**УДК 33** **Экономические науки**

***Селин Александр Петрович,*** *кандидат экономических наук, доцент, ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна», г. Санкт-Петербург*

# ПРОБЛЕМА КИБЕРМОШЕННИЧЕСТВА НА КРИПТОВАЛЮТНОМ РЫНКЕ

**Аннотация:** в настоящей статье рассматривается тематика кибермошенничества на рынке криптовалют. Обосновывается актуальность тематики – даются комментарии относительно текущей популярности криптовалют, приводятся некоторые статистики. Кратко перечисляются главные проблемы криптовалютного рынка, а затем внимание акцентируется на кибермошенничестве.

**Ключевые слова:** криптовалюта, рынок, кибермошенничество, проблемы.

**Abstract:** this article deals with the topic of cyber fraud in the cryptocurrency market.

The relevance of the topic is justified - comments are given on the current popularity of cryptocurrencies, some statistics are given. The main problems of the cryptocurrency market are briefly listed, and then the attention is emphasized on cyber fraud.

**Keywords:** cryptocurrency, market, cyber fraud, problems.

## 1. Криптовалюты на современном этапе развития рынка

В последние годы криптовалюты приобрели значительную популярность. Если вначале они представляли исключительно нишевый интерес для осведомленных специалистов, то теперь они охватили более широкую аудиторию, привлекая частных лиц, предприятия и даже институциональных

инвесторов. Глобальное распространение криптовалют неуклонно растет, и в настоящее время миллионы людей по всему миру владеют и пользуются различными цифровыми валютами. Такие крупные криптовалюты, как Bitcoin и Ethereum, получили широкое признание и даже были интегрированы в традиционные финансовые системы.

Существуют следующие факты об использовании криптовалюты:

- более 85% американских компаний, занятых в сфере торговли, видят внедрение криптовалют в качестве платёжного средства как один из приоритетов;

- торговые компании, уже принимающие платежи в криптовалюте, отчитываются, что, благодаря этому нововведению им удалось добиться рентабельности инвестиций (ROI) на уровне более 300%, а также нарастить темпы привлечения новых клиентов на 40%;

- удалось нарастить и показатели прибыли, так как клиент, рассчитывающийся в криптовалюте, в среднем, платит на 250 долларов больше в пересчёте на транзакцию, нежели обычный клиент [4].

По другим данным, 40% в возрасте от 18 до 35 лет заявили, что планируют расплачиваться криптовалютами в ближайшем будущем. Еще 10% заявили, что будут делать это регулярно.

Ежемесячный объем платежей в криптовалютах подбирается к цифре в 1 млрд. долларов [5].

Криптовалюты постепенно внедряются в различных странах мира, используются для оплаты товаров, услуг, оплаты пожертвований и прочего. При этом, разумеется, это пока не универсальное средство оплаты – воспользоваться им можно только в определённых местах. Таким образом, по удобству криптовалюты значительно уступают традиционным популярным валютам, таким как доллар или евро. Причины здесь, во многом, кроются в проблемах, которыми сопровождается развитие криптовалютного рынка.

## 2. Некоторые проблемы криптовалютного рынка. Проблема кибемошенничества

Первая проблема, о которой упоминает практически любой исследователь

– это волатильность. Цены на криптовалюты исторически волатильны, они быстро растут и падают. Достаточно взглянуть на график котировок любой криптовалюты, чтобы понять, о чём идёт речь. Сильные колебания не только от месяца к месяцу, но даже иногда и от дня к дню – обычное явление даже для таких известных валют, как биткоин.

Приведём пример. В мае 2021 года цена Ethereum превысила 4 000 долларов. К июлю 2021 года цена упала до уровня чуть ниже 1800 долларов. По состоянию на 10 декабря 2021 года цена вернулась к отметке 4 000 долларов США, что ниже исторического максимума ноября 2021 года - 4 858,52 доллара. Более мелкие валюты, такие как Dogecoin, могут испытывать еще более резкие колебания.

Вторая проблема – криптовалюты чрезвычайно сложно поддаются регулированию [2]. Суть заключается в том, что на рынке криптовалют нет своего регулятора (центрального банка), нет контролирующих органов. Рынок децентрализован и характеризуется почти полным отсутствием на нём государства.

