Observatoire ARGA

ARGA Atlas

РЕГЛАМЕНТ MICA, ЗЛОУПОТРЕБЛЕНИЯ НА РЫНКЕ И РАСКРЫТИЕ ИНФОРМАЦИИ: ПОЧЕМУ РЕГУЛИРОВАНИЕ КРИПТОВАЛЮТНОГО РЫНКА СТАНОВИТСЯ ВОПРОСОМ ПРАВОВОЙ ЗАЩИТЫ

Авторы:

Сергей Храбрых — президент ARGA, PhD,

Наталия Цмакалова

Организация: Observatoire ARGA, ARGA Atlas

Адрес для корреспонденции: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

Контакты: info@argaobservatory.org, +33 7 58 49 62 27

Сайт: www.argaobservatory.org, https://www.arga-atlas.com/

Англет, 6 мая 2026

Цель документа

Настоящий доклад подготовлен с целью комплексного анализа того, каким образом регулирование рынка криптоактивов, требования к раскрытию информации и правила противодействия злоупотреблениям на рынке становятся не только вопросом финансового надзора, но и самостоятельным направлением правовой защиты. Особое внимание уделяется Регламенту Европейского союза 2023/1114 о рынках криптоактивов, известному как MiCA, а также тем правовым рискам, которые возникают для эмитентов, поставщиков услуг, инвесторов, владельцев токенов и лиц, вовлечённых в трансграничные споры.

Практическая задача документа состоит в выявлении ситуаций, в которых требования к раскрытию информации, правила допуска криптоактивов к обращению, надзор за поставщиками услуг, оценка рыночного поведения, предупреждение манипулирования рынком и использование цифровых данных могут приводить к серьёзным юридическим последствиям. Эти последствия могут выражаться в отказе в листинге, ограничении доступа к платформам, блокировке операций, расследованиях со стороны регуляторов, гражданско-правовой ответственности, уголовно-правовых рисках и репутационном ущербе.

Для ARGA данная тема имеет стратегическое значение, поскольку криптоактивы всё чаще становятся частью международных имущественных структур, инвестиционных проектов, корпоративных конфликтов, санкционных проверок, уголовных дел и процедур финансового мониторинга. Ошибочная или формальная оценка цифровых доказательств, технических отчётов, данных блокчейна, раскрытия информации или рыночного поведения может привести к неправомерным ограничениям, финансовым потерям и нарушению права на эффективную защиту.

Настоящий доклад рассматривает регулирование крипторынка как часть более широкой системы защиты прав инвесторов, владельцев активов, предпринимателей и участников трансграничных правовых отношений. Его задача состоит в формировании практической модели анализа, пригодной для адвокатов, регуляторов, судов, комплаенс-подразделений, эмитентов, поставщиков услуг и международных правозащитных механизмов.

ОГЛАВЛЕНИЕ

Executive Summary

Регулирование криптоактивов постепенно переходит из стадии общего надзорного эксперимента в стадию полноценной правовой инфраструктуры. Регламент MiCA формирует единую европейскую рамку для эмитентов криптоактивов, эмитентов токенов, привязанных к активам, эмитентов токенов электронных денег и поставщиков услуг в сфере криптоактивов. Он устанавливает требования к авторизации, раскрытию информации, корпоративному управлению, защите клиентов, предотвращению злоупотреблений на рынке и взаимодействию с компетентными органами. Европейское управление по ценным бумагам и рынкам указывает, что MiCA предусматривает, в том числе, центральные реестры документов о криптоактивах, авторизованных поставщиков услуг и несоответствующих субъектов, а Европейское банковское управление развивает технические стандарты для токенов, привязанных к активам, и токенов электронных денег. (ESMA)

Однако расширение регулирования создаёт не только защитные возможности, но и новые правовые риски. Чем более формализованным становится рынок, тем выше значение документов о раскрытии информации, технических отчётов, сведений о резервах, описания бизнес-модели, структуры управления, маркетинговых сообщений, данных о транзакциях и аналитики блокчейна. Ошибка, неполнота, противоречие или односторонняя интерпретация таких данных могут стать основанием для регуляторного вмешательства, ограничения деятельности, отказа в доступе к рынку или претензий со стороны инвесторов.

Особое значение имеет блок правил о предотвращении и запрете злоупотреблений на рынке криптоактивов. В структуре MiCA этому посвящен отдельный раздел, направленный на обеспечение честности и целостности рынков криптоактивов. Европейское управление по ценным бумагам и рынкам подчёркивает, что правила о предотвращении и выявлении злоупотреблений на рынке должны способствовать доверию к рынкам криптоактивов и их целостности. (ESMA)

Центральный вывод настоящего доклада состоит в том, что регулирование криптоактивов нельзя рассматривать только как техническую или финансовую область. Оно непосредственно связано с правом на защиту, правом собственности, справедливой процедурой, достоверностью доказательств, пределами регуляторного усмотрения и риском формального принятия цифровых данных без достаточной проверки. В условиях, когда технические сведения могут стать основанием для серьёзных юридических последствий, качество анализа, раскрытия информации и судебной оценки приобретает принципиальное значение.

Context & Problem Statement / Почему эта тема имеет правовое и международное значение

Регламент MiCA является первым комплексным наднациональным актом, формирующим единую правовую основу для обращения криптоактивов на территории Европейского союза. Его значение выходит далеко за пределы технического регулирования цифрового рынка. На практике MiCA создает новую институциональную среду, в которой вопросы допуска криптоактивов к обращению, раскрытия информации, маркетинговых сообщений, управления резервами, корпоративного контроля и предотвращения злоупотреблений на рынке приобретают непосредственное правовое значение.

До принятия MiCA рынок криптоактивов развивался в условиях фрагментарного регулирования. Требования к эмитентам, поставщикам услуг и торговым платформам различались в зависимости от юрисдикции, что создавало значительную правовую неопределённость. Одни участники рынка действовали в рамках сравнительно строгого надзора, другие фактически опирались лишь на общие нормы гражданского, корпоративного

и финансового права. Отсутствие единой системы затрудняло как защиту инвесторов, так и оценку ответственности участников рынка.

С введением MiCA формируется более структурированная система, в которой ключевое значение приобретают документы о криптоактивах, обязательные раскрытия, процедуры авторизации, стандарты корпоративного управления, требования к хранению активов клиентов, правила обработки жалоб и механизмы внутреннего контроля. Юридическое значение получают не только финансовые показатели, но и технические описания, маркетинговые заявления, данные блокчейна и алгоритмические характеристики отдельных проектов.

