УДК 658.14/.17 / 343.721

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В КРИПТОИНДУСТРИИ: ВИДЫ И ПРАВИЛА БЕЗОПАСНОСТИ

Стовбыра Т.В.,
ФГБОУ ВО «Оренбургский государственный педагогический университет», Оренбург,
email: till969@mail.ru

Аннотация. *Данная статья посвящена проблеме финансового мошенничества в криптоиндустрии. Рассматриваются актуальные тенденции и новые виды крипто мошенничества (их общие признаки и специфические характеристики), которые злоумышленники используют для обмана инвесторов и владельцев криптовалют. Особое внимание уделено способам предотвращения крипто мошенничества и правилам безопасности, которые помогут избежать попадания в ловушки мошенников. Описываются правила противодействия мошенническим схемам, указывается необходимость обучения финансовой грамотности для предотвращения потерь, подчеркивается необходимость осторожности, осмотрительности при работе с криптовалютами, а также внимательного отношения к собственным финансовым решениям. В целом, данный материал призван сделать читателей более осведомленными и защищенными в мире криптовалютных операций, помогая им избежать попадания в ловушки мошенников, и сохранить свои средства в безопасности.*

Ключевые слова: финансовое мошенничество, крипто мошенничество, правила безопасности при работе с криптоактивами, криптокошелек, криптопирамида, фишинг, фейковые стартапы и фейковые ICO/IDO, фейковые криптобиржи, мошенничество в P2P-торговле, мошенничество в майнинге.

FINANCIAL FRAUD IN THE CRYPTO INDUSTRY: TYPES AND SECURITY RULES

Stovbyra T.V.,
Federal State Budgetary Educational Institution of Higher Education «Orenburg State Pedagogical University», Orenburg,
email: till969@mail.ru

Abstract. *This article is devoted to the problem of financial fraud in the crypto industry. Current trends and new types of crypto fraud (their general features and specific characteristics) that attackers use to deceive investors and owners of cryptocurrencies are considered. Particular attention is paid to ways to prevent crypto fraud and security rules that will help avoid falling into the traps of scammers. The rules for countering fraudulent schemes are described, the need for financial literacy training to prevent losses is indicated, and the need for caution and prudence when working with cryptocurrencies, as well as careful attention to one's own financial decisions, is emphasized. Overall, this material is intended to make readers more aware and protected in the world of cryptocurrency transactions, helping them avoid falling into the traps of scammers and keeping their funds safe.*

Keywords: financial fraud, crypto fraud, safety rules when working with crypto assets, crypto wallet, crypto pyramid, phishing, fake startups and fake ICO/IDO, fake crypto exchanges, P2P trading fraud, mining fraud.

Изучение видов финансового мошенничества в криптоиндустрии является необходимым для обеспечения безопасности, защиты интересов участников рынка, развития регулирования и поддержания положительной репутации индустрии.

С появлением криптовалют и блокчейн-технологий рынок стал более доступным для широкой публики. Однако этот быстрый рост также привлекает мошенников, которые пытаются использовать недостатки и слабости в системе для собственной выгоды. Изучение типов финансового мошенничества поможет выявить такие схемы и предпринять меры по их предотвращению. Криптовалюты предоставляют возможность осуществления анонимных и непрозрачных транзакций, что делает их привлекательными для мошенников. Отсутствие централизованного контроля и персональных идентификационных данных облегчает совершение преступлений, включая отмывание денег, финансирование терроризма и другие незаконные действия.

Инвесторы и участники криптовалютного рынка часто сталкиваются с мошенническими схемами, такими как Ponzi-схемы, фишинг, кражи средств и прочее. Понимание видов и типов финансового мошенничества помогает инвесторам остерегаться опасных ситуаций и принимать разумные решения при инвестировании. Волатильность криптовалютного рынка и его высокий уровень спекуляции создают благоприятные условия для различных мошеннических схем, таких как пирамиды и фальшивые ICO. Инвесторы, стремящиеся быстро обогатиться, часто становятся жертвами мошенников, привлекаемых ложными обещаниями и высокими доходами.

