УДК 004.056.52

П.В. Бабак [1], Т.К. Кириллова[1], И.Е. Пинин [1]
[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

БЕЗОПАСНОСТЬ КРИПТОВАЛЮТ

Аннотация. В данном исследовании авторы фокусируются на описании угроз безопасности криптовалютных платформ. Выполнен обзор уязвимостей, которые могут быть обнаружены на криптовалютных биржах, кошельках и смарт-контрактах. Задача исследования заключается в понимании механизмов, на которых эти платформы основаны, а также определения возможных проблем, связанных с ними. В фокусе исследования находятся уязвимости к атакам типа «51%», фишингу и социальной инженерии. Кроме того, исследование включает рекомендаций по улучшению безопасности системы, на основе результатов проведенных исследований. Результаты исследования будут полезны разработчикам, пользователям и регуляторам криптовалютных платформ, что особенно важно в свете участившихся случаев взломов и мошенничества в криптоиндустрии.

Ключевые слова: *криптовалюта, уязвимость, криптовалютная биржа, криптокошелек, смарт-контракт, «атака51%», фишинг, социальная инженерия, блокчейн.*

P.V. Babak [1], T.K. Kirillova [1], I.E. Pinin[1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

CRYPTOCURRENCY SECURITY

Abstract. In this study, the authors focus on describing the security threats of cryptocurrency platforms. An overview of vulnerabilities that can be found on cryptocurrency exchanges, wallets and smart contracts has been performed. The aim of the study is to understand the mechanisms on which these platforms are based, as well as to identify possible problems associated with them. The study focuses on vulnerabilities to attacks such as "51%", phishing and social engineering. In addition, the study will include the proposal of recommendations for improving the security of the system, based on the results of the conducted research. The results of the study will be useful to developers, users and regulators of cryptocurrency platforms, which is especially important in light of the increasing cases of hacking and fraud in the crypto industry.

Keywords: *cryptocurrency, vulnerability, cryptocurrency exchange, crypto wallet, smart contract, «51% attack», phishing, social engineering, blockchain.*

Введение. Криптовалюты, основанные на технологии блокчейн [1], стремительно ворвались в мир финансов, предлагая новые возможности для транзакций, инвестиций и создания децентрализованных систем. Вместе с тем, стремительный рост популярности криптовалют сопровождается увеличением числа киберугроз, направленных на эксплуатацию уязвимостей в этой новой и сложной экосистеме.

Данное исследование посвящено анализу безопасности криптовалютных платформ [3-4], сфокусированном на выявлении уязвимостей, присущих криптовалютным биржам, кошелькам и смарт-контрактам. Актуальность исследования обусловлена участившимися случаями взломов и мошенничества в криптоиндустрии [2], что приводит к значительным финансовым потерям и подрывает доверие к криптовалютам как к надежному инструменту.

Целью исследования является глубокое понимание механизмов, лежащих в основе функционирования криптовалютных платформ, а также идентификация потенциальных уязвимостей, связанных с ними. Особое внимание будет уделено анализу следующих угроз:

- атаки 51%: Исследование рассмотрит возможность реализации атак 51% на различные криптовалюты, оценивая вероятность таких атак и их потенциальные последствия;
- фишинг: будут проанализированы распространенные методы фишинга, используемые злоумышленниками для кражи криптовалют, и предложены рекомендации по защите от них;
- социальная инженерия: Исследование рассмотрит тактики социальной инженерии,

применяемые для получения доступа к криптовалютным активам, и предложит меры противодействия.

В работе рассмотрены сервисы децентрализованных финансов и атаки на эти сервисы. На основе сопоставления достоинств, недостатков и ограничений к применению для существующих решений, ряд авторов делают выводы о перспективах развития систем распределенного реестра, обеспечивающие конфиденциальность транзакций [15]. На основании полученных оценок предложены рекомендации по снижению рисков от угроз воздействия крипто вымогателей [17]. Полученные результаты могут быть применены для противодействия компьютерным преступлениям на корпоративные информационные системы.

Защита криптовалют, проблемы и решения. В целях исследования данной темы рассмотрим несколько статей от экспертов данной области. А далее представим свои исследования в данной области.