Особую важность представляет регулирование злоупотреблений на рынке. Манипулирование ценами, распространение вводящей в заблуждение информации, использование инсайдерских сведений и искусственное создание рыночной активности рассматриваются как действия, способные подрывать доверие к рынку и нарушать права инвесторов. При этом оценка таких действий может основываться на анализе больших массивов цифровых данных, торговых паттернов и блокчейн-транзакций.

Значение данной темы выходит за рамки финансового надзора. Решения регуляторов, платформ и участников рынка могут затрагивать имущественные интересы, доступ к капиталу, корпоративные структуры, деловую репутацию и возможность продолжать предпринимательскую деятельность. Ошибочная квалификация рыночного поведения, неполная интерпретация технической информации или формальное отношение к цифровым доказательствам способны повлечь значительные юридические последствия.

Для ARGA данная тема имеет стратегическое значение, поскольку регулирование криптоактивов всё чаще пересекается с трансграничными спорами, санкционными ограничениями, процедурами финансового мониторинга, корпоративными конфликтами и вопросами защиты собственности. В таких ситуациях эффективная правовая защита требует понимания не только технологий, но и сложной системы регуляторных, процессуальных и правозащитных механизмов.

Legal Framework / Нормативная и институциональная рамка

Нормативная база, регулирующая обращение криптоактивов и деятельность участников соответствующего рынка, представляет собой многоуровневую систему, включающую наднациональные акты Европейского союза, национальное законодательство государств-членов, международные стандарты финансового регулирования, правила защиты инвесторов и внутренние процедуры частных организаций.

Первый уровень составляет Регламент (ЕС) 2023/1114 о рынках криптоактивов (MiCA). Этот акт устанавливает единые требования к эмитентам криптоактивов, эмитентам токенов, привязанных к активам, эмитентам токенов электронных денег и поставщикам услуг в сфере криптоактивов. Регламент регулирует порядок выпуска и публичного предложения токенов, раскрытие информации, корпоративное управление, требования к резервам, защиту средств клиентов, обработку жалоб, а также полномочия национальных и европейских органов надзора.

Второй уровень образуют сопутствующие нормативные акты Европейского союза, включая Регламент (ЕС) 2023/1113 об информации, сопровождающей переводы денежных средств и отдельных криптоактивов, правила противодействия легализации преступных доходов, акты о санкционном контроле, нормы о защите персональных данных и положения о цифровой операционной устойчивости финансового сектора.

Третий уровень включает законодательство государств-членов Европейского союза, регулирующее административную, гражданско-правовую и уголовную ответственность, порядок лицензирования, судебного обжалования и исполнения решений компетентных органов.

Четвёртый уровень составляют стандарты и технические рекомендации Европейского управления по ценным бумагам и рынкам (ESMA) и Европейского банковского управления (EBA). Эти органы разрабатывают технические стандарты, методические документы и надзорные подходы, определяющие практическое применение положений MiCA.

Пятый уровень образуют международные стандарты, прежде всего рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (FATF), регулирующие идентификацию клиентов, оценку рисков, раскрытие информации о переводах и применение риск-ориентированного подхода к виртуальным активам.

Шестой уровень включает нормы, регулирующие предотвращение злоупотреблений на рынке. В их число входят правила, касающиеся использования инсайдерской информации, манипулирования рынком, распространения ложных или вводящих в заблуждение сведений и иных действий, способных повлиять на формирование цены и инвестиционные решения участников рынка.

Седьмой уровень составляют договорные документы и внутренние процедуры частных субъектов: криптовалютных бирж, кастодиальных сервисов, торговых платформ, эмитентов токенов и поставщиков аналитических услуг. Именно эти документы определяют порядок листинга, ограничения доступа, раскрытия информации, проведения проверок и взаимодействия с клиентами.

Восьмой уровень связан с судебной и административной практикой. Национальные суды, регуляторы, арбитражные органы и международные правозащитные институты формируют подходы к оценке достоверности раскрываемой информации, достаточности доказательств, соразмерности ограничений и соблюдению процессуальных гарантий.

Таким образом, регулирование криптоактивов представляет собой интегрированную систему, в которой технические характеристики токенов, корпоративные процедуры, надзорные требования и правозащитные стандарты взаимосвязаны. Любое существенное действие на рынке криптоактивов одновременно имеет технологическое, финансовое и юридическое измерение.

Mechanisms of Practice / Abuse / Ключевые механизмы практики, злоупотребления или конфликта

Первый ключевой механизм связан с раскрытием информации при выпуске, публичном предложении или допуске криптоактива к обращению. В условиях регулирования MiCA документ о криптоактиве становится не вспомогательным описанием проекта, а юридически значимым источником сведений для инвесторов, платформ, регуляторов и иных участников рынка. Если такой документ содержит неполные, неточные, вводящие в заблуждение или чрезмерно общие сведения, это может создать основания для надзорного реагирования, гражданско-правовых требований и ограничения доступа к рынку.

Второй механизм состоит в использовании маркетинговых сообщений как элемента правового риска. Информационные материалы, публичные заявления, рекламные кампании, презентации, публикации в социальных сетях и сообщения для инвесторов могут оцениваться не только как коммерческое продвижение, но и как сведения, влияющие на ожидания

участников рынка. Несоответствие между маркетинговыми заявлениями и реальной структурой проекта может рассматриваться как вводящее в заблуждение раскрытие информации.

Третий механизм связан с оценкой технических данных. В делах о криптоактивах существенное значение имеют смарт-контракты, данные блокчейна, структура владения токенами, движение средств, торговые паттерны, сведения о ликвидности, объёмах торгов и поведении связанных адресов. Эти данные могут использоваться для выявления манипулирования рынком, инсайдерской торговли, искусственного формирования цены или сокрытия реальной структуры контроля. При этом технические данные требуют квалифицированного анализа и не должны восприниматься как самоочевидное доказательство без проверки методологии.

Четвёртый механизм заключается в квалификации действий как злоупотребления на рынке. В сфере криптоактивов манипулирование может выражаться в искусственном увеличении объёмов торгов, согласованных операциях между связанными адресами, распространении недостоверной информации, создании ложного впечатления спроса, использовании инсайдерских сведений, координированных действиях группы лиц или управлении ликвидностью таким образом, который вводит рынок в заблуждение.

Пятый механизм связан с решениями торговых платформ. Платформа может отказать в листинге, приостановить торги, ограничить операции, удалить токен из обращения, запросить дополнительные документы или уведомить регулятора о подозрительном поведении. Такие решения могут быть основаны на внутренних правилах платформы, требованиях MiCA, оценке риска, жалобах пользователей или данных аналитических систем. Для эмитента или держателя токенов подобное решение может иметь значительные финансовые и репутационные последствия.