Изучение видов финансового мошенничества в криптоиндустрии способствует повышению уровня безопасности в сфере криптовалют и блокчейна. Оперативное распознавание мошеннических схем позволяет разрабатывать эффективные меры защиты, улучшать системы финансового контроля и предотвращать угрозы для безопасности участников рынка. Блокчейн и криптовалютные технологии не лишены технических уязвимостей, которые могут быть использованы злоумышленниками для совершения мошенничества. Утечки персональных данных, взлом криптовалютных бирж, фишинг, вирусы и другие киберугрозы создают угрозы для безопасности пользователей криптовалют.

Недостаточное или отсутствие регулирования криптовалютного рынка оставляет простор для действий мошенников. Отсутствие четких правил и нормативов облегчает создание финансовых пирамид, разнообразных псевдоинвестиционных схем, а также уклонение от уплаты налогов и декларирования полученных доходов. Знание типов финансового мошенничества помогает законодателям и регуляторам разрабатывать более эффективные правовые механизмы для борьбы с преступными схемами в сфере криптовалют. Правильное понимание проблемы позволит создать новые и улучшить существующие формальные ограничения, закрепленные в законодательных документах, которые помогут минимизировать риски финансового мошенничества и защитят в будущем участников рынка.

Многие участники криптовалютного рынка не имеют достаточной финансовой грамотности и понимания принципов функционирования криптовалют и работы с ними, что делает их уязвимыми перед мошенниками. Часто отсутствие знаний и опыта приводит к потере средств при участии в мошеннических схемах.

Отметим также, что мошенничество и преступная деятельность в криптоиндустрии могут нанести серьезный ущерб репутации всей отрасли и подорвать доверие к цифровым активам. Изучение видов финансового мошенничества и борьба

с ними способствуют поддержанию положительного имиджа криптовалют и блокчейна как инновационных технологий.

Все перечисленные выше факторы в совокупности создают благоприятную почву для финансового мошенничества на криптовалютном рынке. Развитие регулирования, повышение финансовой грамотности участников рынка, а также совершенствование технических мер безопасности могут помочь бороться с этим явлением.

Цель исследования

Целью исследования выступает классификация и характеристика современных видов финансового мошенничества на криптовалютном рынке, в частности, и криптоиндустрии в целом. Описание современных способов финансового мошенничества в криптовалютной сфере позволит определить и разработать наиболее эффективные превентивные меры, базовые правила безопасности работы с криптоактивами, а также методы борьбы с крипто мошенничеством.

Предмет, объект и методы исследования

Предметом исследования выступают виды финансового мошенничества в криптоиндустрии, в том числе разнообразные схемы и техники, а также правила безопасности при работе с цифровыми активами.

Объект исследования – криптовалютный рынок и криптовалютная индустрия в целом.

Исследование видов финансового мошенничества в криптоиндустрии осуществлялось с применением следующих методов и подходов: анализ данных, экспертные оценки, кейс-стади, интервью с потерпевшими, анализ зарубежной судебной практики.

Использование методов анализа данных, включая статистические методы и программные инструменты, для изучения характеристик и закономерностей мошеннических схем в криптовалютной среде, позволяет выявить типичные признаки финансового мошенничества и определить их типологию.

Изучение экспертных оценок и проведение опросов экспертов в области криптовалют и финансового рынка способствуют выявлению новых типов финансового мошенничества, с которыми они сталкиваются, а также поиску, разработке и совершенствованию методов их предотвращения.

Изучение судебных дел и решений (к сожалению, в основном зарубежных), связанных с мошенническими схемами в криптовалютной сфере направлено на выявление типов преступлений, схем и практик, используемых крипто мошенниками.

Применение кейс-стади предполагает изучение конкретных случаев финансового мошенничества в криптовалютной сфере для выявления типов схем и подходов, используемых преступниками, а также для анализа их хода и последствий.

Кроме того, в качестве исследовательского метода был использован метод интервьюирования потерпевших, что дает возможность выявления типичных сценариев действий мошенников и определения оптимальных превентивных мероприятий.

Указанные методы исследования использованы как отдельно, так и в комбинации друг с другом для более полного и комплексного анализа проблемы типологии финансового мошенничества в криптовалютной индустрии.

