

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2025, Том 17, № s2 / 2025, Vol. 17, Iss. s2 <https://esj.today/issue-s2-2025.html>

URL статьи: <https://esj.today/PDF/91FAVN225.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Бабанская, А. С. Угрозы и уязвимости легализации (отмывания) преступных доходов и финансирования терроризма в инфраструктурном секторе выпуска, учета и обращения цифровых финансовых активов / А. С. Бабанская // Вестник евразийской науки. — 2025. — Т. 17. — № s2. — URL: <https://esj.today/PDF/91FAVN225.pdf>.

For citation:

Babanskaya A.S. Threats and vulnerabilities of legalization (laundering) of criminal proceeds and financing of terrorism in the infrastructure sector of issuance, accounting and circulation of digital financial assets. 2025;17(s2): 91FAVN225. Available at: <https://esj.today/PDF/91FAVN225.pdf>. (In Russ., abstract in Eng.).

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации»

УДК 346.546

Бабанская Анастасия Сергеевна

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Институт экономической политики и проблем экономической безопасности
Ведущий научный сотрудник, доцент
Кандидат экономических наук
E-mail: banasti@mail.ru

РИНЦ: https://elibrary.ru/author_profile.asp?id=754154

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=57216711030>

Угрозы и уязвимости легализации (отмывания) преступных доходов и финансирования терроризма в инфраструктурном секторе выпуска, учета и обращения цифровых финансовых активов

Аннотация. В статье проводится комплексный обзор проблем незаконного использования элементов инфраструктурного сектора цифровых финансовых активов (ЦФА) и обосновываются их внешние и внутренние уязвимости. Актуальность исследования обусловлена стремительным развитием рынка ЦФА при недостаточной зрелости регуляторных механизмов, что создает значительные возможности для их криминального использования. Цель — выявление, классификация и систематизация ключевых уязвимостей и угроз инфраструктурного сектора ЦФА, способствующих рискам отмывания денежных средств и финансирования терроризма (ОД/ФТ). Методологическую основу работы составляют анализ отчетов FATF и других международных организаций, изучение судебной практики по делам, связанным с незаконными операциями с ЦФА, а также обзор современных научных и аналитических публикаций. На основе анализа реальных кейсов и научных исследований выявлены наиболее распространенные схемы использования ЦФА для ОД/ФТ. В ходе исследования систематизированы ключевые уязвимости инфраструктуры ЦФА, которые классифицированы на внешние (регуляторные пробелы, технологические риски блокчейн-систем, трансграничный характер операций) и внутренние (недостатки систем комплаенса, слабая идентификация пользователей, уязвимости смарт-контрактов и угрозы кибербезопасности, проблемы изолированности цифровых платформ друг от друга). Основным результатом исследования является классификация уязвимостей инфраструктурного сектора ЦФА, что

позволят выработать научно обоснованные рекомендации по повышению устойчивости инфраструктуры ЦФА к угрозам использования их в незаконных целях, особенно с учетом российской специфики рынка ЦФА. Исследование вносит вклад в развитие методики оценки угроз и рисков ОД/ФТ в условиях цифровизации финансовой системы. Полученные выводы имеют практическую ценность для исследователей, регуляторов, участников рынка цифровых финансовых активов и правоохранительных органов, занимающихся противодействием экономическим преступлениям.

Ключевые слова: угрозы; уязвимости; легализация (отмывание) преступных доходов; финансирование терроризма; цифровые финансовые активы; инфраструктурный сектор

Введение

По мере ускорения цифровой трансформации и внедрения финансовыми учреждениями новых технологий возрастает и интерес мошенников к новым инструментам финансирования. Федеральный закон о цифровых финансовых активах (ЦФА)¹ вступил в силу в январе 2021 года, однако реальное функционирование рынка цифровых активов началось только летом 2022 года, когда произошли их первые выпуски. Несмотря на относительную новизну данных финансовых продуктов, рынок ЦФА за последние годы демонстрирует экспоненциальный рост, что свидетельствует о его высокой адаптивности и инвестиционной привлекательности.

Однако трансграничная природа операций с ЦФА, обеспечивая беспрецедентную скорость и доступность расчетов, одновременно создает новые возможности для киберпреступности, усложняя регуляторный контроль и повышая риски финансовых злоупотреблений. Стремительное развитие цифровых финансовых активов (ЦФА) и их интеграция в экономические процессы создают новые вызовы для систем противодействия отмыванию доходов (ПОД) и финансированию терроризма (ФТ).

Инфраструктурный сектор выпуска, учета и обращения ЦФА, включая токенизированные активы и иные формы цифровых ценностей, обладает специфическими уязвимостями, которые могут быть использованы преступными структурами для получения и легализации незаконных доходов.

Сложная природа цифровых финансовых активов и различия в международных подходах к их выпуску, учету и обращению усложняют усилия по регулированию. В условиях недостаточной зрелости нормативно-правового регулирования и технологических особенностей ЦФА, актуализируется необходимость системного анализа угроз и разработки эффективных механизмов их минимизации, что обуславливает актуальность данного исследования.

Целью настоящего исследования является выявление, классификация и систематизация ключевых уязвимостей и угроз инфраструктурного сектора ЦФА, способствующих рискам отмывания денежных средств и финансирования терроризма (ОД/ФТ).

Объектом исследования выступают цифровые финансовые активы и инфраструктурный сектор их выпуска, учета и обращения. Предметом — угрозы и уязвимости легализации (отмывания) преступных доходов и финансирования терроризма в инфраструктурном секторе выпуска, учета и обращения цифровых финансовых активов.

¹ Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Режим доступа — URL: https://www.consultant.ru/document/cons_doc_LAW_358753/?ysclid=m99p47lsds177207089 (дата обращения 01.04.2025).

Теоретическая значимость работы заключается в структурировании угроз ОД/ФТ и уязвимостей инфраструктурного сектора обращения ЦФА, разработке их комплексной классификации. Практическая ценность исследования определяется возможностью применения его результатов регуляторами, участниками рынка ЦФА и правоохранительными органами для совершенствования мер противодействия преступным схемам.

Основным результатом исследования является классификация уязвимостей инфраструктурного сектора ЦФА, что позволит выработать научно обоснованные рекомендации по повышению устойчивости экосистемы ЦФА к угрозам использования их в незаконных целях, особенно с учетом российской специфики инфраструктуры ЦФА.

1. Методы и материалы

Методологическую основу исследования составляют анализ отчетов FATF и других международных организаций по регулированию ЦФА, изучение международной практики в части незаконных операций с использованием ЦФА, обзор современных аналитических и научных публикаций по проблемам ПОД/ФТ в данном сегменте.

В работе решаются следующие задачи:

1. Обзор структуры и особенностей функционирования инфраструктурного сектора выпуска, учета и обращения цифровых финансовых активов.
2. Анализ реальных случаев незаконного использования ЦФА на основе международного опыта, в том числе обзор проблемной практики в инфраструктурном секторе криптовалют.
3. Формирование перечня и классификация уязвимостей с учетом особенностей инфраструктурного сектора обращения ЦФА.

