

МЕТОДИКА ОЦЕНКИ КВАНТОВОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН-ПЛАТФОРМ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Ларина М.В.¹, Скиба В.Ю.²

Ключевые слова: квантовые угрозы, консенсус, критическая информационная инфраструктура, оценка рисков, постквантовая криптография, формализация атак, цифровые платформы, Proof-of-Stake, Proof-of-Work.

Аннотация

Цель работы состоит в разработке методики оценки квантовой устойчивости блокчейн-платформ на основе математического аппарата сетей Петри, предназначенной для моделирования сценариев квантовых атак и выявления критических состояний функционирования распределенной системы.

Методы исследования: анализ устойчивости механизмов консенсуса Proof-of-Work и Proof-of-Stake, формализация атак и сценариев нарушений в терминах сетей Петри, оценка влияния криптографических, сетевых и вычислительных параметров на вероятность реализации угроз.

Результаты исследования: предложена модель, учитывающая зависимости между состояниями системы, параметрами переходов и вероятностями успешного выполнения атак. На основе данного подхода разработан программный комплекс для моделирования и сравнительного анализа сценариев безопасности блокчейн-платформ.

Научная новизна: методика оценки квантовой устойчивости блокчейн-платформ объединяет в единой модели криптографические, вычислительные и сетевые параметры, а также сценарный анализ устойчивости механизмов консенсуса Proof-of-Work и Proof-of-Stake. Формализация в терминах сетей Петри связывает логическую последовательность этапов атаки с количественными условиями их прохождения и позволяет выявлять критические состояния системы, оценивать вероятность реализации атак и учитывать взаимосвязь между криптографическими механизмами и структурой сети.

Практическая значимость: предложенная методика может быть использована при создании квантово-устойчивых блокчейн-экосистем и систем защиты критической информационной инфраструктуры.

DOI: 10.24412/1994-1404-2026-3-17-28

Введение

Развитие квантовых вычислений является одним из факторов, способных значительно изменить существующие подходы к обеспечению информационной безопасности. Создание квантовых вычислительных систем с достаточным количеством логических кубитов потенциально позволит решать ряд математических задач эффективнее классических вычислительных систем. Проблема особенно актуальна для криптографических механизмов, поскольку стойкость широко используемых алгоритмов с открытым ключом

основана на вычислительной сложности задач, которые могут эффективно решаться с применением квантовых алгоритмов.

Вопрос перехода к постквантовой криптографии в настоящее время рассматривается на уровне международных организаций и национальных органов стандартизации. Национальный институт стандартов и технологий США (NIST) в августе 2024 года утвердил первые три федеральных стандарта постквантовой криптографии: FIPS 203 для механизма установления

¹ Ларина Мария Васильевна, лаборант-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация. ORCID: 0009-0009-7826-0180.

E-mail: larina.mv@talantiuspeh.ru

² Скиба Владимир Юрьевич, доктор технических наук, старший научный сотрудник, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус»», пгт Сириус, Краснодарский край, Российская Федерация, профессор кафедры ИБМ-6 ФГАОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», г. Москва, Российская Федерация, профессор кафедры № 2 «Автоматика» национального исследовательского ядерного университета «МИФИ», г. Москва, Российская Федерация. ORCID: 0000-0002-9805-7800.

E-mail: skiba.vy@talantiuspeh.ru

ключей ML-KEM, FIPS 204 для цифровой подписи ML-DSA и FIPS 205 для цифровой подписи SLH-DSA. В NIST отмечается, что данные стандарты предназначены для защиты от будущих атак с использованием квантовых компьютеров и являются основой перехода к криптографическим механизмам, устойчивым к квантовым угрозам³.

Необходимость заблаговременной подготовки к такому переходу отмечается и Европейским агентством по кибербезопасности (ENISA). В материалах ENISA подчеркивается, что переход к постквантовой криптографии не ограничивается выбором новых алгоритмов и их стандартизацией: требуется адаптация существующих протоколов и информационных систем, а сам процесс миграции может занимать значительное время⁴. При этом организация отдельно указывает на необходимость уже на современном этапе учитывать угрозы, связанные с квантовыми вычислениями, несмотря на то что полномасштабные квантовые вычислительные системы, способные практически взламывать широко используемые криптографические схемы, пока не получили широкого распространения.

В соответствии с Концепцией обеспечения устойчивости цифровых платформ и блокчейн-экосистем в условиях появления квантовых угроз [1] особую значимость проблема приобретает для блокчейн-экосистем, поскольку криптографические механизмы являются одним из фундаментальных элементов их архитектуры. Согласно определению NIST, блокчейн представляет собой распределенный цифровой реестр криптографически подписанных транзакций, объединенных в блоки, причем каждый блок криптографически связан с предыдущим после проверки и принятия соответствующего решения механизмом консенсуса⁵. Таким образом, обеспечение целостности реестра и подтверждение прав участников непосредственно связаны с криптографическими механизмами и протоколами распределенного консенсуса. В NISTIR 8202 отмечается, что существенной составляющей блокчейн-технологий являются механизмы консенсу-

са, определяющие порядок формирования новых блоков и разрешения конфликтов между участниками распределенной сети. В документе рассматриваются различные модели консенсуса, в том числе Proof-of-Work (PoW) и Proof-of-Stake (PoS), отличающиеся ресурсом, определяющим возможность участника влиять на формирование состояния распределенного реестра.

Следовательно, квантовая угроза для блокчейн-экосистем не сводится исключительно к возможности компрометации используемого криптографического алгоритма. Изменение соотношения вычислительных возможностей участников сети, компрометация ключей и нарушение механизмов подтверждения транзакций могут иметь последствия для целостности распределенного реестра. Для платформ с PoW существенное значение приобретает изменение соотношения вычислительных ресурсов участников, тогда как для PoS критическим параметром является доля контролируемого стейка. При этом успешная атака может включать несколько последовательных этапов, например получение необходимого количества идентичностей, достижение требуемой доли ресурса консенсуса, создание конкурирующей ветви цепочки и последующую реализацию двойного расходования.

Дополнительную сложность представляет необходимость учитывать не только возможность наступления отдельного события, но и взаимосвязь последовательных этапов атаки. Например, достижение нарушителем определенной доли вычислительных ресурсов в PoW или доли стейка в PoS само по себе не характеризует итоговый риск в полном объеме. Необходимо дополнительно учитывать количество подтверждений транзакции, вероятность формирования конкурирующей цепочки, временные ограничения, механизмы обнаружения конфликта и экономические последствия реализации атаки. Методы количественной оценки квантовой устойчивости блокчейн-платформ рассматривались в [2]. Однако существующие подходы могут быть дополнены формализацией последовательности реализации угрозы с использованием сетей Петри⁶, позволяющих описывать состояния системы, события и условия перехода между состояниями. Применение данного математического аппарата дает возможность представить сценарий атаки как последовательность взаимосвязанных состояний и формально определить условия достижения конечного состояния.

Данная статья является продолжением работ [3, 4], посвященных классификации информационных систем в условиях развития квантовых информационных технологий и стратификации угроз безопасности инфор-

³ Федеральные стандарты NIST:

FIPS 203. Federal Information Processing Standards Publication. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.203.