Результаты и их обсуждение

Бурное развитие криптовалютного рынка закономерно привело к увеличению случаев финансового мошенничества в данной сфере, злоумышленники постоянно ищут новые способы обмана. Появление криптовалютных аферистов вызвано, в частности, недостаточной осведомлённостью рядовых граждан и новоявленных криптоинвесторов о принципах функционирования криптовалют, специфики работы блокчейна и о методах защиты от мошенников. Ущерб от криптовалютного мошенничества действительно значительный. В отчете компании Chainalysis данный ущерб за последние годы оценивается в миллиарды долларов, и, согласно прогнозам, данная тенденция будет прослеживаться и в дальнейшем [1].

Основные виды крипто мошенничества можно разделить на две базовые категории:

- получение доступа к техническим устройствам (гаджетам), цифровому криптокошельку / депозиту на криптобирже или учетным данным аутентификации, таким как: секретные пароли, сид-фразы, коды безопасности и пр.
- получение криптовалюты напрямую от владельца, посредством выдачи себя за другое лицо и прямого обмана владельца, использование мошеннических инвестиционных проектов, финансовых пирамид, поддельных, фиктивных деловых возможностей или иных сомнительных мошеннических схем [2].

Стоит отметить, что существуют и иные виды мошенничества, отличные от указанных категорий, либо, наоборот, совмещающие их характеристики; они активно используются киберпреступниками для обмана пользователей криптовалют и получения незаконной выгоды от них. Пользователям и владельцам криптовалют необходимо проявлять осторожность и осмотрительность, важно уделять часть времени обучению, повышать свою финансовую грамотность: изучать основные характеристики криптовалют и принципы функционирования криптобирж, потенциальные риски и угрозы криптоиндустрии, а также следовать определённым правилам безопасности при работе с цифровыми активами, чтобы избежать участи жертвы крипто мошенников, поскольку предупреждён – значит вооружен.

Рассмотрим подробнее наиболее распространенные виды финансового мошенничества, попутно описывая элементарные правила безопасности при работе с криптоактивами. Начнем с первой категории, когда злоумышленники пытаются получить доступ к устройствам, цифровым кошелькам, аккаунту на криптобирже или конфиденциальной информации.

Наиболее распространенной схемой, неоднократно проверенной и усовершенствованной на традиционных финансовых активах, выступает фишинг. Явление фишинга является серьезной угрозой для пользователей сети Интернет, поскольку злоумышленники активно используют эту схему для получения доступа к конфиденциальным данным, таким как логины и пароли. Фишеры создают поддельные веб-сайты и криптокошельки, которые часто выглядят практически идентичными оригинальным, вводя пользователей в заблуждение [3]. Для того чтобы избежать стать жертвой подобных атак, важно быть бдительным и следовать основным правилам безопасности в сети:

1. Внимательно проверять URL-адрес сайта, на который осуществляется переход, особенно если это биржа криптовалют. Избегать ввода конфиденциальных данных на подозрительных ресурсах.

2. Не переходить по подозрительным ссылкам от незнакомых пользователей в социальных сетях и мессенджерах.

3. Распределять свои криптовалютные активы между горячими и холодными кошельками для повышения безопасности.

4. Как дополнительная мера предосторожности, целесообразно сохранить информацию для входа на биржу в записных книжках или хранилище паролей, чтобы уменьшить риск их утраты в следствие фишинговых атак.

Аккуратность и внимательность – вот ключи к защите собственных криптовалютных средств от возможных угроз фишинга в Интернете.

Не менее опасны взломы криптовалютных / мультивалютных кошельков, которые представляют серьезную угрозу для сохранности цифровых активов пользователя. Мошенники активно используют различные методы, чтобы получить доступ к средствам на кошельках, в том числе через поддельные приложения, подозрительные ссылки или уязвимости в безопасности [4]. Чтобы минимизировать риск стать жертвой взлома криптокошелька, важно соблюдать несколько ключевых мер безопасности:

Всегда загружать приложения для работы с криптокошельками только с официальных и проверенных источников. Избегать использования сторонних и неизвестных источников, чтобы избежать установки вредоносных программ.

Обращать внимание на репутацию разработчика кошелька и его надежность. Проверять, имеются ли рекомендации по безопасности на официальном сайте.

