Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

- **Ограничения для платформ электронной коммерции**
- **Доступ к данным**
- **Ценообразование на платформах**
- **Регулирование криптоактивов**
- **Ответственное использование ИИ**

Мониторинг №7 (19) (Июль 2025)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института экономической политики имени Е. Т. Гайдара (Института Гайдара).

Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Магомедова О.С., науч. сотр. Черновол К.А., юрисконсульт Фонда Экономической политики Голованова Д.А.

«Июль – макушка лета. –
Напомнила газета,
Но прежде всех газет –
Дневного убыль света.»
А. Твардовский

В июле 2025 г. можно выделить 5 событий, которые определяют тренды развития регулирования цифровой экономики в мире.

Тренд № 1. Ограничения для платформ электронной коммерции

В июле 2025 г. в России принят Закон о регулировании посреднических платформ, включая платформы занятости. Установлено право продавца не участвовать в распродажах платформы, необходимость уведомления пользователей платформы при изменении договора и пр. В Китае введена процедура сбора публичных мнений при изменении правил платформ, а также урегулировано новое направление в электронной коммерции – livestream-продажи.

Тренд № 2. Доступ к данным

Суд ЕС отменил решение европейского регулятора об отказе пользователю в доступе к информации о деятельности обработчика данных. Еврокомиссия разработала условия бесплатного доступа исследователей к данным платформ. В Италии обсудили практику сбора платформами данных пользователей в качестве платы за доступ к контенту. А ЕС и США объявили о торговом соглашении, включая беспошлинную передачу данных.

Тренд № 3. Ценообразование на платформах

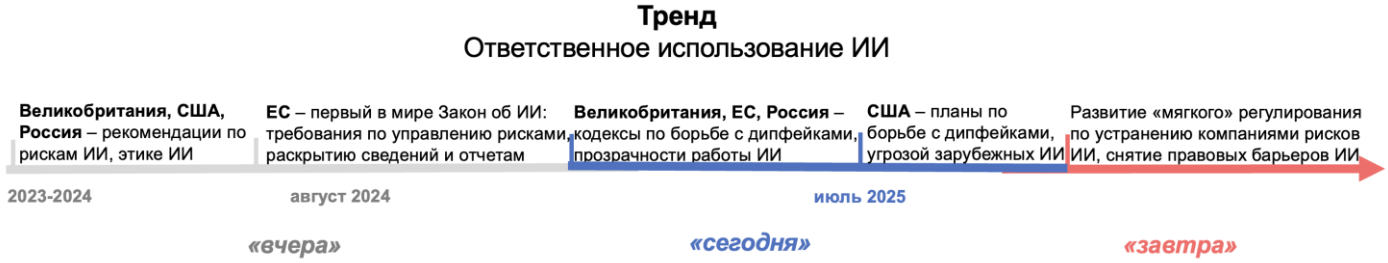
В июле 2025 г. Канада подготовила обзор практик алгоритмического ценообразования, а Франция оштрафовала маркетплейс Shein на 40 млн евро за недостоверную информацию о ценах на распродажах.

Тренд № 4. Регулирование криптоактивов

В июле 2025 г. ESMA[1] опубликовало руководство для поставщиков услуг криптоактивов о необходимости чёткого разделения регулируемых и нерегулируемых криптоактивов на их платформе (в рекламе, в договорах и пр.). В США вступил в силу первый федеральный закон, регулирующий платёжные стейблкоины. В России в Госдуму внесён законопроект о штрафах за расчёты в криптовалюте.

Тренд № 5. Ответственное использование ИИ

В июле 2025 г. в ЕС и Великобритании выпущены рекомендации по ответственному ИИ, касающиеся борьбы с дипфейками, безопасности ИИ. В США План по ИИ теперь включает поддержку стартапов, проверку иностранных систем ИИ на угрозы и иные темы. В России в Кодексе этики ИИ на финансовом рынке закрепляется право клиента на отказ взаимодействовать с ИИ, а также право знать, почему он принял то или иное решение и т.д.



В июле 2025 г. в России введен ряд нововведений:

1. Утверждены критерии онлайн-рекламы[2]

Утверждение критериев особенно важно после введения с апреля 2025 г. 3% сбора с доходов от размещения онлайн-рекламы[3]. Онлайн-рекламой признаётся информация на маркетплейсах (агрегаторах), классифайдах, в поиске и соцсетях, направленная на продвижение товара, услуги или бренда. При этом рекламой не является информация:

1) которая носит характер справочно-информационных или аналитических материалов. Например, результаты поисковой выдачи без признаков продвижения; каталог товаров/услуг и пр.