FIPS 204. Federal Information Processing Standards Publication. Module-Lattice-Based Digital Signature Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.204.

FIPS 205. Federal Information Processing Standards Publication. Stateless Hash-Based Digital Signature Standard. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8900. Published August 13, 2024. DOI: 10.6028/NIST.FIPS.205.

⁴ European Union Agency for Cybersecurity. Post-Quantum Cryptography: Current State and Quantum Mitigation. Heraklion: ENISA, 2021.

⁵ Yaga D., Mell P., Roby N., Scarfone K. Blockchain Technology Overview: NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology, 2018. 57 p. DOI: 10.6028/NIST.IR.8202.

⁶ Например, использование обычных и цветных сетей Петри для анализа блокчейн-систем рассматривалось в работах: Pinna A., Tonelli R., Orrù M., Marchesi M. A Petri Nets Model for Blockchain Analysis // The Computer Journal. 2018. Vol. 61. No. 9. P. 1374—1388. DOI: 10.1093/comjnl/bxy001; Liu Z., Liu J. Formal Verification of Blockchain Smart Contract Based on Colored Petri Net Models // 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). Milwaukee, WI, USA: IEEE, 2019. P. 555—560. DOI: 10.1109/COMPSAC.2019.10265.

мации в них, а также работы [5], в которой предложена модель цифровой платформы для анализа её устойчивости к квантовым угрозам. В отличие от подхода, ориентированного исключительно на оценку стойкости отдельных криптографических механизмов, в данной работе предлагаемая методика рассматривает с использованием сетей Петри⁷ развитие атаки как совокупность взаимосвязанных событий и позволяет учитывать вероятность успешного прохождения отдельных этапов, параметры механизма консенсуса PoW и PoS и применяемые защитные меры.

Математическая постановка задачи

В рамках предлагаемого подхода блокчейн-экосистема задается вектором параметров Θ , характеризующим тип консенсуса, применяемые политики безопасности, сеть и количество ее участников. Сценарий атаки рассматривается как последовательность событий, которая при фиксированном наборе параметров Θ может привести к нарушению заданного свойства безопасности. В качестве конечного события могут выступать компрометация ключа, несанкционированный вывод активов, получение контроля над критической долей ресурса консенсуса или успешное двойное расходование.

Для формального представления сценария используется сеть Петри:

$$N = \{P, T, I, O, \mu^0\},$$

где P — конечное множество позиций;

T — множество переходов;

I и O — входная и выходная функции;

μ^0 — начальная маркировка.

Позиции интерпретируются как состояния моделируемого сценария, а переходы — как события, изменяющие состояние системы. Наличие фишки в позиции означает достижение соответствующего состояния. Переход разрешен, если выполнены необходимые условия и на входных позициях присутствуют требуемые фишки.

Такое представление позволяет отделить количественную часть оценки от логики развития атаки. Вероятностная модель определяет значения показателей, используемых в условиях переходов, а сеть Петри фиксирует допустимую последовательность событий.

В этом случае можно сформировать четыре типа сценариев:

1. PoW_1 — компрометация ключей в блокчейн-платформе с консенсусом PoW;
2. PoS_1 — компрометация ключей в блокчейн-платформе с консенсусом PoS;
3. PoW_2 — составная атака «Сивилла — 51% или двойная трата» для PoW;
4. PoS_2 — составная атака «Сивилла — 51% или двойная трата» для PoS.

Сценарии первого и второго типа ориентированы на анализ криптографического звена, а сценарии третьего и четвертого типа описывают развитие составной атаки на уровне консенсуса. Такое разделение позволяет исследовать как локальную уязвимость отдельного механизма защиты, так и ее возможные последствия для функционирования распределенного реестра.

Таким образом, выделены можно выделить следующие задачи:

1. для выбранных сценариев атак на блокчейн-экосистемы построить сети Петри $N(\Theta)$ и отображение параметров Θ на структуру сети и на условия переходов;
2. определить набор показателей устойчивости $U(N, \Theta)$ при реализации сценариев атак при заданных условиях;
3. реализовать уравнения динамики сети Петри и построение множества достижимых состояний;
4. разработать методику оценки $U(N, \Theta)$.

Методика оценки сценариев компрометации ключей

Учитывая, что криптографические механизмы (цифровые подписи, процедуры управления ключами и т. д.) являются фундаментальными компонентами блокчейн-экосистем и используются для подтверждения прав на совершение транзакций, получение злоумышленником приватного ключа или достаточного количества ключей в пороговой схеме позволяет сформировать корректную с точки зрения протокола транзакцию от имени владельца скомпрометированного ключа.

В отличие от сценариев двойной траты, рассматриваемая атака не предполагает непосредственного нарушения механизма консенсуса. Злоумышленнику не требуется изменять состояние распределенного реестра путем формирования альтернативной цепи или получать контроль над большей частью вычислительных либо стейкинг-ресурсов сети. Достаточно пройти предусмотренные платформой процедуры авторизации и подписания операции. Для блокчейн-экосистем с механизмами консенсуса PoW и PoS базовая логика развития атаки совпадает, а различия учитываются параметрами модели, связанными с особенностями соответствующего участника сети. Устойчивость блокчейн-экосистем при этом определяется не только механизмом консенсуса, но и криптографической стойкостью используемых примитивов [6].

В модели сценарий представляется с помощью сети Петри (Рис. 1). Начальное состояние соответствует отсутствию атаки (p1). Далее последовательно моделируются компрометация ключа (p2), формирование и подписание транзакции (p3 и p4), проверка баланса (p5), проверка адреса назначения (p6) и ожидание исполнения операции (p7). При срабатывании защитного механизма переход осуществляется в состояние блокирования (p8 и p11), а при успешном прохождении всех проверок — в состояние исполнения транзакции (p9 и p10).

⁷ Pinna, A. A Petri Nets Model for Blockchain Analysis / A. Pinna, R. Tonelli, M. Orrù, M. Marchesi // IEEE Access. 2017. DOI: 10.1109/ACCESS.2017.2749606.

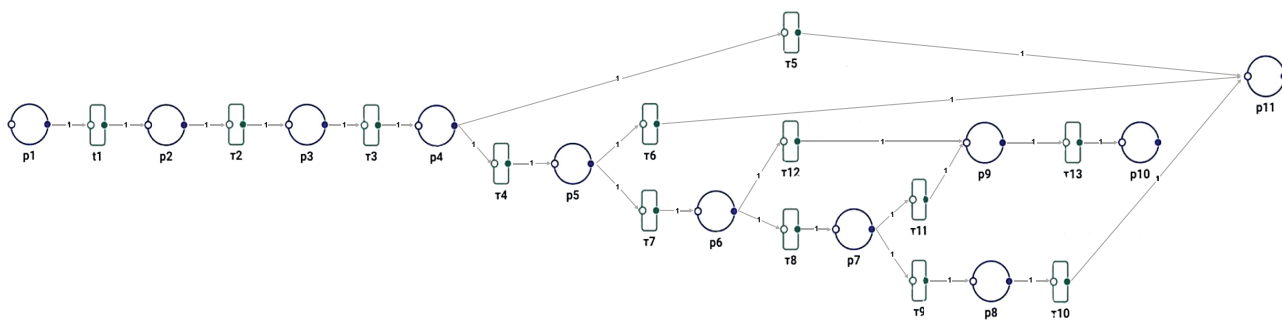


Рис. 1. Сеть Петри для сценария компрометации ключей

Возникновение криптографически значимых квантовых вычислений связано, в частности, с возможностью применения квантовых алгоритмов криптоанализа, включая алгоритм Шора [7—9]. В предлагаемой модели влияние квантовых вычислений учитывается посредством коэффициента квантового ускорения K .