Шестой механизм состоит в применении регуляторных полномочий. Компетентные органы могут запрашивать документы, требовать раскрытия дополнительной информации, проводить проверки, ограничивать деятельность, применять административные меры и передавать материалы в иные органы при наличии признаков правонарушений. В условиях цифрового рынка такие действия могут развиваться быстро и затрагивать широкий круг лиц.

Седьмой механизм связан с использованием цифровых данных в судебных и административных процедурах. Отчёты аналитических компаний, выводы экспертов, данные блокчейна, внутренние журналы платформ и технические заключения могут становиться основой для решений, затрагивающих права лиц. Поэтому принципиальное значение имеет возможность проверить источник данных, методологию анализа, полноту выборки, наличие альтернативных объяснений и квалификацию экспертов.

Восьмой механизм заключается в трансграничном распространении последствий. Решение регулятора одной юрисдикции, delisting токена, публичное сообщение о нарушениях, санкционная или комплаенс-проверка могут повлиять на отношение к проекту или лицу в других странах. Крипторынок по своей природе трансграничен, поэтому правовые последствия часто распространяются быстрее, чем механизмы защиты.

Девятый механизм связан с совмещением частного и публичного контроля. Эмитенты, платформы, аналитические сервисы и кастодиальные организации принимают решения в рамках договорных и внутренних процедур, но последствия таких решений могут быть сопоставимы с публично-правовым ограничением. При этом процессуальные гарантии пользователя или эмитента зависят не только от закона, но и от внутренних правил конкретного участника рынка.

Десятый механизм состоит в закреплении негативного профиля. Даже если подозрения не подтверждаются, сведения о риске, проверке, приостановке торгов или претензиях к раскрытию информации могут сохраняться в системах платформ, регуляторных материалах, рыночных публикациях и аналитических отчётах. Это может продолжать влиять на доступ к рынку, привлечение инвестиций и деловую репутацию.

Case Patterns / Типовые сценарии, модели развития ситуации или практика применения

Первый типовой сценарий связан с выпуском криптоактива, по которому документ о раскрытии информации подготовлен формально, неполно или без достаточного описания рисков. На начальном этапе проект может восприниматься как технологически перспективный и коммерчески привлекательный, однако впоследствии инвесторы, платформа или регулятор могут установить, что в документации не были раскрыты существенные сведения о структуре управления, правах держателей токенов, механизме обеспечения, зависимости от связанных лиц, ликвидности, технических ограничениях или рисках прекращения проекта. В таких случаях проблема переходит из области маркетинга в область юридической ответственности.

Второй сценарий возникает при расхождении между публичными заявлениями проекта и его фактической структурой. Эмитент или связанная с ним команда могут заявлять о децентрализованном характере управления, широкой рыночной поддержке, стабильной ликвидности или независимости проекта, тогда как технические и корпоративные данные показывают концентрацию контроля, зависимость от ограниченного числа лиц, искусственное поддержание спроса или отсутствие достаточных резервов. Такое расхождение может рассматриваться как существенный фактор при оценке добросовестности раскрытия информации.

Третий сценарий связан с подозрениями в манипулировании рынком. Резкий рост объёмов торгов, повторяющиеся операции между связанными адресами, согласованные действия нескольких счетов, нестандартные изменения цены перед публичным объявлением или использование нераскрытой информации могут стать основанием для внутренней проверки платформы или регуляторного расследования. При этом сами по себе необычные торговые данные не должны автоматически признаваться доказательством нарушения. Требуется анализ экономического контекста, технической структуры операций, наличия связи между участниками и альтернативных объяснений.

Четвёртый сценарий касается использования данных блокчейна в качестве доказательства. В административном или судебном процессе может быть представлен отчёт аналитической компании, указывающий на движение активов между определёнными адресами, связь с высокорискованными кошельками, концентрацию владения или подозрительные торговые паттерны. Однако такие выводы зависят от методологии, полноты данных, точности атрибуции адресов и качества экспертного анализа. Если суд или регулятор принимает такие данные формально, без проверки исходных предпосылок, возникает риск ошибочного вывода.

Пятый сценарий связан с отказом платформы в листинге или удалением токена из обращения. Для проекта такое решение может иметь критическое значение, поскольку доступ к крупной торговой площадке влияет на ликвидность, доверие инвесторов и рыночную стоимость актива. Основаниями могут быть претензии к раскрытию информации, подозрения в манипулировании, санкционные риски, несоответствие внутренним стандартам платформы или запросы регуляторов. Даже если решение формально является частным коммерческим действием, его последствия могут быть сопоставимы с публичным ограничением доступа к рынку.

Шестой сценарий возникает при привлечении инвесторов на основе неполной или чрезмерно оптимистичной информации. Если проект делает акцент на потенциальной доходности, технологической уникальности, ожидаемом листинге или будущем развитии экосистемы, но не раскрывает существенные ограничения, риски и зависимости, инвесторы могут впоследствии заявлять требования о введении в заблуждение. В таких ситуациях значение имеют не только формальные документы, но и весь массив коммуникаций с рынком.

Седьмой сценарий связан с трансграничным расследованием. Компетентный орган одной юрисдикции может начать проверку раскрытия информации, торговли токеном или действий поставщика услуг, после чего данные распространяются между регуляторами, платформами, банками и комплаенс-подразделениями. В результате лицо или проект сталкивается с ограничениями сразу в нескольких странах, даже если исходное расследование ещё не завершено.

Восьмой сценарий касается уголовно-правовой квалификации действий на крипторынке. В отдельных случаях претензии, изначально связанные с раскрытием информации, рыночным поведением или защитой инвесторов, могут быть интерпретированы как мошенничество, легализация преступных доходов, злоупотребление полномочиями или иное уголовное правонарушение. Такая трансформация существенно повышает риски: появляются основания для ареста активов, международного сотрудничества, розыска, экстрадиции и банковских ограничений.

Девятый сценарий связан с ошибочной или неполной экспертизой. Суд, регулятор или платформа могут опираться на техническое заключение, которое не учитывает специфику протокола, особенности торговой инфраструктуры, роль маркет-мейкеров, автоматизированных стратегий, мостов между сетями или внутренних процедур биржи. При недостаточной проверке такое заключение может сформировать ошибочную картину событий.

Десятый сценарий представляет собой ситуацию, при которой проект или лицо формально устраняет нарушение, обновляет раскрытие информации, предоставляет документы или меняет структуру управления, однако негативный регуляторный или рыночный профиль сохраняется. Предыдущие претензии продолжают влиять на отношения с платформами, инвесторами, банками и контрагентами. Поэтому восстановление правового и рыночного статуса требует отдельной работы, а не только устранения первоначального нарушения.

