



Доклад ФАТФ

Целевой отчет по стейблкоинам и некастодиальным кошелькам

Пиринговые транзакции



Март 2026



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) — независимый межправительственный орган, который разрабатывает и продвигает политику, направленную на защиту глобальной финансовой системы от отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ признаны глобальным стандартом в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ).

Для получения дополнительной информации о ФАТФ посетите сайт: www.fatf-gafi.org.

Настоящий документ и/или любые включенные в него карты не затрагивают статус или суверенитет какой-либо территории, делимитацию международных границ и рубежей, а также наименование любой территории, города или района.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

ФАТФ (2026), *Целевой отчет по стейблкоинам и некастодальным кошелькам – Пиринговые транзакции*, ФАТФ, Франция, www.fatf-gafi.org/content/fatf-gafi/en/publications/virtualassets/targeted-report-stablecoins-unhosted-wallets

© 2026 ФАТФ/ОЭСР. Все права защищены.

Никакое воспроизведение или перевод данной публикации не допускается без предварительного письменного разрешения.

Заявки на получение такого разрешения, полностью или частично в отношении данной публикации, следует направлять в Секретариат ФАТФ, 2 rue André Pascal 75775 Paris Cedex 16, Франция или e-mail: contact@fatf-gafi.org

Фотография на обложке : © Shutterstock

Оглавление

Аббревиатуры и сокращения.....	2
Резюме.....	3
Введение.....	4
Цели и структура.....	4
Предыдущая работа ФАТФ по стейблкоинам.....	4
Охват.....	5
Методология.....	5
Предпосылки.....	6
Общая информация об экосистеме стейблкоинов и определения.....	6
Требования ФАТФ к ПУВА и применимость к стейблкоинам.....	8
Часть первая: Анализ текущей ситуации, угроз и уязвимостей.....	11
Текущая ситуация.....	11
Использование стейблкоинов субъектами угроз.....	12
Уязвимости.....	18
Часть вторая: Передовые практики по снижению рисков неправомерного использования стейблкоинов, включая пиринговые транзакции.....	22
Эффективная реализация стандартов ФАТФ.....	22
Применение мер контроля эмитентами стейблкоинов.....	24
Использование передовых инструментов для выявления и мониторинга подозрительных транзакций.....	27
Эффективный надзор за эмитентами стейблкоинов и другими участниками механизмов стейблкоинов.....	29
Эффективное взаимодействие государственного и частного секторов.....	31
Отработка следственных версий.....	32
Меры по снижению рисков ОД/ФТ/ФРОМУ, связанных с некастодиальными кошельками и пиринговыми транзакциями.....	32
Заключение.....	34
Рекомендуемые меры.....	34
Приложение А: Перечень индикаторов риска.....	37

Аббревиатуры и сокращения

КПА	Криптовалюта с повышенной анонимностью
ПОД/ФТ/ФРОМУ	Противодействие легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения
ЦВЦБ	Цифровые валюты центральных банков
НПК	Надлежащая проверка клиента
ДЦФ	Децентрализованные финансы
ДЦБ	Децентрализованная биржа
ТРР	Технология распределенного реестра
КНДР	Корейская Народно-Демократическая Республика
Субъект НОН	Организации, занимающиеся незаконным оборотом наркотиков
УПК	Углубленная проверка клиента
ФУ	Финансовые учреждения
ЗСК	Знай своего клиента
ОД/ФТ/ФРОМУ	Отмывание доходов / финансирование терроризма / финансирование распространения оружия массового уничтожения
ОТС	Внебиржевые операции
P2P	Пиринговый
ГЧП	Государственно-частное партнерство
СПО	Сообщение о подозрительной операции
ЦФС	Целевая финансовая санкция
КМП	Кошелек, подпадающий под Маршрутное правило
ВА/ПУВА	Виртуальные активы/Провайдеры услуг виртуальных активов

Резюме

1. Масштабы использования стейблкоинов и их интеграция в экосистему виртуальных активов и традиционную финансовую систему стремительно растут. По состоянию на середину 2025 года в обращении находилось более 250 стейблкоинов, при этом их совокупная рыночная капитализация превышала 300 млрд долларов США, а ежедневные объемы торгов превосходили показатели биткойна. Стейблкоины, обеспеченные фиатными активами и управляемые централизованно — преимущественно привязанные к доллару США — доминируют на рынке и широко используются в различных блокчейнах. Несмотря на все более широкое применение в законных целях, их характерные особенности — ценовая стабильность, высокая ликвидность и совместимость — также делают их привлекательным инструментом для мошенников.
2. Стейблкоины, в том числе с использованием некастодиальных кошельков, стали распространенным элементом схем ОД/ФТ/ФРОМУ, основанных на виртуальных активах. Хотя наблюдаются и относительно простые и/или прямые способы их использования, во многих схемах стейблкоины выступают лишь одним из элементов более сложной цепочки транзакций, направленной на сокрытие происхождения средств и их дистанцирование от конечного использования. По имеющимся данным, стейблкоины являются наиболее часто используемым видом виртуальных активов в незаконных операциях.
3. В целом стейблкоины обладают теми же уязвимостями, что и другие виртуальные активы. Эти уязвимости усиливаются их характеристиками, такими как ценовая стабильность и высокая ликвидность, что повышает вероятность их использования в пиринговых транзакциях. Пиринговые транзакции через некастодиальные кошельки представляют собой ключевую уязвимость экосистемы стейблкоинов. Поскольку такие операции осуществляются без участия посредников, обязанных соблюдать требования ПОД/ФТ/ФРОМУ, они могут нести повышенные риски, особенно при многоуровневом перемещении средств через некастодиальные кошельки. Кроме того, стейблкоины могут иметь дополнительные, специфичные для данного класса активов уязвимости, в частности связанные с их взаимосвязью с традиционной финансовой системой. Практика показывает, что субъекты угроз используют стейблкоины для приобретения запрещенных товаров без вывода средств через посредников, однако данные о более широком использовании стейблкоинов для покупки товаров и услуг или для пиринговых транзакций остаются ограниченными. В этой связи важно, чтобы юрисдикции и заинтересованные стороны продолжали внимательно отслеживать, в какой степени стейблкоины все чаще используются для покупок без обращения к традиционным каналам ввода и вывода средств, а также насколько возможно получение достоверных данных о масштабах и доле пиринговых транзакций.
4. В ответ на выявленные риски и уязвимости в докладе представлен ряд лучших практик, которые могут быть внедрены юрисдикциями и частным сектором. Часть из них применима ко всем виртуальным активам, тогда как другие характерны именно для стейблкоинов. К таким мерам относятся: формирование комплексной правовой базы в соответствии со Стандартами ФАТФ; установление четких требований ПОД/ФТ/ФРОМУ для эмитентов стейблкоинов, посредников и кастодиальных провайдеров; оценка рисков и внедрение мер по их снижению для операций с использованием некастодиальных кошельков; а также использование передовых технологических инструментов. В докладе также подчеркивается необходимость дальнейшей координации между компетентными органами и на международном уровне, а также важность оказания технической помощи юрисдикциям, которые еще не внедрили в полной мере регуляторные и надзорные механизмы в отношении стейблкоинов. Кроме того, в докладе представлены примеры юрисдикций, применяющих инновационные подходы, такие как требование к эмитентам внедрять программируемые механизмы контроля в смарт-контракты стейблкоинов для обеспечения замораживания активов, включения в «черные списки» или применения иных мер по снижению рисков на вторичных рынках.
5. В заключение, данный доклад предоставляет участникам Глобальной сети ФАТФ индикаторы неправомерного использования стейблкоинов, в частности через некастодиальные кошельки. Также он содержит внутренние рекомендации для Глобальной сети ФАТФ, направленные на возможное снижение рисков в среде обращения стейблкоинов.

Введение

Цели и структура

6. Предыдущая работа ФАТФ была сосредоточена на стейблкоинах в более широком контексте. Цель данного проекта — углубить понимание возникающих рисков ОД/ФТ/ФРОМУ, субъектов угроз и уязвимостей, связанных со стейблкоинами и некастодиальными кошельками, особенно в рамках пиринговых транзакций. Кроме того, проект направлен на выявление и распространение лучших практик по снижению этих рисков¹.

Указанные цели достигаются через три раздела:

- **Предпосылки:** описывает различных участников экосистемы стейблкоинов, дает соответствующие определения и раскрывает применимость Стандартов ФАТФ к механизмам обращения стейблкоинов, а также текущее состояние их внедрения.
- **Первая часть:** анализирует текущее состояние развития экосистемы стейблкоинов и отличия стейблкоинов от других виртуальных активов, а также выявляет субъектов угроз и национальные и отраслевые уязвимости, которыми они пользуются.
- **Вторая часть:** рассматривает лучшие практики по мерам снижения рисков со стороны государственного и частного секторов, а также по проведению расследований и национальному/международному сотрудничеству.

Предыдущая работа ФАТФ по стейблкоинам

7. ФАТФ занимается вопросами стейблкоинов с 2019 года, начиная с публичного исследования «Риски отмывания денег, связанные со «стейблкоинами» и другими новыми активами», а также доклада «Отчет ФАТФ для G20 о так называемых стейблкоинах»². ФАТФ продолжала уточнять применение Стандартов ФАТФ для помощи юрисдикциям в снижении этих рисков³. В «Целевом обновлении по реализации Стандартов ФАТФ в отношении виртуальных активов и поставщиков услуг виртуальных активов» (2025) ФАТФ отметила, что использование стейблкоинов различными незаконными субъектами, включая субъектов КНДР, лиц, занимающихся финансированием терроризма, и сети наркоторговли, со временем продолжает расти⁴.
8. ФАТФ подчеркнула необходимость постоянного мониторинга развития экосистемы стейблкоинов для обеспечения эффективности Стандартов ФАТФ в условиях продолжающейся эволюции виртуальных активов. В частности, ФАТФ указала на важность дальнейшего наблюдения за: (1) достигают ли стейблкоины глобального массового распространения таким образом, что позволяют приобретать товары и услуги с минимальной зависимостью или без зависимости от традиционных каналов ввода и вывода средств; и (2) в какой степени юрисдикции и частный сектор способны получать достоверные данные о масштабах и доле пиринговых транзакций.

¹ ФАТФ определяет пиринговые транзакции как переводы виртуальных активов, осуществляемые без использования или участия ПУВА или иной обязанной организации (например, переводы виртуальных активов между двумя некастодиальными кошельками, пользователи которых действуют от собственного имени).

² ФАТФ «Риски отмывания денег, связанные со «стейблкоинами» и другими новыми активами» (2019); ФАТФ (2020), Отчет ФАТФ для G20, ФАТФ, Франция.

³ ФАТФ «12-месячный обзор пересмотренных Стандартов ФАТФ по виртуальным активам и поставщикам услуг виртуальных активов» ФАТФ «Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов» (2021); ФАТФ «Второй 12-месячный обзор пересмотренных Стандартов ФАТФ по виртуальным активам и поставщикам услуг виртуальных активов» (2021).

⁴ ФАТФ «Целевое обновление по реализации Стандартов ФАТФ в отношении виртуальных активов и поставщиков услуг виртуальных активов» (2025).

Охват

9. Настоящий доклад отражает развитие экосистемы стейблкоинов по состоянию на конец 2025 года. В нем разъясняется применимость Стандартов ФАТФ к различным участникам механизмов обращения стейблкоинов, анализируется развитие рынка стейблкоинов, а также демонстрируется рост рисков ОД/ФТ/ФРОМУ, связанных со стейблкоинами, особенно при использовании некастодиальных кошельков в рамках пиринговых транзакций.
10. В докладе рассматриваются уязвимости стейблкоинов, часть из которых характерна для большинства виртуальных активов, тогда как другие являются специфичными именно для стейблкоинов. Основное внимание уделено практическим мерам по снижению рисков, связанным со стейблкоинами, с акцентом на пиринговые транзакции, с приведением различных тематических примеров из практики юрисдикций. Доклад завершается перечнем рекомендуемых мер для заинтересованных сторон. Как и все руководящие документы ФАТФ, данный документ не носит обязательного характера.

Методология

11. Методология включала сбор и анализ материалов, представленных проектной группой ФАТФ и участниками Контактной группы по виртуальным активам (VACG), взаимодействие с соответствующими заинтересованными сторонами, а также анализ и доработку существующих материалов по механизмам обращения стейблкоинов, включая:
 - проведение двух раундов запросов информации к проектной группе ФАТФ и участникам VACG. В результате было получено: (a) 29 тематических примеров по угрозам, типологиям и мерам, применяемым в юрисдикциях; (b) 25 материалов по обязательствам ПОД/ФТ/ФРОМУ участников экосистемы стейблкоинов, регуляторным вызовам и лучшим практикам по снижению рисков.
 - привлечение представителей частного сектора, включая эмитентов стейблкоинов и компании, занимающиеся блокчейн-аналитикой, к участию в целевом опросе, посвященном проблемам и лучшим практикам по снижению рисков незаконных финансовых операций, связанных со стейблкоинами.
 - проведение виртуального круглого стола с ключевыми заинтересованными сторонами на основе результатов опроса для получения более детальной информации о мерах по снижению рисков.

