Russian Journal of Economics and Law. 2023. Т. 17, № 2 / Russian Journal of Economics and Law, 2023, Vol. 17, No. 2
Криптомир и цифровые финансы / Crypto-World and Digital Finance

ISSN 2782-2923

Научная статья **DOI: 10.21202/2782-2923.2023.2.327-341**

УДК 343.9:336:004

Э. Л. СИДОРЕНКО[1]

[1] *Московский государственный институт международных отношений Министерства иностранных дел России, г. Москва, Россия*

DEFI-ПРЕСТУПНОСТЬ: СОСТОЯНИЕ, ТЕНДЕНЦИИ И КРИМИНОЛОГИЧЕСКИЕ МОДЕЛИ

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 иностранных 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: разработка криминологической концепции *DeFi*-преступности и мер по ее сдерживанию.

Методы: диалектический материализм и основанные на нем общенаучные методы познания, используемые в отечественной криминологии.

Результаты: разработана криминологическая концепция *DeFi*-преступности как разновидности цифровой преступности, т. е. предложена новая частная криминологическая теория DeFi-преступности (*DeFi*-криминология) в структуре цифровой криминологии. Определены информационные факторы, влияющие на состояние, структуру и тенденции *DeFi*-преступности, и предложены меры по ее сдерживанию криминологическими и технологическими средствами.

Научная новизна: представленная работа является первым и единственным исследованием, проведенным в рамках цифровой криминологии, отражающим состояние, тенденции и структуру *DeFi*-преступности, раскрывающим основные причины, ее формирующие, а также описывающим варианты сдерживания этого вида цифровой преступности технологическими и криминологическими средствами.

Практическая значимость: результаты исследования могут быть использованы в правоприменительной деятельности при оценке потенциальных угроз от *DeFi*-преступности и выработке мер по их снижению, в образовательной деятельности – в процессе преподавания курсов криминологии, киберкриминологии, цифровой криминологии, в научно-исследовательской деятельности – получения дополнительных знаний по отдельным видам *DeFi*-преступности: *DeFi*-кражам и *DeFi*-мошенничеству в процессе их дальнейшего исследования в рамках *DeFi*-криминологии.

Ключевые слова: криминология, киберкриминология, цифровая криминология, *DeFi*-криминология, преступность, цифровая преступность, предупреждение преступности, *DeFi*-преступность, децентрализованные финансы, *DeFi*-кража, *DeFi*-мошенничество.

Как цитировать статью: Сидоренко Э. Л. DeFi-преступность: состояние, тенденции и криминологические модели // Russian Journal of Economics and Law. 2023. Т. 17, № 2. С. 327–341. DOI: 10.21202/2782-2923.2023.2.327-341

Russian Journal of Economics and Law. 2023. T. 17, № 2 / Russian Journal of Economics and Law, 2023, Vol. 17, No. 2
Криптомир и цифровые финансы / Crypto-World and Digital Finance

ISSN 2782-2923

Scientific article

E. L. SIDORENKO[1]

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

DEFI-CRIME: CONDITION, TRENDS AND CRIMINOLOGICAL MODELS

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 develop a criminological concept of DeFi-crime and measures to deter it.
Methods: dialectical materialism and the general scientific methods of cognition based on it, used in the Russian criminology.
Results: a criminological concept of DeFi-crime as a type of digital crime was developed, i.e. a new specific criminological theory of DeFi-crime (DeFi-criminology) within the structure of digital criminology was proposed. The information factors influencing the DeFi-crime state, structure and trends were determined, and measures for its deterrence by criminological and technological means were proposed.
Scientific novelty: the presented work is the first and only study conducted within the framework of digital criminology, reflecting the state, trends and structure of DeFi-crime, revealing the main causes that form it, as well as describing options for deterring this type of digital crime by technological and criminological means.
Practical significance: the study results can be used in law enforcement activities when assessing potential threats from DeFi-crime and developing measures to reduce them; in educational activities – in the process of teaching courses in criminology, cybercriminology, digital criminology; in research activities – when obtaining additional knowledge on certain types of DeFi–crime: DeFi-theft and DeFi-fraud during their further research in DeFi-criminology.

Keywords: Criminology, Cybercriminology, Digital criminology, DeFi-criminology, Crime, Digital crime, Crime prevention, DeFi-crime, Decentralized finance, DeFi-theft, DeFi-fraud

For citation: Sidorenko, E. L. (2023). Defi-crime: condition, trends and criminological models. *Russian Journal of Economics and Law*, *17*(2), 327–341. (In Russ.). DOI: 10.21202/2782-2923.2023.2.327-341

Введение

Развитие новых финансовых технологий заметно повлияло на состояние, структуру и динамику преступности, вызвав к жизни ранее не встречавшиеся формы противоправной деятельности. И хотя правоохранительные органы указывают на некоторое снижение уровня преступности в сфере информационных технологий[1], на практике этот спад оборачивается ростом латентной цифровой преступности. К сожалению, правоохранительная система оказалась не готова к выявлению и расследованию преступлений в цифровой сфере. В числе причин можно назвать и недостаточность знаний о технических особенностях совершаемых деяний, и отсутствие криминалистических моделей расследования цифровых финансовых преступлений,

[1] Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/32515852/ (дата обращения: 20.03.2023).

ISSN 2782-2923

и рассогласованную позицию государств и международных организаций в вопросах регулирования новых финансовых инструментов.

Одним из самых латентных и вместе с тем стремительно растущих сегментов цифровой преступности стали посягательства, совершаемые с использованием децентрализованных финансов (*DeFi*-преступность). Децентрализованные финансы (*DeFi*) как продукт блокчейн-технологий появились в 2018–2019 гг., но уже в 2021 г. их капитализация достигла невероятных показателей. Как отмечается в докладе Банка России, за период с января 2019 г. по март 2022 г. она возросла, по одним источникам, с 1 до 77 млрд долл. США, по другим – до 200 млрд долл. США [1].

По данным зарубежных статистических агентств, по состоянию на апрель 2023 г. рынок *DeFi* составил 77,29 млрд долларов США при общем количестве пользователей 6,68 млн человек[2]. Рост популярности *DeFi* объясняется как самой технологией распределенного реестра и разнообразием возможных цифровых проектов, так и уникальной структурой отношений между пользователями. Фактически *DeFi* представляют собой новую философию финансов, исключающую вертикальный контроль и посредников. Пользователи свободны в своей финансовой деятельности, а децентрализованные финансы лишь помогают выбрать оптимальную клиентскую стратегию. Популярность *DeFi* среди пользователей объясняется анонимностью расчетов, отсутствием географических привязок, ощущением самостоятельности и возможности получения более высокой доходности, в том числе за счет спекуляций на волатильности криптоактивов и др. [1, 2].

В наиболее общих чертах децентрализованные финансы представляют собой блокчейн-приложения, использование которых невозможно без смарт-контракта с внедренным в него протоколом.

