



Отчет ФАТФ

**Целевой отчёт о проблемах
регулирования децентрализованных
финансов (DeFi)**



Июль, 2026



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимым межправительственным органом, который разрабатывает и продвигает политики, направленные 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).

Дополнительную информацию о ФАТФ можно найти на сайте: 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 какой-либо территории, города или района.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

ФАТФ (2026), Целевой отчет о проблемах регулирования децентрализованных финансов, Париж, Франция, <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Virtualassets/targeted-report-decentralised-finance-2026.html>

© 2026 ФАТФ/ОЭСР. Все права защищены.

Воспроизведение или перевод настоящей публикации без предварительного письменного разрешения запрещены.

Запросы на получение такого разрешения в отношении всей публикации или ее части следует направлять в Секретариат ФАТФ по адресу: 75775, Париж, Франция, 16-й округ, ул. Андре Паскаля, д. 2, или по электронной почте: contact@fatf-gafi.org.

Фотография на обложке: © Shutterstock

Оглавление

Резюме.....	2
1. Обзор ситуации.....	3
1.1. Введение.....	3
1.2. Сфера охвата отчета.....	7
2. Характеристики и уязвимости механизмов DeFi.....	7
2.1. Характеристики механизмов DeFi.....	7
2.2. Уязвимости и препятствия для эффективного надзора в сфере ПОД/ФТ/ПРОМУ.....	9
3. Статус имплементации Стандартов ФАТФ.....	10
3.1. Применимая нормативно-правовая база.....	10
3.2. Имплементация Рекомендации 15 в отношении механизмов DeFi юрисдикциями.....	13
4. Риски финансовых преступлений и типологии, связанные с механизмами DeFi.....	15
4.1. Субъекты угроз, риски и типологии.....	15
5. Лучшие практики имплементации Р.15 в отношении механизмов DeFi.....	18
5.1. Эффективная оценка рисков механизмов DeFi.....	18
5.2. Определение контролирующих лиц механизмов DeFi.....	19
5.3. Факторы для определения контроля в механизмах DeFi.....	21
5.4. Оценка контроля над механизмами DeFi.....	24
5.5. По-настоящему децентрализованные механизмы DeFi.....	26
5.6. Требования лицензирования и/или регистрации централизованных механизмов DeFi.....	27
5.7. Надзорная практика.....	30
5.8. Взаимодействие механизмов DeFi с регулируруемыми финансовыми учреждениями и ПУВА.....	32
6. Правоприменительные и иные меры по снижению рисков, связанных с механизмами DeFi.....	36
6.1. Использование инструментов блокчейн-аналитики в расследованиях, связанных с DeFi.....	36
6.2. Координация с другими компетентными органами.....	37
6.3. Замораживание и возврат преступных средств.....	37
7. Международное сотрудничество.....	39
7.1. Трансграничный обмен информацией.....	39
7.2. Трансграничные расследования.....	40
7.3. Государственно-частное сотрудничество.....	41
Заключение.....	42
Рекомендации по снижению рисков, связанных с механизмами DeFi.....	43
1.1. Для юрисдикций.....	43
1.2. Для частного сектора.....	45

Резюме

1. С момента публикации в 2021 году обновленного Руководства ФАТФ по [применению риск-ориентированного подхода к виртуальным активам и провайдерам услуг виртуальных активов](#) сектор DeFi быстро расширился. Хотя его доля в общем рынке виртуальных активов по-прежнему сравнительно невелика, рост сектора в сочетании с расширением участия институциональных инвесторов, ПУВА и иных регулируемых организаций повысил его значимость для глобальной финансовой системы и потенциальную подверженность рискам отмывания денег (ОД), финансирования терроризма (ФТ) и финансирования распространения оружия массового уничтожения (ФРОМУ).
2. Экосистема DeFi обладает особыми преимуществами для развития глобального финансового сектора. Вместе с тем такие уникальные особенности DeFi, как псевдонимность, доступ без разрешения, автоматизация на основе смарт-контрактов, компонуемость и трансграничный охват, также создают структурные уязвимости, способные облегчать быстрое проведение сложных и непрозрачных финансовых транзакций. В отчете установлено, что эти характеристики все чаще используются различными противоправными субъектами, включая мошенников, операторов программ-вымогателей, сети профессиональных отмывателей и субъектов, занимающихся финансированием распространения оружия массового уничтожения. Противоправная деятельность нередко включает сложные методы, такие как перемещение между блокчейнами, межсетевые мосты, децентрализованные биржи, миксеры и манипулирование механизмами управления, что позволяет осуществлять расслоение и смешение незаконных средств с законными финансовыми потоками. Эти риски усиливаются там, где меры ПОД/ФТ отсутствуют либо реализованы недостаточно эффективно.
3. Стандарты ФАТФ технологически нейтральны и применяются во всех случаях, когда физическое или юридическое лицо оказывает финансовые услуги. Руководство ФАТФ 2021 года разъясняет, что механизмы DeFi подпадают под действие Рекомендации 15, если физическое или юридическое лицо осуществляет контроль или оказывает достаточное влияние на такой механизм.
4. Однако на практике юрисдикции Глобальной сети ФАТФ по-прежнему испытывают трудности с выявлением и регулированием механизмов DeFi, действующих на их территории, вследствие их трансграничного характера, отсутствия четкой юрисдикционной привязки, ограниченной технической компетентности надзорных органов и сложностей при разграничении изначально децентрализованной технологии механизмов DeFi и потенциально централизованной системы управления.
5. Одна из основных проблем заключается в выявлении «контроля или достаточного влияния» в механизмах DeFi. Хотя многие механизмы позиционируют свою систему управления как децентрализованную, в настоящем отчете установлено, что на практике централизованные элементы часто сохраняются, в том числе в форме концентрации токенов управления, административных полномочий, контроля за обновлениями, получения значительной экономической выгоды и влияния на разработку и инфраструктуру. В отчете приведен исчерпывающий перечень ончейн- и офчейн-индикаторов, которые могут помочь юрисдикциям определить наличие такого контроля.
6. С учетом структуры управления и контроля в отчете выделяются три широкие категории механизмов DeFi: i) механизмы с установленными контролирующими лицами («централизованные»); ii) механизмы, которые на практике являются централизованными, но их контролирующие лица не могут быть легко установлены; и iii) по-настоящему децентрализованные механизмы. Стандарты ФАТФ применяются к первым двум категориям. Хотя по-настоящему децентрализованные механизмы не подпадают под действие Стандартов, поскольку последние не могут быть непосредственно применены к ним, такие механизмы все же создают значительные риски, требующие альтернативных риск-ориентированных мер по их снижению.

7. В отчете подчеркивается, что для эффективной имплементации Стандартов ФАТФ применительно к DeFi необходимы функциональный и риск-ориентированный подходы. В нем представлен ряд рекомендаций, призванных помочь юрисдикциям регулировать механизмы DeFi и осуществлять надзор за ними, в том числе определять наличие контроля. Для снижения риска преступного использования рекомендации также адресованы механизмам DeFi, а также взаимодействующим с ними финансовым учреждениям и ПУВА.

1. Обзор ситуации

1.1. Введение

1. В последние годы сектор децентрализованных финансов (DeFi) значительно вырос: в 2026 году общий объем заблокированной стоимости (TVL)¹ достиг 86,644 млрд долларов США, что примерно на 85% больше, чем в 2023 году.² Несмотря на сравнительно небольшую долю в расчетной совокупной рыночной капитализации виртуальных активов³, DeFi представляет собой растущую уязвимость режима ПОД/ФТ/ПРОМУ вследствие своих отличительных характеристик и все более активного использования противоправными субъектами.⁴ Кроме того, институциональные инвесторы, провайдеры услуг виртуальных активов (ПУВА) и другие регулируемые организации все чаще размещают финансовые ресурсы в механизмах DeFi, привлеченные высокой доходностью и преимуществами блокчейн-технологии, используемой в приложениях DeFi, включая трансграничные платежи, прозрачность транзакций и удобный доступ к клиентам по всему миру.
2. Эти тенденции существенно повышают риск использования DeFi для смешения незаконных средств с законными активами, что подрывает преимущества инновационного подхода DeFi к финансам. С учетом столь стремительного развития в настоящем отчете рассматриваются риски финансовых преступлений, связанные с DeFi, и разъясняются обстоятельства, при которых Стандарты ФАТФ применяются к определенным механизмам DeFi. В настоящем отчете ФАТФ использует следующие определения:
 - DeFi означает технологию и услуги, предоставляемые посредством смарт-контрактов на основе блокчейна. Механизм DeFi, в свою очередь, охватывает более широкую экосистему, включая лиц, структуры управления и операционные компоненты, обеспечивающие функционирование таких услуг.
 - Термин «лицо», особенно в контексте контролирующих лиц механизма DeFi, включает физических лиц, а также товарищества, фонды и иные формы юридических лиц или правовых образований.
3. Экосистема DeFi обладает особыми преимуществами для развития глобального финансового сектора. Участие новых разработчиков и других субъектов способствует финансовым инновациям и создает ценную среду для апробации инновационных технологий

¹ Общий объем заблокированной стоимости (TVL) — ключевой показатель, используемый в децентрализованных финансах (DeFi) для измерения совокупного объема активов, размещенных в протоколе DeFi. Он отражает, какой объем стоимости пользователи направили на кредитование, стейкинг, предоставление ликвидности или иные услуги на основе смарт-контрактов. Вместе с тем TVL не является исчерпывающим показателем масштаба протокола или связанных с ним рисков; например, децентрализованные биржи (DEX), как правило, удерживают сравнительно небольшой объем заблокированных активов, генерируя при этом значительные объемы торгов.

² По данным DeFiLlama, по состоянию на 10 мая 2026 года TVL составлял 86,644 млрд долларов США по сравнению с 46,86 млрд долларов США на 10 мая 2023 года. <https://defillama.com/>

³ По оценкам, около 4–6% рынка виртуальных активов связано с DeFi: <https://www.coingecko.com/en/charts>

⁴ <https://academic.oup.com/cybersecurity/article/11/1/tyae029/7962044> ; <https://www.chainalysis.com/reports/crypto-crime-2026/> ; <https://www.crowdfundinsider.com/2026/05/276717-defi-hacks-report-april-2026-becomes-most-hacked-month-in-crypto-history-by-number-of-incidents/>

на основе блокчейна. Защита экосистемы DeFi от противоправного использования позволит клиентам в большей степени воспользоваться преимуществами этих инновационных финансовых услуг.

4. Стандарты ФАТФ технологически нейтральны и в равной мере применяются ко всем поставщикам финансовых услуг. Применительно к механизмам DeFi Стандарты ФАТФ действуют во всех случаях, когда установленное лицо осуществляет контроль или оказывает достаточное влияние на механизм. Однако на практике сектор DeFi остается преимущественно нерегулируемым, и многие юрисдикции испытывают трудности с реализацией эффективных мер ПОД/ФТ. Отчасти это связано с тем, что некоторые механизмы DeFi позиционируют себя как по-настоящему децентрализованные, хотя фактически контролируются установленными лицами. Ключевое различие проводится между базовой технологией, такой как блокчейн и смарт-контракты, которая обеспечивает автоматизированные транзакции без посредника и присуща всем механизмам DeFi, и системами управления этими механизмами, которые могут как находиться, так и не находиться под контролем или влиянием установленных лиц.
5. В 2019 году ФАТФ обновила Р.15 и распространила применение Стандартов ФАТФ на виртуальные активы (ВА) и ПУВА. В Глоссарии ФАТФ ПУВА определяется следующим образом:⁵ «Любое физическое или юридическое лицо, не охваченное иными положениями Рекомендаций, которое в рамках своей деятельности осуществляет одно или несколько из следующих видов деятельности или операций в интересах либо от имени другого физического или юридического лица:
 - i. обмен виртуальных активов на фиатные деньги;
 - ii. обмен одной или нескольких форм виртуальных активов;
 - iii. перевод виртуальных активов;
 - iv. хранение и/или управление виртуальными активами либо инструментами, позволяющими осуществлять контроль над виртуальными активами; и
 - v. участие в предоставлении финансовых услуг, связанных с предложением и/или продажей виртуального актива эмитентом, и предоставление таких услуг».
6. Руководство ФАТФ 2021 года по ВА и ПУВА⁶ (далее — «Руководство») признает сложность регулирования деятельности, связанной с ВА, и определяет, в каких случаях физическое лицо или организация должны классифицироваться как ПУВА, исходя прежде всего из выполняемых функций, а не используемой технологии. Руководство призывает юрисдикции разграничивать децентрализованный технический характер базового протокола DeFi⁷ и централизованную систему управления, которая может формироваться вследствие контроля или влияния, осуществляемых над механизмом определенными лицами, такими как создатели, разработчики программного обеспечения или инвесторы. Кроме того, Руководство рекомендует юрисдикциям отслеживать возникающие риски и активно взаимодействовать с сообществом DeFi для понимания потенциальных угроз ОД/ФТ/ПРОМУ и принятия мер по их устранению. Ожидается, что страны будут проводить оценку рисков DeFi с учетом риска и контекста и принимать соразмерные меры в соответствии с Р.1. Компетентным органам также следует выпускать для финансовых учреждений и ПУВА руководящие указания по

⁵ [Рекомендации ФАТФ с изменениями по состоянию на октябрь 2025 года.](#)

⁶ [Обновленное руководство по применению риск-ориентированного подхода к виртуальным активам и провайдерам услуг виртуальных активов.](#)

⁷ Протокол DeFi — это код смарт-контракта, развернутый в блокчейне и автоматически выполняющий определенные финансовые функции, такие как торговля, кредитование или предоставление ликвидности, без участия центрального посредника.

лучшим практикам взаимодействия с механизмами DeFi. С момента публикации Руководства экосистема DeFi развивалась, и с механизмами DeFi стали взаимодействовать различные субъекты, включая регулируемые организации.

7. ФАТФ не определяет термин «DeFi» в своих Стандартах. В настоящем отчете выделяются три вида механизмов DeFi в зависимости от их систем управления и контроля:
 - о **Централизованные:** механизм DeFi имеет установленных контролирующих лиц или лиц, оказывающих достаточное влияние (например, администраторов, держателей токенов управления, разработчиков, источники финансирования). Механизмы, которые в маркетинговых целях представляют себя как по-настоящему децентрализованные, на практике могут оставаться централизованными. Такие механизмы подпадают под действие Стандартов ФАТФ и всегда должны регулироваться.
 - о **Централизованные механизмы, контролирующие лица которых не могут быть легко установлены:** контроль или достаточное влияние на механизм DeFi существует, однако лицо (лица), осуществляющее такой контроль, невозможно установить вследствие псевдонимности или других факторов. Такие механизмы подпадают под действие Стандартов ФАТФ и должны регулироваться. Вместе с тем надзорные органы могут сталкиваться с практическими трудностями при применении регуляторных мер. Если требования регулирования невозможно эффективно применить, в практических целях такие механизмы следует считать нерегулируемыми. В этих случаях юрисдикциям следует применять те же меры по снижению рисков, что и в отношении по-настоящему децентрализованных механизмов.
 - о **По-настоящему децентрализованные:** ни одно лицо не осуществляет контроль и не оказывает достаточного влияния на механизм DeFi. Такие механизмы не подпадают под действие Стандартов ФАТФ и, как правило, не регулируются.⁸
8. Странам следует применять Стандарты ФАТФ, широко толкуя соответствующие определения и одновременно учитывая практическую цель функционального подхода. На практике применительно к DeFi Стандарты ФАТФ распространяются на:
 - i. лицо (лица), осуществляющее контроль или оказывающее достаточное влияние на механизм DeFi, даже если механизм выглядит или позиционирует себя как децентрализованный. В Руководстве ФАТФ разъясняется, что при определении контроля или достаточного влияния юрисдикции могут учитывать различные факторы, включая получение лицом прибыли от механизма DeFi либо наличие у него возможности устанавливать или изменять параметры протокола. Дополнительные факторы, имеющие значение для оценки контроля и влияния, приведены в разделе 5.3 настоящего отчета. Приложение DeFi (то есть программное обеспечение) не является ПУВА согласно Стандартам ФАТФ, поскольку Стандарты не применяются к базовому программному обеспечению или технологии.
 - В качестве примера таких лиц любое лицо, которое обеспечивает доступ к механизму DeFi (например, через пользовательские интерфейсы, платформы, приложения и т. п.) и активно содействует предоставлению финансовых услуг, подпадает под определение ПУВА ФАТФ.⁹ Это особенно актуально, когда базовый механизм DeFi не регулируется в целях ПОД/ФТ.

⁸ По-настоящему децентрализованный механизм может добровольно обратиться за регуляторным надзором, чтобы продемонстрировать более высокий уровень целостности системы ПОД/ФТ и облегчить деловые отношения с обязанными организациями.