Предпосылки

Общая информация об экосистеме стейблкоинов и определения

Базовые определения

12. Стейблкоин — это одна из форм виртуальных активов, представляющая собой цифровое выражение стоимости, которое может быть передано или обращено в цифровой форме и использоваться в целях платежа или инвестирования. Хотя ФАТФ признает, что стейблкоины не являются юридической или технической категорией и подчеркивает, что использование данного термина не означает подтверждения заявлений об их стабильности, под ним обычно понимается вид виртуального актива, имеющий механизм стабилизации и используемый как средство платежа и/или средство сохранения стоимости⁵. Как правило, стейблкоины стремятся поддерживать ценовую стабильность путем привязки своей стоимости к одному или нескольким базовым активам, таким как фиатные валюты или ВА, и могут быть обеспечены такими активами. Независимо от подхода к их квалификации на национальном уровне, поставщики услуг, связанных со стейблкоинами, подпадающие под определение ПУВА или ФУ, установленное ФАТФ, должны соблюдать соответствующие обязательства в соответствии со Стандартами ФАТФ⁶.

Стейблкоины, обеспеченные активами

13. Стейблкоины, обеспеченные активами, подкреплены финансовыми активами, такими как фиатные валюты или государственные облигации. Эмитенты таких стейблкоинов, как правило, заявляют и обязуются обеспечивать возможность их погашения пользователями по обеспечиваемому активу в соотношении 1:1 в любое время, что может способствовать поддержанию ценовой стабильности. Как правило, такие стейблкоины имеют централизованную структуру управления, часто осуществляемую эмитентом.

Стейблкоины, обеспеченные ВА

14. Стейблкоины, обеспеченные ВА, выпускаются с использованием ВА и токенизированных финансовых инструментов в качестве обеспечения. В связи с волатильностью стоимости таких активов подобные механизмы, как правило, требуют и поддерживают избыточное обеспечение. Выпуск, погашение, управление обеспечением и ликвидация часто осуществляются через автономные смарт-контракты, и в некоторых случаях пользователи могут выпускать стейблкоины напрямую без участия централизованных управляющих структур.

Алгоритмические стейблкоины

15. Алгоритмические стейблкоины, как правило, предназначены для поддержания ценовой стабильности путем регулирования предложения через смарт-контракты или алгоритмы (например, синтетически обеспеченные доллароподобные стейблкоины)⁷ без наличия обеспечивающих активов. Алгоритмы, управляющие экономикой стейблкоина, увеличивают предложение при росте цены и сокращают его при снижении цены с целью поддержания стабильности. Выпуск и управление, как правило, осуществляются через автономные смарт-контракты, а система управления может быть более децентрализованной по сравнению со стейблкоинами, обеспеченными активами. Как правило, такие стейблкоины не предусматривают погашение в фиатной валюте, а стремятся поддерживать стабильность цены за счет механизмов, таких как обмен стейблкоинов или их сжигание.

⁵ Совет по финансовой стабильности, [Рекомендации высокого уровня по регулированию, надзору и контролю глобальных механизмов стейблкоинов: итоговый доклад](#).

⁶ ФАТФ (2021), Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов.

⁷ Такие стейблкоины включают механизмы, компенсирующие ценовую волатильность за счет сочетания ВА с производными финансовыми инструментами.

Участники экосистемы стейблкоинов

16. В экосистеме стейблкоинов участвуют различные субъекты. Конкретный состав участников и их функции могут различаться в зависимости от структуры и характера стейблкоинов и соответствующих механизмов.

- **Эмитенты стейблкоинов:** отвечают за выпуск и погашение стейблкоинов, а также за поддержание заявленной стабильности в период обращения. Как правило, они выпускают стейблкоины в обмен на фиатные валюты или иные активы, взимая комиссии за выпуск и погашение. Во многих случаях эмитент также разрабатывает и поддерживает смарт-контракты, необходимые для всех операций в блокчейне с данным стейблкоином. Кроме того, эмитент может передавать часть своих функций, например погашение, посредникам — ПУВА.
- **Хранители резервов:** обеспечивают хранение и управление резервными активами, обеспечивающими стейблкоины, от имени эмитента.
- **Посредники:** ПУВА, включая биржи ВА и финансовые учреждения, предоставляющие услуги по покупке, продаже, хранению, торговле или конвертации стейблкоинов. Некоторые биржи могут приобретать стейблкоины у эмитента и распространять их на розничном рынке. Децентрализованные финансы (ДЦФ) также могут предоставлять пользователям услуги, такие как переводы, платежи, обмен и кредитование с использованием стейблкоинов.
- **Поставщики платежных услуг / карточные сети:** обеспечивают возможность использования стейблкоинов для оплаты товаров и услуг, предоставляя соответствующую платежную инфраструктуру торговым предприятиям. Они также могут содействовать осуществлению денежных переводов физическим лицам.
- **Некастодиальные кошельки:** кошельки ВА, которые не размещаются и не управляются сторонним поставщиком услуг, при этом пользователь полностью контролирует ключи доступа. Некоторые поставщики услуг некастодиальных кошельков также предлагают функции обмена стейблкоинов.
- **Поставщики инструментов блокчейн-аналитики:** формируют аналитические данные на основе информации, полученной при анализе блокчейнов и субъектов с пользовательскими интерфейсами (например, поставщиков кошельков). Эти данные могут использоваться эмитентами стейблкоинов и посредниками для поддержки мер по снижению рисков незаконных финансовых операций, включая выполнение требований по ограничительным мерам. Используемые ими различные таксономии затрудняют сопоставимость результатов анализа.

Жизненный цикл и характеристики стейблкоинов

17. Как правило, эмитент выпускает стейблкоины, после чего они обращаются между пользователями и ПУВА, а затем погашаются с получением фиатной валюты. Несмотря на различия в механизмах выпуска и погашения в зависимости от типа стейблкоина, в данном разделе описывается общий процесс жизненного цикла для централизованно выпускаемых стейблкоинов, обеспеченных активами.

18. Обычно эмитенты выпускают стейблкоины, получая фиатные валюты или ВА от контрагентов и создавая (эмитируя) стейблкоины, соответствующие полученной стоимости. Выпуск стейблкоинов формирует два типа рынков:

- **Первичный рынок:** первичные клиенты приобретают или погашают стейблкоины напрямую у эмитента, после чего могут выводить их в более широкий оборот на вторичном рынке. Такие клиенты, как правило ПУВА или институциональные участники, проходят процедуры НПК и онбординга. К ним также могут относиться розничные клиенты.

- **Вторичный рынок:** держатели стейблкоинов на вторичном рынке могут использовать кастодиальные кошельки с участием ПУВА или финансового учреждения, подпадающего под требования ПОД/ФТ, либо использовать некастодиальные кошельки для хранения и перевода стейблкоинов в формате пиринговых транзакций без участия обязанной организации в сфере ПОД/ФТ. Соответственно, такие пользователи могут не подпадать под требования ПОД/ФТ.
19. Эмитенты стейблкоинов, как правило, сохраняют определенную степень контроля над своими стейблкоинами как на первичном, так и на вторичном рынке с использованием смарт-контрактов. Эмитенты могут программировать смарт-контракты таким образом, чтобы запрещать определенным адресам кошельков проводить операции (например, включение в «черный список») или изымать стейблкоины из обращения на вторичном рынке (например, замораживание или сжигание). Кроме того, эмитенты могут просматривать все транзакции в блокчейне по своим стейблкоинам, учитывая публичную природу блокчейнов.
 20. Как правило, возможность погашения у эмитента доступна только первичным клиентам и осуществляется в соответствии с правилами эмитента. В ряде случаев погашение может осуществляться через назначенных эмитентом посредников в соответствии с применимыми правовыми рамками. Держатели стейблкоинов как на первичном, так и на вторичном рынке могут обменивать их на фиатную валюту или другие ВА через централизованных посредников (ПУВА), децентрализованные биржи (ДЦБ) или посредством пиринговых транзакций.

Структура управления

21. Как правило, механизмы обращения стейблкоинов имеют структуру управления, отвечающую за функционирование соответствующих сервисов. Централизованный орган управления, такой как эмитенты или посредники, может выполнять ключевые функции (например, соблюдение требований ПОД/ФТ/ФРОМУ и управление механизмами стабилизации). Во многих существующих моделях именно эмитент играет основную роль в управлении механизмом обращения стейблкоина, хотя отдельные функции могут выполняться посредниками или технологическими провайдерами. Вместе с тем такие механизмы могут быть организованы и в децентрализованной форме, как указано выше, что может приводить к размытости ответственности.

Требования ФАТФ к ПУВА и применимость к стейблкоинам

22. Рекомендация 15 Стандартов ФАТФ требует от всех юрисдикций⁸:
 - a. выявлять, оценивать и понимать риски ОД/ФТ/ФРОМУ, связанные с ВА и ПУВА.
 - b. обеспечивать, чтобы ПУВА подлежали лицензированию или регистрации в юрисдикции, в которой они созданы.
 - c. применять санкции к физическим и юридическим лицам, осуществляющим деятельность ПУВА без необходимой лицензии или регистрации.
 - d. обеспечивать, чтобы ПУВА подлежали надзору.
 - e. применять соразмерные и сдерживающие санкции к ПУВА, не соблюдающим требования ПОД/ФТ/ФРОМУ.
 - f. обеспечивать применение требований целевых финансовых санкций к ПУВА.

⁸ См. Пояснительную записку к Рекомендации 15 Стандартов ФАТФ www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf

23. ВА определяются ФАТФ как цифровое выражение стоимости, которое может быть передано или обращено в цифровой форме и использоваться в целях платежа или инвестирования. Виртуальные активы не включают цифровые формы фиатных валют, ценных бумаг и других финансовых активов, уже охватываемых Стандартами ФАТФ. С учетом их характеристик ФАТФ рассматривает стейблкоины как ВА.
24. Лица и организации, участвующие в механизмах обращения стейблкоинов, могут классифицироваться как ПУВА или ФУ в следующих случаях⁹:
- **Эмитенты стейблкоинов:** в соответствии со Стандартами ФАТФ само по себе действие по выпуску ВА не подпадает под определение деятельности ПУВА. Однако эмитенты стейблкоинов¹⁰, которые в рамках своей деятельности осуществляют одно из следующих действий, подпадают под определение ПУВА¹¹ или ФУ¹²: 1) осуществляют операции обмена или перевода, например, обменивают фиатные валюты/ВА клиентов на свои стейблкоины в процессе выпуска или погашения; или 2) участвуют в предоставлении финансовых услуг, связанных с предложением и/или продажей виртуального актива эмитентом¹³.
 - **Посредники:** посредники, осуществляющие обмен стейблкоинов на фиатную валюту или ВА, перевод стейблкоинов либо предоставляющие услуги хранения и/или администрирования стейблкоинов, подпадают под определение ПУВА. К таким посредникам могут относиться биржи, торговые платформы, поставщики кастодиальных кошельков, отдельные виды поставщиков услуг некастодиальных кошельков, а также внебиржевые брокеры. Некастодиальные кошельки, которые в рамках бизнеса осуществляют или активно содействуют осуществлению деятельности с ВА, подпадающей под Рекомендацию 15, в интересах или от имени другого лица, должны регулироваться как ПУВА¹⁴.
 - **ДЦФ-механизмы:** разработчики, владельцы, операторы и иные лица, осуществляющие контроль или оказывающие существенное влияние на ДЦФ-механизмы, даже если такие механизмы выглядят децентрализованными, могут подпадать под опре-

⁹ См. ФАТФ (2021) Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов; Отчет ФАТФ для министров финансов и управляющих центральными банками G20 о так называемых стейблкоинах; ФАТФ, Риски отмывания денег, связанные со «стейблкоинами» и другими новыми активами, октябрь 2019 года.

¹⁰ Данное определение включает как физических, так и юридических лиц.

¹¹ Согласно обновленному руководству ФАТФ 2021 года, само по себе осуществление выпуска ВА не подпадает под подпункт (v) определения ПУВА. Однако лица, которые в рамках своей деятельности осуществляют обмен или перевод выпущенных ВА от имени или в интересах другого лица, подпадают под данное определение, равно как и участие в предоставлении финансовых услуг, связанных с любым первичным размещением токенов (ICO), связанным с выпуском.

¹² Согласно Отчету ФАТФ для министров финансов и управляющих центральными банками G20 о так называемых стейблкоинах, ФАТФ считает, что такие разработчики и органы управления, как правило, будут квалифицироваться как финансовые учреждения (например, как субъекты, осуществляющие деятельность по «выпуску и управлению средствами платежа») или как ПУВА (например, как субъекты, участвующие в «предоставлении финансовых услуг, связанных с предложением и/или продажей виртуального актива эмитентом») в соответствии с пересмотренными Стандартами ФАТФ.

¹³ Согласно обновленному руководству ФАТФ 2021 года, само по себе осуществление выпуска ВА не подпадает под подпункт (v) определения ПУВА. Вместе с тем Стандарты ФАТФ применяются к деятельности, связанной с ICO (см.: стр. 30, ФАТФ, Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов, 2021).

¹⁴ Пункт 83, [Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов](#).

деление ПУВА в понимании ФАТФ, если они предоставляют или активно содействуют предоставлению услуг ПУВА. В случаях, когда невозможно идентифицировать физическое или юридическое лицо, осуществляющее контроль или оказывающее достаточное влияние на ДЦФ-механизм, может отсутствовать централизованный владелец/оператор, подпадающий под определение ПУВА. Однако на практике многие ДЦФ-механизмы являются децентрализованными лишь номинально.

25. ФАТФ не относит к ПУВА физических или юридических лиц, предоставляющих вспомогательные услуги или продукты для сети ВА. К таким услугам относятся, например, производство аппаратных кошельков или предоставление некастодиальных кошельков, при условии, что такие лица не осуществляют деятельность ПУВА. Пиринговые транзакции через некастодиальные кошельки прямо не подпадают под требования ПОД/ФТ в рамках Стандартов ФАТФ, поскольку обязательства, как правило, возлагаются на посредников, а не на физических лиц¹⁵.