2) частные объявления, несвязанные с предпринимательством, например, о продаже личного имущества.

Новые критерии исключают риск взимания сбора с нерекламной информации, например, при размещении карточек товаров на маркетплейсах. Вместе с тем новые критерии не учитывают ряд признаков рекламы, ранее отмеченных ФАС, например, размещение описаний товаров и контактных данных продавца на собственных ресурсах.

2. Введены ограничения использования и рекламы VPN

В КоАП РФ[4] введена ответственность за обход блокировок, поиск экстремистских материалов[5][6] через VPN[7] или аналогичные сервисы. Но существует риск расширительного

[1] Европейское управление по ценным бумагам и рынкам.
2 Постановление Правительства РФ от 24.07.2025 № 1087 "Об утверждении критериев отнесения к рекламе информации, распространяемой на отдельных информационных ресурсах в информационно-телекоммуникационной сети "Интернет".
3 Постановление об утверждении особенностей исчисления и уплаты обязательных отчислений, предусмотренных ч. 1 ст. 182 Федерального закона «О рекламе», и порядка осуществления мониторинга за полнотой и своевременностью уплаты таких отчислений.
[4] Кодекс Российской Федерации об административных правонарушениях (ст. 13.53).
[5] Согласно федеральному списку экстремистских материалов Министерства юстиции России.
[6] Федеральный закон от 31.07.2025 № 281-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях.
[7] Программно-аппаратные средства доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

толкования такого запрета. Например, неясно, кто и как будет отслеживать переходы на такие ресурсы по VPN (особенно если меняется IP-адрес). Будет ли нарушением просмотр контента в социальной сети, признанной экстремистской организацией, или нарушение уже будет считаться совершенным при публикации фотографий в этой соцсети?

Также запрещается реклама VPN-сервисов (штраф — до 500 тыс. руб.). Владельцы VPN-сервисов должны по требованию Роскомнадзора ограничивать доступ к запрещённым ресурсам через VPN. Вместе с тем использование VPN в повседневных целях остаётся законным. В то же время применение средств обхода блокировок при совершении административных правонарушений и уголовных преступлений будет признаваться отягчающим обстоятельством с последующим назначением более строгих мер наказания.

Также в целях облегчения идентификации лиц, пользующихся VPN-сервисами для поиска информации, введён запрет на передачу средств идентификации в телекоммуникационных сетях (мобильные телефоны или аккаунты)[8].

Кроме того, в целях облегчения идентификации лиц, пользующихся VPN-сервисами для поиска информации, введён запрет на передачу другому лицу в пользование своего номера мобильного телефона или аккаунта.

3. Ограничения работы RuStore в технике признаны недостатком товара

Еще в 2022 г. правительством РФ был разработан RuStore (единый магазин приложений), который стал обязательным для предустановки на устройства (телефоны, компьютеры). А в июле 2025 г. Закон о защите прав потребителей запретил производителям технически сложных устройств ограничивать возможность установки программ, приложений через RuStore, а также использование таких программ (например, ограничения поиска, обновления, управления их настройками и пр.), ограничивать способы оплаты приложений в RuStore[9]. Введение регулирования связано с тем, что отдельные производители устройств (прежде всего Apple) в лицензионных соглашениях ограничивают возможность скачивания приложений из сторонних сайтов, конкурирующих магазинов приложений и пр.

Теперь ограничение функционирования RuStore и скаченных приложений будет считаться недостатком товара, поэтому потребитель сможет его вернуть продавцу для исправления, замены или возврата средств.

[8] Кодекс Российской Федерации об административных правонарушениях (ст. 13.29).
[9] Федеральный закон от 07.07.2025 № 194-ФЗ "О внесении изменений в Закон Российской Федерации "О защите прав потребителей".

Ключевые аспекты

1. Ограничения для платформ электронной коммерции

Опыт Китая

В июле 2025 г. на обсуждение вынесен проект Положения[10] по соглашениям об обслуживании бизнес-пользователей, потребителей на платформах, включая маркетплейсы, классифайды, соцсети и пр.

Если платформа меняет правила обслуживания – необходимо провести публичные консультации. Требуется опубликовать проект изменений и в течение 7 дней собирать мнения. Все мнения должны учитываться, а в случае непринятия – необходимо указать причины. Далее новые правила нужно опубликовать за 7 дней до их вступления в силу (в России требуется уведомлять за 15 дней об изменениях). Как и в России в Китае требуется хранить все версии правил платформы не менее 3-х лет.