⁹ См. пункт 59 Руководства ФАТФ по ВА и ПУВА: термин «осуществляет» включает предоставление услуги и/или активное содействие ее предоставлению, то есть активное участие в осуществлении деятельности, охваченной подпунктами i)–v) определения ПУВА. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>

- ii. Любое финансовое учреждение или ПУВА, взаимодействующее с механизмами DeFi, должно проводить оценку рисков продуктов, предлагаемых механизмом DeFi, и принимать надлежащие меры по управлению выявленными рисками и их снижению в соответствии с первым пунктом P.15 о снижении рисков, связанных с новыми технологиями.
 - Если механизм DeFi регулируется, финансовым учреждениям и ПУВА следует проводить надлежащую проверку клиента (НПК) в отношении механизма DeFi и анализировать его систему ПОД/ФТ в соответствии с требованиями P.10 и P.13.
 - Если механизм DeFi не регулируется, финансовые учреждения и ПУВА должны обеспечивать, чтобы взаимодействие с ним не подрывало целостность их собственных систем ПОД/ФТ. Это может включать оценку того, насколько эффективно механизм DeFi включает гарантии ПОД/ФТ (например, встроенные решения «Знай своего клиента» (ЗСК)/НПК, использование сторонних поставщиков услуг ЗСК/НПК), и применение надлежащих мер по снижению рисков в отношении базовых пользователей механизма (например, НПК и использование инструментов мониторинга блокчейн-аналитики в режиме реального времени).
9. ФАТФ предоставляет юрисдикциям свободу усмотрения при определении критериев, используемых для оценки наличия у механизма DeFi контролирующего лица или лиц, оказывающих достаточное влияние. Вместе с тем многие юрисдикции по-прежнему сталкиваются с трудностями при выявлении и надлежащем регулировании механизмов DeFi вследствие ряда факторов:
- i. глобальный охват DeFi в сочетании с отсутствием четкой юрисдикционной привязки и, во многих случаях, определенной правовой формы осложняет регулирование, надзор и правоприменение;
 - ii. маркетинговые стратегии и заявления отдельных механизмов DeFi о «децентрализации», которые могут создавать впечатление отсутствия обязанного посредника, ответственного за соблюдение требований ПОД/ФТ;
 - iii. ограниченность информации и понимания технических, операционных и управленческих структур DeFi, что снижает способность органов точно определять наличие контроля или достаточного влияния;
 - iv. ограниченность надзорных ресурсов и технических компетенций, которая может снижать способность органов выявлять, понимать и отслеживать новые протоколы DeFi и связанные с ними решения или инструменты ПОД/ФТ.

1.2. Сфера охвата отчета

10. Цели настоящего отчета:

- i. выявить возникающие риски и уязвимости, связанные с отмыванием денег (ОД), финансированием терроризма (ФТ) и финансированием распространения оружия массового уничтожения (ФРОМУ), в экосистеме DeFi;
 - ii. разъяснить порядок применения Стандартов ФАТФ к механизмам DeFi и изложить лучшие практики и практические инструменты, которые юрисдикции могут использовать для выявления, регулирования, надзора и расследования в отношении механизмов DeFi, подпадающих под сферу действия системы ФАТФ;
 - iii. представить критерии, которые юрисдикции могут применять на риск-ориентированной основе для выявления контролируемых лиц или лиц, оказывающих достаточное влияние на механизмы DeFi;
 - iv. предложить рекомендованные меры для соответствующих заинтересованных сторон.
11. Настоящий отчет обновляет и дополняет предыдущий анализ DeFi, проведенный ФАТФ и изложенный в Руководстве 2021 года по ВА и ПУВА, с учетом существенного расширения и развития сектора после публикации этого Руководства. Настоящий целевой отчет следует рассматривать совместно с более широкими руководящими материалами и работой ФАТФ по ВА, доступными на сайте ФАТФ и в Приложении А.
12. Настоящий отчет подготовлен с учетом исследования, проведенного в рамках подготовки 7-го [Целевого обновления ФАТФ 2026 года об имплементации Стандартов ФАТФ по виртуальным активам и провайдерам услуг виртуальных активов](#). Ссылки в настоящем отчете на практику отдельных юрисдикций приводятся исключительно в качестве примеров и не должны рассматриваться как одобрение ФАТФ или подтверждение эффективности системы какой-либо юрисдикции. Как и все целевые отчеты ФАТФ, настоящий документ не имеет обязательной силы. Кроме того, юрисдикциям следует продолжить работу, чтобы в полной мере понять, каким образом с учетом собственного контекста проверять механизмы DeFi на наличие контроля или достаточного влияния.

2. Характеристики и уязвимости механизмов DeFi

2.1. Характеристики механизмов DeFi

13. Под DeFi обычно понимается широкий спектр финансовых услуг, таких как торговля, обмен, кредитование, заимствование и управление активами, предоставляемых посредством самоисполняющихся смарт-контрактов на основе блокчейна, а не традиционными финансовыми посредниками. Пользователи могут хранить средства в кастодиальных или, чаще, некастодиальных кошельках и взаимодействовать с протоколами DeFi, которые программным способом обеспечивают проведение сложных пиринговых финансовых транзакций и транзакций между пользователем и пулом. Пользователи могут взаимодействовать с механизмом DeFi напрямую — через платформу DeFi или базовый протокол — либо косвенно, через обязанную организацию (например, ПУВА).
14. Механизмы DeFi обладают общими характеристиками с более широкой экосистемой виртуальных активов: они основаны на блокчейне или технологии распределенного реестра (ТРР), обеспечивают незамедлительные трансграничные переводы и публично фиксируют

все транзакции, хотя обычно на псевдонимной основе.¹⁰ Кроме того, им присущ ряд уникальных особенностей:

- i. Автоматизация финансовых услуг на основе смарт-контрактов: протоколы DeFi используют зачастую общедоступные смарт-контракты для полной автоматизации финансовых услуг и функций, что может затруднять отнесение контроля над механизмом к конкретному лицу.
- ii. Открытая и компонуемая архитектура протоколов: протоколы DeFi, как правило, хотя и не всегда, разрабатываются как программное обеспечение с открытым исходным кодом, позволяющее любому лицу изучать, повторно использовать и воспроизводить базовый код. Это способствует быстрому созданию аналогичных протоколов DeFi. Хотя такая взаимосвязанная архитектура повышает эффективность для добросовестных пользователей, она также может использоваться противоправными субъектами для перемещения средств с беспрецедентной скоростью между несколькими уровнями DeFi и связанными организациями, включая нерегулируемых офшорных ПУВА и внебиржевых брокеров. Скорость блокчейн-транзакций в сочетании с псевдонимным доступом и возможностью быстро и последовательно выполнять автоматизированные операции посредством смарт-контрактов является значимым фактором риска и может снижать эффективность традиционных сроков надзорного и правоприменительного реагирования.
- iii. Алгоритмические рыночные механизмы и механизмы управления рисками: некоторые механизмы DeFi создают рыночные структуры, такие как автоматизированные маркет-мейкеры, пулы ликвидности и механизмы кредитования, которые алгоритмически корректируют процентные ставки и запускают автоматическую ликвидацию при нарушении пороговых значений обеспечения, нередко без участия регулируемых посредников. Эти особенности позволяют формировать сложные уровни транзакций, которые трудно отслеживать с помощью традиционных инструментов комплаенса и блокчейн-аналитики.
- iv. Предоставление ликвидности пользователями и получение комиссионного вознаграждения: механизмы DeFi позволяют пользователям выступать поставщиками ликвидности и получать комиссионное вознаграждение пропорционально своей доле в пулах ликвидности, сохраняя псевдонимность. Этой возможностью могут пользоваться противоправные субъекты, размещая и смешивая преступные доходы с крупными пулами законной ликвидности и получая комиссионное вознаграждение на такие средства.¹¹
- v. Участие: многие механизмы DeFi позволяют любому владельцу блокчейн-кошелька получать доступ к финансовым услугам и пользоваться ими без прохождения надлежащей проверки клиента. Такой зачастую открытый и неограниченный доступ создает значительные риски ОД/ФТ/ФРОМУ, поскольку противоправные субъекты могут псевдонимно входить в экосистему и использовать ее сложность для отмывания средств.

¹⁰ В данном контексте термин «псевдонимный» означает, что транзакции связываются с уникальными цифровыми идентификаторами, а не с реальными личностями, вследствие чего деятельность может быть публично наблюдаемой без прямого раскрытия личности участвующих сторон. Поэтому личности сторон транзакции неизвестны, если только механизм DeFi не проводит надлежащую проверку клиента (НПК) либо в транзакции не участвует регулируемый ПУВА, который может располагать такой информацией в рамках своей программы соблюдения требований. Хотя большинство механизмов DeFi работают по псевдонимной модели, некоторые смарт-контракты могут быть закрытыми или обеспечивать конфиденциальность, скрывая ключевые сведения, такие как суммы транзакций, адреса или логика контракта, что не позволяет третьим лицам связывать деятельность с конкретными пользователями или даже отслеживать транзакции в блокчейне.

¹¹ <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>, с. 18–19.

- vi. Зависимость от оракулов: механизмы DeFi могут зависеть от оракулов, которые передают смарт-контрактам внешние данные (например, цены активов и процентные ставки). Оракулы обеспечивают основные функции экосистемы DeFi, включая ценообразование, оценку обеспечения и механизмы ликвидации. Однако недостатки архитектуры оракулов, их управления или каналов данных могут использоваться противоправными субъектами для манипулирования входными данными и искажения рыночных условий. Такие манипуляции могут способствовать противоправной деятельности, включая мошенническую ликвидацию и отмывание преступных доходов.

2.2. Уязвимости и препятствия для эффективного надзора в сфере ПОД/ФТ/ФРОМУ

15. Механизмы DeFi имеют ряд уязвимостей, присущих более широкой экосистеме виртуальных активов.¹² Некоторые определяющие характеристики, особенно трансграничный характер, открытый исходный код и возможность проведения сложных финансовых операций, создают неотъемлемые риски. Помимо этих внутренних особенностей, экосистема DeFi также имеет структурные уязвимости, обусловленные базовой технологией, политическими решениями, системами управления и текущей стадией развития рынка. К ним относятся:
 - i. *Отсутствие нормативно-правовой базы*: многие юрисдикции Глобальной сети ФАТФ по-прежнему не имплементировали Р.15 в отношении механизмов DeFi, подпадающих под действие Стандартов ФАТФ (см. раздел 3.2). Это позволяет противоправным субъектам пользоваться неравномерной и часто фрагментарной имплементацией требований регулирования на глобальном уровне (регуляторным арбитражем) и ослабляет защиту потребителей.
 - ii. *Несоблюдение требований механизмами DeFi, подпадающими под регулирование*: механизмы DeFi, подпадающие под действие Стандартов ФАТФ, могут не регистрироваться в соответствующих компетентных органах или не реализовывать требуемые меры ПОД/ФТ, включая целевые финансовые санкции, обязательства по принципу «Знай своего клиента» (ЗСК) и НПК. Во многих механизмах также отсутствуют способы взаимодействия с правоохранительными органами (ПО) и надзорными органами, что препятствует расследованиям и надзорной деятельности.
 - iii. *Киберуязвимости*: механизмы DeFi подвержены значительным киберрискам вследствие недостатков безопасности смарт-контрактов, неодинакового уровня зрелости практики кибербезопасности и открытого исходного кода многих протоколов, позволяющего злоумышленникам анализировать код и выявлять уязвимости, пригодные для эксплуатации.¹³ Механизмы, в которых хранится значительный объем активов, являются особенно привлекательными целями для хакеров, что повышает потенциальные последствия успешных атак.¹⁴ Появление новых технологий, включая искусственный интеллект и квантовые вычисления, может дополнительно повысить эти риски.

¹² <https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html>

¹³ Некоторые авторы утверждают, что программное обеспечение с открытым исходным кодом является более устойчивым и безопасным, чем программное обеспечение с закрытым исходным кодом, поскольку более широкий круг участников, нередко технически подготовленных пользователей с различными взглядами, может проводить его проверку и вносить вклад в разработку, что повышает вероятность выявления и устранения уязвимостей. Риски, связанные с программным обеспечением с открытым исходным кодом, могут дополнительно снижаться механизмами DeFi посредством таких мер, как аудит смарт-контрактов, программы вознаграждения за обнаружение ошибок и привлечение «белых» хакеров. Другие авторы отмечают, что риски эволюционируют, а появление передового искусственного интеллекта способно усугубить киберуязвимости механизмов DeFi, в том числе за счет анализа программного обеспечения с открытым исходным кодом.

¹⁴ Дополнительную информацию о киберуязвимостях механизмов DeFi см. по адресу: <https://www.fsb.org/uploads/P160223.pdf>

- iv. *Переход к платежам без централизованных точек ввода и вывода:* по мере развития платежных систем пользователям может больше не требоваться конвертировать виртуальные активы в фиатные деньги через регулируемые финансовые учреждения или ПУВА. Кроме того, у них может уменьшиться заинтересованность в конвертации виртуальных активов в стейблкоины или депозитные токены для проведения платежей. В результате сдерживающий эффект точек регуляторного доступа¹⁵ к механизмам DeFi может ослабнуть.
- v. *Регуляторный арбитраж, основанный на границах регуляторного периметра:* хотя Стандарты ФАТФ требуют от юрисдикций выявлять механизмы DeFi, входящие в их регуляторный периметр, юрисдикции сохраняют определенную гибкость при установлении порядка такой оценки на практике. Различия в национальных подходах, отражающие внутренние политические решения, основанные на риске и контексте, могут позволять глобально распределенным механизмам DeFi размещать деятельность в юрисдикциях с менее строгой или менее четко определенной нормативно-правовой базой, тем самым повышая возможности для регуляторного арбитража.

3. Статус имплементации Стандартов ФАТФ

3.1 Применимая нормативно-правовая база

16. В соответствии с основополагающим принципом Стандарты ФАТФ технологически нейтральны, а риск-ориентированные меры ПОД/ФТ должны применяться к услугам и видам деятельности, входящим в сферу их действия, независимо от используемой технологии. Юрисдикциям следует руководствоваться принципом, согласно которому система ФАТФ применяется к физическим или юридическим лицам, которые в рамках своей деятельности оказывают финансовые услуги, охватываемые определением ПУВА.¹⁶
17. После публикации Руководства ФАТФ в 2021 году экосистема DeFi значительно эволюционировала. Она прошла путь от преимущественно технических платформ, призванных расширить доступ к финансовым услугам, до все более сложных механизмов, предлагающих широкий спектр финансовых продуктов, получающих доход и стремящихся масштабировать деятельность, в том числе посредством предоставления услуг регулируемым финансовым учреждениям. Рост инвестиций институциональных инвесторов в отдельные механизмы DeFi свидетельствует о том, что некоторые из них превращаются в более значимых поставщиков финансовых услуг, функционально сопоставимых с традиционными финансовыми учреждениями, хотя и действующих на основе блокчейн-инфраструктуры.
18. Юрисдикциям следует создать надлежащую нормативно-правовую базу, обеспечивающую, чтобы лица, осуществляющие контроль или оказывающие достаточное влияние на механизмы DeFi, применяли риск-ориентированные меры ПОД/ФТ/ПРОМУ в соответствии со Стандартами ФАТФ с учетом индикаторов, приведенных в разделе 5.3 настоящего отчета, хотя соответствующие факторы могут различаться в зависимости от конкретных характеристик механизма.¹⁷

¹⁵ Точки регуляторного доступа — это централизованные посредники, например регулируемые ПУВА, которые выступают ключевыми контрольными точками, через которые пользователи вводят средства в экосистему DeFi или выводят их из нее. Поскольку эти организации или лица обязаны соблюдать требования ПОД/ФТ, они предоставляют органам важную возможность осуществлять надзор, выявлять противоправных субъектов и пресекать финансовые преступления.

¹⁶ Пункт 68 Руководства ФАТФ по ВА и ПУВА: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>

¹⁷ Дополнительные указания по определению контроля приведены в разделе 5 настоящего отчета («Лучшие практики»).