Переход к состоянию компрометации определяет условием $P_{raw} > 0$.

После формирования транзакции проверяется достаточность баланса:

$$V_{attack} \leq B,$$

где V_{attack} — сумма вывода, B — баланс счета.

При использовании списка разрешенных адресов транзакция также должна быть направлена на адрес, включенный в *allowlist*. При наличии задержки вывода операция может быть обнаружена и заблокирована до исполнения. Такая последовательность соответствует общей логике оценки угроз, включающей анализ способа реализации, возможностей нарушителя и последствий атаки.

Для количественной оценки используются базовая вероятность компрометации ключа p_{base} , длина ключа key_bits , горизонт наблюдения t_{obs} , срок действия ключа t_{valid} , коэффициент квантового ускорения K , параметры схемы подписания и коэффициенты эффективности защитных механизмов.

Тогда долю периода риска можно определить как:

$$m_T = \frac{\min(t_{valid}, t_{obs})}{t_{obs}}.$$

Для учета длины ключа используется нормированный коэффициент:

$$f_{key} = \min(1, \max(0, 1, \frac{key_bits}{256})).$$

Для параметризации влияния длины ключа на вероятность его компрометации введем множитель $k_{len} = 2 - f_{key}$. При этом значение 256 бит принимается в качестве нормирующего значения в предлагаемой модели, а введение коэффициента позволяет учитывать повышенную уязвимость более коротких ключей в рамках рассматриваемой модели.

Базовая вероятность компрометации ключа до учета квантового ускорения определяется как:

$$P_{raw}^0 = p_{base} \cdot m_T \cdot k_{len},$$

где p_{base} — базовая вероятность компрометации ключа за горизонт наблюдения;

m_T — доля эффективного срока ключа внутри горизонта наблюдения;

k_{len} — множитель, отражающий зависимость вероятности компрометации от длины криптографического ключа.

Учет возможного вычислительного преимущества нарушителя выполняется с помощью коэффициента $K \geq 1$:

$$P_{raw} = \min(1, P_{raw}^0 \cdot K).$$

Необходимость учета такого параметра связана с перспективой появления криптографически значимых квантовых вычислительных систем и переходом к постквантовым алгоритмам⁸. При этом K является параметром сценарного анализа, а не характеристикой конкретного квантового устройства.

Для обычной схемы с одним ключом вероятность прохождения этапа подписания принимается равной P_{raw} . Если используется пороговая схема *t*-из-*n*, вероятность компрометации необходимого количества участников определяется биномиальной моделью:

$$P_{binomial} = P(X \geq t) = \sum_{k=t}^n C_n^k \cdot p_{party}^k (1 - p_{party})^{n-k},$$

где p_{party} — вероятность компрометации одного участника.

Итоговая вероятность после подписания имеет вид:

$$P_{after-sign} = P_{raw} \text{ — для одного ключа,}$$

$P_{after-sign} = \min(1, P_{raw} \cdot P_{binomial})$ — для схемы *t*-из-*n*.

Влияние механизмов защиты учитывается коэффициентами ε_i , характеризующими вероятность блокирования атаки отдельным механизмом. В модели рассматриваются HSM, ротация ключей, *allowlist*, мониторинг, ручное подтверждение, задержка вывода и ограничение суммы транзакции.

При допущении независимости защитных механизмов вероятность после их применения определяется как:

$$P_{after-defend} = P_{after-sign} \cdot \prod_i (1 - \varepsilon_i).$$

Если механизм защиты отсутствует, соответствующий множитель принимается равным единице. Значе-

⁸ National Cybersecurity Center of Excellence. Frequently Asked Questions about Post-Quantum Cryptography. URL: <https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/FAQ/index.htm>

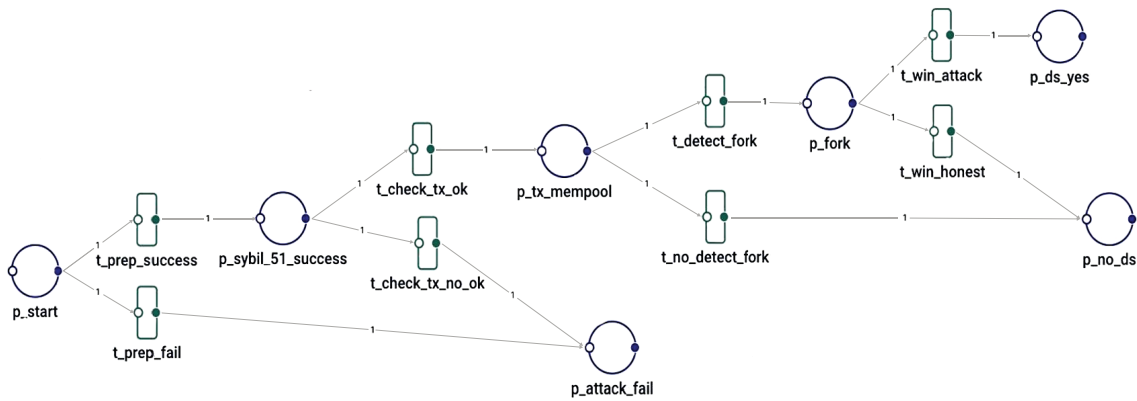


Рис. 2. Сеть Петри для сценария двойной траты для блокчейн-платформы с консенсусом PoW

ния ϵ_i могут задаваться на основе экспертных оценок, результатов аудита или испытаний системы.

При наличии задержки вывода вводится коэффициент:

$$\eta_{delay} = \min(1, \max(0, \frac{T_{det}}{T_{pol}^{PoS}}))$$

где T_{det} — время обнаружения инцидента;

T_{pol} — длительность защитного окна.

Для валидатора PoS дополнительно учитывается период разблокировки стека:

$$T_{pol}^{PoS} = T_{pol} + T_{unbond}.$$

Итоговая вероятность успешного завершения атаки определяется выражением

$$p_{succ} = P_{after-defend} \cdot \eta_{delay}.$$

Для оценки экономических последствий учитывается ограничение максимальной суммы одной транзакции:

$$V_{eff} = \min(V_{attack}, V_{cap}),$$

где V_{cap} — установленный лимит вывода.

