ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
2025. Т. 7, № 2 (21). С. 143–154 http://siit.ugatu.su
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.056 DOI 10.54708/2658-5014-SIIT-2025-no2-p143 EDN CXNIYP

Способы защиты криптовалютных блокчейн-систем и систематизация угроз

Н. В. Вилаков • М. И. Бочаров

Аннотация. В данной статье проведен анализ ключевых уязвимостей криптовалютных блокчейн-систем, их классификация и оценка потенциального ущерба в зависимости от вероятности реализации угрозы. Представлена статистика количества научных публикаций по данной тематике в российских и зарубежных источниках, а также статистика хакерских атак и ущерба, нанесенного блокчейн-сетям за последние семь лет. Рассмотрены основные методы защиты от выявленных угроз, а также перспективные направления развития механизмов безопасности технологии распределенного реестра.

Ключевые слова: блокчейн; безопасность распределительных реестров; уязвимости блокчейн-систем; конфиденциальность данных.

Введение

В последние годы технология блокчейн привлекает все больше внимания со стороны научного сообщества благодаря своему потенциалу в обеспечении безопасности, прозрачности и децентрализованного хранения и передачи данных. Первоначально блокчейн-системы были разработаны для проведения криптовалютных транзакций, но сегодня их применение значительно расширилось. Технология находит использование в таких областях, как здравоохранение [Mis19], финансовый сектор [Pet15], государственное управление [Yi19], логистика и интернет вещей (IoT) [Max23a].

Несмотря на очевидные преимущества, такие как неизменяемость записей, защита от несанкционированного доступа и устранение необходимости в доверенных посредниках, блокчейн-системы сталкиваются с серьезными вызовами в области безопасности и конфиденциальности. Развитие смарт-контрактов, появление новых моделей токенизации и внедрение масштабируемых решений, таких как многослойные архитектуры и кроссчейн-взаимодействие, способствуют эволюции технологии, но одновременно создают новые векторы атак [Mak21, Chr16]. К числу наиболее значимых угроз относятся атака 51 %, уязвимости консенсусных механизмов, централизованные точки отказа в децентрализованных приложениях (DApps) и недостатки в защите смарт-контрактов, что требует детального анализа и разработки эффективных мер противодействия.

В данной работе проводится систематизированное исследование актуальных угроз безопасности блокчейн-систем, анализируются распространенные атаки и стратегии их предотвращения. Особое внимание уделено современным криптографическим методам защиты, таким как zk-SNARKs, мультиподписи и гомоморфное шифрование, которые могут существенно повысить уровень конфиденциальности и устойчивости блокчейна к возможным угрозам.

Несмотря на растущий интерес к данной тематике в российском научном сообществе [Сок19, Мар19], уровень теоретической проработки и практического внедрения остается ниже, чем в зарубежных исследованиях. Концепция блокчейна, впервые предложенная Сатоши Накамото в 2008 году, за последние годы трансформировалась в сложную экосистему с широким спектром приложений, что делает вопросы обеспечения ее безопасности и конфиденциальности особенно актуальными.

СТАТИСТИЧЕСКИЙ АНАЛИЗ ПУБЛИКАЦИЙ И АТАК НА БЛОКЧЕЙН-СИСТЕМЫ

Для количественной оценки научного интереса к безопасности блокчейн-систем были проанализированы публикации в РИНЦ, а также в международных базах ScienceDirect и IEEE Xplore. По запросам «блокчейн» и «распределенный реестр» за 2018–2024 годы в РИНЦ было найдено 6594 публикации, в ScienceDirect – 20 402, а в IEEE Xplore – 30 661. Поиск включал статьи, книги и материалы конференций. После удаления дубликатов и нерелевантных источников (например, на языках, отличных от русского и английского) было выявлено распределение публикаций по годам (рис. 1).

