

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

- ЦФА сбрасывают оковы
- Большие модели, большие счета: ИИ и экология
- Опасные связи: регулирование антропоморфных чат-ботов

Мониторинг №12 (24) (Декабрь 2025)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик 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., науч. сотр. Фонда Экономической политики Голованова Д.А.

При частичном или полном использовании материалов ссылка на источник обязательна



ЦФА сбрасывают оковы

Как Банк России спустя 5 лет меняет свое отношение к криптомиру

Авторы: Диана Голованова,
Иван Ермохин

Спустя 5 лет после принятия закона о цифровых финансовых активах (ЦФА) кажется, что в 2026 г. институт цифровых прав и цифровых валют в России ждут большие изменения. В последнюю неделю прошлого года Банк России [выступил](#) с заявлением о том, что регулятор подготовил Концепцию по регулированию криптовалют на российском рынке. Самого текста Концепции в публичном доступе нет, но есть описание документа, которое приводит ЦБ РФ на своем сайте.

В основном документ посвящен вопросу урегулирования деятельности криптобирж в России. Этот вопрос ждал своего решения с момента начала дискуссии о рынке криptoактивов, т.е. с 2017 г. В частности, предполагается, что торговля криптовалютой будет осуществляться через существующую инфраструктуру – брокеров и биржи. В документе не сказано, смогут ли другие участники рынка, не имеющие лицензии брокера или биржи, оказывать услуги, получив иную специальную лицензию. Напомним, что большинство крупнейших криптобирж в мире сегодня были созданы новыми компаниями на рынке, а не существовавшими финансовыми организациями. Ограничение же новых компаний может привести к сокращению инноваций и снижению

возможности выхода российских криптобирж на международные рынки. В документе также предлагается ограничить покупку криптовалют неквалифицированным инвесторам: 300 тыс. руб. в год на одной площадке. Но с учетом того, что пользователь из РФ может купить криптовалюту на иную сумму на других зарубежных площадках, запрет не снизит инвестиционные риски граждан, однако, возможно, ограничит приток денежных средств на российские криптобиржи.

Что же касается ЦФА, а также утилитарных и гибридных цифровых прав, то для них Банк России подготовил «тихую революцию»: их оборот будет разрешен в открытых сетях. Что это значит для компаний и инвесторов? Это, например, возможность выпустить российской компании ЦФА облигацию не на российских площадках – организаторах выпуска и обмена, где покупателями выступают исключительно российские пользователи, а, в частности, в сети Ethereum. В дальнейшем такие ЦФА могут быть открыты для покупки на крупнейших криптобиржах, а также в DeFi-протоколах. По сути, российские компании вновь, после введения санкционных ограничений, получат доступ к международной ликвидности, обращаемой в криптовалютах, а значит, смогут привлечь финансирование на более выгодных условиях, чем внутри страны. В связи с этим нововведением возникает вопрос: будет ли у российской компании возможность принять оплату за ЦФА, например, в Bitcoin и выплатить купонный доход в криптовалюте?

↑ **в 1,6 раза**

выросло количество размещений ЦФА за 9 месяцев 2025 г. и достигло 972 млрд руб.

Развитие регулирования ЦФА и появление новых правовых конструкций с участием цифровых прав – тренд второй половины 2025 г.

В декабре был [подписан](#) закон, который ввел регулирование для долговых ЦФА (по сути – облигации). В том же месяце был предложен еще один законопроект, который разрешит инвестиционным фондам покупать ЦФА на тех же условиях, что и обычные акции или облигации. Ранее фонды практически не могли этого делать, потому что не существовало удобной системы учета таких активов.

И в этом же месяце был сделан еще один шаг для развития рынка ЦФА: в Госдуму был внесен [законопроект](#), разрешающий использовать недвижимость в качестве залога по обязательствам, оформленным в виде ЦФА. Проще говоря, если долг

оформлен в виде ЦФА, его можно будет обеспечить недвижимостью (например, квартирой, домом или земельным участком). Законопроект также устанавливает порядок регистрации такого обеспечения в Росреестре: будет указываться, какая недвижимость обеспечивает конкретный выпуск ЦФА, а его владельцы будут признаваться получателями залога. Для этого вводятся следующие правила:

- каждому выпуску ЦФА будет присваиваться уникальный номер;
- этот номер будет указываться при регистрации обеспечения в Росреестре;
- покупать и продавать такие ЦФА можно будет только после официальной регистрации обеспечения в виде недвижимости.

А что дальше?