19. Экосистема DeFi обычно описывается как многоуровневая архитектура, в которой каждый уровень опирается на расположенный ниже (так называемый «стек DeFi»). Уровни различаются по степени автоматизации и децентрализации, и Стандарты ФАТФ могут применяться к каждому из них по-разному:

- i. Уровень расчетов: базовая инфраструктура распределенного реестра (например, Ethereum, Solana, Hedera и др.), которая регистрирует транзакции и обеспечивает безопасность, консенсус и окончательный расчет по всем транзакциям, совершаемым на более высоком прикладном уровне.
 - o Стандарты ФАТФ, как правило, не применяются к платежной инфраструктуре, если только лица, действующие на этом уровне, также не оказывают услуги, подпадающие под определение ПУВА ФАТФ.
- ii. Уровень активов: включает нативные токены блокчейнов (например, ETH, SOL, HBAR и др.), являющиеся неотъемлемой частью функционирования и безопасности блокчейна, а также другие цифровые активы, созданные или запрограммированные, развернутые и функционирующие в блокчейне, включая стейблкоины. Эти активы представляют собой единицы стоимости, которыми можно торговать или иным образом использовать в финансовых транзакциях, совершаемых в протоколах DeFi или посредством них.
 - o Стандарты ФАТФ применяются к лицам, оказывающим услуги с цифровыми активами, которые подпадают под определение ПУВА ФАТФ.¹⁸
- iii. Уровень протокола: включает смарт-контракты, в которых закодирована финансовая логика, например автоматизированные маркет-мейкеры (АММ), рынки кредитования/заимствования и пулы ликвидности. Эти протоколы определяют порядок движения активов, формирования цен и правила для пользователей и представляют собой внутреннюю часть экосистемы DeFi.
 - o Стандарты ФАТФ не применяются непосредственно к смарт-контрактам, поскольку они представляют собой автоматизированное и децентрализованное программное обеспечение. Однако Стандарты ФАТФ применяются к лицам, осуществляющим контроль или оказывающим достаточное влияние на смарт-контракты.
- iv. Прикладной уровень: включает пользовательские интерфейсы, такие как веб-сайты и приложения для смартфонов, информационные панели, приложения или кошельки и иные инструменты, которые делают базовый протокол, предоставляющий услуги DeFi, доступным для пользователей без технических знаний. Большинство розничных и институциональных пользователей DeFi получают доступ к услугам через этот уровень, хотя это не является обязательным. Прикладной уровень может управляться отдельно от уровня протокола и иметь иных контролирующих лиц.
 - o Стандарты ФАТФ применяются к лицам, действующим на прикладном уровне, в той мере, в какой они предоставляют услуги ПУВА или содействуют их предоставлению.
- v. Уровень агрегации: включает офчейн- и/или ончейн-протоколы, позволяющие объединять многочисленные протоколы DeFi в одном удобном месте на прикладном уровне. Агрегаторы предназначены для предоставления конечным пользователям

¹⁸ <https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html>

оптимального способа предоставления активов в кредит, покупки или продажи активов, выпуска новых активов и т. п.¹⁹

- о Стандарты ФАТФ применяются к лицам, действующим на уровне агрегации, в той мере, в какой они предоставляют услуги ПУВА или содействуют их предоставлению.²⁰

Вставка 1. Позиция международных органов в отношении механизмов DeFi

Стандарты ФАТФ технологически нейтральны, то есть механизмы DeFi подлежат применению мер ПОД/ФТ/ПРОМУ, если они осуществляют один или несколько видов деятельности, охватываемых Рекомендациями ФАТФ. Другие международные органы также подчеркивали принцип технологической нейтральности применительно к DeFi, призывая к *регуляторному паритету* и достижению механизмами DeFi результатов в области защиты инвесторов и целостности рынка, сопоставимых с традиционными финансовыми рынками. На практике этот подход может быть реализован посредством *функционального анализа*, сосредоточенного на деятельности, осуществляемой механизмами DeFi, и на том, каким образом действующие нормативно-правовые системы могут применяться или адаптироваться к контексту DeFi.

Совет по финансовой стабильности (СФС): по оценке СФС, DeFi воспроизводит отдельные функции традиционной финансовой системы, вследствие чего наследует и иногда усиливает обычные уязвимости, например автоматическую ликвидацию позиций по дериватам, встроенную в смарт-контракты.²¹

Международная организация комиссий по ценным бумагам (IOSCO): по оценке IOSCO, в соответствии с принципом «одинаковая деятельность, одинаковый риск, одинаковое регулирование/регуляторный результат» регуляторам следует анализировать механизмы DeFi в своих юрисдикциях для применения к ним нормативно-правовых систем, когда это применимо. Им следует стремиться выявлять лиц или организации, осуществляющие контроль или оказывающие достаточное влияние на финансовые продукты и услуги, предлагаемые механизмами DeFi, и требовать от них раскрытия ясной и всесторонней информации для содействия защите инвесторов и целостности рынка. IOSCO также отмечает важность регуляторного сотрудничества для реагирования на трансграничные риски и потенциальный регуляторный арбитраж.²²

¹⁹ <https://hedera.com/learning/defi-stack/#:~:text=The%20DeFi%20ecosystem%20is%20built,the%20settlement%20and%20asset%20layers>

²⁰ К примерам агрегаторов, которые могут не подпадать под определение ПУВА ФАТФ, относятся агрегаторы, которые лишь предоставляют информационные или сравнительные услуги, например информационные панели или агрегаторы цен, отображающие общедоступные рыночные данные, но не контролируют перевод виртуальных активов и не содействуют ему. Аналогичным образом интерфейсы, которые позволяют пользователям исключительно просматривать, анализировать или сравнивать протоколы DeFi, не выполняя транзакции, не направляя поручения и иным образом не участвуя в переводе, обмене или хранении активов, могут не соответствовать определению ПУВА. Классификация таких агрегаторов должна проводиться в каждом конкретном случае с учетом того, осуществляют ли они деятельность, охватываемую определением ПУВА в Стандартах ФАТФ, или содействуют ее осуществлению.

²¹ <https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/>

²² [FR14/23 Итоговый отчет с рекомендациями по вопросам политики в области децентрализованных финансов \(DeFi\).](#)

Международный валютный фонд (МВФ): МВФ рассматривает DeFi как инновационное, но сопряженное с высокими рисками направление, которое остается в пределах регуляторного периметра и по мере усиления взаимосвязей с традиционной финансовой системой может создавать риски для финансовой стабильности и целостности финансовой системы. МВФ подчеркивает, что многие механизмы DeFi сохраняют фактическое управление или контроль через разработчиков, концентрированное владение токенами управления, архитектуру протокола или децентрализованные автономные организации (DAO), вследствие чего к ним могут по-прежнему применяться регуляторные обязанности и ожидания в сфере ПОД/ФТ. Поэтому МВФ выступает за технологически нейтральный и функциональный подход к регулированию, сосредоточенный на рисках, а не правовой форме, включая выявление регуляторных «якорей» в случаях наличия контроля или экономической выгоды и применение соразмерных мер по снижению рисков, в том числе ограничений, если риски невозможно надлежащим образом контролировать.²³

3.2. Имплементация Рекомендации 15 в отношении механизмов DeFi юрисдикциями

20. С 2021 года ФАТФ собирает данные и отслеживает развитие рынка в экосистеме DeFi в рамках целевых обновлений об имплементации Стандартов ФАТФ по ВА и ПУВА.²⁴ Согласно Целевому обновлению 2026 года, большинство ответивших юрисдикций²⁵ еще не имплементировали Р.15 в отношении механизмов DeFi, подпадающих под действие Стандартов ФАТФ. Лишь меньшинство юрисдикций (26 из 142) оценило риски, связанные с DeFi, тогда как подавляющее большинство (132 из 142) не выявило на своей территории ни одного соответствующего механизма. Кроме того, только четыре юрисдикции ввели требования лицензирования и регистрации, и лишь две фактически лицензировали или зарегистрировали такие механизмы.
21. Эти результаты свидетельствуют о том, что страны по-прежнему сталкиваются со значительными трудностями при применении Р.15 к механизмам DeFi, включая:
 - i. проведение надлежащей оценки рисков с учетом сложных структур управления DeFi и его трансграничного характера;
 - ii. выявление механизмов DeFi, подпадающих под нормативно-правовую базу юрисдикции;
 - iii. выявление лиц, если таковые имеются, которые осуществляют контроль или оказывают достаточное влияние на механизм DeFi;
 - iv. применение регуляторных или правоприменительных мер к механизмам DeFi, которые подпадают под сферу регулирования, но не соблюдают применимые требования.

²³ <https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/>

²⁴ 2025-Targeted-Update-VA-VASPs.pdf.coredownload.pdf; <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASPpdf.coredownload.inline.pdf>; <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html>; <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html>

²⁵ Настоящая статистика основана на результатах Опроса ФАТФ 2026 года о состоянии имплементации Р.15. Информацию предоставили в общей сложности 142 юрисдикции.

22. Трудности имплементации P.15 отчасти обусловлены неточным использованием термина «механизм DeFi», которое позволяет некоторым механизмам позиционировать себя как децентрализованные, несмотря на наличие централизованного управления или контроля. При наличии такого контроля или достаточного влияния эти механизмы подпадают под действие Стандартов ФАТФ и должны подлежать надлежащему регулированию.

Вставка 2. Риск-ориентированный подход и соображения существенности

Хотя настоящее руководство призвано внести дополнительную ясность в применение P.15 в контексте экосистемы DeFi, оно признает, что степень подверженности стран потенциальным рискам ОД/ФТ/ФРОМУ, связанным с DeFi, существенно различается. Юрисдикциям Глобальной сети ФАТФ следует применять Стандарты ФАТФ в соответствии с национальным профилем риска и существенностью, руководствуясь риск-ориентированным подходом. Странам следует определять наиболее значимые риски ОД/ФТ/ФРОМУ и соответствующим образом расставлять приоритеты в мерах реагирования и снижения рисков.

Стандарты ФАТФ требуют от всех юрисдикций оценивать риски ОД/ФТ, связанные с ВА и ПУВА, включая DeFi. Юрисдикциям с более значительным объемом деятельности DeFi следует выделять больше ресурсов на ее понимание и надзор, а также на разработку подходов к снижению рисков противоправного финансирования, связанных с механизмами DeFi, с учетом особенностей сектора. И напротив, юрисдикциям с ограниченными возможностями и меньшей подверженностью рискам ВА, ПУВА и DeFi следует выделять меньше ресурсов, соразмерно выявленным рискам, сосредоточившись, например, на мониторинге рыночных изменений и возникающих типологий.

С точки зрения существенности имеющиеся данные свидетельствуют о высокой концентрации деятельности DeFi: на Северную Америку и Европу приходится около 60% глобальной деятельности, тогда как совокупная доля Ближнего Востока и Африки оценивается менее чем в 10%.^{26, 27} Аналогичным образом, несмотря на большое число механизмов DeFi, многие из которых имеют небольшой масштаб, неактивны или дублируют друг друга, деятельность в секторе также характеризуется высокой концентрацией. На 12 крупнейших протоколов приходится более 60% глобального TVL, а 20 крупнейших протоколов, по оценкам, обеспечивают свыше 70% совокупной ликвидности DeFi.²⁸ Поэтому при регулировании и надзоре следует учитывать такую асимметрию рынка и уделять приоритетное внимание взаимодействию с крупнейшими и наиболее системно значимыми протоколами DeFi и связанными с ними заинтересованными сторонами.

²⁶ <https://coinlaw.io/decentralized-finance-market-statistics/>; <https://www.chainalysis.com/blog/middle-east-north-africa-crypto-adoption-2024/>

²⁷ Региональная деятельность DeFi обычно оценивается на основе совокупности косвенных показателей, включая TVL, объемы транзакций и торгов, участие пользователей и потоки капитала, при этом географическая принадлежность определяется по таким данным, как активность на биржевых точках ввода, кластеризация кошельков, модели использования платформ и происхождение инвестиций.

²⁸ <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

4. Риски финансовых преступлений и типологии, связанные с механизмами DeFi

4.1. Субъекты угроз, риски и типологии

23. Противоправные субъекты используют как неотъемлемые характеристики, так и уязвимости механизмов DeFi. Эти риски дополнительно усиливаются при отсутствии эффективного регулирования или его недостаточной имплементации, особенно в отношении механизмов, подпадающих под действие Стандартов ФАТФ, но не выполняющих применимые обязательства.

Мошенники

24. В последние годы масштабы мошенничества, связанного с виртуальными активами, во всем мире росли экспоненциально, а механизмы DeFi все чаще используются для отмывания преступных доходов.²⁹ Кроме того, отдельные мошеннические схемы непосредственно эксплуатируют протоколы DeFi или выдаются за платформы DeFi с целью обмана потерпевших. Хотя механизмы DeFi способны поддерживать инновационные платежные решения, они также могут предоставлять сложные финансовые услуги пользователям с низким уровнем финансовой грамотности, что по мере их более широкого распространения вызывает серьезные опасения в сфере защиты потребителей.³⁰

Вставка 3. Тематические исследования: схема с токеном SafeMoon и дело Forsage (США)

Схема с токеном SafeMoon

В схеме с токеном SafeMoon (SFM), действовавшей с марта 2021 года по июнь 2022 года, участвовало более двух миллионов инвесторов, а ее рыночная капитализация превышала 9 млрд долларов США. В ходе расследования было установлено, что лицо X, первоначальный разработчик SafeMoon (SFM), создало мошенническую схему, основанную на ложных заявлениях о заблокированной ликвидности и отсутствии инсайдерской торговли. Несмотря на заявления о защищенности пулов ликвидности, лицо X и двое соучастников тайно сохранили контроль над ликвидностью посредством токенов поставщиков ликвидности (LP), что позволило им выводить крупные объемы SFM для личной выгоды. За несколько недель в начале 2021 года они вывели десятки триллионов SFM и в итоге получили прибыль свыше 7 млн долларов США, которую использовали для приобретения предметов роскоши, инвестиций в недвижимость и личной торговли. Лицу X были предъявлены обвинения в сговоре с целью совершения мошенничества с ценными бумагами, мошенничества с использованием средств связи и отмывания денег.

Дело Forsage

Лицо X и трое соучредителей создали и контролировали Forsage — платформу, которая рекламировалась как законная инвестиционная возможность DeFi на основе смарт-контрактов. В действительности Forsage представляла собой схему Понци и финансовую пирамиду, действовавшую в сетях Ethereum, Binance Smart Chain и Tron. Инвесторы должны были приобретать «слоты», приносящие доход за счет привлечения новых

²⁹ <https://www.chainalysis.com/blog/crypto-scams-2026/>

³⁰ Дополнительный анализ вопросов защиты потребителей в DeFi см. в документах БМР и IOSCO: <https://www.bis.org/publ/bppdf/bispap156.pdf>; <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>

участников и распределения прибыли, однако после внесения платежей средства необратимо перераспределялись между более ранними участниками. Лицо X и ее соучастники контролировали кошельки верхнего уровня, например Forsage ID 1, которые получали наибольший доход и не требовали вложения каких-либо средств. Хотя Forsage заявляла, что доход прозрачно и полностью распределяется между пользователями, часть кода смарт-контракта (в частности, контракт xGold) напрямую переводила средства на кошельки, контролируемые учредителями. Большинство инвесторов в конечном итоге потеряли средства, а кошелек лица X оказался единственным, получившим более 1 млн долларов США. В настоящее время соучастникам предъявлены обвинения в мошенничестве за введение инвесторов в заблуждение и организацию схемы с использованием средств электронной связи.

Источник: INTERPOL, Соединенные Штаты

Сети профессиональных отмывателей (PMLN) и транснациональная организованная преступность

25. Широкий круг противоправных субъектов, часто связанных с транснациональными преступными организациями, все активнее использует сети профессиональных отмывателей (PMLN) для отмывания средств через механизмы DeFi. Эти сети применяют сложные методы расслоения, призванные скрыть след транзакций и обойти централизованные биржи, применяющие меры ПОД/ФТ. Как правило, средства дробятся и перемещаются через многочисленные кошельки, после чего направляются через сервисы DeFi, такие как децентрализованные биржи, межсетевые мосты, миксеры и свопы, для создания сложной многоуровневой структуры сокрытия, нередко с использованием быстрых автоматизированных транзакций и перемещения между блокчейнами. После длительного расслоения средства консолидируются и выводятся в фиатные деньги через централизованные биржи со слабыми мерами контроля либо нелицензированных внебиржевых (ОТС) брокеров, а затем возвращаются клиентам через подпольные банковские системы и неформальные системы перевода ценностей.³¹

Сети финансирования распространения оружия массового уничтожения

26. Связанные с государством КНДР высокотехнологичные группы все чаще совершают кибератаки на механизмы DeFi и применяют в экосистеме DeFi сложные многоуровневые методы отмывания для получения доходов в целях финансирования распространения оружия массового уничтожения. В апреле 2026 года на две крупные атаки на платформы DeFi, приписываемые КНДР, пришлось около 76% годовых убытков от взломов, связанных с виртуальными активами:³²
 - i. Взлом Drift Protocol — крупной децентрализованной биржи бессрочных фьючерсов в сети Solana — на сумму 285 млн долларов США широко приписывался субъектам, связанным с КНДР, и был осуществлен примерно за 12 минут.³³ Злоумышленники с помощью социальной инженерии получили предварительно авторизованные мультиподписные транзакции, воспользовались удалением ключевого механизма временной блокировки и ввели фиктивный токен, который оракулы приняли в ка-

³¹ [Addressing APAC's Informal Crypto Market: P2P & OTC Trading — Regulation Asia.](#)

³² https://www.trmlabs.com/resources/blog/north-korea-stole-76-of-all-crypto-hack-value-in-2026-with-just-two-attacks?trk=public_post_comment-text

³³ <https://www.trmlabs.com/resources/blog/north-korean-hackers-attack-drift-protocol-in-285-million-heist>; <https://www.chainalysis.com/blog/lessons-from-the-drift-hack/>; <https://www.elliptic.co/blog/drift-protocol-exploited-for-286-million-in-suspected-dprk-linked-attack>

честве действительного обеспечения. Это позволило искусственно завысить стоимость токена и быстро вывести значительный объем реальных активов. Инцидент выявил критические уязвимости в управлении, архитектуре оракулов и операционной безопасности, а также растущую сложность атак на механизмы DeFi.