«Единственное, что стоит между злоумышленниками и вашей криптовалютой – установленные вами степени безопасности. Некоторые люди думают, что хакеру нет смысла атаковать конкретно их, но это не значит, что нужно легкомысленно относиться к защите. Зачастую злоумышленники атакуют не кого-то определенного, а сразу массу людей. А если случится потеря денег, то никто не сможет их вам вернуть. Эксперты Profinvestment изучили тему и подготовили ряд советов по безопасному хранению монет в некастодиальных кошельках, основываясь на собственном опыте и известных правилах [5]».

Предлагаемые решения:

- владелец криптовалютного кошелька должен быть единственным, кто имеет доступ к своим цифровым активам. Это подразумевает безопасное хранение приватного ключа и резервной фразы;
- аппаратные (холодные) кошельки считаются одними из самых безопасных для хранения криптовалют, поскольку они не подключены к интернету и, следовательно, менее подвержены хакерским атакам;
- горячие кошельки (мобильные, десктопные, веб), хотя и обеспечивают удобство доступа к цифровым активам в любое время, более подвержены риску взлома по сравнению с оффлайн кошельками;
- бумажные кошельки – другой вид оффлайн-хранения, где ключи для доступа к цифровым активам хранятся на бумаге. Они могут быть утеряны или уничтожены, поэтому важно хранить их в безопасном месте;
- некоторые пользователи предпочитают хранить свои цифровые активы на биржах, но это большой риск, биржа может стать жертвой взлома или заблокировать аккаунт по каким-то свои соображениям;
- владелец кошелька должен регулярно обновлять программное обеспечение и устанавливать надежные пароли/PIN-коды. Некоторые приложения позволяют ставить биометрическую защиту;
- наконец, следует знать о фишинговых атаках и других видах скама в криптоиндустрии [4].

«Лучший способ защиты биткоинов и других цифровых активов от кражи - хранить приватные ключи в холодном кошельке. Холодные кошельки не подключены к Интернету или даже другому устройству. Ни одно устройство хранения данных не является на 100% безопасным, но есть несколько методов, которым можно воспользоваться для защиты ключей от криптовалюты [6]».

Предлагаемые решения:

- холодные кошельки, также называемые холодным хранилищем, являются лучшим способом обезопасить ваши приватные ключи от биткоинов;
- некоторые биржи предоставляют безопасное холодное хранение ключей пользователей на институциональном уровне, но некоторые критики советуют отказаться от этого метода;

- некоторые биржи имеют страховку от кражи криптовалюты при определенных обстоятельствах, но охватываемые инциденты очень ограничены;
- совмещение использования холодного и горячего кошельков, чтобы в подключенном кошельке была только криптовалюта, которая необходима в данный момент [6].

«Защита криптовалюты — необходимость любого пользователя. В настоящее время криптовалюта является привлекательным предметом воровства для хакеров. Для защиты своих средств необходимо быть предельно внимательными и следовать простым правилам».

Предлагаемые решения:

- для повседневных нужд рекомендуется использовать небольшую сумму. Распределение средств между несколькими депозитариями, сводит к нулю возможность кражи всех средств за один раз;
- создавать резервную копию кошелька. Хранение резервной копии криптокошелька позволит восстановить его в случае выхода компьютера из строя, а также если ваш мобильный телефон был украден;
- использование надежного пароля, а также офлайн-кошельки. Последние считаются наиболее надежными, так как позволяют хранить криптовалюту без выхода в интернет [7]. Таким образом, кошелек не может быть взломан злоумышленниками.

Анализ наиболее популярных уязвимостей. В данном разделе проведем анализ трех ключевых уязвимостей, характерных для криптовалютной сферы в виде таблицы:

Таблица 1.

