасности и получение разрешения на регистрацию собственной «большой модели», предоставляющей коммерческие услуги для общественности.

Предприятия с иностранными инвестициями должны представить дополнительные материалы, такие как информационные отчеты об иностранных инвестициях и сведения о структуре акционерного капитала, чтобы регулятор мог удостовериться в отсутствии уклонения от соблюдения нормативных требований через «фирмы-прокладки». Также компания должна продемонстрировать соответствие требованиям трансграничной передачи данных.

Проверка моделей ИИ на **соответствие китайским национальным ценностям** представляет многоуровневый процесс при участии как государственных, так и коммерческих структур.

Упорядочить данный процесс, в частности, призван т.н. Проект промежуточных мер для общественного обсуждения, опубликованный САС в январе 2026 года⁴⁷. Согласно

⁴⁶ Там же.

⁴⁷ <https://www.allenandgledhill.com/perspectives/publications/knowledge-updates-china/2026/china-proposes-new-rules-to-govern-human-like-ai/?agreed=cookiepolicy>

«Временные меры по управлению гуманизированными интерактивными услугами на основе искусственного интеллекта (проект для общественного обсуждения)»

https://www.cac.gov.cn/2025-12/27/c_1768571207311996.htm

проекту, поставщики услуг должны обеспечить соответствие своих обучающих датасетов "основным социалистическим ценностям" и традиционной китайской культуре, используя «чистые» данные из законных источников, имеющие соответствующую маркировку.

Перед запуском или существенным обновлением услуги провайдеры обязаны провести оценку безопасности и представить отчеты в местные органы управления киберпространством, особенно в случае, если услуги достигают определенных пороговых значений для пользователей. Эти оценки, наряду с обязательным анализом алгоритмов и оценкой этических норм, должны подтвердить, что ИИ-модели:

- не угрожают национальной безопасности;
- не распространяют дезинформацию;
- не продвигают запрещенный контент.

Установленный порядок (фреймворк) требует, чтобы контент приводился в соответствие посредством предпродажного тестирования, постоянного мониторинга и специальных механизмов фильтрации.

3.3 Некоторые кейсы государственного регулирования дипфейк-технологий в КНР

3.3.1 Общенациональная кампания по борьбе с немаркированным и вводящим в заблуждение контентом с использованием ИИ

В феврале 2026 года САС объявила о результатах масштабной кампании по борьбе с несанкционированным контентом, созданным с помощью искусственного интеллекта. Масштаб акции оказался значительным: были оштрафованы 13,4 тыс. учетных записей, удалено более 543 тыс. единиц незаконного или несоответствующего требованиям контента.⁴⁸ Под ударом регулятора оказались аккаунты и продавцы электронной продукции на таких платформах, как *Xiaohongshu*, *Taobao* и *Pinduoduo*, предоставляющие ПО или учебные пособия для удаления ИИ-меток и водяных знаков. Были выделены отдельные категории аккаунтов, нарушающих законодательство. Например, «Ping 9419» и подобные ему пользователи в WeChat, использовали искусственный интеллект для смены лиц и клонирования голоса, чтобы выдавать себя за спортсменов, актеров и предпринимателей, привлекать подписчиков и продавать несанкционированные видеоролики с «благословениями», произведенные генеративным ИИ. Такие аккаунты, как «Fish in the Alley» на Douyin, использовали ИИ для создания ложных изображений и видеозаписей с места пожара, для придания

⁴⁸ Китайские власти взяли за немаркированный ИИ-контент - BRICS Competition, URL: <http://bricscompetition.org/ru/news/chinese-authorities-crack-down-on-unlabeled-ai-generated-content> (дата обращения: 15.02.2026).

сенсационного характера сфабрикованным несчастным случаем с целью нарушения общественного порядка.⁴⁹ Кампания явилась ещё одним проявлением бескомпромиссной борьбы с контентом, который вводит общественность в заблуждение или нарушает общественный порядок.

В марте 2026 года завершилось общественное обсуждение Закона о предотвращении киберпреступности и борьбе с ней (*Law on the Prevention and Control of Cybercrime*.) Согласно будущему НПА, поставщикам услуг, отказавшимся маркировать ИИ-контент должным образом, грозят штрафы в размере от 50 тыс. до 5 млн юаней в серьезных случаях, а нарушения, затрагивающие несовершеннолетних, наказываются штрафами до 500 тыс. юаней и лишением свободы на срок до 15 дней.