Банк России планирует представить проект озвученных поправок уже летом 2026 г., их принятие активизирует развитие ЦФА в России, потенциально мы увидим использование ЦФА для привлечения международных инвестиций и расчетов по ВЭД. Это возможно в том числе благодаря автоматизации проведения сделок с использованием смарт-контрактов, что снизит санкционные и иные регуляторные риски сторон.

Что же касается будущего расчетов в цифровых валютах, то тут изменений не предвидится: рассчитываться внутри и вовне в Bitcoin будет также нельзя.

ВЧЕРА

2020

принят Закон о ЦФА

СЕГОДНЯ

2025

предложены поправки в Закон о ЦФА

ЗАВТРА

Оборот ЦФА только на платформах РФ, низкий спрос на инструмент

Растет спрос на долговые ЦФА, возможность привлечь капитал на внешних рынках

ЦФА – ключевой инструмент привлечения капитала в РФ

Большие модели, большие счета

Сегодня дата-центры в мире потребляют до 1,5% электроэнергии, а к 2030 г. потребление удвоится.

Французское антимонопольное ведомство выпустило Отчет о проблемах конкуренции, связанных с воздействием ИИ на энергетику и экологию. По данным МЭА, если обычный дата-центр имеет мощность 10–25 МВт, то дата-центр, ориентированный на ИИ – более 100 МВт. Это сопоставимо с годовым потреблением электроэнергии 100 тыс. домохозяйств.

Очевидно, что ИИ оказывает влияние на окружающую среду. Энергия для дата-центров часто производится из ископаемого топлива. Хотя наблюдается тренд на инвестиции в декарбонизированные источники энергии, как ВИЭ, атомная энергетика, особенно в районах с высокой нагрузкой на электросети. Так, корпорация Microsoft в 2024 г. договорилась с компанией Brookfield о поставке 10,5 ГВт «зеленой» мощности в США и Европе. Технологические гиганты Amazon, Google и Oracle заявили о внедрении малых модульных реакторов.

Закон об ИИ ЕС (Регламент 2024/1689) уже ставит задачу разработки кодексов поведения в части минимизации воздействия систем ИИ на окружающую среду.

Если говорить о конкуренции, Французское антимонопольное ведомство выделяет 3 проблемы.

↑ 91%

потребления воды возникает на этапе обучения и инференса ИИ

Как регуляторы учатся считать «цену» ИИ в киловаттах и CO₂

Автор: Мария Гирич

Первая – трудности доступа к электросетям, неопределенность цен на энергию (затраты на энергию – это 30–50% операционных затрат дата-центра).

В связи с ростом дата-центров увеличилось количество заявок на технологическое присоединение к электросети с высокой мощностью. Усилился риск перегрузки сети в местах концентрации спроса: дата-центры часто организуются в виде кластеров с резервированием (т.е. установка нескольких технических ресурсов, предназначенных для замены друг друга в случае сбоя). Также есть риск «перехвата» выгодных площадок крупными игроками в ущерб мелким.

Во Франции, в частности, был принят ряд мер. Например, введена ускоренная процедура подключения энергоемких промышленных потребителей (0,4–1 ГВт). Государство заранее выбирает несколько зон, где возможно подключение гигантов, и держит там мощность под потенциальные проекты, чтобы потом инвестор мог зайти и быстро подключиться к электроэнергии. Также есть проблема наличия у некоторых энергопотребителей «хищнических» стратегий. Например, резервируется в сети огромная мощность, чтобы эту мощность не получили конкуренты, но фактически она не используется, что создает искусственный дефицит. В связи с этим введено правило: нельзя бронировать мощность без подтверждения прав на использование земли, на которой планируется размещение проекта. А если запрошенная мощность не используется, ее могут уменьшить. Обсуждается идея «динамического» распределения мощности: мощность резервируется не за тем, кто первым

подал заявку, а за тем, кто быстрее строит и вводит объект.

Вторая проблема связана с возникновением концепции «фругального ИИ» – приоритетное развитие решений, которые минимизируют материальные и энергетические затраты, экологический след для оценки «нужности» использования ИИ (т.е. ИИ-решение применяют только когда без него нельзя), и которые по всей цепочке (разработка, внедрение, использование) оптимизированы так, чтобы минимизировать ресурсы. Фактически стал вопрос разработки более мелких моделей ИИ, которые помогают «экономить» вычисления. Например, помогает open-source: если модель уже обучена, ее можно переиспользовать, экономя ресурсы, а не каждый раз обучать с нуля.