Классификация уязвимостей

№	Уязвимость	Определение уязвимости	Основа уязвимости	Примеры атак	Методы защиты
1	Атака 51%	Ситуация, в которой злоумышленник или группа злоумышленников получают контроль над 51% вычислительной мощности сети блокчейна [11].	Криптовалюты с низким хешрейтом, такие как Bitcoin Gold, Verge, Ethereum Classic, наиболее уязвимы к атаке 51%.	В марте 2022 года хакеры взяли под контроль пять из девяти проверяющих узлов сайдчейна, связанного с эфириумом. Хакеры подделали вывод из сети 56.25 миллиардов рублей [8].	Proof-of-Work (PoW) - наиболее распространенный механизм защиты от атак 51% [12]. Proof-of-Stake (PoS) и Delegated Proof-of-Stake (DPoS) - альтернативные механизмы консенсуса, где влияние пользователей на сеть определяется количеством монет [13].
	Фишинг	Вид кибератаки, целью которой является получения конфиденциальных данных пользователя.	Злоумышленники используют различные уловки для введения пользователей в заблуждение.	2022 год - «год утечек». За год общий объем выставленных на продажу или размещенных в открытом доступе данных россиян превысил 2,8 терабайта [9].	-Распознавание фишинговых сайтов и писем (проверка доменных имен, ссылок, грамматики и т.д.). Использование антивирусного ПО.

	Социальная инженерия	Совокупность приемов манипуляций человеком или группой людей с целью получения выгоды [14].	Злоумышленники используют различные психологические тактики.	В 2023 году мошенники выманили у GlowToken LLC сумму около 22,5 млн. руб [10].	Повышение осведомленности пользователей о тактиках социальной инженерии. Обучение сотрудников компаний.

Анализируя таблицу 1, приведем основные методы защиты от уязвимостей в криптосфере, в виде рисунка 1.

Рисунок 1. Методы защиты криптовалюты от различных уязвимостей

Заключение. В настоящем исследовании были рассмотрены ключевые уязвимости, присущие криптовалютной сфере, такие как атака 51%, фишинг и социальная инженерия. Анализ выявил, что, несмотря на растущую популярность и внедрение передовых технологий в индустрии криптовалют, существуют серьезные риски, связанные с безопасностью криптовалютных платформ.

Результаты исследования показали, что атака 51% представляет значительную угрозу для многих криптовалют, особенно для тех, которые имеют низкий хешрейт и децентрализованы в меньшей степени. Фишинг и социальная инженерия активно используются злоумышленниками для кражи криптовалютных активов, эксплуатируя человеческие слабости, такие как доверчивость, жадность и невнимательность.

В рамках данной работы были предложены эффективные методы защиты от выявленных уязвимостей. Обзор практических работ показал, что для предотвращения атак

51% рекомендуется использовать механизмы консенсуса, такие как Proof-of-Stake и Delegated Proof-of-Stake, а также стремиться к более равномерному распределению вычислительной мощности в сети. Для борьбы с фишингом и социальной инженерией необходимо повышать осведомленность пользователей, использовать надежные технические средства защиты и строго следовать протоколам безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Н. Федосеев, А. Патрушева. «Связанные одной цепочкой: как блокчейн защищает данные» // URL: https://practicum.yandex.ru/blog/chto-takoe-blokchain-i-kak-eto-rabotaet (дата обращения: 24.05.2024).
2. А. Брисколини, «Все о криптоиндустрии за 30 минут. История Blockchain, стратегии заработка, криптоценность Bitbon» // URL: https://www.youtube.com/watch?v=_cHAyBueGiw (дата обращения: 24.05.2024).
3. А.Пасютина, «Криптовалюта» // URL: https://secrets.tinkoff.ru/glossarij/kriptovalyuta/ (дата обращения: 24.05.2024).
4. С.Воробей, «Лучшие криптовалютные платформы и площадки: ТОП-25 криптоплатформ в 2024». // URL: https://profinvestment.com/cryptocurrency-trading-platforms/ (дата обращения: 24.05.2024).
5. С.Воробей, «Защита криптовалютного кошелька от взлома: 19 рекомендаций и способов для безопасного использования криптовалют» // URL: https://profinvestment.com/cryptocurrency-wallet-protection/ (дата обращения: 24.05.2024).
6. Н.Райфф, «Защитите свои биткоины от кражи и взлома». // URL: https://www.investopedia.com/tech/ways-protect-your-bitcoin-investment-against-theft-and-hacks/ (дата обращения: 24.05.2024).
7. А.Макаров, «Как защитить свои криптовалютные активы». // URL: https://www.anti-malware.ru/practice/solutions/how-protect-your-cryptocurrency-assets (дата обращения: 26.05.2024).
8. Атака 51%: что нужно знать об этом? // URL: https://dzen.ru/a/Y-VSVwAcr0_3oLaz (дата обращения: 26.05.2024).
9. На крючке: как изменился фишинг в 2022 году и на что мошенники ловили своих жертв, // URL: https://habr.com/ru/companies/solarsecurity/articles/708694/ (дата обращения: 26.05.2024).
10. В. Кодолова, «Пострадавший от мошенников основатель Glow Token потребовал компенсации от Crypto.com». // URL: https://bits.media/postradavshiy-ot-moshennikov-osnovatel-glow-token-potreboval-kompensatsii-ot-crypto-com/ (дата обращения: 26.05.2024).
11. «Атака 51%», // URL: https://academy.binance.com/ru/articles/what-is-a-51-percent-attack
12. «Что такое Proof of Work (PoW)?» //URL: https://academy.binance.com/ru/articles/proof-of-work-explained (дата обращения: 26.05.2024).
13. «Что такое социальная инженерия?». // URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 26.05.2024).
14. С.Погудин, «Хешрейт простыми словами». // URL: https://www.finam.ru/publications/item/kheshreyt-prostymi-slovami-20230922-1909/ (дата обращения: 26.05.2024).
15. Помогалова А.В., Донсков Е.А., Котенко И.В. Децентрализованные финансовые сервисы: общий алгоритм атаки. // URL: https://elibrary.ru/item.asp?id=49265247 (дата обращения: 26.05.2024).
16. Запечников С.В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций. // URL: https://elibrary.ru/item.asp?id=44365097 (дата обращения: 26.05.2024).