Отличительной чертой *DeFi* является то, что отношения между сторонами строятся по принципу горизонтальных связей *P2P*, а операции осуществляются в автоматическом режиме в соответствии с протоколом контракта. Горизонтальный характер отношений предполагает, что каждый пользователь самостоятелен в своих решениях и в полном объеме отвечает за сохранность собственных средств. *DeFi* исключают и наличие внешнего регулятора в виде национального банка или финансовой организации.

Система децентрализованных финансов включает в себя ряд важных, не имеющих аналогов в традиционной финансовой системе элементов:

– стейблкоины – блокчейн-активы, стоимость которых привязана к фиатным валютам или биржевым товарам;

– децентрализованные криптокошельки – специальные программы, позволяющие пользователям хранить, учитывать и отчуждать криптовалюту и иные блокчейн-активы и обеспечивать доступ к ним при помощи публичного и приватного ключа – криптографического кода;

– межсетевые мосты – технологии, обеспечивающие передачу информации от одной сети блокчейна к другой;

– платформы взаимного кредитования – проекты финансирования, где сторонами выступают физические лица без участия банков и кредитных организаций;

– децентрализованные криптобиржи (*Decentralized Exchange*, *DEX*) – цифровые площадки купли-продажи криптовалюты *P2P* при помощи протоколов смарт-контрактов. Фактически это площадки-посредники между пользователями для оборота активов по принципу одноранговой обменника;

– сервисы страхования – децентрализованные проекты, где страхователем выступает не компания, а пользователи, которые предоставляют свои средства в пул ликвидности сервиса. При этом страховая премия зависит от актива, вероятности рисков, протокола смарт-контракта и других факторов;

– сервисы управления – программы, позволяющие участвовать в принятии решений относительно будущего проекта на основании наличия токена управления (*governance tokens*);

[2] Decentralized Finance (DeFi) – statistics & facts. URL: https://www.statista.com/topics/8444/decentralized-finance-defi/ (дата обращения: 20.03.2023).

ISSN 2782-2923

– агрегаторы – программы, собирающие сведения из других *DeFi*-сервисов и предоставляющие пользователям наиболее выгодные возможности;

– платформы ликвидного скейтинга – проекты, в рамках которых пользователи «замораживают» свои активы в специальном контракте, а затем получают пассивный доход за то, что удостоверяют транзакции в сети;

– оракулы – это своеобразные агенты, которые подтверждают наступление конкретных юридических фактов из внешней среды и передают эти данные в смарт-контракт. Показательно то, что для самого *DeFi*-сервиса оракулы являются внешним участником. Обращение к ним обычно «зашивается» в смарт-контракт, и только через это взаимодействие обеспечивается их работа в децентрализованной системе [3].

Особая архитектура *DeFi* расширяет горизонты понимания цифровых отношений и их форматов, но вместе с тем таит в себе ряд рисков технического, экономического и правового характера. Вопрос о рисках *DeFi*-сервисов в современной доктрине является одним из самых обсуждаемых.

В числе основных рисков децентрализованных финансов исследователи называют: уязвимости *DeFi*-протоколов [4]; высокую волатильность монет [5]; сложное устройство межсетевых мостов [6], формат отношений *P2P* между участниками экосистемы [7], отсутствие четкого взаимодействия между централизованными и децентрализованными финансами [8] и др.

Интерес представляет работа С. Каура, С. Синха и др. [9]. Авторы не ограничиваются перечислением отдельных уязвимостей *DeFi*, а предлагают многофакторный анализ рисков этой технологии. В числе ключевых уязвимостей они называют:

– операционные риски (потери закрытых ключей, риски обновления, управления и компонуемости);

– технические риски (риски смарт-контрактов, риски майнеров, транзакционные риски и риски оракулов);

– финансовые уязвимости (риски ликвидности, рыночные и кредитные риски);

– правовые и нормативные риски (отсутствие регулирования либо избыточная регламентация) [9].

Перечисленные выше факторы негативно влияют на общий криминологический фонд использования *DeFi*-сервисов: технологические уязвимости позволяют с легкостью обходить защиту и организовывать массированные кибератаки, которые будут описаны ниже, а отсутствие правового регулирования фактически нивелирует все меры оперативного и процессуального сдерживания *DeFi*-преступности.

На правовых рисках новых технологий как факторе воспроизводства криминальной активности хотелось бы остановиться особо. Сегодня *DeFi*-сервисы не имеют однозначного правового статуса во многом из-за непонимания того, что должно выступать ключевым идентификационным критерием: технология, смарт-контракт, продуктовая сфера, правовые риски либо особый правовой статус участников правоотношений. Развитие *DeFi* обострило и дискуссию о том, какой из принципов должен быть положен в основу правового регулирования: технологически нейтральный или технологически релевантный подход [3].

Фактически децентрализованные финансы в России и зарубежных странах находятся вне закона. С одной стороны, точечное и очень осторожное регулирование технологии распределенного реестра практически не затрагивает сущностных характеристик *DeFi*-сервисов и не может упорядочить отношения между пользователями.

С другой – использование продуктового принципа регулирования – «те же риски, те же правила» – затрудняется тем, что существующие между сторонами отношения регулируются в формате *peer-to-peer* (*P2P*), а это, как известно, исключает применение к *DeFi* традиционного регулирования страхования, кредитования, построенного на принципах *B2P*.

Пробельность правового регулирования *DeFi* и техническая уязвимость кода предопределяют стремительный рост преступлений, совершаемых с использованием децентрализованных финансов. Устойчивость моделей преступлений, единство детерминационного комплекса и мотивационной составляющей позволяют говорить о формировании принципиального нового криминологического феномена – *DeFi*-преступности.

В рамках настоящего исследования ее можно определить как устойчивое криминологическое явление, совокупность преступлений, совершаемых в сфере децентрализованных сервисов (бирж, платформ взаимного кредитования, страхования, управления, ликвидного стейкинга и др.) с использованием стейблкоинов,

ISSN 2782-2923

децентрализованных криптокошельков, межсетевых мостов и (или) оракулов. *DeFi*-преступность технологически связана с развитием распределенных реестров, и ключевым фактором ее воспроизводства являются уязвимости децентрализованных финансов.

Как и любой другой сегмент преступности, *DeFi*-преступность имеет ряд устойчивых признаков и свойств, выраженных в состоянии, структуре и динамике посягательств.

В настоящее время как никогда важно не только обозначить предметные границы *DeFi*-преступности как нового криминологического явления, но и показать тенденции ее развития и сформировать правильный запрос практики на выявление, анализ и предупреждение данных преступлений.

Именно поэтому в рамках настоящего исследования будут последовательно рассмотрены и решены следующие вопросы:

– оценка основных криминологических трендов *DeFi*-преступности;

– рассмотрение видов *DeFi*-преступности с выделением моделей криминальной активности в сфере децентрализованных финансов;

– определение ключевых задач предупреждения этого сегмента цифровой преступности без привязки к проблемам квалификации преступлений.

