МЕТОД ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ БЛОКЧЕЙН-ПЛАТФОРМ НА ОСНОВЕ КИБЕРИММУНИТЕТА

Балябин А. А.[1], Петренко С. А.[2]

DOI: 10.21681/2311-3456-2025-6-127-139

Цель исследования: *обеспечение устойчивости функционирования облачных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации на основе кибериммунитета в условиях гибридных квантово-классических атак.*

Методы исследования: *методы системного анализа, методы теории вероятностей и математической статистики, методы теории устойчивости сложных систем.*

Полученные результаты: *анализ исследований в предметной области показал, что существующие методы обеспечения устойчивости различных информационно-вычислительных систем учитывают по отдельности либо классические, либо квантовые угрозы и не позволяют в полной мере обеспечить устойчивость функционирования облачных блокчейн-платформ в условиях гибридных атак, характеризующихся наличием обеих составляющих. Для разрешения данной проблемной ситуации поставлена задача разработки нового метода обеспечения устойчивости облачных блокчейн-платформ на основе кибериммунитета, а также сформулирована гипотеза о возможности достижения цели исследования за счет применения данного метода.*

Разработан метод обеспечения устойчивости облачных блокчейн-платформ на основе кибериммунитета в условиях гибридных квантово-классических атак, позволяющий обеспечивать требования к показателю вероятности компрометации при ограничении на время выполнения программного цикла узла блокчейн за счет варьирования длины криптографического ключа и коэффициента покрытия кибериммунитета.

Проведено исследование разработанного метода, в ходе которого показана возможность обеспечения требуемой устойчивости облачных блокчейн-платформ в условиях гибридных квантово-классических атак, а также определены условия существования решения, что позволило подтвердить сформулированную гипотезу.

Научная новизна: *разработанный метод впервые учитывает такие новые условия, как гибридные атаки на облачные блокчейн-платформы, которые в формализованном виде описываются через вновь вводимые параметры количества кубитов квантового компьютера, доступных атакующему, и доли вредоносных входных данных. Кроме того, применение метода впервые наделяет облачные блокчейн-платформы новым эмерджентным свойством кибериммунитета, заключающимся в способности обнаруживать известные и ранее неизвестные атаки, направленные на нарушение семантики вычислений, противодействовать им и осуществлять восстановление штатного функционирования при возникновении нарушений.*

Ключевые слова: *угрозы безопасности информации, квантовые угрозы безопасности, облачные блокчейн-экосистемы и платформы, кибербезопасность, методы анализа и синтеза квантово-устойчивого блокчейн.*

Введение

С момента своего появления блокчейн прошел несколько этапов эволюции, каждый из которых связан с внедрением новых технологических решений [1]. Современное состояние развития технологий распределенного реестра характеризуется активным созданием блокчейн-экосистем и платформ, на базе которых разрабатываются смарт-контракты, децентрализованные приложения (dApps), системы децентрализованных финансов (DeFi), децентрализованные организации (DAO) и другие. Ведутся исследования по применению технологий блокчейн для обеспечения безопасности платформ интернета вещей (IoT), облачных, туманных и пограничных вычислений, иных технологий Индустрии 4.0, а также для создания децентрализованной сети Интернет (Web3) [2].

В Российской Федерации технологии распределенного реестра относятся к так называемым «сквозным» технологиям, применяемым в рамках реализации национального проекта «Экономика данных», направленного на цифровизацию отраслей экономики и социальной сферы, достижение технологического суверенитета и лидерства.

Поддержание функционирования полных узлов современных блокчейн-платформ зачастую требует больших вычислительных ресурсов, поэтому в настоящее время ведутся исследования по созданию технологии Blockchain-as-a-Service (BaaS). Данная технология предоставляет возможность разработки, тестирования и развертывания программного обеспечения (ПО) блокчейн-платформ в облачной вычислительной среде [3, 4], как показано на рис. 1.