Использовать сложные и уникальные пароли для доступа к кошелькам, и регулярно их менять. Двухфакторная аутентификация также поможет повысить уровень безопасности кошелька.

Обязательно сохранять seed-фразу (код восстановления) на бумаге или в другом надежном месте, не публиковать её в Интернете и никому не сообщать. Это ключевой элемент для доступа к личным активам в случае утери пароля или других проблем.

Безопасность цифрового кошелька напрямую зависит от соблюдения правил безопасности и предосторожности. Не стоит забывать следить за безопасностью своих аккаунтов, личных данных и активности в сети, чтобы избежать потерь и осложнений, связанных с взломом кошелька.

Поддельные приложения, связанные с криптовалютами, несут отдельную угрозу для инвесторов, поскольку они могут быть использованы мошенниками также для кражи цифровых активов и личной информации. Этот метод обмана особенно опасен, поскольку мошенники часто создают поддельные приложения, которые выглядят очень похоже на официальные, таким образом соблазняя пользователей скачать их, более того, мошенникам удается их размещать в известных магазинах приложений, таких как Google Play и Apple App Store [4].

Чтобы не стать жертвой поддельных криптовалютных приложений важно соблюдать ряд мер предосторожности:

1. Загружать приложения только с официальных сайтов. Перед загрузкой удостовериться, что приложение имеет множество положительных отзывов и хороший рейтинг.

2. Быть внимательным к деталям приложения, таким как название разработчика, дата публикации, количество загрузок и т.д. Поддельные приложения часто имеют отличия от официальных версий.

3. Не размещать конфиденциальную информацию, такую как данные аккаунта, пароли или seed-фразы, через поддельные приложения, поскольку официальные никогда не попросят раскрывать подобные данные.

В современном цифровом мире важно быть очень осторожным и бдительным в отношении загрузки приложений и обращения с личной информацией.

Ещё одним хитрым и эффективным способом кражи криптовалюты становятся «пылевые атаки», основанные на невнимательности и ложной уверенности пользователей. Этот вид атаки нацелен на кошельки с большими суммами цифровых активов и может принести мошенникам значительные выгоды за счет манипуляции с адресами и отправкой незначительных сумм криптовалюты.

Для реализации «пылевой атаки» злоумышленники создают фальшивый кошелек, адрес которого очень похож на адрес потенциальной жертвы. Это позволяет им отправлять незначительные суммы криптовалюты на фейковый адрес, чтобы он отразился в истории транзакций жертвы. Затем мошенники рассчитывают на то, что пользователь совершит ошибку и отправит более значительные суммы на фейковый адрес, думая, что это адрес получателя [3].

Для предотвращения «пылевых атак» пользователи криптовалют должны быть особенно внимательными при проведении транзакций. Важно всегда проверять адрес получателя несколько раз, убеждаясь в его точности и легитимности. Также стоит избегать восприятия незначительных поступлений на кошелек как безопасных и не загружать подозрительные адреса, даже если они похожи на обычный адрес. Важной мерой безопасности является обучение и информирование пользователей о таких видах атак, чтобы они могли быть готовы к ним и способны защитить свои средства.

Кражи с криптобирж, взломы аккаунтов и потери крупных сумм криптовалют являются серьезной угрозой для всей индустрии криптовалюты. Как показывают примеры взломов, таких как нападения на Coincheck, BitGrail, Binance, Zaif и многих других, хакеры постоянно ищут уязвимости в системах бирж и аккаунтах пользователей, чтобы получить доступ к цифровым активам. Одним из наиболее важных способов защиты от подобных атак является обеспечение безопасности своего аккаунта. Важно использовать надежные и сложные пароли, которые сложно подобрать, а также активировать двухфакторную аутентификацию, чтобы обеспечить дополнительный уровень защиты. Также стоит торговать на проверенных и надежных биржах, которые имеют хорошую репутацию и принимают меры по обеспечению безопасности пользователей. Не стоит хранить все свои средства на бирже, лучше использовать комбинацию горячих и холодных кошельков, чтобы минимизировать потенциальные потери в случае взлома [5].