При отсутствии лимита $V_{eff} = V_{attack}$. Если при вероятности p_{succ} злоумышленник провел атаку, то он выведет всю сумму V_{eff} с вероятностью $1 - p_{succ}$, а если нет успешной атаки, то и ущерб равен нулю. Тогда ожидаемый ущерб L вычисляется так

$$L = p_{succ} \cdot V_{eff} + (1 - p_{succ}) \cdot 0 = p_{succ} \cdot V_{eff}.$$

Таким образом, методика объединяет формальное описание последовательности атаки в сети Петри и вероятностную оценку ее реализации. Для PoW и PoS используется единая логика сценария, а различие между платформами учитывается параметрами модели, включая дополнительный период разблокировки стека для PoS. Формулы являются расчетной частью предлагаемой авторской модели, тогда как использованные источники обосновывают роль криптографических ключей, оценку угроз и необходимость учета постквантового фактора [1—22].

Методика оценки сценария двойной траты в блокчейн-платформе с консенсусом Proof-of-Work

В блокчейн-платформах с механизмом консенсуса Proof-of-Work (PoW) безопасность распределенного реестра обеспечивается за счет вычислительной слож-

ности формирования блоков и принятия в качестве канонической цепи ветви с наибольшим объемом выполненной работы. Такой принцип лежит в основе механизма защиты от двойного расходования: при условии, что совокупная вычислительная мощность добросовестных участников превышает мощность нарушителя, альтернативная цепь не успевает опередить основную⁹. NIST также относит возможность получения злоумышленником достаточной доли вычислительных ресурсов, известную как атака 51%, к основным угрозам механизмам PoW.

В настоящей работе сценарий двойной траты для PoW рассматривается как последовательность взаимосвязанных этапов:

- атака Сивиллы;
- получение необходимой доли вычислительных ресурсов;
- атака 51%;
- формирование конфликтующей транзакции;
- возникновение конкурирующих цепей;
- разрешение форка;
- двойная трата.

Сеть Петри (Рис. 2) позволяет представить указанный сценарий как последовательность состояний и событий, при которой переход к следующему этапу осуществляется только при выполнении заданного условия.

На первом этапе определяется возможность реализации атаки Сивиллы. Максимальное число узлов, которое нарушитель способен создать с учетом имеющихся вычислительных ресурсов, определяется выражением:

$$N_{tech} = N_{phys} \cdot V_{per-phys}$$

где N_{phys} — количество физических серверов нарушителя, $V_{per-phys}$ — количество виртуальных узлов на одном сервере.

После учета ограничений сети определяется фактическое количество узлов атакующего N_{att} . В модели учитываются ограничения по IP-адресам и доверенным организационным сущностям.

Доля узлов, контролируемых нарушителем, определяется как

⁹ Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

$$P_{sybil} = \frac{N_{att}}{N_{total} + N_{att}}$$

где N_{total} — количество добросовестных узлов сети.

Атака Сивиллы считается успешной при выполнении условия

$$P_{sybil} \geq T_{sybil}^p$$

где T_{sybil} — установленный порог успешности атаки.

При этом даже при недостижении основного порога может быть разрешен переход к следующему этапу, если доля ресурсов нарушителя превышает минимальный порог продолжения сценария.

На втором этапе определяется доля вычислительной мощности, контролируемой нарушителем. С учетом коэффициента квантового ускорения K базовая мощность условной единицы сети рассчитывается следующим образом:

$$H_{base} = \frac{H_{net}}{m+n \cdot K}$$

где H_{net} — суммарный хешрейт сети,

m — количество добросовестных узлов,

$n = N_{att}$ — количество узлов нарушителя.

Вычислительная мощность одного узла атакующего составляет $H_{att} = K \cdot H_{base}$, а его суммарная доля вычислительных ресурсов определяется выражением

$$D_{att} = \frac{n \cdot H_{att}}{H_{net}} \cdot 100\%$$

В рамках модели условие атаки 51% выполняется при $D_{att} \geq 51\%$. Достижение данного значения рассматривается как условие, при котором нарушитель получает возможность формировать альтернативную цепь с достаточной вычислительной мощностью для последующей реорганизации истории транзакций

На следующем этапе моделируется двойная трата. Нарушитель формирует конфликтующую транзакцию, которая направляется получателю, одновременно создавая альтернативную ветвь цепи. Количество подтверждений z , полученных основной транзакцией, используется в качестве параметра, характеризующего глубину ее нахождения в цепи. Вероятность создания следующего блока нарушителем определяется как

$$q = \frac{D_{att}}{100}, p = 1 - q,$$

где p — вероятность формирования блока добросовестными участниками.

Для $q < 0,5$ вероятность того, что атакующий сможет догнать добросовестную цепь после z подтверждений, определяется по вероятностной модели Накамото:

$$\lambda = z \cdot \frac{q}{p}, P_{nak} = 1 - \sum_{k=0}^z (e^{-\lambda} \cdot \frac{\lambda^k}{k!}) (1 - (\frac{q}{p})^{z-k}).$$

При $q = 0$ вероятность успеха принимается равной нулю, а при $q \geq 0,5$ — единице в соответствии с принятой моделью гонки цепей.

Дополнительно учитывается ограничение на максимальную последовательность блоков, которую способен сформировать атакующий: $L_{req} = z + 1$.

Если $L_{req} > L_{max}$, сценарий считается технически блокируемым.

Также в модели учитывается вероятность обнаружения конфликтующей транзакции в мемпуле. При включенной проверке коэффициент прохождения данного защитного механизма определяется как

$$f_{mempool} = 1 - \frac{S_{detect}}{100}$$

где S_{detect} — вероятность обнаружения конфликтующей транзакции.

Итоговая вероятность успешной двойной траты определяется как

$$P_{final} = \min(1, P_{after-sequence} \cdot f_{mempool}).$$

Ожидаемый ущерб рассчитывается как:

$$E_{damage} = V_{tx} \cdot P_{final}$$

где V_{tx} — стоимость конфликтующей транзакции.

Данная величина позволяет перейти от оценки вероятности реализации атаки к количественной оценке ее последствий.

Таким образом, разработанная методика позволяет оценить устойчивость PoW-блокчейна с учетом последовательного характера атаки, вычислительных ресурсов нарушителя, квантового ускорения, количества подтверждений и механизмов обнаружения двойного расходования. Формализация сценария сетью Петри обеспечивает связь между расчетными вероятностными показателями и дискретными состояниями развития атаки, что позволяет получить итоговую оценку вероятности успешной двойной траты и ожидаемого ущерба.

Методика оценки сценария двойной траты в блокчейн-платформе с консенсусом Proof-of-Stake

В блокчейн-платформах с механизмом консенсуса Proof-of-Stake (PoS) возможность влияния нарушителя на процесс формирования и подтверждения блоков определяется не вычислительной мощностью, как в Proof-of-Work, а величиной контролируемого им стейка. Поэтому после реализации общего для рассматриваемых сценариев этапа атаки Сивиллы, описанного в прошлом разделе, основное внимание уделяется оценке доли стейка, находящейся под контролем нарушителя.

