ОТЧЕТ О ТИПОЛОГИЯХ 2025

Инновации в противодействии финансовым преступлениям в эпоху стремительных изменений

Elliptic

Неофициальный перевод на русский язык. Терминология приведена в соответствие с подходами ФАТФ и ЕАГ в сфере ПОД/ФТ, виртуальных активов и поставщиков услуг виртуальных активов (ПУВА). Термин «cryptoasset» в настоящем переводе передается как «криптоактив», а термин VASP - как «поставщик услуг виртуальных активов (ПУВА)».

Содержание

Резюме для руководства

С момента публикации первого Отчета Elliptic о типологиях в ноябре 2018 года финансовые преступления в сфере криптоактивов существенно эволюционировали. Более подготовленные преступники и иные субъекты угрозы используют все более сложные методы легализации (отмывания) преступных доходов (ОД) для осуществления противоправной деятельности с использованием криптоактивов.

Последнее издание Отчета Elliptic о типологиях представляет углубленный анализ пяти областей риска финансовых преступлений, наиболее наглядно отражающих изменение характера противоправной деятельности с криптоактивами и содержащих выводы, применимые к более широким усилиям по пресечению преступлений, связанных с криптоактивами. К таким областям относятся:

1. использование искусственного интеллекта (ИИ) в мошенничестве и иных противоправных схемах с криптоактивами;
2. промышленная профессионализация экосистемы мошенничества типа «pig butchering» - длительных инвестиционных схем, при которых преступники постепенно завоевывают доверие жертвы и побуждают ее переводить все более крупные суммы;
3. распространение использования стейблкоинов лицами и организациями, находящимися под санкциями;
4. все более широкая интеграция криптоактивов в схемы отмывания денег, используемые наркокартелями;
5. рост сложности межсетевого (cross-chain) отмывания денег.

В отчете описываются методы, применяемые противоправными субъектами при совершении указанных преступлений, а также приводятся подробные примеры практических мер, которые специалисты по соблюдению требований (комплаенс), сотрудники правоохранительных органов и регулирующих органов могут применять для их выявления и пресечения.

Кроме того, в отчете показано, каким образом Elliptic развивает свою платформу данных и аналитической информации, чтобы предоставлять подразделениям комплаенс, следователям и регулирующим органам практически применимую информацию о соответствующих рисках и угрозах. В частности:

- инструменты и аналитика на основе ИИ позволяют повысить эффективность рабочих процессов аналитиков и следователей, отвечающих за выявление рисков и отслеживание движения денежных средств в режиме реального времени;
- возможности поведенческого выявления позволяют автоматически обнаруживать противоправную деятельность в блокчейне, формируя предупреждения об индикаторах («красных флагах») отмывания денег и мошенничества;
- данные о кошельках и транзакциях более чем в 50 блокчейнах позволяют аналитикам и следователям получать информацию о рисках в режиме реального времени по мере перемещения преступниками средств между различными блокчейнами;
- автоматизированное отслеживание средств через межсетевые мосты с использованием событий передачи виртуальной стоимости (Virtual Value Transfer Events, VVTE) дает возможность выявлять и визуализировать сложные схемы отмывания денег;
- возможности мониторинга экосистемы (Ecosystem Monitoring) обеспечивают эмитентов стейблкоинов, их партнеров и регулирующие органы данными как на уровне отдельных транзакций, так и по экосистеме токена в целом, что позволяет заблаговременно снижать риски и замораживать преступные доходы;
- подразделения комплаенс крупных организаций и государственные органы могут дополнять имеющиеся офчейн-источники информацией и аналитическими данными о криптокошельках, субъектах и поведении в блокчейне. Это обеспечивает гибкий и масштабируемый анализ быстро

меняющегося сектора криптоактивов, который все теснее интегрируется с традиционным финансовым сектором.

Введение

Как использовать настоящий отчет

Как и предыдущие отчеты Elliptic о типологиях, настоящее издание представляет собой практическое руководство для специалистов по противодействию финансовым преступлениям, работающих в подразделениях комплаенс регулируемых организаций и в государственных органах. По тексту приводятся ссылки на другие материалы Elliptic - публикации в блоге и исследовательские отчеты, содержащие дополнительную информацию по отдельным темам. В конце документа также приведен сводный перечень материалов для дальнейшего изучения.

Помимо описания того, как типологии финансовых преступлений реализуются на практике, в отчете используются следующие обозначения:

- **Индикаторы («красные флаги»)** - ключевые модели поведения и признаки, которые могут помочь в выявлении конкретных типологий и рисков.
- **Ключевые меры контроля и рекомендации по расследованию** - превентивные меры, инструменты комплаенс, методы расследования и возможности блокчейн-аналитики, способствующие выявлению и снижению конкретных рисков.
- **Практические примеры (case studies)** - реальные случаи, иллюстрирующие типологии финансовых преступлений и методы, использованные для их выявления и пресечения.

Инновации для пресечения финансовых преступлений в эпоху стремительных изменений

С 2018 года ежегодный Отчет Elliptic о типологиях помогает подразделениям комплаенс поставщиков услуг виртуальных активов (ПУВА) и финансовых учреждений, правоохранительным и регулирующим органам понимать механизмы преступного поведения в сфере криптоактивов. Когда был опубликован первый отчет, его целью было помочь специалистам государственного и частного секторов получить комплексное представление о противоправной деятельности с криптоактивами, которая в тот момент для большинства оставалась сравнительно новым явлением.

За последующие годы характер противоправной деятельности в сфере криптоактивов и масштабы мер по противодействию ей существенно изменились.

В 2018 году преступники, действовавшие в сфере криптоактивов, в основном использовали относительно простые и несложные методы отмывания преступных средств. ОД с использованием криптоактивов преимущественно было связано с киберпреступниками, операторами и пользователями рынков даркнета, а также мошенниками, деятельность которых осуществлялась в сравнительно небольших масштабах. Для сокрытия движения средств обычно применялись достаточно прямолинейные способы, в том числе сервисы смешивания криптоактивов (миксеры) и ПУВА, не соблюдающие установленные требования.

Профессиональные организации и сети по отмыванию денег (PMLO), государства и лица, находящиеся под санкциями, а также другие субъекты, способные перемещать значительные объемы средств, в тот период лишь начинали использовать криптоактивы. Технологические решения, которые впоследствии существенно изменили блокчейн-экосистему, включая децентрализованные финансы (DeFi), находились на ранней стадии развития.

К 2025 году ситуация кардинально изменилась. По мере того как торговля криптоактивами все быстрее становится частью массовой финансовой практики, более широкий круг преступных субъектов начал использовать криптоактивы как доступный инструмент противоправной финансовой деятельности. Мошенничество с криптоактивами приобрело промышленный масштаб, поскольку все больше розничных пользователей становятся объектами эксплуатации и обмана.

PMLO все активнее используют криптоактивы в сложных схемах ОД, связанных с различными видами преступной деятельности, включая незаконный оборот наркотиков и торговлю людьми. Государства и лица, находящиеся под санкциями, в том числе КНДР, Россия, Иран и Венесуэла, регулярно используют криптоактивы для получения доходов и обхода международных финансовых ограничений.

Развитие DeFi и иных инноваций, прежде всего стейблкоинов, также радикально изменило способы отмывания средств в экосистеме криптоактивов. Средства быстро перемещаются между активами и блокчейнами по все более сложным маршрутам. Одновременно развитие ИИ предоставляет преступникам дополнительные инструменты для масштабирования противоправной деятельности.

Эволюция противоправной деятельности с криптоактивами

С учетом этих быстрых изменений в настоящем году Elliptic применяет новый подход к ежегодному Отчету о типологиях. Многие типологии из предыдущих отчетов по-прежнему актуальны для следователей по финансовым преступлениям и специалистов комплаенс и остаются доступными на сайте Elliptic.

В настоящем отчете основное внимание уделяется ключевым тенденциям и формирующимся рискам финансовых преступлений с криптоактивами, которые, по оценке Elliptic, являются наиболее значимыми и актуальными в преддверии 2026 года и лучше всего отражают меняющийся характер противоправной деятельности:

- **Использование ИИ в мошенничестве с криптоактивами.** Преступники регулярно применяют дипфейки и другие технологии на основе ИИ для совершения все более сложных мошеннических действий. Дальнейшее развитие ИИ будет усиливать связанные с этим вызовы. Одновременно ИИ может использоваться и для пресечения преступной деятельности - за счет более глубокого понимания преступного поведения и повышения эффективности работы аналитиков и следователей в режиме реального времени.
- **Промышленная профессионализация экосистемы «pig butchering».** Так называемые схемы «pig butchering», то есть мошеннические инвестиционные схемы с использованием криптоактивов и длительным завоеванием доверия жертвы, в последние годы вызывают все большую обеспокоенность правоохранительных органов. Резонансные случаи 2025 года показывают, что глобальная экосистема таких схем действует в промышленном масштабе и отличается высоким уровнем организации. Для выявления и пресечения этих сетей критически важны блокчейн-аналитика и поведенческое выявление.
- **Рост использования стейблкоинов санкционными субъектами.** Стейблкоины стали одним из предпочтительных видов криптоактивов для государств, лиц и организаций, находящихся под санкциями и стремящихся обходить финансовые и экономические ограничения. Вместе с тем современные возможности блокчейн-аналитики позволяют заблаговременно выявлять риски обхода санкций.
- **Интеграция криптоактивов в схемы ОД наркокартелей.** Исторически криптоактивы в контексте наркотрафика чаще фигурировали в торговле через даркнет и реже - в операциях крупных международных наркокартелей, занимающихся распространением наркотиков вне сети. Сегодня картели все чаще используют услуги PMLO для отмывания средств через криптоактивы и применяют все более сложные схемы. Эта тенденция имеет значение и для других преступлений организованных преступных групп (ОПГ), включая торговлю людьми и незаконный ввоз мигрантов, где применяются схемы преобразования наличных денежных средств в криптоактивы.
- **Рост сложности межсетевого отмывания денег.** Противоправные субъекты перемещают более 21 млрд долларов США в криптоактивах с использованием межсетевых методов ОД, эксплуатируя инновационные механизмы, особенно в экосистеме DeFi, для быстрого перевода средств между активами и блокчейнами. Такие типологии усложняют расследования, однако блокчейн-аналитика позволяет раскрывать их в режиме реального времени даже при перемещении средств между различными цепочками и активами.

Каждой из этих пяти тенденций посвящена отдельная глава. В каждой главе приводятся конкретные типологии, используемые преступниками при совершении соответствующих преступлений и легализации их доходов.

Диаграмма: совокупный рост межсетевой преступной деятельности по месяцам. По данным Elliptic, за последние два года наблюдается устойчивый рост межсетевого ОД. В разрезе сервисов в диаграмме указаны DEX - около 12 млрд долларов США, межсетевые мосты - около 5,4 млрд долларов США, сервисы обмена криптоактивов (coin swap) - около 3,6 млрд долларов США.

Диаграмма: доля потерь от мошенничества, связанных с криптоактивами. Мошенничество с использованием криптоактивов составляет растущую и существенную долю совокупных потерь от мошенничества в ряде юрисдикций.

Реагирование на эволюцию финансовых преступлений: блокчейн-аналитика нового поколения

Несмотря на постоянное появление новых способов злоупотребления криптоактивами, за последние семь лет государственный и частный секторы добились существенного прогресса в противодействии таким преступлениям. Подразделения комплаенс ПУВА и финансовых учреждений значительно повысили способность выявлять и пресекать противоправную деятельность, используя блокчейн-аналитику корпоративного уровня для выявления и управления рисками.

Правоохранительные органы существенно расширили возможности отслеживания противоправных потоков криптоактивов и в рамках расследований ОД в блокчейне провели ряд крупнейших в истории финансовых изъятий. Возрастает число государственно-частных партнерств и инициатив, позволяющих участникам отрасли и государственным органам формировать более полную аналитическую картину и обмениваться полученными знаниями с целью повышения эффективности пресечения преступной деятельности в сфере криптоактивов.

Elliptic поддерживает эти усилия путем постоянного развития платформы данных и аналитической информации и создания нового поколения инструментов блокчейн-аналитики для государственного и частного секторов. По мере усложнения противоправной деятельности Elliptic стремится предоставлять пользователям сведения, необходимые для выявления и пресечения все более сложных типологий финансовых преступлений.

За последние два года платформа была дополнена следующими возможностями:

6. **Комплексный охват более 50 блокчейнов.** Преступники могут осуществлять противоправные операции с тысячами активов в десятках блокчейнов. Платформа Elliptic охватывает более 50 блокчейнов и формирует практически применимую информацию о преступном поведении даже при перемещении и отмывании средств между различными элементами криптоэкосистемы.
7. **Комплексный (holistic) скрининг.** В рамках ОД преступники регулярно применяют «chain-hopping» - перемещение между различными блокчейнами, в том числе через межсетевые мосты. Комплексный скрининг позволяет аналитикам оперативно оценить риск, связанный с такими моделями поведения.
8. **События передачи виртуальной стоимости (VVTE).** Для отслеживания особо сложных схем межсетевого ОД Elliptic использует VVTE, автоматизирующие движение средств более чем через 300 комбинаций межсетевых мостов и позволяющие одним действием визуализировать полный граф потоков средств в блокчейне.
9. **Поведенческое выявление.** Решения Elliptic по расследованиям и скринингу используют поведенческий анализ, предоставляя пользователям сведения почти по двум десяткам типологий преступного поведения, включая «цепочки дробления» (peel chain), автоматизированное наслоение (layering), первичное поступление средств из миксеров (mixer-first funding), мошенническое поведение и другие модели.
10. **Мониторинг экосистемы (Ecosystem Monitoring).** Эмитенты стейблкоинов могут получать проактивные предупреждения о противоправной деятельности, затрагивающей их токен, а также

агрегированную аналитику, помогающую им, их партнерам и регулирующим органам снижать возникающие риски.