- ii. Эксплуатация уязвимости KelpDAO привела к потерям в размере около 292 млн долларов США вследствие использования недостатка архитектуры с единственным верификатором в мосте LayerZero. Злоумышленник манипулировал межсетевой валидацией, чтобы вывести средства из протокола. Хотя около 75 млн долларов США похищенных активов удалось заморозить, оставшиеся преступные доходы были отмыты через THORChain, что подчеркивает уязвимости архитектуры мостов и сложности отслеживания и возврата преступных межсетевых потоков.
27. По данным компаний, занимающихся блокчейн-аналитикой, связанные с КНДР хакеры используют различные способы обхода мер контроля, включая атаки на механизмы DeFi, не применяющие меры ПОД/ФТ либо применяющие их в ограниченном объеме; проведение через механизмы DeFi частых, структурированных, зачастую автоматизированных транзакций на небольшие суммы; а также преднамеренное смешение незаконных средств с крупными пулами несвязанных или законных активов для дополнительного сокрытия их происхождения.³⁴
28. Имеются свидетельства того, что иранские сети финансирования распространения оружия массового уничтожения использовали отдельные инструменты экосистемы DeFi и блокчейна, такие как мосты, миксеры и механизмы межсетевого перевода, для сокрытия движения средств, хотя основная часть их деятельности по-прежнему основывается на злоупотреблении централизованными биржами и платежными каналами на основе стейблкоинов.³⁵

Группы программ-вымогателей и хакеры

29. В последние годы атаки программ-вымогателей и преступные взломы стали более сложными, в том числе за счет злоупотребления механизмами DeFi. Субъекты, использующие программы-вымогатели, преимущественно требуют оплату в виртуальных активах и все чаще применяют механизмы DeFi, включая децентрализованные биржи (DEX), свопы и межсетевые инструменты, чтобы сразу после атаки конвертировать доходы в другие виртуальные активы и скрыть происхождение средств. Они также активно используют миксеры для дополнительного сокрытия последующего движения незаконных средств. Киберпреступники, кроме того, эксплуатируют уязвимости в смарт-контрактах, управляющих механизмами DeFi, для хищения виртуальных активов; скорость перемещения между блокчейнами и транзакций DeFi нередко позволяет отмыть средства до того, как отрасль или правоохранные органы смогут отреагировать.

³⁴ [North Korea IT Workers: Inside the DPRK's Crypto Laundering Network.](#)

³⁵ [Targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf](#)

Вставка 4. Типология риска — атака на систему управления

Мошенники могут использовать особенности структуры децентрализованных автономных организаций (DAO), управляющих многими механизмами DeFi. DAO позволяет пользователям, владеющим токенами управления механизма, голосовать по критически важным изменениям или обновлениям протокола. Противоправные субъекты могут накапливать токены управления, иногда с использованием мгновенных займов, чтобы получить фактический контроль над системой управления законного механизма DeFi. После получения контроля мошенники могут изменять ключевые параметры смарт-контрактов, перенаправлять средства или выполнять вредоносные предложения для хищения активов, хранящихся в протоколе.

5. Лучшие практики имплементации P.15 в отношении механизмов DeFi

30. В настоящем разделе изложены лучшие практики, которую юрисдикции могут применять для снижения рисков, выявленных в предыдущих разделах. Раздел охватывает выявление и установление контролирующих лиц механизмов DeFi, лицензирование, регистрацию и надзор.
31. Регуляторам и надзорным органам следует разграничивать децентрализованный характер базовой технологии DeFi, создающий возможности для финансовых инноваций, и управление механизмами DeFi, которое на практике может быть централизованным и, следовательно, подпадать под требования ПОД/ФТ. Органам следует тщательно оценивать, является ли управление механизмом DeFi понастоящему децентрализованным либо механизм лишь заявляет о децентрализации, тогда как в действительности контроль остается сосредоточенным у определенных лиц.

5.1. Эффективная оценка рисков механизмов DeFi

32. Большинство юрисдикций по-прежнему испытывают трудности с надлежащим выявлением и оценкой рисков ОД/ФТ/ФРОМУ, связанных с DeFi (см. раздел 3.2). Юрисдикциям следует понимать общую степень своей подверженности деятельности DeFi и проводить оценку рисков сектора DeFi, соответствующую национальному контексту. Такая оценка может быть включена в существующие национальные, секторальные или отраслевые оценки рисков, включая оценку рисков ВА и ПУВА. В рамках оценки следует определить характер и существенность рисков ОД/ФТ/ФРОМУ, связанных с DeFi, в том числе степень внутренней подверженности, трансграничные аспекты и потенциальные уязвимости, возникающие вследствие функционирования, управления и использования механизмов DeFi. Для общих принципов, применимых также к оценке рисков DeFi, юрисдикции могут обращаться к руководству ФАТФ по оценке рисков.³⁶
33. Кроме того, P.15 требует, чтобы механизмы DeFi, подпадающие под действие Стандартов ФАТФ, проводили оценку рисков ОД/ФТ на институциональном уровне и до запуска или использования программного обеспечения либо платформы. Такие механизмы DeFi также должны принимать надлежащие меры по управлению рисками ОД/ФТ/ФРОМУ и их снижению на постоянной и перспективной основе, а также применять надлежащие меры внутреннего контроля и снижения рисков в рамках эффективной системы комплаенса.³⁷

³⁶ <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Money%20Laundering%20National%20Risk%20Assessment%20Guidance.pdf.coredownload.inline.pdf>; <https://www.fatf-gafi.org/en/publications/Methodsand Trends/quick-guide-on-assessing-ML-risks-of-VA-and-VASPs.html>

³⁷ <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf>

Вставка 5. Проведение оценки рисков механизмов DeFi

Соединенные Штаты

В опубликованной Министерством финансов США в апреле 2023 года Оценке рисков противоправного финансирования в сфере децентрализованных финансов (DeFi)³⁸ применяется риск-ориентированная и функциональная методология оценки возможного использования деятельности DeFi в целях противоправного финансирования. Оценка сочетает качественный анализ известных типологий с тематическими исследованиями, блокчейн-криминалистикой и консультациями с правоохранительными органами, регуляторами и экспертами частного сектора США. Вместо рассмотрения DeFi как единой категории в ней оцениваются риски различных функций DeFi (таких как децентрализованные биржи, протоколы кредитования, мосты и механизмы, аналогичные миксерам), выявляются соответствующие субъекты, способные осуществлять контроль или оказывать услуги, и сопоставляется эта деятельность с этапами цикла отмывания денег. В отчете рассматриваются основные области угроз, включая ОД, ФТ, программы-вымогатели, обход санкций, мошенничество и хищение, а также структурные уязвимости, такие как псевдонимность, автоматизация, отсутствие посредников и трансграничный охват. Важно, что отчет разграничивает вопрос о том, могут ли отдельные механизмы DeFi квалифицироваться как регулируемые организации в рамках действующих в США систем ПОД/ФТ, и более широкие практические трудности надзора и правоприменения, одновременно указывая на действующие меры снижения рисков и пробелы в политике.

Гонконг, Китай

Гонконг, Китай, на постоянной основе оценивает риски, связанные с децентрализованными финансами (DeFi), сочетая мониторинг рынка, оперативную информацию и анализ конкретных случаев. Поскольку многие протоколы DeFi действуют без официального создания юридического лица или регистрации в какой-либо одной юрисдикции, Полиция Гонконга (НКРПФ) непрерывно отслеживает изменения в глобальной экосистеме DeFi. Это включает анализ широко используемых протоколов DeFi, изучение их структур управления, операционных моделей и механизмов получения дохода, а также оценку потенциальных уязвимостей, которые могут использоваться в целях противоправного финансирования.

5.2. Определение контролирующих лиц механизмов DeFi

34. Одна из основных проблем для юрисдикций заключается в определении того, что представляет собой «контроль или достаточное влияние» на механизм DeFi. Руководство ФАТФ разъясняет, что под контролем следует понимать способность принимать ключевые решения в рамках механизма DeFi. Контролирующим лицом (лицами) механизма DeFi может быть любое лицо, которое на практике уполномочено определять ключевые операции протокола или предоставление услуг пользователям либо существенно влиять на них и/или получает значительную экономическую выгоду от такой деятельности.³⁹ «Значительная экономическая

³⁸ <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

³⁹ При рассмотрении вопроса о контроле механизмов DeFi юрисдикции также могут обращаться к Рекомендациям IOSCO по вопросам политики в области DeFi и рекомендациям о необходимости устанавливать «ответственных лиц»: <https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf>

ская выгода» не включает широко распределенные доходы (например, рост цены или вознаграждения), получаемые держателями токенов, которые не осуществляют контроль и не оказывают влияние на механизм. Контролирующие лица могут иметь возможность:

- i. *направлять, утверждать или влиять на выполнение действий на уровне протокола, включая, помимо прочего, распределение экономических вознаграждений, комиссий или эмиссии среди пользователей либо участников;*
- ii. *изменять, обновлять, приостанавливать или прекращать работу протокола либо любого из компонентов его смарт-контракта с помощью ключей обновления, административных полномочий, аварийных функций или механизмов управления;*
- iii. *определять, распределять или управлять активами протокола либо казначейскими ресурсами, включая полномочия размещать, перераспределять или отчуждать активы от имени механизма;*
- iv. *добавлять, удалять, включать в белый список или иным образом определять участников, валидаторов либо иных критически важных пользователей, взаимодействующих с протоколом DeFi или его компонентами, которые в конечном итоге содействуют предоставлению финансовых услуг;*
- v. *назначать, отстранять или оказывать влияние на лиц, выполняющих ключевые управленческие, операционные или административные функции, включая разработчиков, подписантов мультиподписных кошельков⁴⁰, операторов оракулов или делегатов управления.*

35. Юрисдикции могут сталкиваться с различными практическими трудностями при установлении контролирующих лиц, особенно если влияние осуществляется косвенно, неформально либо посредством децентрализованного управления и технических механизмов. Для установления контролирующих лиц юрисдикции могут использовать ряд взаимодополняющих источников информации, включая:

- i. **информацию из открытых источников:** общедоступные данные блокчейна, документацию протокола, предложения по управлению и результаты голосования, опубликованные аудиторские заключения, веб-сайты, блоги, активность в социальных сетях, форумы и иные онлайн-коммуникации, которые могут выявлять модели влияния, полномочия по принятию решений или получение экономической выгоды;
- ii. **информацию третьих сторон:** блокчейн-аналитику, криминалистический анализ, аудиторские отчеты, картирование потоков транзакций, раскрытие информации поставщиками услуг (такими как операторы пользовательских интерфейсов, кастодианы или поставщики оракулов), сведения, полученные в ходе надзорного взаимодействия, а также отчеты научных, отраслевых или исследовательских организаций, материалы конференций и хакатонов;
- iii. **разведывательную информацию, предоставленную ПФР или правоохранительными органами:** включая сообщения о подозрительных операциях (СПО), результаты расследований, изъятые цифровые доказательства или сообщения (например, переписку в приложениях для обмена мгновенными сообщениями, электронные письма или каналы координации), способные подтвердить фактиче-

⁴⁰ Подписанты мультиподписного кошелька — это физические лица или организации, которые совместно контролируют блокчейн-счет, смарт-контракт или административную функцию посредством мультиподписного кошелька. Для авторизации транзакции или решения в рамках механизма DeFi требуются их подтверждения (подписи).

ский контроль, координацию или полномочия по принятию решений, осуществляемые конкретными лицами или группами в рамках механизма DeFi.

5.3. Факторы для определения контроля в механизмах DeFi

36. ФАТФ не устанавливает фиксированный набор критериев для выявления лиц, способных осуществлять контроль или оказывать достаточное влияние на механизм DeFi. Вместе с тем в настоящем отчете предлагаются индикаторы (см. ниже), которые надзорные органы могут использовать наряду с другими для установления контролирующих лиц механизмов DeFi, созданных или действующих на их территории. Эти индикаторы следует применять гибко с учетом различных операционных структур и структур управления.
37. Степень централизации структур управления механизмами DeFi может различаться. Исследования показывают, что в некоторых случаях более сложные и зрелые механизмы DeFi сохраняют установленных контролирующих лиц, которые получают выгоду от базовой коммерческой деятельности и продолжают с течением времени осуществлять полномочия по принятию решений, в том числе при переходе механизма к модели децентрализованной автономной организации (DAO).⁴¹ Приведенные ниже возможные индикаторы носят ориентировочный и неисчерпывающий характер.

Ончейн-индикаторы контроля:

- i. **Возможность обновления и скрытые привилегии:** наличие обновляемых контрактов, прокси-шаблонов или функций аварийного отключения, особенно если такие полномочия сохраняются за конкретным лицом или группой, может указывать на централизованный контроль. Хотя прозрачно раскрытые аварийные функции, сохраняемые в целях безопасности и защиты (например, для защиты активов при кибератаке), сами по себе могут как указывать, так и не указывать на контроль, нераскрытые или односторонние права доступа конкретных лиц, которые при злоупотреблении способны создавать существенные риски (например, скрытый доступ), часто свидетельствуют о контроле.
- ii. **Установление параметров:** права лица или группы в одностороннем порядке устанавливать или изменять ключевые параметры протокола, включая лимиты риска, комиссии, вознаграждения, коэффициенты обеспечения либо аналогичные экономические или операционные настройки, являются существенными индикаторами контроля.
- iii. **Контроль над оракулами:** возможность выбирать, настраивать или изменять каналы ценовых и иных данных оракулов, включая переход к ручному ценообразованию или переопределение входных данных оракула, может указывать на контроль.
- iv. **Контроль над критически важной инфраструктурой смарт-контрактов протокола:** исключительный или доминирующий контроль над ключами развертывания, реестрами контрактов либо основными зависимостями контрактов (например, автоматизированными киперами, сетями исполнителей, расчетными контрактами) может указывать на прямое операционное влияние на целостность и непрерывность работы протокола.
- v. **Потоки комиссий и прибыль:** наличие контроля может предполагаться, если конкретные адреса получают экономические потоки на уровне протокола, такие

⁴¹ https://www.bis.org/publ/qtrpdf/r_qt2112b.htm;
<https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3208~051a880042.en.pdf>

как комиссии, возвраты максимальной извлекаемой стоимости (MEV), штрафы при ликвидации или эмиссия токенов (то есть вновь выпущенные токены). Такие потоки могут свидетельствовать о сохраняющемся влиянии или контроле со стороны получателей.

- vi. **Администрирование / контроль доступа:** если доступ к пулам ликвидности или функциям протокола разрешен только утвержденным участникам или участникам из белого списка, лица, администрирующие такие разрешения и определяющие права доступа, могут быть признаны контролирующими лицами.
- vii. **Концентрация управления и право голоса:** концентрированное владение токенами управления, влиятельные блоки делегированных голосов или низкий уровень участия, позволяющий небольшому числу субъектов определять результаты управления, могут указывать на фактический контроль над стратегическими решениями, обновлениями и распределением казначейских ресурсов.

Офчейн-индикаторы контроля:

- viii. **Хранение и операционная деятельность:** лица, назначенные подписантами решений по управлению или административным вопросам, лица, контролирующие ключи обновления, а также лица, координирующие или получающие услуги хранения в отношении активов от имени механизма, могут обоснованно признаваться контролирующими лицами, поскольку способны влиять на критически важные операционные функции или функции безопасности.⁴²
- ix. **Эксплуатация и распространение пользовательских интерфейсов:** контроль над общедоступными веб-интерфейсами (включая мобильные приложения) и связанными материалами или инструментами (например, кошельками) может указывать на централизованное влияние, поскольку лица, эксплуатирующие, поддерживающие или распространяющие такие интерфейсы, способны определять порядок доступа пользователей к механизму DeFi и взаимодействия с ним.
- x. **Корпоративные организации:** компании, фонды, лаборатории, операционные компании или иные юридические лица, которые нанимают ключевых участников, владеют правами интеллектуальной собственности, управляют казначействами либо оплачивают услуги поставщиков, могут осуществлять централизованный контроль. Степень контроля зависит от их фактической независимости от протокола и от того, насколько они влияют на управление, разработку или операционную деятельность.
- xi. **Контроль над разработкой, дорожной картой или офчейн-инфраструктурой:** лица, определяющие приоритеты разработки, контролирующие релизы или управляющие важнейшей офчейн-инфраструктурой (например, индексаторами, сервисами данных и системами автоматизации), могут оказывать существенное влияние на направление развития и функционирование механизма DeFi. Этот индикатор следует отличать от деятельности отдельных разработчиков, которые вносят вклад в инфраструктуру механизмов DeFi, но не осуществляют реального контроля.