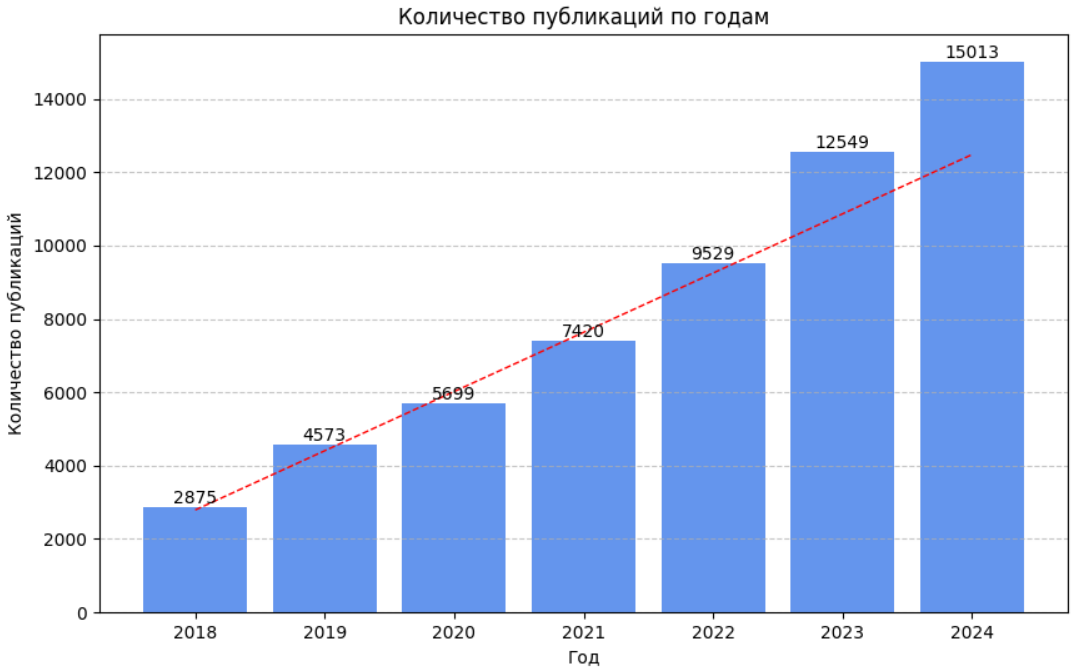

Рис. 1 Динамика публикаций статей по заданной тематике за 2018–2024 годы

Как показано на диаграмме, количество публикаций стабильно увеличивается со среднегодовым приростом в 31.72 %. Исключение составляют 2020–2021 годы, когда в России наблюдалось временное снижение числа публикаций (с 1100 в 2019 году до 835 в 2020 и 809 в 2021). Однако в целом тенденция роста сохраняется, что указывает на растущий интерес научного сообщества к вопросам безопасности блокчейн-технологий.

Дополнительно был проведен анализ атак на блокчейн-системы за 2015–2024 годы (рис. 2). Данные свидетельствуют о значительном увеличении числа атак и объема похищенных активов в период с 2018 по 2022 год, когда общий ущерб достиг рекордных $3.7 млрд. Однако после 2022 года объем украденных средств сократился ($1.8 млрд в 2023 году и $2.2 млрд в 2024 году), несмотря на рост числа атак (303 инцидента в 2024 году). Это может свидетельствовать о повышении эффективности защитных механизмов, но также о переходе злоумышленников к атакам меньшего масштаба, включая эксплойты смарт-контрактов и фишинговые схемы.

Особого внимания заслуживает инцидент, произошедший в феврале 2025 года, когда хакеры осуществили крупнейший в истории взлом криптовалютной биржи Bybit. В результате атаки злоумышленники получили доступ к одному из холодных кошельков биржи и похитили более $1 млрд в криптовалюте Ethereum. Этот случай подчеркивает необходимость дальнейшего совершенствования кибербезопасности, проведения регулярных аудитов смарт-контрактов и разработки нормативных механизмов регулирования криптовалютного рынка.

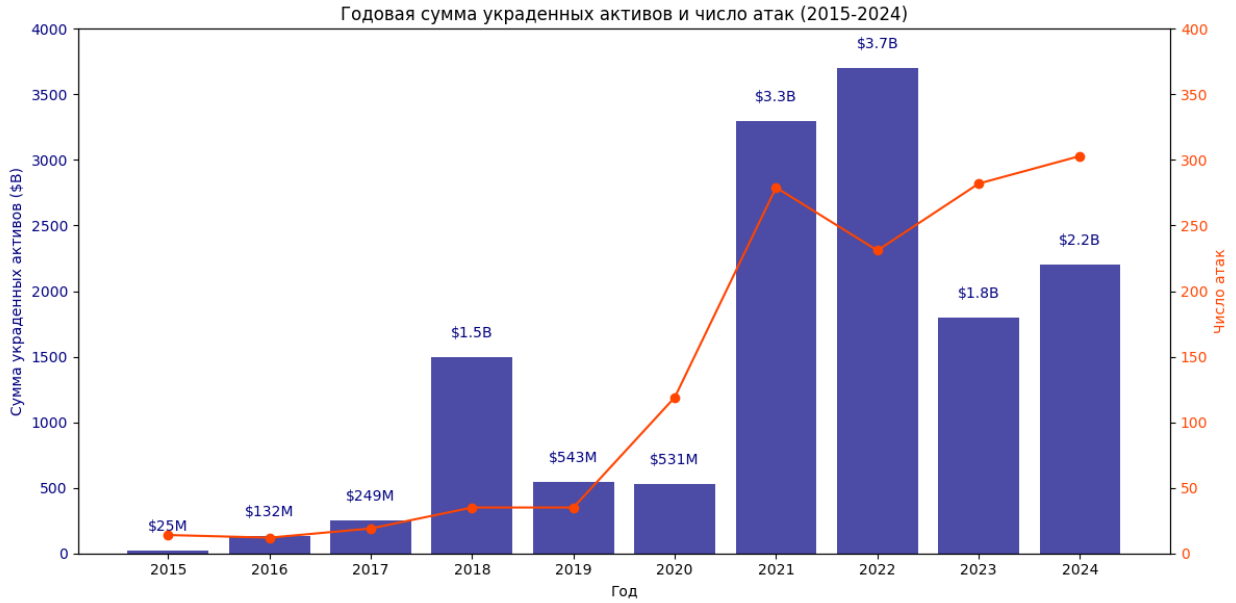

Рис. 2 Общая сумма украденных активов и число хакерских атак за 2016–2024 годы

Обеспечение информационной безопасности блокчейн-сетей требует детального изучения различных угроз, которые отличаются по своему характеру, механизму реализации и потенциальным последствиям. Для эффективного анализа рисков и разработки мер противодействия необходимо классифицировать угрозы с учетом их воздействия на ключевые аспекты безопасности: доступность, целостность и конфиденциальность.