Запрещено устанавливать для бизнес-пользователей невыгодные условия:

1) необоснованные послепродажные обязательства без согласия продавца – обязательство вернуть деньги покупателю без возврата товара (в России нет такого ограничения);

2) принуждение к участию в рекламных акциях платформы за счет продавца (в России аналогичное ограничение);

3) необоснованные сборы:

- перекладывание на продавцов расходов, если товар продан по цене ниже, установленной продавцом, из-за технического сбоя на платформе;
- взимание платы за доступ продавца к его собственным бизнес-данным;
- принуждение покупать дополнительные услуги: требование подключить платную услугу под угрозой потери видимости товара.

Сегодня в мире развивается новое направление электронной коммерции – livestream-продажи – прямые эфиры (стримы), во время которых продаются товары/услуги. Объемы livestream-продаж растут на 20–30% ежегодно во всем мире.

В июле 2025 г. в Китае к обсуждению предложено Положение о регулировании livestream-продаж[11]. На платформах формируются стрим-залы, через которые проводится эфир. Эфир проводит стример, рекламирующий товары или услуги продавцов. Также к эфирам подключаются рекламные агентства, отвечающие за планирование, настройку и пр. для прямых эфиров. Для каждого типа участников установлены обязанности.

Через платформу формируются стрим-залы, поэтому платформа должна проверять личность стримера, который верифицируется в начале прямого эфира и во время эфира через динамические системы проверки. Платформа обязана проводить обучение стримеров и рекламных агентств.

Платформа должна создать систему управления стрим-залами: выполнить градацию с учетом соответствия аккаунта стрим-зала требованиям законодательства, а также по количеству подписчиков и просмотров, объёма продаж и сумм транзакций и пр. Для стрим-залов с большим количеством посетителей и объемом продаж внедряются дополнительные меры, как технический мониторинг на предмет нарушений в реальном времени, увеличение срока хранения видеозаписей трансляций и пр.

Платформа должна предотвращать использование стримерами дипфейков и пр.

Операторы стрим-залов обязаны:

1) размещать информацию о товарах и услугах продавцов. Информация должна предоставляться без навязанных проверок (captcha), требований донатов и пр.;

2) проводить проверку стримеров (личность, квалификация, статус и пр.);

3) модерировать чат во время стрима, удаляя запрещённый контент.

Опыт России

В июле 2025 г. принят Закон о платформенной экономике, регулирующий «посреднические платформы», которые позволяют размещать заказы, карточки товаров и услуг, совершать сделки, проводить оплату и пр. Регулирование охватывает отношения между платформами

[10] https://www.samr.gov.cn/hd/zjdc/art/2025/art_ed7d047de7cd423e981890d4ece9e974.html

[11] https://www.samr.gov.cn/hd/zjdc/art/2025/art_da63265146f741cd8bc80d2bba4e1e37.html

(как маркетплейсы, классифайды, платформы такси, курьерских услуг и пр.) и их партнерами (исполнителями услуг, работ; продавцами товаров; ПВЗ).

Посреднические платформы, в том числе иностранные, будут включаться в специальный реестр. Иностранные платформы также должны соблюдать закон о «приземлении».

Партнерами платформ могут быть иностранные лица, самозанятые.

Во-первых, новый Закон устанавливает обязанности платформ в отношении продавцов товаров и услуг:

- предоставить возможность размещать в карточке товара информацию о продавце, его товарах/услугах, о лицензиях, сертификатах и пр., о соответствии товаров требованиям технического регулирования и маркировке, в том числе в системе Честный знак;
- проверять информацию в карточке товара на предмет торговли изъятыми из оборота товарами;
- правительство создаст порядок доступа в информационные системы, содержащие перечисленные сведения, чтобы платформа могла их проверить;
- отделять товары, услуги, продаваемые платформой, от продаваемых ее партнерами.