1 Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус». Федеральная территория «Сириус», Россия. https://orcid.org/0009-0006-3949-154X. E-mail: Balyabin.AA@talantiuspeh.ru

2 Петренко Сергей Анатольевич, доктор технических наук, профессор, руководитель группы, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус». Федеральная территория «Сириус», Россия. ORCID 0000-0003-0644-1731. E-mail: Petrenko.SA@talantiuspeh.ru

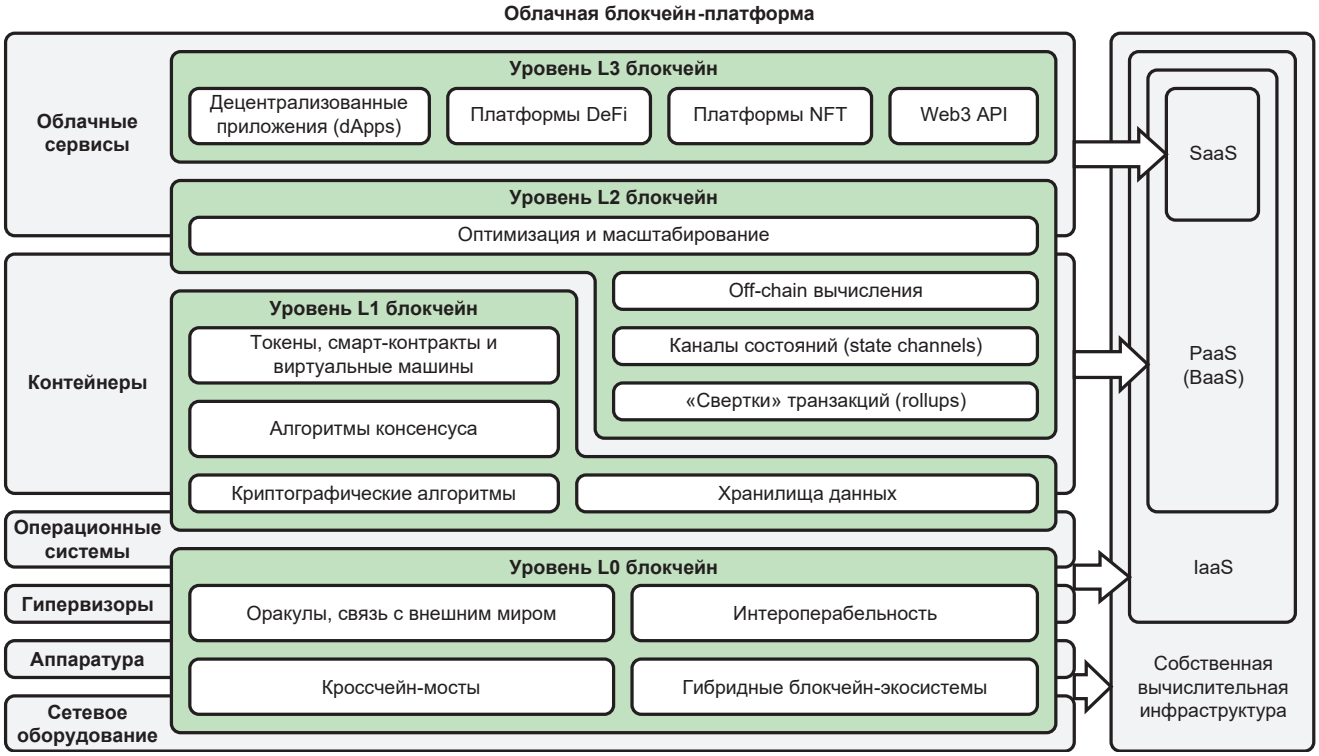

Рис. 1. Архитектура типовой облачной блокчейн-платформы

В то же время усложнение архитектуры информационно-вычислительных систем связано с возникновением новых вызовов. Одним из таких вызовов для облачных блокчейн-платформ является обеспечение требуемой устойчивости их функционирования в условиях гибридных квантовых [5, 6] и классических [7] атак.

Известен ряд исследований в области обеспечения квантовой устойчивости блокчейн. В работах [8–11] предлагается внедрить постквантовые криптографические алгоритмы хэширования, шифрования и цифровой подписи в классические блокчейн-платформы. В работах [12–15] предлагается создание блокчейн-платформ как физических систем, использующих квантовые каналы связи и алгоритмы консенсуса. В работах [16, 17] совмещаются идеи первых двух подходов и предлагается создание гибридного блокчейн. В работах [18, 19] предлагаются новые модели и методы оценивания квантовой устойчивости блокчейн. Классификация данных подходов представлена на рис. 2.