В основу настоящей работы положен объемный теоретический и статистический материал. Эмпирическую базу исследования составила аналитика международных организаций. Проанализированы доклады Банка международных расчетов [10], ФАТФ (Группа разработки финансовых мер по борьбе с отмыванием денег – *Financial Action Task Force*, *FATF*) [11], Международной комиссии по ценным бумагам (*IOSCO*) [12], Совета по финансовой стабильности [13], отчет Всемирного экономического форума [14] и другие, изучены материалы крупных экспертных центров (*Chainalysis* [15], юридического колледжа Американского университета [16] и др.), проработан доклад Банка России «Децентрализованные финансы» [1], изучены работы отечественных и зарубежных исследователей, а также материалы судебной практики.

Результаты исследования

Состояние и динамика *DeFi*-преступности

Согласно зарубежным исследованиям, в 2022 г. каждый второй мошеннический проект в сфере оборота криптовалюты был связан с *DeFi*. Это объясняется в первую очередь ажиотажем вокруг сектора. Только в 2021 г. с протоколов *DeFi* было украдено около 2,7 млрд долларов США[3]. В целом темпы прироста *DeFi*-хищений в 2022 г. в 13 раз превысили показатели 2021 г., а *DeFi*-легализации – в 19 раз[4]. По данным аналитиков *Chainalysis*, в 2022 г. у криптовалютных компаний украли около 3 млрд долларов США посредством взлома платформ децентрализованных финансов (*DeFi*)[5].

Интересные данные о масштабах и динамике *DeFi*-преступности представлены в докладе *Crystal Blockchain*[6]. В нем, в частности, отмечается, что за годы существования децентрализованных финансов произошел 231 взлом *DeFi*, 135 крупных хакерских *DeFi*-атак и 95 мошенничеств. Ущерб от преступлений совокупно составил 16,7 млрд долларов (более 4,5 млрд долларов в результате хакерских атак, около 7,5 млрд долларов с помощью мошенничества и более 4,81 млрд долларов с помощью взломов кода *DeFi*).

[3] The 2022 Crypto Crime Report Original data and research into cryptocurrency-based crime. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf (дата обращения: 20.03.2023).

[4] Там же.

[5] The 2023 Crypto Crime Report. Everything you need to know about cryptocurrency-based crime. URL: https://ohmyswift.ru/Crypto_Crime_Report_2023.pdf (дата обращения: 20.03.2023).

[6] Crypto & DeFi Security Breaches, Fraud & Scams Report. Discover the largest hacks, scams and security breaches involving crypto and DeFi that have taken place since 2011. URL: https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/ (дата обращения: 20.03.2023).

ISSN 2782-2923

Если в 2019 г. самым прибыльным считался взлом централизованных криптовалютных бирж, то в 2022 г. соотношение централизованных и децентрализованных площадок обмена криптовалюты составляет 1 : 13[7].

В новом докладе Министерства финансов США также отмечена тревожная динамика роста *DeFi*-преступности[8]. Преступники, как правило, используют уязвимости в режимах регулирования, надзора и правоприменения в сфере ПОД/ФТ.

В 2022 г. ущерб от криптопреступлений составил 13,76 млрд долларов США. Из них: отмывание денег – 7,33 млрд долларов США, кибератаки/эксплойты – 3,6 млрд долларов США, финансовые пирамиды – 1 млрд долларов США и мошенничество – 830 млн долларов США[9]. При этом наиболее уязвимыми для совершения преступлений были *DeFi*-сервисы и особенно межсетевые мосты. Так, только взлом моста принес преступникам 1,89 млрд долларов в 2022 г.

Анализ большого массива статистических и научных данных позволил выделить ряд устойчивых тенденций развития *DeFi*-преступности:

– постепенно очерчивается криминальная специализация преступников. Если ранее на *DeFi* совершались атаки с целью демонстрации уязвимости системы, то уже в 2022 г. стало увеличиваться число высокоорганизованных преступлений четкой направленности;

– основными видами криминальной специализации *DeFi*-преступников являются кража цифровых активов, мошенничество, легализация преступных доходов и др.;

– увеличивается материальный ущерб от преступных посягательств на *DeFi*-сервисы. Так, в 2022 г. такие преступления причинили ущерб в размере 32,6 млн долларов, что вдвое превысило показатели 2021 г.;

– наряду с ростом ущерба снижается общее количество взломов. В 2022 г. кибератаки повторялись в среднем раз в четыре дня, а годом ранее – один раз в три дня, что является лишним свидетельством ориентации преступников на совершение высокоорганизованных посягательств;

– изменяются и представления об уязвимости используемых технологий. Если ранее лидером по количеству сбоев была технология *Ethereum*, то в настоящее время – *Binance Smart Chain* (*BSC*);

– самыми уязвимыми для преступных посягательств были и остаются межсетевые мосты (*chain hopping*), которые позволяют пользователям обмениваться информацией между различными блокчейнами. По экспертным оценкам, в 2022 г. из этих сервисов было украдено более 1,2 млрд долларов – почти 70 % от всех взломов. Это вдвое больше, чем в 2021 г., когда было похищено 640 млн долларов[10];

– современная *DeFi*-преступность демонстрирует высокую адаптивность и гибкость к изменяющимся условиям. В случаях активного противодействия со стороны государственных органов и международных организаций преступники достаточно быстро меняют направление своей деятельности.

В качестве примера можно привести последствия ограничительной политики в отношении *DeFi*-сервиса *Tornado Cash*. Усложнение превентивных механизмов привело к тому, что хакеры в течение месяца изменили свою специализацию и занялись легализацией преступных доходов. В итоге за октябрь 2022 г. преступниками через межсетевые мосты было легализовано более 295 млн долларов США[11];

– существенно осложнились способы совершения преступлений. Сегодня преступники не ограничиваются использованием одноранговых технологий, а выстраивают цепочки движения денежных средств не только в рамках *DeFi*-пространства, но и с использованием централизованных финансовых блокчейн-институтов. Взлом криптовалютного кошелька сопровождается переводом похищенных средств через межсетевые мосты

---

[7] Там же.

[8] Illicit Finance Risk Assessment of Decentralized Finance. URL: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (дата обращения: 20.03.2023).

[9] Доклад исследовательской фирмы Beosin EagleEye. URL: https://beosin.com/resources/Global_Web3_Security_Report_2022_.pdf (дата обращения: 20.03.2023).

[10] Top Five DeFi Crime Trends of 2022. Crypto Theft Fraud Mixers DeFi Investigations and Reporting. URL: https://hub.elliptic.co/analysis/top-five-defi-crime-trends-of-2022 (дата обращения: 20.03.2023).

[11] Там же.

ISSN 2782-2923

в другие блокчейны, дроблением и направлением на централизованные криптовалютные биржи и прочим, что существенно снижает возможности правоохранительных органов в части выявления и расследования *DeFi*-преступлений.