В рамках рассматриваемой модели (Рис. 3) этап атаки Сивиллы для PoS не рассматривается повторно, поскольку алгоритм формирования подконтрольных узлов и оценки их количества является общим для сценариев PoW_2 и PoS_2. Отличие возникает на следующем этапе, когда определяется ресурс, позволяющий нарушителю влиять на механизм консенсуса. Для PoW таким ресурсом является вычислительная мощность, тогда как для PoS — контролируемая доля стейка [21].

Совокупная доля стейка валидаторов, контролируемых нарушителем, определяется выражением

$$D_{stake} = \frac{S_{total}}{S_{att}} 100\%$$

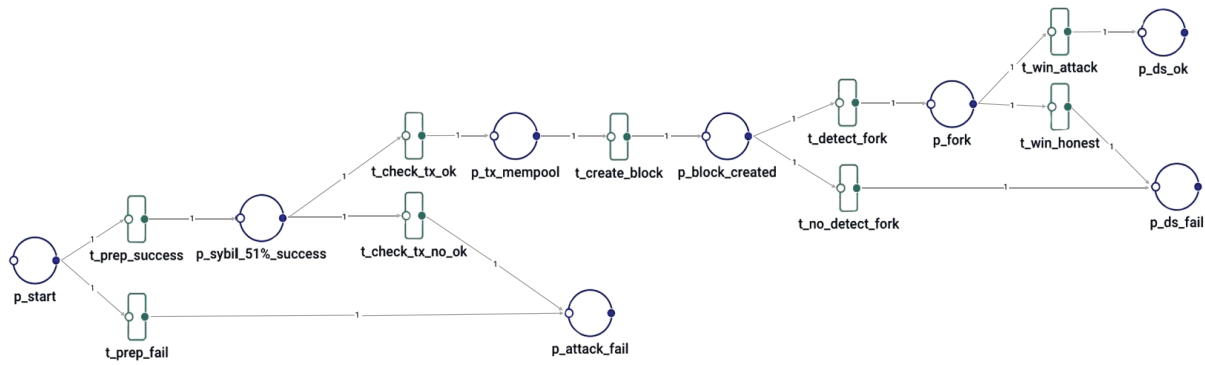


Рис. 3. Сеть Петри для сценария двойной траты для блокчейн-платформы с консенсусом Proof-of-Stake

где S_{att} — совокупный стейк валидаторов, контролируемых нарушителем,

S_{total} — общий объем стейка сети.

Условием перехода к этапу формирования альтернативной ветви является достижение установленного порога

$$D_{stake} \geq T_{stake},$$

где T_{stake} — критическая доля стейка, необходимая для реализации рассматриваемого сценария.

Таким образом, общая структура атаки Сивиллы сохраняется для обоих механизмов консенсуса, однако критерий получения контроля над процессом подтверждения транзакций различается: в PoW оценивается доля вычислительных ресурсов нарушителя, а в PoS — доля контролируемого стейка [1, 21, 22]. После получения необходимой доли стейка нарушитель формирует конфликтующую транзакцию и начинает построение альтернативной ветви блокчейна. При этом вероятность успешного формирования и подтверждения альтернативной цепочки зависит от доли голосующей силы, контролируемой атакующим. В модели вводится величина $q = \frac{D_{stake}}{100}$, характеризующая долю ресурса, доступного нарушителю. Оставшаяся доля $p = 1 - q$ соответствует добросовестным валидаторам.

При $q < 0,5$ вероятность успешного формирования альтернативной цепочки уменьшается с увеличением количества подтверждений исходной транзакции. В качестве базовой модели вероятности догоняющей цепи используется вероятностный подход Накамото, адаптированный для рассматриваемого механизма консенсуса:

$$\lambda = z \cdot \frac{q}{p}, P_{nak} = 1 - \sum_{k=0}^z (e^{-\lambda} \cdot \frac{\lambda^k}{k!}) (1 - (\frac{q}{p})^{z-k}).$$

В PoS дополнительно учитывается временной фактор, связанный с периодом разблокировки стейка. При наличии механизма unbonding нарушение может быть обнаружено до момента, когда контролируемый стейк станет доступен для вывода. Поэтому эффективное защитное окно определяется выражением

$$T_{pol}^{PoS} = T_{pol} + T_{unbound},$$

где T_{pol} — базовая задержка операции,

T_{unbond} — период разблокировки стейка.

Увеличение данного интервала повышает продолжительность периода, в течение которого может быть обнаружена подозрительная активность и применены защитные меры. Вероятность прохождения временно-го защитного механизма определяется как

$$\eta_{delay} = \min(1, \max(0, \frac{T_{det}}{T_{pol}^{PoS}})),$$

где T_{det} — время обнаружения атаки.

Итоговая вероятность успешной двойной траты определяется с учетом вероятности формирования альтернативной цепочки и эффективности временного механизма защиты

$$P_{final} = P_{nak} \cdot \eta_{delay}.$$

При наличии дополнительных механизмов защиты итоговая вероятность может быть скорректирована с учетом соответствующих коэффициентов их эффективности. Как и для PoW, окончательная оценка сценария включает потенциальный экономический ущерб:

$$E_{damage} = V_{tx} \cdot P_{final}$$

где V_{tx} — стоимость конфликтующей транзакции.

Таким образом, разработанная методика позволяет оценить вероятность успешной двойной траты в PoS-блокчейне с учетом количества контролируемых валидаторов, доли принадлежащего им стейка, количества подтверждений, временных механизмов защиты и потенциального ущерба. В отличие от рассмотренного ранее сценария PoW, в котором ключевым ресурсом является вычислительная мощность, для PoS определяющим параметром является доля стейка, находящаяся под контролем нарушителя. Это позволяет применять единую общую структуру сети Петри для анализа обоих механизмов консенсуса при различии количественных параметров соответствующих переходов.

Результаты и сравнительный анализ

Для оценки разработанной методики проведен вычислительный эксперимент по рассмотренным сценариям компрометации ключей и двойной траты в блокчейн-платформах с механизмами консенсуса Proof-of-Work и Proof-of-Stake. В качестве основных показателей использовались вероятность успешной реализации атаки и ожидаемый ущерб.

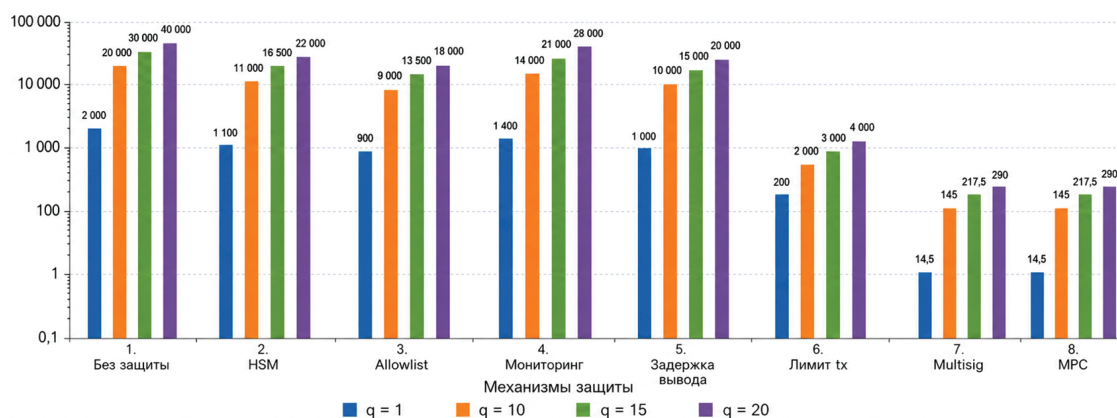


Рис. 4. Зависимость ожидаемого ущерба от квантового ускорения при различных механизмах защиты

Результаты моделирования сценария компрометации ключей показывают, что увеличение коэффициента квантового ускорения K приводит к росту вероятности успешной атаки и, соответственно, ожидаемого ущерба (Рис. 4).

