

КРИПТОМИР И ЦИФРОВЫЕ ФИНАНСЫ / CRYPTO-WORLD AND DIGITAL FINANCE

Редактор рубрики *З. И. Хисамова* / Rubric editor *Z. I. Khisamova*

Научная статья
УДК 343.9:336.7:004

<https://doi.org/10.21202/2782-2923.2023.4.822-836>

Э. А. Сидоренко¹

¹ *Московский государственный институт международных отношений Министерства внутренних дел России,
г. Москва, Россия*

Легализация преступных доходов с использованием *DeFi*: типовые схемы и индикаторы риска

Сидоренко Элина Леонидовна, доктор юридических наук, профессор, директор Центра цифровой экономики и финансовых инноваций, профессор кафедры уголовного права, уголовного процесса и криминалистики, Московский государственный институт международных отношений Министерства внутренних дел России
E-mail: 12011979@list.ru
ORCID: <http://orcid.org/0000-0002-4741-0184>
Researcher ID: <http://www.researcherid.com/rid/P-9046-2015>
eLIBRARY ID: SPIN-код: 3744-0382, AuthorID: 434856

Аннотация

Цель: повышение эффективности противодействия использованию типовых схем отмывания преступных доходов на основе выявления технологических и правовых уязвимостей инфраструктуры *DeFi*: децентрализованных бирж, блокчейн-мостов, децентрализованных кошельков и валют повышенной конфиденциальности.

Методы: общенаучные (анализ и синтез, метод индукции и дедукции, метод теоретического моделирования, юридическая интерпретация) и специальные методы научного познания (структурно-функциональный, конструктивный, ситуационный, инновационный, целевой, программно-целевой и риск-ориентированный).

Результаты: обозначены основные тренды развития легализации преступных доходов с использованием децентрализованных финансов; выявлена детерминационная значимость технологических характеристик *DeFi* в генезисе отмывания преступных доходов; определены основные типы легализации с использованием децентрализованных финансов; изучены схемы совершения преступлений и оценен криминогенный потенциал инфраструктуры *DeFi* (децентрализованных бирж, блокчейн-мостов, миксеров, токенов повышенной конфиденциальности и др.).

Научная новизна: предложено рассматривать легализацию преступных доходов с использованием *DeFi* как особую разновидность цифровых финансовых преступлений. В статье предложена авторская типология отмывания преступных доходов, обосновывается идея о невозможности применения к децентрализованным финансам матрицы традиционного финансового регулирования и стандартов *AML*. Аргументируется вывод о том, что предупреждение отмывания преступных доходов с использованием децентрализованных финансов должно осуществляться в тесной связке с выявлением индикаторов риска и разработкой эффективных мер контроля в точках входа преступных доходов на централизованные биржи.

© Сидоренко Э. Л., 2023

Практическая значимость: анализ типовых механизмов легализации преступных доходов с использованием *DeFi* позволяет системно подойти к организации ранней профилактики преступности и потенциально может стать основой для разработки рекомендаций для служб финансовой разведки и мониторинга.

Ключевые слова:

децентрализованные финансы, легализация, DeFi-сервисы, блокчейн, правовое регулирование, цифровые платформы, криптовалюта, токены, стейблкоины, миксеры, блокчейн-мосты, токены повышенной конфиденциальности

Статья находится в открытом доступе в соответствии с Creative Commons Attribution Non-Commercial License (<https://creativecommons.org/licenses/by-nc/4.0/>), предусматривающем некоммерческое использование, распространение и воспроизводство на любом носителе при условии упоминания оригинала статьи.

Как цитировать статью: Сидоренко, Э. Л. (2023). Легализация преступных доходов с использованием *DeFi*: типовые схемы и индикаторы риска. *Russian Journal of Economics and Law*, 17(4), 822–836. <https://doi.org/10.21202/2782-2923.2023.4.822-836>

Scientific article

E. L. Sidorenko¹

¹ *Moscow State Institute of International Relations of the Russian Ministry of Foreign Affairs, Moscow, Russia*

Legalization of criminal income using DeFi: typical schemes and risk indicators

Elina L. Sidorenko, Doctor of Law, Professor, Director of the Center for digital economy and financial innovations, Professor of the Department of Criminal Law, Criminal Procedure and Criminology, MGIMO University

E-mail: 12011979@list.ru

ORCID: <http://orcid.org/0000-0002-4741-0184>

Researcher ID: <http://www.researcherid.com/rid/P-9046-2015>

eLIBRARY ID: SPIN-код: 3744-0382, AuthorID: 434856

Abstract

Objective: to increase the effectiveness of countering the use of typical criminal money laundering schemes by identifying the technological and legal vulnerabilities of the DeFi infrastructure: decentralized exchanges, blockchain bridges, decentralized wallets, and privacy-enhanced currencies.

Methods: general scientific (analysis and synthesis, induction and deduction, theoretical modeling, legal interpretation) and special methods of scientific cognition (structural-functional, constructive, situational, innovative, target-oriented, program-target, and risk-oriented).

Results: the main trends in the development of money laundering using decentralized finance were outlined; the determinative significance of DeFi technological characteristics in the genesis of money laundering was revealed; the main types of money laundering using decentralized finance were identified; the schemes of committing crimes were studied and the criminogenic potential of DeFi infrastructure (decentralized exchanges, blockchain bridges, mixers, privacy-enhanced tokens, etc.) was assessed.

Scientific novelty: it is proposed to consider money laundering using DeFi as a special type of digital financial crime. The article proposes the author's typology of money laundering, substantiates the idea that the matrix of traditional financial regulation and AML standards cannot be applied to decentralized finance. It is argued that prevention of money laundering using decentralized finance should be carried out in close connection with the identification of risk indicators and the development of effective control measures at the points of entry of criminal incomes to centralized exchanges.

Practical significance: the analysis of typical mechanisms of money laundering using DeFi allows a systematic approach to the organization of early crime prevention and can potentially become the basis to develop recommendations for financial intelligence and monitoring services.

Keywords:

decentralized finance, legalization, DeFi services, blockchain, legal regulation, digital platforms, cryptocurrency, tokens, stablecoins, mixers, blockchain bridges, privacy-enhanced tokens

The article is in Open Access in compliance with Creative Commons Attribution Non-Commercial License (<https://creativecommons.org/licenses/by-nc/4.0/>), stipulating non-commercial use, distribution and reproduction on any media, on condition of mentioning the article original.

For citation: Sidorenko, E. L. (2023). Legalization of criminal income using *DeFi*: typical schemes and risk indicators. *Russian Journal of Economics and Law*, 17(4), 822–836. (In Russ.). <https://doi.org/10.21202/2782-2923.2023.4.822-836>

Введение

Децентрализованные финансы (далее – *DeFi*) представляют собой не только новый этап в развитии технологии распределенного реестра (блокчейна), но и заметную угрозу для мировой финансовой системы ввиду их частого использования в легализации преступных доходов и финансировании терроризма.

Принципиальное отличие децентрализованных финансов от традиционных (централизованных) заключается в том, что отношения между сторонами строятся в формате одноранговых транзакций *P2P* (*peer-to-peer*) на основе протокола смарт-контракта и не предполагают обращение к банкам и другим официальным финансовым институтам.