Виды *DeFi*-преступлений и криминологические модели их совершения

Кража криптоактивов. Согласно современным исследованиям, этот вид *DeFi*-преступности лидирует как по количеству взломов, так и причиненному ущербу. Так, по данным казначейства США, в 2022 г. злоумышленники украли у владельцев виртуальных активов миллиарды долларов США[12]. Причина роста этих преступлений связана с повышенным интересом инвесторов к децентрализованным финансам, открытый характер услуг и уязвимости межсетевых коммуникаций.

Как правило, преступники прибегают к следующим способам краж криптовалюты в *DeFi*-сервисах:

– модель флеш-кредита (*flashloan*, или мгновенного кредита). Мгновенные кредиты – это необеспеченные займы цифровых активов без ограничений по заимствованиям, при которых пользователь занимает средства и возвращает их в одной и той же транзакции. Если пользователь не может погасить кредит, смарт-контракт отменяет транзакцию и возвращает деньги кредитору. Мгновенные кредиты позволяют должникам оперативно получить необходимые средства для краткосрочных операций на крипторынке.

Схема движения средств такова: провайдер мгновенного кредита передает запрошенные активы пользователю; пользователь использует заемные средства в работе с другими смарт-контрактами, после завершения операций он возвращает активы провайдеру мгновенных кредитов, если пользователь вернул недостаточно средств, провайдер немедленно отменяет транзакцию[13].

В рамках мгновенных кредитов преступник, как правило, использует приток привлеченных средств для манипулирования ценами на криптоактивы через различные *DeFi*-сервисы. Его конечной целью является получение доступа к управлению смарт-контрактом или протоколом с дальнейшими изменением кода и выводом ликвидности.

Возможна также ситуация, когда лицо манипулирует базовым кодом контракта и размещает в системе запись транзакции о возврате кредита, в то время как он либо погашен частично, либо не погашен вовсе.

Приведем несколько ярких примеров использования этой модели хищения криптоактивов.

В 2020 г. платформа децентрализованного финансирования *Cheese Bank* понесла убытки в размере 3,3 млн долларов в результате использования мгновенных кредитов. Преступники брали заем, обменивали средства на другие активы, депонировали их и повторно брали заем на еще большее количество токенов. Тем самым они манипулировали ценой определенного токена на одной бирже[14].

В апреле 2020 г. хакер украл цифровые активы на сумму 25 млн долларов США у *Lendf.Me*. Он использовал уязвимость повторного входа, чтобы манипулировать внутренней записью *Lendf.Me* о залоге. Преступник сначала внес значительную сумму актива *imBTC* в качестве залога, впоследствии инициировал еще один депозит *imBTC*, но в рамках обратного вызова и до фактического перевода *imBTC* снял свой первоначальный депозит *imBTC*. В протоколе блокчейна залоговый баланс злоумышленника увеличился до 25 млн долларов США, после чего он вывел ликвидность через *DeFi*-обменник. Под давлением властей преступник вернул средства[15].

---

[12] Illicit Finance Risk Assessment of Decentralized Finance. URL: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (дата обращения: 20.03.2023).

[13] DeFi flash loans explained. A brief explanation of what flash loans are, how they impact the crypto ecosystem, and ways to prevent flash loan attacks. URL: https://www.moonpay.com/learn/defi/defi-flash-loans (дата обращения: 20.03.2023).

[14] Cheese Bank's multi-million-dollar hack explained by security firm URL: https://cointelegraph.com/news/cheese-bank-s-multi-million-dollar-hack-explained-by-security-firm (дата обращения: 20.03.2023).

[15] How the dForce hacker used reentrancy to steal 25 million. URL: https://quantstamp.com/blog/how-the-dforce-hacker-used-reentrancy-to-steal-25-million (дата обращения: 20.03.2023).

ISSN 2782-2923

Представляет интерес и случай хищения 55 млн долларов США с *DeFi*-платформы для заимствования/кредитования и маржинальной торговли *BZx*. Лица получили кредит в размере 10 млн долларов в криптоактивах через экспресс-кредит, не внося при этом залога. Затем они провели эти средства через несколько протоколов *DeFi*. По сообщениям руководства организации, причиной стало раскрытие закрытого ключа к адресу с криптоактивами[16];

– модель «эксплойта кода». Эксплойт (англ. *exploit* – «эксплуатировать») кода представляет собой программу, использующую уязвимости *DeFi*-сервисов для совершения атак. С целью совершения хищения криптоактивов преступники находят уязвимости в смарт-контрактах и с их помощью выводят денежные средства с кошельков пользователей. В отдельных случаях они прибегают к совместному использованию эксплойтов и торговых ботов.

Так, в 2020 г. хакер украл криптовалютные активы на сумму около 24 млн долларов из службы децентрализованных финансов (*DeFi*) *Harvest Finance*. Он инвестировал большое количество криптовалютных активов в сервис, а затем использовал криптографический эксплойт, чтобы перекачать средства платформы на свои кошельки. *DeFi*-сервис признал, что атака произошла из-за уязвимости системы[17].

В ноябре 2022 г. *DeFi*-компания *Solend* пострадала от эксплойта в отношении оракулов ценообразования. Ее совокупные потери составили 1,26 млн долларов. Эксплойт был нацелен на стейблкоины *Hubble* (*USDH*) и затронул кредитные пулы *Stable*, *Coin98* и *Kamino*[18].

В октябре 2022 г. *Mango Markets* – *DeFi*-компания взаимного кредитования и трейдинга на базе блокчейна Солана – потеряла более 100 млн долларов из-за эксплойта, который манипулировал ценой *MNGO*[19];

– модель хакинга. Хакинг в *DeFi*-сервисах представляет собой противоправную модификацию либо смарт-контракта, либо его протокола.

В *DeFi*-отрасли прослеживается закономерность: чем дольше работает сервис, тем он безопаснее ввиду того, что разработчики сами устраняют программные ошибки.

Наибольшее количество хакинга в *DeFi* наблюдается при использовании межсетевых мостов. Они держат у себя большое количество токенов, при этом их протоколы, как правило, открыты. С одной стороны, открытость доказывает честность организаторов и отсутствие у них мошеннических намерений. С другой – подобрать ключи к протоколам таких сервисов гораздо проще, чем к защищенным криптобиржам. Все это обеспечивает блокчейн-мостам наивысший риск взлома и кражи. По оценкам экспертов, в результате 13 атак в августе 2022 г. злоумышленники похитили из межсетевых мостов криптовалюту на сумму $2 млрд, что составляет 69 % всех украденных криптоактивов в 2022 г.[20] За один только октябрь 2022 г. было взломано три моста и украдено почти 600 млн долларов[21].

***DeFi*-мошенничество**. Мошенничество в сфере децентрализованных финансов демонстрирует тревожную динамику роста во многом из-за увеличения капитализации *DeFi* и повышения их инвестиционной привлекательности.

---

[16] Around the Block #3: analysis on the bZx attack, DeFi vulnerabilities, the state of debit cards in crypto, and other crypto news. URL: https://www.coinbase.com/blog/around-the-block-analysis-on-the-bzx-attack-defi-vulnerabilities-the-state-of-debit-cards-in?__cf_chl_f_tk=.SdMzsbVHjA7w_VpmcsHIsGYrHqiuMLOd6CBbJjBKhc-1673089889-0-gaNycGzNCdE (дата обращения: 20.03.2023).