11. **Повышение эффективности и точности с использованием ИИ.** Elliptic применяет ИИ и машинное обучение для получения новых сведений о моделях финансовых преступлений в блокчейне. Интеграция инструментов ИИ также позволяет снижать неэффективность рабочих процессов, способную препятствовать оперативным расследованиям.
12. **Обновление настраиваемого механизма оценки риска.** С 2013 года настраиваемые правила риска Elliptic лежат в основе продуктов для скрининга кошельков и транзакций и позволяют применять эффективный риск-ориентированный мониторинг с приоритизацией наиболее значимых рисков. Обновленный механизм обеспечивает более детальную оценку, включая прямую и косвенную подверженность риску.
13. **Data Fabric.** В июне 2025 года Elliptic объявила о запуске Data Fabric - сервиса, позволяющего подразделениям комплаенс и государственным органам напрямую подключаться к платформе данных и аналитики Elliptic и интегрировать блокчейн-данные в рабочие процессы наряду с другими, в том числе офчейн, источниками. По мере интеграции криптоактивов с традиционным финансовым сектором прямой доступ к аналитике на основе данных становится ключевым условием оперативного и гибкого реагирования на меняющиеся риски и угрозы.
14. **Комплексная проверка эмитента (Issuer Due Diligence).** В августе 2025 года Elliptic объявила о новом решении для банков и финансовых учреждений, позволяющем проводить анализ на уровне адресов и мониторить риск как внутри кластеров кошельков, так и за их пределами. Банки могут отслеживать изменение поведения кошельков и соответствующих рисков во времени, что важно для выполнения требований банковского комплаенс при установлении и поддержании отношений с эмитентами стейблкоинов.

В последующих разделах подробно рассматривается применение этих возможностей для пресечения конкретных типологий финансовых преступлений.

1. Использование искусственного интеллекта (ИИ) в мошенничестве с криптоактивами

Понимание риска

После выпуска ChatGPT компанией OpenAI в ноябре 2022 года резко возрос интерес к преобразующему потенциалу ИИ, одновременно стремительно увеличилось число решений на основе ИИ, влияющих практически на все сферы жизни. Возможности генеративного ИИ, в том числе большие языковые модели (LLM), стали доступны миллиардам людей; ежедневно ChatGPT используют более 120 млн пользователей. Компании в сфере технологий, финансов, медицины и других отраслях применяют ИИ для повышения эффективности, улучшения качества решений и клиентского опыта.

Как и в случае с другими технологическими инновациями, преступники оказались среди ранних пользователей ИИ. Подобно законным предпринимателям и разработчикам, они используют ИИ для увеличения прибыли и масштабирования своей деятельности.

В отчете Elliptic за июнь 2024 года о преступности с применением ИИ в экосистеме криптоактивов были определены пять основных способов воздействия таких преступлений на сектор:

15. **Использование генеративного ИИ для обмана в криптомошенничестве.** Мошенники создают дипфейки и иные материалы, сгенерированные ИИ, для продвижения и рекламы мошеннических схем, придавая им видимость легитимности. Например, применяются видеодипфейки, создающие впечатление, что знаменитость или политик поддерживает определенный криптотокен, либо дипфейки, имитирующие сотрудника компании в сфере криптоактивов, чтобы убедить людей инвестировать в мошенническую схему. Сгенерированные ИИ изображения также используются для создания убедительных маркетинговых материалов и веб-сайтов.
16. **Мошенничество с криптоактивами и манипулирование рынком под видом ИИ.** Мошенники используют ажиотаж вокруг ИИ и создают фиктивные инвестиционные схемы, заявляя о применении технологий ИИ. Например, создаются сайты, предлагающие инвесторам использовать якобы «торговых ботов на базе ИИ», которые фактически представляют собой схемы «rug pull», направленные на хищение средств инвесторов.
17. **Использование больших языковых моделей для содействия киберпреступности.** Киберпреступники применяют инструменты ИИ для выявления уязвимостей в программном коде, которые затем используются для взломов, атак с применением программ-вымогателей и иных противоправных целей. По имеющимся сообщениям, киберпреступники из КНДР и российские операторы программ-вымогателей используют ИИ для содействия разработке вредоносного программного обеспечения.
18. **Масштабирование криптомошенничества и дезинформации.** ИИ ускоряет создание поддельных маркетинговых материалов и распространение дезинформации. Например, социальные боты могут публиковать сгенерированные ИИ сообщения и быстро распространять сведения о мошеннической схеме среди ничего не подозревающих пользователей.
19. **Развитие противоправных рынков.** Продавцы на рынках даркнета предлагают инструменты и возможности, усиленные ИИ, которые помогают другим преступникам осуществлять противоправную деятельность.

В настоящем разделе рассматриваются три практические типологии мошенничества с криптоактивами, усиленного ИИ, с которыми могут столкнуться специалисты комплаенс и следователи. Также приведены индикаторы и меры, способствующие выявлению и предупреждению таких схем, а также описано использование ИИ самой Elliptic для повышения эффективности выявления и пресечения противоправной деятельности.

Офчейн- и ончейн-риски, связанные с ИИ

ПУВА, включая криптобиржи, могут подвергаться следующим видам риска:

- документы, удостоверяющие личность, созданные ИИ, используются для обхода процедур «Знай своего клиента» (KYC);
- дипфейки имитируют руководителей высокого уровня;
- враждебные государственные субъекты применяют кибератаки, усиленные ИИ;
- пользователи приобретают кредиты или доступ к противоправным сервисам на базе ИИ;
- жертвы переводят средства в мошеннические схемы, использующие ИИ;
- пользователи отмывают средства, полученные от противоправной деятельности, осуществленной с применением ИИ.

Пример типологии: противоправный субъект открывает счета у ПУВА с использованием изображений и коммуникаций, созданных ИИ

Мошенники, использующие криптоактивы, давно применяют поддельные удостоверения личности при открытии счетов на криптобиржах и у других ПУВА. В предыдущих отчетах Elliptic подробно описывалось, что поддельные документы широко продаются в даркнете и используются для обхода процедур KYC и мер ПОД/ФТ. Открытие счетов по поддельным документам также часто связано с сетями денежных мулов либо лицами, нанятыми преступными группами для ОД.

Все чаще противоправные субъекты получают доступ к документам и сопроводительным материалам, улучшенным с помощью генеративного ИИ. При отсутствии надлежащих механизмов выявления такие материалы могут успешно проходить проверки KYC. Генеративный ИИ также позволяет создавать поддельные селфи, видеозаписи и иные изображения, предоставляемые клиентами в ходе идентификации и верификации.

В настоящее время материалы, созданные ИИ, по-прежнему нередко содержат ошибки и несоответствия, позволяющие выявить мошенничество. Однако по мере совершенствования технологий они будут становиться все более убедительными, усложняя работу подразделений комплаенс.

Как работает схема

20. Клиент обращается к ПУВА для открытия счета и предоставляет скан паспорта, селфи или видеозапись.
21. Подразделение комплаенс ПУВА не знает, что изображения документов и видеозаписи были созданы с использованием генеративного ИИ. Клиент успешно проходит KYC, счет открывается.
22. Вскоре после открытия счета на него начинают поступать средства из внешних криптокошельков, связанных с мошенничеством, киберпреступностью или иной противоправной деятельностью.
23. Получив криптоактивы преступного происхождения, клиент быстро конвертирует их в фиатные валюты или иные криптоактивы либо переводит на внешние кошельки.
24. В некоторых случаях клиент неоднократно отправляет или получает средства по внутри-платформенным переводам от счетов других клиентов того же ПУВА.
25. После периода активных операций счет может стать неактивным. При обращении ПУВА клиент не отвечает либо предоставляет неполную или противоречивую информацию.
26. По результатам анализа операций и повторной проверки документов подразделение комплаенс устанавливает, что счет был открыт мошенническим путем. В иных случаях ПУВА получает сведения от правоохранительного органа или другого ПУВА, указывающие на противоправную деятельность клиента.

Индикаторы, связанные с документами и изображениями

- Документы клиента противоречат иной предоставленной им информации; например, место проживания не совпадает со сведениями в удостоверяющих документах.
- Несколько документов одного клиента содержат небольшие расхождения, например различающиеся адреса проживания.
- Изображения в документах содержат визуальные дефекты или несоответствия; например, возраст лица на фотографии явно не соответствует заявленной дате рождения.
- Видеозаписи, представленные для проверки личности, содержат аномалии, указывающие на дипфейк, например движения губ не синхронизированы с голосом.

Транзакционные индикаторы

- После открытия счета клиент сначала проводит небольшие тестовые операции, а затем резко наращивает частоту и суммы транзакций.
- По счету наблюдаются необъяснимо большие объемы или суммы операций, не соответствующие известной цели деловых отношений или профилю клиента.
- Имеется значительная либо необъяснимая прямая или косвенная связь с кошельками, которые по данным блокчейн-аналитики ассоциируются с мошенничеством, киберпреступностью или иной противоправной деятельностью.
- Совершаются внутри-платформенные переводы другим клиентам того же ПУВА со сходными моделями операций, что может указывать на использование счетов денежных мулов.
- Транзакции имеют признаки «chain-hopping»: средства проходят через многочисленные промежуточные кошельки до поступления на счет клиента.
- Криптоактивы приобретаются с использованием дебетовых или кредитных карт, впоследствии идентифицированных как похищенные.
- После периода интенсивной активности операции внезапно прекращаются.

Поведенческие и иные индикаторы

- Клиент входит в счет с IP-адреса, географическое местоположение которого не соответствует заявленному месту проживания.
- Клиент не отвечает на запросы ПУВА.
- Ответы клиента неясны, противоречат характеру его операций или не имеют разумного объяснения.
- В сообщениях клиента имеются признаки использования LLM, например несвязный текст или случайно оставленная фраза типа «как большая языковая модель, я не могу... ».
- Данные клиента и характер его операций совпадают с данными других клиентов того же ПУВА. Например, несколько клиентов используют одинаковый или сходный адрес проживания, одновременно участвуют в необъяснимой подозрительной активности и совершают сходные операции с одними и теми же некастодиальными кошельками. Это может указывать на сеть денежных мулов.

Пример типологии: клиент биржи или другого ПУВА становится жертвой мошенничества с использованием генеративного ИИ

Генеративный ИИ позволяет мошенникам усиливать схемы за счет все более реалистичных изображений и дипфейков. Пока некоторые такие схемы сравнительно легко выявлять по дефектам контента, постоянное повышение качества дипфейков и других материалов, созданных ИИ, будет усложнять их обнаружение.

Как работает схема

27. Лицо видит в социальной сети или другом интернет-ресурсе рекламу инвестиционного продукта, связанного с криптоактивами и обещающего высокую доходность. В публикации содержится видео с известной знаменитостью или политиком, якобы поддерживающим продукт.
28. Переход по рекламе ведет на убедительно оформленный сайт онлайн-платформы для торговли криптоактивами. На сайте размещены фотографии руководства, ссылки на службу поддержки и сведения о лицензировании, создающие впечатление регулируемой и законной деятельности.
29. При регистрации пользователя просят перевести криптоактивы на кошелек платформы. С ним могут активно связываться сотрудники «поддержки» через чат, электронную почту или мессенджеры.
30. Пользователь открывает счет у ПУВА, приобретает криптоактивы банковской картой или переводом и направляет их с собственного счета ПУВА на кошелек «торговой платформы».
31. Операторы платформы присваивают криптоактивы, причиняя жертве значительный ущерб и лишая ее возможности вернуть средства.
32. Последующий анализ показывает, что видеоролик со «знаменитостью» являлся дипфейком, а сайт, изображения, коммуникации службы поддержки и утверждения о регулируемом статусе были созданы при помощи генеративного ИИ.

Индикаторы, связанные с ИИ

- Дипфейки в рекламных материалах выглядят неубедительно или содержат явные дефекты, например несинхронные движения губ.
- Знаменитости или публичные лица, использованные в дипфейках, публично заявляли, что никогда не рекламировали соответствующий криптоактив или финансовый продукт.
- Сайт и сопроводительные материалы содержат несоответствия; поиск изображений может показать, что фотографии «руководителей» принадлежат другим людям, не связанным с платформой.
- Коммуникации службы поддержки содержат ошибки или признаки создания большой языковой моделью.
- Открытые реестры регулирующих органов и базы лицензий не подтверждают наличие разрешения у торгового сервиса.

Транзакционные и иные индикаторы

- Клиент ПУВА внезапно начинает покупать крупные суммы криптоактивов и переводить их на внешние кошельки, не имея существенной предыдущей истории торговли.
- Скрининг кошелька и операций показывает необъяснимо высокую прямую или косвенную связь с адресами, связанными с мошенническими схемами.
- Клиент не может достоверно объяснить операции, неохотно предоставляет информацию либо демонстрирует слабое понимание криптоактивов и торговли ими.
- Клиент относится к категории повышенной уязвимости: например, пожилой возраст, финансовые трудности либо серьезное жизненное событие, такое как безработица или развод.

Пример типологии: преступники атакуют ПУВА через сотрудников с использованием созданных ИИ изображений и контента

Третий способ использования ИИ для завладения криптоактивами заключается в обмане сотрудников ПУВА или иного сервиса методами социальной инженерии. Дипфейки, поддельные документы и коммуникации позволяют преступнику убедить сотрудника, что перед ним доверенный внешний контрагент или известный коллега, и использовать это доверие для получения доступа к системам ПУВА и хищения активов ПУВА, его клиентов, поставщиков или партнеров.