Третья проблема, приобретающая в связи со второй проблемой особую остроту – киберпреступность и кибермошенничество. Автор особенно отмечает эти проблемы, поскольку крипторынок имеет репутацию спекулятивного рынка; а, кроме того, в отсутствие регулирующих органов, противодействовать мошенникам сложно.

Динамика кибермошенничества выглядит неутешительно – в частности, А.В. Бердышев, Ю.Н. Коровкина, В.Д. Сергеева отмечают рост кибермошенничества в России в 2021 году на 180% по сравнению с 2019 годом [1]. Растущая киберпреступность характерна не только для России – так, Google в 2021 году обнаружил свыше 2,1 млн. фишинговых сайтов, что на 27% превышает показатель 2020 года. При этом, аналитики Cyberverse-curity Ventures считают, что ежегодный ущерб от киберпреступности будет находиться на уровне 10,5 трлн. долларов США к 2025 году [6].

Наиболее популярный метод кибермошенничества – это последующее

хищение цифровых финансовых активов пользователя. Но методы, которыми может осуществляться это хищение, могут быть весьма изощренными.

Одним из методов является «pump&dump» (буквально – накачать и сбросить). Мошенник выбирает не очень популярный крипто-токен, который стоит дёшево, и разными способами начинает подогревать к нему интерес. Цена токена резко растёт, участники рынка скупают его в надежде на прибыль. При этом, рост не обусловлен никакими фундаментальными причинами – только спекуляциями кибермошенника. Затем мошенник продаёт по выросшей цене скупленные ранее по дешёвке токены. В результате, цены на актив резко обваливаются (иногда за несколько секунд). Классический пример «pump&dump» - криптовалюта e-coin, с которой произошла в точности такая же история (сначала рост на 10 000%, а затем обвал на 100%). Подобные методы давно признаны мошенническими на фондовом рынке, но крипторынок не так хорошо регулируется, как классический фондовый рынок. Поэтому среди кибермошенников такой метод мошенничества весьма популярен.

Далее, существует метод «Rug Pull» (буквально – вытягивание коврика). Этот метод очень похож на предыдущий с той лишь разницей, что криптомошенниками являются разработчики криптовалюты. В этом случае мошенники осознанно создают криптовалюту с единственной целью её дальнейшей спекулятивной раскрутки и собственного обогащения. При этом, разработчики могут вводить лимиты на продажу, чтобы защититься от метода «pump&dump». Пример – валюта SQUID GAME. На начальном этапе размещения цифровая монета продавалась по $0,01 за штуку. На следующий день на торгах ее цена поднялась до $7,7. Перед выводом средств мошенниками стоимость Squid составляла уже $2861 за штуку. Активная продажа разработчиками токенов спровоцировала снижение стоимости Squid до $0,003. По различным оценкам в общей сложности доходность мошенников составила 2,1-3,38 млн $ [1].

Наиболее традиционная схема кибермошенничества – фишинг. Фишинг – это вид киберпреступлений, при котором злоумышленники, маскируясь под

надежные организации, получают конфиденциальную информацию от ничего не подозревающих жертв. Фишинговые атаки обычно заключаются в отправке поддельных электронных писем, сообщений или веб-сайтов, которые представляются сообщениями от легитимных компаний или организаций. Цель атаки - обманом заставить человека сообщить свою личную информацию, например, учетные данные, номера кредитных карт или номера социального страхования.

Фишинг наносит большой ущерб доверчивым пользователям и иногда приводит к крупным финансовым потерям.

До сих пор речь велась об отдельных случаях мошенничества со стороны конкретных недобросовестных участников рынка. Но мошенничество на крипторынке может принимать и гораздо более серьёзный масштаб.

В этой связи стоит привести в пример крах крупной криптовалютной биржи FTX в конце 2022 года. Это событие имело огромный масштаб и колоссальные последствия в контексте крипторынка – биржа владела крупными капиталами, ущерб понесли многие пользователи (минимум 1 млрд. долларов клиентских средств был потерян) [3]. Причина краха оказалась достаточно проста и заключалась в махинациях основателей биржи, преследовавших корыстные мотивы личного обогащения. По мнению многих экспертов, крах FTX – это мощнейший удар по репутации крипторынка в целом. Это болезненные последствия, поскольку репутация этого рынка ещё не сформировалась, а критики, утверждавшие, что криптовалюты – это всего лишь спекулятивный инструмент, могли лишь убедиться в правильности своей позиции.