Наиболее существенное снижение риска достигается при использовании пороговых схем подписи Multisig и MPC, поскольку для завершения атаки требуется компрометация нескольких участников. Дополнительное снижение потенциальных потерь обеспечивается ограничением суммы одной транзакции. Для PoS важным фактором также является период разблокировки стейка, увеличивающий время, доступное для обнаружения и блокирования подозрительной операции.

При анализе сценария двойной траты в PoW установлено, что увеличение доли вычислительных ресурсов, контролируемых нарушителем, сопровождается ростом вероятности успешного формирования альтернативной цепи и ожидаемого ущерба (Рис. 5).

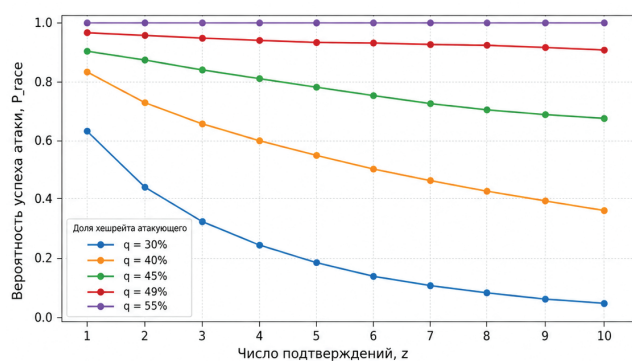


Рис. 5. Зависимость вероятности успешной двойной траты от числа подтверждений в PoW

При относительно небольшой доле ресурсов увеличение числа подтверждений z существенно снижает вероятность атаки.

Однако при приближении доли ресурсов нарушителя к критической области влияние количества подтверждений уменьшается. Таким образом, одного по-

рогового значения 51% недостаточно для комплексной оценки устойчивости: необходимо учитывать вероятность выигрыша гонки цепей и эффективность механизмов обнаружения конфликта.

Аналогичная закономерность наблюдается для PoS, однако определяющим ресурсом выступает доля стейка, контролируемая нарушителем (Рис. 6).

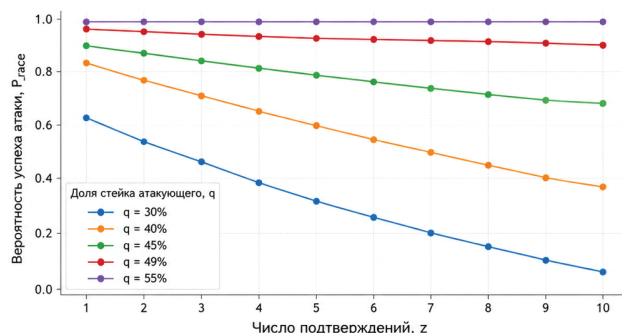


Рис. 6. Зависимость вероятности успешной двойной траты от числа подтверждений в PoS

При ее увеличении ожидаемый ущерб возрастает и в критической области достигает высокого уровня. Механизм slashing в рассматриваемой модели влияет прежде всего на экономическую привлекательность атаки и не уменьшает непосредственно размер уже возникшего ущерба. Более существенное влияние на вероятность успешного завершения сценария оказывают механизмы обнаружения конфликтующих транзакций и временные ограничения.

Сравнение результатов показывает, что для PoW и PoS характерна общая зависимость: чем выше доля ресурса, контролируемого нарушителем, тем выше вероятность успешной атаки и потенциальный ущерб. Различие заключается в природе данного ресурса: для PoW им является вычислительная мощность, для PoS — контролируемый стейк. В обоих случаях увеличение числа подтверждений эффективно преимущественно при относительно небольшом влиянии атакующего.

Таким образом, результаты эксперимента подтверждают, что оценка квантовой устойчивости блокчейн-платформ не должна ограничиваться проверкой достижения одного порогового значения. Более информативным является комплексный анализ последовательности развития атаки, вероятности прохождения отдельных этапов, механизмов защиты и потенциального ущерба. Предложенная методика позволяет проводить такую оценку в единой формальной модели на основе сетей Петри и сопоставлять устойчивость платформ с различными механизмами консенсуса.

Выводы

В работе предложена методика оценки квантовой устойчивости блокчейн-платформ на основе математического аппарата сетей Петри. Методика позволяет формализовать последовательность развития квантовых атак, учитывать особенности механизмов консенсуса Proof-of-Work и Proof-of-Stake и получать количественные оценки вероятности успешной реализации атаки и ожидаемого ущерба.

В рамках исследования сформированы модели четырех сценариев квантовых угроз: компрометации криптографических ключей в PoW и PoS, а также двойной траты в блокчейн-платформах с соответствующими механизмами консенсуса. Для каждого сценария определены состояния, события и условия переходов, отражающие последовательность реализации атаки.

Для сценариев компрометации ключей разработанная методика позволяет учитывать длину ключа, срок его действия, квантовое ускорение, используемый механизм подписи и применяемые средства защиты. Для сценариев двойной траты учитываются доля контролируемых нарушителем ресурсов, количество подтверждений транзакции, вероятность обнаружения

конфликта и дополнительные ограничения, влияющие на возможность завершения атаки.

Проведенные вычислительные эксперименты показали, что увеличение контролируемого атакующим ресурса приводит к росту вероятности успешной реализации двойной траты и ожидаемого ущерба. При этом увеличение числа подтверждений эффективно преимущественно при относительно небольшой доле ресурсов нарушителя; при приближении к критической области защитный эффект данного механизма снижается. Для PoW определяющим ресурсом выступает вычислительная мощность, тогда как для PoS — контролируемая доля стейка.

Установлено также, что применение отдельных механизмов защиты воздействует на различные характеристики риска. Пороговые схемы подписи и ограничения суммы транзакции снижают вероятность или потенциальный размер ущерба при компрометации ключей, тогда как механизмы обнаружения конфликтующих транзакций непосредственно ограничивают вероятность успешного завершения сценария двойной траты. В PoS механизм slashing дополнительно формирует экономические последствия для нарушителя, однако не исключает непосредственно возникновение ущерба от состоявшейся атаки.