Установлены правила, ограничивающие злоупотребления платформ:

1) платформа не вправе принуждать продавцов делать скидки на распродажах за их счет. Платформа должна уведомлять о введении скидки за 5 дней и получать от партнера письменное согласие, в котором партнер устанавливает минимальную цену, количество товаров со скидкой и сроки участия в скидке. Платформа может вводить скидки без согласия партнера только за свой счет. Запрещено наказывать за отказ от участия в распродажах, например, снижать рейтинг, изменять положение карточки товара в поисковой выдаче и пр.;

2) платформа вправе в одностороннем порядке изменять договор с партнером, ПВЗ, но при условии уведомления за 15 дней (аналогично в ЕС). И за 45 дней, если платформа изменяет меры ответственности партнера, увеличивает комиссии, снижает размер вознаграждения ПВЗ, меняет условия приемки, хранения, доставки, выдачи, возврата товара продавца;

3) платформа может ограничивать возможности размещения карточки товара и доступ к личному кабинету только при уведомлении за 3 дня, либо в день уведомления, если личный кабинет взломан.

Логистическая инфраструктура платформ (склады, распределительные центры, ПВЗ и пр.) должна соответствовать требованиям пожарной безопасности, санитарно-эпидемиологическим требованиям, в том числе продовольственных. В договоре с ПВЗ следует прописать правила о распределении рисков повреждения или случайной гибели товаров.

Кроме того, Законом внедрены нормы регулирования платформенной занятости – курьеров, таксистов и других исполнителей работ и услуг на платформах по гражданско-правовому договору (ГПД). Установлены критерии для работы по ГПД:

- выполнение исполнителем отдельных услуг без привязки к графику и необходимости соблюдения правил внутреннего трудового распорядка;
- исполнитель может отказаться от заказа, а платформа не вправе применять к нему санкции;
- вознаграждение исполнителю должно начисляться отдельно за каждый заказ;
- исполнитель не может вовлекать в работы / услуги третьих лиц – только самостоятельное исполнение;
- платформа не обязана предоставлять социальные гарантии, еженедельные выходные и отпуска и пр.

Интересно, что платформа обязана обеспечивать возможность исполнителей подать заявку на заключение договора с поставщиком страховых услуг (медицинских, пенсионных и пр.) через платформу, а также предоставлять преференции исполнителям, добровольно вступившим в системы страхования (правительство установит минимальный объем таких преференций). Например, платформа вправе полностью или частично возмещать расходы исполнителей на страхование.

Платформа должна контролировать:

- рабочее время в отношении работ, услуг, связанных с источником повышенной опасности, риском для жизни, здоровья,

имущества (например, ограничивать время работы таксиста 12 часами);
- риски привлечения несовершеннолетних к работе, выполнение которой несовершеннолетними не допускается;
- предельно допустимые нормы физических и иных нагрузок;
- соблюдение законодательства о правовом положении иностранных лиц.

Платформа вправе для формирования заказов, определения вознаграждения (порядка и сроков его выплаты) использовать технологии автоматизированного принятия решений (таких, как алгоритмы ИИ), размещать рейтинги исполнителей, предоставлять возможности дополнительного профессионального образования,
предоставлять исполнителю инструменты и материалы для исполнения заказа (например, одежда), проверять наличие у исполнителя опыта, квалификации, производить оценку рисков безопасного выполнения работ, услуг.

2. Доступ к данным

Опыт ЕС

В июле 2025 г. Суд ЕС вынес решение по делу Лизы Баллманн против Европейского Совета по защите данных (EDPB)[12]. Баллманн требовала от EDPB предоставления документов из расследования деятельности Meta[13], которая была обработчиком данных истицы в Facebook. EDPB отказал, поскольку Баллманн не была участником процесса расследования и не может требовать доступа к материалам расследования.

Однако Суд ЕС признал, чтобы иметь право на доступ к данным расследования, необязательно быть стороной процесса. Согласно ст. 77 Регламента о защите ПД[14], каждый пользователь вправе обратиться в надзорный орган с жалобой о нарушении Регламента и быть информированным о процессе рассмотрения жалобы, включая материалы расследования. Суд ЕС дал широкое толкование нормы: субъект данных имеет право на доступ к информации не только об обработке его собственных данных, но и о работе обработчика с данными в целом.

Также в июле 2025 г. Еврокомиссия утвердила правила бесплатного доступа исследователей к данным очень крупных платформ. Еще в 2022 г. в ЕС был принят Акт о цифровых услугах (DSA)[15], который возложил на такие платформы обязательства предоставлять публичный доступ исследователей к их данным по системным рискам, связанным с дизайном, архитектурой, функционированием платформ и их алгоритмическими системами[16]. Теперь в ЕС создается специальный портал по обмену перечисленными данными – исследователи смогут направлять запросы на получение конкретных данных платформ. Доступ к данным будут иметь только те организации, исследование которых не связано с коммерческими интересами, и результаты работы которых будут публично доступны. Заявки исследователей адресуются не платформам, а национальным координаторам цифровых услуг (органам, уполномоченным по имплементации DSA), которые проверяют заявки и формулируют технические требования к платформам по предоставлению доступа к запрашиваемым данным.