¹⁵ Существуют отдельные исключения, например требования, связанные с применением целевых финансовых санкций.

Часть первая: Анализ текущей ситуации, угроз и уязвимостей

Текущая ситуация

26. Первый стейблкоин, заявленный как привязанный к доллару США в соотношении 1:1, появился в 2014 году. С тех пор количество стейблкоинов в обращении резко выросло: по состоянию на конец июня 2025 года их насчитывалось 259¹⁶. Рыночная капитализация и объемы торгов стейблкоинов также значительно увеличились. В октябре 2025 года рыночная капитализация стейблкоинов достигла 316 млрд долларов США, что составляет около 8% от общей капитализации рынка ВА. При этом суточный объем торгов достиг 156 млрд долларов США, что почти в три раза превышает показатель биткоина (55 млрд долларов США). В целом в 2025 году стейблкоины составляют около 30% всего объема транзакций с ВА в блокчейне¹⁷.
27. На рынке стейблкоинов доминируют стейблкоины, обеспеченные фиатной валютой, на долю которых приходится 95% общей рыночной капитализации по состоянию на октябрь 2025 года. Из них стейблкоины, обеспеченные долларом США, составляют 97% сегмента фиатно-обеспеченных стейблкоинов. Стейблкоины, обеспеченные ВА, составляют около 3% общего объема операций со стейблкоинами, а алгоритмические стейблкоины — лишь 0,2%. По состоянию на середину 2025 года 90% стейблкоинов имели централизованную структуру.
28. Рост распространения стейблкоинов обусловлен рядом факторов. Финансовые учреждения, ПУВА и розничные пользователи заинтересованы в потенциальных преимуществах операций со стейблкоинами, включая более быстрые расчеты, более низкие комиссии, трансграничные возможности и независимость от традиционного графика работы финансовых организаций. В ряде случаев финансовые учреждения все чаще принимают стейблкоины в качестве средства платежа. Некоторые пользователи рассматривают стейблкоины как средство сохранения стоимости, поэтому в странах с нестабильной или слабой национальной валютой население активно их использует. Вместе с тем анализ Европейского совета по системным рискам ставит под сомнение объемы использования стейблкоинов для платежей и предполагает, что их рыночная капитализация в большей степени обусловлена объемами торговли необеспеченными виртуальными активами. По мере того, как крупные юрисдикции разрабатывают или уточняют регуляторные рамки, интерес институциональных участников к стейблкоинам значительно вырос за последние годы: банки, карточные сети, платежные организации, крупные технологические компании и другие участники проявляют интерес к выходу на рынок стейблкоинов¹⁸.

¹⁶ [Отчет «Стейблкоины и CBDCs», июнь 2025.](#)

¹⁷ www.trmlabs.com/reports-and-whitepapers/2025-crypto-adoption-and-stablecoin-usage-report

¹⁸ ФАТФ, [Международный валютный фонд](#), [Совет по финансовой стабильности \(FSB\)](#), совместно с органами по установлению стандартов поддерживают и продвигают глобально скоординированный подход к политике и регулированию в сфере ВА и стейблкоинов. В отчете о статусе реализации дорожной карты G20 по виртуальным активам отмечается, что почти во всех юрисдикциях — членах FSB уже действуют регуляторные рамки в отношении ВА и стейблкоинов либо имеются планы по их пересмотру или разработке новых; [Тематический обзор глобальной регуляторной рамки FSB для деятельности с виртуальными активами: отчет по результатам взаимной оценки.](#)

Использование стейблкоинов субъектами угроз

29. Стейблкоины все чаще используются для ОД, ФТ и ФРОМУ. По данным Chainalysis, в 2025 году на стейблкоины приходилось 84% (154 млрд долларов США) объема незаконных транзакций с ВА, что позволило им превзойти биткоин как основной актив в операциях, связанных с киберпреступностью в блокчейне^{19, 20}. Характеристики, делающие стейблкоины привлекательными для законных пользователей, одновременно привлекают преступников, использующих их для отмыывания денег, финансирования терроризма, обхода санкций и финансирования распространения. По сравнению с более волатильными активами, такими как Bitcoin (BTC) или Ether (ETH), стейблкоины, например USDT (Tether) и USDC (Circle), обеспечивают относительно стабильное средство перемещения доходов. Дополнительно их привлекательность для субъектов угроз обусловлена высокой ликвидностью, совместимостью и удобством трансграничных переводов.
30. Субъекты угроз все чаще используют стейблкоины в различных блокчейнах, включая Aptos, Avalanche, Ethereum, Solana и Tron. Основной объем незаконной активности со стейблкоинами приходится на вторичный рынок.
31. Несмотря на различия в методах в зависимости от типа преступлений или групп, общими остаются следующие практики: использование нелегализованных или незарегистрированных ПУВА, часто расположенных в юрисдикциях без эффективных механизмов ПОД/ФТ для ПУВА, либо ПУВА, не соблюдающих соответствующие требования, включая внебиржевых брокеров и пиринговые платформы. Субъекты угроз также используют методы сокрытия, такие как миксеры и «перескок между блокчейнами». Стейблкоины применяются на различных этапах сложных транзакционных цепочек, в том числе для получения доходов от предикатных преступлений или на завершающем этапе при конвертации незаконных ВА в фиатную валюту.
32. Некоторые субъекты угроз, такие как лица, занимающиеся финансированием терроризма, или наркоторговцы, используют стейблкоины и другие ВА как один из инструментов привлечения и перемещения средств, при этом продолжая использовать и традиционные методы. Другие субъекты угроз, в частности КНДР, активно опираются на ВА и широко используют стейблкоины в процессах отмыывания и вывода средств. В целом субъекты угроз, злоупотребляющие ВА и использующие нелегализованных ОТС-брокеров для вывода средств в фиат, как правило, используют стейблкоины, поскольку именно их требуют такие брокеры.

Финансирование распространения КНДР и Ирана

33. Связанные с государством киберпреступные группы активно перешли к использованию стейблкоинов как предпочтительного инструмента для отмыывания доходов от программ-вымогателей, фишинга и других киберпреступлений. В частности, группы КНДР — Lazarus Group, Andariel и Onyx Sleet — специализируются на хищениях ВА, шпионаже и деструктивных атаках, включая программы-вымогатели. Например, в феврале 2025 года связанные с КНДР группы, включая Lazarus, использовали вредоносное ПО и методы социальной инженерии для проникновения в компании, работающие с ВА, и похищения средств на сумму около 1,46 млрд долларов США. В данном случае похищенные средства отмыывались через миксеры, кроссчейн-мосты и более чем 125 000 кошельков Ethereum, что свидетельствует о быстрых и масштабных транзакциях, направленных на усложнение отслеживания. КНДР также использует децентрализованные биржи (ДЦБ) и в отдельных случаях криптовалюты с повышенной анонимностью (КПА) в процессе отмыывания. После этого средства часто конвертируются в стейблкоины, преимущественно USDT в сети Tron, а затем выводятся в фиат через ОТС-брокеров или пиринговые платформы.
34. По данным MSMT, по меньшей мере с 2023 года Генеральное бюро 221 КНДР стремится расширить использование стейблкоинов за пределы киберпреступной деятельности, включая

¹⁹ [Введение к отчету «Отчет о киберпреступности 2026» - Chainalysis.](#)

²⁰ [Стейблкоины доминируют в незаконной криптоактивности, опережая биткоин.](#)

их применение в качестве средства обмена и оплаты товаров и услуг, запрещенных резолюциями Совета Безопасности ООН²¹. По оценке MSMT, Генеральное бюро 221 выполняет функции основной организации КНДР по торговле вооружениями и включено ООН в санкционные списки под своим прежним названием — Корейская горнодобывающая торговая корпорация (KOMID). В частности, установлено, что структуры КНДР используют Tether (USDT) в операциях, связанных с продажей и поставкой военной техники, а также сырья, такого как медь, используемая в производстве боеприпасов. Такая деятельность свидетельствует о целенаправленных усилиях КНДР по практическому использованию стейблкоинов в закупках, связанных с оружием массового уничтожения.

35. Возможность проведения транзакций с использованием стейблкоинов, таких как USDT, для запрещенной деятельности предоставляет включенным в санкционные списки ООН структурам КНДР дополнительный механизм обхода международных санкций. По сравнению с наличными операциями, которые часто требуют физического перемещения через границы, платежи в USDT менее обременительны с точки зрения логистики, быстрее и потенциально менее рискованны, что облегчает осуществление закупок, запрещенных соответствующими резолюциями Совета Безопасности ООН.
36. Кроме того, иранские субъекты используют стейблкоины для финансирования распространения. В частности, Корпус стражей исламской революции (IRGC) начал активно использовать ВА для финансирования деятельности по обходу санкций; по оценкам компаний, занимающихся блокчейн-аналитикой, в 2024–2025 годах на связанные с IRGC адреса в блокчейне поступили средства на сумму в несколько миллиардов долларов США. Подсанкционные иранские субъекты используют ВА для приобретения компонентов для беспилотных летательных аппаратов и другого высокотехнологичного оборудования, а также начали принимать ВА в качестве оплаты за вооружение. Также установлено, что иранские субъекты используют ВА для перевода средств другим подсанкционным субъектам в регионе, таким как хуситы, с целью закупки вооружений. В таких операциях предпочтение часто отдается стейблкоинам благодаря их большей эффективности при финансировании международной торговли. Иран адаптирует свои подходы в ответ на ограничения, чтобы обеспечить возможность дальнейшего обхода санкций. Например, замораживание USDT по адресам, связанным с IRGC, в середине 2025 года может стимулировать переход на другие стейблкоины, такие как DAI, которые не предусматривают функцию замораживания²².

Отмывание денег

37. Наблюдается использование стейблкоинов отмывателями денежных средств и злоумышленниками для получения доходов от инвестиционного мошенничества, мошенничества с выдачей себя за другое лицо, романтических схем, схем «разделки свиньи» (pig butchering) и шантажа с использованием интимных материалов. Злоумышленники могут запрашивать средства в различных ВА, чаще всего в биткойне или стейблкоинах, а также использовать стейблкоины в процессе отмывания. Процесс отмывания, как правило, включает использование услуг ПУВА, которые могут быть нерегулируемыми в отдельных юрисдикциях или не соблюдать регуляторные требования, а также применение миксеров, ДЦБ, платформ обмена монет и пиринговых платформ. Эти сервисы часто взаимодействуют с незарегистрированными или нелицензированными ПУВА, включая ОТС-брокеров, для обмена стейблкоинов на фиатную валюту, что завершает цикл отмывания денег.

²¹ [MSMT\(Многосторонняя группа мониторинга санкций\).](#)

²² [Криптоэкономика Ирана в 2025 году: снижение объемов, рост напряженности и изменение доверия | TRM Блок.](#)

Блок 1. Практический пример: использование онлайн-гемблинг-платформ

Была выявлена серия транзакций, связанных со средствами, поступающими из онлайн-казино с использованием ВА. Эти средства были оперативно конвертированы в стейблкоины с использованием кастодиального кошелька, размещенного у ПУВА, действующего во Франции. После этого стейблкоины были обменены на фиатную валюту и зачислены на несколько банковских счетов. ПУВА направил сообщение о подозрительной операции (СПО) в TracFin — подразделение финансовой разведки Франции.

ПУВА выявил ряд индикаторов, свидетельствующих о неправомерном использовании онлайн-гемблинг-платформ и стейблкоинов, включая использование онлайн-казино лицами, чья игровая активность не соответствовала их клиентскому профилю или заявленному источнику средств. Кроме того, быстрая конвертация выигрышей в стейблкоины без очевидной экономической цели указывает на попытки сокрытия происхождения средств.

Источник: Франция

38. Организации, занимающиеся незаконным оборотом наркотиков, все активнее используют стейблкоины, в частности USDT в сети TRON и USDC в сети Ethereum, для расчетов с зарубежными поставщиками прекурсоров синтетических наркотиков, проведения наркосделок и отмывания доходов от наркоторговли. При закупках переведенные стейблкоины быстро конвертируются в местную валюту либо реинвестируются в дальнейшее производство наркотиков. Схемы отмывания часто включают использование подставных лиц (money mules), ОТС-брокеров и пиринговых платформ, а также быстрые транзакции с ВА через несколько блокчейнов, что существенно усложняет выявление и пресечение таких операций со стороны правоохранительных органов и подразделений финансовой разведки. Организации, занимающиеся наркоторговлей, также используют высокооборотные онлайн-гемблинг-платформы и схемы возврата средств торговыми организациями, при которых товары приобретаются с использованием украденных данных, а затем возвращаются с получением возврата в стейблкоинах на сторонние кошельки. Аналогично отмыванию доходов от мошенничества, доходы от наркоторговли часто конвертируются в фиатную валюту через незарегистрированные или нелицензированные ПУВА, включая ОТС-брокеров, в юрисдикциях со слабыми или отсутствующими механизмами ПОД/ФТ.