3.3.2 Кампания NRTA по борьбе с культурным вандализмом

В течение января 2026 года Национальное управление радио и телевидения (NRTA) провело кампанию по борьбе с видео, измененными с помощью генеративного ИИ, которые «искажают, пародируют или вульгаризируют» культурное наследие Китая⁵⁰, в частности классические китайские фильмы и литературу, такие как «Путешествие на Запад» и «Романтика троецарствия». Кроме того, преследовались видеоролики с участием классических персонажей в жестоких, причудливых или вульгарных сценах (например, Будда с пистолетом в руках).

В обоснование принятых мер власти Китая утверждали, что данные видеоролики нарушают авторские права, вредят развитию ИИ-индустрии и мешают пониманию культуры детьми. Цель кампании состоит в том, чтобы «обратить вспять негативную тенденцию распространения видео, измененных с помощью ИИ, и создать благоприятную онлайн-среду для здорового роста молодежи». В рамках кампании от онлайн-платформ требовалось усилить проверку контента и наказывать аккаунты-нарушители, тем самым укрепляя роль государства в сохранении культурных традиций и защите несовершеннолетних.

3.3.3 Административное задержание за дезинформацию о дорожно-транспортном коллапсе в Шанхае

14 февраля 2026 года полиция Шанхая подвергла административному задержанию 49-летнюю женщину Луо, которая создала и распространила видео, полностью созданное с

⁴⁹傳播無 AI 標識的虛假不實資訊, 13421 個賬號被處置_財經_中國網, URL:

<http://big5.china.com.cn/gate/big5/finance.china.com.cn/industry/20260213/6294240.shtml> (дата обращения: 16.02.2026).

⁵⁰ China launches crackdown on 'vulgar' AI-altered videos – CNA, URL: https://www.channelnewsasia.com/east-asia/china-crackdown-campaign-vulgar-ai-videos-5785366?cid=internal_mcdrecs_03012026_mcs#mcdrecs_s (дата обращения: 16.02.2026).

помощью искусственного интеллекта. На видео демонстрируется «несуществующий» крупный дорожный коллапс на строительной площадке шанхайского метро. Видео стало вирусным, вызвав «негативные социальные последствия». ⁵¹ Правоохранительные органы приняли меры: полиция быстро определила вброшенную информацию как дипфейк и задержала женщину за распространение дезинформации. Случай демонстрирует, что власти КНР готовы использовать меры вплоть до ограничения свободы, чтобы удержать людей от использования ИИ для создания паники в обществе или распространения ложных сообщений.

3.3.4 Противоправное использование дипфейков для финансовых преступлений

Новым форматом борьбы является трансграничное сотрудничество по выявлению и предотвращению финансовых преступлений, совершаемых с помощью дипфейк-технологий. В конце 2024 года Прокуратура Тайваня предъявила обвинения четырем членам сети кибермошенников в Тайчжуне. Мошенники вели сбор личной информации китайских граждан. Они использовали эти данные для создания фальшивых видеороликов о жертвах, которые затем использовались для обхода распознавания лиц в приложениях мобильного банкинга в китайском цифровом юане (e-CNY), похитив более 200 млн новых тайваньских долларов (~6,33 млн долларов США), их жертвами стали по меньшей мере 55 человек. ⁵² В ходе расследования и розыскных мероприятий лидер мошенников был арестован в Таиланде и экстрадирован на Тайвань, а оборудование, использованное в преступлениях (320 смартфонов и шесть компьютеров) конфисковано.

3.3.5 «Дело Тодда»: судебный процесс о замене лица иностранным ИИ

Одним из наиболее значимых прецедентов является судебный иск, поданный Тоддом, американским актером и моделью, проживающим в Пекине, против китайской технологической компании Lexin Shenwen. ⁵³ Тодд обнаружил, что его лицо и голос были обработаны искусственным интеллектом в более чем 700 рекламных роликах мобильных игр, таких как «Пасьянс Маджонг». Рекламные ролики, в которых Тодд изображался как фальшивый врач, рекламирующий мнимые преимущества для здоровья, были распространены по всему миру в сервисах Meta ⁵⁴. Компания-ответчик

⁵¹ Chinese police detain woman over AI-generated video of Shanghai road collapse, URL: <https://www.aa.com.tr/en/asia-pacific/chinese-police-detain-woman-over-ai-generated-video-of-shanghai-road-collapse/3830234> (дата обращения: 14.02.2026).