Проблема использования ЦФА в схемах ОД/ФТ находится в фокусе внимания различных международных организаций и научного сообщества.

Основополагающими международными документами в области регулирования рисков ОД/ФТ применительно к ЦФА выступают публикации FATF. Так в отчете «Виртуальные активы и провайдеры услуг виртуальных активов» («Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers», 2021)² подробно рассматриваются уязвимости различных финансовых активов, в том числе криптоактивов, включая анонимность транзакций, трансграничный характер операций и недостатки систем комплаенс-контроля. Дополнительный анализ представлен в докладе ОЭСР «Налогообложение виртуальных валют: обзор налоговых режимов и возникающих вопросов налоговой политики» («Taxing Virtual Currencies», 2020)³, где особое внимание уделено налоговым рискам и схемам уклонения от налогообложения с использованием ЦФА.⁴

² FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. Режим доступа — URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf> (дата обращения 01.04.2025).

³ OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues, OECD, Paris. Режим доступа — URL: <https://www.skadden.com/-/media/files/publications/2020/10/the-distributed-ledger/taxingvirtualcurrenciesanoverviewoftaxtreatmentsan.pdf> (дата обращения 01.04.2025).

⁴ Банк России. Децентрализованные финансы Москва 2022. Режим доступа — URL: https://cbr.ru/Content/Document/File/141992/report_07112022.pdf (дата обращения 01.04.2025).

Надо отметить, что во многих государствах все многообразие видов и форм виртуальных активов (включая цифровые финансовые активы, криптовалюты и пр.) находятся в одном поле правового регулирования. Поэтому возникают угрозы использования регуляторных лазеек при осуществлении трансграничных операций с ЦФА, что подчеркивается в Отчете ОЭСР «Регуляторные подходы к токенизации активов» («Regulatory Approaches to the Tokenisation of Assets», 2021).⁵

В научной литературе выделяются несколько направлений изучения проблематики использования ЦФА в неправомерных целях. Общее упоминания экономической природы, регулирования оборота и рисков ЦФА рассмотрены в работах Караниной Е.В. [1], Жиронкин С.А., Сафиуллин Л.Н., Коновалова М.Е., Кузьмина О.Ю. [2] Мнацакян Л.С., Гамиловская А.А. [3] Апостолов А. [4]. Проблемы технологических уязвимостей поднимаются в работах Tschorsch и Scheuermann [5], A. Joshi, M. Han Y. Wang [6] Авторы Mustafa Ababneh, Ayat Aljarrah [7] рассматривают обратную ситуацию, как использование цифровых технологий помогает в обеспечении безопасности расчетов и минимизирует уязвимости системы. Авторы анализируют риски, связанные с особенностями блокчейн-технологий, включая возможность манипуляций смарт-контрактами и уязвимости консенсус-алгоритмов. Акценты на регуляторных пробелах широко представлены в исследованиях Arner D. W., Auer R., Frost J. [8] М.Г. Гирич, И.С. Ермохин, А.Д. Левашенко, Костян О.А. [9] Шубенкова К.В. [10] Авторы обращают внимание на проблемы фрагментированного регулирования и разницы в подходах к регулированию ЦФА на международном уровне с учетом возможностей трансграничных операций с ЦФА. Криминологические аспекты незаконного использования цифровых активов и криптовалют представлены в работах Raquet-Clouston и др. [11], Хоружий Л.И. [12] где авторы систематизируют общие подходы к мошенничеству с финансовой информацией и специфические схемы их использования в Darknet и для ransomware-атак, рассматривают способы организации сложных мошенничеств за счет манипулирования цифровыми активами.

Изучение материалов уголовных дел демонстрирует эволюцию методов использования цифровых активов в преступных целях — от простого обмена на фиатные валюты до сложных схем с микшированием транзакций и децентрализованными биржами [13].

Публикации Deloitte⁶, Chainalysis⁷ содержат анализ отраслевой специфики рисков ОД/ФТ только в части криптоактивов и игровой валюты. Например, в банковском секторе основной проблемой выступает обналичивание криптоактивов через корреспондентские счета, для игровой индустрии характерно использование NFT для обхода санкционных ограничений, упоминаются случаи оплаты санкционных товаров в криптовалюте.

Таким образом, с учетом быстрого развития технологий и рынка ЦФА отмечается многоаспектность проблемы появления новых схем их криминального использования для целей ОД/ФТ. Поэтому важным шагом при обеспечении безопасности операций с ЦФА становится комплексное представление угроз и уязвимостей.

⁵ OECD (2021) Organisation for Economic Co-operation and Development Regulatory Approaches to the Tokenisation of Assets. OECD Blockchain Policy Series. Режим доступа — URL: <https://cognizium.io/uploads/resources/OECD%20-%20Regulatory%20Approaches%20to%20the%20Tokenisation%20of%20Assets%20-%202021%20-%20Feb.pdf> (дата обращения 01.04.2025).

⁶ Deloitte. (2021). Disruptive Digital Technologies in the Financial Services Industry. Режим доступа — URL: <https://www2.deloitte.com/us/en/pages/financial-services/articles/disruptive-digital-technologies-in-the-financial-services-industry.html> (дата обращения 01.04.2025).

⁷ Chainalysis. (2022). The 2022 Crypto Crime Report. February 2022. Режим доступа — URL: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf> (дата обращения 01.04.2025).

2. Результаты и обсуждение

Российский рынок ЦФА ежегодно показывает стремительные темпы роста (рис. 1), например, за 2024 год относительно 2023 рынок ЦФА вырос более чем в 8 раз. В рыночной динамике ЦФА за 2024 год наблюдаются сезонные колебания, с ноября по февраль и в июле наблюдались периоды спада, в то время как в мае, августе и сентябре рынок ЦФА рос наиболее быстрыми темпами. Это говорит о наличии инвестиционных циклов на рынке ЦФА, которые можно объяснить сочетанием макроэкономических циклов, фискальным закрытием года, налоговыми периодами и снижением активности эмитентов в отпускные и праздничные периоды.

