УДК 347.44:004.056

Забродин Илья Андреевич,
студент юридического факультета
Финансовый университет при
Правительстве Российской Федерации
Научный руководитель: Исмаилов Исмаил Шапурович,
к.ю.н.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ: ЧАСТНОПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ И РАСПРЕДЕЛЕНИЯ РИСКОВ

Аннотация: *В статье исследуются механизмы частноправовой защиты цифровых финансовых активов в условиях нарастающих киберугроз и неопределённости правового регулирования. Анализируется специфика правовых рисков, связанных с оборотом цифровых прав в информационных системах на базе распределённых реестров. Рассматриваются договорные инструменты распределения ответственности между участниками цифровых экосистем - операторами информационных систем, эмитентами ЦФА, инвесторами. Обосновывается необходимость совершенствования гражданско-правовых средств защиты, включая презумпцию владения на основе криптографического ключа, признание юридической значимости блокчейн-записей и институционализацию смарт-контрактов. Результаты исследования применимы для формирования эффективной модели частноправового регулирования цифровых активов в России.*

Ключевые слова: *цифровые финансовые активы, информационная безопасность, частноправовые механизмы защиты, распределение рисков, смарт-контракты, блокчейн, договорная ответственность.*

Annotation: *The article examines the mechanisms of private law protection of digital financial assets in the context of growing cyber threats and uncertainty of legal regulation. The specifics of legal risks associated with the circulation of digital rights in information systems based on distributed ledgers are analyzed. Contractual instruments for allocating responsibility between participants in digital ecosystems - operators of information systems, DFA issuers, investors - are considered. The necessity of improving civil law remedies is substantiated, including the presumption of ownership based on cryptographic key, recognition of legal significance of blockchain records, and institutionalization of smart contracts. The research results are applicable for developing an effective model of private law regulation of digital assets in Russia.*

Keywords: *digital financial assets, information security, private law protection mechanisms, risk allocation, smart contracts, blockchain, contractual liability.*

Цифровизация финансовых отношений породила целый класс новых объектов гражданских прав - цифровые финансовые активы, утилитарные цифровые права и гибридные цифровые инструменты, функционирующие в информационных системах. Статья 141.1 Гражданского кодекса РФ, введённая Федеральным законом № 34-ФЗ от 18 марта 2019 года, определила цифровые права как обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы. Принятие Федерального закона № 259-ФЗ от 31 июля 2020 года «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» ознаменовало переход к формированию полноценной правовой среды для выпуска и обращения цифровых активов. Однако стремительное развитие цифровой инфраструктуры опережает нормативное регулирование -

практика демонстрирует критические пробелы в механизмах защиты прав участников оборота ЦФА.

Особенность цифровых финансовых активов состоит в том, что их существование и оборот происходят исключительно в цифровой среде, а доступ к активам детерминирован владением криптографическим ключом. Это создаёт специфический профиль рисков, не характерный для традиционных финансовых инструментов.

Правовая природа цифровых финансовых активов и специфика угроз информационной безопасности.

Цифровые финансовые активы представляют собой цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг. Выпуск ЦФА осуществляется посредством внесения в информационную систему решения о выпуске, содержащего сведения об эмитенте, объёме выпуска, правах, закрепляемых каждым ЦФА, условиях их осуществления. Такая конструкция порождает серьёзные правовые коллизии - речь идёт не столько о технологической форме фиксации традиционного права, сколько о новом типе объектов, существование которых невозможно вне информационной системы.

Технологической основой большинства информационных систем, в которых выпускаются и обращаются ЦФА, служит технология распределённых реестров (блокчейн). Эта технология обеспечивает неизменность записей, прозрачность истории транзакций и децентрализованное хранение данных [1]. Однако именно специфика блокчейна формирует уникальный профиль угроз информационной безопасности - утрата криптографического ключа означает безвозвратную потерю доступа к активам, компрометация ключа влечёт

несанкционированное распоряжение имуществом, а ошибки в коде смарт-контрактов могут привести к массовому хищению средств.