17. Сердечный А.Л., Скогорева Д.А., Длинный Е.П., Ле Т.Ч., Чьеу Д.В. Сердечный А.Л. Картографическое исследование blockchain-транзакций и смарт-контрактов киберпреступников, атакующих автоматизированные информационные системы, и оценка ущербов от реализации их атак // Информационная безопасность. 2021. Т. 24. ВЫП. 4. С. 471-500. URL: https://elibrary.ru/item.asp?id=48158181 (дата обращения: 26.05.2024).

REFERENCES

1. N. Fedoseev, A. Patrusheva. «Svyazannye odnoj cepochkoj: kak blokchejn zashchishchaet dannye» // URL: https://practicum.yandex.ru/blog/chto-takoe-blokchain-i-kak-eto-rabotaet (data obrashcheniya: 24.05.2024).
2. Briskolini, «Vse o kriptoindustrii za 30 minut. Istoriya Blockchain, strategii zarabotka, kriptocennost' Bitbon» // URL: https://www.youtube.com/watch?v=_cHAyBueGiw (data obrashcheniya: 24.05.2024).
3. A.Pasyutina, «Kriptovalyuta» // URL: https://secrets.tinkoff.ru/glossarij/kriptovalyuta/ (data obrashcheniya: 24.05.2024).
4. S.Vorobej, «Luchshie kriptovalyutnye platformy i ploshchadki: TOP-25 kriptoplatform v 2024». // URL: https://profinvestment.com/cryptocurrency-trading-platforms/ (data obrashcheniya: 24.05.2024).
5. S.Vorobej, «Zashchita kriptovalyutnogo koshel'ka ot vzloma: 19 rekomendacij i sposobov dlya bezopasnogo ispol'zovaniya kriptovalyut» // URL: https://profinvestment.com/cryptocurrency-wallet-protection/ (data obrashcheniya: 24.05.2024).
6. N.Rajff, «Zashchitite svoi bitkoiny ot krazhi i vzloma». // URL: https://www.investopedia.com/tech/ways-protect-your-bitcoin-investment-against-theft-and-hacks/ (data obrashcheniya: 24.05.2024).
7. A.Makarov, «Kak zashchitit' svoi kriptovalyutnye aktivy». // URL: https://www.anti-malware.ru/practice/solutions/how-protect-your-cryptocurrency-assets (data obrashcheniya: 26.05.2024).51% Attack: What do you need to know about it? https://changelly.com/blog/51-percent-attack/
8. Ataka 51%: chto nuzhno znat' ob etom? // URL: https://dzen.ru/a/Y-VSVwAcr0_3oLaz (data obrashcheniya: 26.05.2024).
9. Na kryuchke: kak izmenilsya fishing v 2022 godu i na chto moshenniki lovili svoih zhertv, // URL: https://habr.com/ru/companies/solarsecurity/articles/708694/ (data obrashcheniya: 26.05.2024).
10. V. Kodolova, «Postradavshij ot moshennikov osnovatel' Glow Token potreboval kompensacii ot Crypto.com». // URL: https://bits.media/postradavshiy-ot-moshennikov-osnovatel-glow-token-potreboval-kompensatsii-ot-crypto-com/ (data obrashcheniya: 26.05.2024).
11. «Ataka 51%», // URL: https://academy.binance.com/ru/articles/what-is-a-51-percent-attack
12. «Chto takoe Proof of Work (PoW)?» //URL: https://academy.binance.com/ru/articles/proof-of-work-explained (data obrashcheniya: 26.05.2024).
13. «Chto takoe social'naya inzheneriya?». // URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (data obrashcheniya: 26.05.2024).
14. S.Pogudin, «Heshrejt prostymi slovami». // URL: https://www.finam.ru/publications/item/kheshreyt-prostymi-slovami-20230922-1909/ (data obrashcheniya: 26.05.2024).
15. Pomogalova A.V., Donskov E.A., Kotenko I.V. Decentralizovannye finansovye servisy: obshchij algoritm ataki. // URL: https://elibrary.ru/item.asp?id=49265247 (data obrashcheniya: 26.05.2024).
16. Zapechnikov S.V. Sistemy raspredelennogo reestra, obespechivayushchie konfidencial'nost'