В целом существующие подходы к обеспечению квантовой устойчивости блокчейн-платформ сводятся к применению постквантовых криптографических алгоритмов и не учитывают классические атаки. Однако устойчивость блокчейн-платформ необходимо рассматривать в контексте той вычислительной системы, в которой они функционируют. Облачная платформа дает наиболее общее представление о стеке технологий, применяемых на различных уровнях вычислительных систем, включая уровни сети связи, аппаратного обеспечения, гипервизоров, операционных систем, контейнеров и прикладного ПО. На каждом из этих уровней могут возникать уязвимости, эксплуатация которых может повлиять на устойчивость функционирования облачной блокчейн-платформы [20].

К числу перспективных интеллектуальных и биоинспирированных подходов к обеспечению устойчивости различных информационно-вычислительных систем можно отнести подходы на основе реконфигурации и гомеостаза [21], антиципации и синтеза упреждающего поведения систем защиты [22], совершенствования систем обнаружения вторжений с использованием алгоритмов машинного обучения [23], глубокого обучения [24], федеративного обучения [25], искусственных иммунных систем [26], а также подходы на основе организации самовосстанавливающихся вычислений и кибериммунитета [27, 28]. Однако вышеуказанные подходы к обеспечению устойчивости не учитывают наличие квантовых угроз.

С учетом вышесказанного можно сделать вывод о том, что существующие методы учитывают по отдельности либо классические, либо квантовые угрозы и не позволяют в полной мере обеспечить устойчивость функционирования облачных блокчейн-платформ в условиях гибридных атак,

Рис. 2. Основные подходы к обеспечению устойчивости блокчейн-платформ в условиях квантовых атак

характеризующихся наличием обеих составляющих. Рост гибридных квантово-классических угроз для облачных блокчейн-платформ, невозможность обеспечения требуемой устойчивости их функционирования с использованием существующих технических и технологических решений, а также невозможность разработки таких научно-обоснованных решений ввиду несовершенства существующего научно-методического аппарата характеризует проблемную ситуацию, разрешение которой является актуальной научной задачей.

В настоящем исследовании предлагается метод обеспечения устойчивости облачных блокчейн-платформ на основе кибериммунитета в условиях гибридных квантово-классических атак. Идея *кибериммунитета* заключается в наделении таких платформ способностью обнаруживать как известные, так и ранее неизвестные гибридные атаки, противодействовать им, не допуская нарушений, а также оперативно восстанавливать штатное функционирование в случае их возникновения.

1. Возможные сценарии гибридных квантово-классических атак

На узлах блокчейн функционирует идентичное или схожее ПО одного типа, обеспечивающее обмен данными и синхронизацию состояния распределенного реестра. Взаимодействие узлов осуществляется в одноранговой сети посредством p2p-каналов, поэтому выявление и эксплуатация уязвимостей ПО блокчейн-платформы может привести к компрометации узла и распространению атаки на остальную блокчейн-сеть.

Гибридные квантовые и классические атаки могут использовать сценарии воздействий, сочетающие применение вычислительного потенциала квантового компьютера для вскрытия криптографических алгоритмов и эксплуатацию ранее неизвестных программных уязвимостей, как показано на рис. 3. Такие воздействия могут позволить злоумышленнику создавать ботнет-сети из зараженных узлов блокчейн [29], координировать их действия для внедрения вредоносных транзакций, принятия произвольных цепочек блоков и влияния на алгоритмы консенсуса, что создает серьезную угрозу устойчивости функционирования облачных блокчейн-платформ.

Для противодействия подобным угрозам необходимо применять комплексные меры, обеспечивающие невозможность воздействия на вычислительную среду и алгоритмы функционирования облачных блокчейн-платформ. Данные меры включают наделение ПО блокчейн-платформ свойством кибериммунитета и управление устойчивостью их функционирования.

2. Постановка задачи разработки метода

Устойчивость функционирования облачной блокчейн-платформы с кибериммунитетом в условиях гибридных квантово-классических атак зависит от способности узлов блокчейн противодействовать таким