В связи с этим государство и компании начинают внедрять «зеленые» параметры в закупки и тендеры. Это создает риски, что компании могут завышать

экологические преимущества своих ИИ-решений и дата-центров из-за отсутствия научно-корректных методик расчета, получая незаслуженное преимущество в закупках. Также крупные операторы могут отказываться раскрывать данные об экологическом следе и фругальности, снижая прозрачность.

Третья проблема – необходимость развития единых методик оценки экологического воздействия ИИ. Сейчас существует много различных методик, которые не всегда достаточно научно обоснованы. Либо же стандарт может быть разработан крупными игроками, которые лоббируют собственные интересы, не предлагая экологических улучшений.

В России Минцифры [прогнозирует](#) рост энергопотребления российских центров обработки данных (ЦОД) в 2,5 раза к 2030 г., что также может стимулировать удорожание электроэнергии в условиях энергодефицита в России.

А что дальше?

В условиях роста спроса на энергию регулирование будет двигаться в сторону «энергетического допуска» для ИИ и ЦОД (а также и для других сфер, таких как майнинг) в России и за рубежом, особенно в регионах с энергодефицитом. Страны будут стимулировать переход на атомную, а также на низкоуглеродную энергию. Параллельно можно ожидать введение обязательной отчетности компаний и разработки методик сопоставимости данных по ресурсоэффективности. В то же время возможен рост долгосрочных контрактов на энергию, что будет создавать антимонопольные риски, например, из-за дискриминации и закрытия доступа к энергосетям для более мелких поставщиков ЦОД, услуг ИИ и пр.

ВЧЕРА

2024

принят Закон ЕС об ИИ

Идея развития экологических стандартов для ИИ

СЕГОДНЯ

2025

Франция ввела требования, направленные на снижение захвата энергосетей крупными поставщиками ИИ

Обсуждаются правила экологических стандартов ИИ для снижения рисков для конкуренции

ЗАВТРА

Введение зеленых закупок ИИ, экологической отчетности для поставщиков ИИ как фактора конкурентного преимущества

Опасные связи

Как страны стремятся урегулировать вопросы безопасности антропоморфных чат-ботов

Автор: Кирилл Черновол

Регуляторы стран обращают все больше внимания на «человекоподобные» чат-боты. Это вид генеративного ИИ, задача которого – имитировать человеческое общение для разных целей. При неумелом обращении они могут навредить, и виновными принято считать разработчиков. Регуляторы стремятся к тому, чтобы в чат-боты были встроены меры, способные обезопасить пользователей.

9 декабря 2025 г. генпрокуроры штатов США [направили письмо](#) 13 компаниям, разрабатывающим чат-боты на базе генеративного ИИ – OpenAI, Google, Meta, xAI и др. Прокуроры выделяют две проблемы.

Первая – «стремление угодить»: бот чрезмерно соглашается, подтверждает тревоги и ошибочные убеждения пользователя и может подталкивать к опасным решениям. Дообучение на оценках людей и быстрые кнопки «нравится/не нравится» усиливают этот эффект.

Вторая – вводящие в заблуждение ответы, включая моменты, когда бот пишет так, будто он живой человек. Особый акцент делается на взаимодействиях чат-ботов с детьми: упоминаются сексуализированные «романтические» диалоги, просьбы скрывать переписку от родителей, подталкивание к приему наркотиков, причинению вреда самим себе и пр. Около 72% подростков США хотя бы раз общались с чат-ботом.

В США уже есть ряд исков против компаний-разработчиков ИИ по делам о нарушении прав несовершеннолетних, причинению

вреда психическому здоровью пользователей – причем, как минимум, 7 дел с 2020 г.¹ Например, в деле Garcia v. Character Technologies Inc. истница заявляла, что разработчики платформы не приняли «достаточных мер» по предупреждению непоправимых для ее 14-летнего сына последствий. После спора компании внедрили автоматическое прекращение чата при поднятии определенных тем.

Чат-боты могут давать и медицинские советы или советы в области психологии, что нарушает законодательства о необходимости наличия советующих лицензий для предоставления таких советов.

Компании просят повысить меры безопасности их продуктов, таких как тестирование безопасности до запуска; постоянные предупреждения на экране ввода; отключение чат-бота, если опасные ответы не удается остановить; независимые аудиты и оценки воздействия на детей; публичный журнал инцидентов и целевой срок реакции (например, до 24 часов для самых опасных случаев); возрастная настройка диалогов и протокол, когда сообщать о случаях угроз насилия, употребления наркотиков и самоповреждений специалистам, полиции и родителям и пр. Фактическое обеспечение безопасности пользователей возлагается преимущественно на разработчиков чат-ботов.