Risk Assessment / Основные риски, правовые уязвимости и проблемные зоны

Первый риск заключается в формальном восприятии цифровых данных как объективного и самодостаточного доказательства. Данные блокчейна, отчёты аналитических компаний, алгоритмические выводы, статистика торгов и технические журналы могут создавать впечатление высокой точности. Однако любые такие материалы зависят от исходных данных, выбранной методологии, корректности атрибуции адресов, полноты выборки и профессионального уровня эксперта. Без проверки этих факторов существует риск ошибочной квалификации событий и необоснованных ограничений.

Второй риск связан с неполным или неточным раскрытием информации. Документ о криптоактиве, маркетинговые материалы, сведения о резервах, структуре управления и технических особенностях проекта формируют основу для оценки его надёжности. Если существенные факты не раскрыты, описаны неоднозначно или представлены в форме, способной вводить в заблуждение, это может повлечь претензии со стороны регуляторов, инвесторов, платформ и контрагентов.

Третий риск состоит в расширительном толковании правил о злоупотреблениях на рынке. Необычные торговые паттерны, высокая концентрация токенов, согласованные действия маркет-мейкеров или резкие изменения цены могут интерпретироваться как признаки манипулирования рынком. При отсутствии достаточного анализа экономического контекста и технических особенностей существует вероятность того, что допустимое рыночное поведение будет ошибочно квалифицировано как нарушение.

Четвёртый риск связан с концентрацией дискреционных полномочий у платформ и иных частных участников рынка. Биржи, кастодиальные сервисы, эмитенты токенов и аналитические компании принимают решения, которые могут определять доступ к ликвидности, возможность листинга, продолжение обслуживания и рыночную репутацию. При этом процессуальные гарантии и стандарты проверки зависят от внутренних правил соответствующих организаций.

Пятый риск заключается в трансграничном распространении последствий. Одно регуляторное расследование, публичное предупреждение, delisting токена или негативный аналитический отчёт могут вызвать ограничения в нескольких юрисдикциях одновременно. Это повышает вероятность множественных проверок, отказов в обслуживании и репутационного ущерба.

Шестой риск связан с преобразованием административных или регуляторных претензий в уголовно-правовые последствия. Нарушения, первоначально относящиеся к раскрытию информации или рыночному поведению, могут стать основанием для обвинений в мошенничестве, злоупотреблении полномочиями, манипулировании рынком или легализации преступных доходов.

Седьмой риск состоит в утрате доступа к капиталу и ликвидности. Ограничение торгов, удаление токена с платформ, блокировка операций или прекращение обслуживания могут резко снизить стоимость актива и затруднить исполнение обязательств перед инвесторами, кредиторами, партнёрами и клиентами.

Восьмой риск связан с информационной асимметрией. Лицо или проект часто не располагают полной информацией о том, какие данные были использованы, какие критерии применялись и каким образом был сформирован вывод о наличии нарушения. Это существенно затрудняет подготовку эффективной защиты.

Девятый риск заключается в сохранении негативного профиля после устранения нарушений. Даже при обновлении документации, предоставлении доказательств и выполнении требований регулятора сведения о прошлых претензиях могут продолжать влиять на отношения с платформами, банками, инвесторами и контрагентами.

Десятый риск состоит в правовой неопределённости. Несмотря на развитие MiCA и сопутствующих актов, судебная и административная практика продолжает формироваться. Подходы к оценке цифровых доказательств, раскрытия информации, рыночного поведения и соразмерности ограничений могут существенно различаться, что увеличивает значение квалифицированного правового анализа и стратегической подготовки.

Institutional Gaps / Институциональные ограничения, пробелы, дефицит гарантий или системные слабости

Первое институциональное ограничение заключается в том, что нормативная база развивается быстрее, чем судебная и административная практика, способная обеспечить единообразное и предсказуемое применение новых правил. MiCA формирует детальную регуляторную систему, однако многие вопросы, связанные с оценкой цифровых доказательств,

квалификацией рыночного поведения, пределами раскрытия информации и критериями соразмерности ограничений, будут разрешаться постепенно. На переходном этапе это создаёт значительную правовую неопределённость.

Второе ограничение связано с высокой технической сложностью рассматриваемых вопросов. Судьи, регуляторы, адвокаты, инвесторы и комплаенс-подразделения вынуждены оценивать смарт-контракты, алгоритмические модели, структуру резервов, распределение токенов, торговые паттерны и данные блокчейна. При недостаточной технической подготовке возрастает риск чрезмерного упрощения или некритического восприятия экспертных заключений.

Третье ограничение состоит в информационной асимметрии между участниками рынка и контролирующими субъектами. Платформы, аналитические компании и регуляторы могут располагать существенно большим объёмом данных, чем эмитент, инвестор или лицо, в отношении которого проводится проверка. При отсутствии эффективных механизмов раскрытия и проверки такой дисбаланс затрудняет реализацию права на защиту.

Четвёртое ограничение связано с концентрацией фактической власти у ограниченного числа частных организаций. Крупные торговые платформы, поставщики аналитических услуг и кастодиальные сервисы способны принимать решения, определяющие доступ проекта к ликвидности, капиталу и рынку. При этом их внутренние процедуры не всегда обеспечивают уровень процессуальных гарантий, сопоставимый с публично-правовыми процедурами.

Пятое ограничение заключается в отсутствии унифицированных стандартов оценки технических доказательств. Методологии аналитических компаний, способы атрибуции адресов, подходы к выявлению манипулирования и критерии оценки раскрытия информации могут существенно различаться. Это увеличивает вероятность противоречивых выводов и затрудняет сопоставимость результатов.

Шестое ограничение связано с трансграничным характером крипторынка. Эмитент, инвесторы, торговые платформы, резервы, кастодиальные сервисы и регуляторы могут находиться в разных юрисдикциях. Такая структура осложняет определение применимого права, компетентного органа, процессуальных сроков и порядка исполнения решений.

Седьмое ограничение состоит в ограниченной способности системы к восстановлению статуса после устранения нарушений. Даже после обновления документации, выполнения предписаний или прекращения расследования негативный профиль может сохраняться в аналитических отчётах, внутренних системах платформ и публичных источниках.

Восьмое ограничение связано с недостаточной интеграцией правозащитных стандартов в частные процедуры. Решения о delisting, ограничении операций, отказе в обслуживании и блокировке активов нередко принимаются на основе договорных и внутренних правил, однако их последствия непосредственно затрагивают имущественные права, деловую репутацию и возможность продолжения деятельности.

Девятое ограничение заключается в высокой зависимости участников рынка от внешних поставщиков информации. Регуляторы, платформы и инвесторы могут опираться на данные аналитических компаний, рейтинговых агентств, аудиторов и технических консультантов. Если исходные выводы содержат ошибки, последствия распространяются по всей системе.