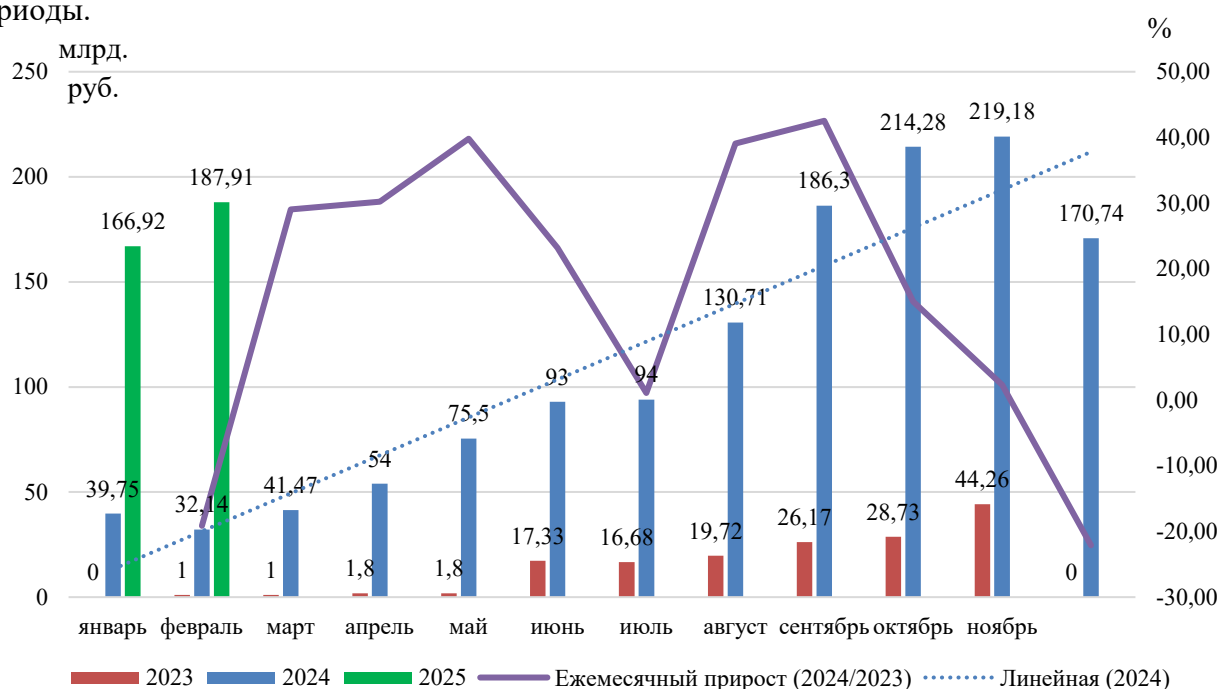


Рисунок 1. Динамика объема рынка ЦФА в России с января 2023 по февраль 2025, млрд руб. (ежемесячный прирост в %) (составлено автором на основе данных⁸)

По состоянию на февраль 2025 года объем российского рынка ЦФА оценивается в 187,91 млрд рублей.² Для сравнения только за 2024 год ущерб россиянам от кибермошенничества составил более 295 млрд рублей. Закономерно, что такое интенсивное развитие ЦФА влечет угрозу отставания темпов формирования эффективных механизмов для их защиты, а становление инфраструктуры может способствовать эксплуатации имеющихся уязвимостей со стороны мошенников.

Типология, структура и проблемное поле инфраструктурного сектора выпуска, учета и обращения цифровых финансовых активов

Регулированием ЦФА занимается Банк России обеспечивая высокий уровень безопасности и управления рисками ОД/ФТ.⁹ В отличие от других стран в России дробление ЦФА не предусмотрено и не регламентируется законодательством. Хотя на платформе оператора информационной системы ООО «Атомайз» упоминается о возможности дробления

⁸ База данных Cbonds. Режим доступа — URL: <https://cbonds.ru/dfa/> (дата обращения 03.04.2025).

⁹ ФЗ — № 259 от 31.07.2020 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

и формирования диверсифицированной корзины из разных ЦФА. В исследовании Jang, Lee, Chung, Park, Shin [14] авторы пришли к выводу, что неполные токены в токенизаторах байтового парного кодирования (BPE) на уровне байтов значительно более склонны к возникновению аномалий по сравнению с полными токенами. Уязвимости неполных токенов, присутствующих в токенизаторах BPE на уровне байтов.

В России урегулированы два способа токенизации активов:

- во-первых, путем выпуска ЦФА на существующие ценные бумаги, в этом случае задействована традиционная инфраструктура рынка ценных бумаг;
- во-вторых, путем выпуска акций в DLT-системе, где происходит учет и хранение таких акций без необходимости использования центрального депозитария.¹⁰

Мировыми аналогами отечественных ЦФА являются следующие активы: NFT (Невзаимозаменяемые токены), Security Tokens (Токены безопасности), Utility Tokens (Сервисные токены), Asset Tokens (Токены-активы). Поэтому одним из проблемных вопросов для Банка России остается квалификация иностранных цифровых инструментов в качестве ЦФА на предмет их соответствия принципам регулирования, закрепленным в российском законодательстве.

Полный жизненный цикл сделок с ЦФА включает в себя выпуск актива эмитентом, его первичное приобретение инвестором, обращение актива на платформе, его продажу на вторичном рынке и итоговое погашение актива (рис. 2).

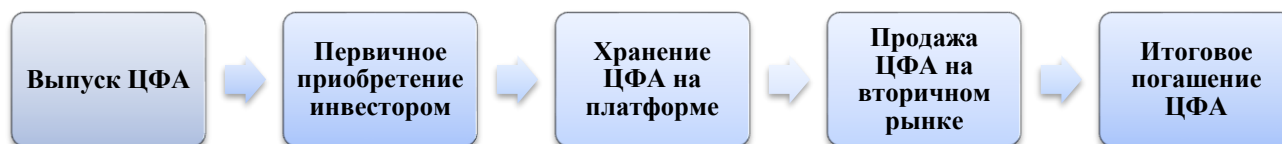


Рисунок 2. Жизненный цикл обращения ЦФА (составлено автором)

На разных этапах жизненного цикла ЦФА задействованы различные элементы инфраструктуры. К основным из них можно отнести: Эмитентов, осуществляющих эмиссию ЦФА; Инвесторов, приобретающих ЦФА (квалифицированные и неквалифицированные); Банк России и органы государственного финансового контроля, осуществляющие контроль и регулирование операций с ЦФА; операторов информационной системы, обеспечивающие выпуск и хранение ЦФА, операторов обмена в обязанности которых входит оформление сделок купли-продажи ЦФА (табл. 1).

Ключевыми участниками являются: оператор информационной системы (ОИС) — инфраструктурный игрок, выполняющий функцию депозитария, и оператор обмена (ОО) — своеобразная биржа, которая взаимодействует с пользователем через приложение. Оператор выпуска ЦФА одновременно может быть оператором обмена. Другими словами, ОИС отвечает за создание и поддержание ИТ-инфраструктуры, а также за хранение и неизменность данных, а ОО — за привлечение пользователей и организацию торгов через «интерфейс-витрину». В реестре Банка России к операторам информационных систем, уполномоченным на выпуск ЦФА, по состоянию на 08.04.2025 значатся 15 компаний. По данным ассоциации российских банков лидером по выпуску ЦФА с долей рынка 49 % является ООО «Атомайз».¹¹

¹⁰ Basar, S. INX ATS Prepared for Securities Token Listings / Newsletter. Режим доступа — URL: <https://www.marketmedia.com/inx-ats-prepared-for-securities-token-listings/> (дата обращения 04.04.2025).