Элементами экосистемы децентрализованных финансов являются: стейблкоины (блокчейн-активы), децентрализованные криптокошельки, межсетевые мосты – технологии, обеспечивающие передачу информации от одной сети блокчейна к другой; платформы взаимного кредитования, децентрализованные криптобиржи – цифровые площадки купли-продажи криптовалюты при помощи протоколов смарт-контрактов, сервисы страхования, сервисы управления, агрегаторы; платформы ликвидного скейтинга и оракулы (Сидоренко, 2023а).

Использование типовых протоколов смарт-контрактов позволяет обеспечить слаженность действий всех участников *DeFi*-инструментов, привлечь ликвидность в децентрализованные проекты и обеспечить безопасность и финансовую независимость участников децентрализованных сервисов. С одной стороны, экосистема *DeFi* предполагает свободу и независимость ее участников, но с другой – отсутствие внешнего контролера повышает риски взлома, фишинга и кражи активов (Сидоренко, 2023б).

Основными мишенями для преступников становятся децентрализованные криптокошельки и блокчейн-мосты. Высоким криминогенным потенциалом обладают и алгоритмы управления децентрализованными сервисами. В децентрализованных системах они позволяют в автоматическом режиме принимать решения о направлении средств, вносить изменения в структуру проекта и иным образом влиять на его функциональность и прибыльность, но при этом сама технология не исключает возможность злоупотреблений при сосредоточении власти у одного лица (Schuppli & Jafari, 2021).

Однако самым главным риском для экономики *DeFi* является нормативная неопределенность децентрализованных финансов (Carter & Jeng, 2021; Harvey, 2021). Ни на международном, ни на национальном уровнях не выработаны единые подходы к определению их правовой природы (Momtaz, 2022). Как следствие, пользователи децентрализованных финансовых услуг не могут юридически закрепить свои права на цифровые активы, верифицировать действия и восстановить права в случае хищения криптоактивов.

Именно пробелы в правовом регулировании *DeFi* приводят к тому, что данная технология все чаще используется преступниками для легализации преступных доходов. Как правило, платформы *DeFi* имеют слабую политику по борьбе с отмыванием денег (*AML*) и не всегда применяют процедуру идентификации *KYC* («знай своего клиента»), что затрудняет, а в ряде случаев и вовсе исключает отслеживание и прекращение незаконной деятельности.

Проблема усугубляется еще и тем, что правоохранительные органы не понимают природу децентрализованных финансов и потому не могут выстроить матрицу уголовно-правовых рисков их использования

и определить перечень тех операций, которые должны подлежать обязательному финансовому контролю в рамках риск-ориентированного подхода (Maia & Vieira dos Santos, 2021).

Именно риск-ориентированный подход был выбран Группой разработки финансовых мер борьбы с отмыванием денег (далее – ФАТФ) в качестве основной методики оценки криминальной уязвимости криптоактивов. В 2014 г. был опубликован отчет ФАТФ «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ», а в 2015 г. – Руководство по применению риск-ориентированного подхода: провайдеры услуг по обмену конвертируемой виртуальной валюты (ФАТФ, 2015).

В 2019 г. ФАТФ уточнила отдельные требования к финансовой деятельности, связанной с виртуальными активами. В частности, были предусмотрены следующие требования для провайдеров услуг виртуальных активов (ПУВА): регулирование деятельности в рамках ПОД/ФТ, лицензирование и регистрация компаний, а также разработка эффективных систем контроля и надзора (FATF, 2019).

Однако, как показала практика, этих мер оказалось недостаточно для минимизации уголовно-правовых рисков децентрализованных финансов. В отличие от криптовалюты и других централизованных цифровых финансов (*CeFi*) *DeFi* не связаны с внешними финансовыми институтами и устанавливаемыми ими правилами. Взаимодействие в рамках автоматизированных протоколов в формате *P2P* воспринимается как реализация частной воли участников и фактически исключает легальное давление на них со стороны публичных институтов. А это означает, что существующие модели правового регулирования крипторынка применительно к *DeFi* должны быть пересмотрены и уточнены.

Современное антиотмывочное законодательство целесообразно ориентировать на создание системы оперативного выявления фактов неправомерного использования децентрализованных технологий и отслеживания вывода средств в фиатную валюту или на централизованные криптовалютные площадки. Важным условием успеха такой деятельности является то, что, несмотря на стремительное развитие *DeFi*, общая капитализация этого рынка пока еще незначительна, а инфраструктура не готова обеспечивать безопасность полного цикла оборота активов. На практике это означает, что преступники не могут долго оставаться в сфере децентрализованных финансов и вынуждены выходить в сферу оборота фиатной валюты, используя централизованные криптовалютные биржи и обменники, где и попадают в зону финансового контроля при необходимой слаженности действий финансовой разведки и знания ключевых индикаторов отмывания преступных доходов в сфере *DeFi*.

Для того чтобы правоохранительная деятельность носила эффективный характер, важно знать основные схемы легализации преступных доходов с использованием децентрализованных финансов и выявлять признаки-индикаторы противоправной финансовой деятельности.

В рамках представленного ниже анализа практики легализации преступных доходов с использованием децентрализованных финансов предложена типология механизмов отмывания доходов и обозначены основные индикаторы рисков легализации. В основу анализа вошли данные, полученные в рамках мониторинга оборота цифровых активов с использованием децентрализованных финансов, проведенных крупнейшими экспертными центрами, а также отечественными и зарубежными исследователями.

Результаты исследования

Легализация преступных доходов с использованием децентрализованных финансов: типовые схемы

На динамику роста *DeFi*-преступности указывают следующие цифры: в 2017 г. было задокументировано 16 таких преступлений, в 2021 г. – 308, а в 2022 г. – 435 посягательств. В половине преступлений убыток превысил 356 000 долл., при этом самый маленький ущерб составил всего 158 долл., а самый крупный – 3,6 млрд долл.¹

Аналитическая компания *Elliptic*, используя материалы Европола, в докладе за август 2022 г. расписала многочисленные преступные схемы в криптосфере². Эксперты описали три основных канала отмывания преступных доходов в *DeFi*-секторе:

¹ <https://www.csh.ac.at/criminal-activities-in-the-crypto-sector/>

² *Elliptic*. (2022). Preventing Financial Crime in Cryptoassets. <https://www.elliptic.co/hubfs/Typologies-2022-Preventing%20Financial%20Crime%20in%20Crypto-NH.pdf?hsCtaTracking=459bfdd0-05d4-4c16-ade1-d73d88236fe8%7Ce1df3ed3-2a59-40bc-990d-a11d6a803e24>

- децентрализованные биржи (*DEX*);
- децентрализованные миксеры;
- блокчейн-мосты.

На практике преступники используют несколько адресов и намеренно осуществляют переход из децентрализованных сервисов в централизованные и наоборот. Эта деятельность представляет собой «расслоение» – искусственное усложнение транзакций с целью воспрепятствования отслеживанию средств. В большинстве случаев расслоение сопровождается дроблением суммы на мелкие платежи, не подпадающие под финансовый контроль. Гипотетически движение средств можно отследить через *DApps* благодаря прозрачности блокчейна, однако на практике правоохранители, не понимая сам механизм отмывания, не могут контролировать движения средств и переходы в различные *DeFi*-протоколы³.

Существующие механизмы легализации преступных доходов с использованием *DeFi* можно условно разделить на следующие типы:

- 1) отмывание преступных доходов с использованием децентрализованных бирж (*DEX*);
- 2) легализация с помощью криптовалютных миксеров;
- 3) отмывание с использованием блокчейн-мостов;
- 4) легализация преступных доходов с использованием токенов повышенной конфиденциальности;
- 5) отмывание с использованием проектов предложения монет (*ICO*);
- 6) легализация преступных доходов с использованием децентрализованных финансов и игорных криптосервисов.