Таким образом, результаты исследования подтверждают целесообразность сценарного подхода к оценке квантовой устойчивости блокчейн-платформ, при котором учитывается не отдельный пороговый показатель, а совокупность последовательных событий, параметров механизма консенсуса, криптографических характеристик, защитных механизмов и потенциальных последствий атаки. Разработанная методика может использоваться для сравнительного анализа различных конфигураций блокчейн-платформ и выбора мер, направленных на повышение их устойчивости к квантовым угрозам.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение от 27.09.2024 г. № 23—03).

Литература

1. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. P. 56—73. DOI: 10.18721/JCSTCS.18205. EDN: DCDMZF.
2. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2—22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
3. Ларина М.В., Скиба В.Ю. О классификации угроз информационных систем в условиях развития квантовых технологий // Правовая информатика. 2026. № 1. С. 5—15. DOI: 10.24412/1994-1404-2026-1-00-01. EDN: XMQASS.
4. Ларина М.В., Скиба В.Ю. Уточнение классификации информационных систем и угроз в условиях развития квантовых технологий // Экономика устойчивого развития региона: инновации, финансовые аспекты, технологические драйверы развития в сфере туризма и гостеприимства : материалы XII межд. науч.-практ. конф.,

- посвященной празднованию 80-летия победы, Ялта, 26—29 марта 2025 г. Симферополь : ООО «Типография «Ариал», 2025. С. 182—184. EDN: CDFVGN.
5. Ларина М.В., Скиба В.Ю. Модель цифровой платформы для анализа устойчивости к квантовым угрозам // Правовая информатика. 2025. № 3. С. 12—26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
 6. Ищукова Е.А. О влиянии криптографической стойкости функций хеширования на устойчивость современных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 3 (67). С. 63—71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
 7. Sahu S.K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects // Frontiers in Physics. 2024. Vol. 12. Art. 1456491. DOI: 10.3389/fphy.2024.1456491.
 8. Петренко С.А., Балябин А.А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 1 (65). С. 7—17. DOI: 10.21681/2311-3456-2025-1-7-17. EDN: YYRSOI.
 9. Абдуллин Р.Р., Егоров Д.А., Крупенина Н.В., Рудь В.Ю., Сапожникова Ю.Д. Исследование безопасности квантовых вычислений классическими алгоритмами шифрования // Информационные процессы. 2025. Т. 25, № 3.1. С. 559—572. DOI: 10.53921/18195822_2025_25_3.1_559. EDN: HYZMFC.
 10. Балябин А.А., Петренко С.А. Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. № 3 (67). С. 72—82. DOI: 10.21681/2311-3456-2025-3-72-82. EDN: YEVGTS.
 11. Балябин А.А., Петренко С.А. Методика синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом // Вопросы кибербезопасности. 2025. № 4 (68). С. 46—54. DOI: 10.21681/2311-3456-2025-4-46-54. EDN: CEPHDA.
 12. Ищукова Е.А., Балябин А.А., Петренко С.А. Математическая модель киберустойчивой информационной системы на основе блокчейн-платформы // Вопросы кибербезопасности. 2026. № 3 (73). С. 92—100. DOI: 10.21681/2311-3456-2026-3-92-100. EDN: OWTROC.
 13. Ищукова Е.А., Петренко С.А., Леонтьева Ю.П. Уязвимости асимметричных шифров блокчейн-платформ // Вопросы кибербезопасности. 2025. № 6(70). С. 35—47. DOI: 10.21681/2311-3456-2025-6-35-47. EDN: HUXBQW.
 14. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Вопросы кибербезопасности. 2023. № 1 (53). С. 100—115. DOI: 10.21681/2311-3456-2023-1-100-115. EDN: COMUIK.
 15. Петренко А.С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2025. № 2 (66). С. 52—63. DOI: 10.21681/2311-3456-2025-2-52-63. EDN: RHCWAK.
 16. Петренко А.С. Подход к оптимизации устойчивости национальных блокчейн-платформ и экосистем с помощью квантово-вдохновлённых алгоритмов. Часть 1 // Вопросы кибербезопасности. 2026. № 2 (72). С. 101—111. DOI: 10.21681/2311-3456-2026-2-101-111. EDN: FFBYJF.
 17. Петренко А.С. Подход к оптимизации устойчивости национальных блокчейн-платформ и экосистем с помощью квантово-вдохновлённых алгоритмов. Часть 2 // Вопросы кибербезопасности. 2026. № 3 (73). С. 82—91. DOI: 10.21681/2311-3456-2026-3-82-91. EDN: KWDDJV.
 18. Сундеев П.В. Кластерная модель защиты распределенного реестра // Вопросы кибербезопасности. 2025. № 4 (68). С. 2—8. DOI: 10.21681/2311-3456-2025-4-2-8. EDN: RAXVGN.
 19. Сундеев П.В. Метод оценки выполнения нормативных требований к защите информации // Правовая информатика. 2025. № 4. С. 4—15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
 20. Сундеев П.В. Функциональная устойчивость распределенного реестра в условиях появления новой квантовой угрозы // Вопросы кибербезопасности. 2025. № 3 (67). С. 83—89. DOI: 10.21681/2311-3456-2025-3-83-89. EDN: MIYFUK.
 21. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Vol. 34. No. 3. P. 1156—1190. DOI: 10.1093/rfs/hhaa075.
 22. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717. EDN: EFXKUB.

METHODOLOGY FOR ASSESSING THE QUANTUM RESILIENCE OF BLOCKCHAIN PLATFORMS BASED ON PETRI NETS

Larina M.V.¹⁰, Skiba V.Yu.¹¹

Keywords: quantum threats, consensus, critical information infrastructure, risk assessment, post-quantum cryptography, attack formalization, digital platforms, Proof-of-Stake, Proof-of-Work.

Abstract

Purpose of work is to develop a methodology for assessing the quantum resilience of blockchain platforms based on the mathematical apparatus of Petri nets, designed to model quantum attack scenarios and identify critical states in the operation of a distributed system.

Research methods: analysis of the resilience of Proof-of-Work and Proof-of-Stake consensus mechanisms, formalization of attacks and disruption scenarios using Petri nets, and assessment of the impact of cryptographic, network, and computational parameters on the probability of successful threat realization.

Results of the study: the paper proposes a model that accounts for the relationships between system states, transition parameters, and the probabilities of successful attacks. Based on this approach, a software system was developed for modeling and comparative analysis of security scenarios for blockchain platforms.

Scientific novelty: the proposed methodology for assessing the quantum resilience of blockchain platforms integrates cryptographic, computational, and network parameters within a unified model, together with a scenario-based analysis of the resilience of Proof-of-Work and Proof-of-Stake consensus mechanisms. Formalization in terms of Petri nets links the logical sequence of attack stages with quantitative conditions for their execution, making it possible to identify critical system states, assess the probability of successful attacks, and account for the relationship between cryptographic mechanisms and network structure.

Practical significance: the proposed methodology can be used in the design of quantum-resilient blockchain ecosystems and protection systems for critical information infrastructure.