Вторая категория финансового мошенничества связана с получение криптовалюты или фиатных активов напрямую от владельца, к ней относятся многочисленные виды мошеннических схем и инструментов. Криптопирамиды являются крайне опасными схемами, которые маскируются под инновационные инвестиционные проекты, но на самом деле представляют из себя мошеннические схемы, преследующие цель обогащения их организаторов на деньгах новых участников. Эти схемы ведут к обману многих людей, часто приводят к большим финансовым потерям и разрушению доверия к криптовалютной индустрии в целом. Основные признаки криптопирамид включают отсутствие информации о создателях проекта, неясность в предлагаемом продукте или услуге, недостаток прозрачности в структуре и меха-

низмах работы схемы, постоянную необходимость привлечения новых участников для обеспечения выплат и недавнюю регистрацию компании с небольшим уставным капиталом. Все эти характеристики могут служить признаками того, что вы имеете дело с криптопирамидой, а не с серьёзным инвестиционным проектом [6].

OneCoin и Finiko – это примеры финансовых пирамид, которые обманывали людей, привлекая их средства под видом инвестиций в криптовалюту. По сути, они предлагали схему быстрой и легкой прибыли, но на самом деле являлись мошенническими проектами, цель которых – обогащение создателей за счет доверчивых инвесторов. OneCoin, стартовавшая в 2014 году, позиционировала себя как аналог биткоина, но на самом деле была финансовой пирамидой, в которую по оценкам были вложены значительные средства. Майнинг OneCoin мог проводиться только компанией-организатором, что уже является красным флагом для инвесторов. Finiko, в свою очередь, стала известна в России как финансовая пирамида, обещающая инвестирование в криптовалюту и фондовые рынки. Оценки ущерба от ее деятельности и количество пострадавших вкладчиков свидетельствуют о том, что многие люди попали в ловушку этого мошеннического проекта [6].

Фейковые криптовалютные инвестиционные фонды получили довольно широкое распространение в криптоиндустрии и представляют собой очередную угрозу даже для опытных инвесторов, так как они обманывают людей, предлагая им быструю и легкую прибыль, но на деле не выполняют свои обещания. Это может привести к финансовым потерям и разочарованию [7].

Во избежание подобных ситуаций важно придерживаться нескольких основных правил. Во-первых, необходимо быть реалистичными и не попадаться на обещания огромных прибылей без рисков. Инвестиции всегда сопряжены с определенным уровнем риска, и предложения о стабильных высоких доходах за короткий срок часто являются слишком хорошими, чтобы быть правдой. Во-вторых, проводить тщательное исследование фонда, прежде чем переводить туда свои средства. Просмотреть отзывы и рейтинги фонда, узнать больше о его руководстве и команде, проверить наличие лицензий и регистрацию. Также необходимо уделить время изучению инвестиционного плана, чтобы понять, как работает фонд, какие инвестиции предлагаются и какую доходность обещают: чем более прозрачен и понятен инвестиционный план, тем меньше вероятность обмана. Кроме того, не стоит забывать об изучении медиа и пресс-релизов фонда, чтобы оценить общественное мнение о нем. Доверие к ресурсу также играет важную роль в принятии решения о вложении средств.

Фейковые стартапы и фейковые ICO/IDO являются распространенной проблемой в криптомире из-за его относительной новизны и недостаточной регулировки. Мошенники используют эти схемы для привлечения средств под ложными обещаниями, а затем могут исчезнуть, украв деньги у вкладчиков. Инвестиции в ICO или IDO могут быть прибыльными, но также несут существенные риски, особенно при работе с неизвестными или сомнительными проектами [6]. Для того чтобы избежать столкновения с фейковыми стартапами, важно придерживаться следующих рекомендаций.

Прежде всего, необходимо тщательно изучить проект, в который вы собираетесь инвестировать. Обратите внимание на состав команды проекта: их профессиональный опыт, наличие профилей в социальных сетях и LinkedIn. Это позволит оценить доверие к проекту и его реальные перспективы. Также важно изучить

Whitepaper проекта – документ, который представляет собой детальное описание идеи, технологий, схемы распределения токенов и другие важные аспекты. Если Whitepaper составлен грамотно и содержит информацию, подкрепленную фактами, это уже хороший знак. Необходимо также оценить репутацию проекта на других ресурсах: изучить обзоры, отзывы и мнения экспертов в криптовалютном сообществе. Подобные исследования помогут понять, насколько проект реально заслуживает доверия и является ли он надежным. И последнее, но не менее важное – оценить перспективность идеи проекта: насколько она оригинальна, нужна рынку криптовалют и какие преимущества она предлагает. Инвестировать стоит только в проекты, которые имеют реальный потенциал и инновационный подход.