Блок 2. Практический пример: отмывание доходов от трансграничной наркоторговли с использованием стейблкоинов

Организованная преступная сеть подозревалась в отмывании доходов от наркоторговли путем приобретения Ether (ETH) у регулируемого поставщика услуг в сфере виртуальных активов (ПУВА). Далее ETH обменивался на USDT (Tether) и USDC (Circle) на децентрализованных биржах (ДЦБ) и платформах обмена криптоактивов без прохождения процедур надлежащей проверки клиентов (ЗСК / НПК). USDT и USDC переводились на кошельки, контролируемые подставной импортно-экспортной компанией в Канаде. Денежные средства проходили через несколько кошельков (многоуровневое «расслоение»), после чего выводились в фиатную систему через ОТС-брокеров и регулируемые ПУВА. В ряде случаев фиатные средства, выведенные через регулируемый ПУВА, переводились на внутренние банковские счета преступников под видом «инвестиционных доходов». Финансовая разведка ПФР и стратегический анализ позволили правоохранительным органам отследить доходы от наркоторговли и выявить финансовую инфраструктуру и методы деятельности организованной преступной сети.

Источник: Канада

39. Профессиональные отмыватели денежных средств применяют сложные методы «расслоения» с использованием стейблкоинов, включая переход между блокчейнами, дробление транзакций и межсетевые переводы, с целью сокрытия источника и конечного назначения средств. Аналогично схемам отмывания доходов от мошенничества, афер и наркоторговли, такие лица часто используют нерегулируемые или нелицензированные ПУВА либо ПУВА, не соблюдающие требования ПОД/ФТ. Также используются децентрализованные биржи (ДЦБ), не предусматривающие процедуры НПК, криптоматы (банкоматы виртуальных активов) и онлайн-гемблинг-платформы, что дополнительно усложняет отслеживание операций. Кроме того, в отдельных случаях стейблкоины применяются для расчетов в рамках подпольных банковских систем.

Блок 3. Практический пример: выплаты жертвам торговли людьми в Юго-Восточной Азии через платежного провайдера региона

Операционный анализ был проведен ПФР Индии в отношении группы лиц, получавших депозиты в виртуальных цифровых активах (VDA) от платежного провайдера, базирующегося в Юго-Восточной Азии. Индийский поставщик услуг в сфере виртуальных цифровых активов (VDA SP) выявил модель поведения среди группы клиентов, IP-адреса которых указывали на страны Юго-Восточной Азии. Указанные лица демонстрировали устойчивую модель поведения, заключающуюся в пополнении счетов в USDT, немедленной их конвертации и выводе соответствующих сумм в индийских рупиях (INR) на свои банковские счета без осуществления иных видов операций.

В рамках усиленных мер надлежащей проверки клиентов (EDD) поставщик услуг в сфере виртуальных цифровых активов (VDA SP) пытался связаться с клиентами по мобильным номерам, однако они были либо отключены, либо недоступны. Поскольку связаться с клиентами по телефону не удалось, поставщик услуг в сфере виртуальных цифровых активов (VDA SP) предпринял попытки установить контакт через платформу обмена сообщениями. После неоднократных попыток VDA SP удалось установить связь с 21 клиентом, при этом было установлено, что клиенты находились в различных странах Юго-Восточной Азии и работали в качестве строительных рабочих, сотрудников ресторанов и т.д. Несколько клиентов также имели совпадающий отпечаток устройства, то есть вход в учетные записи осуществлялся с одного и того же устройства, а различные пользователи использовали один и тот же IP-адрес при совершении операций с VDA.

Таким образом было установлено, что граждане Индии, работающие в мошеннических центрах в Юго-Восточной Азии (преимущественно в Камбодже и Мьянме), используют платежного провайдера, базирующегося в Юго-Восточной Азии, для перевода заработной платы (выплачиваемой наличными в тайских батах или долларах США) своим семьям, друзьям и родственникам в Индии. Шесть пользователей VDA SP были выявлены в списке индийских граждан, не вернувшихся из стран Юго-Восточной Азии. Эти лица выехали по туристической визе и не вернулись в течение трех месяцев. Было установлено 241 местоположение пользователей, расположенное вблизи мошеннических центров, действующих в Камбодже. Также были выявлены новые местоположения таких центров.

Кроме того, в октябре 2025 года ПФР Индии инициировало меры комплаенса и вынесло уведомление в соответствии со статьей 13 Закона «О предотвращении отмыwania денег» 2002 года в отношении платежного провайдера, базирующегося в Юго-Восточной Азии, который осуществлял незаконную деятельность в Индии. Деятельность данного субъекта на территории Индии была впоследствии заблокирована.

Источники: Индия

Финансирование терроризма

40. Террористические организации, использующие виртуальные активы, все чаще отдают предпочтение стейблкоинам по сравнению с биткоином по причинам, аналогичным тем, которые характерны для лиц, занимающихся отмыwанием денежных средств. Террористические организации ИГИЛ (Даиш) и ее региональные аффилированные структуры, а также «Аль-Каида», как сообщается, осуществляют сбор пожертвований в стейблкоинах через зашифрованные платформы и социальные сети и используют стейблкоины для перевода средств внутри группы. Они предоставляют сменяемые адреса кошельков для получения виртуальных активов, включая стейблкоины, от сторонников по всему миру с целью сокрытия по-

лучателей переводов. Также установлено, что они используют стейблкоины для дробления крупных сумм на множество мелких переводов, проходящих через несколько ПУВА, с целью снижения риска выявления.

41. Как отмечается в Комплексном обновлении ФАТФ по рискам финансирования терроризма за 2025 год, виртуальные активы чаще используются в сочетании с более традиционными методами финансирования терроризма. Например, кампания по сбору средств может быть организована на специализированной краудфандинговой платформе, распространяться через социальные сети и принимать платежи в ВА. После завершения краудфандинговой кампании террористические организации и посредники используют различные офлайн- и онлайн-инструменты для управления и перемещения средств, включая HOSSP.
42. Наблюдается, что лица, осуществляющие финансирование терроризма, все чаще комбинируют стейблкоины с агрегаторами децентрализованных финансов (ДЦФ), платформами обмена криптоактивов (coin-swap), инструментами повышения анонимности и некастодиальными кошельками с целью обхода требований комплаенса. Установлено, что в их кампаниях используются повторно применяемые QR-коды, домены и адреса для смены получателя, что позволяет сохранять функционирование схем финансирования даже после мер принудительного пресечения. Транзакционные модели, как правило, характеризуются плотными многошаговыми переводами, дроблением средств на микросуммы и последующей их консолидацией перед выводом в фиат, зачастую через ОТС-брокеров, заявляющих минимальные или отсутствующие требования по НПК. Эти методы позволяют подсанкционным или включенным в перечни сетям скрывать происхождение и назначение средств, одновременно получая доступ к глобальным пулам ликвидности, что создает значительные сложности для подразделений финансовой разведки и органов регулирования.

Блок 4. Практический пример: выявление случая финансирования терроризма с использованием стейблкоинов

В начале 2025 года ПУВА, осуществляющий деятельность во Франции, выявил аномальные модели транзакций, связанные с розничным клиентом. В течение нескольких недель клиент регулярно осуществлял исходящие переводы стейблкоинов на один и тот же внешний кошелек. Эти транзакции отличались небольшими суммами, высокой частотой и отсутствием обоснованной коммерческой или личной цели, что послужило первоначальными индикаторами подозрительности.

Получатель средств предположительно был связан с террористической организацией. Анализ блокчейна показал, что кошелек получателя имел прямые связи с ранее санкционированными адресами, связанными с сетями финансирования терроризма. Отправитель, по-видимому, выступал в роли посредника. Характер транзакций указывал на преднамеренное дробление (smurfing) с целью обхода пороговых значений контроля и процедур мониторинга.

Подозрительная активность была выявлена с использованием инструментов блокчейн-аналитики. Соответствующий ПУВА применял инструменты ончейн-анализа, позволяющие отслеживать связь кошельков с высокорисковыми субъектами. Эти инструменты идентифицировали кошелек получателя как имеющий прямые связи с несколькими адресами, ранее задействованными в схемах финансирования терроризма. ПУВА направил СПО в TracFin — ПФР, включив в него полные данные о транзакциях, ссылки на блокчейн и идентификационные данные клиента.

Источник: Франция

Уязвимости

Уязвимости на различных этапах жизненного цикла стейблкоинов и в рамках их экосистемы (выпуск, обращение, погашение)

Выпуск

43. По своей природе деятельность со стейблкоинами носит трансграничный характер, что может создавать стимулы для эмитентов стейблкоинов размещать свои штаб-квартиры в юрисдикциях с более слабыми регуляторными режимами, осуществляя при этом деятельность на международном уровне. В результате эмитенты стейблкоинов, включая офшорные и децентрализованные структуры, могут создавать сложности для компетентных органов в части эффективного мониторинга и надзора, аналогично тем, которые наблюдаются в отношении других офшорных ПУВА. Риски, связанные с деятельностью офшорных ПУВА, включая регуляторный арбитраж и «слепые зоны» надзора, дополнительно рассматриваются в документе ФАТФ «Понимание и снижение рисков, связанных с офшорными ПУВА».
44. Кроме того, схемы мультиэмиссии стейблкоинов могут создавать риски финансовых преступлений. Такие схемы предполагают, что организация из юрисдикции А совместно выпускает стейблкоин с организацией из юрисдикции В, в результате чего выпущенные стейблкоины являются взаимозаменяемыми и неразличимыми между двумя эмитентами. Подобные механизмы могут затруднять деятельность правоохранительных органов, особенно в части отслеживания, «заморозки» или конфискации стейблкоинов, поскольку задействованы два или более эмитента из разных юрисдикций. Дополнительной ключевой проблемой для органов надзора и правоохранительных органов является обеспечение эффективного контроля в сфере ПОД/ФТ и получение информации о клиентах, поскольку может быть сложно определить четкое распределение обязанностей по соблюдению требований между эмитентами, которые могут подчиняться различным режимам ПОД/ФТ. Кроме того, определение геолокации усложняется использованием VPN, в связи с чем может быть затруднено установление того, какая именно организация обладает соответствующей информацией и ответственностью.

Обращение

45. Целостность экосистемы стейблкоинов зависит от регулирования посреднических ПУВА и надлежащей реализации мер ПОД/ФТ. Существенной проблемой является значительная неоднородность уровней комплаенса среди участников экосистемы стейблкоинов: одни посреднические ПУВА применяют более продвинутые системы комплаенса, например с использованием инструментов блокчейн-аналитики, тогда как другие располагают ограниченными ресурсами или менее эффективными программами комплаенса. Посреднические ПУВА, действующие в юрисдикциях, не внедривших Рекомендацию 15, могут вовсе не иметь программ комплаенса, что создает критическую уязвимость в глобальной системе регулирования стейблкоинов.

Погашение

46. Погашение означает конвертацию стейблкоинов обратно в фиатные деньги или соответствующий базовый актив. ФАТФ требует, чтобы ПУВА и финансовые учреждения, предоставляющие услуги по погашению, применяли меры ПОД/ФТ/ФРОМУ в отношении конечных бенефициаров активов. Регулируемые ПУВА и финансовые учреждения, осуществляющие обмен стейблкоинов на базовый актив, обязаны собирать информацию о клиентах, проводить проверку по санкционным спискам и соблюдать Маршрутное правило (где применимо), а также иные требования комплаенса. Операции по погашению, осуществляемые через соблюдающие требования ПУВА или финансовые учреждения, должны находиться под эффективным надзором с доступностью соответствующей информации для компетентных органов.
47. Ключевая уязвимость на этапе погашения заключается в том, что держатели стейблкоинов не обязаны использовать официальные каналы погашения для конвертации стейблкоинов в фиатные деньги. Хотя операции на вторичном рынке формально не являются погашением, стейб-

лкоины могут обмениваться на фиатные деньги или базовые активы через неформальные каналы или несоблюдающих требования провайдеров услуг, включая ОТС-брокеров или пиринговые платформы, действующие без лицензированного или зарегистрированного посредника.

Это создает возможности для преступников обходить формальные меры контроля и получать активы, которые могут быть реинвестированы или использованы вне экосистемы виртуальных активов. Юрисдикциям следует активно выявлять и контролировать такие неофициальные и нерегулируемые механизмы обмена, приводящие к эффекту, аналогичному погашению, поскольку они представляют собой критическую уязвимость.