Опыт Италии

В июле 2025 г. завершились публичные консультации по бизнес-практике, принуждающей пользователей выбирать: либо согласиться на сбор данных с помощью трекинговых технологий («ok option») или оплатить ресурсы или сервисы («pay option»)[17]. То есть либо оставь свои данные, либо платить за использование контента, платформы – схема «consent wall».

Данная схема лишает пользователей свободы выбора: пользователь должен иметь право платить или не платить, а схема «pay or ok» принуждает платить либо деньгами, либо данными. Схема нарушает правило конкретности согласия: по действующим нормам пользователь предоставляет данные для конкретной цели

[12] European Data/Case T-183/23.
[13] Деятельность компании Meta признана экстремистской и запрещена на территории Российской Федерации.
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
[15] https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa
[16] П. 3 ст. 40 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services
[17] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10126652

их обработки, тогда как доступ к контенту является не целью обработки данных, а фактически услугой в обмен на данные. Также для пользователя может быть не ясно, кто и зачем собирает данные, как они будут использоваться и когда обработка его данных прекратится. Если по результатам консультаций практика будет признана неправомерной, государство сможет ввести запрет на применение платформами схемы «pay or ok», что ограничит незаконный доступ платформ к поведенческим данным пользователей.

Опыт США и ЕС

В июле 2025 г. США и ЕС объявили о заключении Соглашения о сотрудничестве в области торговли[18], включая устранение барьеров в цифровой торговле. Страны согласились сохранить нулевые таможенные пошлины на электронные передачи данных (например, аудиовизуального контента). Таким образом, стороны договорились не усложнять условия ведения цифровой торговли, что важно для европейских компаний на фоне ужесточения торговой политики США (повышение таможенных импортных пошлин).

Опыт России

В отличие от ЕС, в России слабо развита практика поддержки права пользователей на информацию. Так, в действующем законодательстве о персональных данных пользователь имеет право только на доступ к информации о процессе обработки его персональных данных, но не о деятельности оператора данных. Поэтому в России у пользователей нет права на доступ к информации о результатах проверки качества мер безопасности, принимаемых платформами (как в ЕС). С учетом национальных целей по развитию экономики данных в России необходимо развивать практики организации предоставления доступа исследователей к данным крупнейших платформ, в том числе через отдельный портал.

3. Ценообразование на платформах

Опыт Канады

В июле 2025 г. обсуждался документ «Алгоритмическое ценообразование и конкуренция»[19]. Алгоритмическое ценообразование – процесс использования автоматизированных алгоритмов для установления, рекомендации цен на товары, услуги, часто в режиме реального времени, на основе набора входных данных.

Данные могут быть получены от потребителей (онлайн-поведение, демографическая информация, история транзакций), а могут содержать информацию о рыночных условиях (о спросе и предложении, ценах конкурентов, уровне запасов). С развитием ИИ появилась возможность постоянного обучения алгоритмов на основе данных, особенно если данные постоянно обновляются («обучение с подкреплением»[20]). Однако процесс принятия решений такими алгоритмами часто непрозрачный и сложный для понимания (проблема «черного ящика»). Поэтому для контроля за такими алгоритмами важно вмешательство человека.

В зависимости от типа данных существуют разные типы алгоритмов:

1) алгоритмы динамического ценообразования – установление цен на основе рыночных условий (спрос, предложение, цены конкурентов и пр.). Основная цель такого алгоритма – максимизировать прибыль компании;

2) алгоритмы персонализированного (или контролирующего) ценообразования – установление цен на основе личных характеристик человека или группы лиц. Основная цель – определение готовности потребителей платить, чтобы максимизировать прибыль.