Десятое ограничение состоит в преобладании превентивного подхода. В условиях неопределённости платформы и регуляторы нередко предпочитают приостановить операции, ограничить доступ к рынку или инициировать проверку до окончательного выяснения

обстоятельств. Такой подход снижает регуляторные риски для принимающих решение субъектов, но переносит значительную часть негативных последствий на эмитентов, инвесторов и иных добросовестных участников рынка.

Practical Guidance / Практические рекомендации и модель правового действия

Первый практический шаг состоит в том, чтобы рассматривать требования MiCA и сопутствующего регулирования не как формальную обязанность по подготовке документов, а как центральный элемент правовой защиты проекта, эмитента, поставщика услуг и инвесторов. Документ о криптоактиве, маркетинговые материалы, описание технической архитектуры, сведения о рисках и данные о структуре управления должны быть подготовлены таким образом, чтобы их можно было использовать не только для допуска к рынку, но и для защиты в случае претензий, расследований или споров.

Второй шаг заключается в предварительной правовой проверке всей информации, раскрываемой рынку. Необходимо сопоставлять публичные заявления, техническую документацию, внутренние материалы, сведения о резервах, корпоративную структуру, права держателей токенов, ограничения проекта и фактическую практику его функционирования. Любое расхождение между этими уровнями может впоследствии рассматриваться как признак недобросовестного раскрытия информации.

Третий шаг состоит в документировании технических решений и управленческих процедур. Проект должен иметь понятную и проверяемую внутреннюю документацию, объясняющую работу смарт-контрактов, распределение полномочий, порядок изменения протокола, управление резервами, роль связанных лиц, механизмы внутреннего контроля и процедуры реагирования на технические или рыночные инциденты. Это имеет значение не только для регулятора, но и для защиты от последующих претензий инвесторов и контрагентов.

Четвёртый шаг заключается в независимой проверке цифровых данных и технических отчётов. Если в деле используются данные блокчейна, выводы аналитических компаний, торговая статистика или технические заключения, необходимо проверять методологию, полноту исходных данных, точность атрибуции адресов, наличие альтернативных объяснений и квалификацию экспертов. Цифровой характер доказательства не делает его автоматически полным, достоверным или юридически достаточным.

Однако на практике одного общего требования “проверять методологию и исходные данные” недостаточно: в спорах по MiCA, злоупотреблениям на рынке и раскрытию информации сторонам и органу, рассматривающему дело, нужна воспроизводимая рамка, позволяющая отличать проверяемый факт от интерпретации и корректно оценивать доказательственный вес технических материалов. Ниже приводится практическая модель судебной оценки цифровых доказательств и технических отчётов, ориентированная на международную аудиторию.

Судебная оценка цифровых доказательств и технических отчётов в криптоспорах (MiCA / злоупотребления на рынке / раскрытие информации): как избежать «автоматического доверия» к односторонним данным

Усиление регулирования крипторынка (включая режимы, связанные с раскрытием информации, мониторингом операций и выявлением злоупотреблений) делает «цифровые следы» центральным объектом доказывания: ончейн-транзакции, данные бирж и кастодианов, выгрузки через интерфейсы и API, журналы входов и подтверждений, результаты блокчейн-аналитики и технические экспертизы. Основной процессуальный риск — подмена доказательства интерпретацией: технический отчёт начинает восприниматься как

установленный факт, хотя нередко он является продуктом настроек системы, порогов срабатывания, эвристик и неполных исходных данных.

Практически полезно, чтобы суд (или орган, рассматривающий спор) оценивал такие материалы по трём разным вопросам: (а) допустимость, (б) доказательственный вес, (в) достаточность в совокупности. Технический отчёт может быть допустимым, но иметь низкий вес; и почти никогда не «закрывает» сам по себе весь стандарт доказывания без опоры на проверяемые исходники и независимую проверку.

Ниже — рамка из семи шагов, которая помогает избежать формального принятия односторонних цифровых данных.

1) Разделить «первичные данные» и «аналитические выводы» — и требовать обоснование для каждого слоя

Суду целесообразно отдельно фиксировать:
Первичный слой: идентификаторы транзакций, временные метки, адреса, записи ввода/вывода, системные журналы, исходные выгрузки (не «картинки», а данные).
Интерпретационный слой:кластеризация адресов, атрибуция, риск-скоринг, графовые реконструкции, выводы о «связи» и «контроле».
Правовой слой: квалификация (например, «манипулирование рынком», «использование инсайдерской информации», «вводящее в заблуждение раскрытие»).

Ключевая мысль для мотивировки: отчёт аналитика — это мнение на основе данных, а не сами данные. Поэтому суду важно показать, какие факты он принимает, и отдельно — почему он принимает (или не принимает) интерпретацию.

2) Проверить происхождение, целостность и воспроизводимость (аналог «цепочки сохранности»)

Минимальный набор вопросов:
кто собрал/выгрузил сведения, когда и из какого источника (провайдер, биржа, кастодиан, узел, обозреватель, устройство);
как обеспечивалась неизменность: контроль доступа, версии файлов, журналы изменений, контрольные суммы/хэши (где применимо);
какие промежуточные шаги обработки были до отчёта (склейка таблиц, фильтры, «очистка», удаление строк, агрегация);
может ли независимый специалист повторить получение сопоставимого результата при тех же входных данных и описанных шагах (хотя бы по ключевым элементам).

Если повторяемость недостижима, это не всегда исключает материал, но обычно существенно снижает его вес и повышает требования к поддерживающим доказательствам.

3) Оценить надёжность методики по «судебно-проверочным» критериям (Daubert-подобная логика без привязки к юрисдикции)

Даже в правопорядках без формального «теста Дауберта» суды, как правило, проверяют близкие вопросы:
описана ли методика так, чтобы её можно было проверить (пусть без раскрытия коммерческих секретов, но с объяснением логики, входных данных, параметров и ограничений);
известны ли типичные ошибки/ложные совпадения и как они учитывались;
есть ли процедуры контроля качества (валидация, внутренний аудит, сравнение с контрольными наборами);
не является ли вывод «чёрным ящиком» вида «так показал инструмент — значит так и было».

Для споров о злоупотреблениях на рынке и раскрытии информации это критично: корреляции (время публикаций, сделки, перемещения токенов) легко превращаются в «доказанность инсайда/манипуляции», хотя могут объясняться маркет-мейкингом, хеджированием, арбитражем, исполнением клиентских поручений, работой ботов или особенностями маршрутизации внутри платформы.