Анализ инцидентов 2024 года показывает, что значительная часть потерь в криптоиндустрии обусловлена базовыми просчётами информационной безопасности: отсутствием многофакторной аутентификации, слабыми паролями, фишинговыми атаками на сотрудников операторов платформ. По оценкам аналитиков, свыше 60% инцидентов могли быть предотвращены при соблюдении элементарных требований кибергигиены [2]. Технология блокчейна сама по себе защищена криптографически, но уязвимы периферийные элементы экосистемы - пользовательские интерфейсы, узлы взаимодействия с внешними системами (оракулы), личные устройства пользователей.

В отличие от традиционных финансовых инструментов, где потерпевший может обратиться в банк или депозитарий для восстановления доступа к счёту или реестру, в системе с распределённым реестром физический контроль над ключом заменяет все формы идентификации. Это порождает фундаментальную проблему - как обеспечить баланс между технологической автономностью и правовой защищённостью.

Пробелы в частноправовом регулировании защиты цифровых активов.

Действующее законодательство РФ создало нормативную рамку для функционирования ЦФА, но оставило открытыми ключевые вопросы распределения ответственности и средств защиты. Статья 8 Федерального закона № 259-ФЗ устанавливает, что оператор информационной системы обязан обеспечивать конфиденциальность информации, составляющей охраняемую законом тайну, и принимать меры по защите информации. Однако закон не содержит конкретизации объёма и содержания этих мер, равно как не определяет последствия их нарушения [3].

Особо проблематична ситуация с идентификацией владельца ЦФА. В силу специфики блокчейн-технологии владение цифровым активом подтверждается обладанием приватным ключом, а не записью в централизованном реестре с указанием персональных данных. Российское законодательство требует от операторов информационных систем проведения идентификации клиентов в соответствии с законодательством о противодействии легализации доходов, полученных преступным путём. При этом в самой информационной системе на базе блокчейна могут фигурировать только криптографические адреса без привязки к реальным личностям, что создаёт дуализм: юридически значимая информация о владельце хранится вне распределённого реестра, а техническое распоряжение активом осуществляется через блокчейн.

Принципиальная проблема - отсутствие нормативного регулирования смарт-контрактов как способа осуществления цифровых прав. Термин «смарт-контракт» не определён в российском законодательстве, хотя на практике значительная часть операций с ЦФА осуществляется именно посредством программного кода, автоматически исполняющегося при наступлении заданных условий. Некоторые исследователи полагают, что смарт-контракт следует рассматривать как особую форму автоматизации договорных отношений, где программа не просто фиксирует волеизъявление сторон, но и самостоятельно реализует права и обязанности [4]. Проблема состоит в том, что в гражданском праве отсутствует механизм судебной коррекции автоматически исполненной смарт-контрактной транзакции - если код содержал ошибку или условия изменились, вернуть переданные активы можно лишь в порядке кондикции, что на практике крайне затруднительно.

Судебная практика по спорам, связанным с утратой доступа к цифровым активам или их несанкционированным списанием, пока немногочисленна и противоречива. Суды признают цифровые права имуществом, подлежащим гражданско-правовой защите, однако отсутствуют устоявшиеся подходы к

определению надлежащего ответчика - оператора информационной системы, эмитента ЦФА или третьих лиц, получивших активы в результате несанкционированной операции [5]. Это создаёт правовую неопределённость для всех участников оборота.

Договорные механизмы распределения рисков в экосистемах цифровых активов.

В условиях неполноты законодательного регулирования ключевое значение приобретают договорные инструменты распределения ответственности. Основным документом, определяющим правоотношения между участниками экосистемы ЦФА, выступают правила информационной системы - документ, утверждаемый оператором и подлежащий согласованию с Банком России. Статья 4 Федерального закона № 259-ФЗ относит к обязательным условиям правил информационной системы порядок доступа к информационной системе, требования к её функционированию, обязанности оператора, права и обязанности пользователей.

На практике правила информационной системы представляют собой сложный гибридный документ, сочетающий элементы публично-правового регламента (требования Банка России) и договора присоединения (условия об ответственности, порядке разрешения споров). Пользователь, желающий получить доступ к системе, обязан принять эти правила целиком без возможности внесения изменений. Формально такая конструкция соответствует модели публичного договора или договора присоединения по статьям 428 и 426 ГК РФ, однако судебная практика признаёт возможность признания отдельных условий недействительными, если они существенно ущемляют права слабой стороны.