⁴² К таким функциям относятся, например, подписанты казначейских или резервных кошельков, в которых хранятся средства протокола; администраторы мультиподписных кошельков, используемых для исполнения решений органов управления; владельцы ключей обновления, позволяющих изменять смарт-контракты; или организации, координирующие кастодиальные механизмы в отношении активов пользователей либо протокола. Эти функции обеспечивают практический контроль над ключевыми аспектами механизма, включая движение средств, реализацию изменений протокола и снижение последствий инцидентов безопасности.

- хii. **Брендинг, коммуникации и направление пользователей:** контроль над официальным брендингом, публичными сообщениями, документацией, раскрытием информации о рисках или образовательными материалами может указывать на влияние.
38. К контролирующим лицам механизмов DeFi могут относиться лица, выполняющие различные функции и несущие различные обязанности в рамках механизма. Наличие нескольких контролирующих лиц, управляющих различными компонентами механизма DeFi, само по себе не отменяет и не уменьшает обязательств в сфере ПОД/ФТ. На практике большинство механизмов DeFi предоставляют финансовые услуги, аналогичные услугам, охватываемым определениями финансового учреждения и ПУВА ФАТФ,⁴³ и любое лицо, осуществляющее контроль или оказывающее достаточное влияние на механизм, следует считать предоставляющим финансовые услуги либо активно содействующим их предоставлению.
39. Контролирующими лицами могут быть разработчики, держатели токенов управления, основные сопровождающие, операторы пользовательских интерфейсов, инвесторы, поставщики оракулов (и иных данных), фонды или корпоративные организации. Этот перечень не является исчерпывающим; в зависимости от конкретных характеристик механизма DeFi функции контролирующих лиц могут пересекаться, а сами лица — относиться к нескольким категориям. Юрисдикциям следует применять функциональный подход к установлению контролирующих лиц в контексте DeFi, оценивая, кто фактически контролирует различные аспекты механизма или влияет на них. Например, в отдельных юрисдикциях организации, эксплуатирующие веб-сайты или интерфейсы, которые облегчают взаимодействие пользователей с протоколами DeFi, могут входить в регуляторный периметр, если они предоставляют услуги с ВА или «организуют» их предоставление, даже не имея прямого контроля над базовыми смарт-контрактами. Другие юрисдикции могут применять иной подход.

⁴³ Некоторые механизмы DeFi не предоставляют финансовые услуги и поэтому не подпадают под действие Стандартов ФАТФ. Обычно к ним относятся протоколы или платформы, поддерживающие инфраструктурные, управленческие или информационные функции, а не содействующие переводу, обмену или хранению активов. Например, платформы децентрализованного управления, позволяющие держателям токенов голосовать за изменения протокола, блокчейн-оракулы, предоставляющие внешние данные смарт-контрактам, а также инструменты разработчиков или интерфейсы протоколов, позволяющие пользователям взаимодействовать с блокчейн-сетями, сами по себе не являются финансовыми услугами.

Вставка 6. Меры Японии по разработке надлежащей и соразмерной нормативно-правовой базы для контроля механизмов DeFi

Агентство финансовых услуг Японии (JFSA) обсуждало подходы к регулированию систем криптоактивов в рамках Рабочей группы по системам криптоактивов Совета по финансовой системе с участием экспертов частного сектора. В ходе обсуждений JFSA обращалось к вопросам DeFi. В отчете Рабочей группы, опубликованном в декабре 2025 года, отмечалось, что организации, предоставляющие жителям Японии пользовательские интерфейсы, например приложения, соединяющие пользователей с децентрализованными биржами (DEX), возможно, должны подлежать регулированию, соразмерному рискам. Такое регулирование может включать обязанности по ясному разъяснению рисков, связанных с подключаемыми услугами, а также требования ПОД/ФТ, включая обязательства по НПК в соответствии с Законом Японии о ПОД/ФТ.

Кроме того, в отчете указано, что, хотя разработка и развертывание протоколов DEX могут не подпадать под действующую правовую систему, протоколы DEX имеют недостатки или уязвимости и также создают риск использования для отмывания денег. В отчете отмечается необходимость продолжать изучение соразмерных и специфичных для технологии мер по снижению рисков, отличных от мер, применимых к действующим поставщикам биржевых услуг, с надлежащим учетом международных дискуссий по вопросам регулирования. Опираясь на направления, изложенные в отчете, JFSA продолжает углублять анализ и укреплять взаимодействие с заинтересованными сторонами DeFi, проводя специальные круглые столы с компаниями частного сектора и другими соответствующими участниками.

Источник: Япония

5.4. Оценка контроля над механизмами DeFi

40. Хотя многие механизмы DeFi представляют себя как децентрализованные, в ряде случаев у них могут быть контролирующие лица, сохраняющие полномочия по принятию решений в отношении ключевых аспектов деятельности.⁴⁴ Поэтому надзорным органам следует сохранять бдительность и сосредотачиваться на функциях, выполняемых механизмами DeFi, и базовой деловой цели, а не на их наименовании или маркетинговом позиционировании. Если механизм DeFi фактически предоставляет коммерческие услуги, аналогичные услугам финансовых учреждений или ПУБА, контролирующие лица могут осуществлять операционное управление и получать экономическую выгоду от его деятельности. В таких случаях механизм должен подпадать под нормативно-правовую и надзорную систему юрисдикции.
41. Надзорным органам следует уделять особое внимание следующим сценариям, при которых контроль может сохраняться в механизмах DeFi, заявляющих о децентрализации:
 - i. *Передача управления от юридического лица DAO*: если проект передает управление от компании или фонда к децентрализованной автономной организации (DAO), такая передача может быть номинальной, а не фактической. Органам следует искать индикаторы сохраняющегося контроля, включая сохранение учредителями токенов управления или специальных прав голоса, внесение ими большинства предло-

⁴⁴ <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3208~051a880042.en.pdf>; [2024-2nd-global-cryptoasset-regulatory-landscape-study.pdf](#); [Ecosystem Map | DeFi Navigator](#)

жений по управлению, сохранение фактического операционного контроля над DAO либо получение большей части комиссионных потоков и прибыли.

- ii. *Распределение токенов управления:* концентрация токенов управления в небольшом числе кошельков (например, в протоколе, где менее 1% кошельков обладают контролирующим большинством голосов) может указывать на контроль над механизмом DeFi. Надзорным органам следует тщательно оценивать практические привилегии и влияние, связанные с токенами управления, включая вес голоса, право вносить предложения, право вето и полномочия по обновлению, чтобы определить, приводит ли концентрация токенов к существенному фактическому контролю за принятием решений. Лица также могут осуществлять контроль или оказывать достаточное влияние на механизм DeFi, владея токенами управления в нескольких внешне несвязанных кошельках. Поэтому при оценке структур управления надзорным органам следует учитывать возможную кластеризацию кошельков и модели поведения, способные указывать на консолидированный контроль.
- iii. *Делегирование права голоса и модели голосования:* держатели небольшого объема токенов управления или неактивные держатели могут делегировать право голоса другим участникам, тем самым усиливая влияние иных держателей токенов на механизм. Хотя делегирование часто представляется как способ расширения участия и повышения эффективности управления, оно также может существенно концентрировать фактический контроль, усиливать влияние крупных держателей токенов и скрывать степень консолидированного влияния. Делегирование права голоса может быть сложным и непрозрачным, поэтому органам следует тщательно оценивать конкретные обстоятельства, чтобы установить, создает ли оно фактический контроль.

Вставка 7. Пример контроля в механизмах DeFi

Ooki DAO — Соединенные Штаты⁴⁵

Комиссия по торговле товарными фьючерсами США (CFTC) предъявила обвинения децентрализованной автономной организации Ooki (DAO) в административном постановлении в отношении предшественника Ooki DAO — компании bZeroX LLC.

1. *Использование структуры DAO для уклонения от надзора:* bZeroX LLC передала контроль над программным обеспечением DAO. Учредители прямо рекламировали этот шаг сообществу bZeroX как способ избежать соблюдения Закона о товарных биржах и возможных правоприменительных мер, однако фактически контроль сохранился у нескольких лиц.
2. *Влияние учредителей посредством токенов управления:* формально права голоса и административные ключи были распределены между держателями определенного токена управления. В число таких держателей входили учредители, которые могли вносить предложения и голосовать за изменения протокола, а также влиять на ключевые финансовые операции. В Ooki DAO отсутствовало официальное централизованное руководство, однако фактически учредители продолжали осуществлять контроль посредством токенов управления.

В июне 2023 года федеральный судья вынес решение в пользу CFTC и признал Ooki DAO «лицом» в соответствии с Законом о товарных биржах, при этом держатели токенов фактически осуществляли коллективные управленческие полномочия, хотя деятельностью не руководила центральная исполнительная группа. Суд обязал Ooki DAO уплатить гражданско-правовой денежный штраф в размере свыше 643 000 долларов США. Однако решение было вынесено заочно, поскольку Ooki DAO не явилась в суд, и поэтому имеет ограниченное прецедентное значение в законодательстве США.

5.5. По-настоящему децентрализованные механизмы DeFi

42. Хотя некоторые механизмы DeFi имеют централизованные элементы, другие могут быть в высокой степени децентрализованными, и ни одно лицо не осуществляет контроль и не оказывает достаточного влияния на их деятельность. Такие механизмы DeFi не подпадают под действие Стандартов ФАТФ. До признания механизма по-настоящему децентрализованным надзорным органам следует оценить структуру контроля с применением ряда критериев⁴⁶. Органы не должны полагаться исключительно на информацию, предоставленную самим механизмом DeFi, или на маркетинговые термины, описывающие степень его децентрализации; им следует проводить независимый анализ для понимания различных видов структур контроля, которые могут существовать в механизме (например, операционного контроля и контроля в сфере управления).
43. Регуляторные и надзорные органы не смогут снижать риски, создаваемые по-настоящему децентрализованными механизмами DeFi, путем прямого возложения требований ПОД/ФТ. Вместо этого им следует рассмотреть более широкие риск-ориентированные и комплексные меры по снижению рисков, включая выпуск для регулируемых организаций руководящих указаний о рисках взаимодействия с такими механизмами и разъяснение

⁴⁵ <https://www.taxnotes.com/research/federal/court-documents/court-opinions-and-orders/court-orders-shutdown-blockchain-based-software-operator/7jhws>

⁴⁶ См. факторы, изложенные в разделе 5.3 настоящего отчета.

того, допустимо ли такое взаимодействие и при каких условиях (например, при применении усиленных мер ПОД/ФТ). К регулируемым организациям, взаимодействующим с экосистемой DeFi, могут относиться:

- i. *эмитенты стейблкоинов*, сохраняющие возможность замораживать и сжигать стейблкоины, используемые в по-настоящему децентрализованных протоколах DeFi;
 - ii. *ПУВА, предоставляющие точки ввода и вывода*⁴⁷ в экосистему DeFi, которые обязаны соблюдать требования ЗСК и НПК, а также направлять сообщения о подозрительных операциях (СПО);
 - iii. *платформы пользовательских интерфейсов*⁴⁸, используемые для доступа к базовому механизму DeFi, которые могут иметь установленных контролирующих лиц и обязательства в сфере ПОД/ФТ;
 - iv. *финансовые учреждения*, взаимодействующие с механизмом DeFi.
44. Одновременно регуляторным и надзорным органам рекомендуется активно взаимодействовать с частным сектором для рассмотрения инновационных решений ПОД/ФТ, которые также могут применяться к по-настоящему децентрализованным механизмам DeFi, включая использование криптографических технологий и технологий цифровой идентификации, а также блокчейн-аналитики.

5.6. Требования лицензирования и/или регистрации централизованных механизмов DeFi

Централизованные механизмы DeFi

45. Для соблюдения Р.15 юрисдикциям следует устанавливать требования лицензирования или регистрации централизованных механизмов DeFi.⁴⁹
- i. Как минимум механизмы DeFi, контролируемые юридическими лицами, должны подлежать лицензированию или регистрации в юрисдикции (юрисдикциях), где они созданы.
 - ii. Если контролирующим лицом или лицом, оказывающим достаточное влияние на механизм DeFi, является физическое лицо, оно должно подлежать лицензированию или регистрации в юрисдикции по месту ведения деятельности или проживания.

⁴⁷ Точки ввода и вывода — это услуги, обеспечивающие перемещение средств между традиционной финансовой системой и экосистемой виртуальных активов. Точка ввода позволяет пользователям конвертировать фиатные деньги (например, евро или доллары США) в виртуальные активы либо один виртуальный актив в другой и служит точкой входа в среду виртуальных активов. Точка вывода, напротив, позволяет пользователям конвертировать виртуальные активы обратно в фиатные деньги, обеспечивая выход из экосистемы виртуальных активов и возможность погашать виртуальные активы в фиатные деньги, пригодные для использования в реальной экономике. <https://www.coinbase.com/en-fr/learn/crypto-basics/what-are-fiat-on-ramps-and-off-ramps>

⁴⁸ Органы вправе по своему усмотрению определять порядок регулирования поставщиков пользовательских интерфейсов — как компонента механизма DeFi либо как самостоятельной функции.

⁴⁹ Пункт 3 Пояснительной записки к Рекомендации 15: [FATF Recommendations 2012.pdf.coredownload.inline.pdf](#)

- iii. Юрисдикции также могут требовать лицензирования или регистрации лиц, контролирующих механизмы DeFi, которые предоставляют, содействуют предоставлению или продвигают продукты и услуги клиентам в пределах данной юрисдикции.⁵⁰

Централизованные механизмы DeFi, контролирующие лица которых не могут быть легко установлены

46. Хотя надзорные органы могут определить наличие у механизма DeFi контролирующих лиц, например посредством анализа прав голоса, связанных с токенами управления, поведения соответствующих кошельков и других факторов, установление личности таких лиц может оставаться сложным из-за псевдонимного характера блокчейн-экосистемы. Для решения этих проблем надзорным органам следует максимально тесно сотрудничать с другими организациями, которые могут располагать дополнительной информацией о личности и функциях контролирующих лиц, включая:
 - i. соответствующие национальные органы, включая ПФР и правоохранительные органы;
 - ii. зарубежных партнеров с использованием установленных механизмов международного сотрудничества;⁵¹
 - iii. частный сектор, включая компании блокчейн-аналитики, которые могут собрать дополнительные идентифицирующие сведения с применением технологических инструментов.
47. По возможности надзорным органам следует взаимодействовать с механизмами DeFi и запрашивать информацию о лицах, осуществляющих контроль, особенно если их невозможно легко установить, несмотря на распространяющиеся на них обязательства по лицензированию или регистрации в соответствии с P.15.
48. Надзорным органам следует применять риск-ориентированный подход к установлению контролирующих лиц и расставлять приоритеты с учетом существенности механизма DeFi и создаваемых им рисков в данной юрисдикции. Надзорным органам следует использовать все разумные способы⁵² установления лиц, осуществляющих контроль. Если после принятия таких мер установить контролирующих лиц по-прежнему невозможно, могут применяться меры по снижению рисков, аналогичные рекомендуемым для по-настоящему децентрализованных механизмов DeFi.
49. Надзорным органам следует на постоянной основе принимать меры по установлению контролирующих лиц и эффективной реализации регуляторных мер в отношении централизованных механизмов DeFi в соответствии со Стандартами ФАТФ, особенно если такие механизмы создают повышенные риски. К примерам таких мер относятся, помимо прочего:
 - i. **постоянное проведение блокчейн-аналитики**, включая отслеживание транзакций, кластеризацию кошельков и сетевой анализ, для выявления связей между адресами и потенциальными контролирующими лицами;

⁵⁰ В марте 2026 года ФАТФ проанализировала риски и регуляторные проблемы, связанные с офшорными ПУВА (включая соответствующие механизмы DeFi): <https://www.fatf-gafi.org/en/publications/Virtualassets/Understanding-Mitigating-Risks-Offshore-VASPs.html>

⁵¹ См. информацию, приведенную в разделе 6.1 настоящего отчета.

⁵² В зависимости от риска и контекста юрисдикции «разумные способы» могут включать действия, изложенные в пункте 47, а также сотрудничество с организациями, указанными в пункте 44.

- ii. **мониторинг точек управленческого и операционного контроля**, таких как голосование, внесение предложений, подписанты мультиподписных кошельков, управление казначейскими кошельками и использование ключей обновления или административных ключей;
- iii. использование **регулируемых организаций** в качестве информационных шлюзов, в том числе посредством требования к ПУВА и финансовым учреждениям собирать, анализировать и сообщать сведения о взаимодействии с механизмами DeFi;
- iv. использование **инструментов надзора и финансовой разведки**, включая СПО, надзорную отчетность и данные точек ввода/вывода фиатных денег, для содействия установлению лиц;
- v. поддержание **систем постоянного мониторинга**, обеспечивающих непрерывность мер по установлению лиц и их адаптацию по мере появления новой информации, инструментов или рисков;
- vi. **документирование и периодическую переоценку принятых мер**, включая ведение учета предпринятых следственных действий, их результатов и обновленных с течением времени оценок рисков.