Поэтому возникает ценовая дискриминация – когда компания взимает с разных людей разные цены за один и тот же продукт или услугу в зависимости от «готовности платить». Ценовая дискриминация бывает нескольких степеней:

1) первой степени – компания устанавливает точную цену, которую потребитель готов заплатить (т.е. персонализированное ценообразование);

[18] https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-united-states-and-european-union-reach-massive-trade-deal/

[19] https://competition-bureau.canada.ca/en/how-we-foster-competition/education-and-outreach/publications/algorithmic-pricing-and-competition-discussion-paper

[20] reinforcement learning

2) второй степени – установление различных цен в зависимости от условий продажи (например, снижение цены при покупке оптом, подключении подписки);

3) третьей степени – установление разных цен для разных групп потребителей в зависимости от возраста, местоположения и других характеристик (например, понижение цен для студентов или пенсионеров).

Алгоритмическое ценообразование приводит к антиконкурентным практикам:

1) сотрудничеству между конкурентами для ценового сговора, раздела рынка и пр. Например, компании вступают в сговор по типу «ступица и спицы» (hub-and-spoke) – несколько компаний используют один и тот же алгоритм (одинаковое ПО), который обрабатывает данные, предоставляемые конкурентами, и устанавливает цены одновременно для всех конкурентов. И если между конкурентами происходит прямое взаимодействие – это явный сговор, если взаимодействие отсутствует возможен молчаливый сговор;

2) применению антиконкурентных практик с использованием алгоритмов. Например, в хищническом ценообразовании, когда доминирующая компания намеренно занижает цену ниже себестоимости, чтобы вытеснить конкурентов с рынка (фаза хищничества), и повышает цены после ухода конкурентов: компенсируя понижение цены (фаза возмещения). Компании используют алгоритм для таргетирования клиентов: выявляют клиентов, которые с наибольшей вероятностью перейдут к другому продавцу, чтобы удержать клиентов низкими ценами.

Опыт Франции

В июле 2025 г. был оштрафован маркетплейс Shein на 40 млн евро за мошенничество с ценами: рекламировались «зачёркнутые цены» (определялись как «скидка»)[21]. Однако в 57% предложений снижения цены не было, в 19% – предлагалась скидка в меньшем размере, чем было обещано, а в 11% – выявилось повышение цены. При этом Кодекс прав потребителей Франции устанавливает, что при размещении информации о снижении цен необходимо указывать минимальную цену, по которой продавался продукт в течение 30 дней, предшествующих акции. Эта цена является референтной, от которой должна рассчитываться скидка. В России аналогичного правила не существует.

Опыт России

В России использование алгоритмов для реализации антиконкурентных соглашений, в том числе для ценообразования, в частности, в рамках явного сговора, признается отягчающим обстоятельством.

4. Регулирование криптоактивов

Опыт ЕС

Европейский регулятор ESMA в июле 2025 г. выпустил Руководство для поставщиков услуг, связанных с криптоактивами (CASP), такими, как криптокошельки, криптобиржи, криптообменники и др. Руководство направлено против маркетинговых практик, которые вводят в заблуждение потребителей относительно того, регулируются ли торгуемые активы MiCA[22] или нет.

ESMA предупреждает: если платформа с лицензией CASP, выданной по регламенту MiCA на оказание услуг с криптоактивами, одновременно предлагает как регулируемые MiCA криптоактивы (например, стейблкоины), так и нерегулируемые (например, NFT[23]), это создаёт риск введения потребителей в заблуждение относительно уровня защиты каждого актива. Наличие лицензии CASP создает эффект «ореола»: потребители ошибочно полагают, что все продукты платформы надёжны и регулируются. ESMA запрещает использовать MiCA-лицензию как маркетинговый инструмент для продвижения продуктов, не подпадающих под регулирование MiCA, а также дает рекомендации CASP:

- на каждом этапе взаимодействия с потребителем – в рекламе, на сайте и в договоре, необходимо отмечать, подпадает ли конкретный продукт под регулирование MiCA, при этом нерегулируемые услуги должны обозначаться как таковые, а информация о них размещаться отдельно;
- перед подключением клиента к нерегулируемой услуге необходимо

[21] https://www.economie.gouv.fr/files/files/directions_services/dgccrf/media-document/cp-dgccrf-SHEIN-sanctionne-amende-40millions.pdf

[22] Регламент ЕС № 2023/1114 регулировании рынка криптоактивов.

[23] Невзаимозаменяемый токен.

предупреждать его об этом и получить подтверждение об ознакомлении.