⁵² Prosecutors indict 4 in deepfake fraud case targeting Chinese - Taipei Times, URL: <https://www.taipeitimes.com/News/taiwan/archives/2026/02/03/2003851707> (дата обращения: 12.02.2026).

⁵³ 颜星悦. (2026, February 11). "那是我的脸 · 但说的全是谎言" [That's my face, but the words are all lies]. 北青深一度 (Beijing Youth Daily - Deep One Degree), URL: <http://report.yynet.com/2026/02/11/3985843t1335.html> (дата обращения: 14.02.2026).

⁵⁴ Экстремистская организация, деятельность которой на территории Российской Федерации запрещена.

организовала свою деятельность таким образом, чтобы обойти регулирование, разместив IP-адрес игры в Китае, а рекламную деятельность вела от имени сингапурской подставной компании.

Первоначально Тодду было сложно подать в суд в Китае из-за неясности юрисдикции. Дело было успешно передано в окружной суд Хайдянь в Пекине в ноябре 2025 года после того, как команда истца добыла ключевые доказательства: Lexin Shenwen публично объявила игру своим собственным «успешным продуктом» на своем китайском веб-сайте. Это позволило китайским судам применить юрисдикцию на основе принципа «фактического контролирующего субъекта». В результате ответчик удалил видеоролики, нарушающие авторские права. «Дело Тодда» стало важным прецедентом по успешному привлечению китайских компаний к ответственности за вред, наносимый генеративным ИИ даже в тех случаях, когда они пытаются использовать иностранные подставные компании для его осуществления.

3.4 Меры саморегулирования со стороны крупных компаний

С 2001 года в Китае функционирует национальная отраслевая некоммерческая организация «Интернет-общество Китая» (ISC), которая служит единым органом для саморегулирования в сфере интернет-технологий. В состав ISC входят порядка 1300 представителей китайской интернет-индустрии, включая интернет-компании, операторов сетевого доступа, интернет-провайдеров, производителей оборудования и НИИ.⁵⁵ Важность ISC заключается в разработке правил саморегуляции, в том числе «Публичного обязательства по самодисциплине для китайской Интернет-индустрии», которое подписали тысячи компаний, включая Baidu, Soseen, Yahoo, Microsoft и Google. Подписав это обязательство, компании берут на себя ответственность за выявление и предотвращение распространения информации, которую китайские власти считают нежелательной, включая материалы, «нарушающие законы, пропагандирующие суеверия или непристойность», а также те, что представляют угрозу государственной безопасности или нарушают социальную стабильность.

Базовым элементом саморегуляции стала практика добровольной регистрации алгоритмов. В январе 2023 года Alibaba, Tencent и Baidu стали одними из первых, кто внес свои алгоритмы глубокого синтеза в официальный реестр, проведя предварительную оценку рисков перед предоставлением данных регулятору САС. А уже

⁵⁵ 中国互联网协会, URL: <https://www.isc.org.cn/en> (дата обращения: 15.02.2026).

к маю 2023 года в системе присутствовали сведения о 262 алгоритмах от более 100 платформ.⁵⁶

Кроме того, ведущие китайские технологические компании постепенно осуществляют повсеместное внедрение систем идентификации ИИ-контента. Одной из первых компаний, внедривших алгоритмы безопасности для генеративного ИИ, стала уже упомянутая Alibaba. В июле 2025 года Alibaba Cloud представил продукт AI Guardrails, представляющий собой специализированную систему защиты, интегрируемую непосредственно в процесс функционирования больших языковых моделей.⁵⁷ Эта система автоматически фильтрует как входящие запросы пользователей, так и генерируемые ответы, анализируя их по множеству параметров, от политической корректности до выявления потенциальных попыток взлома.