Как работает схема

33. Киберпреступник создает убедительную онлайн-персону и использует ее для контакта с сотрудниками криптобиржи. Например, создается профиль LinkedIn сотрудника отдела кадров или рекрутера, предлагающего работу. В иных случаях преступник выдает себя за сотрудника поставщика ПУВА или даже за сотрудника самого ПУВА, включая финансового директора.
34. После установления контакта преступник продолжает коммуникацию для формирования доверия: регулярно направляет электронные письма, голосовые сообщения и проводит короткие видеозвонки.
35. Сотрудники могут открывать полученные вложения и предоставлять чувствительную информацию о работодателе, включая сведения об ИТ-системах и финансовых счетах.
36. Сотрудники не знают, что фотографии, тексты писем и видеозаписи в ходе звонков были созданы генеративным ИИ.
37. Получив необходимую информацию, киберпреступник использует уязвимость ПУВА. Если сотрудник открыл файл с вредоносным ПО, преступник может получить прямой доступ к «горячим» кошелькам и похитить средства. Альтернативно он может убедить сотрудников перевести активы на подконтрольные ему внешние некастодиальные кошельки либо использовать доступ к системам и коммуникациям ПУВА для перенаправления средств клиентов или партнеров.

Индикаторы в целом соответствуют указанным выше признакам ИИ-мошенничества: дефекты дипфейков, несоответствия в документах и веб-ресурсах, отсутствие подтверждения лицензий, а также нетипичные или подозрительные коммуникации.

Практический пример: политические дипфейки в криптомошенничестве перед выборами в США 2024 года

В преддверии выборов в США в ноябре 2024 года мошенники использовали генеративный ИИ для хищения криптоактивов у ничего не подозревающих жертв. Они также воспользовались более благожелательной к криптоактивам риторикой американских политиков для создания убедительного контента.

Один из примеров представлял собой мошеннический веб-сайт, выдававший себя за официальный предвыборный ресурс президента Дональда Трампа. На сайте предлагалась «раздача» биткоинов на сумму до 100 млн долларов США: каждому, кто отправлял средства на указанный Bitcoin-адрес, обещалось удвоение платежа.

На сайте размещались дипфейк-фотографии и видеоролики президента Трампа и Илона Маска. В поддельных видео они якобы рекламировали схему. Один ролик использовал фрагменты реального выступления Трампа на конференции Bitcoin 2024, но к нему был добавлен текст о мошеннической инвестиционной схеме. Несмотря на правдоподобное звучание голосов, аудиозапись не совпадала с движениями губ - характерный индикатор дипфейка.

Elliptic установила, что криптоадреса, связанные с несколькими сайтами, использовавшими такие схемы, получили от жертв криптоактивы примерно на 24 тыс. долларов США. Блокчейн-анализ показал, что преступники отмывали средства, переводя их через несколько промежуточных кошельков, после чего направляли их в сервис обмена криптоактивов, расположенный в России.

ИИ как часть решения

Несмотря на рост преступного использования ИИ, важно учитывать, что ИИ и связанные технологии способны существенно повысить эффективность выявления и пресечения финансовых преступлений. Elliptic уже использует ИИ для развития следующего поколения блокчейн-аналитики.

Машинное обучение для повышения эффективности выявления ОД с использованием криптоактивов

Блокчейны являются благоприятной средой для методов машинного обучения благодаря публичной доступности данных о транзакциях и информации о типах участвующих субъектов. В традиционных финансах такие данные, напротив, часто разделены между различными системами, что затрудняет применение аналогичных методов.

Первое исследование Elliptic по этой теме было опубликовано в 2019 году совместно с MIT-IBM Watson AI Lab. В нем модель машинного обучения обучалась выявлять Bitcoin-транзакции, совершенные противоправными субъектами, например операторами программ-вымогателей или рынков даркнета.

В мае 2024 года Elliptic опубликовала новое исследование с применением усовершенствованных методов к набору почти из 200 млн транзакций. Исследование, также выполненное совместно с MIT-IBM Watson AI Lab, выявило новые модели, включая использование промежуточных «вложенных сервисов» (nested services). Знание таких моделей ОД полезно специалистам ПОД и следователям и может быть включено в набор поведенческих признаков, выявляемых инструментами Elliptic.

Расширение возможностей комплаенс с помощью Elliptic Copilot

38. В апреле 2025 года Elliptic объявила о запуске Elliptic Copilot - первой из серии функций на основе ИИ.
39. Copilot существенно сокращает время, необходимое аналитикам для обработки предупреждений скрининга и оценки контекстной информации, включая визуальные графы риска, данные о транзакциях и сведения о кошельках контрагентов. Инструмент агрегирует информацию платформы и автоматически формирует анализ Risk Graph, содержащий данные, необходимые для комплексного риск-ориентированного решения.
40. Copilot использует аналитический граф, охватывающий более 50 блокчейнов и тысячи активов, и поддерживает выявление более 300 мостов и миксеров. Если требуется дополнительное расследование, для каждого предупреждения формируется граф расследования, автоматически визуализирующий наиболее значимые операции.
41. Copilot объединяет данные аналитического графа Elliptic с внешними источниками для углубления контекста по субъектам и организациям. ИИ формирует сводный отчет по предупреждению и результатам расследования, который может использоваться при подготовке сообщений о подозрительной деятельности (SAR) и иных отчетных материалов, существенно сокращая трудозатраты аналитиков и следователей.
42. Copilot уменьшает время на сбор информации и формирование контекста для управления предупреждениями о риске, позволяя специалистам уделять больше внимания задачам, требующим человеческого профессионального суждения.

2. Промышленная профессионализация экосистемы мошенничества типа «pig butchering»

Понимание риска

Среди различных видов преступлений, затрагивающих индустрию криптоактивов, в последние годы особенно пристальное внимание привлекают схемы «pig butchering» - разновидность романтического и инвестиционного мошенничества, при которой жертву постепенно убеждают расстаться с денежными средствами через фиктивные, но внешне весьма убедительные инвестиционные проекты с криптоактивами.

Название происходит от китайского выражения *Sha Zhu Pan*. Транснациональные организованные преступные группы в Юго-Восточной Азии реализуют такие схемы из крупных мошеннических центров, расположенных, в частности, в Лаосе, Мьянме и Камбодже. Многие непосредственные исполнители мошенничества сами являются жертвами торговли людьми и принуждаются участниками организованных преступных групп к совершению преступлений, в то время как конечную прибыль получают организаторы.

Ежегодные потери от «pig butchering» исчисляются миллиардами долларов США и обеспечивают преступным организациям огромные доходы. Масштаб таких схем стал возможен благодаря формированию промышленной экосистемы, позволяющей проводить их все более прибыльно, эффективно и профессионально.

В центре этой экосистемы находятся крупные торговые площадки, известные как «guarantee marketplaces» - гарантийные маркетплейсы. Эти китайскоязычные сервисы электронной коммерции действуют как универсальные площадки, на которых можно приобрести все необходимые инструменты для масштабного осуществления мошенничества. Продавцы, обычно работающие в открытом интернете и рекламирующие услуги через Telegram и другие мессенджеры, предлагают технологии, персональные данные и услуги по ОД, необходимые мошенникам на всех этапах схемы.

Появление таких площадок позволило масштабировать «pig butchering» аналогично тому, как несколько лет назад модель «ransomware-as-a-service» (RaaS) на рынках даркнета способствовала росту прибыльности атак с применением программ-вымогателей. Поскольку отдельные задачи можно передавать специализированным поставщикам услуг, организаторы мошенничества концентрируются на извлечении из жертв все более крупных сумм с более высокой доходностью.

Мошенники также используют ИИ и связанный с ним общественный интерес, приобретая через такие площадки дипфейки и иной контент, сгенерированный ИИ. Это дополнительно свидетельствует о профессионализации противоправной индустрии.

Ключевую роль в поддержании многомиллиардной экосистемы играют специализированные сервисы и сети по ОД, скрывающие доходы от «pig butchering» с использованием различных методов. Среди них - гарантийные маркетплейсы, «цепочки дробления» (peeling chain) и переходы между блокчейнами (chain-hopping), применяемые для сокрытия финансовой активности.

Государства предпринимают жесткие меры против таких схем, включая финансовые санкции и аналогичные инструменты. Среди мер, принятых с начала 2025 года:

- **26 февраля:** Сеть по борьбе с финансовыми преступлениями Министерства финансов США (FinCEN) напомнила финансовым учреждениям о необходимости проявлять повышенную бдительность при выявлении и направлении сообщений об операциях, связанных со схемами «pig butchering».
- **7 апреля:** Австралийская комиссия по ценным бумагам и инвестициям (ASIC) прекратила деятельность 95 компаний, подозреваемых в содействии таким схемам.
- **1 мая:** FinCEN признала Huione Group, управлявшую гарантийным маркетплейсом и платежными сервисами, «основным объектом обеспокоенности в сфере отмывания денег» в соответствии с

разделом 311 Закона USA PATRIOT Act и предложила обязать финансовые учреждения США применять специальные меры к субъектам Huione Group. Компании группы обеспечивали транзакции на миллиарды долларов, связанные с «pig butchering» и иными преступлениями, предоставляя технологическую и платежную инфраструктуру и услуги по ОД.

- **5 мая:** Управление по контролю за иностранными активами Министерства финансов США (OFAC) ввело санкции против Karen National Army - вооруженной группировки в Мьянме - и трех представителей ее руководства за деятельность в качестве транснациональной преступной организации, получавшей миллиарды долларов от кибермошенничества, включая «pig butchering».
- **29 мая:** OFAC ввело санкции против зарегистрированного на Филиппинах поставщика облачной инфраструктуры Funnull и связанного с ним лица Liu Lizhi за размещение сайтов, использовавшихся в схемах «pig butchering».

Используя поведенческое выявление на основе блокчейна и иные методы, специалисты комплаенс и следователи способны устанавливать потоки средств, связанные с такими схемами. Эта информация имеет решающее значение для пресечения деятельности преступных сетей. В первой половине 2025 года два крупнейших маркетплейса, поддерживавших экосистему «pig butchering», - Huione Guarantee и Xinbi Guarantee - были ликвидированы в рамках скоординированных действий правоохранительных органов. В другом деле правительство США изъяло более 225 млн долларов США в криптоактивах, связанных с такими схемами.

Пример типологии: клиент ПУВА является жертвой «pig butchering»

Аналитики комплаенс ПУВА способны содействовать пресечению «pig butchering», выявляя случаи, когда их собственные клиенты могли стать жертвами. Данные, собираемые ПУВА в таких ситуациях, могут иметь критическое значение для правоохранительных органов при формировании полной аналитической картины деятельности более широких мошеннических сетей и преступных организаций.

Как работает схема

43. Мошенник связывается с лицом через сайт знакомств или социальную сеть и в течение недель или месяцев формирует доверие. Общение может происходить в основном в текстовой форме, но также включать голосовые и видеозвонки.
44. После формирования доверия мошенник убеждает жертву инвестировать в криптоактивы, утверждая, что сам получил значительную прибыль и что жертва также может заработать.
45. Жертве направляют ссылки на сайты, внешне похожие на законные инвестиционные платформы с высокой доходностью. Жертву убеждают вложить сбережения в криптоактивы и открыть счет у ПУВА для конвертации фиатной валюты.
46. Жертва открывает счет у ПУВА, покупает криптоактивы банковским переводом либо дебетовой/кредитной картой и направляет небольшую сумму на некастодиальный кошелек, якобы связанный с инвестиционной платформой, но фактически контролируемый мошенниками.
47. Через несколько дней обратно на счет жертвы у ПУВА переводится небольшая доля первоначальной суммы, например 4-5 %. Это «приманочная» (baiting) транзакция, создающая впечатление реальной инвестиционной доходности.
48. В последующие дни или недели жертва переводит на мошеннический кошелек все более крупные суммы - тысячи и десятки тысяч долларов. Мошенник может вернуть еще одну-две небольшие суммы, стимулируя дальнейшие переводы, пока общий размер вложений не достигнет десятков или сотен тысяч, а иногда миллионов долларов США в криптоактивах.
49. В определенный момент мошеннический сайт начинает выдавать ошибки либо требует дополнительную «комиссию» для разблокирования средств. К этому моменту жертва фактически утрачивает криптоактивы.
50. После хищения преступники приступают к ОД и конвертации средств в фиатную валюту, используя различные методы, описанные далее.

Индикаторы

- Новый клиент без предыдущего опыта торговли криптоактивами внезапно открывает счет и покупает крупную сумму криптоактивов - на десятки или сотни тысяч долларов.
- История операций соответствует типологии: небольшие первоначальные исходящие тестовые переводы либо входящие «приманочные» транзакции, за которыми следует серия крупных исходящих переводов при отсутствии последующих входящих средств.
- Блокчейн-анализ показывает значительную связь с адресами, ранее установленными как относящиеся к «pig butchering» или иным мошенническим схемам.
- Клиент может относиться к уязвимой категории либо переживать обстоятельства, повышающие восприимчивость к мошенничеству: пожилой возраст, значительные долги, финансовые трудности, недавний развод или вдовство.
- При уточнении характера операций клиент демонстрирует слабое понимание криптоактивов, выглядит растерянным, занимает оборонительную позицию либо неохотно раскрывает детали, возможно из-за стыда или смущения.
- Анализ адреса назначения показывает, что другие клиенты ПУВА также переводили средства на тот же кошелек. Это может указывать на нескольких жертв и на аккумулирование похищенных средств в одном кошельке перед дальнейшим ОД.

Пример типологии: отмывание доходов от «pig butchering»

После получения средств от жертв преступники должны скрыть их происхождение и обеспечить возможность конечного использования доходов организаторами. Все чаще для этого применяются специализированные услуги по ОД, которые рекламируются на гарантийных маркетплейсах именно как инструмент сокрытия доходов от «pig butchering».

Выявление потоков таких средств критически важно не только для пресечения деятельности непосредственных мошенников, но и для разрушения инфраструктуры услуг, поддерживающей их деятельность. Эти сведения также могут способствовать возврату активов жертвам.