Пиринговые транзакции через некастодиальные кошельки

48. Пиринговые переводы через некастодиальные кошельки (пиринговые транзакции) создают риски незаконных финансовых операций, которые не всегда могут быть снижены в рамках системы ПОД/ФТ/ФРОМУ, применяемой к экосистеме стейблкоинов. Такие транзакции осуществляются напрямую между физическими или юридическими лицами без участия регулируемого посредника — ПУВА или финансового учреждения, и, соответственно, выходят за пределы требований ПОД/ФТ/ФРОМУ, что делает их по своей природе более рискованными.
49. Ранее ФАТФ проводила анализ рыночных метрик пиринговых транзакций, однако не смогла представить окончательные количественные оценки из-за значительных расхождений в данных различных компаний²³. Несмотря на сложности оценки масштаба пирингового сегмента, крайне важно, чтобы юрисдикции продолжали мониторинг рисков, связанных с пиринговыми транзакциями и некастодиальными кошельками.
50. Для устранения данного пробела Руководство ФАТФ по риск-ориентированному подходу к ВА и ПУВА прямо указывает, что ПУВА должны собирать необходимую информацию об отправителе и получателе даже при осуществлении перевода между клиентом и некастодиальным кошельком. Юрисдикциям, допускающим проведение ПУВА операций с некастодиальными кошельками, следует оценивать соответствующие риски и внедрять соразмерные меры по их снижению²⁴.
51. Несмотря на подход ФАТФ, субъекты угроз по-прежнему могут переводить стейблкоины с использованием многоуровневых некастодиальных кошельков, находящихся на значительном транзакционном удалении от кошельков, подпадающих под Маршрутное правило (КМП). Риски ОД/ФТ/ФРОМУ в таких транзакциях могут дополнительно усиливаться при их трансграничном характере. Ввиду практически мгновенного зачисления стейблкоинов на адреса получателей, расположенные вне юрисдикции отправителя, компетентные органы могут сталкиваться с дополнительными трудностями при мониторинге и отслеживании таких переводов.
52. Хотя пиринговые транзакции в публичных блокчейнах остаются видимыми и поддающимися отслеживанию, информация о транзакциях по своей природе является псевдонимной, что позволяет преступникам использовать повышенный уровень псевдонимности для сокрытия принадлежности транзакций и маскировки своей личности от компетентных органов. Риски сокрытия дополнительно усиливаются в случаях, когда преступники регулярно создают новые адреса кошельков и отказываются от ранее использованных. Массовое появление новых адресов усложняет для компетентных органов оценку того, связаны ли пиринговые транзакции с преступной деятельностью или подсанкционными субъектами.
53. Еще одним структурным ограничением системы ПОД/ФТ/ФРОМУ в отношении пиринговых транзакций через некастодиальные кошельки является вопрос представления сообщений о подозрительных операциях (СПО), учитывая отсутствие обязанных субъектов, ответственных за их направление по таким транзакциям. Хотя ПУВА могут внедрять строгие требования Маршрутного правила в отношении операций с некастодиальными кошельками своих

²³ ФАТФ (2021) 2-й 12-месячный обзор пересмотренных Стандартов ФАТФ — виртуальные активы и поставщики услуг виртуальных активов

²⁴ www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

клиентов, включая мониторинг таких операций и направление СПО в ПФР, их возможности по наблюдению, а следовательно, и по выявлению или сообщению о подозрительных транзакциях, связанных с многоуровневыми некастодиальными кошельками, находящимися на значительном транзакционном удалении от КМП, остаются ограниченными.

54. В данном контексте эмитенты стейблкоинов могут играть дополнительную роль, поскольку правоохранительные органы могут обращаться к ним с запросами о замораживании некастодиальных кошельков, предположительно содержащих неправомерно используемые стейблкоины. В ответ на такие запросы эмитенты могут отслеживать транзакции, связанные с выявленными адресами некастодиальных кошельков, и, при необходимости в рамках применимого правового режима, направлять СПО в ПФР.

Ограничения применения блокчейн-среды к стейблкоинам

Кроссчейн-активность

55. Блокчейн-сети и разработчики их экосистем все чаще отдают приоритет развитию интероперабельности стейблкоинов по сравнению с другими виртуальными активами. Такая интероперабельность позволяет стейблкоинам функционировать в нескольких блокчейнах и юрисдикциях, обеспечивая эффективные трансграничные переводы²⁵. Хотя это способствует законным денежным переводам и повышает ликвидность, одновременно это может увеличивать возможности использования мультитейн-потокот субъектов угроз и усложнять отслеживание транзакций, создавая дополнительные вызовы для мер ПОД/ФТ/ФРОМУ.
56. Рыночный анализ показывает, что подсанкционные субъекты и другие субъекты угроз все чаще используют стейблкоины, в том числе в рамках кроссчейн-операций, которые могут использоваться для фрагментации потоков транзакций и усложнения их отслеживания при перемещении средств между блокчейн-сетями. Эта проблема может дополнительно усугубляться при использовании техник chain-hopping с задействованием нескольких блокчейнов, поскольку отдельные блокчейны функционируют изолированно и не способны напрямую взаимодействовать друг с другом²⁶. Интероперабельность между несколькими блокчейнами может ослаблять один из ключевых механизмов контроля, доступных эмитентам стейблкоинов, а именно возможность замораживания или внесения активов в «черные списки», когда централизованно выпущенные стейблкоины обращаются в других блокчейнах в форме вновь созданных стейблкоинов, производных от исходных²⁷.

Пробелы в данных

57. Архитектура стейблкоинов, основанная на блокчейне, одновременно способствует и затрудняет надзор в сфере ПОД/ФТ/ФРОМУ. Несмотря на то, что каждая транзакция неизменно фиксируется в публичных блокчейнах, такие записи не содержат критически важного контекста и являются псевдонимными, поэтому сбор информации в рамках НПК, включая данные о географическом местоположении, в соответствии с Рекомендациями 10 и 15 имеет ключевое значение для обеспечения возможности правоохранительных органов получать информацию от ПУВА и финансовых учреждений. Кроме того, отсутствие данных о географическом расположении базовых кошельков может подрывать способность компетентных органов эффективно взаимодействовать с соответствующими зарубежными партнерами.
58. Важно отметить, что не все транзакции происходят в блокчейне. Например, операции с ВА между клиентами одного и того же ПУВА, как правило, осуществляются вне блокчейна, при этом передача активов фиксируется только во внутреннем реестре ПУВА, а соответствующая информация о клиентах, включая потенциально данные об их местоположении, хранит-

²⁵ [Вопросы использования механизмов стейблкоинов в трансграничных платежах](#) (BIS, 2023).

²⁶ <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>

²⁷ [Что такое обернутые токены? Практическое руководство по кроссчейн-активам.](#)

ся во внутренних системах ПУВА. Такие переводы обычно быстрее и дешевле, поскольку не требуют уплаты сетевых комиссий и ожидания подтверждения блоков, однако в случае, если ПУВА не имеет лицензии или регистрации, отсутствует посредник, осуществляющий сбор идентификационных данных клиентов и направление СПО, что затрудняет выявление и расследование незаконной деятельности правоохрательными органами. Кроме того, биржи, эмитенты и кастодианы могут сопоставлять ончейн- и офчейн-данные для выявления потенциально незаконной деятельности, тогда как регуляторы и правоохрательные органы не имеют прямого доступа к офчейн-данным или выявленным паттернам.

Часть вторая:

Передовые практики по снижению рисков неправомерного использования стейблкоинов, включая пиринговые транзакции

Эффективная реализация Стандартов ФАТФ

59. Крайне важно, чтобы юрисдикции устанавливали обязательства в сфере ПОД/ФТ/ФРОМУ для ПУВА в экосистеме стейблкоинов, включая эмитентов стейблкоинов и посреднические ПУВА. Эти обязательства изложены в Рекомендации 15 Стандартов ФАТФ и должны включать внедрение превентивных мер в соответствии с Рекомендациями 9–21²⁸. Учитывая количество участников экосистемы стейблкоинов, четкое разграничение конкретных обязательств в сфере ПОД/ФТ/ФРОМУ для каждой стороны имеет ключевое значение для обеспечения соблюдения требований. Юрисдикции также должны обеспечивать применение соответствующих обязательств ПОД/ФТ/ФРОМУ к финансовым учреждениям, участвующим в механизмах стейблкоинов, включая кастодиальных провайдеров резервных активов эмитентов стейблкоинов.

Блок 5: Япония – реализация мер в отношении эмитентов и посредников

Как эмитенты стейблкоинов, так и посредники подпадают под требования ПОД/ФТ/ФРОМУ в соответствии с Законом о предотвращении передачи доходов от преступной деятельности. Допустимые эмитенты — провайдеры услуг по переводу денежных средств и трастовые компании — обязаны проводить НПК на этапах выпуска и погашения, а также внедрять меры по снижению рисков, такие как ограничение переводов, связанных с предполагаемой преступной деятельностью, на основе информации, полученной от компаний, осуществляющих блокчейн-аналитику, или от следственных органов. Посредники, осуществляющие операции со стейблкоинами (как внутренними, так и иностранными) в Японии, должны регистрироваться в качестве провайдеров услуг по обмену электронных платежных инструментов и соблюдать требования ПОД/ФТ/ФРОМУ, включая НПК, направление СПО и соблюдение Маршрутного правила. С учетом рисков ОД, связанных с децентрализованными биржами (ДЦБ), рассматривается возможность установления соразмерных и надлежащих обязательств ПОД/ФТ/ФРОМУ, в частности в отношении их приложений и других пользовательских интерфейсов, с учетом дальнейшего международного обсуждения данного вопроса.

Источник: Япония

60. Вместе с тем экосистема стейблкоинов является сложной, и распределение соответствующих обязательств ПОД/ФТ/ФРОМУ между ее участниками не является простой задачей.

²⁸ В резолюции 2462 (2019) Совет Безопасности ООН также настоятельно призвал все государства внедрить всеобъемлющие международные стандарты, закрепленные в пересмотренных Рекомендациях ФАТФ. Дополнительные разъяснения содержатся в документе Контертеррористического комитета Совета Безопасности ООН «Необязывающие руководящие принципы по предотвращению, выявлению и пресечению использования новых и развивающихся финансовых технологий в террористических целях», январь 2025, [S/2025/22](#).

На практике лишь ограниченное число юрисдикций внедрило регулирование стейблкоинов, прямо учитывающее их особенности, отличающие их от других виртуальных активов (см. Блок 5).

Блок 6. Примеры: обязательства ПОД/ФТ/ФРОМУ в экосистеме стейблкоинов

ЕС

Стейблкоины классифицируются в соответствии с Регламентом о рынках криптовалют (MiCA) как токены электронных денег (EMT), привязанные к одной фиатной валюте, и токены, обеспеченные активами (ART), которые не являются электронными деньгами и предназначены для поддержания стабильной стоимости путем привязки к иному значению, праву или их комбинации (включая одну или несколько официальных валют). Эмитенты ART являются юридическими лицами, зарегистрированными в ЕС и получившими разрешение в соответствии со статьей 16 MiCA; однако сам по себе выпуск ART не делает эмитентов ART субъектами, на которых распространяются обязательства ПОД/ФТ/ФРОМУ. Услуги по обмену ART на другие криптовалюты или фиатные валюты, хранение ART, а также услуги, связанные с выпуском (например, размещение ART, прием и передача распоряжений), требуют получения разрешения провайдера услуг криптовалют (CASP), и в качестве обязанных субъектов на CASP распространяются обязательства, включая наличие политик управления рисками, идентификацию и верификацию клиентов, мониторинг транзакций, направление СПО и процедуры санкций/замораживания активов. Компетентные органы учитывают риски ОД/ФТ при принятии решений о предоставлении, отказе или отзыве разрешения для эмитента ART и, как правило, проверяют наличие судимостей, связанных с ПОД/ФТ/ФРОМУ, у членов руководящих органов и акционеров с существенным участием. Кроме того, эмитент обязан предоставить информацию о своих взаимодействиях с CASP (при наличии), в частности о процедурах, обеспечивающих соблюдение требований по предотвращению легализации доходов и финансирования терроризма в соответствии с Директивой (ЕС) 2015/849. Компетентные органы могут отказать в предоставлении разрешения, если бизнес-модель эмитента может подвергнуть его или сектор существенным рискам ОД/ФТ. Отсутствие посредника — обязанного субъекта — при предложении и размещении ART может рассматриваться как индикатор такого риска, и компетентный орган может использовать это положение для отказа в авторизации. Таким образом, несмотря на то что эмитенты ART не являются обязанными субъектами, они должны обеспечивать постоянное эффективное управление рисками ОД/ФТ. EMT выпускаются лицензированными кредитными организациями или учреждениями электронных денег, на которые распространяются обязательства ПОД/ФТ/ФРОМУ.

Казахстан

В Международном финансовом центре «Астана» (МФЦА) эмитенты стейблкоинов и посредники подпадают под комплексные обязательства ПОД/ФТ/ФРОМУ в соответствии с Правилами ПОД/ФТ и санкций МФЦА (AML Rules). Для выпуска стейблкоинов, обеспеченных фиатными валютами или товарами, эмитент должен получить лицензию Управления по финансовым услугам Астаны (AFSA) на предоставление услуг, связанных с цифровыми активами.

Лицензированные эмитенты обязаны внедрять надежные процедуры НПК на этапах выпуска, погашения и иных точках взаимодействия — включая проверку клиентов и бенефициарных владельцев, проведение углубленной проверки для операций повышенного риска и постоянный мониторинг транзакций. Они также должны иметь процедуры по выявлению, ограничению или замораживанию стейблкоинов, связанных с незаконной деятельностью,

на основе данных блокчейн-аналитики, информации правоохранительных органов или указаний AFSA. Соблюдение требований обеспечивается операционными мерами: полное обеспечение резервами, их сегрегация; ежемесячная сверка; и ежегодные независимые аудиты с представлением отчетности в AFSA и публикацией, если не установлено иное.

Посредники, обеспечивающие торговлю, обмен или перевод стейблкоинов в рамках МФЦА, должны быть авторизованы и соблюдать полный спектр обязательств ПОД/ФТ/ФРОМУ, включая НПК, ведение учета, направление СПО, санкционный скрининг и соблюдение Маршрутного правила. Эмитенты и посредники должны обеспечивать, чтобы прекращение деятельности, восстановление или сворачивание операций не наносили ущерба держателям и не создавали уязвимостей. В совокупности эти меры интегрируют требования ПОД/ФТ/ФРОМУ с механизмами корпоративного управления, пруденциального и операционного контроля, обеспечивая прозрачность и безопасность операций со стейблкоинами в МФЦА.