С введением новых правил маркировки ИИ-контента в сентябре 2025 года такие гиганты, как Douyin, Tencent, Kuaishou, Bilibili и DeepSeek обязали разработчиков применять как видимые, так и скрытые формы маркировки. Первые включают водяные знаки и текстовые уведомления для пользователей, вторые — незаметные для человеческого глаза метаданные, позволяющие проследить источник любого сгенерированного материала.⁵⁸

В декабре 2025 года восемь крупнейших игровых площадок, в том числе JD.com, Meituan, Douyin и Xiaohongshu, подписали первое в КНР соглашение об ответственном использовании ИИ с Пекинской ассоциацией потребителей. Этот документ закрепил шесть основополагающих принципов, среди которых – прямой запрет на создание дипфейков с использованием образов знаменитостей в мошеннических целях, а также требование комбинировать автоматическое обнаружение нарушений с человеческим надзором. Этот шаг стал значительным движением от разрозненных инициатив к формированию общепромышленного стандарта.⁵⁹

В начале 2026 года власти КНР сообщили, что основные платформы для создания контента с использованием искусственного интеллекта, включая Doubao, DeepSeek, Qwen и Yiyan, прикрепили ярлыки с использованием искусственного интеллекта к более чем 150 млрд фрагментов сгенерированного контента. В то же время ведущие

⁵⁶ SAC опубликовала список зарегистрированных алгоритмов глубокого синтеза от Alibaba, Tencent и Baidu - BRICS Competition, URL: <https://bricscompetition.org/ru/news/cac-unveils-first-list-of-registered-deep-synthesis-algorithms-developed-by-likes-of-alibaba-baidu> (дата обращения: 15.02.2026).

⁵⁷ What is AI Guardrails - Content Moderation - Alibaba Cloud Documentation Center, URL: <https://www.alibabacloud.com/help/en/content-moderation/latest/what-is-ai-security-barrier>

⁵⁸ 中國規管 AI 生成內容 抖音騰訊等上線標識功能, URL: <https://hkcna.hk/h5/docDetail.jsp?channel=2813&id=101098270> (дата обращения: 17.02.2026).

⁵⁹ Chinese platforms sign first responsible-AI pledge after probe flags oversight gaps | MLex | Specialist news and analysis on legal risk and regulation, URL: <https://www.mlex.com/mlex/articles/2418533/chinese-platforms-sign-first-responsible-ai-pledge-after-probe-flags-oversight-gaps> (дата обращения: 18.02.2026).

платформы социальных сетей опубликовали на экране информацию о более чем 220 млн единицах контента, созданного с помощью ИИ.⁶⁰

Показательным примером превентивного добровольного ограничения стал случай с видеогенеративной моделью Seedance 2.0 от ByteDance в феврале 2026 года.⁶¹ Обнаружив, что модель способна воспроизводить человеческую речь на основе лишь фотографии, создавая тем самым беспрецедентные риски мошенничества, компания оперативно, ещё до поступления каких-либо указаний со стороны регуляторов, приостановила данную функцию. Взамен была внедрена улучшенная процедура верификации в реальном времени, требующая одновременной записи изображения и голоса пользователя. Подобные решения наглядно демонстрируют готовность бизнеса идти на компромисс в функциональности ради обеспечения безопасности.

IV ОСНОВНЫЕ ВЫВОДЫ

Общие особенности китайского регулирования глубокого синтеза

Китайская стратегия направлена на уравнивание мер по развитию и контролю новых технологий на основе генеративных алгоритмов. С одной стороны, государство стимулирует инновации и технологический суверенитет (целевое финансирование, образование, развитие инфраструктуры), а с другой — достаточно жестко контролирует риски, стремясь на раннем этапе не допустить дестабилизации общества и потери управляемости информационным полем.

Регулирование глубокого синтеза в Китае направлено на реализацию сразу нескольких задач и приоритетных векторов:

- не тормозить инновации и сохранять технологическое лидерство;
- обеспечить четкий и полноценный государственный контроль и защищать социалистические ценности;
- не выпадать из мировых тенденций⁶² и совершенствовать законодательную базу так, чтобы укреплять выгодное партнёрство в проектах, которые приносят коммерческие

⁶⁰ China's AI content-labelling rules tame risks - People's Daily Online, URL: <https://en.people.cn/n3/2026/0210/c90000-20424448.html> (дата обращения: 14.02.2026).