[17] Home Tech Security Hacker steals $24 million from cryptocurrency service «Harvest Finance». URL: https://www.zdnet.com/article/hacker-steals-24-million-from-cryptocurrency-service-harvest-finance/ (дата обращения: 20.03.2023).

[18] DeFi Protocol Solend Struck by $1.26M Oracle Exploit URL: https://www.coindesk.com/business/2022/11/02/defi-protocol-solend-struck-by-126m-oracle-exploit/ (дата обращения: 20.03.2023).

[19] Solana-Based Decentralized Finance Platform Mango Hit by $100 Million Exploit. URL: https://www.coindesk.com/business/2022/10/11/breaking-news-solana-based-decentralized-finance-platform-mango-hit-by-potential-100-million-exploit/ (дата обращения: 20.03.2023).

[20] Chainalysis says $2 bln stolen in cross-chain bridge hacks this year, more expected. URL: https://forkast.news/chainalysis-2-bln-cross-chain-bridge-hacks-rogue/ (дата обращения: 20.03.2023).

[21] China's Judicial Blockchain Platform Used to Store Evidence Sees 18% More Activity. URL: https://tokenist.com/chinas-judicial-blockchain-platform-used-to-store-evidence-sees-18-more-activity/ (дата обращения: 20.03.2023).

ISSN 2782-2923

По данным ФБР США, в 2021 г. общее количество жалоб, связанных с криптоактивами, сократилось примерно на 3 %, но при этом сумма убытков от мошенничества увеличилась на 600 %, с 246 млн долларов в 2020 г. до 1,6 млрд долларов США в 2021 г.[22]

Как правило, преступники используют следующие способы совершения мошенничеств:

– модель привлечения инвестиций в *DeFi*-проект. Мошенники вносят средства в пул ликвидности, привлекают новых инвесторов, увеличивают цену виртуального актива, погашают обязательства перед инвесторами первой очереди за счет вкладчиков второй очереди, а потом выводят активы при помощи вредоносного кодирования смарт-контракта.

Ярким примером финансовой *DeFi*-пирамиды является проект *Terra* с использованием токенов *Luna* (*LUNA*) и *TerraUSD* (*UST*). Автор проекта До Квон предложил покупателям *Terra* передать ему токены по договору займа под 20 % годовых. За несколько месяцев проект собрал 15 млрд долларов США. Когда инвесторы усомнились в надежности проекта, на рынке началось беспокойство и отток инвестиций. В итоге инвесторы потеряли деньги, а в отношении До Квона было возбуждено уголовное дело по факту мошенничества[23].

Еще один пример финансовой пирамиды приводится в докладе Казначейства США. В июне 2022 г. гражданину Вьетнама Ле Ань Туану предъявили обвинение в совершении мошенничества с использованием электронных средств связи. Туан с соучастниками создал проект *Daller Ape Club*, который продавал *NFT* в виде различных мультяшных фигурок. После того как фигурки были проданы, он завершил проект, удалил его веб-сайт и вывел деньги инвесторов[24];

– модель инвестирования на мошеннической инвестиционной платформе. На протяжении некоторого времени лица демонстрируют успешность инвестирования на платформе, привлекают новых пользователей и повышают доходность. Затем они предлагают разместить криптоактивы в новый прибыльный проект через приложение кошелька виртуальных активов, используют уязвимости кошелька и получают доступ ко всем привлеченным средствам.

Легализация преступных доходов с использованием *DeFi*. В настоящее время отмывание преступных доходов в *DeFi* является одним из этапов преступной деятельности, связанной с хищением криптоактивов.

DeFi-сервисы используются преступниками для запутывания транзакций перемещения и дробления преступных доходов и др.

Можно выделить несколько основных моделей легализации доходов в *DeFi*:

– модель использования децентрализованных бирж. Популярность данного способа легализации связана с тем, что децентрализованные биржи, в отличие от централизованных, не подпадают под контроль ФАТФ. Но вместе с тем они позволяют при желании отследить все транзакции, поскольку последние отражаются не в реестре биржи, а в смарт-контрактах. Чаще всего преступники прибегают к одновременному использованию децентрализованных бирж и миксеров. Преступные доходы размещаются на децентрализованных кошельках, затем обмениваются на биржах на другие токены. Последние депонируются на централизованных биржах и конвертируются в фиатную валюту;

– модель использования межсетевых мостов. Преступник отправляет криминальные токены на межсетевой мост и получает новые цифровые монеты. Позднее он обменивает их на стейблкоины *DeFi*, а их, в свою очередь, конвертирует на бирже. В случае применения данной модели внимание правоохранителей должен

---

[22] FBI, 2021 Internet Crime Report, (2021). URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (дата обращения: 20.03.2023).

[23] Kerner at Blockchain Coinvestors says Terra was a Ponzi strategy. URL: https://forkast.news/kerner-terra-ponzi-strategy-blockchain-coinvestors/ (дата обращения: 20.03.2023); Is Terra LUNA a Ponzi Scheme? How to Buy Terra LUNA 2022. URL: https://www.analyticsinsight.net/is-terra-luna-a-ponzi-scheme-how-to-buy-terra-luna-2022/ (дата обращения: 20.03.2023); Is Terra LUNA an Archetype of Ponzi Schemes? The Answer Lies in Its Timeline. URL: https://cryptonews.net/editorial/analytics/is-terra-luna-an-archetype-of-ponzi-schemes-the-answer-lies-in-its-timeline/ (дата обращения: 20.03.2023).

[24] Illicit Finance Risk Assessment of Decentralized Finance. URL: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (дата обращения: 20.03.2023).

ISSN 2782-2923

вызывать тот факт, что лицо часто получает токены с адресов, связанных с межсетевыми мостами, и не может объяснить причину этих транзакций.

Известен случай, когда один межсетевой мост использовался для отмывания доходов от программ-вымогателей, полученных от более чем 13 криминальных сервисов [17];

– модель использования *DeFi*-миксеров. Лицо получает преступным путем некоторые цифровые активы, отправляет их на адрес криптовалютного миксера и получает «чистые» токены, после чего переводит их на централизованную или децентрализованную биржу и конвертирует в фиатную валюту. В рамках рискориентированного подхода на такую схему легализации могут указывать: частое получение клиентом биржи входящих переводов от децентрализованных миксеров, совершение частых переводов с участием миксеров. В настоящее время преступники не ограничиваются миксерами, а дополняют схемы использованием децентрализованных обменных площадок, покупкой *NFT* и других криптоактивов.

В рамках настоящего исследования *DeFi*-преступность рассматривается как совокупность преступлений, совершаемых в сфере децентрализованных сервисов (бирж, платформ взаимного кредитования, страхования, управления, ликвидного стейкинга и др.) с использованием стейблкоинов, децентрализованных криптокошельков, межсетевых мостов и (или) оракулов. Мы намеренно оставляем за рамками исследования посягательства, опосредованно связанные с *DeFi*, но технологически не привязанные к этим сервисам.