Вставка 8. Установление требований лицензирования и регистрации в отношении механизмов DeFi

1. Юрисдикциям следует обеспечивать, чтобы процедуры пересмотра регуляторного периметра позволяли выявлять механизмы DeFi, действующие на их территории, при необходимости с применением тех же методов и тактики, которые используются для выявления ПУВА-нерезидентов («офшорных» ПУВА).⁵³ К ним могут относиться: веб-скрейпинг и сведения из открытых источников для выявления рекламы, рекламных сообщений или иных предложений услуг; сведения от населения, обязанных организаций (например, ПУВА) и отраслевых кругов; информация ПФР или иные сведения от подотчетных организаций, такие как СПО или следственные ориентировки; правоохранные или разведывательные отчеты, включая информацию, полученную в рамках международного сотрудничества (например, сведения от зарубежных партнеров).
2. После выявления механизма DeFi надзорным органам следует проводить комплексную «оценку контроля», чтобы определить, действительно ли механизм является децентрализованным. Такая оценка может основываться на индикаторах, приведенных в разделе 5.3 настоящего отчета, а также на дополнительных критериях, установленных надзорным органом.
3. Если установлено, что механизм является централизованным и имеет лиц, осуществляющих контроль или оказывающих достаточное влияние на его деятельность, надзорным органам следует выделить надлежащие ресурсы для всестороннего анализа структуры контроля механизма.
 - a. Если контролирующее лицо (лица) установлено, механизм DeFi следует включить в надзорный периметр в качестве ПУВА или финансового учреждения в зависимости от осуществляемой деятельности и нормативно-правовой базы юрисдикции.

⁵³ Раздел 3.1 отчета об офшорных ПУВА: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf>

- б. Если после использования всех разумных способов контролирующее лицо (лица) не установлено, надзорные органы могут рассмотреть альтернативные меры по снижению рисков, аналогичные применяемым к по-настоящему децентрализованным механизмам DeFi. Надзорным органам следует на постоянной основе принимать меры по установлению контролирующих лиц и эффективной реализации регуляторных мер в отношении таких механизмов DeFi в соответствии со Стандартами ФАТФ, особенно если эти механизмы создают повышенные риски.
- 4. Если механизмы являются по-настоящему децентрализованными, они не подпадают под действие Стандартов ФАТФ; вместе с тем юрисдикциям все равно следует применять риск-ориентированный подход и рассматривать альтернативные меры, которые могут быть приняты для снижения рисков противоправного финансирования, создаваемых такими механизмами.

5.7. Надзорная практика

- 50. При формировании подхода к уникальным особенностям экосистемы DeFi и снижению связанных с ней рисков противоправного финансирования юрисдикциям следует учитывать приведенную ниже надзорную практику. Странам следует избегать формального подхода по принципу проставления отметок, поскольку механизмы DeFi часто имеют крайне разнообразные и специфические особенности. Надзорные меры должны быть соразмерными, риск-ориентированными и адаптированными к конкретным рискам и контекстуальным факторам каждого механизма DeFi. Кроме того, крайне важно, чтобы надзорные органы выпускали четкие руководящие указания по действующим требованиям (в том числе о необходимости лицензирования или регистрации механизмов DeFi при наличии контролирующих лиц), чтобы обязанные организации полностью понимали ожидания юрисдикции.
- 51. *Установление четких стандартов аудита смарт-контрактов:* юрисдикции могут рассмотреть возможность установления строгих и прозрачных стандартов аудита смарт-контрактов, чтобы обеспечить всесторонность, независимость проверки механизмов DeFi и ее соответствие признанным лучшим практикам в области безопасности. Юрисдикции также могут рассмотреть возможность сделать аудит обязательным для отдельных категорий механизмов DeFi, особенно тех, которые обрабатывают значительные средства пользователей, используют сложные межсетевые мосты или зависят от высокорисковых архитектурных компонентов (например, мультиподписных административных ключей и прокси-шаблонов).
- 52. *Требование или как минимум поощрение встроенных мер ПОД/ФТ на уровне протокола и/или интерфейса:* юрисдикции могут рассмотреть возможность требовать или как минимум поощрять встраивание механизмами DeFi мер ПОД/ФТ непосредственно в уровень интерфейса смарт-контрактов либо во внешнюю оболочку. К таким мерам могут относиться, например, автоматизированные механизмы замораживания адресов, связанных с лицами, в отношении которых действуют санкции; ончейн-логика оценки риска; меры контроля, задерживающие или блокирующие высокорисковые транзакции до завершения проверки; либо требования о проверяемых учетных данных (например, подтверждении прохождения процедуры ЗСК) до выполнения отдельных высокорисковых функций. Такие встроенные меры контроля могут способствовать снижению рисков противоправного финансирования без несоразмерного ограничения отличительных и инновационных особенностей экосистемы DeFi.

Вставка 9. Рабочая группа Франции по сертификации смарт-контрактов

В январе 2024 года Управление пруденциального надзора и урегулирования (ACPR) и Управление по финансовым рынкам (AMF) совместно создали рабочую группу в рамках Финтех-форума ACPR-AMF для изучения вопросов сертификации смарт-контрактов в более широком контексте возможного будущего регулирования DeFi. Группа сосредоточилась на определении возможных стандартов сертификации и методик аудита. [Ее выводы были опубликованы в феврале 2025 года в отчете, размещенном на веб-сайтах ACPR и AMF.](#)

В отчете рассматривается, каким образом сертификация может снизить риски для пользователей, укрепить доверие и, возможно, способствовать формированию будущей нормативно-правовой базы. В нем изложены общие принципы и позиции членов рабочей группы, а также рассмотрены варианты регулирования сертификации смарт-контрактов. Подчеркивается, что доверие к экосистемам DeFi и их устойчивость требуют сертификации на основе ясных, измеримых стандартов, включая стандарты соблюдения требований.

В отчете отмечается, что меры по противодействию ОД/ФТ/ФРОМУ могут быть технически встроены непосредственно в отдельные смарт-контракты, что облегчает их использование организациями, на которые распространяются требования ПОД/ФТ, включая поставщиков услуг в сфере криптоактивов и другие финансовые учреждения. Например, смарт-контракты могут включать регулярно обновляемые перечни адресов, взаимодействие с которыми запрещено. Кроме того, могут быть интегрированы элементы проверки клиентов на основе доказательств с нулевым разглашением (ZKP), чтобы доступ к определенным функциям смарт-контрактов предоставлялся только пользователям, прошедшим усиленную проверку личности или надлежащую проверку. В исследовании подчеркивается, что при сертификации смарт-контрактов могут оцениваться такие области, как безопасность и качество кода, управление и возможность обновления, среда исполнения, прозрачность и контроль доступа, управление жизненным циклом и защита пользователей.

Источник: Франция

53. *Выпуск лучших практик по прозрачным и ответственным аварийным мерам контроля:* юрисдикции могут рассмотреть возможность выпуска набора лучших практик проектирования и использования аварийных мер контроля (например, функций приостановки и механизмов аварийного отключения) в механизмах DeFi. В этих руководящих принципах следует разъяснить порядок прозрачной реализации мер контроля при наличии надлежащих гарантий управления и подотчетности для снижения серьезных рисков, включая кибератаки, эксплуатацию уязвимостей протокола или крупномасштабное отмывание, с максимально возможным сохранением децентрализованных характеристик механизма.
54. *Усиление надзора за поставщиками пользовательских интерфейсов и операторами оракулов:* юрисдикции могут рассмотреть возможность усиления надзора за ключевыми поставщиками офчейн-инфраструктуры, особенно пользовательскими интерфейсами и операторами оракулов, поскольку эти компоненты оказывают существенное влияние на взаимодействие пользователей и поведение протокола. Надзорные органы могут рекомендовать или требовать от таких поставщиков применять меры по сокращению противоправной деятельности, включая автоматизированный скрининг, оценку риска, геоблокировку с учетом санкций или повышение прозрачности источников данных оракулов и их устойчивости к манипулированию.
55. *Проведение блокчейн-мониторинга высокорисковых механизмов DeFi:* юрисдикции могут рассмотреть возможность внедрения инструментов блокчейн-аналитики для мониторинга

га механизмов DeFi, действующих на их территории. Это может включать отслеживание подозрительных потоков, выявление моделей, соответствующих противоправному финансированию, и постоянную оценку рисков на основе данных транзакций. Юрисдикции также могут рассмотреть возможность передачи соответствующих результатов регулируемым финансовым учреждениям и ПУВА, взаимодействующим с такими механизмами, чтобы повысить эффективность выявления незаконных средств.

56. *Повышение прозрачности структур управления DeFi*: юрисдикции могут рассмотреть возможность введения мер, обеспечивающих наличие у механизмов DeFi прозрачных и легко устанавливаемых структур управления. Это поможет снизить риск сокрытия управления, концентрации контроля или скрытого влияния противоправных субъектов. Меры могут включать поощрение публичного раскрытия процессов управления, обеспечение ясности в отношении прав голоса и делегирования, а также повышение прозрачности сведений о лицах, влияющих на обновления, изменения параметров или работу протокола.
57. *Регуляторные «песочницы»*: регуляторные «песочницы» — это механизмы, создаваемые компетентными органами и позволяющие регулируемым и нерегулируемым организациям испытывать инновационные продукты или услуги в установленных пределах. Юрисдикции могут рассмотреть возможность создания регуляторных «песочниц» для механизмов DeFi с целью апробации надзорных подходов в контролируемой среде с управлением рисками. Регуляторные «песочницы» могут требовать значительных ресурсов как государственного, так и частного сектора и не во всех случаях являются наиболее подходящим инструментом.⁵⁴

Вставка 10. Регуляторные «песочницы» для механизмов DeFi

Бермудские Острова

DerivaDex Bermuda 1, лицензия класса Т («песочница»): деятельность в ограниченном масштабе при постоянном пруденциальном надзоре, надзоре за киберрисками и в сфере ПОД в отношении рисков, управления и развития компании. Объем деятельности ограничен: поскольку компания недавно начала работу, лицензия предусматривает не более 1 000 активных пользователей. Компания не хранит средства клиентов. Единственный механизм DeFi, действующий в настоящее время из данной юрисдикции, обратился за лицензией, а структура его управления известна надзорному органу.

Единственный действующий механизм DeFi внедрил на основании договора аутсорсинга услуги проверки в рамках принципа «Знай своего клиента»/надлежащей проверки клиента (KYC/CDD), проверки в сфере ПОД, подтверждение адреса, проверки криптоактивов в сфере ПОД, аутентификацию документов, удостоверяющих личность, проверку соответствия изображению лица и постоянный мониторинг в сфере ПОД.

Источник: Бермудские Острова

5.8. Взаимодействие механизмов DeFi с регулируемыми финансовыми учреждениями и ПУВА

58. Юрисдикциям следует обеспечивать, чтобы обязанные организации, включая финансовые учреждения и ПУВА, в достаточной мере понимали риски финансовых преступлений, связанные с экосистемой DeFi. Финансовый сектор проявляет все больший интерес к взаимодействию с механизмами DeFi как в средах с разрешительным доступом, так и в

⁵⁴ [Building A Regulatory Sandbox](#) | [Digital Finance Inclusion: Regulatory sandbox toolkit](#) | [OECD: How Regulatory Sandboxes Foster Innovation and Compliance in Crypto](#).

средах без разрешительного доступа, чтобы воспользоваться операционными преимуществами, включая автоматизированные расчеты, трансграничный охват, круглосуточную доступность (24/7) и, как правило, более высокую доходность. По мере усиления взаимосвязей между регулируемыми финансовыми учреждениями, ПУВА и механизмами DeFi изменения в экосистеме DeFi могут иметь более широкие последствия для соблюдения требований ПОД/ФТ и потенциально повышать уязвимости ОД/ФТ/ФРОМУ в более широкой системе виртуальных активов и финансовой системе.

59. Финансовые учреждения и ПУВА, взаимодействующие с механизмами DeFi, должны проводить оценку рисков продуктов и принимать надлежащие меры по управлению рисками, создаваемыми такими механизмами, и их снижению в соответствии с пунктом 1 Р.15. Если финансовые учреждения и ПУВА предоставляют услуги механизмам DeFi, они также должны соблюдать Рекомендацию 10 (НПК, если механизм DeFi намерен стать или уже является клиентом) и Рекомендацию 13 (если механизм DeFi намерен установить корреспондентские банковские отношения) и воздерживаться от взаимодействия с механизмами DeFi, если эти конкретные обязательства по Стандартам ФАТФ невозможно выполнить. Они также несут общее обязательство сохранять целостность собственных систем ПОД/ФТ и обеспечивать эффективное применение превентивных мер в своих экосистемах. Финансовым учреждениям и ПУВА следует оценивать механизмы DeFi на риск-ориентированной и соразмерной основе и применять надлежащие меры по снижению рисков в различных сценариях:
 - i. Централизованные механизмы DeFi: финансовым учреждениям и ПУВА следует проводить НПК в отношении механизма DeFi в соответствии со Стандартами ФАТФ по корреспондентским банковским отношениям, в том числе устанавливать, лицензирован или зарегистрирован ли механизм и подлежит ли он надлежащему надзору. Финансовые учреждения и ПУВА должны проводить надлежащую проверку либо обеспечивать, чтобы механизм реализовал меры ПОД/ФТ в соответствии с Рекомендациями 10 и 13.⁵⁵
 - ii. Централизованные механизмы DeFi, контролируемые лица которых не могут быть легко установлены, и по-настоящему децентрализованные механизмы DeFi: финансовым учреждениям и ПУВА следует применять надлежащие меры ПОД/ФТ к базовым клиентам механизма DeFi, включая проверку личности, и, при необходимости, осуществлять постоянный мониторинг целостности и безопасности протокола. Финансовые учреждения и ПУВА сохраняют ответственность за обеспечение соответствия своего взаимодействия с такими механизмами требованиям ПОД/ФТ. Надзорным органам следует предоставлять обязанным организациям дополнительные руководящие указания с учетом рисков юрисдикции, а также особенностей сектора и конкретной организации.
60. Взаимодействие финансовых учреждений и ПУВА с механизмами DeFi должно сопровождаться надежными мерами по снижению рисков. Механизмы DeFi, допускающие неограниченный доступ пользователей без каких-либо мер ПОД/ФТ, могут считаться более высокорисковыми, поскольку способны обеспечивать прямое взаимодействие с потенциальными противоправными субъектами. Финансовым учреждениям и ПУВА следует тщательно оценивать, могут ли они в рамках собственной системы комплаенса применять надлежащие меры по снижению рисков ПОД/ФТ для взаимодействия с такими механизмами без нарушения своих обязательств по соблюдению требований.

⁵⁵ Некоторые механизмы DeFi создали среды с разрешительным доступом для взаимодействия с регулируемыми финансовыми учреждениями при соблюдении регуляторных ожиданий. Финансовым учреждениям следует оценивать уровень развития мер ПОД/ФТ, реализованных такими механизмами DeFi, и обеспечивать их совместимость с собственными программами ПОД/ФТ.

61. Хотя понимание структуры управления механизмом DeFi, результатов аудита и мер кибербезопасности соответствует лучшим практикам, обязанным организациям следует в первую очередь оценивать надлежащий характер и эффективность мер ПОД/ФТ, реализованных механизмом, и создавать надежные системы эффективного установления и проверки личности его базовых пользователей. При необходимости им также следует применять дополнительные меры по снижению рисков (например, мониторинг в режиме реального времени с использованием инструментов блокчейн-аналитики).
62. Регуляторные и надзорные органы могут рассмотреть возможность применения адаптированного и более гибкого подхода, если по-настоящему децентрализованные механизмы DeFi включают эффективные меры снижения рисков ПОД/ФТ на уровне протокола. Такие меры могут включать использование сторонних поставщиков услуг ЗСК/НПК, встроенных решений ЗСК/НПК и белых или черных списков на уровне смарт-контракта либо пользовательского интерфейса. В таких случаях остаточный риск, связанный с механизмом DeFi, может быть ниже, а меры ПОД/ФТ, применяемые финансовыми учреждениями и ПУВА к базовым клиентам механизма DeFi, могут корректироваться при условии эффективного и постоянного снижения рисков.

Вставка 11. Тематические исследования: взаимодействие финансовых учреждений и ПУВА с механизмами DeFi

Внутреннее сотрудничество финансового регулятора и правоохранительных органов для обеспечения надежного надзора

В Соединенном Королевстве применяется межведомственный подход к внутреннему сотрудничеству для реагирования на возникающие риски, связанные с DeFi, особенно когда такая деятельность пересекается с традиционными финансовыми услугами и более широкой экосистемой виртуальных активов. Управление по финансовому регулированию и надзору (FCA), являющееся регулятором ПУВА, тесно взаимодействует с правоохранительными органами, такими как Национальный центр по борьбе с экономической преступностью, посредством регулярных встреч и площадок обмена информацией о рисках ОД/ФТ/ФРОМУ.

Эти механизмы позволяют правоохранительным органам информировать FCA о новых бизнес-моделях с участием регулируемых финансовых учреждений, ПУВА и DeFi. В ответ FCA проводит целевые надзорные мероприятия для оценки применения и эффективности мер контроля финансовых преступлений в отношении новых продуктов, не охваченных на этапе авторизации.