Как работает схема

51. После того как жертвы переводят криптоактивы, лица, осуществляющие ОД в интересах мошенников, аккумулируют похищенные средства в одном специализированном кошельке либо группе кошельков.
52. Затем средства в короткий период времени направляются через большое количество промежуточных кошельков - реализуется «цепочка дробления» (chain peeling). В отдельных случаях используется до ста промежуточных адресов.
53. Параллельно применяются другие методы, например переходы между блокчейнами или криптомиксеры.
54. После этого средства направляются на один или несколько ПУВА, включая платежные сервисы или биржи, которые могут входить в ту же группу, что и гарантийный маркетплейс. Средства распределяются по многочисленным счетам денежных мулов, открытым по поддельным документам и с недостоверными KYC-данными.
55. В отдельных случаях криптоактивы со счетов мулов выводятся на некастодиальные кошельки и подвергаются дополнительному ОД через новые цепочки промежуточных адресов.
56. Некоторые счета мулов действуют как «транзитные» (pass-through) счета: преступники переводят средства между собственными счетами внутри платформы, имитируя законную активность с крупными суммами.
57. После завершения указанных этапов криптоактивы конвертируются в фиатные валюты для последующего ОД через банковскую систему.

Индикаторы

- Некастодиальный кошелек регулярно получает переводы от клиентов ПУВА, сообщивших, что стали жертвами «pig butchering». История кошелька состоит практически исключительно из приема и консолидации средств жертв с последующей быстрой отправкой на другие адреса.
- Потоки из «пуловых» кошельков демонстрируют частые переводы на адреса, связанные с известным мошенничеством, цепочки дробления либо попытки перехода в другие блокчейны через межсетевые мосты, платежные сервисы или гарантийные площадки, где рекламируются услуги по ОД.
- Счета мулов у ПУВА имеют общие признаки: совпадающие KYC-данные, например адреса проживания; сходные IP-адреса при входе; регулярные внутри-платформенные переводы между несколькими счетами.
- KYC-данные указывают на нахождение владельцев счетов в юрисдикциях, откуда часто исходят схемы «pig butchering», включая Вьетнам, Филиппины, Таиланд, Лаос, Мьянму и Камбоджу.
- Фотографии и селфи, полученные ПУВА в рамках KYC, могут показывать, что владельцы счетов находятся на территории склада или колл-центра.

Практический пример: США изъяли 225 млн долларов США доходов от «pig butchering»

В июне 2025 года Министерство юстиции США (DOJ) подало гражданский иск о конфискации 225 млн USDT у сети, занимавшейся отмыванием доходов от «pig butchering». В материалах дела подробно описаны методы ОД, с помощью которых только через один ПУВА было перемещено более 3 млрд долларов США, что демонстрирует масштаб и сложность сетей, обслуживающих такие схемы.

Правоохранительные органы США подключились к делу после обращения криптобиржи OKX. Биржа выявила 144 счета, предположительно связанных с «pig butchering» и ОД. В результате масштабного расследования было установлено, что преступная сеть, управлявшая этими счетами, отмывала доходы от мошенничества в отношении 434 отдельных потерпевших.

Жертвы находились, в частности, в США, Великобритании, Германии и Австралии. Мошенники связывались с ними через социальные сети, включая LinkedIn, выдавали себя за успешных инвесторов в криптоактивы и убеждали вкладывать средства. После общения через Telegram, WhatsApp и иные мессенджеры потерпевшие снимали значительные суммы с банковских счетов и покупали криптоактивы на крупных биржах, в том числе зарегистрированных в США. Один потерпевший, занимавший должность генерального директора банка в Канзасе, присвоил почти 50 млн долларов США из средств банка для финансирования таких покупок.

После приобретения криптоактивов потерпевшие переводили их на один из 93 некастодиальных адресов, предоставленных мошенниками. Они считали, что направляют средства на законную инвестиционную платформу. Им предоставлялись ссылки на сайты, внешне похожие на торговые платформы, под названиями «FX6Pro» и «YoBitProl.lol». Некоторые жертвы сначала могли вывести небольшие суммы, например 500 долларов США, после чего доступ к сайту блокировался и остальные средства терялись. Это указывало на использование «приманочных» транзакций для формирования доверия.

После поступления средств на один из 93 кошельков участники сети быстро переводили их через многочисленные промежуточные адреса, многие из которых получали средства и от других жертв. В отдельных случаях использовалось почти сто промежуточных кошельков. Некоторые адреса ранее фигурировали в сообщениях о мошенничестве, направленных в Internet Crime Complaint Center (IC3) ФБР и Федеральную торговую комиссию США (FTC).

После многочисленных переходов средства депонировались на 22 счета OKX, использовавшихся для консолидации доходов от большого числа жертв. Блокчейн-анализ показал отсутствие законной экономической цели этих счетов - они использовались исключительно для аккумулирования похищенных средств.

Затем сеть часто выводила средства с биржи, переводила их через дополнительные некастодиальные промежуточные кошельки и вновь вносила на OKX - уже на один из дополнительных 122 счетов, находившихся под контролем сети. Между этими счетами неоднократно совершались внутренние переводы.

Все 144 счета демонстрировали не только взаимосвязанную финансовую активность, но и иные признаки общего контроля: совпадающие IP-адреса на Филиппинах, аналогичные KYC-данные, документы, удостоверяющие личность, выданные во Вьетнаме, и общие адреса компаний. Эти признаки указывали на сеть денежных мулов.

Фотографии, представленные владельцами счетов при регистрации, по-видимому, были сделаны в одном и том же помещении, напоминавшем колл-центр. Сочетание вьетнамских документов и фактического местоположения на Филиппинах позволило следователям предположить, что лица, на которых были оформлены счета, могли являться принудительными работниками мошеннического центра.

Анализ показал, что с ноября 2022 года по ноябрь 2023 года сеть провела более 257 тыс. транзакций на общую сумму около 2,9 млрд долларов США - в среднем около 700 операций в день примерно на 8 млн долларов США.

После многократного перемещения средств через 144 счета OKX участники сети направляли их через группу из 35 промежуточных некастодиальных кошельков и затем консолидировали в другой группе кошельков. Выявление восьми таких адресов позволило правоохранительным органам США изъять 225 млн USDT. Эмитент USDT, компания Tether, сотрудничала с органами и заморозила средства.

Американские ПУВА также сыграли важную роль в пресечении сети. В июле 2025 года биржа Kraken сообщила об участии в недельной совместной операции с правоохранительными органами и другими ПУВА, в ходе которой следователи смогли связать блокчейн-данные с KYC-информацией о потерпевших.

Ключевые меры контроля и рекомендации по расследованию

Меры комплаенс-контроля

- Использовать скрининг кошельков и транзакций для выявления операций клиентов с необычно высокими объемами и суммами, связанными с адресами, относимыми к схемам «pig butchering».
- Анализировать граф транзакций для выявления связанных потоков, включая сведения из сообщений о подозрительной деятельности/операциях и взаимодействия с правоохранительными органами.
- Настраивать системы скрининга таким образом, чтобы активность, потенциально связанная с «pig butchering», получала надлежащий риск-рейтинг и формировала предупреждения в соответствии с риск-аппетитом организации.
- Предупреждать клиентов о рисках мошенничества и проводить информационные кампании.
- Обучать сотрудников комплаенс характерным признакам схем, включая «приманочные» платежи и использование денежных мулов.
- Устанавливать лимиты для новых клиентов и применять дополнительные меры надлежащей проверки клиента до повышения лимитов по счету и операциям; например, запрашивать дополнительную информацию о цели торговли.

Рекомендации по расследованию

- Использовать поведенческое выявление для установления кошельков, потенциально связанных с «pig butchering», и строить графы связей и потоков с другими адресами и субъектами.
- Использовать блокчейн-аналитику для выявления кошельков, которые направляют средства на гарантийные маркетплейсы.

- Сопоставлять данные корпоративных реестров - наименования компаний, структуру собственности - для установления связей между гарантийными сайтами и другими юридическими лицами, оказывающими сопутствующие услуги.
- Анализировать IP-адреса, полученные при установлении деловых отношений и входе в систему ПУВА, для выявления признаков нахождения лиц в странах, связанных с «pig butchering».
- Проверять базы сообщений о мошенничестве, чтобы установить, фигурировали ли адреса, получавшие соответствующие доходы, в иных эпизодах.

Значение поведенческого выявления в противодействии мошенничеству

Одним из фундаментальных элементов выявления и пресечения «pig butchering» является использование поведенческого анализа для идентификации подозрительных кошельков. Эти инструменты применимы не только к данной типологии, но и к другим видам мошенничества в экосистеме криптоактивов.

Elliptic указывает, что поведенческое выявление позволяет автоматически определять не менее 15 других видов мошенничества, включая:

58. **Ice phishing** - поддельные раздачи и airdrop-кампании побуждают жертв подключать кошельки к вредоносным смарт-контрактам, которые выводят их активы.
59. **Токены-имитаторы (impersonation tokens)** - создание токенов, внешне похожих на популярные и законные активы, например USDT или USDC, с целью спровоцировать ошибочную покупку или инвестицию.
60. **Rug pull** - использование скрытого («backdoor») кода в смарт-контракте, позволяющего мошенникам вывести вложенные в проект средства.
61. **Подмена/«отравление» адреса (address poisoning)** - создание адресов, визуально похожих на привычные адреса контрагентов жертвы.

Подразделения комплаенс ПУВА и финансовых учреждений могут использовать такие данные при скрининге входящих депозитов и запрашиваемых клиентами выводов средств. При выявлении кошелька, потенциально связанного с мошенничеством, система формирует предупреждение, после чего комплаенс может принять меры по предупреждению операции и направлению соответствующей отчетности.

Аналитики и следователи, в свою очередь, могут проводить углубленные расследования потоков ОД, связанных с мошенническими схемами, что потенциально способствует возврату активов потерпевшим.

3. Расширение использования стейблкоинов санкционными субъектами

Понимание риска

Стейблкоины - криптоактивы, стоимость которых привязана к фиатной валюте, корзине валют или иным активам, - в настоящее время относятся к числу наиболее перспективных инноваций в сфере криптоактивов. За счет снижения ценовой волатильности, характерной для большинства криптоактивов, стейблкоины выполняют особую функцию в экосистеме виртуальных активов.

Стабильность стоимости делает их пригодными для платежных сценариев, включая расчеты с торговыми предприятиями и повседневные розничные операции. Трансграничная природа позволяет переводить стоимость между юрисдикциями без необходимости использования традиционных посредников для расчетов.

В последние годы стейблкоины сыграли важную роль в развитии DeFi, обеспечивая ликвидность на децентрализованных биржах (DEX) и способствуя росту стоимости активов, заблокированных в DeFi-протоколах, до 200 млрд долларов США в год.

Еще более важно, что стейблкоины все чаще рассматриваются как одна из технологий, способных обеспечить массовое внедрение криптоактивов. Объемы торговли и использования стейблкоинов последовательно растут. Совокупный мировой объем переводов в стейблкоинах превышает 27 трлн долларов США, что позволяет им потенциально конкурировать с традиционными платежными системами.

Эта динамика привлекла внимание не только участников криптоиндустрии, но и традиционных финансовых организаций, финтех-платформ, электронной коммерции и других отраслей. Societe Generale, PayPal, Stripe и Shopify уже запустили собственные стейблкоины либо интегрируют их в свои продукты. Citi, Wells Fargo и Bank of America заявляли о планах использования стейблкоинов. Apple, Airbnb, Walmart, Amazon и другие крупные компании также сообщали об изучении возможных сценариев их применения.

Коммерческий интерес усиливается формированием более благоприятной и определенной нормативной среды. Европейский союз и Гонконг сформировали специальные режимы регулирования эмитентов стейблкоинов; США также начали внедрять собственную нормативную базу. Рост правовой определенности повысил готовность крупных корпораций безопасно использовать такие инструменты.

Хотя основная часть операций со стейблкоинами носит законный характер, расширение их использования неизбежно сопровождается ростом противоправного применения. В настоящем отчете уже рассматривалось использование стейблкоинов в мошеннических схемах типа «pig butchering». Значимым направлением риска также является обход финансовых и экономических санкций.

Стейблкоины обладают характеристиками, особенно привлекательными для находящихся под санкциями лиц, организаций и государств: относительно стабильная стоимость, высокая скорость расчетов и возможность перемещать средства через границы вне традиционной банковской системы. Для субъектов, исключенных из международной финансовой системы, эти свойства особенно важны.

Кроме того, крупнейшие стейблкоины привязаны к доллару США. Это позволяет санкционным субъектам, ограниченным в доступе к банковской системе США, осуществлять коммерческие операции, в том числе торговлю нефтью и газом, традиционно номинированную в долларах США, без непосредственного использования системы долларового клиринга на этапе расчетов.

В результате санкционные субъекты уже интегрировали стейблкоины в схемы обхода санкций.

Основные формы обхода санкций с использованием стейблкоинов

62. **Трансграничные переводы средств.** Санкционные субъекты могут осуществлять международные операции через некастодиальные кошельки, обходя банки и других традиционных посредников. Для этого все чаще используются специализированные брокеры по криптоактивам, которые проводят операции через ПУВА повышенного риска, создающие существенный риск обхода санкций.
63. **Прямая оплата товаров и услуг.** Санкционные субъекты могут напрямую оплачивать услуги или товары контрагентам в стейблкоинах, не проводя расчеты через традиционные финансовые каналы. Это также может снижать риск вторичных санкций для банков третьих стран, поскольку исключает их из прямого взаимодействия с финансовыми учреждениями санкционных юрисдикций на этапе расчетов.
64. **Хищение.** Санкционные киберпреступные группы, включая хакерские структуры КНДР, нередко получают стейблкоины в результате атак на криптоплатформы и DeFi-протоколы. Обычно активы затем конвертируются в другие криптоактивы, иногда вновь в стейблкоины, а впоследствии - в фиатную валюту.
65. **Выпуск собственных стейблкоинов.** Некоторые санкционные субъекты и юрисдикции, включая Россию и Иран, публично выражали интерес к выпуску собственных стейблкоинов как альтернативному расчетному механизму для торговли. В июле Elliptic опубликовала исследование об использовании российскими субъектами привязанного к рублю криптоактива A7A5 для обхода санкций в отношении банковской системы России. Российская оборонная компания «Ростех» также сообщала о намерении использовать собственный стейблкоин RUBx для расчетов по военным товарам. Собственный выпуск стейблкоинов может снижать риск замораживания средств эмитентами, находящимися в США, Европе и других юрисдикциях.