⁶¹ ByteDance suspends Seedance 2.0 feature that turns facial photos into personal voices over potential risks · TechNode, URL: <https://technode.com/2026/02/10/bytedance-suspends-seedance-2-0-feature-that-turns-facial-photos-into-personal-voices-over-potential-risks/> (дата обращения: 18.02.2026).

⁶² Управление ИИ: Актуальные международные инструменты, Аналитический обзор, Центр глобальной ИТ-кооперации, Игнатъев А.Г., Курбатова Т.А., Шамраев Р.А., 33 С, 2025 <https://cgitic.ru/research/upravlenie-ii-aktualnye-mezhdunarodnye-instrumenty/>

дивиденды, наращивать конкурентоспособность и эффективно проводить научное сотрудничество и торговые операции на глобальном рынке ИИ.

Терминология

В китайском подходе к определению моделей, основанных на технологиях генеративного ИИ применяется термин «глубокий синтез», который с точки зрения китайских специалистов более широко и технически достоверно отражает специфику данной области регулирования. По отношению к определению «дипфейки» (одна из форм возможных продуктов, произведенных с помощью ИИ) данный китайский термин («глубокий синтез»), по мнению китайских исследователей, несет в себе большую нейтральность.

Быстрое реагирование и многоуровневость, обеспечивающее лидерство.

Регулирование не опирается на один всеобъемлющий правовой акт, а выстраивается по принципу быстрого реагирования по мере возникновения новых технологических возможностей и соответствующих правовых коллизий, новых видов нарушений и злоупотреблений.

Китай демонстрирует одну из самых оперативных реакций на технологические изменения в мире. В стране водятся в действие инструменты, которые со временем дополняются и развиваются, в том числе с учетом накопленных и зарегистрированных инцидентов и ситуаций правовой неопределенности. Это позволяет Китаю играть роль первопроходца во многих сферах, связанных с регулированием ИИ.

Вместе с тем, Китай внимательно наблюдает за происходящим на международных площадках⁶³, в т. ч. применительно к вопросам регулирования больших языковых моделей.⁶⁴ Власти стремятся строить внутреннее законодательство так, чтобы не выпадать из международных норм, правил и современных тенденций регулирования. Национальные законодательные инструменты учитывают мировую практику, однако, в чувствительных для себя областях могут идти на внедрение особых режимов для своего рынка.

Маркировка как обеспечение большей прозрачности

⁶³ Там же, см. Управление ИИ: Актуальные международные инструменты.

⁶⁴ Зарубежные подходы к регулированию больших языковых моделей (LLM), Аналитический обзор, Игнатъев А.Г., Центр глобальной ИТ-кооперации, 26 С, 2026

<https://cgitc.ru/research/zarubezhnye-podkhody-k-regulirovaniyu-bolshikh-yazykovykh-modeley-llm/>

Введение обязательной маркировка контента, связанного с ИИ, является ключевым инструментом обеспечения прозрачности и борьбы с дезинформацией. Провайдеры и пользователи обязаны четко обозначать текст, изображения, аудио и видео, сгенерированные искусственным интеллектом. Это обеспечивается как отражением в метаданных, так и визуальными водяными знаками, чтобы потребитель мог идентифицировать происхождение контента. Такой регуляторный инструмент изначально снижает риски мошенничества, введения в заблуждение, манипуляции, негативных форм влияния на аудиторию и т. п.

Трудности внедрения маркировки

Помимо положительных эффектов маркировки, возникают и проблемы, угрожающие подорвать эффективность нормативно-правовой базы. Появился подпольный рынок, специально предназначенный для обхода вступивших в силу правил маркировки. Так, например, поиск в Интернете по запросу «удаление ИИ-меток» позволяет найти инструменты обхода всего за 9,9 юаней ($\approx 1,4$ доллара США), а также обнаружить и другие, более специализированные услуги (под конкретный продукт) за более высокую плату.⁶⁵

Исследования китайского подпольного рынка показали, что методы «уклонения» эволюционировали от простого обрезания меток до «многоуровневых процессов, включающих очистку метаданных, многократное преобразование форматов файлов и кросс-платформенную перепечатку». Контент, помеченный на одной платформе, может остаться незамеченным на другой из-за различий в стандартах обнаружения. Кроме того, как отмечают юристы, штрафы за нарушение правил маркировки не имеют четких критериев, а технические характеристики самих индикаторов еще не стандартизированы для всех платформ. Технологии регулирования дипфейков и в целом генеративного ИИ на большинстве платформ остаются «хрупкими», и для предотвращения «белых пятен» требуется разработка новых стандартов и спецификаций (как правового, так и технического свойства).