Классификация угроз по аспектам информационной безопасности

Анализ известных исследований позволяет выделить три основные категории угроз в блокчейн-системах:

1) **Нарушение доступности**. Данный тип атак направлен на дестабилизацию работы сети, перегрузку вычислительных узлов или блокирование доступа пользователей к данным. Наиболее распространенные примеры включают DDoS-атаки, атаку 51 %, а также манипуляции с маршрутизацией интернет-трафика (BGP hijacking).

2) **Нарушение целостности**. К этой группе относятся атаки, целью которых является изменение данных в блокчейне или компрометация механизмов консенсуса. В частности, угрозу представляют атаки двойной траты, Selfish Mining, эксплуатация уязвимостей смарт-контрактов и взлом криптографических алгоритмов.

3) **Нарушение конфиденциальности**. Этот тип угроз включает атаки, связанные с раскрытием информации о пользователях и их транзакциях. Среди таких атак можно выделить deanonymization-атаки, анализ метаданных транзакций и эксплуатацию слабостей в механизмах генерации случайных чисел в смарт-контрактах.

Предложенная классификация позволяет структурировать угрозы и выявить их взаимосвязь. Например, атака 51 % может одновременно затронуть доступность сети (из-за доминирования одного участника) и целостность данных (путем проведения двойных трат).

Методологические подходы к систематизации угроз

На данный момент существуют несколько методологических подходов к классификации угроз в блокчейн-системах:

- **Функциональный анализ угроз**, при котором атаки рассматриваются в контексте конкретных элементов блокчейн-архитектуры, таких как узлы сети, механизмы консенсуса,

смарт-контракты и криптографические алгоритмы. Данный подход позволяет выявлять уязвимости на уровне отдельных компонентов системы.

- **Классификация по степени воздействия**, при которой угрозы оцениваются с точки зрения потенциального ущерба и вероятности реализации. Согласно последним исследованиям, к наиболее критическим угрозам относятся атака 51 %, эксплуатация уязвимостей смарт-контрактов и компрометация приватных ключей пользователей.
- **Риск-ориентированный анализ**, предполагающий применение математических моделей для прогнозирования вероятности атак и их последствий. Такой метод позволяет учитывать текущее состояние сети и поведение ее участников для выявления потенциальных точек уязвимости.

Комплексное использование этих подходов дает возможность разрабатывать стратегии защиты, направленные не только на устранение известных угроз, но и на снижение рисков их реализации в будущем.

Атака 51 % как угроза безопасности блокчейн-сетей

Одной из наиболее серьезных угроз для блокчейн-систем является атака 51 %, представляющая собой захват контроля над большей частью вычислительных мощностей сети (Proof-of-Work) или доли стейкинга (Proof-of-Stake). Это позволяет злоумышленнику изменять историю транзакций и в некоторых случаях проводить двойные траты. Рассмотрим сценарий реализации данной атаки в сети, использующей Proof-of-Work, поскольку этот механизм более подвержен такому типу угроз.

Предположим, что злоумышленник нацелился на небольшую блокчейн-сеть с суммарным хешрейтом 100 TH/s, использующую алгоритм консенсуса Ethash. В качестве первого шага он анализирует сеть, оценивая ликвидность токена на биржах, сложность майнинга, распределение мощности среди пулов и существующие меры защиты. Например, если в сети не предусмотрено большого количества подтверждений для депозитов на биржах, вероятность успешного проведения атаки возрастает.

После сбора информации злоумышленник приступает к атаке, арендуя вычислительные мощности на специализированных сервисах, таких как NiceHash. Допустим, аренда 100 TH/s на один час стоит 0.1 BTC. Решив атаковать сеть в течение нескольких часов, злоумышленник приобретает необходимую мощность и начинает скрытный майнинг альтернативной цепи блоков, начиная с определенного момента (например, блока N). Найденные блоки при этом не транслируются в основную сеть, а хранятся приватно.

Одновременно злоумышленник отправляет крупную транзакцию на биржу, например, 1000 Xcoin, и дожидается ее подтверждения. После конвертации средств в другую криптовалюту (например, Bitcoin или USDT) и успешного вывода активов он публикует свою альтернативную цепь, которая оказывается длиннее основной. Согласно правилам консенсуса, сеть автоматически переключается на более длинную цепочку, что приводит к аннулированию неподтвержденных транзакций, включая перевод на биржу. В результате злоумышленник сохраняет как Xcoin, так и выведенные средства, а у биржи не остается записей о депонировании.

Подобная атака становится возможной при недостаточном уровне децентрализации и низком общем хешрейте сети. Для защиты от подобных угроз разработчики блокчейн-систем внедряют механизмы увеличения сложности сети, используют методы типа checkpointing, а также ужесточают требования к подтверждениям транзакций на биржах. В крупных блокчейнах, таких как Bitcoin и Ethereum, атака 51 % практически невозможна из-за высокого уровня децентрализации и огромного объема требуемых ресурсов. Однако в небольших и средних блокчейн-сетях угроза остается актуальной и требует постоянного мониторинга и совершенствования механизмов консенсуса.

После успешного завершения атаки злоумышленник прекращает использование арендованных вычислительных мощностей, что приводит к восстановлению нормального функционирования сети. Однако при этом он получает значительную финансовую выгоду за счет ранее проведенных манипуляций. Криптовалютные биржи, обнаружив факт атаки, могут временно приостановить ввод и вывод данной монеты, но ущерб уже нанесен, а доверие к сети существенно подорвано. Данный сценарий становится возможным из-за недостаточной децентрализации сети, низкого общего хешрейта и отсутствия строгих требований к подтверждению транзакций на биржах.