¹¹ Российский рынок ЦФА. Итоги, тренды и бизнес-кейсы 16.01.2024. Режим доступа — URL: https://arb.ru/b2b/pointofview/rossiyskiy_rynok_tsfa_itogi_trendy_i_biznes_keyisy-10663679/?ysclid=m99r63ddd0662348404 (дата обращения 08.04.2025).

Таблица 1

Проблемное поле отдельных инфраструктурных элементов ЦФА в России

Элемент	Субъекты инфраструктуры	Описание	Ключевые участники	Проблемное поле для Од/ФТ
Контрольный	Регуляторы и надзорные органы	Государственные институты, регулирующие и контролирующие оборот ЦФА	Банк России, Росфинмониторинг, Минфин РФ	Недостаточная скорость реагирования, законодательные лазейки, пробелы в регулировании
Учетный	Операторы информационной системы (ОИС)	Юридические лица (российские), включенные Банком России в реестр таких операторов	ООО «Атомайз», ПАО Сбербанк, ООО «Лайтхаус», АО «Альфа-банк», ООО «Системы распределенного реестра», ООО «Токены», Т-Банк, ООО ВТБ Капитал Трейдинг, ПАО «СПБ Биржа» и др.	Возможность выпуска токенов для сомнительных активов. Недостаточная верификация клиентов (KYC), уязвимости удаленного прохождения процедуры идентификации клиента в целях предупреждения и недопущения использования преступных схем.
Торговый	Операторы обмена данных о ЦФА (ОО)	Юридические лица (российские), уполномоченные выпускать и учитывать ЦФА (включенные в реестр операторов обмена ЦФА) Имеют самостоятельную платформа с собственными технологическими решениями и уникальным распределенным реестром	В России их всего два: ПАО «Московская Биржа», ПАО «СПБ Биржа»	Уязвимости смарт-контрактов, возможность манипуляций с реестром сделок с ЦФА
Информационный	Участники сети — Узлы информационной системы	Пользователи информационной системы, владеющие узлом (узлами) на основе распределенного реестра, обеспечивающие тождественность информации, содержащейся в указанной информационной системе	Юридические лица или индивидуальные предприниматели, зарегистрированные в соответствии с законодательством РФ	Уязвимости распределенного реестра. Взломы и утечки данных. Риск уязвимости смарт-контрактов, ошибки в работе систем обмена информацией между блокчейнами и внешним миром, риски концентрации управления протоколом
Вспомогательный	Организаторы инфраструктуры	Обеспечивают функционирование основных инфраструктурных элементов	Удостоверяющий центр, разработчик платформы, сертификация ПО, лицензии ФСБ на работу со средствами криптографической защиты информации (СКЗИ)	Отсутствие соответствующего лицензирования. Взломы и утечки данных. Вирусное ПО. Использование подставных кошельков

Составлено авторами по результату обзора¹²

Оператор обмена подключается к оператору информационной системы, разворачивая в своей инфраструктуре узел распределенного реестра, и получает все преимущества технологии для торговли цифровыми финансовыми активами.

¹² ФЗ от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Atomyze. Цифровые финансовые активы. Версия 2.0. 2024. 70с. Режим доступа — URL: <https://atomyze.ru/files/20240812-Kniga-DFA-mobile.pdf> (дата обращения 08.04.2025).

Банк России (2022). Консультационный доклад «Развитие рынка цифровых активов в РФ». Режим доступа — URL: http://www.cbr.ru/Content/Document/File/141991/Consultation_Paper_07112022.pdf (дата обращения 04.02.2025).

ЦФА ХАБ. Правила информационной системы ООО «Блокчейн Хаб». 2023. 64 с. Режим доступа — URL: <https://www.cbr.ru/Queries/XsltBlock/File/98365/1460> (дата обращения 08.04.2025).

При обращении ЦФА для поддержания работоспособности всей инфраструктурной системы могут принимать участие прочие субъекты, предоставляющие узлы информационной системы и взаимодействия, удостоверяющие центры, разработчики платформ, органы по сертификации ПО и лицензированию работы со средствами криптографической защиты информации (СКЗИ).

Таким образом, российская инфраструктура ЦФА фрагментирована и сочетает контрольные, учетные, товарные, информационные и вспомогательные элементы. При этом степень их регулирования и контроля различная в ключевых и прочих субъектах. В целом проблемное поле использования ЦФА в целях ОД/ФТ связано с: регуляторными аспектами, манипуляций с удаленным прохождением процедуры идентификации клиента и ограниченности KYC-контроля, техническим уязвимостям смарт-контрактов, распределенного реестра, манипуляций с реестром сделок с ЦФА и угрозами информационной безопасности в виде взломов и утечек данных, вирусного ПО. Так же в отчетах Банка России и по мнению отдельных авторов отмечаются повышенные угрозы технологии DeFi ввиду незрелости KYC-процедур.

Так же в качестве проблем можно отметить отсутствие правового и технического механизма использования ЦФА для международных расчетов и слабую совместимость информационных платформ у различных ОИС, что вынуждает инвестора регистрироваться у разных операторов и может быть использовано как уязвимость с целью ОД/ФТ.

В России, в соответствии со ст. 2 ФЗ № 259 от 31.07.2020, выпуск ЦФА осуществляется путем внесения в информационную систему, в которой выпускаются ЦФА, записи об их зачислении указанному лицу. То есть выпуск может осуществляться простой записью в DLT — реестре через информационную систему оператора выпуска ЦФА. Для выпуска ЦФА эмитенту достаточно пройти идентификацию и опубликовать на сайте оператора и на своем сайте единственный документ — решение о выпуске ЦФА. В нем указывается основная информация об активе и эмитенте. Для сравнения в международной практике отдельных стран должны соблюдать требования к регистрации проспекта ценных бумаг в соответствующих органах, а также соблюдать другие требования законодательства о ценных бумагах и финансовых инструментах.

Учет и хранение ЦФА осуществляется в DLT-реестре на основе внесения соответствующих записей. Если ЦФА выпускаются на существующие ценные бумаги, то они будут храниться у традиционных депозитариев. В международной практике допускается конвертация ЦФА и классических ценных бумаг, а в России на основании ст. 13 ФЗ № 259 от 31.07.2020 установлен запрет на подобные операции. Закономерно, что дальнейшее развитие рынка ЦФА пойдет по пути интеграции и объединения/обмена информацией из реестров владельцев ценных бумаг от лица, осуществляющего традиционное хранение и учет биржевых ценных бумаг и реестров владельцев ЦФА в информационной системе оператора выпуска ЦФА, что усилит уязвимости каналов обмена данными.

На рынке ЦФА применяются практики идентификации и ПОД/ФТ, контроля операционной надежности и информационной безопасности.¹³ Для целей ФЗ 115-ФЗ любая цифровая валюта признается имуществом, а в соответствии со ст. 6, п. 1, пп. 5) операции с цифровыми финансовыми активами подлежат обязательному контролю. Так же в целях обеспечения безопасности не допускается обналичивания ЦФА, а деньги с кошелька ЦФА можно вывести только на банковский счет, принадлежащий владельцу кошелька ЦФА. В

¹³ Atomyze. Цифровые финансовые активы. Версия 2.0. 2024. 70 с. Режим доступа — URL: <https://atomyze.ru/files/20240812-Kniga-DFA-mobile.pdf> (дата обращения 09.04.2025).