## 3. Противодействие кибермошенничеству в контексте развития рынка криптовалют

Кибермошенничество – серьёзная угроза для развития криптовалютного рынка, препятствующая формированию доверия инвесторов к данному рынку и регулярно наносящая пользователям рынка крупный финансовый ущерб.

Противодействие кибермошенничеству – одна из важнейших задач, решение которой будет способствовать динамичному развитию криптовалют и, к

примеру, более быстрой их интеграции в платёжные системы. Дело в том, что кибермошенничество на крипторынке в текущих масштабах – следствие отсутствия на этом рынке государства и недостаточного контроля и регулирования криптовалютного рынка со стороны государственных органов.

В этой связи целесообразно будет установление над криптовалютным рынком контроля, аналогичного традиционному фондовому рынку. Это сразу решит ряд проблем, связанных с теми или иными схемами мошенничества (такими как «pump&dump»).

Следует понимать, что киберпреступность на криптовалютном рынке может выступать первопричиной всех остальных проблем – в частности, легко проследить прямую связь между кибермошенничеством на криптовалютном рынке и волатильностью криптовалют, ведь одно порождает другое.

Криптовалютный рынок, как и любой другой рынок, взаимосвязан – шоки, случающиеся с одной из криптовалют, могут ударить по другим криптовалютам и по рынку в целом.

Поэтому мошеннические действия в отношении одной валюты могут спровоцировать скачки курсов других валют крипторынка, и на деле, ущерб от подобных действий будет намного серьёзнее.

Крипторынку будет полезен не только государственный законодательный контроль и регулирование, но и упорядочение самой работы криптовалютного рынка. Операции с криптовалютой, к примеру, могут осуществляться только в привязке к банковскому счёту клиента. Это, во-первых, поможет идентифицировать пользователя, а во-вторых, поспособствует безопасности и защищенности транзакций.

Такие меры, разумеется, не встретят однозначной поддержки у участников криптовалютного рынка, так как некоторыми из них именно отсутствие государства на данном рынке рассматривается как основное преимущество. Но, как мы видим на примере кибермошенничества, отсутствие государства на рынке выливается в масштабные финансовые махинации, наносящие огромный ущерб пользователям и дестабилизирующие рынок. Притом, часто эти махинации

остаются безнаказанными. По мнению автора, криптовалютный рынок не сможет преодолеть свою неблагонадежную, спекулятивную репутацию без прихода государства и ужесточения регулирования.

**Заключение**

Кибермошенничество названо серьёзной проблемой криптовалютного рынка, которая, зачастую, может являться первопричиной ряда других проблем, таких как волатильность.

Во многом, такая проблема связана с отсутствием должного контроля за развитием крипторынка и отсутствием регулирования.

Решение, почти наверняка, лежит в плоскости установления государственного законодательного регулирования над криптовалютным рынком.

**Библиографический список:**

1. Бердышев А.В., Коровкина Ю.Н., Сергеева В.Д. Кибермошенничество в сфере криптовалют // Финансовые рынки и банки. 2023. №1. URL: https://cyberleninka.ru/article/n/kibermoshennichestvo-v-sfere-kriptovalyut (дата обращения: 19.09.2023).

2. Левин Л.Л. Актуальные проблемы регулирования оборота криптовалют в Российской Федерации // Государственная служба. 2021. №5 (133). URL: https://cyberleninka.ru/article/n/aktualnye-problemy-regulirovaniya-oborota-kriptovalyut-v-rossiyskoy-federatsii (дата обращения: 19.09.2023).

3. Милькова А. Как крах биржи FTX изменит крипторынок: отвечают эксперты, 24.11.2022 // Банки.ру. URL: https://www.banki.ru/news/daytheme/?id=10976085 (дата обращения: 19.09.2023).

4. Global Crypto Adoption // Triple-A. URL: https://triple-a.io/crypto-ownership-data/ (дата обращения: 19.09.2023).

5. Houlgrave J. (2022). 5 stats that show what consumers think about crypto payments // Checkout. URL: https://www.checkout.com/blog/what-consumers-think-about-crypto-payments (дата обращения: 19.09.2023).

6. The universe of cyber risks of 2021 sample: methods of management and relief: [Electronic resource] // PLUS Journal No. 4 (280). - Available at: https://plusworld.ru/journal/2021/ plus-4-2021/vselennaya-kiberriskov-obraztsa-2021 -metody-upravleniya-i-kupirovaniya/ (last viewed on 19.09.2023).