Если рассматривать аналогичную атаку в сети, использующей механизм **Proof-of-Stake (PoS)**, процесс приобретает несколько иной характер. В отличие от **Proof-of-Work (PoW)**, алгоритм PoS считается более устойчивым к подобным атакам, особенно в условиях высокой степени децентрализации. Однако при недостаточном распределении стейкинга злоумышленник может получить контроль над сетью, скупив значительное количество токенов. Например, если в блокчейне PoS Coin всего 10 миллионов монет, а в стекинге участвуют 4 миллиона, приобретение 3 миллионов токенов позволит атакующему установить доминирующее влияние на процесс выбора валидаторов. Получив контроль, злоумышленник может манипулировать консенсусом, снижая штрафы за нарушение правил (slashing) или создавая форки с целью проведения двойных трат.

В некоторых случаях такие атаки могут быть предотвращены путем внедрения экономических барьеров, таких как обязательное замораживание токенов в стекинге на определенный срок или использование случайного выбора валидаторов, что делает атаку значительно более затратной. Однако в недостаточно защищенных сетях угроза остается актуальной.

Таким образом, атака 51 % представляет серьезную опасность для блокчейнов с низким уровнем децентрализации и слабой системой защиты. В целях предотвращения подобных атак разработчики внедряют механизмы повышения сложности сети, реализуют алгоритмы checkpointing, ужесточают требования к подтверждениям транзакций на биржах и внедряют штрафные механизмы в PoS. В крупнейших сетях, таких как Bitcoin и Ethereum, атака 51 % становится практически невозможной из-за колоссального объема требуемых ресурсов, однако в небольших и средних блокчейнах эта угроза сохраняется, что требует постоянного мониторинга и совершенствования механизмов консенсуса.

Уязвимости смарт-контрактов

Анализ современных исследований в области безопасности блокчейн-технологий показывает, что значительное число атак связано с уязвимостями в смарт-контрактах. Эти уязвимости присутствуют на различных платформах, таких как Ethereum, Binance Smart Chain и другие экосистемы, поддерживающие децентрализованные вычисления. Их можно классифицировать в зависимости от характера и механизма воздействия на систему. Среди наиболее распространенных уязвимостей выделяют ошибки, связанные с некорректным управлением памятью, использованием неинициализированных переменных и нарушениями в логике выполнения. Одним из наиболее известных типов атак является атака повторного входа (reentrancy), при которой злоумышленник может многократно вызывать внешний контракт до завершения выполнения исходной транзакции, обходя ожидаемую последовательность операций. Классическим примером является эксплойт, обнаруженный в 2016 году в смарт-контракте The DAO [Kos16]. Уязвимость заключалась в том, что контракт позволял производить внешние вызовы до обновления баланса пользователя, что давало атакующему возможность многократно инициировать вывод средств. В результате из фонда было выведено более 3.6 миллиона ETH, что составило значительную часть оборота сети Ethereum на тот момент.

Для лучшего понимания рассмотрим пример уязвимого смарт-контракта на языке **Solidity**, содержащего ошибку, которая позволяет выполнить атаку повторного входа (рис. 3).

Критическая ошибка данного контракта заключается в том, что обновление баланса пользователя происходит **после** выполнения внешнего вызова msg.sender.call. Если атакующий

развернет вредоносный контракт, содержащий fallback-функцию с повторным вызовом withdraw, он сможет неоднократно выводить средства, пока баланс контракта не будет исчерпан.

```
pragma solidity ^0.8.0;

contract VulnerableContract {
    mapping(address => uint) public balances;

    function deposit() public payable {
        balances[msg.sender] += msg.value;
    }

    function withdraw(uint _amount) public {
        require(balances[msg.sender] >= _amount, "Insufficient balance");
        (bool success, ) = msg.sender.call{value: _amount}("");
        require(success, "Transfer failed");
        balances[msg.sender] -= _amount;
    }
}
```

Рис. 3 Пример кода уязвимого смарт-контракта на языке Solidity

Для защиты от таких атак рекомендуется использовать принцип checks-effects-interactions, согласно которому перед выполнением внешнего вызова сначала обновляется состояние контракта. Дополнительно можно применять механизмы блокировки повторных вызовов (реентерабельные блокировки) и проводить аудит смарт-контрактов перед их развертыванием.

В перспективе дальнейшие исследования должны быть направлены на разработку автоматизированных инструментов анализа кода, совершенствование методов формальной верификации и внедрение систем обнаружения атак в реальном времени. Эти меры позволят значительно повысить безопасность смарт-контрактов в публичных блокчейн-сетях.

Ниже представлены угрозы в виде таблицы, учитывая уровень вероятности их реализации и возможный ущерб для сети (табл.).