Типичные условия правил информационной системы о распределении рисков включают: ограничение ответственности оператора случаями умысла или грубой неосторожности; возложение на пользователя обязанности по обеспечению сохранности приватного ключа; отказ оператора от обязанности

по восстановлению доступа при утрате ключа; установление процедуры блокировки подозрительных транзакций; определение порядка взаимодействия с правоохранительными органами при выявлении инцидентов.

Проблема состоит в том, что такие условия зачастую формулируются в пользу оператора информационной системы, перекладывая основные риски на конечных пользователей. По оценкам исследователей, проанализировавших правила 15 российских операторов информационных систем, в 12 случаях условия об ответственности предусматривали практически полное освобождение оператора от обязанности возмещения убытков при инцидентах информационной безопасности [6].

Когда инцидент обусловлен недостатками самой информационной системы - уязвимостями в коде, ненадлежащей архитектурой безопасности, недостаточной защитой от DDoS-атак - ответственность должна возлагаться на оператора независимо от включённых в правила оговорок. Российское законодательство о защите прав потребителей (для физических лиц) и общие нормы о недопустимости злоупотребления правом (статья 10 ГК РФ) позволяют корректировать явно несправедливые условия.

Для институциональных участников рынка распространена практика заключения договоров страхования киберрисков. Такие договоры покрывают убытки от несанкционированного доступа к системам, утечки данных, атак программ-вымогателей, ошибок в коде. Однако российский рынок страхования цифровых активов находится на начальной стадии развития - страховщики опасаются непредсказуемости и масштабности киберугроз, а тарифы остаются высокими, что делает страхование недоступным для небольших операторов и частных инвесторов [7].

Смарт-контракты как инструмент автоматизированного распределения ответственности.

Смарт-контракты открывают принципиально новые возможности для управления рисками в экосистемах цифровых активов. Программный код может автоматически реализовывать условные обязательства: блокировать транзакции при превышении лимитов, перечислять компенсации при наступлении страховых случаев, возвращать средства при невыполнении контрагентом обязательств. Однако правовая квалификация смарт-контрактов остаётся дискуссионной.

Существуют две основные концепции. Согласно первой, смарт-контракт - это способ технического исполнения традиционного договора, своего рода «электронная форма сделки». В таком случае к смарт-контракту применяются общие положения договорного права, включая правила о форме, содержании, недействительности сделок. Вторая концепция трактует смарт-контракт как самостоятельное правовое явление - алгоритмически организованное правоотношение, где воля сторон выражена не в тексте, а в логике программного кода [8]. Большинство смарт-контрактов в реальных проектах представляют собой гибрид: юридически значимое соглашение оформляется традиционным письменным договором, а смарт-контракт используется для автоматизации отдельных аспектов исполнения.

Ключевая проблема смарт-контрактов - невозможность изменения условий после активации. Если в традиционном договоре стороны могут по соглашению внести изменения, расторгнуть договор или обратиться в суд для корректировки условий, то смарт-контракт, записанный в блокчейн, исполняется автоматически и необратимо. Это создаёт риск несправедливых результатов при изменении обстоятельств, ошибках в коде или непредвиденных ситуациях. В юридической литературе предлагается вводить в смарт-контракты «аварийные выходы» - функции приостановки или отмены исполнения при наступлении критических событий.

Зарубежная практика демонстрирует попытки создания «правовых оберток» для смарт-контрактов. В США ряд штатов (Аризона, Теннесси,

Вайоминг) принял законы, признающие юридическую силу смарт-контрактов и устанавливающие их соответствие требованиям к письменной форме сделок. В Европейском союзе Регламент о рынках криптоактивов (MiCA), вступивший в силу в 2024 году, предусматривает требования к раскрытию информации об алгоритмах функционирования смарт-контрактов и ответственность разработчиков за критические уязвимости [9]. Российскому законодателю целесообразно учитывать этот опыт при формировании национального регулирования.

Перспективные направления совершенствования механизмов защиты.