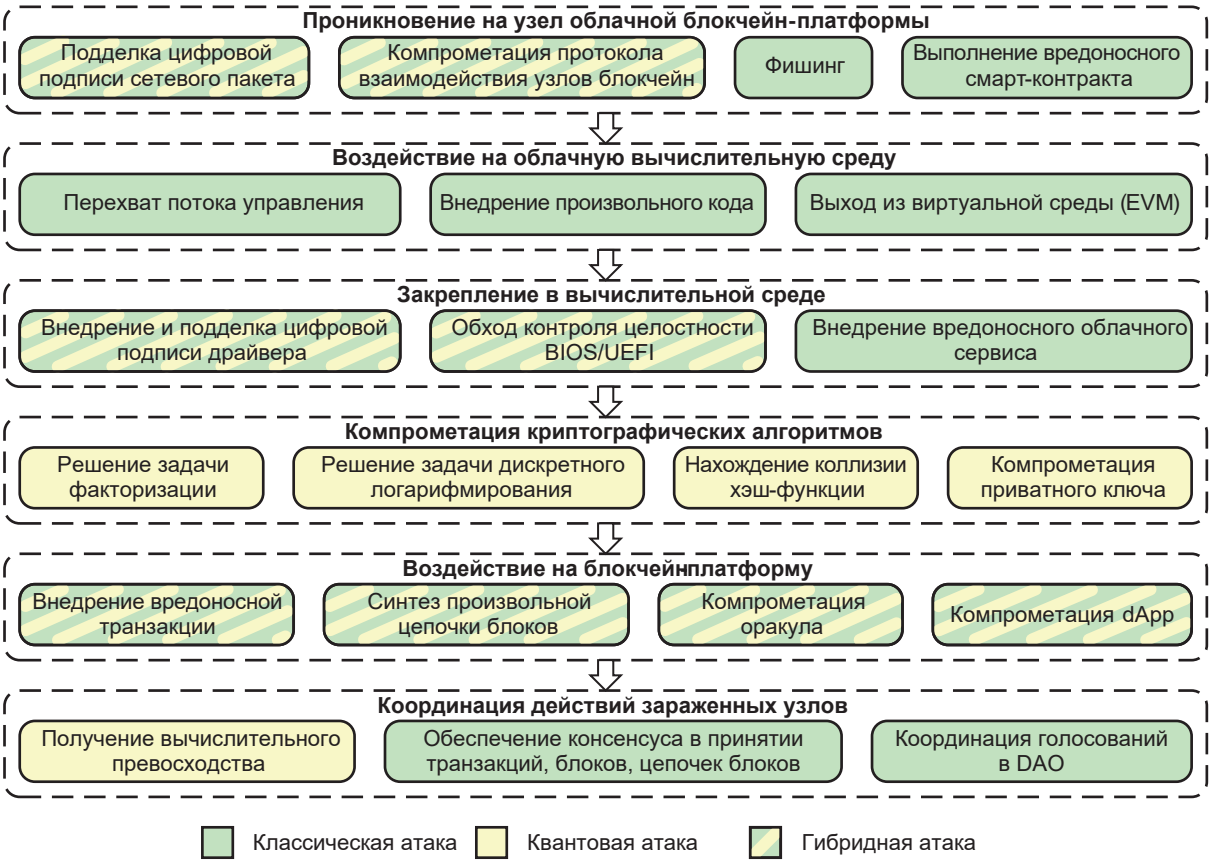

Рис. 3. Возможные сценарии гибридных квантово-классических атак на облачные блокчейн-платформы

атакам, не допуская нарушений, и восстанавливать штатное функционирование при их возникновении. При этом квантовые атаки направлены на компрометацию криптографических алгоритмов с использованием вычислительной мощности квантового компьютера, а классические атаки – на нарушение семантики вычислений путем отправки вредоносных входных данных. Управление устойчивостью облачной блокчейн-платформы должно осуществляться путем варьирования параметров противодействия квантовым и классическим атакам. Введем обозначения:

L – облачная блокчейн-платформа;

$P_{\text{компр}}$ – вероятность компрометации облачной блокчейн-платформы вследствие гибридной атаки;

$P_{\text{компр.узла}}$ – вероятность компрометации узла облачной блокчейн-платформы;

$T_{\text{цикла}}$ – время выполнения цикла вычислений на узле;

$N_{\text{вал}}$ – общее количество валидаторов, участвующих в алгоритме консенсуса;

$N_{\text{конс}}$ – количество голосов валидаторов, необходимое для влияния на алгоритм консенсуса (в блокчейн-системах для получения вычислительного превосходства злоумышленнику достаточно получить контроль над 51 % узлов, поэтому примем данный параметр равным $0{,}51N_{\text{вал}}$);

Q – доступное количество логических кубитов квантового компьютера;

$k_{\text{вред}}$ – доля вредоносных входных данных облачной блокчейн-платформы;

$n_{\text{ключа}}$ – длина криптографического ключа в битах;

$k_{\text{покр}}$ – коэффициент покрытия кибериммунитета, определяющий долю линейных блоков программ, подлежащих контролю семантики вычислений.