Таблица

Ранжированный список основных угроз и способов их решения

Тип атаки	Возможное решение	Уровень угрозы	Аспект ИБ, нарушаемый атакой	Аспект ИБ, защищаемый решением
1	2	3	4	5
Угроза захвата большей части сети (>50 %)	Увеличение числа подтверждений для транзакций, снижение концентрации вычислительных мощностей. В случае захвата – хардфорк сети, что несет существенные риски	Высокий	Целостность (возможность двойной траты)	Целостность (подтверждение транзакций)
Взлом криптографических алгоритмов	Регулярное обновление и апгрейд криптографических решений. Использование постквантовых алгоритмов шифрования [Alp22, Day20]	Высокий	Конфиденциальность (доступ к закрытым данным)	Конфиденциальность (защита ключей)
Уязвимости в смарт-контрактах	Проведение тщательного тестирования и аудита кода, а также использование проверенных библиотек и стандартов при разработке контрактов	Высокий	Целостность (изменение логики контракта)	Целостность (корректность выполнения)
Атака с использованием маршрутизации	Шифрование трафика, децентрализация узлов передачи данных	Средний	Доступность (разделение сети)	Доступность (стабильность соединения)
Атака Сивиллы	Ограничение числа узлов с одного IP, верификация участников	Средний	Конфиденциальность (маскировка участников)	Конфиденциальность (идентификация узлов)

Продолжение табл.

1	2	3	4	5
Двойная трата	Введение механизмов временных задержек перед подтверждением транзакций	Средний	Целостность (повторное использование активов)	Целостность (уникальность транзакций)
Внесение в реестр некорректной информации	Проверка данных перед включением в реестр, механизм консенсуса	Низкий	Целостность (фальсификация данных)	Целостность (фальсификация данных)
DDoS	Использование систем защиты от DDoS, таких как межсетевые экраны (firewalls) и системы обнаружения вторжений (IDS), для фильтрации и блокирования подозрительного сетевого трафика	Низкий	Доступность (перегрузка сети)	Доступность (обеспечение работы сети)

Определение степени угроз в блокчейн-сетях в первую очередь зависит от масштабов потенциального ущерба, который может быть нанесен при эксплуатации той или иной уязвимости. Вторым важным критерием является вероятность реализации данной угрозы в различных сетях. В таблице представлены наиболее значимые уязвимости блокчейн-систем, расположенные в порядке убывания их опасности. Особое внимание следует уделять угрозам с высоким уровнем риска, так как их эксплуатация может привести к серьезным последствиям для всей сети.

Для лучшего понимания функционирования блокчейн-систем можно построить схематическое представление их архитектуры (рис. 4), выделив ключевые источники уязвимостей. Анализ показывает, что ошибки в коде (баги) могут присутствовать практически на любом уровне системы. На уровне узла сети (ноды) существует риск захвата вычислительных мощностей и манипуляции маршрутизацией трафика. Внутри самого блокчейна возможны атаки на криптографические алгоритмы, включая взлом цифровых подписей и хэш-функций, однако на данный момент такие атаки практически неосуществимы. Большая часть уязвимостей сосредоточена на стороне клиента, включая ошибки в смарт-контрактах, уязвимости в мобильных приложениях криптовалютных кошельков и бирж, атаки социальной инженерии и косвенное воздействие других типов атак.

Определив и проанализировав основные типы уязвимостей в блокчейн-сетях, а также существующие методы повышения их безопасности, можно перейти к рассмотрению перспективных направлений исследований в области защиты распределенных реестров. В частности, рассмотрим передовые криптографические методы защиты и их практическое применение.

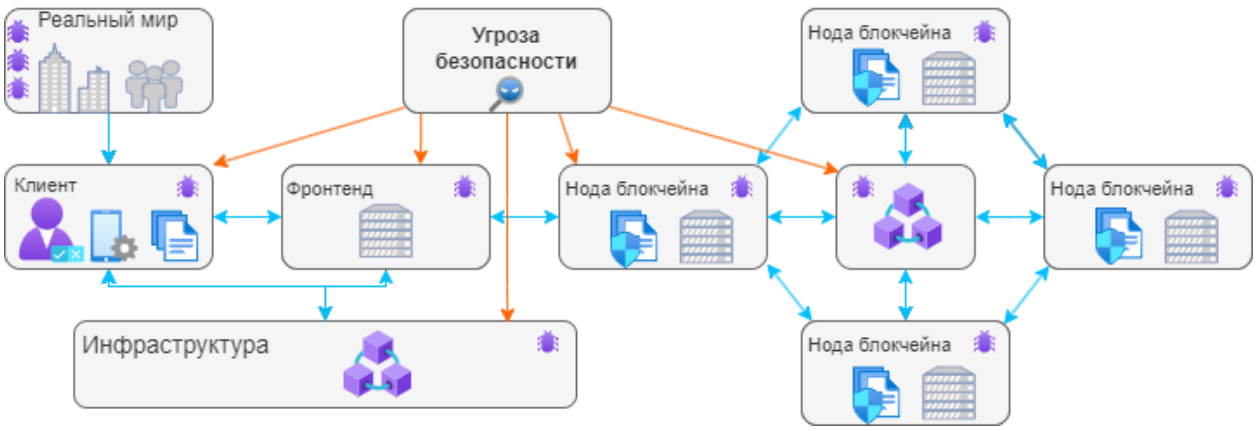

Рис. 4 Модель уязвимостей блокчейн-систем

Метод защиты zk-SNARKs

Метод доказательства с нулевым разглашением zk-SNARKs (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*) представляет собой один из наиболее эффективных криптографических подходов, позволяющий верифицировать вычисления без раскрытия входных данных [Bow17]. Главное преимущество zk-SNARKs заключается в том, что проверяющая сторона получает подтверждение истинности утверждения без доступа к конфиденциальной информации. Однако, несмотря на свою эффективность, данный метод обладает рядом ограничений.