При этом важно подчеркнуть, что сами свойства стейблкоинов создают и возможности для пресечения обхода санкций.

Во-первых, прозрачность блокчейна позволяет выявлять адреса стейблкоинов, используемые санкционными субъектами, включая лиц и организации, включенные в санкционные перечни OFAC, ЕС, Великобритании и других юрисдикций, а также отслеживать связанные потоки средств. Это дает подразделениям комплаенс возможность выявлять и блокировать соответствующие средства, а правоохранительным и регулирующим органам - устанавливать активы санкционных субъектов.

Во-вторых, крупнейшие стейблкоины обычно предусматривают техническую функцию замораживания средств на уровне смарт-контракта. Это позволяет эмитенту по взаимодействию с правоохранительными и регулирующими органами блокировать определенные адреса, связанные с санкционными субъектами.

На этих особенностях основана технология Elliptic Ecosystem Monitoring, позволяющая эмитентам стейблкоинов проактивно замораживать средства, связанные с конкретными эпизодами противоправной деятельности, и получать агрегированную аналитику по рискам во всей экосистеме токена.

Пример типологии: санкционный субъект осуществляет трансграничные операции в стейблкоинах для обхода банковских ограничений

Одной из основных потребностей санкционных лиц и организаций либо субъектов, находящихся в санкционных юрисдикциях, является трансграничное перемещение средств. Для этого они могут использовать специализированные сети брокеров и бирж, получать доступ к стейблкоинам и переводить средства за рубеж, избегая прямого взаимодействия с банковским сектором.

Как работает схема

66. Санкционное лицо намерено переместить средства за рубеж и передает фиатную валюту брокеру, оказывающему услуги по обходу санкций и ОД. Передача может осуществляться наличными либо банковским переводом через счета подставных юридических лиц.
67. Брокер обменивает фиатную валюту на стейблкоины на криптобирже. Как правило, используется площадка в санкционной или иной высокорисковой юрисдикции, где отсутствуют содержательные меры ПОД/ФТ либо даже рекламируется возможность анонимных переводов.
68. Брокер переводит стейблкоины на некастодиальный кошелек, контролируемый лицом или организацией в другой юрисдикции.
69. Стейблкоины направляются ПУВА и обмениваются на фиатную валюту.
70. Фиатные средства выводятся со счета у ПУВА и далее перемещаются через банковскую систему.

Индикаторы

- Клиент ПУВА регулярно получает или принимает крупные переводы стейблкоинов с адресов, связанных с нерегулируемым ПУВА, организацией с минимальными или отсутствующими мерами ПОД/ФТ либо субъектом, обладающим признаками санкционного риска. Например, ПУВА может быть зарегистрирован в несанкционной стране, но его конечные бенефициарные владельцы находятся в санкционной юрисдикции или в непосредственной близости к ней.
- Блокчейн-анализ выявляет иные признаки санкционного риска: прямую или косвенную связь с кошельками лиц и организаций из санкционных перечней либо с адресами, связанными с санкционными юрисдикциями.
- Клиент не способен внятно объяснить экономическую цель операций либо причины наличия санкционной подверженности.

Пример типологии: прямая оплата товаров и услуг в стейблкоинах

Стейблкоины могут быть особенно привлекательны для оплаты товаров и услуг, цена которых номинирована в долларах США, евро или другой валюте, при использовании которой санкционный субъект подвергался бы риску выявления в традиционных финансовых каналах.

Как работает схема

71. Санкционное лицо намерено приобрести товар или услугу у зарубежного контрагента. Стороны договариваются об оплате в стейблкоинах и определяют стоимость в базовой валюте, к которой привязан стейблкоин, например в долларах США или евро.
72. Санкционный субъект приобретает стейблкоины через ПУВА, не соблюдающий установленные требования, либо через посредника-брокера.
73. Санкционное лицо или брокер переводит стейблкоины со своего некастодиального кошелька на некастодиальный кошелек контрагента.
74. Контрагент переводит стейблкоины на кошелек у ПУВА и после получения оплаты поставляет товар или оказывает услугу. Расчет может включать первоначальный депозит и последующую оплату остатка после подтверждения поставки.
75. Контрагент конвертирует стейблкоины в фиатную валюту и интегрирует ее в банковскую систему.

Индикаторы

- Клиент ПУВА получает либо запрашивает крупные или многочисленные переводы стейблкоинов без ясного экономического обоснования.
- Клиент работает в секторе, часто связанном с обходом санкций, например нефтегазовом секторе или торговле предметами роскоши.

- История операций клиента содержит повышенные санкционные риски: связь с субъектами из России, Ирана, КНДР, Венесуэлы либо с контрагентами в третьих юрисдикциях, часто используемых в схемах обхода санкций, например Турции, ОАЭ и Гонконге.
- Анализ операций между контрагентами выявляет попытки скрыть транзакционный след в блокчейне: цепочки дробления, использование миксеров и иные методы.
- Стейблкоины могли быть приобретены через DEX.
- Клиент регулярно входит в свой аккаунт с IP-адресов, связанных с юрисдикционным риском.

Пример типологии: санкционные киберсубъекты отмывают похищенные стейблкоины

Санкционные киберсубъекты, например Lazarus Group, связанная с КНДР, могут получать десятки и сотни миллионов долларов в стейблкоинах в результате взломов ПУВА и DeFi-протоколов. Чтобы избежать замораживания со стороны эмитента, преступникам необходимо быстро осуществить ОД.

Как работает схема

76. Санкционный киберпреступник в результате атаки на ПУВА или DeFi-протокол получает десятки или сотни различных криптоактивов, включая стейблкоины.
77. Чтобы снизить риск падения стоимости менее ликвидных активов до завершения ОД, часть активов конвертируется через DEX в стейблкоины.
78. Полученные стейблкоины и стейблкоины, непосредственно похищенные при атаке, перемещаются в другой блокчейн, например Ethereum, через межсетевой мост.
79. На DEX средства обмениваются на нативный токен соответствующего блокчейна, например Ether. После такой конвертации эмитент исходного стейблкоина уже не может заморозить эти активы.
80. Затем средства направляются ПУВА и конвертируются в фиатную валюту.

Индикаторы

- Клиент ПУВА внезапно получает крупный объем средств вскоре после публично известного взлома; происхождение или цель средств неясны.
- Комплексный блокчейн-скрининг показывает, что средства в короткий период прошли через DEX и межсетевые мосты без очевидного экономического объяснения.
- В операции имеются признаки цепочки дробления, при которой средства быстро проходят через множество промежуточных кошельков.
- Анализ выявляет косвенную связь с адресами санкционных киберпреступных групп, например Lazarus Group.

Практический пример: США раскрывают российские сети обхода санкций

В июне 2025 года Министерство юстиции США объявило о предъявлении обвинения гражданину России в связи со схемой обхода санкций, в рамках которой через США было проведено более 500 млн долларов США в интересах лиц и организаций, имевших счета в российских банках, находящихся под санкциями. Основным инструментом расчетов являлся USDT.

По данным DOJ, гражданин России Юрий Гугнин, проживавший в Нью-Йорке, создал компанию Evita и использовал ее для проведения операций в интересах зарубежных лиц и организаций, обслуживавшихся в санкционных российских банках. Поскольку банкам США запрещено проводить операции в интересах этих банков, их клиенты фактически лишены доступа к системе долларового клиринга. Схема позволяла использовать стейблкоины как «мост» к долларовой системе.

Гугнин открыл от имени Evita счета в банках и на криптобиржах США, однако в ходе KYC не раскрыл российскую направленность бизнеса. Он также получил лицензию на денежные переводы в штате Флорида, используя ложные сведения, чтобы убедить подразделения комплаенс банков и криптобирж США в законности бизнеса.

Через эти счета он проводил операции в интересах российских субъектов, обслуживавшихся санкционными банками. В качестве одного из клиентов DOJ указывает государственную корпорацию «Росатом», которой Гугнин, согласно обвинению, содействовал в приобретении у американской компании чувствительного оборудования, подпадающего под экспортный контроль.

Российский клиент приобретал USDT и переводил их Гугнину. Затем USDT конвертировались на американских криптобиржах в доллары США, после чего на эти средства приобретались товары для российских заказчиков. Помимо чувствительных технологий, приобретались предметы роскоши, включая произведения искусства и яхты; для сокрытия конечной цели платежей создавались ложные чеки и счета-фактуры.

В декабре 2024 года OFAC предприняло меры против отдельной российской сети обхода санкций - TGR Group, международной сети компаний и лиц, обеспечивавшей российским состоятельным клиентам обход ограничений. В рамках этих мер OFAC ввело санкции против Елены Чиркинян, которая, по данным OFAC, использовала USDT в интересах TGR Group, в том числе для покупки российскими клиентами недвижимости в Великобритании.

По версии OFAC, TGR Group принимала наличные рубли от состоятельных российских клиентов, затем средства конвертировались в стейблкоины на связанной с группой бирже Garantex. После этого USDT направлялись на адрес, принадлежавший Чиркинян и включенный OFAC в перечень Specially Designated Nationals and Blocked Persons (SDN).

Практический пример: прекращение деятельности российской биржи Garantex

Одним из ключевых участников, содействовавших обходу санкций с использованием стейблкоинов и других криптоактивов, являлась биржа Garantex. OFAC впервые ввело санкции против нее в апреле 2022 года за ОД в интересах российских рынков даркнета и групп программ-вымогателей. Великобритания и ЕС ввели санкции соответственно в 2023 и 2025 годах.

После начала полномасштабных боевых действий в Украине в феврале 2022 года и последующего расширения санкций Garantex приобрела все более существенное значение для перемещения средств российскими субъектами и олигархами в Россию и из России.

В ноябре 2023 года OFAC также ввело санкции против Екатерины Ждановой, связанной с TGR Group, за содействие операциям в USDT в интересах российских олигархов. По данным OFAC, Жданова помогла одному российскому олигарху переместить в ОАЭ более 100 млн долларов США активов и содействовала другим лицам в получении документов на проживание в ОАЭ; значительная часть платежей проводилась в USDT через Garantex.

Действия OFAC были скоординированы с операцией Destablise Национального агентства по борьбе с преступностью Великобритании (NCA), направленной на выявление и пресечение российских сетей ОД.

Исследование Elliptic показало, что после санкций апреля 2022 года Garantex стала применять более сложные методы сокрытия деятельности. Биржа внедрила технологии, позволяющие скрывать используемые криптоадреса и затруднять их атрибуцию средствами блокчейн-аналитики.

Первоначально эта стратегия была результативной: торговые объемы продолжали расти, и с апреля 2022 года по март 2025 года Garantex обработала транзакции более чем на 60 млрд долларов США. Подавляющая часть операций осуществлялась в USDT в сети TRON и включала не только российские субъекты, но и Lazarus Group КНДР.

Elliptic разработала собственные методы, позволившие выявить адреса, используемые Garantex для уклонения от обнаружения. Эти сведения помогли криптобиржам блокировать операции, связанные с Garantex, а правоохранительным органам - принять меры.

25 марта 2025 года DOJ США объявило о прекращении деятельности Garantex в рамках международной операции. В координации с Tether было заморожено 26 млн долларов США

связанных средств. Elliptic предоставила Секретной службе США данные и аналитическую информацию о деятельности Garantex в USDT.

По состоянию на конец июня 2025 года публикации со ссылкой на данные Elliptic указывали, что часть бывших пользователей Garantex, вероятно, перенесла операции на зарегистрированную в Кыргызстане биржу Grinex. Торговля на Grinex осуществлялась с использованием привязанного к российскому рублю стейблкоина A7A5, выпущенного в сетях Ethereum и TRON. Рублевые резервы, по данным отчета, хранились в Промсвязьбанке - российском финансовом учреждении, находящемся под санкциями США, Великобритании и ЕС.

Эмитент A7A5 связан с ООО «А7», в отношении которого Управление по осуществлению финансовых санкций Великобритании (OFSI) в мае 2025 года применило санкции за предоставление финансовых услуг российскому правительству.

Расследование Centre for Information Resilience (CIFR), цитируемое в отчете, указывает, что российские импортеры, стремящиеся обходить ограничения банковской системы, все чаще покупают A7A5 на Grinex, обменивают его на USDT, после чего используют USDT для приобретения товаров и услуг за рубежом. Такая модель позволяет хранить крупные объемы стоимости в A7A5 и переходить в USDT лишь для трансграничных расчетов.

По оценке авторов отчета, подобная структура может снижать риск замораживания по сравнению с хранением средств исключительно в USDT, поскольку Tether демонстрировала готовность замораживать USDT во взаимодействии с правоохранительными органами. Кроме того, расчеты в стейблкоинах могут снижать непосредственную вовлеченность банков третьих стран в торговые расчеты с Россией и тем самым уменьшать их прямую подверженность риску вторичных санкций.

Диаграмма: ежемесячный объем операций Garantex после введения санкций. После введения санкций Министерством финансов США объем криптовалютных транзакций через Garantex существенно вырос.

Ключевые меры контроля и рекомендации по расследованию

Для эмитентов стейблкоинов

- Использовать Ecosystem Monitoring для выявления частых или крупных операций санкционных субъектов с конкретным стейблкоином и на этой основе замораживать соответствующие кошельки.
- Проводить надлежащую проверку ПУВА и оценивать сервисы, создающие неприемлемый санкционный риск; при необходимости блокировать их адреса в экосистеме стейблкоина.

Для ПУВА

- Использовать скрининг кошельков и транзакций для выявления клиентов, имеющих прямую или косвенную связь с кошельками санкционных лиц и организаций.
- Настраивать блокчейн-скрининг так, чтобы он учитывал как прямую, так и косвенную подверженность санкционным лицам и юрисдикциям.

Для банков, хранящих резервы стейблкоинов

- До установления отношений с эмитентом использовать аналитические панели для оценки наличия неприемлемого санкционного риска в экосистеме токена.
- После установления отношений проводить периодический и событийный мониторинг возникающих рисков и запрашивать у эмитента подтверждение внедренных мер комплаенс.