Направленный (целевой) контроль. Регулирование не технологии, а режимов ее использования. Упреждающий характер правовых норм.

Правовые акты обращены к конкретным категориям акторов (разработчики, провайдеры, пользователи). Таким образом ответственность в определенной части требований лежит на всех участниках: от создателя алгоритма до конечного пользователя, публикующего

⁶⁵ China's AI content-labelling rules tame risks - People's Daily Online, URL: <https://en.people.cn/n3/2026/0210/c90000-20424448.html> (дата обращения: 14.02.2026).

сгенерированный материал (вся цепочка от создания систем до использования произведенного контента).

Китайская модель предполагает превентивный контроль - провайдеры генеративных сервисов (в первую очередь это относится к публично доступным) обязаны до начала работы пройти процедуру оценки безопасности и зарегистрировать алгоритмы в органах власти. Не ожидая пока технологии ИИ вызовут необратимые последствия, регулятор вводит «правила игры» на раннем этапе коммерциализации и массового распространения систем глубокого синтеза. Это позволяет не только минимизировать ущерб, но и задать стандарты, которым вынуждены будут следовать все игроки рынка.

Таким образом со стороны государства обеспечивается должный надзор еще на этапе внедрения технологии (упреждающий характер регулирования), это в свою очередь сокращает зону риска и государству не приходится реагировать на массовые инциденты и негативные последствия.

В этом смысле китайское законодательство предъявляет более жесткие требования, чем существующие в США или Великобритании. Что касается общего сравнения с регуляторным подходом ЕС, можно отметить, что европейские правовые акты делают первостепенный акцент на защиту фундаментальных прав человека (*privacy, non-discrimination*), в то время как в Китае регуляторные требования прежде всего призваны обеспечить суверенитет национального информационного пространства, безопасное социальное развитие общества на основе идеологических установок правящей КПК, которая последовательно проводит социалистические реформы с китайской спецификой.

Влияние на глобальный рынок и мировые стандарты регулирования

Китайская модель регулирования оказывает влияние на формирование глобальных норм и стандартов в сфере ИИ. Транснациональные корпорации, работающие в Китае, боясь потерять важный рынок, адаптируют свои продукты под местные требования (алгоритмическая прозрачность, маркировка, цензура), — это так или иначе способствует распространению этих практик в других юрисдикциях, особенно в странах глобального Юга, которые ориентируются на китайский опыт.

Идеологическая цензура. Защита социалистических ценностей.

Режимы использования ИИ должны гарантировать, что соответствующие модели и результаты их работы соответствуют "основным социалистическим ценностям", не угрожают национальной безопасности и социальной стабильности. Это означает, что системы ИИ проходят проверку на предмет того, что их решения (*output*) не содержит контента, подрывающего государственные устои или общественный порядок. Регулирование здесь напрямую увязано с политическим и идеологическим контролем.

Обязательная проверка алгоритмов на лояльность режиму, идеологическую корректность, на отсутствие последствий, способных подорвать общественный порядок является не менее важной, чем проверка на техническую безопасность.

Промежуточная оценка результатов и перспективы

Китай одним из первых осваивает правовые практики маркировки генеративного ИИ. Это дает определенные позитивные плоды, однако и заставляет первым проходить трудности поиска сбалансированных решений. Такая ситуация превращает страну в регуляторную песочницу, как испытательную лабораторию, к которой прикованы взгляды всего мира.

Тем не менее, безусловно ценный и полезный опыт Китая не может быть заимствован полностью и безоговорочно, поскольку специфика социальной модели этой страны не позволяет в ряде случаев зеркально копировать китайский опыт.