Применение мер контроля эмитентами стейблкоинов

61. Стандарты ФАТФ требуют, чтобы к эмитентам стейблкоинов применялись превентивные меры, предусмотренные Рекомендацией 15 Стандартов ФАТФ. К ним относятся НПК, ведение учета, выявление и сообщение о подозрительных операциях (СПО), а также соблюдение Маршрутного правила и другие меры. Эмитенты стейблкоинов должны в обязательном порядке применять превентивные меры к своим клиентам на первичном рынке (то есть к тем, кто напрямую приобретает или погашает стейблкоины у эмитента).
62. Юрисдикциям целесообразно рассмотреть, каким образом существующие обязательства ПОД/ФТ/ФРОМУ могут применяться на вторичном рынке, в частности — как использовать уникальные технологические возможности эмитентов для выполнения функций смарт-контрактов, таких как «сжигание» или «замораживание». В частности, эмитенты могут в любой момент определять выпуск и погашение своих стейблкоинов. Кроме того, эмитенты могут внедрять функции замораживания и сжигания в смарт-контракты стейблкоинов и применять их при необходимости.
63. Несмотря на возможность мониторинга ончейн-обращения, остатков и переводов стейблкоинов на уровне блокчейн-адресов, личности держателей стейблкоинов в блокчейне публично не раскрываются. В случаях, когда стейблкоины хранятся у ПУВА, информация о личности клиента может быть доступна компетентным органам по законному запросу к соответствующему ПУВА, однако она не доступна напрямую эмитенту. Если же стейблкоины хранятся в некастодиальных кошельках, на блокчейне виден только псевдонимный адрес, без какой-либо информации НПК. Тем не менее, даже при невозможности установить фактического владельца, при выявлении связи адреса с преступной деятельностью применение функций замораживания остается возможным.
64. Юрисдикциям также следует рассмотреть, необходимо ли — с учетом уровня риска и контекста — обязать эмитентов стейблкоинов проактивно отслеживать географию и использование своих стейблкоинов на вторичном рынке с использованием инструментов блокчейн-аналитики, а также применять дополнительные соразмерные меры. Такие меры могут включать регулярную отчетность о циркуляции стейблкоинов на вторичном рынке.
65. Смарт-контракт является ключевым элементом кода, который определяет функционирование стейблкоина в блокчейне, и может быть запрограммирован на выполнение определенных условий, которые должны быть соблюдены перед осуществлением операции как на первичном, так и на вторичном рынках. Эмитенты могут использовать программируемость

смарт-контрактов для разрешения проведения операций только определенными адресами кошельков или, напротив, для запрета проведения операций определенными адресами.

- *«Белый список»:* эмитенты стейблкоинов могут контролировать, кто может владеть, получать или переводить стейблкоины, разрешая их использование только предварительно одобренным лицам или адресам. Это реализуется путем добавления списка контроля доступа в смарт-контракт стейблкоина; если адрес кошелька отправителя или получателя отсутствует в списке, транзакция автоматически отклоняется. Требования НПК, выполняемые либо самим эмитентом стейблкоинов, либо уполномоченным третьим лицом, могут быть включены в процесс предварительного одобрения и периодически повторяться для соблюдения требований постоянной проверки. Использование «белых списков» позволяет снизить риски, связанные с транзакциями через некастодиальные кошельки, поскольку требует идентификации пользователя до совершения операции.
- *«Черный список»:* эмитенты стейблкоинов могут ограничивать конкретные адреса кошельков или субъекты в части владения, получения и перевода стейблкоинов. Это противоположный подход по сравнению с «белым списком»: в смарт-контракт добавляется список запрета, и если адрес кошелька отправителя или получателя включен в него, транзакция автоматически отклоняется. Критерии включения адресов в такой список могут основываться на данных сторонних решений, включая блокчейн-аналитику и информацию правоохранительных органов. Использование «черных списков» может способствовать компетентным органам в замораживании адресов кошельков со стейблкоинами.

Блок 7: Швейцария – снижение рисков, связанных с некастодиальными кошельками

В Швейцарии финансовое учреждение («X AG») планирует выпуск стейблкоинов, номинированных в швейцарских франках, через свою полностью принадлежащую дочернюю компанию («Y AG»). Для снижения рисков, связанных с некастодиальными кошельками, X AG и Y AG внедрят процедуру «белого списка» в блокчейне с использованием смарт-контрактов.

Транзакции будут разрешены только между кошельками, включенными в «белый список», который может включать как кастодиальные, так и некастодиальные кошельки. «Белый список» будет автоматически обновляться при выявлении нового владельца кошелька, соответствующего установленным критериям. Владельцы некастодиальных кошельков будут проходить проверку через швейцарские банки, ПУВА или иностранные банки, подпадающие под сопоставимые регуляторные требования.

После успешной идентификации некастодиальный кошелек будет включен в «белый список», что позволит осуществлять транзакции с другими проверенными кошельками. Кастодиальные кошельки будут идентифицироваться и включаться в «белый список» банками или ПУВА, которые ими управляют.

Источник: Швейцария

66. Подход с использованием «черных списков» применяется чаще, однако он носит более реактивный характер, поскольку эмитенты, как правило, включают адреса в запретительный список на основании обращений правоохранительных органов или включения в национальные санкционные перечни. Подход с использованием «белых списков» является более проактивным, однако может вытеснять из экосистемы стейблкоинов пользователей, которые по соображениям конфиденциальности не желают проходить идентификацию.

Блок 8: Франция – меры комплаенса, применяемые эмитентами стейблкоинов

Во Франции практика показывает, что эмитенты стейблкоинов и поставщики услуг виртуальных активов используют инструменты блокчейн-аналитики для отслеживания стейблкоинов в блокчейне и выявления потенциально рискованных транзакций. Такой мониторинг охватывает как участников первичного рынка (первичных держателей после выпуска), так и последующих держателей на вторичном рынке. Эти инструменты позволяют эмитентам выявлять транзакции с участием блокчейн-адресов, помеченных как подверженные рискам отмыwania денег или финансирования терроризма. Уровень риска может оцениваться как напрямую (в отношении самих держателей), так и косвенно (в отношении их контрагентов). Кроме того, некоторые эмитенты стейблкоинов внедряют в смарт-контракты различные функции, такие как включение в «белый» и «черный» списки, и возможности блокировки/замораживания, которые могут активироваться по запросу государственных органов.

67. Эмитенты стейблкоинов также могут применять или быть обязаны применять иные меры по снижению рисков, такие как:

- Лимиты транзакций: установление ограничений на сумму одной операции или общий объем переводов в день для адресов кошельков, а также механизмов задержки или дополнительной проверки транзакций может дополнять подходы «черного списка» и «белого списка», снижая риск их обхода в случае «черного списка» и способствуя расширению доступа в случае «белого списка»²⁹.
- Функции блокировки, замораживания и изъятия³⁰: эмитентам стейблкоинов рекомендуется внедрять технические механизмы, позволяющие в любой момент блокировать, замораживать и изымать (например, путем «сжигания» и повторного выпуска) стейблкоины при наличии (или попытке совершения) транзакций с участием кошельков, не включенных в «белые списки» или включенных в «черные списки». Эти механизмы также позволяют эмитентам исполнять распоряжения компетентных органов в соответствии с применимым законодательством (например, о конфискации по решению правоохранительных органов).

²⁹ Лимиты транзакций допускаются в рамках стандартов ФАТФ для снижения рисков финансовых преступлений, связанных с счетами, не прошедшими стандартные процедуры ЗСК/НПК, как указано в руководстве ФАТФ по финансовой инклюзии (пункт 142) www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20Anti-Money-Laundering-Terrorist-Financing-Measures.pdf

³⁰ Блокировка означает способность эмитента стейблкоинов предотвращать выполнение конкретной транзакции без обязательного замораживания всего кошелька держателя. Это может включать запрет переводов на определенные адреса (например, подсанкционные субъекты) или отклонение транзакции при несоблюдении условий, таких как авторизация отправителя или получателя. Замораживание, в свою очередь, означает возможность эмитента полностью ограничить активность конкретного адреса кошелька, не позволяя ему перемещать токены.

Использование передовых инструментов для выявления и мониторинга подозрительных транзакций

Использование инструментов государственным сектором

68. Инструменты блокчейн-аналитики могут быть полезны для выявления рисков ОД/ФТ/ФРОМУ в экосистеме стейблкоинов, и ФАТФ ранее анализировала и поощряла использование таких инструментов³¹. Другие международные организации, такие как Контртеррористический комитет Совета Безопасности ООН, придерживаются аналогичного подхода³². Технологические достижения, особенно в области искусственного интеллекта, машинного обучения и анализа больших данных, вероятно, обладают потенциалом для дальнейшего расширения возможностей и сфер применения таких инструментов в целях ПОД/ФТ/ФРОМУ.
69. Юрисдикциям следует учитывать ограничения инструментов блокчейн-аналитики, включая сложности надежного выявления сложных методов сокрытия, используемых субъектами угроз, неоднородность возможностей и методологий различных провайдеров аналитики, стоимость проприетарных лицензий, а также необходимость наличия специализированных технических навыков для интерпретации получаемых результатов. Эти инструменты наиболее эффективны при их комбинированном использовании, а также в сочетании с традиционными методами расследования и экспертной оценкой специалистов, обладающих подготовкой в области расследований, связанных с виртуальными активами.

³¹ fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf;2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

³² Контртеррористический комитет СБ ООН, «Необязывающие руководящие принципы по предотвращению, выявлению и пресечению использования новых и развивающихся финансовых технологий в террористических целях», январь 2025, [S/2025/22](#), п. 22(m).

Блок 9. Китай: использование инструментов блокчейн-аналитики для выявления несанкционированной деятельности со стейблкоинами

Несмотря на запрет в Китае деятельности, связанной с виртуальными активами, включая стейблкоины, сформированы передовые практики по выявлению и снижению рисков на основе модели «ведущая роль регулятора — многостороннее взаимодействие». Ключевые практики включают:

1. Применение технологических инструментов: ончейн-мониторинг и аналитика

Платформа мониторинга виртуальных активов: Народный банк Китая создал платформу мониторинга, обеспечивающую анализ данных блокчейна и отслеживание транзакций. Платформа активно собирает данные из различных публичных блокчейнов, постоянно расширяет библиотеку риск-тегов и формирует основу данных для мониторинга и анализа. Основные функции платформы включают:

- (1) мониторинг выпуска виртуальных валют.
- (2) формирование профилей кошельков с использованием тегов. Типы тегов охватывают различные риск-сценарии, включая криптовалютные биржи, теневые банки, мошенничество в сфере телекоммуникаций, онлайн-гемблинг, незаконный сбор средств, интернет-вымогательство, финансирование терроризма, финансирование распространения ОМУ и санкционные списки.
- (3) построение графа связей кошельков. Эта функция анализирует целевой кошелек, заданный пользователем, и его контрагентов, преобразует сложные данные блокчейн-транзакций в наглядную сеть связей и отображает полную цепочку перемещения средств от источника к получателю.
- (4) мониторинг и выявление аномальных транзакций. Создаются и постоянно совершенствуются модели мониторинга и раннего предупреждения по аномальным операциям с виртуальными активами, проводится углубленный анализ транзакционного поведения и оценка рисков, осуществляется выявление различных видов подозрительных операций.
- (5) визуальное отслеживание ончейн-транзакций. Отслеживаются связанные с ключевыми кошельками входящие и исходящие транзакции с использованием инструментов визуализации.

2. Интеграция ончейн-данных финансовых учреждений: Некоторые крупные банки и небанковские платежные организации осуществляют анализ и отслеживание операций с виртуальными активами на основе данных блокчейна.

Источник: Китай

Использование инструментов частным сектором

70. В ряде юрисдикций эмитенты стейблкоинов и иные участники соответствующих механизмов обязаны использовать инструменты блокчейн-аналитики для снижения рисков незаконных финансовых операций, в то время как в других странах их применение поощряется посредством рекомендаций и иных мер. Эти инструменты являются одним из важных элементов системы предотвращения неправомерного использования стейблкоинов. ФАТФ признает зна-

чимость блокчейн-аналитики и рекомендует юрисдикциям предоставлять эмитентам стейблкоинов и другим участникам экосистемы разъяснения по оценке и надлежащему использованию таких инструментов для выявления и снижения рисков ОД/ФТ/ФРОМУ на уровне организаций.

Блок 10: Сингапур - private sector use of blockchain analytics tools

DPTSP A — лицензированное основное платежное учреждение (MPI), предоставляющее услуги по трансграничным денежным переводам и операциям с цифровыми платежными токенами. В ходе анализа транзакций, проведенного DPTSP A, были выявлены два кошелька (кошелек 1 и кошелек 2), имеющие косвенную связь с кошельком, связанным с финансированием терроризма. DPTSP A использовал инструменты блокчейн-аналитики для анализа высокорисковых транзакций на расстоянии одного шага (one hop), что позволило выявить данную связь.

Кошелек 1 и кошелек 2, находящиеся под управлением DPTSP A, получили соответственно 5,9 млн долл. США и 250 тыс. долл. США в стейблкоине USDT от внешнего кошелька (кошелек 3). Ончейн-анализ показал, что кошелек 3 ранее получил 200 тыс. долл. США в USDT в сети Tron от кошелька, связанного с финансированием терроризма. Кошелек 3 также был включен эмитентом стейблкоина в «черный список», что ограничило возможность проведения операций с USDT с данного адреса и на него, вероятно, ввиду прямой связи с подсанкционным адресом кошелька.

Источник: Сингапур

Эффективный надзор за эмитентами стейблкоинов и другими участниками механизмов стейблкоинов

71. ФАТФ разработала руководство по передовым практикам для органов надзора за ПУВА в своем докладе о лучших практиках надзора за соблюдением Маршрутного правила³³. Эти практики в равной степени применимы к органам надзора за эмитентами стейблкоинов и другими обязанными субъектами, участвующими в механизмах стейблкоинов. Кроме того, при лицензировании и допуске на рынок соответствующих субъектов и продуктов органам надзора следует учитывать риски, присущие стейблкоинам, а также применение специфических мер по их снижению, в частности принимая во внимание, рассматривается ли массовое распространение (массовое принятие) как фактор в рамках оценки рисков ПУВА³⁴.