Легализация преступных доходов с использованием децентрализованных бирж

Децентрализованные биржи (*DEX*) представляют собой приложения для одноранговой (*P2P*) торговли криптоактивами, в которых движение финансов осуществляется при помощи смарт-контрактов.

В настоящее время существует около 600 децентрализованных криптовалютных бирж, совокупный суточный объем которых составляет 1,9 млрд долл. США. Но при этом на общем криптовалютном рынке их объем не превышает 5 %. В тройку крупнейших децентрализованных бирж по объему торгов входят: *Uniswap V3* (*Ethereum*), *Uniswap V3* (*Arbitrum One*) и *Pancakeswap V3* (*BSC*)⁴.

В отличие от централизованных бирж (*CEX*), где работа организована по принципу традиционных фондовых рынков с соответствующей нормативной основой, децентрализованные биржи находятся вне рамок эффективного финансового контроля. В *CEX* предусмотрена обязанность должностных лиц контролировать транзакции, идентифицировать пользователей (*KYC*) и в случае необходимости блокировать операцию или конкретного пользователя. Децентрализованные же биржи не являются контролерами транзакций, не участвуют в сделках, не ведут счета пользователей и не проводят их идентификацию. Клиент идентифицируется при помощи адреса криптовалютного кошелька и специального блокчейн-адреса, и его персональная информация недоступна финансовой разведке.

По мнению экспертов, к техническим преимуществам *DEX* относятся анонимность пользователя, автоматизация процессов с использованием протокола смарт-контракта, невозможность заморозить средства и возможность мгновенно производить листинг (допуск на биржу) цифровых активов при наличии ликвидности (Allen, 2022).

Но на практике эти преимущества нередко оборачиваются недостатками *DEX*. В частности, пользователь не может оспорить сделку через техническую возможность и вернуть ошибочно направленные средства, не может дифференцировать заявки и установить лимиты по сделкам. Кроме того, технические уязвимости протокола повышают риски хакерских атак и хищения денежных средств, а отсутствие централизованной системы листинга увеличивает риски мошенничества при обмене активов на «пустые» токены (ЦСР, 2022).

³ Elliptic. (2022). DeFi. Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/hubfs/downloads/The%20Elliptic%202022%20DeFi%20Report.pdf?utm_campaign=Regulation%207C%20FATF%207C%20Oct%202021&utm_medium=email&_hsmi=184080622&utm_content=184080622&utm_source=hs_automation

⁴ Лучшие децентрализованные биржи по объему торгов за 24 часа. CoinGecko. <https://www.coingecko.com/ru/%D0%BE%D0%B1%D0%BC%D0%B5%D0%BD/decentralized>

Чаще всего децентрализованные биржи используются для отмыwania криптоактивов, полученных в результате незаконного оборота наркотических средств и психотропных веществ (Иванцов и др., 2019). Преступники прибегают к обмену активов, добытых преступным путем, на «нативные» монеты, т. е. на криптовалюту, работающую внутри определенной платформы или сети (например, нативной монетой сети *Ethereum* является *Ethereum*, а сети *Bitcoin* – *Bitcoin*). Затем он направляет средства в *DEX*. Большинство децентрализованных бирж не ограничивают круг клиентов, не ведут их учет и не проверяют депозиты. До того как эмитент токенов узнает о преступной транзакции и заблокирует внешний аккаунт преступника, последний, как правило, успевает конвертировать активы в нативные монеты и перевести их на анонимный кошелек⁵.

Для легализации доходов, полученных от оборота наркотических средств, используется, как правило, несколько схем.

Схема «P2P – транзакции и децентрализованные биржи»:

- 1) продавец наркотиков получает фиатную или виртуальную валюту от покупателя и переводит эти деньги посреднику – физическому лицу в стране конечного потребителя;
- 2) посредник переводит эти средства на *P2P*-счет, созданный на площадке децентрализованной биржи;
- 3) криптоактивы направляются на *P2P*-счет получателя в стране происхождения наркотиков;
- 4) получатель конвертирует эти активы в нативную валюту децентрализованной биржи, а затем обналичивает и переводит деньги на банковский счет;
- 5) получатель переводит фиатную валюту на многочисленные банковские счета, расположенные в стране происхождения наркотиков. Местные банки видят только движение фиатной валюты, но не могут установить происхождение средств и их связь с криптоактивами.

На описанную схему могут указывать:

- а) большие обороты криптоактивов, обналичиваемых на биржах из кошельков, связанных с платформой *P2P*, и последующий перевод денег на банковские счета. Как правило, легальная предпринимательская деятельность не предполагает таких сложных транзакционных схем;
- б) лицо, часто отправляющее криптоактивы на кошельки *P2P*-бирж, делает это систематически вне связи с колебаниями курсов криптовалют;
- с) на кошелек посредника поступают средства от большого, но стабильного круга лиц;
- д) посредник может иметь профиль в социальных сетях с предложением соответствующей услуги, а также размещать информацию на профильных сайтах криптообмена (например, *Bitcointalk.org*, *Bitcoin-otc.com*, *Cryptocompare.com* и др.) либо на ресурсах Даркнета.
- е) криптоактивы могут поступать на адреса посредника из таких источников, как Даркнет или микшеры, затем они быстро переводятся на биржи, откуда быстро обналичиваются на банковские счета нескольких лиц.

Схема «Децентрализованная биржа – централизованная биржа»:

- 1) лицо получает криптоактивы, добытые преступным путем, и переводит их на кошелек децентрализованной биржи;
- 2) токены конвертируются в новые токены (как правило, валюту площадки – нативную валюту) и переводятся на другой кошелек;
- 3) новые токены переводятся на один или несколько счетов подставных лиц (дропов) на централизованной бирже и обналичиваются;
- 4) деньги поступают на банковские счета с легальных криптовалютных кошельков.

На эту схему могут указывать следующие признаки:

- а) клиент централизованной биржи получает большое количество криптоактивов с анонимных счетов *DEX* и пытается немедленно обналичить их;
- б) он не может представить доказательств легитимности транзакции, а равно объяснить причины активного взаимодействия с децентрализованными биржами;
- с) взаимодействие осуществляется с *DEX*, которая уже была замечена в сомнительных транзакциях, а на ее кошельки поступали средства с микшеров и Даркнета.

⁵ Elliptic. (2022). DeFi. Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/hubfs/downloads/The%20Elliptic%202022%20DeFi%20Report.pdf?utm_campaign=Regulation%20%7C%20FATF%20%7C%20Oct%202021&utm_medium=email&hsmt=184080622&utm_content=184080622&utm_source=hs_automation

Легализация преступных доходов с использованием криптовалютных миксеров

Миксер криптовалют представляет собой сервис анонимизации активов в системах распределенного реестра. В основу работы миксеров положен следующий алгоритм: поступившие в него средства дробятся на мелкие части, а затем смешиваются с активами других клиентов. В результате пользователь получает номинальное количество криптовалюты с другими цифровыми кодами небольшими транзакциями с нескольких адресов. Таким образом разрывается цепочка цифровых кодов и затрудняется установление криминального происхождения активов.