По этому основанию к числу *DeFi*-преступлений сложно отнести вымогательство с использованием децентрализованных сервисов, поскольку сегодня вирусы-вымогатели существуют преимущественно в централизованных сервисах, а *DeFi* используются исключительно для перевода средств и запутывания цепочек транзакций.

Трудно отнести к рассматриваемому сегменту преступности и незаконный оборот наркотиков, поскольку сбыт наркотических средств, психотропных веществ и иных запрещенных предметов осуществляется в Даркнете и, как правило, не предполагает использование блокчейна. Равно как и в вымогательстве, *DeFi* используются здесь преимущественно для придания доходам легального характера.

Меры уголовно-правовой превенции *DeFi*-преступности

Вопрос об уголовно-правовой превенции преступлений, совершаемых в сфере децентрализованных финансов, в настоящее время не только не решен, но и должным образом не поставлен. Во многом это объясняется тем, что ни в России, ни в мире не проработан правовой статус *DeFi*-сервисов и не предложены алгоритмы квалификации преступлений, совершаемых с использованием этой технологии.

С некоторой долей условности можно говорить о наличии двух методологических подходов к правовому регулированию децентрализованных финансов, которые априори предопределяют тактическую направленность уголовной политики:

– технологически нейтральный подход. Он предполагает, что децентрализованные сервисы должны регулироваться в зависимости от того, какой продукт они представляют: «схожая деятельность – схожие риски – схожее регулирование»;

– технологически релевантный подход, напротив, ориентирован на максимальный учет технологических особенностей сервисов при максимально осторожных оценках самой возможности правового регулирования. Условно этот подход можно назвать «моделью регулирования Интернета», когда на начальных этапах он практически не регламентировался, а по мере «созревания» технологий под нормативный контроль стали попадать его отдельные продукты и проявления.

Если на начальных этапах появления *DeFi* большинство специалистов предпочитали второй подход, то в связи с развитием децентрализованной преступности все чаще обосновывается необходимость технологически нейтральной позиции.

В частности, Комиссия по биржам и ценным бумагам США (*SEC*) в 2023 г. открыто заявила о том, что регулирование ценных бумаг должно быть в полной мере распространено и на *DeFi*-сервисы, а децентрализованные криптовалютные биржи должны быть приравнены к традиционным биржам ценных бумаг.

ISSN 2782-2923

Это предложение привело к горячей дискуссии. В Интернете было обнародовано письмо в адрес Комиссии, в котором авторы отметили опасность проецирования права ценных бумаг на новый децентрализованный сектор и необходимость выработки специальных правил. SEC намерены изучить эти доводы, но пока их позиция остается прежней[25]. О нецелесообразности разработки специальных правил для *DeFi*-сферы говорится и в аналитическом отчете Министерства финансов США[26].

Менее категоричной является позиция европейского регулятора. В регламенте Европейского союза о рынках криптоактивов (*MiCA*), принятом Европейским парламентом 20 апреля 2023 г., не регулируются такие новые тренды, как децентрализованные финансы, *NFT* и оракулы. По мнению экспертов, все эти новые явления либо уже имеют регулирование, как в случае с секьюрити-токенами, либо обладают такие специфическими особенностями, что необходимо проводить их дальнейший анализ для настройки нормативно-правовой базы[27].

Интересную позицию по данному вопросу занимает ФАТФ. В Путевых правилах (*Travel Rules*) он подчеркивает, что финансовое регулирование не распространяется на программное обеспечение децентрализованных сервисов, а применяется к лицам, которые сохраняют контроль или достаточное влияние на протокол *DeFi*, предоставляющий услуги в сфере цифровых финансов[28]. Особенно это касается сервисов, имеющих элементы централизации. В частности, в Руководстве ФАТФ по цифровым активам 2021 г. определено, что создатели, владельцы, операторы и другие лица, сохраняющие контроль или влияние в протоколах *DeFi*, даже если эти механизмы кажутся децентрализованными, могут подпадать под определение *VASP* (компаний, оказывающих услуги в сфере цифровых активов), если они предоставляют услуги *VASP* или активно содействуют им[29].

Применительно к предупреждению *DeFi*-преступлений важно не только понимать, каков статус децентрализованных финансов, но и четко устанавливать субъекта уголовной ответственности. В этой связи интерес представляет позиция ФАТФ, согласно которой в качестве лица, несущего ответственность за преступления в сфере децентрализованных финансов, следует рассматривать владельца или оператора платформы. Таковыми могут признаваться лица, имеющие контроль или достаточное влияние на активы или работу протокола *DeFi*, а также осуществляющие деловые отношения между ними и пользователями, даже если эти связи строятся на основе смарт-контрактов или протоколов голосования. Если же речь идет об индивидуальном держателе токена, он, по мнению ФАТФ, не несет ответственности, если не осуществляет контроль или достаточное влияние на деятельность *VASP*.

С целью предупреждения преступлений, совершаемых в сфере децентрализованных финансов, ФАТФ предлагает более детально подходить к структуре сервиса. Если у *DeFi*-предприятия нет централизации и ответственного лица, государство может потребовать, чтобы регулируемый *VASP* участвовал в деятельности, связанной с механизмом *DeFi*, и отвечал за минимизацию рисков такого *DeFi*-сервиса[30].

Что же касается Российской Федерации, то и законодательные, и правоохранительные органы оказались не готовы к росту *DeFi*-преступности. Не ставя целью исследования анализ уголовно-правовых проблем

---

[25] SEC Reopens Comment Period for Proposed Amendments to Exchange Act Rule 3b-16 and Provides Supplemental Information. URL: https://www.sec.gov/news/press-release/2023-77 (дата обращения: 20.03.2023).

[26] DeFi Must Comply With Anti-Money Laundering Rules, US Says. URL: https://news.bloomberglaw.com/banking-law/defi-needs-to-comply-with-anti-money-laundering-rules-us-says (дата обращения: 20.03.2023).

[27] EU Markets in Cryptoassets (MiCA) Regulation: What is it and why does it matter? URL: https://www.bbva.com/en/innovation/eu-markets-in-cryptoassets-mica-regulation-what-is-it-and-why-does-it-matter/ (дата обращения: 20.03.2023).

[28] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf (дата обращения: 20.03.2023).

[29] Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. URL.: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 20.03.2023).

[30] URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата обращения: 20.03.2023).

ISSN 2782-2923

квалификации преступлений, совершаемых в сфере децентрализованных технологий, ограничимся лишь основными направлениями уголовно-правовой политики в этой сфере с обозначением ключевых проблем и задач.