С появлением множества криптовалютных бирж, которые предлагают пользователям привлекательные условия без необходимости прохождения процедуры верификации, возникает риск столкнуться с нечестными площадками – фейковыми криптобиржами или скам биржами. Эти недобросовестные биржи могут обещать анонимность, специальные бонусы и акции для привлечения клиентов, но на самом деле преследуют цель обмануть и захватить средства пользователей, исчезнув внезапно [7]. Для того чтобы избежать подобных негативных сценариев, важно прежде всего проводить тщательный анализ репутации и надежности криптобиржи, изучать отзывы других пользователей, а также обращаться к профессиональным обзорам. Также рекомендуется распределять свои криптовалютные средства по разным биржам, не хранить все в одном месте, и отдавать предпочтение известным и проверенным платформам.

Следующим важным феноменом, на который стоит обратить внимание, являются скам-монеты, которые анонсируются на рынке с обещаниями быстрого роста и большого потенциала, но которые в итоге оказываются ничем не обоснованными и подверженными манипуляциям со стороны мошенников. Приобретая такие монеты, пользователи рискуют лишиться своих средств, так как не смогут вывести их обратно на свой кошелек из-за различных ограничений и манипуляций [6]. Чтобы избежать столкновения с скам-монетами, стоит руководствоваться несколькими важными правилами: внимательно изучать информацию о новых криптовалютах, не доверять слишком громким обещаниям доходности, проверять репутацию и реальные данные о разработчиках проекта, а также обращаться к достоверным источникам информации.

Финансовое мошенничество активно процветает в популярных мессенджерах и соцсетях, наиболее часто используемые: Telegram, Twitter, VK, Discord.

Pump & Dump («накачка и сброс») – это давно известная схема, которая применяется мошенниками для личной выгоды за счет недопущения инвесторов. Они создают иллюзию взрывного роста актива, привлекают вложения инвесторов, после чего резко сбрасывают цену, приводя к потере для тех, кто не успел выйти из сделки. Это безответственное поведение, которое портит репутацию рынка криптовалют. Такие схемы могут быть особенно опасными для начинающих инвесторов, которые еще не имеют достаточного опыта и знаний о рынке. В свою очередь, использование подобных каналов не только вредит инвесторам, но и наносит ущерб доверию криптовалютному сообществу в целом [4].

Для того чтобы избежать столкновения с подобными мошенничествами, важно проявлять трезвость ума и разумное отношение к инвестициям. Нельзя слепо доверять неизвестным и высокорисковым активам, а также вкладывать все средства

в один проект. Диверсификация портфеля поможет снизить риски и защитить средства от возможных потерь.

Фейковые телеграм-каналы могут представлять собой подделку известных бирж или проектов, либо предлагать платные / бесплатные торговые сигналы. В любом случае, злоумышленники используют ложные сведения и манипуляции, чтобы обмануть доверчивых пользователей. Мошенники создают иллюзию сходства с официальными каналами, притягивают внимание и подписчиков, а затем начинают распространять мошеннические схемы, такие как фальшивые розыгрыши призов или запросы на передачу личных данных. Для того чтобы избежать столкновения с подобными псевдо-каналами, важно сохранять бдительность и внимательно анализировать любую предлагаемую информацию. Нельзя передавать свои личные данные или ключи от кошельков третьим лицам, особенно через ненадежные и подозрительные каналы. Необходимо проверять каналы и их происхождение, убеждаясь во взаимодействии с официальными и проверенными ресурсами.

Фейковые телеграм-каналы, предлагающие платные подписки на торговые сигналы, зачастую обещают быструю и высокую прибыль. Однако за такими обещаниями могут стоять умышленно ложные сигналы, которые приводят к финансовым потерям для инвесторов [7]. Для того, чтобы избежать попадания в ловушку торговых мошенников, важно обладать знаниями основ крипторынка и трейдинга, а также проводить достаточное исследование перед принятием инвестиционных решений. Проверять достоверность информации, уделять внимание прозрачности действий и принимать решения об инвестировании только на основе проверенных данных и фактов.