По данным экспертов *Chainalysis*, в 2022 г. количество криптовалют в миксерах достигло рекордно высокого уровня. 19 апреля 2022 г. 30-дневная скользящая средняя, полученная миксерами, достигла исторического максимума в криптовалюте на сумму 51,8 млн долл., что вдвое превышает показатели 2022 г.⁶ В целом в 2022 г. криптоадреса, связанные с незаконной деятельностью, перевели почти 10 % своих средств на миксеры, при этом ни один другой тип адреса не отправлял более 0,3 % от общего объема. На легализацию преступных доходов с использованием миксеров указывает и тот факт, что за 2021–2022 гг. в два раза увеличился объем переводов на незаконные адреса децентрализованных сервисов: с 12 % в 2021 г. до 23 % в 2022 г.⁷

Легализация преступных доходов с использованием миксеров характерна, как правило, для лиц, занимающихся мошенничеством и кражей криптоактивов. По данным *Chainalysis*, основную долю незаконных счетов, на которые миксеры направляют средства, составляют площадки даркнет-рынка *Hydra*, *Lazarus Group* и *Blender.io*. Первая площадка представляет собой русскоязычный теневой рынок, а два других рынка связаны с Северной Кореей⁸.

Широкая востребованность миксеров объясняется не только заметным ростом легализации преступных доходов, но и санкционной политикой западных стран в отношении России и Северной Кореи. В частности, невозможность прямой работы с криптовалютными биржами из-за ограничений привела к тому, что к миксерам стали обращаться законопослушные владельцы виртуальных активов исключительно с целью сокрытия страны происхождения криптовалюты⁹. Это привело к смешению потоков поступающих средств и затруднило отслеживание отмываемых денег.

Механизм легализации преступных доходов с использованием криптовалютного миксера выглядит следующим образом:

- 1) пользователь отправляет цифровую валюту на адрес кошелька микшера. Это инициирует процесс смешивания;
- 2) миксер собирает средства от нескольких пользователей в один пул или счет. Такое объединение осуществляется для создания большего пула средств, что затрудняет отслеживание отдельных транзакций;
- 3) как только достаточное количество пользователей внесло свой вклад в пул, миксер начинает смешивать средства. Он делает это, отправляя криптовалюту из пула на различные адреса, разрывая связь между первоначальным отправителем и получателем;
- 4) после завершения процесса микширования пользователи могут вывести свою криптовалюту из микшера. Средства, которые они получают, представляют собой набор различных цифровых кодов, что затрудняет установление происхождения каких-либо конкретных монет;
- 5) миксеры взимают комиссию за свои услуги. Как правило, она составляет 1–3 %¹⁰.

В отличие от централизованных миксеров, где средства находятся под контролем операторов, децентрализованные сервисы предоставляют конфиденциальные услуги и не ведут записи об операциях (Allen, 2023).

⁶ Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cybercriminals Contributing Significant Volume. (2022, July 14). *Chainalysis*. <https://www.chainalysis.com/blog/crypto-mixer-criminal-volume-2022/>

⁷ Там же.

⁸ Nichols, Sh. (2022, 6 May). Cryptocurrency mixer sanctioned over Lazarus Group ties. *TechTarget*. <https://www.techtarget.com/searchsecurity/news/252516845/Cryptocurrency-mixer-sanctioned-over-Lazarus-Group-ties>

⁹ Спрос на криптовалютные миксеры вырос из-за увеличения преступной деятельности. (2022, 15 июля). *SecurityLab.ru*. <https://www.securitylab.ru/news/532807.php>

¹⁰ Singh, O. (2022, March 27). What is a cryptocurrency mixer and how does it work? *Cointelegraph*. <https://cointelegraph.com/explained/what-is-a-cryptocurrency-mixer-and-how-does-it-work>

Ведущим децентрализованным *DApp*-миксером до его блокировок и санкций в США был русскоязычный *Tornado Cash*¹¹. До 8 августа 2022 г. (дата блокировки США) через него проходило 75 % всех средств, направленных на сервисы миксеров за последние три года в сети *Ethereum* (более \$3,5 млрд) с целью дальнейшей легализации на биржах. После наложения санкций многие биржи заблокировали аккаунты своих пользователей, связанных с отправкой средств через этот миксер, однако позднее часть средств была разблокирована при подтверждении пользователями легальности происхождения криптовалюты.

На втором месте по объему денежных средств находится *Blender.io*. С 2017 г. через него прошли криптоактивы на сумму более 500 млн долл. США. Этот сервис в мае 2022 г. тоже попал в санкционный список за отмывание средств, полученных в результате совершения хакерских атак группировки *Lazarus Group*¹².

Практика блокировки миксеров показала, что преступники не сократили объемы переводимых на них средств, а заметно усложнили механизмы.

Ранее ими использовалась следующая схема «Криптовалюта – миксер»:

- 1) преступник отправляет средства, добытые преступным путем, на адрес криптовалютного кошелька;
- 2) получает новые «чистые» криптоактивы из миксера;
- 3) эти активы переводятся на централизованную биржу и конвертируются в фиатную валюту.

На легализацию преступных доходов с использованием *DeFi*-миксеров могут указывать следующие индикаторы:

- а) клиент централизованной биржи получает частые входящие переводы от *DeFi*-миксера, не желает или не может предоставить информацию о первичном источнике средств;
- б) пользователь совершает частые переводы с участием *DeFi*-миксеров без разумного объяснения этой деятельности;
- в) клиент, чья деятельность связана с частым взаимодействием с *DEX*, также участвует в транзакциях с услугами *DeFi*-миксеров.

Наложение санкций и блокировка криптовалютных счетов заметно усложнили эту схему, включив в нее децентрализованные сервисы.

Легализацию «Миксеры – *DeFi*-сервисы» можно представить в виде следующей схемы:

- 1) преступник получает незаконно добытые криптоактивы и переводит средства через несколько кошельков, используя разную криптовалюту и разные *DEX*-кошельки;
- 2) он аккумулирует эти средства в миксере;
- 3) получив новые, «чистые» криптоактивы из миксера, преступник отправляет средства в централизованный обменный сервис для конвертации их в фиатную валюту. При этом средства могут быть отправлены через несколько кошельков-посредников до поступления на биржу.

На описанную схему могут указывать следующие индикаторы:

- а) клиент централизованной биржи получает много средств с различных децентрализованных кошельков и не может доказать легальность происхождения средств;
- б) учетная запись клиента показывает системные переводы на миксеры и с миксеров. Как правило, речь идет о небольших суммах, поступающих с различных адресов за небольшой отрезок времени. При этом клиент не может объяснить происхождение средств.

Более сложной является следующая схема легализации преступных доходов «Миксер – *NFT*»:

- 1) преступник использует миксер для отмывания криптоактивов, полученных преступным путем;
- 2) он переводит «новые» монеты на *NFT*-маркетплейс и покупает на них *NFT* (невзаимозаменяемый токен, используемый, как правило, для создания цифрового слепка уникального предмета);
- 3) получив *NFT*, он перепродает его. Продажа *NFT* в отдельных юрисдикциях признается легальным источником получения средств.

На эту схему могут указывать следующие признаки:

- а) наблюдается рост доходов лица от продажи *NFT*, но он не может указать источник средств на их покупку;

¹¹ Elliptic. (2022). DeFi. Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/hubfs/downloads/The%20Elliptic%202022%20DeFi%20Report.pdf?utm_campaign=Regulation%207C%20FATF%207C%20Oct%202021&utm_medium=email&_hsmi=184080622&utm_content=184080622&utm_source=hs_automation

¹² U. S. Department of the treasury. (2022, 14 April). North Korea Designation Update. <https://ofac.treasury.gov/recent-actions/20220414>

b) замечен след работы лица с криптомиксерами: он прибегает к ним перед покупкой *NFT*.

