УДК 004.056:336.74

АНАЛИЗ ТИПОВЫХ ВЕКТОРОВ МОШЕННИЧЕСКИХ АТАК НА КРИПТОВАЛЮТНЫЕ КОШЕЛЬКИ В СРЕДЕ WEB3

Черкасов Е.В, Гордымов И.Д, студенты гр. ИБт-241, II курс
Научный руководитель: Хакимов П.Е., ассистент
Кузбасский государственный технический университет имени Т.Ф. Горбачева, г. Кемерово

Криптовалютный рынок, долгое время ассоциировавшийся с нестабильностью цены, судя по прогнозным данным, вступает в фазу уверенного и стабильного роста. Как показано на графике 1, ожидается, что к 2035 году его капитализация достигнет 4,2 трлн долларов, увеличившись более чем в 3,5 раза по сравнению с 2020 годом[1].

Рисунок 1. Рост рынка криптовалюты

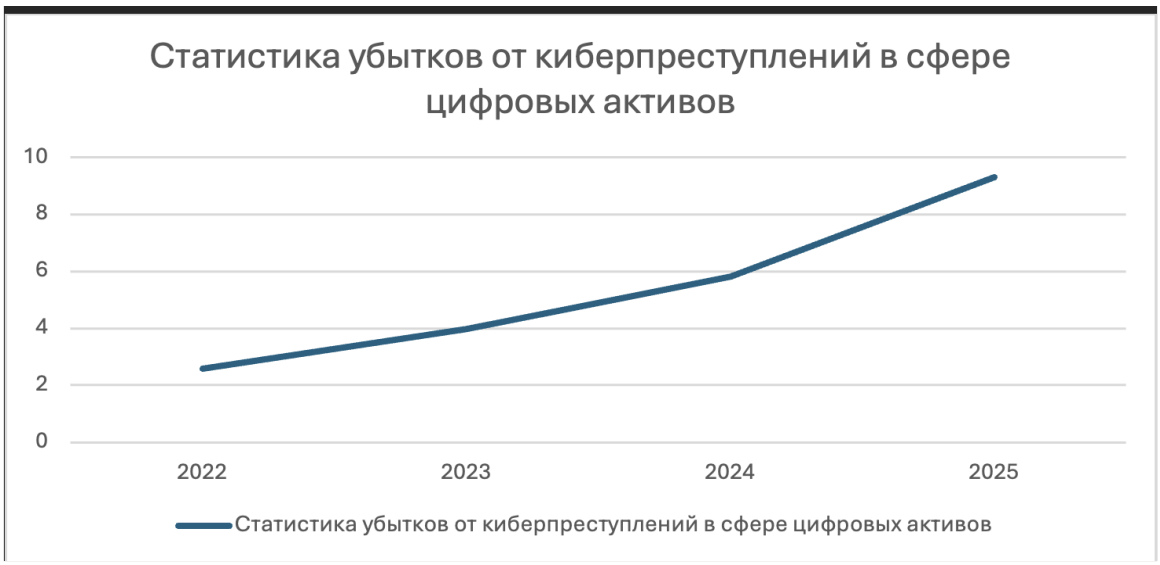

Рисунок 2 Статистика убытков от киберпреступлений с сфере цифровых активов

Цифровые активы стали приоритетной мишенью для киберпреступников: ежегодные убытки от атак и мошенничества в этой сфере исчисляются миллиардами долларов и продолжают расти. Представленные диаграммы отражают динамику потерь за 2021–2025 годы.

В Российской Федерации в сфере правового регулирования цифровых актовов главенствует Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации Несмотря на то, что закон вводит понятия «цифровой финансовый актив» и «цифровая валюта», [2] он преимущественно регулирует деятельность операторов обмена и выпуск активов, оставляя вопросы безопасности криптовалютных кошельков, используемых физическими лицами в среде Web3, в зоне ответственности самих владельцев.

Даже при условии сформированного правового поля и повышения компетенций участников рынка, в сегменте безопасности Web3-кошельков фиксируется значительный дисбаланс между скоростью технологической эволюции и реальным уровнем защищенности пользователей. данного исследования выступает отсутствие стандартизированного подхода к классификации угроз, характерных для децентрализованных финансовых операций. Данный пробел существенно затрудняет создание и внедрение результативных механизмов борьбы против киберугроз.

Подобно наличным, хранящимся в кошельке, цифровые активы держат в криптокошельке. Это программа, предназначенная для отправки и получения

цифровых валют, контроля их баланса и взаимодействия с различными блокчейнами.

Криптокошелек также хранит приватный и открытый ключи. Открытый ключ является адресом (счетом), на который пересылаются цифровые деньги, его видят другие пользователи.[3] Приватный ключ используется для цифровой подписи, без которой невозможно осуществить перевод. Наличие кошелька необходимо, чтобы управлять своими криптоактивами и обеспечивать их безопасность.

В зависимости от наличия кастодиана (третьей стороны), которая отвечает за хранение личных данных, кошельки делятся на кастодиальные и некастодиальные.

Кастодиальный кошелек — это кошелек, в котором личные данные хранятся третьей стороной (кастодианом). В этом есть свои плюсы. Например, утратив пароли или ключи, пользователь сможет восстановить доступ к своим средствам.

Кастодиальные кошельки есть у многих криптобирж (Coinbase, Binance и т. д.) и брокерских сервисов. Подобная интеграция упрощает работу с другими инструментами этих площадок, бывает выгодна при совершении транзакций (например, за счет отсутствия комиссий внутри экосистемы).