4) Учитывать «регуляторную иллюзию достоверности»: алерты комплаенса не равны факту нарушения

В среде усиленного регулирования (в том числе при выполнении требований по мониторингу и внутренним контролям) многие доказательства рождаются как результат фильтров и порогов: «флаг», «алерт», «подозрительная активность», «аномалия». Суду важно прямо проговорить:
алерт подтверждает лишь то, что событие пересекло порог настроек системы, но не доказывает по умолчанию умысел, инсайд, манипуляцию или недобросовестное раскрытие. Поэтому требуется независимая проверка исходных данных и альтернативных объяснений, а не ссылка на «сам факт срабатывания мониторинга».

5) Не отождествлять адрес/аккаунт с лицом: нужен «мостик идентификации»

Даже если транзакции подлинны, остаётся вопрос: кто контролировал ключ/аккаунт в релевантный момент. Для вывода о контроле обычно нужны дополнительные связки: данные биржи/кастодиана (KYC, история входов, устройства, подтверждения операций); логи и события безопасности (смена пароля, восстановление доступа, 2FA, подозрительные входы);
деловая переписка/договоры/экономический контекст;
исключение сценариев делегированного доступа, компрометации, общих корпоративных учётных записей.

При слабом «мостике» суду безопаснее квалифицировать вывод о контроле как вероятностный и не строить на нём единолично ключевые правовые выводы.

6) Обеспечить проверяемость в процессе: раскрытие материалов, симметрия экспертизы, допрос автора отчёта

Чтобы не закрепить одностороннюю картину, суду целесообразно проверить, что у другой стороны была реальная возможность оспорить материал:
доступ к минимально необходимым исходникам (идентификаторы транзакций, адреса, временные метки, ссылки на источники, не только визуализации);
возможность представить независимое заключение специалиста;
возможность задать вопросы автору отчёта по входным данным, фильтрам, допущениям, ошибкам и пределам применимости.

Если полное раскрытие ограничено (тайна следствия, безопасность, коммерческая конфиденциальность), суду полезно применять баланс-подход: допускаются компенсирующие меры (редакция чувствительных частей, доступ эксперта под обязательство конфиденциальности, закрытое заседание, «чистая комната» для ознакомления), но ограничения должны быть мотивированы, а компенсаторы — достаточными для состязательной проверки.

7) Требовать ответа на существенные альтернативы, а не «на всё подряд»

Суд не обязан обсуждать каждую гипотезу, но обычно должен рассмотреть существенные и подкреплённые материаламиальтернативные сценарии (например, маркет-мейкинг,

ребалансировка, хедж, инфраструктурная маршрутизация, агрегированные кошельки, сервисное хранение). В мотивировке важно показать не только «почему версия расследования подтверждается», но и почему разумные альтернативы исключаются либо почему доказательства не позволяют исключить их с требуемой степенью уверенности.

Итоговая формула

Чтобы не допустить формального принятия неподтверждённых или односторонних цифровых материалов, суду полезно последовательно проверять: (1) происхождение и целостность данных, (2) надёжность и проверяемость методики, (3) связку “цифровой след → конкретное лицо”, (4) процессуальную состязательность (доступ к исходникам, контр-экспертиза, проверка существенных альтернатив) — и отдельно различать допустимость, доказательственный вес и достаточность в совокупности.

Эта рамка важна не только для суда или регулятора, но и для самих участников рынка: именно по таким критериям впоследствии оцениваются добросовестность внутреннего контроля, качество мониторинга и устойчивость позиции при споре. Далее перейдём к следующему практическому элементу — построению внутренней системы предупреждения злоупотреблений на рынке.

Пятый шаг состоит в формировании внутренней системы предупреждения злоупотреблений на рынке. Эмитенты и поставщики услуг должны иметь процедуры выявления подозрительных торговых паттернов, операций связанных лиц, необычных изменений ликвидности, использования нераскрытой информации и распространения недостоверных сведений. Наличие такой системы снижает регуляторный риск и показывает добросовестность участника рынка.

Шестой шаг связан с контролем маркетинговых сообщений. Все публичные заявления, рекламные материалы, презентации, публикации на сайте, сообщения в социальных сетях и коммуникации с инвесторами должны соответствовать фактической структуре проекта и раскрывать существенные риски. Нельзя допускать, чтобы маркетинговое описание создавало у инвесторов ожидания, не подтверждённые юридической, финансовой или технической реальностью.

Седьмой шаг заключается в подготовке стратегии взаимодействия с платформами. Если проект зависит от листинга, торговли или обслуживания на конкретной площадке, необходимо заранее понимать её требования, внутренние процедуры проверки, основания для приостановки торгов, правила delisting, порядок подачи возражений и механизмы восстановления доступа. Это особенно важно для проектов, стоимость которых существенно зависит от рыночной ликвидности.

Восьмой шаг состоит в анализе трансграничных последствий. Эмитент, команда проекта, инвесторы, платформы, резервы и пользователи могут находиться в разных юрисдикциях. Поэтому правовая позиция должна учитывать не только требования MiCA, но и национальное законодательство, санкционные ограничения, налоговые последствия, правила финансового мониторинга и возможные требования иностранных регуляторов.

Девятый шаг заключается в обеспечении процессуальной готовности к проверкам и спорам. Проект должен иметь готовый пакет документов, включающий корпоративные сведения, технические материалы, отчёты о рисках, политику раскрытия информации, процедуры внутреннего контроля, доказательства добросовестного поведения и материалы, подтверждающие соблюдение требований регулирования. В случае претензий скорость и качество реакции имеют существенное значение.

Десятый шаг состоит в восстановлении правового и рыночного статуса после возникновения претензий. Если токен был удалён с платформы, доступ к операциям ограничен, регулятор начал проверку или был опубликован негативный отчёт, необходимо не только устранить выявленную проблему, но и добиваться обновления информации, пересмотра внутренних профилей риска, восстановления доступа к рынку и документального подтверждения изменения статуса.

Policy Recommendations / Рекомендации по правовому и институциональному подходу

Во-первых, регулирование криптоактивов должно развиваться с учётом того, что раскрытие информации является не только инструментом надзора, но и механизмом защиты участников рынка. Документы о криптоактивах, технические описания, сведения о резервах, данные о структуре управления и маркетинговые сообщения должны быть понятными, проверяемыми и достаточно полными для того, чтобы инвесторы, платформы и регуляторы могли оценить реальный характер проекта.

Во-вторых, компетентные органы должны уделять особое внимание качеству цифровых доказательств. Данные блокчейна, аналитические отчёты, торговая статистика и технические заключения не должны приниматься формально только потому, что они имеют цифровую природу. Необходима проверка методологии, полноты исходных данных, точности атрибуции адресов, возможных альтернативных объяснений и квалификации экспертов.