Такая схема напоминает классическую легализацию преступных доходов с использованием предметов искусства и антиквариата за тем преимуществом, что предметом оборота являются исключительно цифровые объекты, а отсутствие единых международных критериев их регулирования позволяет преступнику выбрать наиболее слабую юрисдикцию (Clements, 2021).

Легализация преступных доходов с использованием блокчейн-мостов

Все активы, которые работают в том или ином блокчейне, могут использоваться в *DeFi*-протоколах: их можно обменять друг на друга или применить в качестве залога для заимствования другого актива с использованием протокола кредитования. Но проблема заключается в том, что большинство блокчейнов несовместимы друг с другом ввиду несовпадения правил администрирования и механизмов консенсуса, а это, в свою очередь, исключает перемещение активов между площадками. Данную проблему решают блокчейн-мосты.

Блокчейн-мосты (*Blockchain Bridge*, *Cross-chain Bridge*, или сетевые мосты) представляют собой приложения, с помощью которых активы перемещаются с одной блокчейн-площадки на другую.

Для этого, как правило, используется один из трех сценариев транзакций: *lock-and-mint*, *burn-and-release* и *burn-and-mint*.

Lock-and-Mint предполагает, что перечисляемые средства блокируются на одном блокчейне и выпускаются на другом при обязательном наличии посредника, который создает и блокирует токены. Как показывает практика, это наиболее уязвимый способ транзакций ввиду высокой опасности мошенничества и кражи средств (Fei Xiao et al., 2023).

Burn-and-Release дополняет первый сценарий, обеспечивая обратное взаимодействие – отправку активов в исходный блокчейн (Susie Xi Rao et al., 2021).

Burn-and-Mint позволяет в проектах *DeFi* «сжигать» привязанные активы в принимающем блокчейне и создавать такое же количество привязанных активов в другом блокчейне, не затрагивая при этом активы, заблокированные на исходной площадке. Например, если лицо захотело перевести деньги с блокчейна 1 на блокчейн 2, а затем изменило это решение и перевело деньги на блокчейн 3, деньги на блокчейн 2 будут сожжены при помощи алгоритма *Burn-and-Mint*.

Небольшой экскурс к технологии блокчейн-мостов в данном контексте не случаен: он позволяет не только понять само устройство этого сервиса, но и объяснить востребованность сетевых мостов в легализации преступных доходов.

В настоящее время существуют централизованные и децентрализованные мосты: у первых имеется централизованный хранитель, отслеживающий транзакции, у вторых хранение активов осуществляется на основе смарт-контракта и не требует привлечения третьих лиц.

В децентрализованных сервисах доходы от преступной деятельности могут передаваться между блокчейнами без идентификации клиента.

Схема легализации «Децентрализованные сетевые мосты» выглядит следующим образом:

- 1) преступник отправляет активы на межсетевой мост;
- 2) он получает новые токены от кроссчейн-моста на анонимный адрес другого блокчейна;
- 3) токены могут быть направлены и на другие мосты, обменены на децентрализованных биржах, переведены на централизованные обменники и конвертированы в фиатную валюту¹³.

На эту схему могут указывать следующие индикаторы:

- a) лицо часто пользуется межсетевыми мостами;
- b) получаемые активы переводятся на децентрализованные биржи;
- c) средства на аккаунты централизованной биржи переводятся с различных децентрализованных сервисов.

На фоне популяризации децентрализованных сервисов расширяется взаимодействие с использованием блокчейн-мостов, увеличивается количество технических решений и, как следствие, растут объемы легализации преступных доходов с использованием данной схемы. К сожалению, современная финансовая разведка

¹³ Elliptic. (2022). DeFi. Risk, Regulation, and the Rise of DeCrime. https://www.elliptic.co/hubfs/downloads/The%20Elliptic%202022%20DeFi%20Report.pdf?utm_campaign=Regulation%207C%20FATF%207C%20Oct%202021&utm_medium=email&_hsmi=184080622&utm_content=184080622&utm_source=hs_automation

пока не разработала эффективные методики отслеживания криптовалютных потоков в блокчейн-мостах и критерии ограничения легальных и теневых доходов на переходе из одного блокчейна в другой.

Легализация преступных доходов с использованием токенов повышенной конфиденциальности

Отмывание преступных доходов с использованием токенов повышенной конфиденциальности (или валюты конфиденциальности) можно осуществлять и вне рамок *DeFi*, но использование децентрализованных сервисов делает легализацию более латентной.

Самую высокую капитализацию имеют следующие валюты конфиденциальности: *Monero*, *Zcash*, *Dash*, *Decred*, *Beldex* и *Mask Network*.

Под токенами (или криптовалютой) повышенной конфиденциальности понимаются цифровые активы, которые скрывают транзакции внутри сети и тем самым обеспечивают анонимность пользователей. Как правило, при создании монет используются следующие технические приемы: скрытые адреса, доказательства с нулевым разглашением, шифрование с открытым ключом или миксеры. *Monero*, например, использует кольцевые подписи и скрытые адреса, *Zcash* – технологию с нулевым разглашением (*zk-SNARKs*), *Dash* – децентрализованную сеть (Möser et al., 2018).

Использование валюты конфиденциальности является законным, однако в отдельных юрисдикциях (например, в США) транзакции с ее использованием относятся к сомнительным и вызывают повышенное внимание финансовой разведки и налоговой службы. Вместе с тем в отдельных юрисдикциях (например, Мальты и Эквадора) такая криптовалюта не ограничена в обороте, чем и пользуются преступники.

Несмотря на высокую анонимность криптовалют, финансовая разведка научилась работать с такими случаями: преступника выявляют при обращении к услугам централизованных криптовалютных бирж. На них распространяются правила ПОД/ФТ, что позволяет правоохранным органам связать криптовалютную транзакцию с конкретным лицом.

Однако в последнее время преступники заметно усложнили схему легализации, включив в них децентрализованные финансы.

В наиболее общем виде механизм отмывания преступных доходов «Валюты конфиденциальности – децентрализованные финансы» может быть представлен следующим образом:

- 1) лицо конвертирует активы, полученные преступным путем, в криптовалюту повышенной конфиденциальности (например, в *Zcash*);
- 2) обращается на децентрализованную биржу и обменивает эту валюту на другую;
- 3) полученные активы переводит на централизованную биржу с различных децентрализованных кошельков, а затем конвертирует их в фиатную валюту.

На использование этой схемы могут указывать следующие индикаторы:

- a) на централизованную биржу приходит большой объем криптовалюты с децентрализованного обменника;
- b) лицо систематически прибегает к обмену криптовалюты повышенной конфиденциальности;
- c) взаимодействует с децентрализованными обменниками, специализирующимися на валютных парах с токенами повышенной конфиденциальности;
- d) на его аккаунтах находится валюта конфиденциальности.

Как правило, использование токенов конфиденциальности заметно запутывает следы транзакций и препятствует выявлению фактов легализации преступных доходов. Неслучайно в сентябре 2020 г. Налоговая служба США (*IRS*) предложила вознаграждение в размере 625 000 долл. за разработку инструментов выявления и отслеживания валюты *Monero*. Этот контракт был заключен с *Chainalysis* и *Integra FEC*. В экспертных отчетах *Chainalysis* утверждает, что ей удалось создать технологию, отслеживающую 65 % случаев использования *Monero*¹⁴.