перспективе массовое обращение цифрового рубля так же может стать выходом для конвертации ЦФА.

При этом ключевым условием является возможность удаленного прохождения процедуры идентификации клиента в целях ПОД/ФТ. В настоящее время в соответствии с ФЗ от 07.08.2001 № 115-ФЗ «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма» для операторов информационных систем уже предусмотрена возможность делегирования идентификации профессиональным участникам рынка ценных бумаг (брокерам), имеющим статус оператора обмена цифровых финансовых активов. Современный инструментарий по сделкам с ЦФА включает такие способы идентификации пользователей, как: удаленная биометрическая идентификация клиента (аналог его личной явки); применение упрощенной идентификации с использованием Единой системы идентификации и аутентификации (ЕСИА); использование делегированной идентификации. При этом механизм упрощенной идентификации через ЕСИА уже доступен для клиентов инвестиционных платформ, на которых могут выпускаться утилитарные цифровые права (УЦП) и регламентируется ФЗ от 07.08.2001 № 115-ФЗ «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма».¹⁴

Так же повышенные риски незаконного использования ЦФА формируются в системе распределенных финансов на платформах децентрализованного финансирования (DeFi). Несмотря на растущую глобальную осведомленность о финансовых преступлениях на рынках цифровых активов (как криптовалют, так и ЦФА) и развитии требований ПОД/ФТ в отношении новых финансовых инструментов, многим платформам децентрализованного финансирования (DeFi) по-прежнему не хватает надежных протоколов по борьбе с отмыванием денег (AML). По сравнению с традиционными финансовыми учреждениями, которые подчиняются строгим требованиям AML и KYC, на платформах децентрализованного финансирования эти стандарты слабо применяются. Так, например, консалтинговая компания Технологии доверия видят выход из этой ситуации за счет развития ЦФА-ориентированных продуктов KYC/AML с использованием блокчейн-платформы с государственным регулированием (хаб проведения KYC/AML на базе Банка России).¹⁵

Схемы незаконного использования ЦФА и проблемы инфраструктурного сектора в части ПОД/ФТ

Рассмотрим международные кейсы, проблемы и ситуации использования цифровых активов, в т. ч. ЦФА для целей ОД/ФТ.

1. Пирамиды. Распространенные методы мошенничества с цифровыми активами — финансовые пирамиды и фиктивные инвестиционные платформы. Эта проблема так же широко освещена в научных трудах Doli & Kollwitz [16]. Один из самых распространенных методов мошенничества с цифровыми активами — это схема Понци, где более ранним Инвесторам достается доход за счет средств вновь привлеченных участников. Финансовые пирамиды с ЦФА часто рассматриваются под видом легитимных коммерческих фирм или проектов, часто принимают форму первоначальных предложений монет (ICO), распространены на платформах децентрализованного финансирования (DeFi) и в секторах взаимозаменяемых токенов (NFT).

¹⁴ Банк России РАЗВИТИЕ РЫНКА ЦИФРОВЫХ АКТИВОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ Доклад для общественных консультаций Москва 2022. Режим доступа — URL: http://www.cbr.ru/Content/Document/File/141991/Consultation_Paper_07112022.pdf (дата обращения 09.04.2025).

¹⁵ Технологии Доверия. Новое золото. Цифровое будущее финансовых активов. Режим доступа — URL: <https://data.tedo.ru/publications/digital-financial-assets.pdf> (дата обращения 09.04.2025).

Мошенники используют яркие веб-сайты, дополнительные отзывы и агрессивные маркетинговые тактики.

В децентрализованных экосистемах, где низкие или формальные требования AML и KYC создатели токенов действуют безответственно. Описаны случаи «перетягивания ковра» (rug pulls), которые часто ассоциируют с проектами, когда эмитенты внезапно исчезают, оставляя инвесторов ни с чем. Например, в работе Doli & Kollwitz, описан случай, когда разработчики выпускают новый токен или проект, создают ажиотаж с помощью рекламы в социальных сетях, поддержки влиятельных, известных лиц и добиваются роста продаж. Как только собрано достаточно средств, разработчики внезапно исчезают, фактически изымая инвестиционные средства «вытягивая их на себя», оставляя инвесторам лишь бесполезные токены и пустые обещания.

В сентябре 2024 года Банк России так же сообщил о попытке размещения первого актива с признаками финансовой пирамиды на рынке цифровых финансовых активов (ЦФА). Организация не успела привлечь средства, а потенциальные инвесторы не понесли ущерб. Однако данный случай доказывает необходимость усиления контроля за размещением активов на цифровых платформах, востребованность процедур AML и KYC по всей цепочке транзакций.¹⁶

2. Фишинг и методы социальной инженерии. Преступники маскируются под официальные цифровые платформы, провайдеров кошельков или авторитетных операторов, чтобы вынудить жертв передать приватные ключи либо отправить средства на контролируемые ими адреса. Отдельную угрозу представляют методы социальной инженерии, включая деятельность фальшивых операторов службы поддержки, которые под предлогом помощи получают доступ к конфиденциальной информации пользователей, что влечет за собой несанкционированное списание активов.

Платформа по информационной безопасности ZeroFox следующим образом описывает происшествие. Во время заключения контракта на OpenSea, одном из крупнейших рынков NFT, киберпреступники отправляли фишинговые письма, имитирующие официальные сообщения, обманывая инвесторов и заставляя их посещать фишинговые веб-сайты и подписывать мошеннические транзакции. Таким образом киберпреступники смогли украсть сотни громких NFT на общую сумму 2 млн долларов США.¹⁷

3. Схемы Pump-and-Dump. Манипуляция рынком — ключевая стратегия, используемая мошенниками для создания искусственного спроса и повышения цен на цифровые активы. В исследовании Tao Li, Donghwa Shin, Baolian Wang [17] данные схемы описаны на примере рынка криптовалют. Реализации схем pump-and-dump способствуют отсутствие или слабый контроль, непрозрачность и техническая сложность криптовалют. В исследовании осуществлялось наблюдение за двумя платформами группового обмена сообщениями, популярными среди инвесторов в криптовалюту, в результате за шесть месяцев 2018 года было выявлено более 3 400 схем pump-and-dump. В качестве решения в 2021 году Комиссия по торговле товарными фьючерсами США (CFTC) обнародовала программу, которая позволяет любому информатору получить денежное вознаграждение в размере от 10 % до 30 %, если он

¹⁶ РБК. Андрей Лузгин. В ЦБ рассказали о попытке разместить пирамиду на платформе для ЦФА. 05 сентября 2024. Режим доступа — URL: <https://www.rbc.ru/crypto/news/66d9ab749a794726f06d7a8c> (дата обращения 10.04.2025).