В июле 2025 г. ESMA выпустила краткий отчёт экспертной оценки того, как мальтийский регулятор MFSA выдал первую лицензию CASP по MiCA[24]. ESMA отмечает, что процедура выдачи лицензии MiCA для CASP прошла слишком поспешно: не были должным образом проверены планы подключения новых клиентов, качество корпоративного управления компаний CASP, процедуры AML/CFT[25] и др. Поскольку лицензия CASP, выданная в одной стране ЕС, позволяет поставщику оказывать услуги на всей территории ЕС, важным аспектом становится единообразие и качество проверки при лицензировании, поэтому ESMA рекомендовала доработать оценку этих рисков в будущем, а также подчеркнула необходимость раскрытия клиентам информации при совместном предложении регулируемых и нерегулируемых по MiCA услуг.

Опыт США

В июле 2025 г. в США принят Закон о платёжных стейблкоинах (GENIUS Act)[26]. Акт устанавливает требования получения лицензий для эмитентов стейблкоинов, требования к резервному обеспечению стейблкоинов (например, за счет фиатных валют) и регулярной отчётности перед регулятором о составе этих резервов, а также соблюдение AML/KYC. Акт также запрещает начислять проценты держателям стейблкоинов и использовать маркетинговые заявления, создающие впечатление государственной гарантии. Ключевые положения GENIUS Act анализировались в майском Мониторинге № 5 (17), в июле закон вступил в силу на федеральном уровне.

Опыт России

В июле 2025 г. в Госдуму внесен законопроект о штрафах за расчёты в криптовалюте[27] с 2026 г. до 200 000 руб. для физлиц и до 1 млн руб. для юрлиц, а использованная криптовалюта будет конфисковываться. Глава думского комитета назвал крипторасчёты «серой зоной» и уточнил, что законопроект закрепляет статус рубля как единственного законного платежного средства.

Сейчас Закон «О цифровых финансовых активах» № 259-ФЗ[28] запрещает использование цифровых валют как средства расчетов, но санкции за это не предусмотрены. Однако с сентября 2024 г. Банк России получил право запускать экспериментальный правовой режим (ЭПР), в рамках которого разрешались внешнеторговые расчёты в цифровой валюте[29].

Напомним, что в России токены, подпадающие под MiCA (ART/EMT[30]), могут быть квалифицированы как цифровые финансовые активы (ЦФА) в соответствии с 259-ФЗ[31]. К рекламе ЦФА российский закон, как и разъяснение ESMA, предъявляет требования: указывать эмитента и сайт с решением о выпуске, включать предупреждение о рисках/возможной потере средств, запрет обещания доходности и прогнозы роста цены, а также размещение рекламы до публикации решения о выпуске ЦФА. Регулирования стейблкоинов в России на данный момент не предусмотрено.

5. Ответственное использование ИИ

Опыт Великобритании

В июле 2025 г. опубликован доклад о практиках противодействия дипфейкам[32], включая методы маркировки контента, чтобы пользователи распознавали и помечали дипфейки: невидимые водяные знаки[33], метаданные происхождения файла, пометки на контенте («сделано с помощью ИИ») и пр.

Платформы должны использовать водяные знаки и метаданные для приоритизации модерации, а не перекладывать распознавание на

[24] https://www.esma.europa.eu/sites/default/files/2025-07/ESMA42-2004696504-8164_Fast-track_peer_review_on_a_CASP_authorisation_and_supervision_in_Malta.pdf
[25] Противодействие отмыванию денег/борьба с финансированием терроризма.
[26] https://www.congress.gov/bill/119th-congress/senate-bill/1582?q=%7B%22search%22%3A%22GENIUS+Act%22%7D&s=9&r=1
[27] https://iz.ru/1922846/taibat-agasieva-anton-belyj/postavit-na-bit-s-2026-goda-rossiyan-nachnut-shtrafovat-za-oplatu-kriptoj
[28] https://www.consultant.ru/document/cons_doc_LAW_358753/
[29] https://www.garant.ru/hotlaw/federal/1746698
[30] Токены, привязанные к активам/Токены электронных денег.
[31] https://www.consultant.ru/document/cons_doc_LAW_358753/
[32] https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/deepfake-defences-2/deepfake-defences-2---the-attribution-toolkit.pdf?v=399908&__cf_chl_tk=_NpxVdIesx1t_BvJLNhgja0MEbGCtbbw.MA8VxcJEjk-1754490847-1.0.1.1-KvTusrBRDmHDEap6ht4r1YLweNiu9q2rVBfoKo3X5gM
[33] Распознаваемые программами сигналы в изображении/аудио, которые показывают, что контент сделан с помощью ИИ.