Но использование наряду с валютой конфиденциальности децентрализованных сервисов (бирж и сетевых мостов) многократно увеличивает латентность легализации, поскольку не позволяет правоохранным органам отследить движение средств через несколько анонимных адресов в разных блокчейнах.

¹⁴ Monero: All About the Top Privacy Coin. (2023, May 4). Chainalysis. <https://www.chainalysis.com/blog/all-about-monero/>

Легализация преступных доходов с использованием проектов предложения монет (ICO)

ICO (*Initial Coin Offering*) представляет собой форму привлечения инвестиций через выпуск и продажу инвесторам цифровых активов за фиатные денежные средства или иные криптовалюты. ICO содержит в себе элементы различных форм привлечения капитала:

- 1) в большинстве случаев в результате вложений в проект инвестор получает актив, торгуемый на публичных торговых площадках, как при публичном размещении ценных бумаг (IPO);
- 2) как правило, продажа токенов связана с публичной PR-кампанией, свойственной краудфандингу;
- 3) проект находится на ранней стадии, типичной для венчурного инвестирования (Банк России, 2017).

Инициатором первичного монетного размещения может выступать любое юридическое и физическое лицо. При этом никаких проверок проект не проходит. Почти все работы ведутся в режиме онлайн.

Обычно легализация преступных доходов при проведении IPO выглядит следующим образом:

- 1) запускается новый ICO-проект, предлагающий токены для финансирования нового проекта (как правило, цифрового);
- 2) за средства, добытые преступным путем, инвестор приобретает инвестиционные токены;
- 3) преступник находит децентрализованную биржу, где размещены новые токены, и конвертирует их в криптовалюту либо другие токены;
- 4) полученные средства выводятся на централизованные биржи и конвертируются в фиатную валюту.

На отмывание преступных доходов с использованием данной схемы могут указывать следующие индикаторы:

- a) инвестор выходит на децентрализованную биржу и стремится обменять большое количество вновь выпущенных токенов на стейблкоины или криптовалюту;
- b) между покупкой инвестиционных токенов и их продажей нет значительного временного лага, сделки не привязаны к колебаниям курса;
- c) сайт инвестиционного проекта не проводит идентификацию клиентов, нет полной информации об учредителях проекта и о его юрисдикции;
- d) не содержится информации об ограничении продажи токенов физическим и юридическим лицам, находящимся в юрисдикции США и других стран с жестким регулированием крипторынка;
- e) ICO-проект не зарегистрирован в качестве службы перевода денег, брокера по ценным бумагам или провайдера услуг виртуальных активов (ПУВА) в юрисдикциях, где это требуется.

Легализация преступных доходов с использованием децентрализованных финансов и игровых криптосервисов

Впервые типологический анализ легализации преступных доходов с использованием онлайн-игр был представлен в отчете МАНИВЭЛ от 11 апреля 2013 г., утвержденном на 41-м Пленарном заседании МАНИВЭЛ (8–12 апреля 2013 г.) (МАНИВЭЛ, 2013).

В числе основных рисков интернет-игр в рамках антиотмывочной деятельности авторы отчета назвали: появление альтернативных платежных систем для размещения средств на виртуальных счетах для участия в азартных играх; большие обороты игровой валюты; простота открытия игрового бизнеса; отсутствие лицензирования; слабая система идентификации клиентов¹⁵.

Позднее в докладе ФАТФ «Виртуальные валюты. Ключевые определения и потенциальные риски» от июня 2014 г. была особо отмечена опасность отмывания преступных доходов с использованием конвертируемой цифровой валюты (ФАТФ, 2014), но ни в одной стране до сих пор не введены ограничения на использование такого рода валюты.

В январе 2022 г. Росфинмониторинг выступил с официальным заявлением о необходимости регулирования внутриигровой валюты. В ведомстве подчеркнули, что «легализация преступных доходов все чаще совершается именно в онлайн-игровых площадках по причине того, что эта сфера не контролируется ни

¹⁵ Использование азартных игр в Интернете для отмывания денег и финансирования терроризма: отчет МАНИВЭЛ. <https://cbr.ru/content/document/file/124051/maneyval%20-%20%D0%9E%D0%94%D0%A4%D0%A2%D0%D1%87%D0%B5%D1%80%D0%B5%D0%B7%20%D0%BE%D0%BD%D0%BB%D0%B0%D0%B9%D0%BD%20%D0%B8%D0%B3%D1%80%D1%8B.pdf>

государственными ведомствами, ни международными структурами. В онлайн-играх существует два типа валют – конвертируемые и неконвертируемые. Интерес для контролирующих органов представляет первый вид, поскольку эту валюту можно купить за реальные деньги, далее в игре возможно совершать платежи, затем обналичить средства через их вывод из игры. Легкость перевода внутриигровой валюты и высокая загруженность игровых платформ позволяют преступным транзакциям теряться в миллиардах операций»¹⁶.

Уголовно-правовые риски игровых валют усугубляются еще и тем, что игровой бизнес является трансграничным, развивается вне рамок антиотмывочного регулирования и привязан к слабо регулируемым цифровым платежным инструментам, в частности, к децентрализованным финансам.

В 2018 г. немецкие эксперты по кибербезопасности заявили, что выявили масштабную схему легализации средств, похищенных с кредитных карт, в мобильных играх *Clash of Clans*, *Clan Royale* и *Marvel Contest of Champions*. При совершении преступлений использовались уязвимости программы идентификации *Apple ID*, а деньги выводились с использованием криптовалют. Для упрощения процесса генерации внутриигровой валюты злоумышленники использовали автоматизированных ботов, созданных фанатами игр¹⁷.

В настоящее время отмывание преступных доходов с использованием игровой валюты осуществляется по следующей схеме «Игровая валюта – децентрализованные финансы»:

1. Лицо регистрирует аккаунт в играх, не поддерживающих процедуру идентификации и не отслеживающих платежи, и покупает конвертируемую игровую валюту или игровые артефакты.

2. Далее он размещает объявление о продаже аккаунта, игровой валюты или артефакта на специальных игровых ресурсах, пабликах и социальных сетях со значительной скидкой.

3. Деньги от проданных активов направляются на анонимные децентрализованные кошельки.

4. Они обмениваются на другую криптовалюту на децентрализованных биржах и распределяются небольшими транзакциями на других анонимных децентрализованных кошельках.

5. Преступник направляет криптовалюту на централизованную биржу и конвертирует ее в фиатную валюту.

На схему легализации могут указывать следующие обстоятельства:

- а) лицо использует нелицензионные сервисы азартных игр, на которых нет базовой процедуры идентификации клиентов (KYC) и (или) которые берут на себя обязательства по защите анонимности пользователей;

- б) игорные сайты, не публикуют информацию о своей собственности или юрисдикции регистрации и не накладывают ограничений на объемы и стоимость используемых криптоактивов;

- в) лицо регистрирует аккаунт в игре, допускающей применение конвертируемой игровой валюты, часто обмениваемой на децентрализованных биржах;

- г) лицо покупает и продает игровую валюту большими объемами и с небольшим временным лагом; нередко предлагает существенные скидки при продаже игровой валюты, артефактов или аккаунта;

- д) полученные от продажи игровых активов средства переводятся на анонимные децентрализованные кошельки.