Рекомендации по расследованию

- Строить графы потоков средств, связанных со стейблкоин-адресами из санкционных перечней США, Великобритании, ЕС и других юрисдикций, и выявлять ПУВА или иные сервисы, через которые осуществляется вывод средств.
- Анализировать IP-адреса и KYC-информацию лиц, получающих средства с адресов из санкционных перечней, на предмет иных признаков обхода санкций, включая входы из юрисдикций, часто используемых в подобных схемах, например ОАЭ, Турции и Гонконга.
- Если стейблкоины перемещаются через межсетевые мосты, использовать VVTE для визуализации chain-hopping и полного потока средств от источника до конечной точки.

Использование Ecosystem Monitoring для комплаенс и управления рисками стейблкоинов

В июле 2024 года Elliptic объявила о запуске Ecosystem Monitoring - решения, позволяющего эмитентам стейблкоинов в режиме реального времени отслеживать риски финансовых преступлений во всей экосистеме токена.

В основе решения находится система скрининга и предупреждений, которая уведомляет эмитента в момент, когда высокорисковый или включенный в санкционные перечни субъект пытается использовать стейблкоин. Это позволяет оперативно и проактивно замораживать или блокировать кошельки, снижать риск и обеспечивать соблюдение требований ПОД/ФТ и санкционных режимов.

С помощью Risk Engine подразделение комплаенс эмитента может настраивать правила риска, концентрируясь на наиболее существенных угрозах и одновременно сокращая количество ложноположительных срабатываний.

Помимо анализа на уровне кошелька и транзакции, Ecosystem Monitoring предоставляет агрегированную аналитику по рискам всего актива. Пользователи получают текущую и историческую картину законной и противоправной активности, могут фильтровать данные по видам финансовых преступлений и принимать меры в отношении возникающих рисков.

Комплексное представление о рисках может использоваться и для подтверждения регулирующим органам надежности стейблкоина или токена. В апреле 2025 года Elliptic объявила о партнерстве с Monerium - эмитентом EURe, привязанного к евро стейблкоина, разрешенного к использованию в ЕС и соответствующего требованиям Регламента ЕС о рынках криптоактивов (MiCA). На момент отчета объем операций с EURe превышал 4 млрд евро, что делало его одним из наиболее используемых в Европе стейблкоинов по объему транзакций.

Использование Ecosystem Monitoring позволяет Monerium демонстрировать европейским регулирующим органам способность управлять рисками, что создает условия для расширения поддержки блокчейнов и перечня услуг.

4. Все более широкая интеграция криптоактивов в схемы отмывания денег наркокартелей

Понимание риска

Незаконный оборот наркотиков занимает значимое место в истории развития криптоактивов и связанных с ними финансовых преступлений. Получивший широкую известность рынок даркнета Silk Road, запущенный в 2011 году, продемонстрировал, что криптоактивы способны поддерживать новый формат онлайн-торговли наркотиками: продавцы и покупатели могли напрямую взаимодействовать из любой точки мира, а расчеты осуществлялись в формате peer-to-peer с использованием криптоактивов.

Появление после Silk Road еще более крупных рынков даркнета показало, что проблема сохраняется, несмотря на успешные действия правоохранительных органов по ликвидации многих таких площадок.

Вместе с тем роль криптоактивов в деятельности крупных организованных наркокартелей, контролирующих уличную торговлю наркотиками и международные сети их производства и распределения, долгое время была иной. На ранних этапах развития криптоактивов картели в Колумбии и Мексике не использовали их широко. Хотя в 2018-2019 годах были выявлены отдельные попытки применять криптоактивы для трансграничного ОД, такие методы не являлись для картелей обычной практикой. Они продолжали в значительной степени полагаться на традиционные способы ОД, использовавшиеся десятилетиями.

За последние несколько лет ситуация существенно изменилась: криптоактивы стали регулярно использоваться в финансовой деятельности наркокартелей. Одной из причин является интеграция криптоактивов в инструментарий профессиональных организаций по ОД (PMLO), перемещающих средства в интересах картелей.

Доступность криптопродуктов и удобство сервисов позволяют PMLO отмывать значительные суммы без необходимости обладать высокой технической квалификацией. В Национальной оценке угрозы наркотиков США за 2024 год Управление по борьбе с наркотиками (DEA) отмечало, что криптоактивы могут быть «весьма выгодны для организаций, занимающихся наркотрафиком, поскольку позволяют перемещать стоимость через международные границы», а криптоактивы могут быстро перепродаваться за наличные или другие финансовые инструменты любому покупателю криптоактивов в мире.

Растущая доступность стейблкоинов также может способствовать их применению на различных этапах цепочек поставки и распространения наркотиков. Картели могут отдавать предпочтение стабильному средству платежа, способному сохранять стоимость преступных доходов, вместо более волатильных Bitcoin или Ethereum.

Эти тенденции совпали с резким ростом производства и распространения фентанила - чрезвычайно опасного наркотического средства, ставшего причиной масштабного кризиса зависимости, особенно в США. Правительство США усилило меры по пресечению цепочек поставки фентанила, включая принятие в 2024 году закона FEND Off Fentanyl Act. FinCEN уже использовала соответствующие полномочия для применения мер к мексиканским финансовым учреждениям, содействующим ОД доходов от фентанила.

Неудивительно, что участники незаконного оборота ищут альтернативные платежные механизмы, включая криптоактивы, позволяющие проводить расчеты вне традиционной банковской системы и снижать риск выявления.

Цепочка поставок фентанила начинается в Китае, где производится значительная часть химических прекурсоров. Производители взаимодействуют с китайскими брокерами, которые рекламируют химические вещества в интернете. За вознаграждение брокеры продвигают товары на английском

языке и организуют платежные механизмы для покупателей. Покупателями выступают участники крупных наркокартелей, производящих фентанил в Мексике. Расчеты осуществляются в Bitcoin, стейблкоинах и других криптоактивах.

Получив необходимые химические вещества, мексиканские картели производят фентанил и контрабандно перемещают его в США, где наркотики продаются за наличные. Перемещение крупных объемов наличных обратно в Мексику создает риск обнаружения и изъятия пограничными органами. Поэтому картели используют PMLO, которые конвертируют наличные в криптоактивы, прежде всего стейблкоины; впоследствии средства могут быть обменены на фиатную валюту и возвращены картелю после дополнительного ОД.

Правительство США все чаще применяет санкционные полномочия OFAC к цепочке поставок фентанила Китай-Мексика и связанной инфраструктуре ОД. В феврале 2025 года США признали картель Синалоа и Cártel de Jalisco Nueva Generación (CJNG), контролирующие значительную часть торговли фентанилом, иностранными террористическими организациями (FTO) наряду с другими преступными структурами Латинской Америки. ПУВА и финансовым учреждениям необходимо обеспечивать, чтобы их услуги не использовались для операций с такими запрещенными субъектами.

Схема цепочки поставки прекурсоров фентанила: Китай - Мексика - США, включая движение денежных средств для приобретения химических прекурсоров и последующее ОД доходов от продажи готового наркотика.

Пример типологии: наличные доходы от торговли наркотиками конвертируются в криптоактивы для трансграничного перевода

Одной из особенностей ОД, связанного с наркокартелями, является значительная роль наличных денежных средств. Поскольку реализация наркотиков генерирует крупные суммы наличных, преступникам необходимо преобразовать их в криптоактивы.

Один из способов - внесение наличных на банковский счет с последующим переводом средств ПУВА. Другие варианты включают внесение наличных непосредственно в криптомат (crypto ATM) либо использование P2P-брокеров, специализирующихся на обмене наличных на криптоактивы.

Этап «наличные - криптоактивы» представляет собой важную точку возможного выявления и пресечения схем. Банки, через которые проходят такие средства, могут обнаруживать индикаторы и предоставлять правоохранительным органам значимую информацию.

Как работает схема

81. Наркотики продаются за наличные в стране-потребителе, например в США, и у дилера образуется выручка в долларах США.
82. Дилер передает наличные денежным мулам, работающим на PMLO. Мулы вносят деньги на банковские счета, которые могут быть открыты на подставные компании. Затем средства используются для покупки криптоактивов, часто стейблкоинов, на ПУВА.
83. В некоторых случаях доллары сначала переводятся с банковских счетов мулов на счета в промежуточных финансовых учреждениях, например брокерских компаниях или банках офшорных юрисдикций, и уже оттуда используются для приобретения криптоактивов.
84. Криптоактивы переводятся со счетов мулов у ПУВА на некастодиальный кошелек участника сети PMLO в стране происхождения картеля, например в Мексике.
85. Участник PMLO в Мексике может переводить на счета мулов небольшие суммы в Ether, TRON или иных активах для компенсации комиссий («gas fees»).
86. Криптоактивы преступного происхождения направляются на счет у другого ПУВА, где PMLO обменивает их на местную фиатную валюту, например мексиканские песо.
87. Затем песо отмываются через банки Мексики или другой страны происхождения с применением традиционных методов ОД и передаются участникам наркокартеля.

Индикаторы

- На банковские счета физических или корпоративных клиентов, включая компании, заявляющие о работе в налично-интенсивных отраслях, часто вносятся необъяснимые крупные суммы наличными; вскоре после этого средства переводятся ПУВА или офшорным финансовым учреждениям.
- При прямых переводах ПУВА операции явно не соответствуют заявленной деятельности клиента. Например, транспортная компания не имеет очевидной законной причины регулярно приобретать криптоактивы на крупные суммы.
- Клиент ПУВА в стране-потребителе получает крупные банковские переводы в фиатной валюте, быстро приобретает криптоактивы и практически сразу направляет их на внешний некастодиальный кошелек - иногда в течение менее 24 часов.
- После серии быстрых операций баланс счета ПУВА может обнуляться, счет длительное время не используется, а затем внезапно вновь становится активным.
- На счет клиента могут поступать редкие небольшие входящие криптопереводы, соответствующие компенсации комиссий за транзакции.
- При входе в аккаунты используются IP-адреса из стран происхождения наркотиков, например Мексики или Колумбии.
- Пуловый кошелек PMLO может демонстрировать структурированные модели агрегации и распределения средств, соответствующие отдельным эпизодам получения наличных. Например, он получает три перевода эквивалентом 10 тыс., 20 тыс. и 30 тыс. долларов США от разных счетов мулов, а затем направляет те же суммы по отдельности далее, сохраняя учет доходов по каждому эпизоду.
- Адреса могут взаимодействовать с ПУВА в странах присутствия картелей, например Мексике или Колумбии, при этом такие ПУВА могут применять слабые меры ПОД/ФТ.
- Наблюдается связь с криптоматами и иными сервисами обмена наличных на криптоактивы.
- При открытии банковских счетов и счетов у ПУВА в стране-потребителе выявляются признаки денежных мулов: поддельные удостоверения личности, использование студентов для открытия счетов, противоречия в адресах проживания и иной идентификационной информации.

Пример типологии: брокеры по криптоактивам обеспечивают оплату прекурсоров фентанила

Первый критически важный этап цепочки поставки фентанила - приобретение картелями, в том числе находящимися в Мексике, химических прекурсоров, преимущественно производимых в Китае. Расчеты за такие химические вещества в значительной степени используют криптоактивы как способ передачи стоимости вне формальной финансовой системы.

Как работает схема

88. Производитель химических веществ в Китае привлекает брокера для рекламы продукции в интернете на английском языке.
89. Брокер продвигает и продает прекурсоры через англоязычные сайты, предлагая расчеты в USDT или Bitcoin.
90. Покупатель, например из Мексики, связывается с брокером и получает криптоадрес для оплаты.
91. Покупатель приобретает криптоактивы через ПУВА и переводит их на кошелек брокера; брокер организует поставку химических веществ из Китая в Мексику.
92. Брокер обменивает криптоактивы на фиатную валюту через ПУВА, переводит средства производителю в Китае и удерживает комиссию.

Индикаторы

- На счет клиента ПУВА поступают криптоактивы с ПУВА в странах, где могут находиться покупатели прекурсоров, например в Мексике, а затем фиатная валюта выводится на банковские счета в Китае или китайским платежным провайдерам. Это может свидетельствовать об использовании счета брокером.
- Кошельки брокеров имеют связь с адресами лиц и организаций, включенных OFAC в санкционные перечни за участие в незаконном обороте наркотиков.
- Поскольку такие брокеры могут одновременно оказывать услуги ОД в связи с другими преступлениями, их счета демонстрируют необычно высокую связь с кошельками, относимыми к мошенничеству.
- Клиент ПУВА приобретает криптоактивы и быстро направляет их на адрес, который блокчейн-аналитика связывает с поставщиком прекурсоров.
- Используемые ПУВА могут иметь слабые или отсутствующие меры ПОД/ФТ.
- Счет практически не используется для обычной торговли или иной законной деятельности; при запросе клиент не дает правдоподобного объяснения либо после операции счет становится неактивным.

Практический пример: Европол координирует действия по пресечению наркосетей, использующих криптоактивы

Европейские правоохранительные органы также уделяют повышенное внимание пресечению ОД с использованием криптоактивов в интересах наркотрафика.

В мае 2025 года Европол сообщил об аресте во Франции 16 лиц, связанных с картелем Синалоа, что продемонстрировало глобальный масштаб деятельности картеля. Задержанные участвовали в производстве и распространении кристаллического метамфетамина и входили в преступную сеть, действовавшую во Франции, Алжире, Бельгии, ОАЭ и Нидерландах. Сеть использовала логистическую поддержку и производственную экспертизу картеля Синалоа.

При задержании участников сети в Марселе французские органы изъяли более 30 тыс. евро в криптоактивах, применявшихся для трансграничных операций.

В рамках отдельной операции в декабре 2024 года Европол сообщил об аресте девяти наркоторговцев и изъятии 27 млн евро в криптоактивах в ходе действий, скоординированных правоохранительными органами шести стран. Расследование касалось сети торговли кокаином между Испанией и Дубаем и показало, что организаторы использовали участника албанской преступной сети для ОД крупных сумм в криптоактивах.