В-третьих, следует развивать единые подходы к оценке злоупотреблений на рынке криптоактивов. Манипулирование рынком, использование инсайдерской информации и распространение вводящих в заблуждение сведений должны оцениваться с учётом особенностей цифровой инфраструктуры, автоматизированной торговли, роли маркет-мейкеров, кросс-чейн операций и специфики ликвидности на криптовалютных площадках.

В-четвёртых, правила MiCA и сопутствующее регулирование должны применяться таким образом, чтобы не допускать чрезмерного формализма. Нарушение раскрытия информации или необычные торговые данные не всегда свидетельствуют о недобросовестности. В каждом случае требуется оценка контекста, характера нарушения, реального ущерба, поведения участника рынка и принятых им мер по исправлению ситуации.

В-пятых, частные платформы и поставщики услуг должны обеспечивать более прозрачные процедуры принятия решений. Отказ в листинге, приостановка торгов, удаление токена из обращения, блокировка операций или прекращение обслуживания должны сопровождаться достаточным объяснением причин и возможностью представить возражения, если соответствующее решение затрагивает существенные имущественные или деловые интересы.

В-шестых, необходимо усилить связь между регулированием криптоактивов и стандартами защиты права собственности. Ограничение доступа к токенам, ликвидности, торговой инфраструктуре или инвестиционным возможностям может иметь последствия, сопоставимые с традиционными имущественными ограничениями. Поэтому такие меры должны оцениваться с точки зрения законности, необходимости, соразмерности и процессуальной справедливости.

В-седьмых, регуляторы и суды должны учитывать риск трансграничного распространения последствий. Решение, принятое в одной юрисдикции, может повлиять на торговлю, банковское обслуживание, репутацию и правовой статус проекта в других странах. Следовательно, при применении ограничительных мер необходимо учитывать не только непосредственную цель регулирования, но и совокупный международный эффект.

В-восьмых, следует развивать механизмы восстановления статуса после устранения нарушений или опровержения претензий. Обновление раскрытия информации, исправление технических недостатков, снятие ограничений или прекращение расследования должны сопровождаться реальными процедурами обновления данных в реестрах, на платформах и в аналитических системах.

В-девятых, участникам рынка следует внедрять внутренние процедуры правовой и технической проверки до возникновения спора. Добросовестное документирование, независимый технический аудит, контроль маркетинговых сообщений, проверка резервов и прозрачная структура управления должны рассматриваться как обязательные элементы правовой защиты, а не как дополнительные административные расходы.

В-десятых, регулирование крипторынка должно строиться на балансе между защитой инвесторов, предотвращением злоупотреблений и сохранением доступа добросовестных участников к рынку. Чрезмерно жёсткий или непрозрачный подход способен не только снизить риски, но и создать новые формы правовой неопределённости, при которых технические или регуляторные выводы становятся источником несоразмерных ограничений.

Conclusion / Заключение

Регламент MiCA и сопутствующее регулирование криптоактивов формируют новую правовую реальность для цифрового рынка. Криптоактивы больше не могут рассматриваться как область, существующая преимущественно вне традиционного финансового и правового контроля. Их выпуск, обращение, продвижение, хранение, торговля и использование становятся предметом детального регулирования, надзора и правовой ответственности.

Главное значение MiCA состоит не только в создании единых правил для участников рынка Европейского союза, но и в формировании нового стандарта правовой оценки цифровых активов. Документы о криптоактивах, раскрытие информации, корпоративное управление, защита клиентов, устойчивость поставщиков услуг и предотвращение злоупотреблений на рынке становятся центральными элементами правового анализа.

В то же время усиление регулирования не устраняет риск ошибок, формального подхода и непропорциональных ограничений. Напротив, чем более значимыми становятся цифровые данные, технические отчёты и внутренние решения платформ, тем выше необходимость в их критической проверке. Суд, регулятор или платформа не должны принимать данные блокчейна, аналитические выводы или торговые показатели как автоматически достоверные только потому, что они представлены в цифровой форме.

Для ARGA основной вывод состоит в следующем. Регулирование крипторынка становится самостоятельным направлением правовой защиты, поскольку оно затрагивает право собственности, доступ к капиталу, деловую репутацию, корпоративные интересы, свободу предпринимательской деятельности и возможность эффективного судебного оспаривания. Защита в таких делах должна соединять финансовое регулирование, технологический анализ, процессуальные гарантии и международные стандарты прав человека.

Эффективный подход к делам, связанным с MiCA, раскрытием информации и злоупотреблениями на рынке, требует не только знания текста нормативных актов. Он требует способности оценивать реальную структуру проекта, достоверность цифровых данных, качество экспертных заключений, соразмерность ограничений и трансграничные последствия решений. Только такая модель позволяет отличить добросовестное регулирование от ситуации, в которой технические или регуляторные выводы становятся основанием для необоснованного ограничения прав.

Приложение А. Терминология

Криптоактив. Цифровое представление стоимости или права, которое может передаваться и храниться с использованием технологии распределённого реестра или аналогичной технологии.

Документ о криптоактиве. Информационный документ, содержащий сведения о проекте, эмитенте, характеристиках криптоактива, правах держателей, рисках, технической структуре и иных существенных обстоятельствах, необходимых для оценки актива участниками рынка.

Эмитент криптоактива. Лицо или организация, выпускающая криптоактив, предлагающая его публике или добивающаяся его допуска к обращению на торговой платформе.

Поставщик услуг в сфере криптоактивов. Организация, предоставляющая услуги по хранению, обмену, торговле, размещению, исполнению поручений, консультированию или иному обслуживанию операций с криптоактивами.

Токен, привязанный к активам. Вид криптоактива, стоимость которого предполагается стабилизировать посредством привязки к одной или нескольким валютам, товарам, криптоактивам или их сочетанию.

Токен электронных денег. Вид криптоактива, предназначенный для поддержания стабильной стоимости путём привязки к одной официальной валюте.

Раскрытие информации. Предоставление участникам рынка, инвесторам, платформам и регуляторам существенных сведений о проекте, рисках, структуре управления, правах держателей, резервах, технических характеристиках и ограничениях.

Злоупотребление на рынке. Действия, нарушающие честность и прозрачность рынка, включая использование инсайдерской информации, манипулирование рынком, распространение ложных или вводящих в заблуждение сведений и искусственное создание рыночной активности.

Манипулирование рынком. Поведение, направленное на создание ложного или вводящего в заблуждение представления о спросе, предложении, цене, объёмах торгов или рыночной активности в отношении криптоактива.