Для повышения эффективности частноправовой защиты цифровых активов необходим комплекс мер законодательного и институционального характера. Первостепенное значение имеет нормативное закрепление презумпции владения цифровым правом. В настоящее время правовой статус лица, обладающего приватным ключом, не определён - формально это может быть владелец, представитель, похититель. Законодательное установление презумпции, согласно которой лицо, имеющее доступ к приватному ключу, считается владельцем цифрового права до доказательства обратного, создаст правовую определённость и упростит защиту нарушенных прав.

Необходима институционализация смарт-контрактов в гражданском законодательстве. Целесообразно дополнить статью 434 ГК РФ положением о том, что договор может быть заключён путём записи программного кода в информационную систему, если такой код содержит все существенные условия соглашения и стороны согласовали его использование. Одновременно следует установить специальные правила об изменении и расторжении смарт-контрактов, в том числе судебном, с разработкой процедуры принудительной корректировки записей в блокчейне при вынесении соответствующего судебного решения.

Критически важно признание доказательственного значения блокчейн-записей. Действующее процессуальное законодательство относит электронные документы к допустимым доказательствам, однако судебная практика зачастую требует подтверждения подлинности электронной записи квалифицированной электронной подписью. Специфика блокчейна состоит в том, что подлинность и неизменность записи гарантируются криптографическим алгоритмом распределённого реестра, а не подписью уполномоченного лица. Внесение в процессуальные кодексы норм о признании записей в блокчейне достаточным доказательством факта совершения операции существенно упростит защиту прав участников оборота ЦФА [10].

Перспективной мерой является также создание института арбитража смарт-контрактов - включение в программный код механизма передачи спора на рассмотрение третьей стороны (арбитра или арбитражного органа) при возникновении предусмотренных обстоятельств. Решение арбитра может быть реализовано через специальную функцию в смарт-контракте, позволяющую разблокировать средства, перераспределить активы или приостановить исполнение. Такая модель сочетает преимущества автоматизации с гибкостью человеческого правоприменения.

На уровне саморегулирования необходимо формирование стандартов информационной безопасности для операторов информационных систем ЦФА. Стандарты должны охватывать требования к архитектуре информационной системы, процедуры управления криптографическими ключами (многофакторная аутентификация, мультиподпись, холодное хранение), мониторинг аномальных транзакций и реагирование на инциденты, аудит кода смарт-контрактов перед развёртыванием, а также процедуры восстановления после компрометации. Соблюдение стандартов может стимулироваться через механизмы рыночной репутации, страхование

(сниженные тарифы для сертифицированных операторов) и преференции при взаимодействии с институциональными инвесторами.

Заключение.

Информационная безопасность цифровых финансовых активов представляет собой комплексную проблему, находящуюся на стыке технологии, права и экономики. Специфика цифровых прав, существующих исключительно в информационных системах и контролируемых посредством криптографических ключей, создаёт новый профиль рисков, для управления которыми недостаточно традиционных правовых механизмов. Действующее российское законодательство сформировало базовую нормативную рамку для функционирования ЦФА, однако оставило нерешёнными ключевые вопросы распределения ответственности, идентификации владельцев, правовой квалификации смарт-контрактов и средств судебной защиты.

Частноправовые механизмы защиты в настоящее время реализуются преимущественно через договорные инструменты - правила информационных систем, соглашения между операторами и эмитентами, условия использования платформ. Однако асимметрия переговорных возможностей приводит к тому, что основные риски информационной безопасности перекладываются на конечных пользователей, что снижает доверие к цифровым активам и сдерживает развитие рынка. Необходимо законодательное установление минимальных стандартов защиты, которые не могут быть ослаблены договором, - по аналогии с императивными нормами защиты прав потребителей.

Перспективные направления совершенствования включают нормативное закрепление презумпции владения на основе обладания приватным ключом, институционализацию смарт-контрактов как формы договора с особыми правилами изменения и расторжения, признание доказательственного значения блокчейн-записей в судебных процессах. Эффективная модель частноправовой защиты цифровых активов должна

обеспечивать баланс между технологической автономностью, характерной для блокчейн-систем, и правовой определённостью, необходимой для защиты прав участников оборота. Дальнейшее исследование должно сосредоточиться на разработке конкретных механизмов принудительного исполнения судебных решений в отношении активов, зафиксированных в децентрализованных блокчейн-системах, а также на формировании процедур коллективной защиты прав инвесторов при массовых инцидентах информационной безопасности.