Одной из ключевых проблем zk-SNARKs является необходимость доверенной установки параметров (*trusted setup*). На этапе инициализации системы генерируются общедоступные параметры (*Common Reference String, CRS*), используемые в последующих доказательствах. Если на этом этапе произойдет компрометация, злоумышленник может создать ложные доказательства, обходя установленные механизмы безопасности. В некоторых ранних реализациях zk-SNARKs эта уязвимость была выявлена, что привело к разработке новых протоколов, таких как zk-STARKs, не требующих доверенной установки.

Еще одним недостатком является высокая вычислительная сложность, особенно на этапе генерации доказательств. Это ограничивает использование zk-SNARKs в мобильных устройствах и в среде IoT. Кроме того, если параметры системы сгенерированы неправильно, возможны атаки, связанные с предсказуемостью криптографических функций.

Несмотря на указанные ограничения, zk-SNARKs активно используется в системах конфиденциальных платежей, таких как Zcash, где этот метод позволяет подтверждать транзакции без раскрытия информации об отправителе, получателе или сумме перевода.

Рассмотрим практическую реализацию доказательства знания предобраза хеш-функции без его раскрытия. Предположим, что доказывающая сторона хочет подтвердить знание секретного числа x, удовлетворяющего уравнению $H(x) = y$, где H – криптографическая хеш-функция, а y – известное значение. Для этого можно использовать zk-SNARK-схему, которая доказывает существование такого x, не раскрывая его.

Реализация такого доказательства может быть выполнена с использованием фреймворка ZoKrates, который предназначен для разработки zk-SNARK-программ. В языке описания вычислений ZoKrates это можно представить следующим образом (рис. 5).

```
def main(private field x, field y):
    field hash_x = Poseidon(x)
    assert(hash_x == y)
    return true
```

Рис. 5 Пример реализации доказательства на языке ZoKrates

В этом примере Poseidon(x) представляет собой криптографическую хеш-функцию, оптимизированную для использования в zk-SNARK. Код определяет, что пользователь знает x, соответствующий известному y, но при этом проверяющая сторона не получает доступ к x, а лишь подтверждает корректность утверждения. После компиляции и генерации доказательства с использованием CRS проверяющий сможет убедиться в его истинности за минимальное время, так как zk-SNARKs обеспечивают верификацию за постоянное время, что делает их особенно эффективными в условиях масштабируемых блокчейн-систем.

Метод zk-SNARKs является перспективным направлением для защиты конфиденциальных данных в блокчейне. В будущем ожидается развитие новых схем, таких как zk-STARKs, которые устраняют необходимость доверенной установки, а также расширение их применения в распределенных системах, идентификации без паролей и масштабируемых решениях второго уровня.

Метод защиты с использованием мультиподписей

Мультиподпись (*multisignature, multisig*) является одним из эффективных методов защиты цифровых активов, требующим подтверждения транзакций несколькими владельцами ключей перед их исполнением. Такой подход значительно повышает уровень безопасности по сравнению с классическими цифровыми подписями, поскольку компрометация одного из ключей не ведет к полной потере контроля над средствами.

Наиболее распространенной схемой является механизм «*m* из *n*», где *n* – общее количество возможных подписантов, а *m* – минимальное число подписей, необходимых для авторизации транзакции. Например, в модели 2 из 3 подтверждение транзакции требует подписей двух из трех возможных участников, что значительно снижает вероятность несанкционированного доступа.

Однако, несмотря на очевидные преимущества, технология мультиподписей также имеет определенные ограничения. В классических реализациях (например, P2SH-мультиподпись в Bitcoin) все подписи записываются в блокчейн, что увеличивает размер транзакции и делает её проведение дороже по сравнению с обычными операциями.

Дополнительным потенциальным риском является возможность блокировки средств при саботаже одной из сторон. Например, в схеме 2 из 3 один из участников может намеренно отказаться от подписания транзакции, тем самым препятствуя выводу средств. В некоторых случаях эту проблему можно решить с помощью смарт-контрактов, реализующих механизмы тайм-аутов или арбитражных решений.

Криптографические основы мультиподписей

Теоретическая база мультиподписей основана на криптографических алгоритмах совместного управления ключами, таких как Эль-Гамаля, ECDSA и Schnorr [Sun17]. В частности, в сети Bitcoin и других блокчейнах на основе модели UTXO применяется механизм P2SH (Pay-to-Script-Hash), позволяющий создавать адреса, которые требуют выполнения определенного скрипта для разблокировки средств. Вместо хранения индивидуальных подписей в блокчейне используются хеши скриптов, а сами условия подписи раскрываются только в момент проведения транзакции.

Современные решения, такие как MuSig, основанные на подписи Schnorr, предлагают более оптимизированные схемы мультиподписей, позволяющие агрегировать подписи в единое криптографическое доказательство. Это снижает размер транзакций, сокращает нагрузку на сеть и повышает уровень конфиденциальности.

Практическое применение мультиподписей

Механизм мультиподписей востребован в организациях, требующих коллективного управления активами, а также в децентрализованных автономных организациях (DAO), где важны механизмы коллективного принятия решений.

Рассмотрим практическую реализацию мультиподписного кошелька в блокчейне Ethereum, используя смарт-контракт на языке Solidity. В данном примере реализована схема «2 из 3», где три владельца кошелька могут предлагать и утверждать транзакции, но для их выполнения требуется минимум две подписи (рис. 6).