¹⁷ ZeroFox Intelligence. 3 Social Engineering Tactics Targeting the Financial Services Industry. February 24, 2025. Режим доступа — URL: <https://www.zerofox.com/blog/3-social-engineering-tactics-targeting-the-financial-services-industry/> (дата обращения 10.04.2025).

раскрывает меры принудительного манипулирования рынком, которые приводят к денежным убыткам в размере от 1 миллиона долларов.¹⁸

4. Кибербезопасность и взлом цифровых платформ. Цифровые платформы с ростом объемов децентрализованных финансов и рынков цифровых активов часто становятся привлекательными объектами для кибератак. Примером является инцидент взлома биржи Mt. Gox (2014), в результате которого было потеряно около 850 000 биткойнов.¹⁹ С тех пор платформы цифровых активов регулярно сталкиваются с многочисленными нарушениями безопасности, включая фишинговые атаки, взломы кошельков и эксплойты протоколов децентрализованных финансов (DeFi). Согласно исследованиям, эти инциденты подчеркивают важность внедрения надежных методов кибербезопасности, таких как сквозное шифрование, защищенные кошельки и протоколы с несколькими подписями, многофакторной аутентификацией для защиты активов пользователей.

5. Программы-вымогатели, усовершенствованные постоянные угрозы (APT). В исследовании Agulkumaran, Mangal, Singh, Jain, Agarwal & Taqa. отмечается возрастающие случаи все более сложных киберугроз, включая атаки программ-вымогателей и усовершенствованные постоянные угрозы (APT) во всех секторах экономики. Поэтому традиционные меры безопасности, когда-то достаточные для отражения основных киберугроз, теперь не обладают гибкостью, необходимой для противодействия усовершенствованным и постоянным атакам. Авторы подчеркивают необходимость перехода от реактивных к проактивным подходам защиты и использование таких технологий, как искусственный интеллект (ИИ) для обнаружения угроз, предиктивная аналитика и поведенческий анализ, которые помогают предотвращать атаки до их реализации.

6. В исследовании Park, Youm [18] авторы предлагают свою модель обслуживания для токенов безопасности на основе блокчейна и выделяют для нее следующие уязвимости:

(УБ-1) Обман, связанный с количеством выпущенных токенов безопасности. Эмитент может фальсифицировать количество выпущенных токенов безопасности, например, выпустить токены безопасности на сумму большую или меньшую, чем инвестиции. Эта угроза может привести как к отмыванию денег с использованием токенов безопасности, так и к хищению инвестиций.

(УБ-2) Обман, связанный с количеством отозванных токенов безопасности. Эмитент может фальсифицировать количество отозванных токенов безопасности. Например, отозвать токены безопасности на сумму, меньшую, чем сумма выпущенных токенов безопасности. Эта угроза может привести к отмыванию денег с использованием токенов безопасности.

(УБ-3) Несанкционированная передача токенов безопасности. неблагонадежный кастодиан, осуществляющий хранение ценных бумаг, может передавать токены безопасности без разрешения держателя. Эта угроза может привести к отмыванию денег и хищению с использованием токенов безопасности.

(УБ-4 и УБ-5) Утечка персональных данных из объектов инфраструктуры. Огромная база персональных данных инвесторов и владельцев цифровых активов, реестры сделок могут быть украдены у операторов цифровых платформ, в том числе через поставщиков

¹⁸ Rajeev Dhir. Pump-and-Dump: Definition, How the Scheme is Illegal, and Types. Investopedia. January 13, 2022. Режим доступа — URL: <https://www.investopedia.com/terms/p/pumpanddump.asp> (дата обращения 10.04.2025).

¹⁹ РБК. Андрей Лузгин. Биткойны Mt.Gox. Как продажа монет на самом деле повлияет на рынок. 27 апреля 2023. Режим доступа — URL: <https://www.rbc.ru/crypto/news/644a6b0d9a79470c765273a7?from=copyhttps://www.rbc.ru/crypto/news/644a6b0d9a79470c765273a7> (дата обращения 10.04.2025).

информационных услуг, которые хранят и поддерживают идентификационную информацию инвесторов и владельцев активов, торговых реестров. Эта угроза может вызвать усиление фишинговых атак и программ-вымогателей.

(УБ-6) **Злонамеренное поведение.** Владелец ЦФА может фальсифицировать цену своего актива при регистрации в ОИС или зарегистрировать активы других людей посредством кражи личных данных и документов или выставить ЦФА не обеспеченный должными активами. Эта угроза может вызвать финансовые проблемы как у инвестора, так и у ОИС.

7. Скорость операций. Авторы Ababneh, Aljarrah приходят к выводу, что текущие модели приложений на основе блокчейна не способны удовлетворить требуемый уровень защиты данных в цифровых активах с точки зрения низкой задержки и высокой пропускной способности, то есть несоответствия времени операции и принятия регулирующих мер. Таким образом, для ключевых операций с ЦФА требуется высокопроизводительная и безопасная модель на основе блокчейна.

Классификация уязвимостей инфраструктурного сектора ЦФА в рамках ПОД/ФТ

На основе рассмотренных исследований и международных кейсов незаконного использования ЦФА сформирован перечень уязвимостей, характерный для ЦФА. В таблице 2 представлена детальная систематизация уязвимостей инфраструктурного сектора, способствующих использованию ЦФА для целей ОД/ФТ. Классификация охватывает внешние (экзогенные) и внутренние (эндогенные) уязвимости, их характеристики, примеры эксплуатации и возможные последствия.

Таблица 2

Общая классификация уязвимостей ЦФА

Критерий	Виды уязвимостей ЦФА	
По источнику	<ul style="list-style-type: none"> — Технологические (например, уязвимости блокчейна) — Регуляторные (пробелы в законодательстве ЦФА) — Организационные (недостатки внутреннего контроля) 	
По уровню воздействия	<ul style="list-style-type: none"> — Глобальные (например, международные переводы и сделки с ЦФА), — Национальные (использование ЦФА в рамках одной страны), — Локальные (внутри отдельных платформ или экосистем). 	
По источнику	<ul style="list-style-type: none"> — Внешние (связаны с функционированием в глобальной финансовой системе) — Внутренние (связаны с технологическими и организационными аспектами функционирования ЦФА) 	
По степени воздействия	<ul style="list-style-type: none"> — Формирующие высокий риск — Формирующие средний риск — Формирующие низкий/приемлемый риск 	
По типу	<ul style="list-style-type: none"> — Уязвимости токенов — Уязвимости смарт-контрактов — Уязвимости физических активов 	
В зависимости от элемента инфраструктуры	Технические уязвимости	<ul style="list-style-type: none"> — Уязвимости смарт-контрактов — Уязвимости технологии блокчейна — Устаревшее ПО
	Сетевые угрозы	<ul style="list-style-type: none"> — Атаки DDoS (перегрузка серверов, недоступность для пользователей) — Перехват данных (пользователи и транзакции)
	Управление доступом	<ul style="list-style-type: none"> — Слабая аутентификация (уязвимость учетных записей) — Неправильное управление правами доступа (недостаточный контроль над теми, кто имеет доступ к критическим системам и данным)
	Организационные уязвимости	<ul style="list-style-type: none"> — Стандарты KYC не адаптированы к цифровой среде — Разрозненные инфраструктурные элементы и платформы для учета цифровых прав — Слабый международный обмен данными по сделкам ЦФА

Составлено автором

Так же все уязвимости инфраструктурного сектора ЦФА можно классифицировать исходя из источника происхождения на внешние и внутренние (табл. 3).