Выше приведены типовые схемы использования *DeFi* для легализации доходов, полученных преступным путем. Технология децентрализованных финансов с присущими ей анонимностью пользователей и блокчейн-механизмами затрудняет процесс отслеживания финансовых потоков, а отсутствие правового регулирования децентрализованных финансов практически исключает возможность привлечения виновных к уголовной ответственности. Вместе с тем по-прежнему «ахиллесовой пятой» любой из вышеприведенных схем остается перевод средств с децентрализованных сервисов на централизованные биржи, где ведется идентификация пользователей и отслеживаются все транзакции.

Минимизировать риски выявления преступной деятельности позволяет схема цепного дробления (*Chain-peeling*). В настоящее время она используется более чем в 75 % алгоритмов отмывания преступных доходов. Можно условно выделить два алгоритма дробления: с одним или несколькими участниками.

Механизм цепного дробления с одним участником:

- 1) на децентрализованный адрес лица поступает большой объем виртуальных активов;

¹⁶ Онлайн-игры рассматриваются Росфинмониторингом как площадки для отмывания средств. (2022, 8 июля). ВЕСТИ 115-ФЗ. https://115zakon.ru/news/rfm/onlayn_igry_rassmatrivayutsya_rosfinmonitoringom_kak_ploshchadki_dlya_otmyvaniya_sredstv/

¹⁷ Lishchuk, R. (2021, June 23). 6 Major Data Breaches We Found and Reported in 2018. MacKeeper. <https://mackeeper.com/blog/data-breach-reports-2018/>

2) он направляет небольшую часть этих средств на адрес биржи, а затем переводит оставшиеся неизрасходованные криптоактивы на вновь сгенерированный децентрализованный адрес (*DeFi*-кошелек);

3) затем он вновь повторяет этот процесс, направляя деньги на новые биржи и переводя остаток на новый децентрализованный кошелек.

Как правило, централизованная биржа видит только многочисленные отдельные зачисления криптоактивов с большим количеством новых кошельков, вовлеченных в цепочку транзакций, в то время как обратная связь с первоначальным адресом, на который были получены незаконные средства, остается скрытой.

На описанную выше схему указывают следующие индикаторы:

а) клиент получает средства, которые за несколько часов претерпели множественные переходы между разными адресами;

б) в некоторых случаях криптоактивы, связанные с новыми адресами, могут быть депонированы на многочисленные счета денежных мулов;

с) как правило, активность наблюдается после совершения крупного хищения криптоактивов.

Механизм дробления с несколькими участниками можно представить следующим образом:

1) несколько пользователей начинают отправлять криптоактивы между своими счетами в больших объемах и с высокой скоростью;

2) аккаунты пользователей связаны с сомнительными децентрализованными биржами и теневым Интернетом;

3) клиенты стремятся конвертировать средства в фиат сразу после участия в сомнительной операции с несколькими кошельками.

Индикаторами этой схемы являются:

а) более 20 пользователей с общими адресами, мобильными устройствами или другими общими параметрами создают учетные записи на централизованной бирже;

б) они начинают отправлять друг другу средства на постоянной основе в отсутствие явного экономического повода;

с) клиент из одной страны переводит средства со своего кошелька на кошелек клиента из другой страны. Средства немедленно обналичиваются в обменнике или банкомате в короткие сроки;

д) пользователи не готовы предоставить информацию об источнике своих средств и цели повторных переводов.

Выводы

Использование *DeFi*-сервисов в легализации преступных доходов еще только приобретает популярность и уже в 2024 г. может занять лидирующее место среди преступных криптовалютных алгоритмов. К сожалению, современное финансовое регулирование не позволяет осуществлять качественный мониторинг децентрализованных финансов ввиду невозможности обязывания лиц, участвующих в одноранговых транзакциях, идентифицироваться и вести учет финансовых потоков (Банк России, 2022). Но это, однако, не означает, что отмывание преступных доходов в *DeFi* не может быть отслежено и пресечено. Ввиду своей новизны децентрализованные финансы пока лишены возможности обеспечения полного цикла движения преступных доходов. Преступник вынужден «выходить» в зону регулирования, переводя криптоактивы на кошелек централизованных бирж и других ПУВА, что, в свою очередь, позволяет правоохранителям отслеживать операции, зная ключевые индикаторы преступной схемы.

По мере апробации технологии выявления подозрительных транзакций в антиотмывочное законодательство должны быть внедрены положения, позволяющие усилить финансовый контроль ПУВА непосредственно в точках входа преступных доходов с децентрализованных бирж с одновременным усилением обмена данными между национальными службами финансового мониторинга и контроля.

Список литературы

- Банк России. (2017). *Обзор по криптовалютам, ICO (Initial Coin Offering) и подходам к их регулированию: доклад Банка России*. https://cbr.ru/content/document/file/36009/rev_ico.pdf
- Банк России. (2022). *Децентрализованные финансы: информационно-аналитический доклад Банка России*. https://cbr.ru/Content/Document/File/141992/report_07112022.pdf
- Иванцов, С. В., Сидоренко, Э. Л., Спасенников, Б. А., Березкин, Ю. М., Суходолов, Я. А. (2019). Преступления, связанные с использованием криптовалюты: основные криминологические тенденции. *Всероссийский криминологический журнал*, 13(1), 85–93. [https://doi.org/10.17150/2500-4255.2019.13\(1\).85-93](https://doi.org/10.17150/2500-4255.2019.13(1).85-93)
- МАНИВЭЛ. (2013, апрель). *Использование азартных игр в Интернете для отмывания денег и финансирования терроризма*. <https://cbr.ru/content/document/file/124051/maneyval%20-%20D0%9E%D0%94%D0%A4%D0%A2%20%D1%87%D0%B5%D1%80%D0%B5%D0%B7%20%D0%BE%D0%BD%D0%BB%D0%B0%D0%B9%D0%BD%20%D0%B8%D0%B3%D1%80%D1%8B.pdf>
- Сидоренко, Э. Л. (2023). Правовой статус децентрализованных финансов: к постановке проблемы. *Lex Russica*, 76(3), 87–99. <https://doi.org/10.17803/1729-5920.2023.196.3.087-099>
- Сидоренко, Э. Л. (2023). Дефи-преступность: состояние, тенденции и криминологические модели. *Russian Journal of Economics and Law*, 17(2), 327–341. <https://doi.org/10.21202/2782-2923.2023.2.327-341>
- ФАТФ. (2014, июнь). Виртуальные валюты. Ключевые определения и потенциальные риски: отчет ФАТФ. https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf
- ФАТФ. (2015, июнь). Руководство по применению риск-ориентированного подхода: провайдеры услуг по обмену конвертируемой виртуальной валюты. https://eurasiangroup.org/files/uploads/files/FATF_documents/FATF_Guidances/ROP_Virtualnye_valyuty.pdf
- ЦСР. (2022, июль). Виртуальные активы: токенизация и эмиссия токенов: Доклад ЦСР. <https://www.csr.ru/upload/iblock/855/2xdr6q540ixfyb5pmkiszegtlqgh54dh.pdf>
- Allen, H. J. (2023). DeFi: Shadow Banking 2.0? *Wm. & Mary L. Rev.*, 64, 919. <http://dx.doi.org/10.2139/ssrn.4038788>
- Carter, N., & Jeng, L. (2021, June 14). DeFi Protocol Risks: The Paradox of DeFi. “*Regtech, Suptech and Beyond: Innovation and Technology in Financial Services*” *RiskBooks – Forthcoming 3Q 2021*. <http://dx.doi.org/10.2139/ssrn.3866699>
- Clements, R. (2021, October 28). Built to Fail: The Inherent Fragility of Algorithmic Stablecoins. *Wake Forest L. Rev.*, 11, 131. <http://dx.doi.org/10.2139/ssrn.3952045>
- Fei Xiao, Yuncheng Wu, Meihui Zhang, Gang Chen, & Beng Chin Ooi. (2023). MINT: Detecting Fraudulent Behaviors from Time-series Relational Data. *Proceedings of the VLDB*, 16(12), 3610–3623. <https://doi.org/10.14778/3611540.3611551>
- FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021, April 5). *DeFi and the Future of Finance*. <http://dx.doi.org/10.2139/ssrn.3711777>
- Allen, H. J. DeFi: shadow banking 2.0?. *American University Washington College of Law Washington College of Law Research Paper*, No. 2022-02
- Maia, G. & Vieira dos Santos, J. (2021, July 1). MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). In F. P. Coutinho, M. L. Pires, & B. Barradas (Eds.), *Blockchain and the law: dynamics and dogmatism, current and future*. <http://dx.doi.org/10.2139/ssrn.3875355>
- Momtaz, P. P. (2022, March 22). *How Efficient is Decentralized Finance (DeFi)?* <http://dx.doi.org/10.2139/ssrn.4063670>
- Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, Sh., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An Empirical Analysis of Traceability in the Monero Blockchain. In *Proceedings on Privacy Enhancing Technologies Symposium*, 3, 143–163. <http://dx.doi.org/10.1515/popets-2018-0025>
- Schuppli, B., & Jafari, G. A. (2021, October 28). Piercing the Digital Veil: A Case Study for a DAO Legal Framework under Swiss Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law "JIPITEC"*, <http://dx.doi.org/10.2139/ssrn.3951804>
- Susie Xi Rao, Shuai Zhang, Zhichao Han, Zitao Zhang, Wei Min, Zhiyao Chen, Yinan Shan, Yang Zhao, & Ce Zhang. (2021). xFraud: Explainable Fraud Transaction Detection. *Proceedings of the VLDB Endowment*, 15(3), 427–436. <https://doi.org/10.14778/3494124.3494128>