Китай пошел по пути более строгого регулирования. В декабре 2025 г. представлен проект [Временных мер регулирования человекоподобных ИИ-сервисов](#). Устанавливаются запреты

¹ Дела ES v. Character Technologies, Inc., PJ v. Character Technologies, Inc., Montoya v. Character Technologies, Inc., Garcia v.

практик, которые чаще всего приводят к вреду: нельзя поощрять самоубийство и самоповреждение, использовать манипуляции, вводить пользователя в заблуждение и т.д. Провайдер должен выдавать сообщения с призывом обратиться за помощью, а при заявлениях о намерении причинить себе вред – подключать человека и связываться с родителями, законными представителями.

Для несовершеннолетних вводится также специальный режим использования ИИ, а если функция чат-бота – предоставлять «эмоциональное сопровождение», то ребенок может им пользоваться только с явно выраженного согласия опекуна. То есть обязанности по безопасности уязвимых пользователей (детей) в подходе Китая лягут и на провайдеров, и на законных представителей ребенка. Тем самым устраняется риск того, что провайдеру будут предъявлять претензии по логике «ребенок пострадал – значит,

провайдер не обеспечил безопасность».

Сам тренд на защиту уязвимых групп пользователей задала еще ОЭСР в Рекомендациях по ИИ 2019 г. В Законе ЕС об ИИ 2024 г. содержатся повышенные требования к безопасности систем генеративного ИИ, а в 2025 г. в ЕС опубликовано руководство по защите данных в системах генеративного ИИ. Нынешние инициативы – это продолжение и детализация глобального тренда, направленного на более тонкую защиту пользователей, взаимодействующих с генеративным ИИ.

В России регулирование таких систем пока что сводится к отраслевым рекомендациям по этике ИИ. В декабре 2025 г. Правительство [поручило](#) Минцифры разработать предложения по регулированию ИИ, которые могут охватывать и требования безопасности человекоподобных чат-ботов, результаты будут известны в марте 2026 г.

А что дальше?

Тренд на специальные требования к обеспечению безопасности чат-ботов в ближайшие годы будет распространяться по странам на фоне роста масштабов применения: [Gartner прогнозирует](#), что к 2029 г. до 80 % повседневных коммуникаций с ИИ будет осуществляться через человекоподобные системы-агенты. Ключевым здесь будет вопрос распределения ответственности. Скорее всего, большинство стран изберут путь установления закрытого списка мер безопасности, управления рисками и требований к раскрытию информации. Общая логика будет одна: в работе чат-ботов не должно допускаться поведение, которое считалось бы противоправным, если бы так себя вел в переписке человек.

ВЧЕРА

2024

Закон ЕС об ИИ

СЕГОДНЯ

2025

Письмо от прокуроров разработчикам чат-ботов

США

Проект регулирования чат-ботов в Китае

ЗАВТРА

Впервые сформированы нормы о безопасности генеративного ИИ и защите уязвимых пользователей

Регулирование систем генеративного ИИ становится тоньше, появляются специфические требования к чат-ботам, имитирующими человеческое общение

Более строгое регулирование производителей и провайдеров чат-ботов, особенно в вопросах защиты детей

Новости **декабря 2025 г.**, которые показались нам интересными.¹

- Международный финансовый центр Дубая (DIFC) объявил о внедрении специальных инструментов для рассмотрения споров, связанных с криptoактивами: введен механизм временного судебного хранения криptoактивов, а также суды получили возможность использовать сервисы для отслеживания движения криptoактивов.
- Компании, связанные с криптовалютами (например, Circle и Ripple), начали получать предварительные согласования на получение банковских лицензий. Это позволит им подключаться к платежной инфраструктуре США.
- Управление по страхованию Гонконга представило проект правил, разрешающий страховым компаниям инвестировать собственный капитал в криptoактивы.
- В Нью-Йорке (США) продолжился тренд на усиление контроля со стороны правительства за безопасностью выпускаемых моделей ИИ для защиты потребителей – принят Закон об ответственном подходе к безопасности ИИ (RAISE ACT). Разработчики при выводе на рынок штата наиболее мощных передовых моделей ИИ должны публиковать протоколы безопасности. Разработчик должен сообщать генеральному прокурору штата обо всех инцидентах безопасности с ИИ в срок не позднее 72 часов.



¹ С 2025 г. Институт Гайдара разрабатывает цифровую платформу анализа новостей в России и в мире по тематике регулирования цифровой экономики – DigiReg. Представленные новости отобраны экспертами в том числе на основе анализа данных платформы.