По причине контроля ключей третьими лицами важно подходить к выбору кастодиального кошелька особенно осторожно, поскольку доступ кастодиана к кошельку является одновременно и недостатком. Пользователь может потерять доступ к кошельку и средствам по решению властей или суда, а также в результате хакерской атаки.[4]

Ярким примером этого стала кража средств пользователей сотрудниками криптовалютной биржи Thodex на сумму $2 млрд в 2021 году. А в 2022 году американская Coinbase объявила о блокировке кошельков, связанных с российскими гражданами и компаниями из американских санкционных списков.

Сид-фраза (или seed-фраза) — это последовательность из 12, 18 или 24 слов, которая служит главным инструментом для восстановления доступа к криптовалютному кошельку. Эти слова, выбранные из специального словаря, генерируются во время настройки некостодиального кошелька. Seed-фраза представляет собой своего рода мастер-ключ, который предоставляет доступ к вашему криптовалютному кошельку, его данным и средствам.

Смарт-контракт (smart-контракт) — это программный код, выполняющий определенные условия сделки между двумя или более сторонами на основе технологии блокчейн. В отличие от традиционных контрактов, смарт-контракт автоматически исполняется при наступлении заранее определенных условий, без участия посредников и без возможности изменения данных после их внесения в блокчейн.

В отличие от традиционных финансовых систем (Web2), где безопасность и возврат средств обеспечивает банк-посредник, в среде Web3 действует модель некастодиального хранения: пользователь единолично контролирует приватные ключи и несет полную ответственность за сохранность активов. Это обеспечивает финансовый суверенитет, но исключает возможность обращения в централизованную службу поддержки для отмены транзакции или возврата средств в случае компрометации.

Взаимодействие с dApp в Web3 осуществляется через смарт-контракты, что часто требует предоставления разрешения (`approve`) на доступ к токенам пользователя. Злоумышленники эксплуатируют этот механизм: через фишинговые сайты они побуждают жертву подписать транзакцию с неограниченным лимитом расхода средств, маскируя реальные права доступа к кошельку. Фишинг (Phishing). Злоумышленники создают точные копии популярных сервисов (децентрализованных бирж, маркетплейсов NFT) с использованием похожих доменных имен или контекстной рекламы в поисковых системах. Цель атаки — побудить пользователя ввести seed-фразу или приватный ключ на поддельном сайте. Более продвинутая версия фишинга предполагает не кражу ключей, а подмену адреса получателя или подписание вредоносной транзакции Один из наиболее показательных кейсов атак на основе социальной инженерии — инцидент с Кевином Роузом, сооснователем NFT-проектов Proof Collective и Moonbirds. Несмотря на высокий уровень экспертизы в сфере Web3, Роуз стал жертвой целевого фишинга, потеряв NFT на сумму свыше $2 млн

В отличие от векторов социальной инженерии, где ключевым элементом является манипуляция пользователем, технические эксплойты направлены на уязвимости программного кода, сетевой инфраструктуры и клиентского оборудования. Данные атаки часто автоматизированы и могут быть реализованы без прямого контакта с жертвой в момент хищения средств, что повышает их скрытность и масштабность.

Наиболее распространенным вектором на стороне клиента является использование инфостилеров (info-stealers) и троянов. Специализированные вредоносные программы сканируют файловую систему на наличие файлов горячих кошельков (например, хранилища расширений браузеров) и извлекают зашифрованные приватные ключи. Особую категорию составляют «клипперы» (clipboard hijackers), которые мониторят буфер обмена устройства. При обнаружении строки, соответствующей формату криптоадреса, вредоносный скрипт подменяет его на адрес злоумышленника. Пользователь, не осуществляющий визуальную верификацию адреса перед отправкой, неизбежно переводит средства на счет атакующего.

Один из наиболее масштабных и долгосрочных кейсов применения вредоносного ПО для кражи криптовалют — деятельность северокорейской хакерской группировки Lazarus Group в рамках операции «AppleJeus». По данным компаний по кибербезопасности (Kaspersky, ESET, Chainalysis), в результате этих атак было похищено активов на сумму свыше $1,3 млрд, включая инцидент с мостом Ronin Network ($625 млн) и биржей Horizen ($54 млн) .[5]

Проведенное исследование подтвердило высокую актуальность проблемы безопасности криптовалютных кошельков в среде Web3 на фоне прогнозируемого роста капитализации рынка до 4,2 трлн долларов к 2035 году. Параллельно с развитием отрасли наблюдается критическое увеличение убытков от киберпреступлений, которые, по оценкам, вырастут с 2,57 млрд долларов в 2022 году до 9,3 млрд долларов в 2025 году.

На основании анализа нормативно-правовой базы Российской Федерации установлено, что Федеральный закон № 259-ФЗ регулирует деятельность операторов, но оставляет владельцев некастодиальных кошельков без институциональной защиты, перекладывая полную ответственность за сохранность активов на пользователей. Это создает фундаментальный дисбаланс между сложностью технологий и уровнем цифровой грамотности участников рынка [6].

Список литературы

1. Crypto Wallets Market Size and Share Forecast Outlook 2025 to 2035 // fml URL: https://www.futuremarketinsights.com/reports/crypto-wallets-market (дата обращения: 01.03.2026).
2. Crypto crime mid year // fml URL: https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ (дата обращения: 01.03.2026).

3. Как безопасно хранить криптовалюту? Криптокошельки и их особенности // РБК URL: https://www.rbc.ru/crypto/news/625015289a794736280f3737 (дата обращения: 01.03.2026).
4. Что такое seed-фраза — почему используют такой способ защиты // РБК URL: https://www.rbc.ru/crypto/news/625015289a794736280f3737 (дата обращения: 01.03.2026).
5. Что такое смарт-контракты и кому они нужны // РБК URL: https://www.rbc.ru/crypto/news/66f1bcf69a794703cbe6ba1e (дата обращения: 01.03.2026).