Внешние уязвимости связаны с особенностями их функционирования в глобальной финансовой системе и взаимодействием с традиционными финансовыми институтами.

Внутренние уязвимости связаны с технологическими и организационными особенностями их функционирования, включают отсутствие центрального органа и единой платформы управления, что также затрудняет их регулирование и контроль, уязвимости точек доступа и недостатки в системе аутентификации, связанные с их псевдоанонимностью (например, через VPN-подключение), что повышает интерес злоумышленников к использованию ЦФА для незаконных целей.

Выводы

Интенсивное развитие рынка ЦФА и незрелость его инфраструктуры может способствовать эксплуатации имеющихся уязвимостей со стороны мошенников. Анализ научных исследований подтверждает многоаспектность проблемы появления новых схем и криминального использования ЦФА для целей ОД/ФТ.

Сделаны выводы, о том, что российская инфраструктура ЦФА фрагментирована и сочетает контрольные, учетные, товарные, информационные и вспомогательные элементы. При этом степень их регулирования и контроля с учетом особенностей инфраструктурного сектора обращения ЦФА различная в ключевых и прочих субъектах.

В целом проблемное поле использования ЦФА в целях ОД/ФТ связано с: регуляторными аспектами, манипуляций с удаленным прохождением процедуры идентификации клиента и ограниченности КУС-контроля, техническим уязвимостям смарт-контрактов, распределенного реестра, манипуляций с реестром сделок с ЦФА и угрозами информационной безопасности в виде взломов и утечек данных, вирусного ПО.

Для комплексного представления проблемного поля на базе рассмотренных исследований и международных кейсов незаконного использования ЦФА были сформированы перечень и классификация угроз и уязвимостей ЦФА.

Среди базовых внешних уязвимостей были выделены регуляторные пробелы, технологические риски блокчейна, трансграничный характер операций с ЦФА. К внутренним группам уязвимостей отнесены недостатки систем комплаенса, уязвимости смарт-контрактов, угрозы кибербезопасности и проблемы изолированности цифровых платформ друг от друга.

Теоретическая значимость работы заключается в структурировании угроз ОД/ФТ и уязвимостей инфраструктурного сектора обращения ЦФА, разработке их комплексной классификации. Исследование вносит вклад в развитие методики оценки угроз и рисков ОД/ФТ в условиях цифровизации финансовой системы.

Практическая ценность исследования определяется возможностью применения его результатов исследователями, регуляторами, участниками рынка ЦФА и правоохранительными органами для совершенствования мер противодействия преступным схемам ОД/ФТ.

Основным результатом исследования является классификация уязвимостей инфраструктурного сектора ЦФА, что позволит выработать научно обоснованные рекомендации по повышению устойчивости инфраструктурных элементов ЦФА к угрозам использования их в незаконных целях, особенно с учетом российской специфики рынка ЦФА.

Таблица 3

Классификация уязвимостей инфраструктурного сектора ЦФА

Категория	Тип уязвимости	Характеристика	Примеры эксплуатации в ОД/ФТ	Потенциальные последствия
1. Внешние уязвимости	1.1. Регуляторные пробелы	Недостаточная правовая определенность сущности и видов ЦФА в различных юрисдикциях, разные подходы к пониманию ЦФА. Отсутствие единых стандартов регулирования ЦФА на международном уровне. Отсутствие единых критериев отнесения сделок с ЦФА к операциям, подлежащим обязательному контролю в целях ПОД/ФТ. Квалификация иностранных цифровых инструментов в качестве ЦФА на предмет их соответствия принципам регулирования, закрепленным в российском законодательстве. Правовые основы дробления ЦФА. Для осуществления международных операций российские платформы по выпуску ЦФА и их правила должны проходить регистрацию у зарубежных партнеров.	Использование юрисдикций и стран с мягким регулированием для обхода KYC/AML-процедур. Манипуляции долями. Уход от налогообложения через выпуск и обращение ЦФА.	Невозможность эффективного межгосударственного сотрудничества в расследовании. Разная правоприменительная практика к сомнительным операциям с ЦФА. Сдерживание отечественного инвестиционного потенциала.
	1.2. Технологические риски блокчейна	Децентрализация, псевдоанонимность децентрализованных финансов (DeFi), невозможность отмены транзакций.	Смешивание средств для запутывания транзакций.	Усложнение цепочек транзакций, сложности и затруднение отслеживания. Легализация преступных доходов.
	1.3. Трансграничный характер операций	Отсутствие географических ограничений при переводе ЦФА в мировой практике.	Перевод средств в офшорные юрисдикции без уведомления регуляторов.	Уход от налогового контроля и санкционных ограничений.
2. Внутренние уязвимости	2.1. Недостатки систем комплаенса	Не достаточно развитые механизмы верификации пользователей (KYC) и мониторинга транзакций (AML). Проблемы точек входа (использование VPN, Прокси-серверов, обход геоблокировок). Процесс оценки активов перед выпуском ЦФА, защита от финансовых пирамид.	Регистрация цифровых кошельков на поддельные документы. Взлом цифровых кошельков, хищение активов. Вывод денежных средств инвесторов. Фиктивная токенизация активов для привлечения инвестиций.	Легализация преступных доходов. Кибермошенничество. Финансовые пирамиды, мошеннические схемы.
	2.2. Уязвимости смарт-контрактов	Ошибки в коде, возможность эксплуатации уязвимостей (например, reentrancy-атаки).	Хищение средств через взлом DeFi-платформ (пример: Poly Network).	Потеря доверия к цифровым активам, хищения ЦФА, финансовые потери.
	2.3. Угрозы кибербезопасности	Уязвимости платформ и кошельков к хакерским атакам.	Взломы бирж (по принципу Mt. Gox, FTX) с последующей конвертацией. Утечки персональных данных.	Крупномасштабные хищения и отмывание преступных доходов. Кибермошенничество.
	2.4. Проблемы изолированности цифровых платформ друг от друга	Проблемы изолированности платформ, отсутствие «единого окна» для эффективного обмена информацией.	Ограничения для развития вторичного рынка обращения ЦФА. Манипуляции при обмене информацией. Перехват данных.	Потеря доверия к цифровым активам. Утечки информации.