Такая надзорная работа включает анализ механизмов ввода и вывода, оценку рисков продуктов (в том числе связей между фиатными деньгами и виртуальными активами), практики управления кошельками, процессов приема клиентов на обслуживание, мер НПК/усиленных мер НПК и соблюдения требований Маршрутного правила и санкций. Эта работа позволила FCA выявлять пробелы и при необходимости требовать улучшений.

В целом данный пример показывает, как эффективное межведомственное сотрудничество может способствовать раннему вмешательству вне обычного надзорного цикла и формированию у компетентных органов общего понимания рисков ОД/ФТ, связанных с новыми продуктами DeFi.

Источник: Соединенное Королевство

Надзорная практика Денежно-кредитного управления Сингапура (MAS)

В рамках надзора и лицензирования MAS взаимодействует с поставщиками услуг цифровых платежных токенов (DPTSP) на двусторонней основе для оценки их подверженности DeFi. Как минимум:

1. если DPTSP предоставляет услуги клиентам, участвующим в деятельности, связанной с DeFi, источник благосостояния клиента и любая иная существенная связь с такой деятельностью должны учитываться в оценке риска клиента, проводимой DPTSP. При необходимости ПУВА должен применять усиленные меры НПК, включая усиленный постоянный мониторинг. DPTSP следует в полной мере учитывать характер и профиль риска деятельности клиента, связанной с DeFi, и обеспечивать всесторонность и соразмерность оценки риска;
2. если DPTSP сотрудничает с платформой DeFi для предоставления услуг клиентам, он должен оценить риски ОД/ФТ, связанные с предоставлением услуг через платформу DeFi, а также провести надлежащую проверку платформы DeFi для оценки: i) надежности ее системы контроля рисков ПОД/ФТ/ФРОМУ; и ii) соответствия платформы DeFi собственной системе ПОД/ФТ/ФРОМУ DPTSP и регуляторным требованиям.

Источник: Сингапур

6. Правоприменительные и иные меры по снижению рисков, связанных с механизмами DeFi

63. ФАТФ опубликовала руководящие материалы о порядке расследования и конфискации виртуальных активов, включая стейблкоины, которые также имеют значение для механизмов DeFi.⁵⁶ В случае DeFi органы могут сталкиваться с дополнительными проблемами, обусловленными их уникальными характеристиками.⁵⁷ Расследования, связанные с DeFi, часто осложняются сложными методами сокрытия, включая перемещение между блокчейнами, межсетевые свопы и микроструктурирование. Юрисдикциям следует создавать надежные межведомственные механизмы, обеспечивающие совместный оперативный анализ и быстрое реагирование, а также использовать государственно-частные партнерства (ГЧП) для интеграции блокчейн-аналитики в режиме реального времени и современных инструментов отслеживания в деятельность правоохранительных органов.

6.1. Использование инструментов блокчейн-аналитики в расследованиях, связанных с DeFi

64. Правоохранительным органам следует использовать инструменты блокчейн-аналитики для содействия расследованиям, связанным с протоколами DeFi. Эти инструменты позволяют отслеживать движение средств через многочисленные блокчейны и активы, в том числе через миксеры, мосты и сложные взаимодействия со смарт-контрактами, что дает следователям возможность восстанавливать потоки транзакций. Они также предоставляют средства визуализации для картирования связей между кошельками, организациями и протоколами наряду с подробным анализом смарт-контрактов, необходимым для понимания движения средств в среде DeFi. Кроме того, автоматизированное выявление подозрительных моделей, таких как расслоение или последовательное дробление средств, в сочетании с современными методами атрибуции может содействовать установлению организаций, контролирующих кошельки, и их возможных связей с противоправной деятельностью.
65. Хотя инструменты блокчейн-аналитики могут содействовать расследованиям в отношении механизмов DeFi, юрисдикциям следует учитывать, что по мере технического усложнения платформ DeFi их эффективность может снижаться. Например, переход деятельности DeFi с публичных блокчейнов в специализированные сети уровня 1 (Layer 1), многие из которых еще не поддерживаются распространенными аналитическими инструментами, а также объединение депозитов нескольких пользователей в одном смарт-контракте могут снижать прозрачность и затруднять отнесение транзакций к конкретным пользователям.

⁵⁶ [Asset-Recovery-Guidance-Best-Practices.pdf.coredownload.pdf](https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html); <https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-stablecoins-unhosted-wallets.html>; <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>

⁵⁷ См. информацию, приведенную в разделе 2.1 настоящего отчета.

Вставка 12. Гонконг, Китай: расследования в отношении механизмов DeFi

В Полиции Гонконга (НКРФ) специализированная группа по расследованию преступлений с использованием криптовалют проводит расследования и регулярно анализирует использование протоколов DeFi в преступной деятельности. В ходе таких расследований органы выявляют типологии с использованием децентрализованных бирж, межсетевых свопов, пулов ликвидности и других механизмов DeFi, которые могут применяться для содействия мошенничеству, взломам или отмыванию преступных доходов. НКРФ также применяет механизм координации приостановления операций с криптовалютами для содействия быстрому блокированию преступных виртуальных активов. Когда преступные доходы прослеживаются до деятельности, связанной с DeFi, НКРФ может взаимодействовать с соответствующими платформами для получения информации о цифровом следе и, когда это возможно, содействовать предотвращению вывода активов, связанных с преступной деятельностью.

Кроме того, НКРФ расследовала несколько инцидентов, связанных с атаками на платформы DeFi и инфраструктуру Web3. В рамках этих расследований устанавливаются причины уязвимостей безопасности, пострадавшим организациям предоставляются рекомендации по безопасности и координируются меры быстрого реагирования для сокращения потерь. В ряде случаев такие меры позволили заблокировать похищенные виртуальные активы вскоре после происшествия.

Источник: Гонконг, Китай

6.2. Координация с другими компетентными органами

66. Правоохранительным органам следует тесно взаимодействовать с надзорными органами, ПФР и другими соответствующими компетентными органами. Вместо того чтобы полагаться исключительно на традиционные меморандумы о взаимопонимании, внутреннее сотрудничество следует реализовывать через практические механизмы. Это включает:

- i. *Создание совместных стандартных операционных процедур (СОП) для экстренного замораживания активов, предоставление межведомственного доступа к проприетарным платформам блокчейн-аналитики и содействие временному прикомандированию сотрудников между надзорными и правоохранительными органами для формирования устойчивого институционального потенциала и операционной синергии в режиме реального времени;*
- ii. *Специализированные междисциплинарные совместные оперативные группы, способные содействовать расследованиям с учетом высокотехнологичного и трансграничного характера механизмов DeFi. Такие группы должны объединять специализированные знания ПФР, подразделений правоохранительных органов по борьбе с киберпреступностью и финансовых надзорных органов. Объединение ресурсов, включая современные инструменты блокчейн-аналитики, возможности киберкриминалистики и традиционную финансовую разведку, позволяет органам проводить параллельные расследования и предотвращать утрату цифровых доказательств.*

6.3. Замораживание и возврат незаконных средств

67. Замораживание и возврат средств, связанных с противоправной деятельностью в DeFi, создают как операционные, так и регуляторные трудности. Преступники часто используют компонуемость и псевдонимность DeFi для расслоения транзакций или направления их через миксеры, межсетевые мосты и DEX до вмешательства органов. Такая динамика

затрудняет применение традиционных подходов к аресту активов, особенно при отсутствии централизованных посредников.

68. Эффективный подход к снижению этих рисков в рамках действующей нормативно-правовой базы заключается в сосредоточении усилий на смежных компонентах более широкой экосистемы виртуальных активов, которые способны применять механизмы замораживания или отклонения, а также на уникальных посредниках экосистемы DeFi, включая:
- i. *эмитентов стейблкоинов*, обеспеченных фиатными деньгами, способных замораживать, блокировать, сжигать или повторно выпускать токены, связанные с преступной деятельностью. Они играют особенно важную роль, поскольку стейблкоины составляют 90% ВА в экосистеме DeFi.⁵⁸ Для содействия координации компетентным органам следует активно использовать созданные глобальные сети, например защищенный канал связи INTERPOL I-24/7, который позволяет правоохранительным органам быстро координировать действия с юрисдикцией учреждения эмитента стейблкоина и исполнять экстренные запросы о замораживании активов до рассеивания незаконных средств или их вывода из экосистемы. Юрисдикциям также следует рассмотреть возможность включения специализированных уведомлений INTERPOL в процессы трансграничных расследований;
 - ii. *ПУВА, выступающие кастодияльными конечными точками*, могут незамедлительно замораживать преступные активы, отмытые через механизмы DeFi, после получения законного распоряжения, например судебной повестки, ордера на арест или указания о замораживании. ПУВА могут быть критически важными узкими местами для возврата активов, поскольку противоправные субъекты, злоупотребляющие механизмами DeFi, часто используют точки вывода в фиатные деньги;
 - iii. *пользовательские интерфейсы DeFi*, в которые интегрированы отдельные инструменты соблюдения требований, могут автоматически отклонять активы, связанные с противоправными субъектами, с использованием блокчейн-аналитики, рейтингов риска и других риск-индикаторов («красных флагов»). Такое отклонение может не позволить противоправным субъектам, использующим пользовательский интерфейс, получить доступ к DEX, мосту или иному механизму DeFi. После этого оператор пользовательского интерфейса может связаться с соответствующими государственными органами и передать информацию об отклоненных транзакциях.
69. Преступные субъекты все чаще совершают сложные взломы механизмов DeFi. В ответ многие протоколы полагаются на лиц, владеющих административными ключами или участвующих в мультиподписных структурах контроля и способных принимать экстренные меры, например отключать пользовательские интерфейсы, приостанавливать функциональность контрактов, замораживать отдельные хранилища, пулы или модули и корректировать параметры системы, чтобы не позволить злоумышленнику завершить эксплуатацию уязвимости. Правоохранительным органам следует заблаговременно выявлять таких ключевых лиц, действующих в их юрисдикции, и взаимодействовать с ними, чтобы быстро координировать эффективные меры по сохранению средств до их вывода из протокола.

⁵⁸ Дополнительную информацию о возможности эмитентов стейблкоинов замораживать и сжигать стейблкоины см. в документе: [targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf](#)

7. Международное сотрудничество

7.1. Трансграничный обмен информацией

70. Трансграничный обмен информацией имеет основополагающее значение для выявления централизованных механизмов DeFi, которые могут действовать без надлежащей регистрации или лицензии. Эффективное трансграничное сотрудничество также способствует более глубокому пониманию рисков, создаваемых по-настоящему децентрализованными механизмами DeFi, которыми могут злоупотреблять противоправные субъекты, включая возможные каскадные последствия для регулируемых организаций. Органам следует в максимально возможной степени использовать действующие механизмы международного сотрудничества, например Многосторонний меморандум о взаимопонимании (ММоУ) IOSCO, для обмена данными о возникающих рисках, результатах расследований и правоприменительных мерах.⁵⁹
71. Эффективный **обмен информацией между ПФР** также играет ключевую роль в выявлении трансграничных рисков, связанных с DeFi. Опыт Глобальной сети ФАТФ показывает, что обмен оперативным и стратегическим анализом может содействовать выявлению новых способов злоупотребления механизмами DeFi и отслеживанию средств. Юрисдикции сообщили об использовании следующих каналов обмена информацией:
- i. Защищенная сеть Группы «Эгмонт»⁶⁰
 - ii. FIU.net «нового поколения»⁶¹
72. Надзорным органам следует в максимально возможной степени сотрудничать и обмениваться информацией о лицах, осуществляющих контроль или оказывающих достаточное влияние на механизмы DeFi, поскольку такие лица могут находиться в любой части мира, а сведения об их личности могут отсутствовать в юрисдикции, где они осуществляют деятельность. Надзорным органам также следует по возможности обмениваться информацией о механизмах DeFi, включая их технические, операционные структуры и структуры управления, чтобы содействовать единообразному анализу трансграничных механизмов DeFi. Надзорным органам рекомендуется публиковать анализ механизмов DeFi и более широкой экосистемы DeFi в соответствии с применимыми требованиями обмена информацией и защиты конфиденциальности.
73. Наконец, организациям частного сектора следует обмениваться информацией между собой через границы в соответствии с применимыми механизмами обмена информацией для более эффективного выявления и пресечения незаконных потоков в экосистеме DeFi. Отдельные финансовые учреждения или ПУВА могут располагать уникальными и ценными данными как о новых моделях злоупотребления механизмами DeFi, так и о лицах, осуществляющих контроль или оказывающих достаточное влияние на такие механизмы, которые могут быть недоступны регулируемым организациям в других юрисдикциях. Своевременный трансграничный обмен такой неконфиденциальной информацией может повысить способность глобальных подразделений комплаенса выявлять риски и укрепить меры по снижению рисков ОД/ФТ.

⁵⁹ [FR14/23 Итоговый отчет с рекомендациями по вопросам политики в области децентрализованных финансов \(DeFi\).](#)

⁶⁰ [Организация и структура — Группа «Эгмонт».](#)

⁶¹ [FIU.net «нового поколения» — Европейская комиссия.](#)

7.2. Трансграничные расследования

74. **Трансграничное сотрудничество правоохранительных органов:** с учетом трансграничного характера DeFi и отсутствия географических ограничений трансграничное сотрудничество между правоохранительными органами имеет решающее значение. Использование традиционных механизмов, таких как взаимная правовая помощь (ВПП), необходимо для сбора доказательств, однако обычные сроки их реализации иногда не соответствуют мгновенному характеру децентрализованных переводов стоимости. Для дополнения этих официальных каналов и обеспечения критически необходимой срочности активных расследований юрисдикциям рекомендуется создавать ускоренные защищенные механизмы незамедлительного обмена передовыми аналитическими данными блокчейн-разведки между ПФР и подразделениями по борьбе с киберпреступностью. Такой быстрый обмен имеет решающее значение для успешного отслеживания многоэтапных транзакций до утраты следа; традиционные механизмы при этом могут дополнять расследование дополнительными доказательствами.

Вставка 13. Соединенные Штаты: дело Samourai

В ноябре 2025 года Министерство юстиции США вынесло приговор Кеонне Родригесу и Уильяму Лонергану Хиллу, соучредителям Samourai Wallet — миксера DeFi, через который было проведено незаконных транзакций на сумму свыше 237 млн долларов США. Преступные доходы, отмытые через Samourai, были получены, в частности, от наркоторговли, деятельности даркнет-маркетплейсов, кибервторжений, мошенничества, операций с юрисдикциями, находящимися под санкциями, заказных убийств и веб-сайта с материалами сексуального насилия над детьми. Родригес и Хилл активно рекламировали Samourai преступникам, в том числе утверждали на даркнет-форуме, что Samourai делает виртуальные активы «неотслеживаемыми и чистыми». Родригес и Хилл были приговорены соответственно к пяти и четырем годам лишения свободы и уплатили более 6 млн долларов США в виде конфискованных комиссий.

В ходе расследования содействие по этому делу оказывали, в частности, Европол, Судебная полиция Португалии и Полиция Исландии. На основании запроса США о ВПП исландские органы получили сведения с сервера, который Samourai использовал для своей деятельности и который находился в Исландии. Предоставленные правоохранительным органам США данные о транзакциях имели критическое значение для продвижения расследования. Кроме того, в июле 2024 года Хилл был экстрадирован из Португалии, а португальские органы сыграли важную роль в получении дополнительных полезных доказательств по месту его проживания в Португалии. Французские органы также оказали ценное содействие по каналам ВПП. Данный пример продемонстрировал необходимость начинать сотрудничество с иностранными партнерами на раннем этапе сложных дел для выявления значимых цифровых данных и подозреваемых, которые часто могут действовать в нескольких юрисдикциях.

Источник: Соединенные Штаты

7.3. Государственно-частное сотрудничество

75. Государственно-частные партнерства (ГЧП) играют ключевую роль в реагировании на риски ОД/ФТ/ФРОМУ, возникающие в связи с DeFi, поскольку обеспечивают структурированный обмен информацией, совместный оперативный анализ и формирование общего понимания возникающих рисков и регуляторных требований у государственных органов и участников частного сектора. С учетом риска и контекста юрисдикциям следует создавать надлежащие каналы связи для взаимодействия, по возможности, с механизмами DeFi, а также с ПУВА, компаниями блокчейн-аналитики и финансовыми учреждениями для укрепления сотрудничества в экосистеме.
76. ГЧП особенно полезны для содействия органам в реагировании на регуляторные, надзорные и правоприменительные трудности. Они могут помогать органам устанавливать характеристики, особенности управления и структуры контроля механизмов DeFi, а также глубже понимать порядок программирования и развертывания протоколов и смарт-контрактов. ГЧП также играют ключевую роль в содействии разработке и внедрению мер ПОД/ФТ и решений децентрализованной идентификации для усиления идентификации пользователей и снижения рисков, связанных с анонимностью. Кроме того, они облегчают обмен тактической информацией, позволяют разрабатывать типологии противоправной деятельности и возникающих тенденций, укрепляют сбор разведывательной информации и повышают эффективность реагирования на взломы и эксплуатацию уязвимостей. Наконец, ГЧП могут поддерживать инициативы по отраслевой стандартизации, в том числе реализуемые международными организациями (например, IEEE и ISO) и отраслевыми консорциумами, способствуя повышению безопасности, совместимости и уровня соблюдения требований в экосистеме DeFi.