Начать следует с того, что в российском законодательстве нет не только определения *DeFi*, но и приемлемой трактовки стейблкоинов, сетевых мостов, оракулов и др. Ученые высказывают различные точки зрения относительно легализации *DeFi*: от отрицания важности и полезности их регулирования до отождествления токенов *DeFi*-сервисов с криптовалютой и цифровыми правами [18, 19]. Но, как показывает практика, уголовно-правовая природа *DeFi*-преступлений имеет более сложную природу.

Следует начать с того, что ни в УК РФ, ни в судебной практике не выработаны сколько-нибудь приемлемые представления о том, что такое децентрализованные системы и каким образом могут быть определены входящие в них компоненты. В частности, отсутствует понимание оракулов и межсетевых мостов, нет четкой градации между криптовалютой и стейблкоинами, отсутствует алгоритм квалификации преступлений, связанных с администрированием криминальных децентрализованных сервисов [20–22].

В постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» содержится широкое понимание компьютерной информации как сведений, которые могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах либо на любых внешних электронных носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. При таком подходе сведения, содержащиеся в децентрализованных сервисах, могут подпадать под регулирование гл. 28 УК РФ «Преступления в сфере компьютерной информации» и рассматриваться в качестве предмета преступного посягательства.

Иначе наука и правоприменитель подходит к квалификации преступлений, предметом которых является криптовалюта, стейблкоин или иной криптоактив, обладающий стоимостью [23–29].

В настоящее время практика осторожно, но последовательно вырабатывает подход к признанию криптоактивов предметом хищений и других экономических преступлений. Начало этому процессу положило определение Шестого кассационного суда общей юрисдикции от 9 сентября 2020 г. № 7У-10543/2020. Суд указал, что размер похищенной криптовалюты может быть установлен на основании заключения эксперта, а сама криптовалюта является предметом хищения[31]. Это решение послужило началом формирования практики квалификации отдельных *DeFi*-преступлений по статьям гл. 21 и 22 УК РФ «Преступления против собственности».

Фактически можно говорить о том, что в России формируются два алгоритма квалификации преступлений, совершаемых в сфере децентрализованных финансов:

– если криптоактивы выступают предметом преступного посягательства против собственности, деяние квалифицируется по соответствующей статье гл. 21 УК РФ;

– если же *DeFi*-технологии выступают способом совершения преступлений, это подпадает под признак использования информационно-телекоммуникационных технологий.

Заключение

DeFi-преступность находится на начальном этапе своего развития, но уже обладает рядом устойчивых признаков, позволяющих рассматривать ее как относительно самостоятельное криминологическое явление. Ее выделяют четкая криминальная специализация преступников, техногенный характер преступлений, высокая степень технологической мимикрии, гибкость и адаптивность способов совершения посягательств, а равно постоянно растущий ущерб от посягательств при сокращении числа потенциальных потерпевших.

[31] Определение Шестого кассационного суда общей юрисдикции от 9 сентября 2020 г. № 7У-10543/2020 [77-1839/2020].

ISSN 2782-2923

Основными направлениями развития нового сегмента преступности являются *DeFi*-кражи, *DeFi*-мошенничества и легализация преступных доходов с использованием децентрализованных технологий.

В рамках разработки мер уголовно-правового противодействия *DeFi*-преступности приоритетное значение отдается технологически нейтральному направлению, позволяющему квалифицировать преступление, основываясь на продуктовой принадлежности сервиса, а не на его технологической природе. В рамках настоящего подхода принципиально важным являются следующие вопросы: кто осуществляет операционное управление сервисом, какими полномочиями обладает подписант *DeFi*-протокола и какие из совершенных действий могли охватываться его умыслом.

Список литературы

1. Децентрализованные финансы: информационно-аналитический доклад Банка России. URL: https://cbr.ru/Content/Document/File/141992/report_07112022.pdf

2. Алешина А. В., Булгаков А. Л. Воздействие финансовых технологий и децентрализованных финансов (DeFi) на угрозы инфраструктуре национальной экономики // Финансовые рынки и банки. 2023. № 1. С. 121–125.

3. Сидоренко Э. Л. Правовой статус децентрализованных финансов: к постановке проблемы // Lex Russica (Русский закон). 2023. № 76(3). С. 87–99. DOI: https://doi.org/10.17803/1729-5920.2023.196.3.087-099

4. Carter N., Jeng L. DeFi Protocol Risks: The Paradox of DeFi // SSRN Scholarly Paper. 2021. № 3866699. DOI: https://doi.org/10.2139/ssrn.3866699

5. The decentralized financial crisis / L. Gudgeon, D. Perez, D. Harz, A. Gervais, B. Livshits // In 2020 crypto valley conference on blockchain technology (CVCBT). IEEE, 2020. Pp. 1–15.

6. Factors Affecting the Adoption of Electronic Marketplaces: A Fuzzy AHP Analysis / H. Fu, Y. Ho, R.C.Y. Chen, T. Chang, P. Chien // International Journal of Operations & Production Management. 2006. № 26(12). С. 1301–1324. DOI: https://doi.org/10.1108/01443570610710560

7. Blockchain Smart Contracts: Applications, Challenges, and Future Trends / S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, A. Bani-Hani // Peer-to-Peer Networking and Applications. 2021. № 14(5). С. 2901–2925. DOI: https://doi.org/10.1007/s12083-021-01127-0

8. Ozili P. K. Decentralized finance research and developments around the world // J. Bank. Financ. Technol. 2022. № 6. С. 117–133. DOI: https://doi.org/10.1007/s42786-022-00044-x

9. Risk analysis in decentralized finance (DeFi): a fuzzy-AHP approach / S. Kaur, S. Singh, S. Gupta et al. // Risk Manag. 2023. № 25(13). DOI: https://doi.org/10.1057/s41283-023-00118-0

10. Non-Bank Financial Intermediaries and Financial Stability / S. Aramonte, A. Schrimpf, Hyun Song Shin // CEPR Discussion Paper No. DP16962. 2022. January. URL: https://ssrn.com/abstract=4026868

11. Financial Action Task Force. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. Paris, 2021. URL: www.fatf-gafi.org

12. IOSCO Decentralized Finance Report. Report of the Board of IOSCO. URL: https://www.dirittobancario.it/wp-content/uploads/2022/03/IOSCO-decentralized-finance-report.pdf

13. Assessment of Risks to Financial Stability from Crypto-assets, February. Financial Stability Board // FSB. 2022. URL: fsb.org

14. International Monetary Fund's global financial stability report October 2021: COVID-19, Crypto, and Climate: Navigating Challenging Transitions. URL: www.elibrary.imf.org

15. Crypto Crime Report. Chainalysis. 2022. URL: chainalysis.com.

16. Hilary J. Allen. DeFi: Shadow Banking 2.0? // American University Washington College of Law Research Paper. № 2022-02.

17. The State of Cross-Chain Crime // Elliptic. 2022, October 4. Pp. 26–27. URL: https://www.elliptic.co/resources/state-of-cross-chain-crimereport.

18. Криворучко С. В., Понаморенко В. Е. Тенденции международной практики контроля за оборотом цифровых активов в контексте политики ПОД/ФТ и антикоррупционной политики // Банковское право. 2023. № 1. С. 68–76.