В соцсетях и мессенджерах мошенники могут использовать личные сообщения, предлагать доверительное управление криптоактивами, осуществлять фейковые консультации, предлагать якобы «инсайдерскую» информацию о криптоактивах, действовать через взломанные аккаунты известных личностей, предлагать вакансии в криптоиндустрии, завлекать легким заработком, искать жертв на сайтах знакомств и пр. [8]. Перечисленные виды мошенничества составляют далеко не полный перечень реальных и действенных схем мошенничества.

Отдельного внимания заслуживает мошенничество в P2P-торговле (криптовалютные обменники). P2P-торговля предполагает обмен фиатными и криптовалютами напрямую между пользователями. Данный способ был весьма популярен в период с 2011 по 2018 годы, когда рынок криптовалют только начал свое активное развитие и привлекал большое внимание участников. Несмотря на обилие криптобирж и обменников, некоторые пользователи предпочитают пользоваться ими [9]. Однако важно понимать, что на P2P-платформах существует значительное число мошеннических схем. Злоумышленники, действующие в сфере обмена криптовалют на P2P-платформах, чаще всего пытаются использовать доверчивость и невнимательность пользователей в своих целях. Они могут предложить соблазнительный курс обмена, существенно ниже рыночного, чтобы привлечь жертву, а затем либо украсть ее средства, либо осуществить обмен по гораздо менее выгодному курсу, чем было заявлено изначально. Для защиты собственных финансов необходимо выбирать только надежные и защищенные обменники, изучая их репутацию и оценки других пользователей. Важно также уделять внимание категории надежности и безопасности обменников, чтобы уменьшить риск стать жертвой мошенничества.

Фейковые SMS-сообщения, предположительно от банков, являются одним из распространенных методов мошенничества, направленных на пользователей криптовалютных платформ. Этот вид аферы строится на доверии пользователей к подобным сообщениям и может привести к серьезным финансовым потерям. При получении подобного SMS с уведомлением о платеже или пополнении на счет, пользователи должны проявлять крайнюю осторожность и не принимать такие сообщения на веру. Важно помнить, что банки и финансовые учреждения не отправляют подобные уведомления через SMS, особенно когда речь идет о криптовалютных операциях.

Схемы с привлечением третьих лиц или «треугольник». В данной схеме злоумышленник обманывает пользователей двух различных платформ: P2P-платформы и онлайн-барахолки (например, «Авито»). Он предлагает пользователю P2P-платформы обменять криптовалюту на фиатные деньги. Параллельно создает ложное объявление на онлайн-барахолке о продаже товара и убеждает потенциального покупателя отправить задаток, предоставив ему реквизиты первого пользователя с P2P-платформы. Когда пользователь P2P-платформы получает задаток, он отправляет криптовалюту злоумышленникам, после чего мошенник исчезает. В результате пользователь онлайн-барахолки теряет деньги, которые перевел в виде задатка, а пользователь P2P-платформы лишается криптовалюты, указанной в сделке [10].

Еще одной значимой проблемой в криптоиндустрии выступает мошенничество в майнинге, которое ставит под угрозу безопасность и финансовые интересы пользователей. Существуют различные виды мошеннических схем, связанных с облачным и оборудованным майнингом криптовалют. В облачном майнинге злоумышленники могут предлагать услуги с фальшивыми данными о доходности или оказывать некачественные услуги, что в итоге лишает пользователей обещанных доходов или приводит к потере средств. Продажа фальшивого или некачественного оборудования для майнинга также является распространенной схемой мошенничества. Мошенники могут выдавать себя за представителей известных фирм или продавать оборудование, которое не соответствует заявленным характеристикам. Это может привести к финансовым потерям пользователей, так как, либо они получают не работающее оборудование, либо сталкиваются с исчезновением мошенников после предоплаты или полной оплаты оборудования [7].

Во избежание подобных ситуаций крайне важно проверять репутацию компании, с которой планируется сотрудничество в области майнинга. Также стоит провести сравнение предложений различных компаний и быть бдительными, если цена услуг или оборудования значительно ниже среднерыночной стоимости. Осторожность и осмотрительность помогут избежать многих проблем и защитить финансовые активы от мошеннических схем в мире криптовалют и майнинга.