Европол отметил, что сотрудничество с крупным эмитентом стейблкоина и глобальным поставщиком услуг в сфере криптоактивов сыграло существенную роль в успехе операции.

Ключевые меры контроля и рекомендации по расследованию

Для банков

- Настраивать системы мониторинга транзакций на выявление схем «наличные - криптоактивы», например крупных внесений наличных с последующим быстрым переводом средств ПУВА.
- Обучать сотрудников банков типологиям ОД с обменом наличных на криптоактивы для обеспечения выявления и внутреннего сообщения о подозрениях.
- При направлении сообщений о подозрительной деятельности/операциях включать сведения о переводах клиентов ПУВА, поскольку это может позволить правоохранительным органам запросить дополнительную информацию у соответствующего ПУВА.
- Проводить надлежащую проверку ПУВА, получающих средства от банковских клиентов, и формировать риск-ориентированные политики взаимодействия с ПУВА.

Для ПУВА

- Использовать скрининг кошельков и транзакций для выявления клиентов, чья история операций содержит связь с адресами наркокартелей.
- Настраивать правила риска блокчейн-аналитики так, чтобы активность, связанная с торговлей фентанилом, получала соответствующий риск-рейтинг в соответствии с риск-аппетитом организации.
- Анализировать графы транзакций по предполагаемому ОД доходов от наркотрафика и использовать полученные сведения при подготовке сообщений о подозрительных операциях.
- Обучать сотрудников комплаенс типовым транзакционным индикаторам ОД, связанного с картелями.

Для следственных органов

- Строить связи между кошельками, предположительно участвующими в наркотрафике, и выявлять связанные транзакционные модели: переводы со счетов мулов на пуловые кошельки, компенсации gas-fees и иные признаки.
- Анализировать IP-адреса и данные входа в аккаунты ПУВА, чтобы выявить связь участников ОД с юрисдикциями наркотрафика, например Мексикой и Колумбией.
- Проверять корпоративные реестры и базы данных, чтобы установить наличие у компаний, участвующих в операциях, реальной законной цели.
- Обучать следователей видам химических прекурсоров, используемых при производстве фентанила, для выявления операций по их приобретению.
- Государственным следователям следует анализировать базы сообщений о подозрительных операциях с целью выявления банковских сообщений о наличных операциях, связанных с лицами и организациями, одновременно совершающими операции с криптоактивами.

5. Рост сложности межсетевого (cross-chain) отмывания денег

Понимание риска

Криптоактивы позволяют противоправным субъектам быстро перемещать стоимость между различными блокчейнами. Такие типологии ОД, известные как «chain-hopping» (переход между блокчейнами), используются для усложнения транзакционного следа и сокрытия преступного происхождения средств.

Децентрализованные биржи (DEX) позволяют пользователям обменивать активы DeFi без участия традиционного централизованного посредника. Межсетевые мосты обеспечивают перевод стоимости из одного блокчейна в другой. Эти технологические инновации создали более богатую и сложную блокчейн-экосистему, которую преступники используют для межсетевого ОД.

Исследования Elliptic показывают существенный рост масштабов такой деятельности. В первом отчете о cross-chain преступности, опубликованном в 2022 году, было установлено, что через межсетевые и межактивные сервисы, такие как DEX и мосты, было отмыто более 4 млрд долларов США в криптоактивах. В обновленном отчете 2025 года объем межсетевого ОД превысил 21 млрд долларов США. Это свидетельствует о том, что cross-chain операции стали устойчивым элементом противоправной деятельности в криптоэкосистеме.

Одновременно возросла сложность схем. По данным Elliptic, более 20 % всей деятельности по ОД с криптоактивами включает десять и более блокчейнов. Это показывает, насколько быстро преступники способны перемещать средства между различными сетями. Они используют все более широкий набор межсетевых мостов и комбинаций блокчейнов.

Современные кошельки, в том числе совместимые с Ethereum Virtual Machine (EVM), позволяют одному пользователю хранить тысячи активов в нескольких сетях. Поэтому для подразделений комплаенс и следователей важно иметь возможность анализировать одновременно множество активов и блокчейнов.

Преступники также автоматизируют отдельные этапы ОД. Скрипты позволяют за очень короткий период отправлять средства через десятки и сотни промежуточных кошельков, быстро формируя «цепочку дробления» (peeling chain) и затрудняя расследование. В сочетании с межсетевыми переводами это создает крайне сложный транзакционный след.

Такие методы часто сочетаются с традиционными средствами сокрытия происхождения активов: криптомиксерами, ПУВА, не соблюдающими требования либо сознательно содействующими преступникам, и сервисами обмена криптоактивов (coin-swap services), которые не требуют KYC и могут предоставлять доступ к анонимным криптоактивам (privacy coins).

Наиболее активным и инновационным пользователем межсетевого ОД, по оценке Elliptic, является Lazarus Group КНДР. Эта группа похищает и отмывает криптоактивы в крупных масштабах в условиях стремления КНДР обходить санкции и получать финансирование для программы оружия массового уничтожения (ОМУ). По данным Elliptic, деятельность КНДР составляет более 12 % всей противоправной cross-chain активности - свыше 2 млрд долларов США.

Межсетевое ОД используют не только киберпреступники. Доступность мостов и DEX делает соответствующие инструменты доступными мошенникам, наркоторговцам и, в редких, но значимых случаях, субъектам, связанным с материалами сексуального насилия над детьми (CSAM) и финансированием терроризма (ФТ).

Для выявления такой деятельности Elliptic развивает следующие возможности:

93. охват более 50 блокчейнов, позволяющий сохранять видимость противоправной активности при перемещении средств между сетями;
94. события передачи виртуальной стоимости (VVTE), обеспечивающие автоматическое связывание исходной и конечной транзакции при использовании межсетевого моста;

95. поведенческое выявление цепочек дробления, автоматизированного layering, первичного финансирования из миксеров (mixer-first funding) и других моделей, характерных для межсетевого ОД.

Пример типологии: ОД через межсетевые мосты и многократный переход между блокчейнами

Перевод средств между блокчейнами может иметь законную цель. Например, пользователь может перевести активы из сети Bitcoin в Ethereum для доступа к DeFi. Однако многократное перемещение средств туда и обратно между несколькими сетями в короткий период без понятной экономической причины требует повышенного внимания.

Каждый межсетевой перевод создает комиссионные расходы. Готовность пользователя неоднократно нести такие расходы при отсутствии деловой цели может являться индикатором риска.

Как работает схема

96. Противоправный субъект получает криптоактивы в результате киберхищения, мошенничества или другого преступления, например крупную сумму Bitcoin.
97. Средства направляются через многочисленные промежуточные адреса («hops»), образуя цепочку дробления. Большое число переходов за короткий период может указывать на автоматизированное layering. На этом этапе могут применяться миксеры.
98. После прохождения через многочисленные Bitcoin-кошельки средства переводятся через межсетевой мост в другую сеть, например Ethereum.
99. Далее преступник может несколько раз переводить средства между Bitcoin и Ethereum в обе стороны, стремясь дополнительно затруднить прослеживание.
100. Одновременно используются новые цепочки дробления, автоматизированное layering и миксеры, включая ранее санкционированный Tornado Cash.
101. После завершения процесса средства, как правило, выводятся через ПУВА повышенного риска и/или ПУВА, не соблюдающие установленные требования.

Индикаторы

- Средства неоднократно перемещаются между двумя блокчейнами в короткий период без понятной цели.
- Клиент ПУВА не может объяснить деловую или экономическую цель такой активности.
- Пользователь не проявляет обеспокоенности значительными комиссиями, возникающими в результате множества межсетевых операций.
- На счете одновременно присутствуют другие признаки риска: высокая подверженность адресам, связанным с преступной деятельностью, частое использование миксеров и т.п.
- Средства поступают на многочисленные счета у ПУВА, имеющие признаки сети денежных мулов: общие операции, схожие KYC-данные, одинаковые адреса либо документы, выглядящие измененными.

Пример типологии: переход в более популярный блокчейн для доступа к дополнительным услугам по ОД

В отдельных случаях преступники получают малоизвестные криптоактивы, которые не имеют широкого рынка. Например, при взломе биржи или DeFi-протокола преступник может получить токены с низкой капитализацией на сотни тысяч или миллионы долларов, причем токены обращаются в сравнительно небольшой сети.

Аналогичная ситуация возникает при мошенничестве с мемкоинами. Преступник может получить значительный объем токенов, имеющих стоимость, но ограниченную практическую ликвидность.

Попытка сразу реализовать крупную сумму малоизвестного токена через ПУВА является заметным индикатором. Поэтому преступники часто используют мост для перехода в более популярную сеть - одновременно скрывая происхождение средств и создавая возможность последующего вывода.

Как работает схема

102. Преступник получает значительный объем токенов в небольшой сети в результате взлома, мошеннической схемы «rug pull» или иного преступления.
103. Средства через межсетевой мост переводятся в крупный блокчейн, например Ethereum, Bitcoin или Solana.
104. Далее применяются дополнительные методы сокрытия: multi-chain hopping, структурированный chain-hopping, цепочки дробления, автоматизированное layering и миксеры - отдельно либо совместно.
105. В конечном итоге средства депонируются ПУВА и обмениваются на фиатную валюту.

Индикаторы

- Клиент ПУВА получает крупные депозиты в популярных активах, например Bitcoin или Ether, однако анализ показывает, что первоначальным источником являлся мемкоин или малоизвестный токен из небольшой сети.
- За короткое время значительный объем малоизвестного токена переводится в другой блокчейн и одновременно наблюдаются иные признаки ОД - цепочки дробления и множественные межсетевые переходы.
- Клиент не может подтвердить источник средств, использованных для получения мемкоина или нишевого токена.
- Клиент уклоняется от ответов, отказывается предоставлять сведения либо дает объяснения, не соответствующие разумной экономической цели.
- До получения крупного входящего платежа счет практически не использовался.
- Имеется транзакционная связь с кошельками, относимыми к мошенничеству, хищениям или иным преступлениям.
- После быстрого обмена на фиат счет может вновь стать неактивным.

Пример типологии: структурированный переход между блокчейнами (structured chain hopping)

В более сложной разновидности схемы преступники перемещают средства не между двумя сетями, а последовательно и параллельно через несколько блокчейнов. Elliptic называет такой процесс «structured chain hopping».

Как работает схема

106. Противоправный субъект получает преступные доходы в криптоактивах, например USDT, в результате киберпреступления или мошенничества.
107. Чтобы избежать замораживания USDT, на DEX он обменивает их на Ether.
108. Одновременно с цепочками дробления, автоматизированным layering и миксерами средства разделяются и переводятся через несколько межсетевых мостов - например из Ethereum в Bitcoin, Solana и Avalanche. Каждая операция сопровождается отдельной комиссией.
109. После перехода в другие сети продолжается использование цепочек дробления, автоматизированного layering и миксеров.
110. Затем средства могут быть возвращены в Ethereum и консолидированы, после чего на DEX вновь конвертированы в USDT.
111. USDT могут быть далее переведены через мост в еще одну сеть, например TRON.
112. В завершение USDT выводятся через ПУВА повышенного риска и/или ПУВА, не соблюдающий требования.

Дополнительные индикаторы

- За короткий период без понятной экономической причины средства проходят через межсетевые мосты и несколько блокчейнов.
- После многочисленных переходов средства вновь консолидируются в первоначальном или близком к первоначальному активе, что указывает на возможную цель - исключительно затруднить установление источника.
- Схема сочетается с признаками multi-chain hopping, цепочками дробления, миксерами и иными методами ОД.

Практический пример: взлом Bybit - КНДР совершает крупнейшее в истории хищение криптоактивов

В феврале 2025 года Lazarus Group совершила крупнейшее в истории хищение криптоактивов и, возможно, одно из крупнейших хищений любого вида, похитив около 1,46 млрд долларов США в криптоактивах с биржи Bybit, штаб-квартира которой находится в Дубае.

21 февраля Lazarus Group использовала вредоносное программное обеспечение, заразившее один из мультиподписных кошельков биржи. Bybit одобрила вывод средств, полагая, что запросы на перевод в кошельки злоумышленников являются законными.

В течение нескольких часов после хищения активов, включая токены в сети Ethereum, такие как stETH и cmETH, группа начала обменивать их на Ether через DEX. После конвертации в более ликвидный актив Ether был распределен по 50 отдельным кошелькам примерно по 10 000 ETH каждый.

В течение следующих двух недель преступники постепенно опустошали эти кошельки, используя несколько методов layering:

113. перевод через многочисленные промежуточные кошельки по модели chain-peeling перед отправкой в другие сервисы;
114. использование межсетевых мостов для вывода средств из Ethereum в другие сети, включая Bitcoin;
115. перевод части средств в миксеры и сервисы приватности, включая Tornado Cash, Cryptomixer и Wasabi Wallet.

КНДР также активно использовала централизованный сервис обмена монет. После взлома Bybit Lazarus Group направила более 200 млн долларов США похищенных средств в eXch - зарегистрированную в Белизе биржу без KYC, работавшую с 2014 года.

Анализ Elliptic показал, что eXch за годы работы получила криптоактивы на миллиарды долларов, связанные с мошенничеством, рынками даркнета и обходом санкций. В данном случае Lazarus Group после перемещения Ether через сотни промежуточных адресов направила его в eXch и обменяла на Bitcoin.

Bybit публично потребовала от eXch заморозить счета, использовавшиеся для обмена похищенных активов, однако сервис отказался. Elliptic добавила специальное правило риска, относившее кошельки, взаимодействующие с eXch, к высокорисковым, и предоставила пользователям поток данных по адресам, связанным со взломом Bybit, через CSV и API.

Эти сведения позволили ПУВА и эмитентам токенов в различных странах блокировать и замораживать средства, связанные с хищением.