³³ www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

³⁴ Доклад G20, пункт 77, и пункт 139 Руководства 2021 года..

Блок 11: Гонконг, Китай — изучение технологий для снижения рисков анонимности

Денежно-кредитное управление Гонконга (НКМА) внедрило регуляторный режим для эмитентов стейблкоинов в соответствии с Ордонансом о стейблкоинах. НКМА опубликовало регуляторные руководства, устанавливающие требования ПОД/ФТ/ФРОМУ, применимые к эмитентам стейблкоинов³⁵.

Поскольку присущие риски ОД/ФТ могут существенно различаться в зависимости от типа механизма стейблкоина, НКМА применяет риск-ориентированный, но осторожный подход при формировании требований ПОД/ФТ/ФРОМУ. В рамках процесса лицензирования заявители обязаны оценивать риски ОД/ФТ, связанные с их механизмами стейблкоинов, включая риски, возникающие на вторичных рынках и при использовании некастодиальных кошельков, и применять соразмерные меры по их снижению. Хотя на начальном этапе деятельности по выпуску стейблкоинов заявители могут использовать подход включения в «белый список», от них также ожидается представление планируемых мер по снижению рисков в средне- и долгосрочной перспективе для учета потенциального роста бизнеса или перехода к более открытому режиму функционирования. В рамках взаимодействия с частным сектором рассматривались развивающиеся технологические решения (например, децентрализованная цифровая идентификация¹) и блокчейн-протоколы (например, ERC3643), направленные на снижение проблем анонимности при обращении стейблкоинов на вторичном рынке. НКМА внимательно отслеживает данные технологические разработки с целью обеспечения соответствия своего регуляторного режима как национальным условиям, так и международным стандартам и практикам.

Источник: Гонконг, Китай

[1] См. [Руководство ФАТФ по цифровой идентификации](#).

72. Органы надзора должны развивать и поддерживать технические знания, необходимые для понимания и сопровождения внедрения регулирования в сфере стейблкоинов. Они не должны ограничиваться формальным подходом («галочкой»), например проверкой наличия у эмитента инструмента блокчейн-аналитики, но обязаны самостоятельно оценивать эффективность внедренных инструментов и мер контроля с точки зрения снижения рисков ОД/ФТ/ФРОМУ. На этой основе органы надзора также должны предоставлять разъяснения и активно взаимодействовать с частным сектором для выявления новых рисков и определения наиболее эффективных надзорных практик в экосистеме стейблкоинов.
73. В ряде юрисдикций применяется проактивный подход, предусматривающий требование или поощрение сотрудничества между органами надзора³⁶ за механизмами стейблкоинов. К числу формирующихся передовых практик относится создание надзорных коллегий — кооперационных механизмов, объединяющих органы надзора стран происхождения и стран присутствия для обмена информацией и координации надзора за организациями, осуществляющими деятельность в нескольких юрисдикциях. Совет по финансовой стабильности (FSB) отмечает, что глобальные эмитенты стейблкоинов могут обладать характеристиками, схожими с международными финансовыми учреждениями, и что надзорные коллегии при наличии надлежащих механизмов обмена информацией могут способствовать решению

³⁵ www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/

³⁶ В части надзорного взаимодействия ФАТФ отметила важность международного сотрудничества между органами надзора; см. ФАТФ (2021) «Обновленное руководство по риск-ориентированному подходу к виртуальным активам и поставщикам услуг виртуальных активов», стр. 103, пункт 357.

проблем трансграничного надзора. В рамках таких механизмов юрисдикции также могут рассматривать возможность добровольной подачи нерегулируемыми эмитентами стейблкоинов единой заявки на получение лицензии, охватывающей деятельность в нескольких юрисдикциях.

Блок 12: Использование надзорных коллегий для надзора за стейблкоинами в ЕС

В соответствии с MiCAR механизм надзорных коллегий применяется только в определенных случаях и охватывает ограниченный круг деятельности — а именно надзор за выпуском значимых токенов, обеспеченных активами (ART), и значимых токенов электронных денег (EMT). Эмитент ART или EMT считается значимым при выполнении определенных количественных и качественных критериев, например по числу держателей, объему выпуска токенов, ежедневному объему транзакций и степени взаимосвязанности с финансовой системой.

В таких случаях Европейский банковский орган (ЕБА) обязан создавать и возглавлять консультативные надзорные коллегии для координации надзорной деятельности в отношении эмитентов значимых ART и EMT. Поскольку такие эмитенты, как правило, находятся в центре сети организаций, обеспечивающих выпуск, перевод и распространение соответствующих криптоактивов, в состав коллегии должны входить, в частности, компетентные органы наиболее значимых торговых платформ (если такие токены допущены к торгам), а также компетентные органы ключевых организаций и провайдеров услуг криптоактивов, обеспечивающих хранение и администрирование значимых ART и EMT от имени держателей. Надзорная коллегия должна способствовать сотрудничеству и обмену информацией между своими участниками, а также вырабатывать необязывающие заключения, в том числе по вопросам изменения условий авторизации или применения надзорных мер в отношении соответствующих эмитентов.

Источник: Европейский союз

Эффективное взаимодействие государственного и частного секторов

74. Сотрудничество между государственным и частным секторами имеет ключевое значение в сфере виртуальных активов, где риски быстро эволюционируют, а своевременное реагирование на риски ОД/ФТ/ФРОМУ необходимо для возврата активов. ФАТФ отмечает важность взаимодействия государственного сектора с эмитентами стейблкоинов и другими участниками экосистемы с целью углубления понимания новых тенденций, усиления сотрудничества по типологиям и индикаторам риска, а также развития знаний и компетенций соответствующих специалистов, что в конечном итоге способствует укреплению целостности и безопасности экосистемы стейблкоинов.

Отработка следственных версий

75. В случаях неправомерного использования стейблкоинов через обязанных субъектов ПОД/ФТ/ФРОМУ компетентные органы могут запрашивать информацию как в порядке сотрудничества, так и с применением принудительных мер. Проведение расследований существенно усложняется, когда транзакции осуществляются через некастодиальные кошельки, поскольку отсутствует субъект, с которым возможно взаимодействие или к которому можно применить принуждение. Тем не менее у следственных органов имеются определенные инструменты для отслеживания незаконных операций с использованием некастодиальных кошельков:

- отслеживание потоков транзакций до точек выхода (конвертация в фиат или иные каналы вывода) с использованием коммерческих или открытых инструментов блокчейн-аналитики для прослеживания движения средств от целевого адреса через промежуточные адреса и протоколы к потенциальным точкам выхода
- настройка уведомлений по конкретным адресам для анализа активности и поведенческих моделей
- проведение разведки по открытым источникам (OSINT) для повышения уровня атрибуции
- интеграция ончейн-данных с традиционными методами расследования в физическом мире

76. В отношении некоторых централизованных стейблкоинов, таких как USDT или USDC, возможно прямое взаимодействие с эмитентом, поскольку он обладает технической возможностью замораживания стейблкоинов посредством функций смарт-контракта.

Меры по снижению рисков ОД/ФТ/ФРОМУ, связанных с некастодиальными кошельками и пиринговыми транзакциями

77. Стандарты ФАТФ основаны на риск-ориентированном подходе. Несмотря на то что Стандарты ФАТФ прямо не распространяются на некастодиальные кошельки и пиринговые транзакции, юрисдикциям следует учитывать связанные с ними риски ОД/ФТ/ФРОМУ и принимать меры по их снижению. ФАТФ, признавая сложности получения достоверных и полных данных о нерегулируемом сегменте, рекомендует юрисдикциям стремиться максимально полно оценивать частоту пиринговых транзакций и связанные с ними риски ОД/ФТ/ФРОМУ. Юрисдикциям также следует внедрять соразмерные меры по снижению рисков с учетом предполагаемого масштаба и уровня риска таких транзакций³⁷.

78. В рамках Глобальной сети применяются различные подходы к снижению рисков со стороны как государств, так и частного сектора, включая:

- a. ограничение ПУВА сумм средств, которые их клиенты могут переводить на некастодиальные кошельки
- b. применение ПУВА усиленных мер НПК к операциям с некастодиальными кошельками, включая установление личности бенефициарного владельца такого кошелька
- c. использование ПУВА инструментов блокчейн-аналитики для оценки уровня риска контрагентов клиентов, владеющих некастодиальными кошельками
- d. распространение на некастодиальные кошельки, в рамках механизмов стейблкоинов, требований ПОД/ФТ/ФРОМУ, включая НПК на этапах выпуска и погашения.
- e. запрет или отказ в лицензировании платформ, допускающих переводы на некастодиальные кошельки.

³⁷ ФАТФ (2024) «Тематическое обновление по реализации Стандартов ФАТФ в отношении виртуальных активов и поставщиков услуг виртуальных активов», стр. 5, пункты 37–41, 105–107.

Блок 13. Сингапур — обязательства ПОД/ФТ/ФРОМУ в отношении некастодиальных кошельков

В отношении транзакций с использованием некастодиальных кошельков провайдеры услуг цифровых платежных токенов (ПУВА в Сингапуре) обязаны внедрять усиленные меры по снижению рисков с учетом специфических рисков ОД/ФТ, связанных с такими переводами. К числу таких мер относятся, в частности: ограничение переводов виртуальных активов только операциями между собственными счетами клиента, подтверждение владения некастодиальным кошельком клиента, идентификация получателя, усиленный мониторинг счета клиента, а также установление цели транзакции.

Источник: Сингапур

Блок 14. Германия: снижение рисков, связанных с погашением на некастодиальные кошельки

Организация подала заявку на получение лицензии для выпуска токенов электронных денег, номинированных в евро, с возможностью их погашения по требованию. Средства, полученные в обмен на токены, планируется инвестировать, при этом клиенты — исключительно юридические лица — будут распространять эти токены среди конечных пользователей.

Разрешение было выдано при соблюдении следующих условий: инвестиции резервов связаны с рисками ликвидности и концентрации. Для их снижения резервы должны быть диверсифицированы и ограничены краткосрочными высоколиквидными инструментами. Клиенты — юридические лица — не считаются представляющими повышенный риск ПОД/ФТ/ФРОМУ. Однако, учитывая отсутствие у организации информации о конечных бенефициарах, к таким клиентам применяются усиленные меры НПК.

С учетом рисков, связанных с погашением на некастодиальные кошельки, в частности риска их использования в незаконной деятельности, предусмотрены следующие меры защиты:

- **Проверка личности:** организация обязана установить личность владельца кошелька перед осуществлением любого погашения на некастодиальный кошелек.
- **Блокчейн-аналитика:** организация использует инструменты для отслеживания происхождения и назначения виртуальных активов с особым вниманием к адресам повышенного риска или подсанкционным адресам.
- **Лимиты транзакций:** устанавливаются индивидуальные пороговые значения по операциям клиентов для выявления и предотвращения подозрительной активности, при этом для клиентов или юрисдикций повышенного риска применяются более низкие лимиты.
- **ИТ-мониторинг:** система должна обеспечивать постоянный мониторинг с использованием «белых» и «черных» списков, включая интеграцию с санкционными перечнями ЕС и международными санкционными списками.

Источник: Германия

Заключение

78. Стейблкоины продемонстрировали быстрый рост распространения благодаря своим характеристикам, а также доверию пользователей, обусловленному их включением в регуляторные режимы. По мере роста популярности они все чаще используются для ОД, ФТ и ФРОМУ, при этом отчетность показывает, что они являются наиболее распространенным видом виртуальных активов, используемых в незаконных транзакциях. ФАТФ рассматривает стейблкоины либо как виртуальные активы, либо как традиционные финансовые активы — в зависимости от их структуры — и требует от юрисдикций применения одинаковых обязательств ПОД/ФТ/ФРОМУ к посредникам, участвующим в механизмах стейблкоинов, включая ПУВА и финансовые учреждения.
79. Несмотря на существующую рамочную систему ФАТФ, стейблкоины подвержены повышенным рискам ОД/ФТ/ФРОМУ при их переводе на пиринговой основе через некастодиальные кошельки. Эти уязвимости усиливаются такими характеристиками, как стабильность цены и высокая ликвидность, что делает стейблкоины более привлекательными для использования в пиринговых транзакциях. Имеющиеся аналитические данные свидетельствуют о том, что значительная доля незаконных операций со стейблкоинами осуществляется через некастодиальные кошельки, включая пиринговые транзакции, что позволяет участникам обходить требования ПОД/ФТ/ФРОМУ. Практика показывает, что субъекты угроз используют стейблкоины для приобретения запрещенных товаров без вывода средств через посредников, однако данные о более широком использовании стейблкоинов для оплаты товаров и услуг или для пиринговых транзакций остаются ограниченными. В этой связи юрисдикциям и заинтересованным сторонам необходимо продолжать внимательно отслеживать, происходит ли рост использования стейблкоинов для расчетов без опоры на традиционные каналы ввода и вывода средств, а также в какой степени возможно получение достоверных данных о масштабе и доле пиринговых транзакций.
80. В докладе определен ряд передовых практик, которые могут быть реализованы юрисдикциями и частным сектором для снижения указанных рисков, а также сформулированы рекомендации по их внедрению. К ним относятся разработка специализированных регуляторных режимов для эмитентов стейблкоинов, усиленные меры по снижению рисков операций с некастодиальными кошельками, использование передовых инструментов блокчейн-аналитики, внедрение программируемых механизмов контроля в смарт-контракты, а также укрепление механизмов внутреннего и международного сотрудничества.