19. Эволюция криптоэкономики и последние тренды децентрализованных финансов / А. Журавлев, Ю. Брисов, Р. Янковский, А. Левашенко // Банковское обозрение. 2020. № 10. С. 32–35.

20. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / С. В. Иванцов, Э. Л. Сидоренко, Б. А. Спасенников и др. // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 85–93.

21. Макарова О. А., Макаров А. Д. Состояние и перспективы развития цифрового законодательства // Актуальные проблемы экономики и права. 2021. № 15(1). С. 5–14. DOI: https://doi.org/10.21202/1993-047X.15.2021.1.5-14

ISSN 2782-2923

22. Перов В. А. Проблемные вопросы, возникающие при расследовании уголовных дел о преступлениях с использованием криптовалюты // Российский следователь. 2020. № 7. С. 20–22.

23. Пинкевич Т. В. Проблемы уголовно-правового противодействия преступной деятельности с использованием криптовалют // Юрист-Правоведъ. 2020. № 4. С. 45–48.

24. Русскевич Е. А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. № 10. С. 46–49.

25. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 106–125. DOI: https://doi.org/10.17323/2072-8166.2021.3.106.125

26. Сидоренко Э. Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. Т. 10, № 6. С. 147–154.

27. Сидоренко Э. Л. Криптовалюта как новый юридический феномен // Общество и право. 2016. № 2. С. 147–155.

28. Хисамова З. И. Использование цифровой платежной инфраструктуры для легализации преступных доходов: основные тренды // Russian Journal of Economics and Law. 2022. № 16(2). С. 370–378. DOI: https://doi.org/10.21202/2782-2923.2022.2.370-378

References

1. *Decentralized finance:* information-analytical report of the Bank of Russia. (2022). (In Russ.). https://cbr.ru/Content/Document/File/141992/report_07112022.pdf

2. Aleshina, A. V., & Bulgakov, A. L. (2023). The impact of financial technologies and decentralized finance (DeFi) on threats to the infrastructure of the national economy. *Finansovye rynki i banki*, *1*, 121–125. (In Russ.).

3. 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

4. Carter, N., & Jeng, L. (2021). DeFi Protocol Risks: The Paradox of DeFi. *SSRN Scholarly Paper*, 3866699. https://doi.org/10.2139/ssrn.38666991

5. Gudgeon, L., Perez, D., Harz, D., Gervais, A., & Livshits, B. (2020). The decentralized financial crisis. *In 2020 crypto valley conference on blockchain technology (CVCBT)* (pp. 1–15). IEEE.

6. Fu, H., Ho, Y., Chen, R.C.Y., Chang, T., & Chien, P. (2006). Factors Affecting the Adoption of Electronic Marketplaces: A Fuzzy AHP Analysis. *International Journal of Operations & Production Management*, *26*(12), 1301–1324. https://doi.org/10.1108/01443570610710560

7. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain Smart Contracts: Applications, Challenges, and Future Trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

8. Ozili, P. K. (2022). Decentralized finance research and developments around the world. *J Bank Financ Technol*, *6*, 117–133. https://doi.org/10.1007/s42786-022-00044-x

9. Saeed, N., Cullinane, K., Gekara, V. et al. (2021). Reconfiguring maritime networks due to the Belt and Road Initiative: impact on bilateral trade flows. *Marit Econ Logist*, *23*, 381–400. https://doi.org/10.1057/s41278-021-0019

10. Aramonte, S., Schrimpf, A., & Shin, H. S. (2022, January). Non-Bank Financial Intermediaries and Financial Stability. *CEPR Discussion Paper No. DP16962*. https://ssrn.com/abstract=4026868

11. Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris. www.fatf-gafi.org

12. *IOSCO Decentralized Finance Report. Report of the Board of IOSCO*. https://www.dirittobancario.it/wp-content/uploads/2022/03/IOSCO-decentralized-finance-report.pdf

13. Assessment of Risks to Financial Stability from Crypto-assets, February. Financial Stability Board. (2022). FSB. fsb.org

14. *International Monetary Fund's global financial stability report October 2021: COVID-19, Crypto, and Climate: Navigating Challenging Transitions*. www.elibrary.imf.org

15. Crypto Crime Report. (2022). Chainalysis. chainalysis.com..

16. Hilary, J. Allen. (2022). DeFi: Shadow Banking 2.0? *American University Washington College of Law Research Paper No. 2022-02.*

17. The State of Cross-Chain Crime. (2022, October 4) (pp. 26–27). *Elliptic*. https://www.elliptic.co/resources/state-of-cross-chain-crimereport

18. Krivoruchko, S. V., & Ponamorenko, V. E. (2023). Tendencies of the International Practice of Control over Circulation of Digital Assets within the Framework of the AML/CTF Policy and the Anti-Corruption Policy. *Banking Law*, *1*, 68–76. (In Russ.).

ISSN 2782-2923

19. Zhuravlev, A., Brisov, Yu., Yankovsky, R., & Levashenko, A. (2020). Evolution of cryptoeconomics and the recent trends of decentralized finance. *Banking review*, *10*, 32–35. (In Russ.).

20. 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.).

21. Makarova, O. A., & Makarov, A. D. (2021). Status and prospects of digital legislation development. *Actual Problems of Economics and Law*, *15*(1), 5–14. (In Russ.) https://doi.org/10.21202/1993-047X.15.2021.1.5-14

22. Perov, V. A. (2020). Challenging issues arising in the investigation of criminal cases on crimes committed with the use of cryptocurrency. *Rossiiskii sledovatel'*, *7*, 20–22. (In Russ.).

23. Pinkevich, T. V. (2020). Issues of the criminal-legal counteraction to criminal activity using cryptocurrency. *Yurist-Pravoved*, *4*, 45–48. (In Russ.).

24. Russkevich, E. A. (2018). Illegal access to computer information: theory and practice. *Sud'ya*, *10*, 46–49. (In Russ.).

25. Russkevich, E. A., & Malygin, I. I. (2021) Crimes Related to Cryptocurrencies: Features of Qualification. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, *3*, 106–125. (In Russ.). https://doi.org/10.17323/2072-8166.2021.3.106.125

26. Sidorenko, E. L. (2017). Criminological Risks of Crypto Currency Turnover. *Economica. Nalogi. Pravo*, *10*(6), 147–154. (In Russ.).

27. Sidorenko, E. L. (2016). Cryptocurrency as a new legal phenomenon. *Society and Law*, *2*, 147–155. (In Russ.).

28. Khisamova, Z. I. (2022). Using a digital payment infrastructure for criminal incomes legalization: main trends. *Russian Journal of Economics and Law*, *16*(2), 370–378. (In Russ.). https://doi.org/10.21202/2782-2923.2022.2.370-378

Конфликт интересов: автором не заявлен.
Conflict of Interest: No conflict of interest is declared by the author.

Дата поступления / Received 20.04.2023
Дата принятия в печать / Accepted 02.06.2023