Практический пример: британский мошенник использует структурированный chain-hopping для ОД

Дело из Великобритании показывает, что сложные межсетевые схемы используются не только высокопрофессиональными субъектами вроде Lazarus Group, но и все чаще встречаются при отмывании доходов от менее масштабных преступлений.

В мае 2025 года полиция West Mercia сообщила о первом в своем регионе обвинительном приговоре по делу о криптоактивах после сложного расследования, охватывавшего несколько блокчейнов.

Расследование продолжалось почти три года и касалось лица, похитившего у работодателя 150 тыс. фунтов стерлингов (около 200 тыс. долларов США). Работник предложил помочь работодателю инвестировать средства в криптоактивы. Получив фунты стерлингов, он присвоил их и приобрел более 90 различных криптоактивов.

Затем средства перемещались через несколько блокчейнов с использованием межсетевых мостов. Впоследствии криптоактивы использовались для азартных игр в интернете. Обвиняемый признал наличие зависимости от азартных игр. Суд назначил три условных срока лишения свободы продолжительностью от 8 до 24 месяцев.

Ключевые меры контроля и рекомендации по расследованию

Меры комплаенс

- Использовать комплексный (holistic) скрининг кошельков и транзакций для выявления признаков cross-chain поведения.
- Настраивать системы скрининга таким образом, чтобы операции с признаками цепочек дробления и автоматизированного layering получали соответствующий риск-рейтинг. Например, большое число переходов за короткий период может формировать высокий риск и приоритет для проверки.
- Использовать изображения и графы транзакций как подтверждающие материалы при подготовке сообщений о подозрительных операциях и взаимодействии с правоохранительными органами.
- Обучать сотрудников комплаенс пониманию сложных типологий межсетевого поведения.

Рекомендации по расследованию

- Использовать VVTE для выявления и построения схем перемещения средств между блокчейнами, формируя полную картину cross-chain потоков, одновременно визуализируя цепочки дробления, автоматизированное layering и mixer-first funding.
- Если средства поступили ПУВА, устанавливать конкретные адреса внутри кластера ПУВА, получившие средства.
- Анализировать KYC-записи ПУВА, получивших доходы от cross-chain ОД, чтобы идентифицировать владельцев счетов, участвовавших в конвертации в фиатную валюту.

VVTE - автоматизация отслеживания переводов через межсетевые мосты

Традиционно отслеживание межсетевых мостов требовало ручного установления источника и назначения каждого обмена. Если преступник дробит или структурирует перевод между несколькими мостовыми операциями, такой анализ становится трудоемким и длительным.

Elliptic реализовала события передачи виртуальной стоимости (VVTE), которые автоматически связывают конечную точку bridge-транзакции с ее источником без необходимости ручного сопоставления. Функциональность охватывает более 300 комбинаций мостов и существенно сокращает время расследования.

В приведенном в оригинальном отчете примере взлом происходит в Ethereum. Сразу после атаки преступник переводит активы через мост в Bitcoin, затем средства проходят через последовательные промежуточные кошельки и в конечном итоге поступают в миксер и сервис приватного кошелька. В

инструментах Elliptic вся схема может быть построена одним действием без ручного сопоставления идентификаторов транзакций, сумм и временных меток.

Поведенческое выявление: раскрытие сложных схем ОД

Ранее было показано, что поведенческое выявление помогает обнаруживать мошенничество на основе характерных моделей связанных кошельков. Аналогичные возможности имеют большое значение для выявления сложного ОД, часто сопровождающего cross-chain операции, в том числе используемые субъектами угрозы, связанными с КНДР.

Elliptic выделяет три характерные техники:

1. Цепочки дробления (peeling chains)

КНДР и другие противоправные субъекты регулярно направляют активы через десятки и сотни кошельков. Автоматическое выявление характерного потока позволяет специалистам комплаенс и следователям увидеть связанные транзакции. Механизм оценки риска может устанавливать пороги с учетом количества переходов, формируя риск-ориентированный мониторинг.

2. Автоматизированное layering

Признаком автоматизированного layering является прохождение средств через большое количество кошельков за чрезвычайно короткое время. Это указывает на использование автоматизированного сервиса или скрипта, который создает цепочку промежуточных адресов как «ложный след» и затрудняет установление исходного источника. Lazarus Group особенно часто применяет такой метод при ОД крупных сумм. Аналитические решения могут автоматически визуализировать эти цепочки.

3. Mixer-first funding

Это сценарий, при котором первая в истории транзакция криптоадреса поступает непосредственно из миксера. Миксеры могут использоваться и в законных целях для повышения конфиденциальности, однако их частое применение при перемещении крупных сумм также является индикатором повышенного риска и потенциального ОД, поскольку преступники используют такие сервисы для сокрытия происхождения активов.

Если кошелек, получивший средства после миксера, является новым и используется только как транзитный элемент, это может напоминать создание «проходного» банковского счета исключительно для приема средств преступного происхождения и их немедленного дальнейшего перевода. Например, КНДР после использования миксера может получить средства на новый кошелек и затем применить цепочки дробления, увеличивая дистанцию между адресом после миксера и конечным получателем.

Информация о mixer-first funding позволяет ПУВА оценивать риск входящих средств и при необходимости запрашивать у клиента дополнительные сведения о цели операции, источнике и конечном назначении средств, снижая риск непреднамеренного вовлечения в ОД.

Дополнительные материалы

Материалы Elliptic

- *State of Cross-Chain Crime 2025* - «Состояние межсетевой преступности 2025».
- *State of Crypto Scams 2025* - «Состояние мошенничества с криптоактивами 2025».
- *Typologies Report 2024* - «Отчет о типологиях 2024».
- *AI-Enabled Crime in the Cryptoasset Ecosystem* - «Преступность с использованием ИИ в экосистеме криптоактивов».
- *Sanctions Compliance in Cryptocurrencies 2024* - «Соблюдение санкционных требований в сфере криптовалют 2024».
- *Crypto and the Global Fentanyl Trade* - «Криптоактивы и глобальная торговля фентанилом».
- *Enhancing Blockchain Analytics through AI* - «Повышение эффективности блокчейн-аналитики с помощью ИИ».
- *AI-Enabled Crypto Crime: Best Practices for Virtual Asset Service Providers* - «Преступления с криптоактивами, совершаемые с применением ИИ: передовая практика для поставщиков услуг виртуальных активов».

Отчеты международных организаций и национальных органов

- *2025 National Drug Threat Assessment* (Управление США по борьбе с наркотиками, DEA) - «Национальная оценка угрозы наркотиков 2025».
- *2024 National Money Laundering Risk Assessment* (Министерство финансов США) - «Национальная оценка риска отмывания денег 2024».
- *Cryptoassets Threat Assessment July 2025* (Управление по осуществлению финансовых санкций Великобритании, HM Treasury) - «Оценка угроз, связанных с криптоактивами, июль 2025 года».
- *European Migrant Smuggling Centre Report 2024* (Европол) - «Отчет Европейского центра по противодействию незаконному ввозу мигрантов 2024».
- *Financial Flows from Human Trafficking* (ФАТФ) - «Финансовые потоки, связанные с торговлей людьми».
- *FinCEN Alert on Pig Butchering* - предупреждение FinCEN о схемах «pig butchering».
- *Illicit Finance Risk Assessment of Decentralized Finance* (Министерство финансов США) - «Оценка рисков незаконного финансирования в сфере децентрализованных финансов».
- *Money Laundering and Terrorist Financing Risks from Migrant Smuggling* (ФАТФ) - «Риски отмывания денег и финансирования терроризма, связанные с незаконным ввозом мигрантов».
- *National Risk Assessment of Money Laundering and Terrorist Financing 2025* (Home Office и HM Treasury Великобритании) - «Национальная оценка рисков отмывания денег и финансирования терроризма 2025».
- *Targeted Update on the Implementation of the FATF Standards for Virtual Assets and Virtual Asset Service Providers (VASPs)* (ФАТФ) - «Целевое обновление по имплементации Стандартов ФАТФ в отношении виртуальных активов и поставщиков услуг виртуальных активов (ПУВА)».

Глоссарий

ПОД/ФТ (AML/CFT) - противодействие легализации (отмыванию) преступных доходов и финансированию терроризма.

Автоматизированное layering - использование противоправными субъектами автоматизированных скриптов для быстрого перемещения средств через многочисленные промежуточные кошельки («переходы», hops) с целью усложнения транзакционного следа.

Приманочные транзакции (baiting transactions) - операции, при которых мошенники, особенно в схемах «pig butchering», возвращают жертве часть средств якобы в качестве инвестиционной прибыли, чтобы создать видимость законности и укрепить доверие.

Chain-hopping - перемещение средств между различными блокчейн-сетями.

Сервис обмена криптоактивов (coin swap service) - сервис обмена криптоактивов, который, как правило, не требует от пользователей предоставления KYC-информации; многие такие сервисы находятся в высокорисковых юрисдикциях и предоставляют возможность обмена на анонимные криптоактивы.

Межсетевой мост (cross-chain bridge) - механизм, позволяющий передавать стоимость и данные между различными блокчейнами.

CSAM - материалы, содержащие сексуальное насилие над детьми.

Децентрализованные финансы (DeFi) - предоставление финансовых услуг в блокчейне без традиционного посредника с использованием самоисполняемого программного кода - смарт-контрактов.

Децентрализованная биржа (DEX) - сервис DeFi, позволяющий пользователям обменивать криптоактивы посредством смарт-контрактов без участия централизованного брокера.

DOJ - Министерство юстиции Соединенных Штатов Америки.

Ecosystem Monitoring - использование блокчейн-аналитики, позволяющее эмитентам стейблкоинов и токенов отслеживать подверженность рискам как на уровне отдельных транзакций, так и в агрегированном виде по всей экосистеме актива.

FinCEN - Сеть по борьбе с финансовыми преступлениями Министерства финансов США (Financial Crimes Enforcement Network).

Генеративный ИИ - разновидность искусственного интеллекта, способная создавать новый контент, включая тексты, изображения, видео и аудио.

Комплексный скрининг (holistic screening) - возможность блокчейн-аналитики получать в рамках одного скрининга целостное представление о межсетевой подверженности риску по кошельку или транзакции, в том числе если средства перемещались через мосты и другие сервисы.

KYC (Know Your Customer, «Знай своего клиента») - меры по сбору и проверке информации о клиентах регулируемых организаций в рамках установления и поддержания деловых отношений.

Большие языковые модели (LLM) - программы на основе ИИ, способные понимать и генерировать текст, имитирующий человеческую речь.

Мемкоины (meme coins) - криптоактивы, связанные с интернет-мемом, трендом или иной популярной онлайн-тематикой.

Mixer-first funding - ситуация, когда первая транзакция, поступившая на криптоадрес, направлена непосредственно из миксера либо иного сервиса повышения анонимности.

Организованные преступные группы (ОПГ, OCGs) - группа лиц, согласованно планирующих, совершающих или обеспечивающих преступную деятельность; такие группы могут действовать на международном, национальном или местном уровне.

Цепочка дробления / chain peeling (peeling chain) - метод, при котором крупная сумма криптоактивов дробится на меньшие транзакции, каждая из которых направляется на новый, ранее не использовавшийся адрес. Метод применяется для увеличения дистанции между последующими операциями и первоначальным источником средств.

Профессиональные организации по отмыванию денег (PMLO) - организации или сети, оказывающие преступникам за вознаграждение услуги по легализации (отмыванию) преступных доходов.

Мошенническая схема rug pull - схема, при которой организаторы запускают новый криптоактив или проект, привлекают инвестиции, после чего выводят ликвидность или иным образом исчезают с активами, оставляя инвесторов с фактически обесценившимся токеном.

SAR (Suspicious Activity Report) - сообщение о подозрительной деятельности, направляемое подразделению финансовой разведки (ПФР). В отдельных юрисдикциях аналогичная отчетность именуется Suspicious Transaction Report (STR - сообщение о подозрительной операции/сделке) или Suspicious Matter Report (SMR).

Стейблкоины - криптоактивы, предназначенные для поддержания стабильной стоимости путем привязки к фиатной валюте, другим криптоактивам, корзине валют, товарам либо путем алгоритмического регулирования предложения.

Поставщик услуг виртуальных активов (ПУВА, VASP) - физическое или юридическое лицо, которое от имени или в интересах другого лица осуществляет, в частности, обмен, хранение и перевод виртуальных активов в значении, используемом Стандартами ФАТФ.

События передачи виртуальной стоимости (VVTE) - разработанная Elliptic технология, автоматически связывающая конечную точку транзакции через межсетевой мост с ее источником без необходимости ручного расследования каждого перехода.

Об Elliptic

Elliptic позиционирует себя как поставщика данных и аналитической информации для организаций, которым необходимы точность, аналитическая глубина и эффективность при принятии решений в сфере цифровых активов.

Основой компании является комплексная платформа сбора и анализа данных о криптоактивах, используемая для задач комплаенс, управления рисками, аналитической и разведывательной деятельности, обеспечения блокчейн-инфраструктуры и иных сценариев потребления данных.

Elliptic подчеркивает партнерский подход к развитию продуктов и доступу к данным. Платформа ориентирована на корпоративное применение, высокую доступность, масштабируемость и скорость обработки. Для расследований и скрининга она объединяет транзакционные следы между различными блокчейнами, сокращая время и затраты на анализ.

По данным компании:

- охватывается более **50 блокчейнов**;
- поддерживается более **250 межсетевых мостов**;
- размечено около **6,4 млрд адресов**;
- обрабатывается свыше **90 млн событий передачи стоимости в день**.

Elliptic признана Всемирным экономическим форумом (WEF) технологическим пионером. В числе инвесторов компании указываются J.P. Morgan, Wells Fargo Strategic Capital, SBI Group, Santander Innoventures и HSBC.

Компания основана в 2013 году, штаб-квартира находится в Лондоне; офисы расположены также в Нью-Йорке, Вашингтоне, Дубае, Сингапуре и Токио.

Источник оригинала: Elliptic, The Typologies Report 2025. Перевод подготовлен для ознакомительных и аналитических целей.