Составлено авторами

ЛИТЕРАТУРА

1. Каранина, Е.В. Развитие цифровых финансовых активов: зарубежный опыт / Е.В. Каранина, Д.И. Скопин — DOI 10.36871/ek.up.p.r.2023.07.02.018. // Экономика и управление: проблемы, решения. — 2023. — Т. 2, № 7(139). — С. 181–192 — EDN DPY0IY.
2. Развитие рынка цифровых финансовых активов в контексте обеспечения финансового суверенитета России / С.А. Жиронкин, Л.Н. Сафиуллин, М.Е. Коновалова, О.Ю. Кузьмина — DOI 10.18323/3034-2074-2024-3-58-3. // Цифровая экономика и инновации. — 2024. — № 3. — С. 29–40 — EDN OAKCJO.
3. Мнацакянц, Л.С. Риски цифровых финансовых активов / Л.С. Мнацакянц, А.А. Гамиловская — DOI 10.17513/vaael.3540. // Вестник Алтайской академии экономики и права. — 2024. — № 6–2. — С. 345–352 — EDN XSSNRO.
4. Апостолов, А. Расчеты по цифровым финансовым активам в цифровой валюте Банка России / А. Апостолов — DOI 10.17513/fr.43586. // Фундаментальные исследования. — 2024. — № 4. — С. 8–13 — EDN OMPVNH.
5. Tschorsch F., Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies // IEEE Communications Surveys & Tutorials. — 2016. — Т. 18. — № 3. — С. 2084–2123.
6. Anderson R. et al. Measuring the cost of cybercrime // The economics of information security and privacy. — 2013. — С. 265–300.
7. Ababneh M., Aljarrah A. Role of Artificial Intelligence in Data Protection for Digital Asset Systems: A Review of Recent Development // TEM Journal. — 2024. — Т. 13. — № 4. — С. 3431–3444.
8. Arner, D.W., Auer, R., Frost, J. Stablecoins: risks, potential and regulation // Financial Stability Review. BIS Working Paper no. 905 (2020), University of Hong Kong Faculty of Law Research Paper No. 2021/57. — 2020. — № 39. — С. 95–123.
9. Гирич, М.Г. Сравнительный анализ правового регулирования цифровых финансовых активов в России и других странах / М.Г. Гирич, И.С. Ермохин, А.Д. Левашенко — DOI 10.17323/1996-7845-2022-04-07. // Вестник международных организаций: образование, наука, новая экономика. — 2022. — Т. 17, № 4. — С. 176–192 — EDN EZBFHO.
10. Шубенкова, К.В. Особенности правового регулирования цифровых финансовых активов в РФ / К.В. Шубенкова, Е.П. Малахова — DOI 10.15688/lc.jvolsu.2024.4.12. // Правовая парадигма. — 2024. — Т. 23, № 4. — С. 92–97 — EDN RWVRZP.
11. Raquet-Clouston M., Haslhofer B., Dupont B. Ransomware payments in the bitcoin ecosystem // Journal of Cybersecurity. — 2019. — Т. 5. — № 1. — С. 11.
12. Хоружий, Л.И. Мошенничество с финансовой информацией: анализ и оценка деловых партнеров / Л.И. Хоружий, А.С. Бабанская, Н.Ю. Трящина // Бухучет в сельском хозяйстве. — 2018. — № 5. — С. 68–80. — EDN XQVWVP.
13. Arulkumaran Rahul, Mangal Amit, Singh S., Jain Shalu, Agarwal Raghav, Тага Amer. Cyber Security Strategies: Protecting Digital Assets in a Rapidly Evolving Threat Landscape. — 2024. — 12. — С. 2455–6211.

14. Eugene Jang, Kimin Lee, Jin-Woo Chung, Keuntae Park, Seungwon Shin. Improbable Bigrams Expose Vulnerabilities of Incomplete Tokens in Byte-Level Tokenizers // arXiv:2410.23684v1 [cs.CL]. — 31 Oct 2024. Режим доступа — URL: <https://doi.org/10.48550/arXiv.2410.23684>
15. Проблемы внедрения цифровых активов в современный платежный оборот / А.А. Карартынян, Д.Я. Родин, О.С. Зиниша, А.Е. Полковников — DOI 10.18334/ce.15.5.112018. // Креативная экономика. — 2021. — Т. 15, № 5. — С. 2033–2048 — EDN WVKWPV.
16. Doli Pinki, Kollwitz Elbert. The Role of Financial Crime in Digital Asset Scams: Lessons from Convicted Fraudsters. — 2025. Режим доступа — URL: <https://doi.org/10.13140/RG.2.2.31667.54563>.
17. Tao Li, Donghwa Shin, Baolian Wang. Cryptocurrency Pump-and-Dump Schemes. — 2021. — P.90. Режим доступа — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041.
18. Park K., Youm H.Y. Proposal of a Service Model for Blockchain-Based Security Tokens //Big Data and Cognitive Computing. — 2024. — Т. 8. — № 3. — С. 30.

Babanskaya Anastasia Sergeevna

Financial University under the Government of the Russian Federation, Moscow, Russia

E-mail: banasti@mail.ru

RSCI: https://elibrary.ru/author_profile.asp?id=754154

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=57216711030>

Threats and vulnerabilities of legalization (laundering) of criminal proceeds and financing of terrorism in the infrastructure sector of issuance, accounting and circulation of digital financial assets

Abstract. The article provides a comprehensive review of the problems of illegal use of elements of the digital financial assets (DFA) infrastructure sector and substantiates their external and internal vulnerabilities. The relevance of the study is due to the rapid development of the DFA market with insufficient maturity of regulatory mechanisms, which creates significant opportunities for their criminal use. The goal is to identify, classify and systematize the key vulnerabilities and threats of the DFA infrastructure sector that contribute to the risks of money laundering and terrorist financing (ML/FT). The methodological basis of the work is the analysis of reports from FATF and other international organizations, the study of judicial practice in cases related to illegal transactions with DFA, as well as a review of modern scientific and analytical publications. Based on the analysis of real cases and scientific research, the most common schemes for using DFA for ML/FT were identified. The study systematized the key vulnerabilities of the digital financial assets infrastructure, which were classified into external (regulatory gaps, technological risks of blockchain systems, cross-border nature of transactions) and internal (deficiencies in compliance systems, weak user identification, smart contract vulnerabilities and cybersecurity threats, problems of isolation of digital platforms from each other). The main result of the study is the classification of vulnerabilities of the digital financial assets infrastructure sector, which will allow developing scientifically based recommendations for increasing the resilience of the digital financial assets infrastructure to the threats of their use for illegal purposes, especially taking into account the Russian specifics of the digital financial assets market. The study contributes to the development of a methodology for assessing ML/FT threats and risks in the context of digitalization of the financial system. The findings are of practical value for researchers, regulators, digital financial asset market participants and law enforcement agencies involved in combating economic crimes.

Keywords: threats; vulnerabilities; money laundering; terrorist financing; digital financial assets; infrastructure sector