Список литературы:

1. Базис. Технологические инновации в цифровых договорах: влияние технологии блокчейн и искусственного интеллекта // Базис. 2025. № 1. С. 43–58. URL: https://cyberleninka.ru/article/n/tehnologicheskie-innovatsii-v-tsifrovyh-dogovorah-vliyanie-tehnologii-blokcheyn-i-iskusstvennogo-intellekta (дата обращения: 28.05.2026).

2. Белозорова Э.Н. Особенности регулирования цифровых финансовых активов в Российской Федерации // Финансы. 2025. № 8. С. 51–57.

3. Васильев А.С., Ильин И.В. Смарт-контракт как гражданско-правовой способ распоряжения цифровыми правами: проблемы теоретического обоснования и практического применения // Право и цифровая экономика. 2023. № 3. С. 25–39. URL: https://cyberleninka.ru/article/n/smart-kontrakt-kak-grazhdansko-pravovoy-sposob-rasporyazheniya-tsifrovymi-pravami-problemy-teoreticheskogo-obosnovaniya-i (дата обращения: 28.05.2026).

4. Дмитриева Г.К. Инновационные технологии и защита цифровых прав: роль блокчейна и смарт-контрактов // Юридическая наука. 2024. № 2. С. 112–127. URL: https://cyberleninka.ru/article/n/innovatsionnye-tehnologii-i-zaschita-tsifrovyh-prav-rol-blokcheyna-i-smart-kontraktov (дата обращения: 28.05.2026).

5. Ковалева М.А. Регулирование цифровых финансовых активов для предотвращения системных рисков экономической безопасности России //

Экономическая безопасность. 2024. № 1. С. 63–78. URL: https://cyberleninka.ru/article/n/regulirovanie-tsifrovyh-finansovyh-aktivov-dlya-predotvrascheniya-sistemnyh-riskov-ekonomicheskoy-bezopasnosti-rossii (дата обращения: 28.05.2026).

6. Лебедев К.К. Финтех и экономическая безопасность: правовые механизмы противодействия киберугрозам // Банковское право. 2024. № 3. С. 45–59. URL: https://cyberleninka.ru/article/n/finteh-i-ekonomicheskaya-bezopasnost-pravovye-mehanizmy-protivodeystviya-kiberugrozam (дата обращения: 28.05.2026).

7. Новикова Е.В. Правовое регулирование технологии блокчейн в российской правовой системе // Цифровое право. 2023. № 4. С. 88–103. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-tehnologii-blokcheyn-v-rossiyskoy-pravovoy-sisteme (дата обращения: 28.05.2026).

8. Савельев А.И. Правовые аспекты использования цифровых финансовых активов в международных расчётах // Международное публичное и частное право. 2024. № 2. С. 19–28. URL: https://cyberleninka.ru/article/n/pravovye-aspekty-ispolzovaniya-tsifrovyh-finansovyh-aktivov-v-mezhdunarodnyh-raschetah (дата обращения: 28.05.2026).

9. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (с изм. и доп.). URL: https://base.garant.ru/74451466/ (дата обращения: 28.05.2026).

10. Федеральный закон от 11.03.2024 № 45-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: https://www.garant.ru/products/ipo/prime/doc/408584757/ (дата обращения: 28.05.2026).

11. Цифровые финансовые активы в России: виды, правовое регулирование, операторы // Финансовое право. 2024. № 5. С. 67–82. URL:

https://cyberleninka.ru/article/n/tsifrovye-finansovye-aktivy-v-rossii-vidy-pravovoe-regulirovanie-operatory (дата обращения: 28.05.2026).

12. Цифровые финансовые активы разрешили использовать в международных расчётах // Официальный сайт Министерства финансов РФ. URL: https://minfin.gov.ru/ru/press-center/?id_4=38897 (дата обращения: 28.05.2026).

13. Цифровые финансовые активы и их операторы // Официальный сайт Банка России. URL: https://www.cbr.ru/finm_infrastructure/digital_oper/ (дата обращения: 28.05.2026).