В данной реализации каждый из владельцев может предложить транзакцию, после чего другие подписанты голосуют за ее выполнение. Как только количество подтверждений достигает установленного порога (например, 2 из 3), средства отправляются на указанный адрес. Такой механизм предотвращает несанкционированное использование активов, даже если один из подписантов окажется скомпрометирован.

Таким образом, мультиподписи представляют собой важный элемент безопасности в блокчейн-экосистеме [Max23б], позволяя реализовать механизмы коллективного управления средствами и защиты от атак, связанных с компрометацией отдельных приватных ключей. Дальнейшее развитие мультиподписных схем направлено на интеграцию более эффективных крип-

тографических алгоритмов, таких как подписи Schnorr, а также их применение в масштабируемых решениях второго уровня, что позволит повысить безопасность и производительность децентрализованных финансовых приложений.

```
pragma solidity ^0.8.0;

contract MultiSigWallet {
    address[] public owners;
    uint public required;
    mapping(uint => mapping(address => bool)) public confirmations;
    struct Transaction {
        address to;
        uint value;
        bool executed;
    }
    Transaction[] public transactions;

    constructor(address[] memory _owners, uint _required) {
        require(_owners.length >= _required, "Invalid parameters");
        owners = _owners;
        required = _required;
    }

    function submitTransaction(address _to, uint _value) public {
        transactions.push(Transaction({to: _to, value: _value, executed: false}));
    }

    function confirmTransaction(uint _txIndex) public {
        require(isOwner(msg.sender), "Not an owner");
        confirmations[_txIndex][msg.sender] = true;
        if (countConfirmations(_txIndex) >= required) {
            executeTransaction(_txIndex);
        }
    }

    function executeTransaction(uint _txIndex) internal {
        Transaction storage transaction = transactions[_txIndex];
        require(!transaction.executed, "Already executed");
        transaction.executed = true;
        payable(transaction.to).transfer(transaction.value);
    }

    function countConfirmations(uint _txIndex) internal view returns (uint count) {
        for (uint i = 0; i < owners.length; i++) {
            if (confirmations[_txIndex][owners[i]]) {
                count++;
            }
        }
    }

    function isOwner(address _addr) internal view returns (bool) {
        for (uint i = 0; i < owners.length; i++) {
            if (owners[i] == _addr) return true;
        }
        return false;
    }
}
```

Рис. 6 Пример реализации схемы мультиподписи «2 из 3»

Заключение

В данной статье представлен комплексный анализ угроз безопасности блокчейн-сетей, детализированы механизмы их реализации и рассмотрены современные методы защиты, включая zk-SNARKs и мультиподписи. Несмотря на активное развитие блокчейн-технологий, вопросы безопасности остаются актуальными, особенно в контексте децентрализованных финансовых приложений (DeFi) и смарт-контрактов.

Статистический анализ показывает, что число атак на блокчейн-системы продолжает расти, что связано как с усложнением архитектуры самих сетей, так и с появлением новых векторов атак, таких как MEV-эксплойты и атаки на межсетевые протоколы (cross-chain exploits). Однако одновременное снижение объема похищенных средств может свидетельствовать о повышении эффективности мер защиты и развитии стандартов аудита смарт-контрактов.

Рассмотренные методы защиты подтверждают свою практическую ценность, однако требуют дальнейшей оптимизации. В частности:

- **zk-SNARKs** сталкивается с проблемой доверенной установки параметров (*trusted setup*), что требует развития альтернативных схем, таких как zk-STARKs.
- **Мультиподписи** нуждаются в усовершенствовании, включая использование более гибких схем управления ключами и интеграцию пороговых подписей.

Будущее исследований в области безопасности блокчейн-систем должно быть направлено на:

- автоматизированный аудит смарт-контрактов с применением машинного обучения для обнаружения уязвимостей;
- развитие гибридных механизмов консенсуса, сочетающих преимущества PoW и PoS;
- внедрение адаптивных алгоритмов безопасности, прогнозирующих потенциальные атаки на основе анализа сетевого поведения.

Эти меры позволят значительно повысить устойчивость блокчейн-инфраструктуры и обеспечить ее безопасное использование в долгосрочной перспективе.

Список литературы / References

[Alp22] NISTIR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process / J. Alperin-Sheriff, D. Cooper, D. Moody, R. Peralta, A. Perlner, D. Robinson. 2022. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf (Accessed: 15.03.2025).

[Bow17] Bowe S., Gabizon A., Green M. D. A Multi-Party Protocol for Constructing the Public Parameters of the Pinocchio zk-SNARK. 2017. URL: https://z.cash (Accessed: 15.03.2025).

[Chr16] Christidis K., Devetsikiotis M. “Blockchains and smart contracts for the internet of things” // IEEE Access. 2016. Vol. 4. Pp. 2292–2303.

[Kos16] Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts” // 2016 IEEE Symposium on Security and Privacy (SP). 2016. Pp. 839–858.

[Mak21] Makhmutov A., Vulfin A., Mironov K. “On developing secure distributed sensor networks” // Proceedings – ICOECS 2021: 2021 International Conference on Electrotechnical Complexes and Systems, Ufa, November 16–18 2021. Ufa, 2021. Pp. 122–126. DOI 10.1109/ICOECS52783.2021.9657252. EDN CDVQHB.