References

- Allen, H. J. (2023). DeFi: Shadow Banking 2.0? *Wm. & Mary L. Rev.*, 64, 919. <http://dx.doi.org/10.2139/ssrn.4038788>
- Bank of Russia. (2017). *Review on cryptocurrencies, ICO (Initial Coin Offering) and approaches to their regulation: report of the Bank of Russia*. (In Russ.). https://cbr.ru/content/document/file/36009/rev_ico.pdf

- Bank of Russia. (2022). *Decentralized finances: information and analytical report of the Bank of Russia*. (In Russ.). https://cbr.ru/Content/Document/File/141992/report_07112022.pdf
- Carter, N., & Jeng, L. (2021, June 14). DeFi Protocol Risks: The Paradox of DeFi. "Regtech, Suptech and Beyond: Innovation and Technology in Financial Services" *RiskBooks – Forthcoming 3Q 2021*. <http://dx.doi.org/10.2139/ssrn.3866699>
- Clements, R. (2021, October 28). Built to Fail: The Inherent Fragility of Algorithmic Stablecoins. *Wake Forest L. Rev.*, 11, 131. <http://dx.doi.org/10.2139/ssrn.3952045>
- CSR. (2022, July). *Virtual currencies: tokenization and token emission: CSR report*. (In Russ.). <https://www.csr.ru/upload/iblock/855/2xdr6q540ixfyb5pmkiszegtlqgh54dh.pdf>
- FATF. (2014, June). *Virtual currencies. Key definitions and potential risks: FATF report*. (In Russ.). https://eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf
- FATF. (2015, June). *Guidance for a risk-based approach: service providers of virtual currencies exchange*. (In Russ.). https://eurasiangroup.org/files/uploads/files/FATF_documents/FATF_Guidances/ROP_Virtualnye_valyuty.pdf
- Fei Xiao, Yuncheng Wu, Meihui Zhang, Gang Chen, & Beng Chin Ooi. (2023). MINT: Detecting Fraudulent Behaviors from Time-series Relational Data. *Proceedings of the VLDB*, 16(12), 3610–3623. <https://doi.org/10.14778/3611540.3611551>
- FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris. www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021, April 5). *DeFi and the Future of Finance*. <http://dx.doi.org/10.2139/ssrn.3711777>
- Ivantsov, S. V., Sidorenko, E. L., Spasennikov, B. A., Berezkin, Yu. M., & Sukhodolov, Ya. A. (2019). Cryptocurrency-Related Crimes: Key Criminological Trends. *Russian Journal of Criminology*, 13(1), 85–93. (In Russ.). [https://doi.org/10.17150/2500-4255.2019.13\(1\).85-93](https://doi.org/10.17150/2500-4255.2019.13(1).85-93)
- Maia, G. & Vieira dos Santos, J. (2021, July 1). MiCA and DeFi ('Proposal for a Regulation on Market in Crypto-Assets' and 'Decentralised Finance'). In F. P. Coutinho, M. L. Pires, & B. Barradas (Eds.), *Blockchain and the law: dynamics and dogmatism, current and future*. <http://dx.doi.org/10.2139/ssrn.3875355>
- Momtaz, P. P. (2022, March 22). *How Efficient is Decentralized Finance (DeFi)?* <http://dx.doi.org/10.2139/ssrn.4063670>
- MONEYVAL. (2013, April). *Using gambling in the Internet for money laundering and financing terrorism*. (In Russ.). <https://cbr.ru/content/document/file/124051/maneyval%20-%20%D0%9E%D0%94%D0%A4%D0%A2%20%D1%87%D0%B5%D1%80%D0%B5%D0%B7%20%D0%BE%D0%BD%D0%BB%D0%B0%D0%B9%D0%BD%20%D0%B8%D0%B3%D1%80%D1%8B.pdf>
- Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, Sh., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An Empirical Analysis of Traceability in the Monero Blockchain. In *Proceedings on Privacy Enhancing Technologies Symposium*, 3, 143–163. <http://dx.doi.org/10.1515/popets-2018-0025>
- Schuppli, B., & Jafari, G. A. (2021, October 28). Piercing the Digital Veil: A Case Study for a DAO Legal Framework under Swiss Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law "JIPITEC"*, <http://dx.doi.org/10.2139/ssrn.3951804>
- Sidorenko, E. L. (2023). Defi-crime: condition, trends and criminological models. *Russian Journal of Economics and Law*, 17(2), 327–341. (In Russ.). <https://doi.org/10.21202/2782-2923.2023.2.327-341>
- Sidorenko, E. L. (2023). Legal Status of Decentralized Finance: Towards the Articulation of Issue. *Lex Russica*, 76(3), 87–99. (In Russ.). <https://doi.org/10.17803/1729-5920.2023.196.3.087-099>
- Susie Xi Rao, Shuai Zhang, Zhichao Han, Zitao Zhang, Wei Min, Zhiyao Chen, Yinan Shan, Yang Zhao, & Ce Zhang. (2021). xFraud: Explainable Fraud Transaction Detection. *Proceedings of the VLDB Endowment*, 15(3), 427–436. <https://doi.org/10.14778/3494124.3494128>

Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author.

История статьи / Article history

Дата поступления / Received 10.10.2023

Дата одобрения после рецензирования / Date of approval after reviewing 15.11.2023

Дата принятия в печать / Accepted 15.11.2023