Вставка 14. Соединенное Королевство: тематические регуляторные семинары с частным сектором для углубления понимания рисков и соблюдения требований в DeFi

В рамках режима регулирования ВА Управление по финансовому регулированию и надзору Соединенного Королевства (FCA) расширило взаимодействие с заинтересованными сторонами частного сектора для обсуждения рисков, создаваемых DeFi, и потенциальных инструментов соблюдения требований для снижения рисков посредством серии тематических семинаров с участием финансовых учреждений, ПУВА, механизмов DeFi, а также специалистов по соблюдению требований в сфере ОД/ФТ/ФРОМУ и технологическим вопросам.

Семинары были посвящены не только текущим и возникающим рискам ОД/ФТ/ФРОМУ и соответствующей практике снижения рисков, применяемой отраслью, но и технологическим рискам DeFi, включая уязвимости протоколов с открытым исходным кодом и смарт-контрактов, которыми могут воспользоваться хакеры. В ходе обсуждений участники отрасли поделились опытом, касающимся ограничений блокчейн-аналитики и возможностей таких технических решений, как встроенная функция замораживания на уровне протокола и проверки в рамках принципа «Знай своего клиента» на основе доказательств с нулевым разглашением. Семинары позволили FCA актуализировать оценку рисков противоправного финансирования и мер их снижения, а также учесть предложения отрасли в регуляторных разъяснениях.

Источник: Соединенное Королевство

Вставка 15. Сингапур: Global Layer One (GL1)

Global Layer One (GL1) — государственно-частная инициатива при поддержке Денежно-кредитного управления Сингапура (MAS), объединяющая глобальные финансовые учреждения, ПУВА, организации, участвующие в экосистеме DeFi, и разработчиков политики для продвижения токенизации активов посредством открытых и совместимых сетевых стандартов. GL1 разрабатывает эталонные архитектуры для непосредственного включения механизмов контроля за соблюдением нормативных требований в логику ончейн-транзакций. Эти решения призваны содействовать соблюдению соответствующих регуляторных обязанностей, включая требования ПОД/ФТ/ФРОМУ, посредством модульных компонентов комплаенса, позволяющих различным субъектам выполнять отдельные роли на разных этапах цепочки обеспечения соблюдения требований. В рамках системы рассматривается использование проверяемых удостоверений и подтверждений, связанных с личностью, которые могут позволить встроить проверки ПОД/ФТ/ФРОМУ в программируемые условия транзакций. Такой подход призван позволить регулируемым участникам подтверждать соблюдение применимых регуляторных требований при сохранении совместимости между юрисдикциями и сетями токенизированных активов.

Хотя MAS участвует в GL1, само по себе участие в этой системе или ее использование не означает одобрения со стороны надзорного органа. Регулируемые финансовые учреждения по-прежнему подлежат надзору MAS, а соблюдение обязанностей в сфере ПОД/ФТ/ФРОМУ оценивается комплексно с учетом различных механизмов управления, операционного контроля и управления рисками, помимо ончейн-механизмов соблюдения требований.

Источник: Сингапур

Заключение

77. В последние несколько лет DeFi продолжал быстро расти и способен сыграть важную роль в глобальной финансовой системе будущего. Такие технологические особенности, как автоматизация, компонуемость, круглосуточная доступность (24/7) и трансграничный охват, создают как возможности для финансовых инноваций, так и значительные риски ОД/ФТ/ФРОМУ. Эти риски усиливаются широко распространенными заблуждениями о «децентрализации», сохраняющимися пробелами в регулировании и все более активным использованием механизмов DeFi киберпреступниками, мошенниками, профессиональными отмывателями и сетями финансирования распространения оружия массового уничтожения, в том числе посредством злоупотребления передовыми инструментами искусственного интеллекта.
78. Стандарты ФАТФ уже обеспечивают основу для реагирования на эти риски, однако их имплементация остается крайне недостаточной. Большинство юрисдикций еще не выявили действующие на их территории механизмы DeFi, не оценили их риски и не применили R.15 к механизмам, соответствующим определению ПУВА. Основная проблема заключается в определении лиц, осуществляющих контроль или оказывающих достаточное влияние на механизмы DeFi. В отчете приведены примеры критериев, которые юрисдикции могут использовать для комплексной оценки, а также примеры и тематические исследования контроля и «достаточного влияния» на практике.
79. Юрисдикциям следует применять функциональный риск-ориентированный подход к установлению контролируемых лиц, применению требований лицензирования/регистрации

и осуществлению надзора за механизмами DeFi. Органам следует укреплять возможности расследования и правоприменения, включая блокчейн-аналитику, оперативное сотрудничество и государственно-частные партнерства, чтобы эффективно реагировать на все более сложное противоправное финансирование с использованием DeFi. В отношении по-настоящему децентрализованных механизмов, не подпадающих под действие Стандартов, юрисдикциям следует использовать альтернативные меры по снижению рисков, направленные на смежные точки регуляторного доступа, такие как эмитенты стейблкоинов, ПУВА и интерфейсы прикладного уровня. Такие альтернативные меры могут корректироваться, если по-настоящему децентрализованные механизмы применяют надлежащие меры по снижению рисков.

80. Юрисдикциям Глобальной сети ФАТФ следует заблаговременно отслеживать потенциальный рост по-настоящему децентрализованных механизмов DeFi. Одновременно им следует предусматривать надлежащие меры по снижению рисков для регулируемых организаций, взаимодействующим с такими механизмами, как указано в разделе 5.5 настоящего отчета.
81. ФАТФ следует продолжать мониторинг развития рынка и рисков, связанных с экосистемой DeFi, особенно по-настоящему децентрализованных механизмов DeFi, чтобы Стандарты ФАТФ сохраняли актуальность.
82. В конечном счете для эффективного снижения рисков, связанных с DeFi, потребуются скоординированные глобальные действия, прозрачная практика управления, инновационные решения в сфере комплаенса и устойчивое взаимодействие регуляторов, правоохранительных органов и частного сектора. Без таких мер быстрое развитие DeFi, потенциально способствующее модернизации платежей, может создавать растущую регуляторную асимметрию, обеспечивать юрисдикционный арбитраж и содействовать широкомасштабному противоправному финансированию.

Рекомендации по снижению рисков, связанных с механизмами DeFi

1.1. Для юрисдикций

- 1) Соразмерно риску и контексту проводить оценку рисков, связанных с экосистемой DeFi, которая может включаться в национальные, секторальные или отраслевые оценки рисков либо в оценку рисков ВА и ПУВА юрисдикции. В рамках такой оценки следует определять существенность и характер рисков ОД/ФТ/ФРОМУ, связанных с DeFi, включая степень внутренней подверженности, трансграничные аспекты и потенциальные уязвимости, возникающие вследствие функционирования, управления и использования механизмов DeFi.
- 2) На основе оценки рисков применять соразмерные меры по их снижению. Они могут включать требование к централизованным механизмам DeFi и поощрение децентрализованных механизмов DeFi встраивать меры ПОД/ФТ на уровне смарт-контрактов и/или пользовательского интерфейса; требование к другим организациям, взаимодействующим с экосистемой DeFi, таким как финансовые учреждения и ПУВА, применять дополнительные меры ПОД/ФТ для снижения рисков, связанных с базовыми пользователями механизма DeFi; а в сценариях повышенного риска, если механизмы DeFi отказываются сотрудничать с государственными органами, — в качестве крайней меры запрещать их деятельность на территории юрисдикции (включение в черный список).
- 3) Взаимодействовать с участниками отрасли, включая механизмы DeFi, ПУВА, компании блокчейн-аналитики и других поставщиков услуг, взаимодействующих с механизмами DeFi, для выявления инновационных решений и инструментов, повышающих эффективность имплементации мер ПОД/ФТ в экосистеме DeFi без несоразмерного ограничения инноваций (например, цифровая идентификация и встроенные программы ЗСК/НПК).

- 4) Установить надлежащие критерии определения контроля или достаточного влияния в контексте DeFi и, при выявлении такого контроля, применять к соответствующим механизмам меры ПОД/ФТ. Проводить целевую информационно-разъяснительную работу с отраслью (включая участие в соответствующих отраслевых мероприятиях), чтобы централизованные механизмы DeFi были осведомлены о применимых требованиях.
 - о Если контролирующие лица существуют, но не могут быть установлены, а механизм DeFi не способен обеспечить соответствие своей деятельности требованиям ПОД/ФТ, надзорным органам следует считать его нерегулируемым и применять те же меры по снижению рисков, что и к по-настоящему децентрализованным механизмам, продолжая при этом направлять запросы и, когда это уместно и возможно, применять соразмерные санкции.
- 5) Создать четкие регуляторные пути, позволяющие регулируемым учреждениям взаимодействовать с механизмами DeFi при сохранении целостности их систем соблюдения требований ПОД/ФТ и более широкой финансовой системы. Регулируемым учреждениям следует применять надлежащие меры ПОД/ФТ для снижения рисков, создаваемых механизмами DeFi, и эффективно осуществлять меры контроля в отношении базовых клиентов таких механизмов в соответствии с Рекомендацией 10. Эти меры должны быть соразмерны выявленным рискам и учитывать любые меры снижения рисков, реализованные механизмом DeFi, например встроенные меры ПОД/ФТ на уровне смарт-контрактов или использование сторонних поставщиков услуг ПОД/ФТ.
- 6) Когда это уместно с учетом риска и контекста, создавать структурированные и доступные механизмы регуляторного взаимодействия, такие как предварительные встречи перед подачей заявления, инновационные центры, регуляторные «песочницы» и технические семинары, чтобы до выхода механизмов DeFi на рынок разъяснять им ожидания в сфере соблюдения требований.
- 7) Создать механизмы выявления высокорисковых механизмов DeFi или механизмов DeFi, не соблюдающих требования. Они могут включать публичные реестры, надзорные уведомления или раскрытие рейтингов риска, способные направлять участников рынка, стимулировать ответственное поведение и повышать общую целостность рынка.
- 8) Усилить надзор за ключевыми поставщиками офчейн-инфраструктуры, выступающими точками регуляторного доступа в экосистеме DeFi, например операторами пользовательских интерфейсов, и поощрять их к применению адаптированных мер, препятствующих противоправной деятельности.
- 9) Рассмотреть возможность требовать или поощрять все виды механизмов DeFi, действующих в юрисдикции, назначать ответственное лицо для своевременного взаимодействия с компетентными органами, особенно в рамках правоохранных расследований, чтобы устранить существующий недостаток эффективных механизмов сотрудничества.
- 10) Укрепить межведомственную координацию и операционный потенциал расследований, связанных с DeFi, посредством создания надежных механизмов совместного анализа и быстрого реагирования, а также использования государственно-частных партнерств для интеграции блокчейн-аналитики в режиме реального времени и современных инструментов отслеживания.

1.2. Для частного сектора

Для механизмов DeFi

- 11) Централизованные механизмы DeFi и механизмы, которые на практике являются централизованными, но их контролирующие лица не могут быть легко установлены, должны в полном объеме соблюдать требования Рекомендации 15.
- 12) Централизованным механизмам DeFi следует уделять приоритетное внимание инвестициям в разработку инновационных инструментов, обеспечивающих эффективную имплементацию мер ПОД/ФТ, и укреплять технологические возможности для оперативного выявления, ареста и замораживания преступных активов.
- 13) По-настоящему децентрализованным механизмам DeFi, не подпадающим под действие Стандартов ФАТФ, рекомендуется понимать свои риски ОД/ФТ и при необходимости включать соразмерные меры ПОД/ФТ в операционные механизмы для поддержания общей целостности финансовой системы.
- 14) Всем механизмам DeFi следует:
 - i. в максимально возможной степени сотрудничать с компетентными органами в рамках расследований ПОД/ФТ и назначить специальное контактное лицо (Рос) для поддержания официальных каналов связи с правоохранительными органами и ПФР. В централизованных механизмах DeFi контактным лицом может быть контролирующее лицо механизма, а в по-настоящему децентрализованных механизмах DeFi — лица, ответственные за его создание (например, разработчики);
 - ii. подготовить и сделать доступной для компетентных органов документацию, в которой четко изложены структуры контроля и принятия решений в механизме DeFi. Такая документация должна устанавливать лиц, осуществляющих операционное влияние, полномочия в сфере управления или контроль на уровне протокола. В ней также следует указать контактные данные для компетентных органов;
 - o в отношении по-настоящему децентрализованных механизмов DeFi лица, ответственные за их создание, также должны разъяснять модель управления и операционную модель, включая характеристики, подтверждающие заявления о децентрализации;
 - iii. регулярно проводить аудит кибербезопасности протокола и обеспечивать постоянный мониторинг подозрительных тенденций и потенциальных способов эксплуатации уязвимостей для более эффективного предотвращения хищений и злоупотреблений со стороны противоправных субъектов.

Для финансовых учреждений и ПУВА

- 15) Применять Рекомендацию 13 при установлении деловых отношений с централизованными механизмами DeFi и механизмами, которые на практике являются централизованными, но их контролирующие лица не могут быть легко установлены. Если после использования всех разумных способов контролирующие лица в конечном итоге не могут быть установлены, применять те же меры по снижению рисков, что и к по-настоящему децентрализованным механизмам DeFi.
- 16) Взаимодействовать с механизмами DeFi, не подлежащими регулированию, при применении надлежащих мер ПОД/ФТ для снижения рисков, связанных с их клиентами, включая надлежащую проверку клиента (например, проверку личности базовых клиентов) и постоянный мониторинг целостности и безопасности протокола.

- 17) Обмениваться информацией с другими организациями частного сектора, в том числе между юрисдикциями, для более эффективного выявления и пресечения незаконных потоков в экосистеме DeFi с соблюдением применимых правовых и нормативных требований.

Приложение А. Обзор работы ФАТФ по ВА и ПУВА

2018	В Рекомендацию 15 внесены изменения, включая добавление новых определений «виртуальный актив» и «провайдер услуг виртуальных активов».
2019	- Принята Пояснительная записка к R.15 - Создана Контактная группа ФАТФ по виртуальным активам (КГВА) - Первоначальное руководство для регуляторов: риск-ориентированный подход к ВА и ПУВА (обновлено в 2021 году)
2020	12-месячный обзор новых Стандартов ФАТФ: первый 12-месячный обзор - Отчет для «Группы двадцати»: Отчет ФАТФ для «Группы двадцати» о так называемых стейблкоинах - Риск-индикаторы: перечень «красных флагов» ОД/ФТ при использовании ВА
2021	- Обновленное руководство⁶²: Обновленное руководство по применению риск-ориентированного подхода к ВА и ПУВА 24-месячный обзор Стандартов ФАТФ: второй 12-месячный обзор
2022	Отчет о соблюдении R.15 с особым акцентом на Маршрутном правиле и возникающих рисках ВА: Целевое обновление информации об имплементации Стандартов ФАТФ по ВА и ПУВА
2023	- Отчет о программах-вымогателях с акцентом на рисках и тенденциях в сфере ВА: Противодействие финансированию программ-вымогателей - Отчет о соблюдении R.15 с особым акцентом на Маршрутном правиле и возникающих рисках ВА: Целевое обновление информации об имплементации Стандартов ФАТФ по ВА и ПУВА
2024	Статус имплементации Рекомендации 15 членами ФАТФ и юрисдикциями с существенно значимой деятельностью ПУВА
2025	Статус имплементации Рекомендации 15 членами ФАТФ и юрисдикциями с существенно значимой деятельностью ПУВА Лучшие практики надзора за соблюдением Маршрутного правила Краткое руководство по оценке рисков отмывания денег, связанных с виртуальными активами (ВА) и провайдерами услуг виртуальных активов (ПУВА)
2026	Целевой отчет по стейблкоинам и некастодиальным кошелькам — пиринговые транзакции Понимание и снижение рисков офшорных провайдеров услуг виртуальных активов 7-е Целевое обновление информации об имплементации Стандартов ФАТФ по виртуальным активам и провайдерам услуг виртуальных активов

⁶² Обновленное Руководство 2021 года содержало изменения по следующим шести ключевым направлениям: разъяснение определений ВА и ПУВА; указания о применении Стандартов ФАТФ к стейблкоинам; дополнительные указания о рисках и инструментах, доступных юрисдикциям для реагирования на риски ОД/ФТ, связанные с пиринговыми транзакциями; обновленные указания по лицензированию и регистрации ПУВА; дополнительные указания для государственного и частного секторов по имплементации Маршрутного правила; а также принципы обмена информацией и сотрудничества между надзорными органами ПУВА.



Июль, 2026

www.fatf-gafi.org