tranzakcij. // URL: https://elibrary.ru/item.asp?id=44365097 (data obrashcheniya: 26.05.2024).
17. Serdechnyj A.L., Skogoreva D.A., Dlinnyj E.P., Le T.Ch., Ch'eu D.V. Serdechnyj A.L. Kartograficheskoe issledovanie blockchain-tranzakcij i smart-kontraktov kiberprestupnikov, atakuyushchih avtomatizirovannye informacionnye sistemy, i ocenka ushcherbov ot realizacii ih atak // Informacionnaya bezopasnost'. 2021. T. 24. VYP. 4. S. 471-500. URL: https://elibrary.ru/item.asp?id=48158181 (data obrashcheniya: 26.05.2024).

Информация об авторах

Бабак Павел Вячеславович – студент 1 курса кафедры «Информационные системы и защита информации», направления подготовки «Информационная безопасность», Иркутский государственный университет путей сообщения, pasha.babak.3000@gmail.com

Кириллова Татьяна Климентьевна – заведующий кафедрой «Информационные системы и защита информации», доцент, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: kirillova_tk@irgups.ru

Пинин Илья Евгеньевич - студент 1 курса кафедры «Информационные системы и защита информации», направления подготовки «Информационная безопасность», Иркутский государственный университет путей сообщения, ilapinin@gmail.com

Information about the authors

Babak Pavel Vyacheslavovich – 1st year student of the Department "Information Systems and Information Protection", training area "Information Security", Irkutsk State University of Railway Engineering, pasha.babak.3000@gmail.com

Kirillova Tatiana Klimentevna – Head of the ISiZI Department, Associate Professor, Irkutsk State University of Railway Transport, Irkutsk, e-mail: kirillova_tk@irgups.ru

Pinin Ilya Evgenievich - 1st year student of the Department "Information Systems and Information Protection", training area "Information Security", Irkutsk State University of Railway Engineering, ilapinin@gmail.com

Для цитирования

Бабак П.В., Кириллова Т.К, Пинин И.Е. Безопасность крипотовалют// «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №2. – С.30-38. – Режим доступа: http://ismm-irgups.ru/toma/222-2024.

For citations

Babak P.V., Kirillova T.K., Pinin I.E. Security of cryptocurrencies // «Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami»: elektron. nauch. zhurn – 2024. – No.2. – P. 30-38. – Rezhim dostupa: http://ismm-irgups.ru/toma/222-2024