Выводы

Мошенничество в сфере криптовалют является серьезной проблемой, и очень важно знать общие признаки различных видов крипто мошенничества для того, чтобы не стать их жертвой. Некоторые из этих признаков включают спешку и ограниченность во времени, обещание сверхвысокой доходности за короткие сроки, навязчивую рекламу, плохую репутацию проекта и непрозрачность.

Для предотвращения крипто мошенничества важно следовать ряду рекомендаций. В частности, важно постоянно увеличивать свою осведомленность о криптова-

лютах, блокчейне и криптобиржах, быть внимательным и подвергать всё сомнению и анализу. Рекомендуется проверять репутацию проекта, рисковать малым, хранить средства на холодных кошельках, пользоваться проверенными сервисами и изучать доступную информацию о проекте. Кроме того, важно не переходить по незнакомым ссылкам, не поддаваться эмоциям и всегда принимать решения с холодной головой.

Криптовалютный рынок постоянно развивается, и злоумышленники также совершенствуют свои мошеннические схемы. Они могут играть на эмоциях, неопытности и неосведомленности пользователей, придумывая все новые и изощренные способы. Поэтому важно быть бдительным и следовать описанным правилам, чтобы избежать неприятных ситуаций и минимизировать потери.

Литература

1. The 2024 State of Cryptocurrency Investigations Report. Global survey insights on government agencies crypto outlook. Chainalysis. [Электронный ресурс]. URL: https://go.chainalysis.com/rs/503-FAP-074/images/The%202024%20State%20of%20Cryptocur rency%20Investigations%20Report.pdf (дата обращения: 03.07.2024).

2. Семь случаев мошенничества с криптовалютой. Bybit. [Электронный ресурс]. URL: https://learn.bybit.com/ru/investing/crypto-scams/ (дата обращения: 03.07.2024).

3. Фомин Д. Эирдропы, фишинг и фейковые токены. Как теряют миллионы в криптовалюте // РБК-Крипто, 27 мая 2024. [Электронный ресурс]. URL: https://www.rbc.ru/crypto/news/6654699e9a79474d6f5f1aef (дата обращения: 03.07.2024).

4. Как не стать жертвой мошенничества с криптовалютой. [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/cryptocurrency-scams (дата обращения: 03.07.2024).

5. Крупнейшие взломы криптобирж с 2014 по 2024 год. [Электронный ресурс]. URL: https://profinvestment.com/largest-cryptocurrency-exchange-hacks/ (дата обращения: 03.07.2024).

6. Васильева Л. Что такое скам в криптовалюте // Портал Банки.Ру. [Электронный ресурс]. URL: https://www.banki.ru/news/daytheme/?id=10979400 (дата обращения: 21.06.2024).

7. Симагин А. Двадцать семь распространенных способов мошенничества в криптовалюте: как не стать жертвой. [Электронный ресурс]. URL: https://vc.ru/crypto/829077-27-rasprostranennyh-sposobov-moshennichestva-v-kriptovalyute-kak-ne-stat-zhertvoi (дата обращения: 09.07.2024).

8. Беляков Е. «Им верят люди небогатые и несут последние деньги»: Пять самых популярных способов обмана на криптовалюте // Комсомольская правда, 21 ноября 2023. [Электронный ресурс]. URL: https://www.kp.ru/daily/27583/4854253/ (дата обращения: 09.07.2024).

9. Стовбыра Т.В. Криптовалюта: способы получения // Наука и образование: актуальные проблемы естествознания и экономики. Международная научно-практическая конференция. Оренбург, 24 марта 2023 г. / Министерство просвещения Российской Федерации, ФГБОУ ВО «ОГПУ». Оренбург, 2023. С. 542-548.

10. Петров И. На коин чёрт: как россиян обворовывают через криптобиржи // Известия, 11 мая 2024. [Электронный ресурс]. URL: https://iz.ru/1693779/ivan-petrov/na-koin-chert-kak-rossiian-obvorovyvaiut-cherez-kriptobirzhi (дата обращения: 09.07.2024).