[Mis19] Misic V., Mišić J., & Chang X. “Towards a blockchain-based healthcare information system” // IEEE/CIC International Conference on Communications. 2019. Pp. 1-6.

[Pet15] Peters G., & Panayi E. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. B Banking Beyond Banks and Money. Springer. 2015. Pp. 239-278.

[Sun17] Sun S. F., Au M. H., Liu J. K., Yuen T. H. “RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero“// Springer European Symposium on Research in Computer Security. 2017. Pp. 456–474.

[Yi19] Yi H. “Securing e-voting based on blockchain in P2P network” // EURASIP Journal on Wireless Communications and Networking. 2019. Vol. 2019. Article No. 137. May. Pp. 1–11. DOI 10.1186/s13638-019-1473-6. EDN JXAHSY.

[Дау20] Даутов Д. Ш., Миронов К. В. Квантовоустойчивые распределенные реестры // Мавлютовские чтения: Статьи XIV Всероссийской молодежной научной конференции, Уфа, 01–03 ноября 2020 года. Т. 5. Ч. 2. Уфа: УГАТУ, 2020. С. 13. EDN ATNVFE. [[Dautov D. Sh., Mironov K. V. “Quantum-resistant distributed registries” // Mavlyutov Readings: Articles of the

XIV All-Russian youth scientific conference, Ufa, November 01–03, 2020. Volume 5, Part 2. Ufa: Ufa State Aviation Technical University, 2020. P. 13. EDN ATNVFE. (In Russian).]]

[Мар19] Маринкин Д. Н. Проблемы информационной безопасности криптографии пользователя современного блокчейна // Проблемы правоохранительной деятельности. 2019. № 3. С. 39. EDN UAXEMF. [[Marinkin D. N. “Problems of information security of cryptography of the modern blockchain user” // Problems of Law Enforcement Activity. 2019. No. 3, pp. 39. EDN UAXEMF (In Russian).]]

[Мах23а] Махмутов А. Р., Вульфин А. М., Миронов К. В. Исследование возможностей автономной работы конечных устройств интернета вещей // СИИТ. 2023. Т. 5. № 1(10). С. 41–47. EDN DPEMFA. [[Makhmutov A. R., Vulfin A. M., Mironov K. V. “Study of the possibilities of autonomous operation of end devices of the internet of things” // SIIT. 2023. Vol. 5, no. 1(10), pp. 41–47. EDN DPEMFA. (In Russian).]]

[Мах23б] Махмутов А. Р., Вульфин А. М., Миронов К. В. О разработке защищенных распределенных сенсорных сетей // Молодежный вестник УГАТУ. 2023. № 1(27). С. 69–74. EDN PQQDUP. [[Makhmutov A. R., Vulfin A. M., Mironov K. V. “On the development of secure distributed sensor networks” // Youth Bulletin of Ufa State Aviation Technical University. 2023. No. 1(27), pp. 69–74. EDN PQQDUP. (In Russian).]]

[Сок19] Соколова Т. Н., Волошин И. П., Петрунин И. А. Преимущества и недостатки технологии блокчейн // Экономическая безопасность и качество. 2019. № 1(34). С. 49–52. EDN ZCUYZF. [[Sokolova T. N., Voloshin I. P., Petrunin I. A. “Advantages and disadvantages of blockchain technology” // Economic Security and Quality. 2019. No. 1 (34), pp. 49–52. EDN ZCUYZF. (In Russian).]]

Поступила в редакцию 3 февраля 2025 г.

МЕТАДАННЫЕ / METADATA

Title Ways to protect cryptocurrency blockchain systems and systematization of threats.

Abstract. This article analyzes the key vulnerabilities of cryptocurrency blockchain systems, their classification and assessment of potential damage depending on the likelihood of the threat. The article presents statistics on the number of scientific publications on this topic in Russian and foreign sources, as well as statistics on hacker attacks and damage caused to blockchain networks over the past seven years. The main methods of protection against identified threats are considered, as well as promising areas for the development of security mechanisms for distributed registry technology.

Key words blockchain, security of distribution registries, vulnerabilities of blockchain systems, data privacy.

Язык статьи / Language Русский / Russian.

Об авторах / About the authors:

ВИЛАКОВ Никита Владимирович
Финансовый университет при Правительстве Российской Федерации, Россия
Аспирант. Магистр техники и технологии по информатике и вычислительной технике (Национальный исследовательский технологический университет «МИСиС», 2022). Иссл. в области методов и систем защиты информации, информационной безопасности.
E-mail nikitavilakov@mail.ru
ORCID 0009-0006-0951-4528

БОЧАРОВ Михаил Иванович
Финансовый университет при Правительстве Российской Федерации, Россия
Доцент департамента анализа данных и машинного обучения факультета информационных технологий и анализа больших данных.
E-mail mibocharov@mail.ru

VILAKOV Nikita Vladimirovich
Financial University under the Government of the Russian Federation, Russia
Graduate student. Master of Engineering and Technology in Computer Science and Computer Engineering (National Research Technological University "MISiS", 2022). Research in the field of information protection methods and systems, information security.
E-mail nikitavilakov@mail.ru
ORCID 0009-0006-0951-4528

BOCHAROV Mikhail Ivanovich
Financial University under the Government of the Russian Federation, Russia
Associate Professor of the Department of Data Analysis and Machine Learning at the Faculty of Information Technology and Big Data Analysis.
E-mail mibocharov@mail.ru