References

1. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18. No. 2. P. 56—73. DOI: 10.18721/JCSTCS.18205. EDN: DCDMZF.
2. Petrenko A.S., Petrenko S.A. Metod otsenivaniya kvantovoy ustoychivosti blokcheyn-platform // Voprosy kiberbezopasnosti. 2022. No. 3(49). P. 2—22. DOI: 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.
3. Larina M.V., Skiba V.Yu. O klassifikatsii ugroz informatsionnykh sistem v usloviyakh razvitiya kvantovykh tekhnologiy // Pravovaya informatika. 2026. No. 1. P. 5—15. DOI: 10.24412/1994-1404-2026-1-00-01. EDN: XMQASS.
4. Larina M.V., Skiba V.Yu. Utochnenie klassifikatsii informatsionnykh sistem i ugroz v usloviyakh razvitiya kvantovykh tekhnologiy // Ekonomika ustoychivogo razvitiya regiona: innovatsii, finansovye aspekty, tekhnologicheskie drayvery razvitiya v sfere turizma i gostepriimstva: materialy XII mezhd. nauch.-prakt. konf., posvyashchennoy prazdnovaniyu 80-letiya pobedy, Yalta, 26—29 marta 2025 goda. Simferopol: OOO «Tipografiya “Arial”», 2025. P. 182—184. EDN: CDFVGN.

¹⁰ **Maria V. Larina**, research technician of Scientific Center for Information Technology and Artificial Intelligence, Sirius University of Science and Technology, Sirius, Krasnodar region, Russian Federation. ORCID: 0009-0009-7826-0180.

E-mail: larina.mv@talantiuspeh.ru

¹¹ **Vladimir Yu. Skiba**, Doctor of Technical Sciences, Senior Researcher, Chief Research Engineer at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius, Krasnodar region, Russian Federation, Professor of the IBM-6 Department, Federal State Autonomous Educational Institution of Higher Education «Bauman Moscow State Technical University», Moscow, Russian Federation, Professor of Department № 2 «Automation», National Research Nuclear University MEPhI, Moscow, Russian Federation. ORCID: 0000-0002-9805-7800.

E-mail: skiba.vy@talantiuspeh.ru

5. Larina M.V., Skiba V.Yu. Model tsifrovoy platformy dlya analiza ustoychivosti k kvantovym ugrozam // Pravovaya informatika. 2025. No. 3. P. 12—26. DOI: 10.24412/1994-1404-2025-3-00-02. EDN: NDONZQ.
6. Ishchukova E.A. O vliyaniy kriptograficheskoy stoykosti funktsiy kheshirovaniya na ustoychivost sovremennykh blokcheyn-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 63—71. DOI: 10.21681/2311-3456-2025-3-63-71. EDN: UUSWXP.
7. Sahu S.K., Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects // Frontiers in Physics. 2024. Vol. 12. Art. 1456491. DOI: 10.3389/fphy.2024.1456491.
8. Petrenko S.A., Balyabin A.A. Model kvantovykh ugroz bezopasnosti informatsii dlya natsionalnykh blokcheyn-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 1 (65). P. 7—17. DOI: 10.21681/2311-3456-2025-1-7-17. EDN: YYRSOI.
9. Abdullin R.R., Egorov D.A., Krupenina N.V., Rud V.Yu., Sapozhnikova Yu.D. Issledovanie bezopasnosti kvantovykh vychisleniy klassicheskimi algoritmami shifrovaniya // Informatsionnye protsessy. 2025. Vol. 25. No. 3.1. P. 559—572. DOI: 10.53921/18195822_2025_25_3.1_559. EDN: HYZMFC.
10. Balyabin A.A., Petrenko S.A. Model blokcheyn-platformy s kiberimmunitetom v usloviyakh kvantovykh atak // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 72—82. DOI: 10.21681/2311-3456-2025-3-72-82. EDN: YEVGTS.
11. Balyabin A.A., Petrenko S.A. Metodika sinteza kvantovo-ustoychivyykh blokcheyn-platform s kiberimmunitetom // Voprosy kiberbezopasnosti. 2025. No. 4 (68). P. 46—54. DOI: 10.21681/2311-3456-2025-4-46-54. EDN: CEPHDA.
12. Ishchukova E.A., Balyabin A.A., Petrenko S.A. Matematicheskaya model kiberustoychivoy informatsionnoy sistemy na osnove blokcheyn-platformy // Voprosy kiberbezopasnosti. 2026. No. 3 (73). P. 92—100. DOI: 10.21681/2311-3456-2026-3-92-100. EDN: OWTROC.
13. Ishchukova E.A., Petrenko S.A., Leonteva Yu.P. Uyazvimosti asimmetrichnykh shifrov blokcheyn-platform // Voprosy kiberbezopasnosti. 2025. No. 6 (70). P. 35—47. DOI: 10.21681/2311-3456-2025-6-35-47. EDN: HUXBQW.
14. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy kiberbezopasnosti. 2023. No. 1 (53). P. 100—115. DOI: 10.21681/2311-3456-2023-1-100-115. EDN: COMUIK.
15. Petrenko A.S. Metod postroeniya postkvantovykh algoritmov ETsP s dvumya skrytymi gruppami // Voprosy kiberbezopasnosti. 2025. No. 2 (66). P. 52—63. DOI: 10.21681/2311-3456-2025-2-52-63. EDN: RHCWAK.
16. Petrenko A.S. Podkhod k optimizatsii ustoychivosti natsionalnykh blokcheyn-platform i ekosistem s pomoshchyu kvantovo-vdokhnovlennykh algoritmov. Chast 1 // Voprosy kiberbezopasnosti. 2026. No. 2 (72). P. 101—111. DOI: 10.21681/2311-3456-2026-2-101-111. EDN: FFYJF.
17. Petrenko A.S. Podkhod k optimizatsii ustoychivosti natsionalnykh blokcheyn-platform i ekosistem s pomoshchyu kvantovo-vdokhnovlennykh algoritmov. Chast 1 // Voprosy kiberbezopasnosti. 2026. No. 3 (73). P. 82—91. DOI: 10.21681/2311-3456-2026-3-82-91. EDN: KWDDJV.
18. Sundeev P.V. Klasternaya model zashchity raspredelennogo reestra // Voprosy kiberbezopasnosti. 2025. No. 4 (68). P. 2—8. DOI: 10.21681/2311-3456-2025-4-2-8. EDN: RAXVGN.
19. Sundeev P.V. Metod otsenki vypolneniya normativnykh trebovaniy k zashchite informatsii // Pravovaya informatika. 2025. No. 4. P. 4—15. DOI: 10.24412/1994-1404-2025-4-4-15. EDN: DSWFHY.
20. Sundeev P.V. Funktsionalnaya ustoychivost raspredelennogo reestra v usloviyakh poyavleniya novoy kvantovoy ugrozy // Voprosy kiberbezopasnosti. 2025. No. 3 (67). P. 83—89. DOI: 10.21681/2311-3456-2025-3-83-89. EDN: MIYFUK.
21. Saleh F. Blockchain without Waste: Proof-of-Stake // The Review of Financial Studies. 2021. Vol. 34. No. 3. P. 1156—1190. DOI: 10.1093/rfs/hhaa075.
22. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems // Journal of Information Security and Applications. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2020.102717. EDN: EFXKUB.