аудиторию. Рекомендуется явным образом устанавливать различия между полностью и частично сгенерированным контентом, когда ИИ лишь редактировал оригинальный контент (накладывал фильтры, менял элементы в изображении и т.д.).

Опыт ЕС

В июле 2025 г. Еврокомиссия опубликовала Кодекс практик для ИИ общего назначения[34]. Кодекс предполагает:

1) прозрачность. Кодекс содержит «модельную документацию» - универсальную форму отчетности, по которой компании могут раскрывать информацию об ИИ: что система делает, на чем обучалась, сколько ресурсов тратит;

2) безопасность и системные риски (для моделей с системным риском[35]). Нести ответственность может менеджмент компании, команды, которые разрабатывают, обслуживают ИИ, аудиторы. «Перекладывать» ответственность на пользователя не предлагается;

3) защиту интеллектуальных прав. Например, рекомендуется внедрять правила для «краулинга» – автоматического сбора данных для обучения. Данные в этом процессе должны собираться только на законной основе. Системы ИИ общего назначения должны распознавать запреты на использование контента для обучения.

Компания Meta[36] отказалась присоединяться. При этом OpenAI, Amazon, Google, IBM и др. (более 25 компаний) заявили о присоединении к Кодексу.[37]

Опыт США

В июле 2025 г. опубликован «План Америки по ИИ»[38]. План закрепляет меры:

1) поддержки стартапов, разрабатывающих открытые модели ИИ[39] и моделей с открытыми «весами»[40]. Создаётся Национальный ресурс исследований в области ИИ, чтобы дать стартапам доступ к вычислительным мощностям, моделям и данным без дорогих контрактов с частными компаниями;

2) борьбы с дипфейками в судебной системе. Ложные ролики, созданные ИИ, могут попасть в суд как поддельные улики и лишить людей права на правосудие. Поэтому предлагается разработать обязательные стандарты распознавания дипфейков в судах;

3) государственные тесты иностранных моделей на «пропаганду и закладки». Минторг будет проверять зарубежные модели ИИ на наличие цензуры, возможностей тайно передавать данные или управлять системой ИИ без ведома пользователя и угрозы критической инфраструктуре. На данный момент США является единственной страной, где планируется внедрить такие правила.

Опыт России

В июле 2025 г. Банк России опубликовал Кодекс этики ИИ на финансовом рынке[41].

Кодекс выделяет 5 ориентиров: человекоцентричность, справедливость, прозрачность, безопасность и ответственное управление рисками. Например, клиенту должны дать право отказаться от общения с ботом и потребовать пересмотр человеком решений, принятых ИИ (например, в случае отказа в кредите). При оценке клиентов ИИ не вправе учитывать национальность или вероисповедание – наборы данных должны проверяться на такие «перекосы». Компании обязаны будут помечать, что рекомендации роботов-советников сгенерированы ИИ. Меры, предусмотренные Кодексом, должны будут сделать работу ИИ более прозрачной и понятной для клиентов банков и повысить доверие общества к технологии ИИ в целом.

---

[34] ИИ общего назначения - это ИИ-модель, которую учат не под одну функцию, а на очень разнородных данных, чтобы она выучила общие закономерности языка/изображений/звука и умела решать множество задач без отдельной перепрошивки: отвечать на вопросы, писать тексты и код, переводить, резюмировать, разбирать картинки и пр. Важное отличие: это не готовое приложение, а компонент - как универсальный мотор, который можно запустить «как есть» через подсказки («промпты») или приспособить под отрасль с помощью донастройки.

[35] «Модель с системным риском» - модель общего назначения, чьи высокие возможности потенциально могут причинять масштабный вред из-за охвата или по предсказуемым негативным эффектам для здоровья, безопасности, прав частных лиц и для общества в целом.

[36] Признана экстремистской организацией в России.

[37] https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai

[38] https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

[39] Открытые модели - это модели ИИ, у которых публично доступны все ключевые компоненты (исходный код, архитектура, обучающие скрипты и т.д.). Такие модели могут свободно использоваться, изменяться и распространяться всеми желающими (иногда с минимальными условиями, например, указать авторов).

[40] «Веса» - это числовые параметры модели ИИ, которые она «выучивает» во время обучения. Модели с открытыми весами - это модели ИИ, у которых можно свободно скачать и запускать веса, но не обязательно открыт весь остальной «набор»: данные обучения, точные рецепты, часть кода или инструменты могут быть закрыты.

[41] https://www.consultant.ru/document/cons_doc_LAW_509514/