Рекомендуемые меры

Для юрисдикций

- I. Юрисдикциям следует применять Рекомендацию 15 к субъектам, участвующим в механизмах стейблкоинов, обеспечивая, чтобы эмитенты стейблкоинов, промежуточные ПУВА и другие соответствующие участники подпадали под четкие и исполнимые обязательства ПОД/ФТ/ФРОМУ. Юрисдикциям следует определить роли и обязанности всех участников экосистемы стейблкоинов и устанавливать соответствующие обязательства ПОД/ФТ/ФРОМУ на основе риск-ориентированного подхода.
- II. Юрисдикциям следует рассмотреть применение эффективных мер ПОД/ФТ/ФРОМУ, специфичных для эмитентов стейблкоинов и других обязанных субъектов, включая, например, требование к эмитентам обеспечивать и реализовывать технические возможности «сжигания», замораживания и изъятия стейблкоинов на вторичном рынке, применение НПК на этапе погашения, либо ограничение выпуска на блокчейнах повышенного риска. Юрисдикциям также следует рассмотреть возможность требования к эмитентам внедрять механизмы включения в «белые» и «черные» списки на основе риск-ориентированного подхода. Кроме того, юрисдикциям следует институционализировать строгий надзор и комплаенс-проверки до запуска и лицензирования для снижения рисков ОД/ФТ, связанных со стейблкоинами, до начала их обращения.
- III. Юрисдикциям следует уделять приоритетное внимание развитию устойчивых технических возможностей компетентных органов, включая надзорные органы и правоохранительные органы. Это включает формирование экспертных знаний для понимания развивающихся рисков, типологий, бизнес-моделей, функционала смарт-контрактов и механизмов межсетевых транзакций, а также укрепление возможностей эффективного использования инструментов блокчейн-аналитики.
- IV. Юрисдикциям следует рассмотреть возможность создания многосторонних надзорных коллегий для надзора за эмитентами стейблкоинов и другими участниками трансграничных механизмов стейблкоинов, при необходимости.
- V. Юрисдикциям следует обеспечивать компетентные органы, особенно органы надзора и правоохранительные органы, необходимыми инструментами для оперативного взаимодействия с национальными и зарубежными партнерами, включая использование налаженных каналов, меморандумов о взаимопонимании и правовых механизмов, обеспечивающих своевременный обмен информацией о механизмах стейблкоинов.
- VI. Юрисдикциям следует активно отслеживать существующие макроэкономические уязвимости и пробелы в экосистеме стейблкоинов, включая объем и уровень риска, связанный с пиринговыми транзакциями через некастодиальные кошельки, а также использование неформальных или нелицензированных/незарегистрированных каналов погашения. Органы надзора должны понимать и оценивать риски ОД/ФТ/ФРОМУ, связанные с бизнес-моделями, допускающими использование стейблкоинов для платежных и инвестиционных целей, и применять соразмерные меры по их снижению.
- VII. Юрисдикциям следует рассмотреть, необходимо ли — с учетом уровня риска и контекста — обязать эмитентов стейблкоинов проактивно отслеживать географию и использование своих стейблкоинов на вторичном рынке с применением инструментов блокчейн-аналитики, а также подлежат ли им соразмерным дополнительным требованиям к отчетности.
- VIII. Юрисдикциям следует рассмотреть возможность создания структурированных механизмов государственно-частного партнерства для укрепления взаимодействия между компетентными органами и участниками экосистемы стейблкоинов по вопросам типологий, индикаторов риска и возникающих угроз. Также следует рассмотреть формирование оперативных партнерств, особенно в случаях, когда расследования связаны с оффчейн-транзакциями либо требуют замораживания или «сжигания» стейблкоинов.

- IX. Юрисдикциям следует рассмотреть возможность создания регуляторных «песочниц» с участием представителей отрасли, где это уместно, для разработки стандартов и решений, обеспечивающих инновации при одновременной защите от неправомерного использования, например посредством мониторинга смарт-контрактов, блокчейн-аналитики или автоматизированного санкционного скрининга.

Для частного сектора

- I. ПУВА и финансовым учреждениям следует обеспечивать понимание различных типов механизмов стейблкоинов, а также рисков ОД/ФТ/ФРОМУ на этапах выпуска, обращения и погашения. ПУВА и финансовые учреждения должны применять адекватные и эффективные меры ПОД/ФТ/ФРОМУ ко всем участникам и операциям, связанным со стейблкоинами.
- II. Эмитенты стейблкоинов должны оценивать и снижать риски ОД/ФТ/ФРОМУ, связанные с их клиентами. Им также настоятельно рекомендуется принимать меры по снижению рисков на вторичном рынке, включая мониторинг использования стейблкоинов и внедрение специальных механизмов управления и технических мер, встроенных в архитектуру стейблкоинов.
- III. Эмитентам стейблкоинов рекомендуется внедрять технические решения, позволяющие в любой момент блокировать, замораживать и изымать стейблкоины (например, посредством «сжигания» и повторного выпуска), а также программировать смарт-контракты с включением механизмов контроля ПОД/ФТ/ФРОМУ, таких как требования НПК.
- IV. Эмитентам стейблкоинов следует рассмотреть возможность создания публично доступного централизованного контактного пункта для правоохранительных органов, функционирующего в режиме 24/7 и способного оперативно принимать меры по замораживанию стейблкоинов.

Приложение А: Перечень индикаторов риска

Индикаторы, связанные с необычными транзакциями

1. Быстрое трансграничное перемещение стейблкоинов, не соответствующее профилю клиента.
2. Перевод крупных сумм в стейблкоинах, особенно если они получены в результате недавней конвертации других ВА, в пользу нескольких получателей, не имеющих очевидной связи с соответствующим лицом, и осуществляемый в течение короткого периода времени.
3. Запросы на перевод стейблкоинов от разных, на первый взгляд не связанных между собой лиц на один и тот же адрес контрагента; либо зачисление значительных сумм стейблкоинов от множества отправителей, не имеющих видимой связи с соответствующим лицом, особенно в течение ограниченного времени.
4. Использование счета, открытого у ПУВА, в качестве транзитного для проведения операций с ВА на значительные суммы в пользу других лиц и от них.
5. Крупные операции со стейблкоинами одним и тем же лицом в короткий период времени, осуществляемые наличными или с использованием нескольких устройств (например, банкоматов) либо IP-адресов, особенно если они географически удалены друг от друга или от места проживания/деятельности лица, либо при использовании IP-адресов, отличающихся от обычно используемых этим лицом.
6. Использование стейблкоинов для пополнения балансов в азартных играх или создания фиктивных «возвратов», при которых покупки отменяются, а средства возвращаются на кошельки, не связанные с первоначальным плательщиком, что маскирует владение и легализует незаконные средства через внешне легитимные торговые операции.
7. Быстрая конвертация между фиатными валютами и стейблкоинами без очевидного экономического смысла.
8. Быстрый обмен стейблкоинов на другие стейблкоины или ВА без очевидного экономического смысла.
9. Повторяющиеся операции с ВА, предположительно связанные с пиринговыми механизмами обмена, на суммы, эквивалентные значительной стоимости в фиатной валюте.
10. Конвертация стейблкоинов в фиатную валюту на значительную сумму, если виртуальные активы были зачислены недавно, в том числе через несколько мелких операций.
11. Использование одним лицом нескольких счетов или платежных инструментов для проведения операций по конвертации в/из стейблкоинов, особенно в течение короткого периода времени и на значительные суммы.
12. Запрос на конвертацию стейблкоинов в фиатную валюту на экономически невыгодных условиях, включая уплату комиссий, превышающих среднерыночные.
13. Множественные операции по конвертации стейблкоинов в один или несколько ВА с одновременным переводом этих активов, в том числе через операции на небольшие суммы, до обнуления баланса, особенно если средства для покупки стейблкоинов были получены посредством переводов фиатной валюты с разных счетов.

14. Повторяющиеся операции покупки и продажи стейблкоинов за наличные, которые по своим характеристикам (например, сумма, дата, адрес зачисления/списания) выглядят искусственно раздробленными с целью обхода установленных порогов по операциям с наличными или внутренним лимитов, установленных обязанным субъектом.
15. Повторяющиеся операции на крупные суммы в фиатной валюте или стейблкоинах, которым предшествует или за которыми следует длительный период отсутствия какой-либо активности.
16. Множественные крупные операции со стейблкоинами в пользу недавно открытых или ранее неактивных счетов.
17. Покупка стейблкоинов, выпущенных в рамках мультисюрисдикционной схемы, в одной юрисдикции с последующим запросом на их погашение у соэмитента в другой юрисдикции без обоснованной экономической причины.

Индикаторы, связанные с анонимностью

1. Переводы стейблкоинов с использованием некастодиальных кошельков, находящихся на нескольких «шагах» от кошельков, подпадающих под Маршрутное правило (КМП).
2. Некастодиальный кошелек внезапно активируется после длительного периода бездействия, выполняет множественные межсетевые транзакции за короткое время и затем снова становится неактивным.
3. Некастодиальные кошельки регулярно осуществляют «двусторонние операции на крупные суммы» с кастодиальными кошельками офшорных бирж стейблкоинов без разумного делового обоснования.
4. Некастодиальный кошелек переводил средства на адреса незаконных внутренних и офшорных платформ торговли стейблкоинами и даркнет-рынков либо получал средства от таких платформ.
5. Использование офшорных эмитентов, не имеющих лицензии или регистрации в соответствующей юрисдикции.
6. Использование ДЦФ для обмена стейблкоинов, предоставления ликвидности и доходного фермерства с целью сокрытия следов транзакций.
7. Дробленные переводы стейблкоинов, координируемые с использованием пересекающихся устройств, автономных систем IP (IP ASN) и браузеров, с постоянными почти мгновенными конвертациями из фиатной валюты в стейблкоины через ДДЦБ и последующим выводом обратно в фиат в течение менее чем часа с целью минимизации вероятности выявления.
8. Перемещение средств между различными блокчейнами с использованием стейблкоинов для усложнения отслеживания и использования пробелов в инструментах блокчейн-аналитики.
9. Осуществление межсетевых переводов стейблкоинов через несколько блокчейнов за короткий период времени при значительном совокупном объеме операций.
10. Последовательное перемещение стейблкоинов между сетями (например, TRON → Ethereum → Solana) с использованием операций «обертывания/развертывания» (wrap/unwrap) перед выводом средств, добавляя дополнительные контракты и маршрутизацию, что снижает возможность отслеживания.
11. Использование стейблкоинов совместно с миксерами, анонимизирующими криптовалютными или приватными кошельками для повышения анонимности на стадии расслоения операций.
12. Операции с ВА, исходящие от или направленные на лиц/адреса либо осуществляемые через инструменты или счета, прямо или косвенно связанные с даркнетом или иными высокорисковыми контекстами (например, миксинг, «тумблинг», нелегализованные операторы азартных игр).
13. Направление средств через посреднические пиринговые рынки и неформальные ОТС-площадки, принимающие наличные, подарочные карты или переводы третьих лиц, с последующей конвертацией в стейблкоины, их расслоением через множество кошельков и обратной конвертацией через биржевые счета.

14. Использование внебиржевых брокеров (OTC) для конвертации фиатной валюты в стейблкоины с обходом процедур НПК на уровне бирж.
15. Использование прокси- или анонимизирующих сервисов (например, The Onion Router), затрудняющих установление источника интернет-соединения.

Индикаторы, связанные с ФТ и ФРОМУ

1. Многочисленные пожертвования (как правило, в эквиваленте 100–15 000 долл. США) на часто меняющиеся кошельки, которые при этом имеют общие признаки (QR-коды, домены или адреса сдачи), после чего средства направляются через ДЦБ-маршрутизаторы и мосты, а затем консолидируются для вывода.
2. Поступления стейблкоинов, обозначенные как гуманитарная помощь, быстро перенаправляются (часто в течение нескольких часов) в торговые операции, миксеры или межсетевые переводы, что может указывать на финансирование деятельности под прикрытием благотворительных целей.
3. Плотные цепочки более чем из 25 быстрых транзакций, дробление ликвидности через агрегаторы ДЦБ и предварительный обмен в анонимизирующие активы перед выводом, с последующей консолидацией в кошельках, связанных с брокерами и торговыми компаниями.
4. Платежи в стейблкоинах направляются посредникам, находящимся вблизи зон свободной торговли или логистических хабов, для закупки лабораторного оборудования, станков, радиочастотных компонентов, комплектующих для беспилотных летательных аппаратов и других товаров двойного назначения; при этом счета-фактуры и данные о поставках часто искажаются, а расчеты осуществляются исключительно в стейблкоинах вне традиционной банковской системы.
5. Использование межсетевых мостов для обхода ограничений аналитики и регуляторных различий между сетями и сервис-провайдерами, с доступом к глобальной ликвидности и выводом средств через несоблюдающие требования площадки.
6. Конвертация стейблкоинов в фиатную валюту в юрисдикциях со слабыми мерами ПОД/ФТ либо через несоблюдающие требования ПУВА.
7. Взаимодействие с биржами повышенного риска или подсанкционными адресами.
8. Операции со стейблкоинами, особенно на крупные суммы, с участием адресов, по которым невозможно получить достаточную уверенность в отношении бенефициарного владельца либо которые прямо или косвенно связаны с высокорисковыми, несотрудничающими, низконалоговыми юрисдикциями или юрисдикциями с недостаточным регулированием ПОД/ФТ, особенно в части ВА.