Инсайдерская информация. Необщедоступные сведения точного характера, которые прямо или косвенно касаются криптоактива или его эмитента и которые, будучи раскрытыми, могли бы существенно повлиять на цену или инвестиционные решения.

Данные блокчейна. Записи распределённого реестра, отражающие транзакции, адреса, движение активов, взаимодействие смарт-контрактов и иные технические события.

Аналитика блокчейна. Метод анализа данных распределённого реестра, используемый для выявления связей между адресами, отслеживания движения активов, оценки торгового поведения и присвоения показателей риска.

Листинг. Допуск криптоактива к торговле или обращению на торговой платформе.

Удаление из обращения на платформе. Решение торговой платформы прекратить поддержку криптоактива, приостановить его торги или исключить его из перечня доступных активов.

Процессуальная справедливость. Совокупность минимальных гарантий, позволяющих лицу понимать основания претензий, получать доступ к существенным материалам, представлять возражения, добиваться пересмотра решения и пользоваться эффективной защитой.

Приложение В. Матрица рисков / полномочий / правовых последствий

Действие	Правовой риск	Юридический предел	Возможные последствия	Практический комментарий
Выпуск криптоактива без достаточного раскрытия информации	Риск введения инвесторов и платформ в заблуждение	Раскрытие должно быть полным, точным, понятным и не вводящим в заблуждение	Претензии инвесторов, отказ в листинге, регуляторные меры, репутационный ущерб	Необходимо заранее проверять документ о криптоактиве, техническое описание и сведения о рисках
Публичное предложение токена	Риск нарушения требований MiCA и национального законодательства	Предложение должно соответствовать требованиям к раскрытию, уведомлению и допустимости обращения	Приостановка предложения, административные меры, гражданско-правовые требования	Следует документировать все стадии предложения и коммуникации с инвесторами
Использование маркетинговых материалов	Риск несоответствия между рекламой и фактической структурой проекта	Маркетинговые сообщения должны соответствовать раскрываемой информации и не создавать необоснованных ожиданий	Жалобы инвесторов, претензии платформ, регуляторное вмешательство	Все публичные сообщения должны проходить правовую и фактическую проверку
Недостоверное описание резервов или обеспечения	Риск неправильной оценки устойчивости актива	Сведения о резервах должны быть проверяемыми, актуальными и согласованными с фактической структурой	Потеря доверия, ограничения обращения, требования о компенсации	Требуется независимая проверка и регулярное обновление информации
Подозрение в манипулировании рынком	Риск квалификации торгового поведения как злоупотребления	Вывод о нарушении должен учитывать контекст, данные, связь между участниками и альтернативные объяснения	Проверки, приостановка торгов, административная или уголовная ответственность	Необходимо анализировать торговые паттерны, роль маркет-мейкеров и технические особенности операций
Использование инсайдерской информации	Риск нарушения правил честности рынка	Доступ к нераскрытой существенной информации должен контролироваться и документироваться	Расследование, санкции, претензии инвесторов, репутационный ущерб	Следует внедрять внутренние правила обращения с конфиденциальной информацией

Отчёт аналитической компании о подозрительных транзакциях	Риск формального принятия технических выводов	Методология, данные и атрибуция адресов должны быть проверяемыми	Ограничения платформ, регуляторные запросы, банковские проверки	Необходимо готовить контранализ и проверять полноту исходных данных
Отказ платформы в листинге	Ограничение доступа к ликвидности и рынку	Решение должно соответствовать правилам платформы и учитывать представленные документы	Снижение стоимости актива, потеря инвесторов, репутационный ущерб	Следует заранее анализировать требования платформы и готовить пакет раскрытия
Удаление токена из обращения на платформе	Риск резкой потери ликвидности и доверия	Мера должна быть обоснованной, соразмерной и процедурно проверяемой	Падение стоимости, массовые требования держателей, прекращение рыночной активности	Необходимо добиваться объяснения причин и процедуры восстановления статуса
Регуляторный запрос документов	Риск расширения проверки и последующих ограничений	Запрос должен иметь правовое основание и разумный объём	Обязанность раскрытия документов, последующие предписания, административные меры	Ответ должен быть полным, структурированным и согласованным с общей правовой позицией
Использование данных блокчейна в суде	Риск ошибочной оценки цифровых доказательств	Данные должны проверяться с точки зрения источника, полноты, методологии и экспертной интерпретации	Судебные выводы о нарушении, имущественные ограничения, ответственность	Необходимо привлекать квалифицированных технических специалистов и готовить альтернативную интерпретацию
Трансграничное распространение негативной информации	Риск множественных ограничений в разных юрисдикциях	Последствия должны оцениваться с учётом соразмерности и качества исходных данных	Банковские отказы, проверки платформ, репутационный ущерб, ограничения операций	Следует формировать единую международную позицию и добиваться обновления данных
Исправление нарушения без восстановления статуса	Сохранение негативного профиля несмотря на устранение проблемы	Обновление статуса должно отражать фактические изменения и новые документы	Продолжение ограничений, отказ инвесторов, сложности с платформами	Требуется отдельная работа по восстановлению рыночного и правового статуса

Данная матрица отражает типовые ситуации, в которых регулирование криптоактивов, требования к раскрытию информации, правила противодействия злоупотреблениям на рынке и использование цифровых доказательств могут создавать существенные правовые последствия для эмитентов, поставщиков услуг, инвесторов и владельцев активов. Её практическая функция состоит в том, чтобы заранее выявлять точки риска, обеспечивать документальную готовность и не допускать формального принятия технических выводов без надлежащей проверки.

Официальные источники

European Union, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).

European Union, Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets.

European Union, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).

European Union, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

European Union, Directive (EU) 2018/843 amending Directive (EU) 2015/849.

European Securities and Markets Authority (ESMA), technical standards, guidelines and materials relating to the implementation of the Markets in Crypto-Assets Regulation.

European Banking Authority (EBA), technical standards, guidelines and materials concerning asset-referenced tokens, electronic money tokens and prudential requirements for issuers.

Financial Action Task Force (FATF), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

Financial Stability Board (FSB), reports on the regulation and supervision of global stablecoin arrangements and crypto-asset markets.

Bank for International Settlements (BIS), publications on crypto-assets, stablecoins, financial stability and digital market risks.

International Organization of Securities Commissions (IOSCO), reports and recommendations on crypto-asset regulation, trading platforms and market integrity.

European Convention on Human Rights.

Case law of the European Court of Human Rights concerning Article 6 of the European Convention on Human Rights.

Case law of the European Court of Human Rights concerning Article 1 of Protocol No. 1 to the European Convention on Human Rights.

United Nations materials on digital finance, financial integrity and illicit financial flows.