БИБЛИОГРАФИЯ

1. "China implements mandatory AI content labeling standards effective September." *PPC Land*, September 2, 2025. <https://ppc.land/china-implements-mandatory-ai-content-labeling-standards-effective-september/>.
2. "China's Multi-Layered Framework for Regulating Generative AI", *Belgravia Law*, Dec 28, 2025, <https://belgravia.law/news/chinas-multi-layered-framework-for-regulating-generative-ai>
3. "China's new rule requiring tech companies to label AI-generated content." *GeoPolitechs*, March 15, 2025. <https://www.geopolitechs.org/p/chinas-new-rule-requiring-tech-companies>.
4. Cyberspace Administration of China and Ministry of Public Security. «Меры по обеспечению безопасности применения технологии распознавания лиц» [Measures for Security Management of the Application of Face Recognition Technology]. 2025. https://www.lexiscn.com/latest_message.php?id=481510.
5. Cyberspace Administration of China and Ministry of Public Security. «Меры по обеспечению безопасности применения технологии распознавания лиц» [Measures for Security Management of the Application of Face Recognition Technology]. 2025. https://www.gov.cn/zhengce/content/202503/content_7014874.htm.
6. Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and National Radio and Television Administration. "Circular on Issuing the 'Measures for Labeling Artificial Intelligence-Generated Contents'." Notice No. 2025-2. March 7, 2025.
7. Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and National Radio and Television Administration. «Меры по идентификации контента, создаваемого искусственным интеллектом и синтетического контента» [Measures for Identifying Artificial Intelligence-Generated and Synthetic Content]. 2025. <http://politics.people.com.cn/BIG5/n1/2025/0314/c1001-40439289.html>.
8. Cyberspace Administration of China. «Временные меры по управлению услугами генеративного искусственного интеллекта» [Interim Measures for the Administration of Generative Artificial Intelligence Services]. 2023. <https://www.ncwxw.gov.cn/sys-nd/1461.html>.
9. Feng, Coco. "China Rolls Out 'Voluntary' Cyber ID System amid Concerns over Privacy, Censorship." *South China Morning Post*, July 15, 2025. <https://www.scmp.com/tech/tech-trends/article/3318302/china-rolls-out-voluntary-cyber-id-system-amid-concerns-over-privacy-censorship>.
10. Guangzhou Cyberspace Affairs Office. "专家解读 | 给人工智能生成合成内容贴上数字标识" [Expert Interpretation: Affixing Digital Labels to AI-Generated and

- Synthetic Content]. September 22, 2025. <https://gzwx.gov.cn/context/contextId/214197>.
11. ID Tech Wire. "China Prepares Rollout of National Cyberspace ID for Internet Users." July 7, 2025. <https://idtechwire.com/china-prepares-rollout-of-national-cyberspace-id-for-internet-users/>.
12. JunHe LLP. "Key Points of the Interim Measures for the Administration of Artificial Intelligence Generated Content." July 18, 2023. <https://junhe.com/legal-updates/2219?locale=en>.
13. LexisNexis. "Two Departments Publish Measures for Security Management of the Application of Face Recognition Technology." March 24, 2025. https://www.lexiscn.com/latest_message.php?id=481510.
14. Li, Qiangzhi (李强治). "以内容标识化解治理困境，筑牢“人工智能+”行动安全底座" [Resolving Governance Dilemmas with Content Identification, Building a Secure Foundation for the "AI+" Initiative]. China Youth Net, September 6, 2025. https://news.youth.cn/gn/202509/t20250906_16220579.htm.
15. Ministry of Industry and Information Technology of the PRC. «Положение об администрировании услуг интернет-информации с использованием технологий глубокого синтеза» [Provisions on the Administration of Deep Synthesis Internet Information Services]. 2023. https://www.miit.gov.cn/gyhxxhb/jgsj/cyzcyfgs/bmgz/xxtxl/art/2023/art_6a1b68b98a51462c99550ed73a3c655e.html.
16. State Council of the PRC. «Положение о государственной службе сетевой аутентификации личности» [Measures for the National Network Identity Authentication Public Service]. 2025. http://big5.www.gov.cn/gate/big5/www.gov.cn/govweb/gongbao/2025/issue_12166/202507/content_7032498.html.
17. The Register. "China approves rules for national 'online number' ID scheme." May 26, 2025. https://www.theregister.com/2025/05/26/asia_tech_news_roundup/.