Вероятность компрометации облачной блокчейн-платформы $P_{\text{компр}}$ определяется вероятностью того, что атакующему вследствие гибридной атаки удастся получить управление не менее, чем над $N_{\text{конс}}$ узлов валидаторов, обеспечив таким образом возможность влияния на алгоритм консенсуса. Компрометация каждого из узлов является независимым событием, а значит, общую вероятность компрометации облачной блокчейн-платформы можно вычислить с использованием формулы для биномиального распределения:

$$P_{\text{компр}} = \sum_{i=N_{\text{конс}}}^{N_{\text{вал}}} \binom{N_{\text{вал}}}{N_{\text{конс}}} P^{i}_{\text{компр.узла}} (1 - P_{\text{компр.узла}})^{N_{\text{вал}} - N_{\text{конс}}}. \quad (1)$$

Таким образом, необходимо разработать метод M обеспечения требуемой устойчивости

функционирования облачной блокчейн-платформы L по показателю вероятности компрометации $P_{\text{компр}}$ при ограничении на время выполнения цикла вычислений на узле $T_{\text{цикла}}$, в условиях квантовых атак, характеризуемых количеством кубитов Q, и классических атак, характеризуемых долей вредоносных входных данных $k_{\text{вред}}$, за счет варьирования длины ключа $n_{\text{ключа}}$ и коэффициента покрытия киберимунитета $k_{\text{покр}}$:

$$M: <L,\{Q,k_{\text{вред}}\},\{n_{\text{ключа}},k_{\text{покр}}\}> \longrightarrow <P_{\text{компр}},T_{\text{цикла}}>, \quad \begin{cases} P_{\text{компр}} \le P_{\text{компр}}^{\text{тр}} \\ T_{\text{цикла}} \le T_{\text{цикла}}^{\text{тр}} \end{cases}. \tag{2}$$

Гипотеза исследования состоит в том, что применение данного метода позволяет обеспечить требуемую устойчивость функционирования облачных блокчейн-платформ в условиях гибридных квантово-классических атак.

3. Формализация метода обеспечения устойчивости облачных блокчейн-платформ

Для формализации метода введем дополнительные обозначения:

$N_{\text{ур}}$ – количество уровней облачной блокчейн-платформы;

$P_{\text{компр.кв}}$ – вероятность компрометации узла в результате квантовой атаки;

$P_{\text{Шора}}$ – вероятность успеха квантовой атаки с применением алгоритма Шора;

$P_{\text{Гровера}}$ – вероятность успеха квантовой атаки с применением алгоритма Гровера;

t_{gate} – время выполнения квантового вентиля ($t_{\text{gate}} \simeq 10^{-7}$ с);

$t_{\text{ког}}$ – время сохранения когерентности кубитов;

$N_{\text{попыток}}$ – допустимое количество попыток вскрытия криптосистемы;

$P_{\text{компр.кл}}$ – вероятность компрометации узла в результате классической атаки;

$P_{\text{прот}}$ – вероятность успешного противодействия классической атаке;

$T_{\text{ср.атак}}$ – среднее время между пропусками классических атак;

$P_{\text{восст}}$ – вероятность успешного восстановления после нарушения;

$T_{\text{ср.восст}}$ – среднее время восстановления после нарушения;

$P_{\text{раб}}$ – вероятность нахождения облачной блокчейн-платформы в работоспособном состоянии в произвольный момент времени;

$P_{\text{мод}}$ – вероятность модификации вычислений при пропуске классической атаки;

$T_{\text{выч}}$ – время выполнения вычислительных операций;

$T_{\text{обн}}$ – время обнаружения нарушений семантики вычислений;

$T_{\text{восст}}$ – время восстановления штатного функционирования;

t_0 – время выполнения элементарной операции (при расчетах t_0 = 1 ед. времени);

$k_{\text{изв}}$ – доля классических атак, являющихся известными;

p – вероятность обнаружения нарушения, возникшего вследствие ранее неизвестной классической атаки;

k – количество линейных блоков программ;

m – количество вычислительных инструкций в блоке;

n – количество параметров в инструкции.

Каждый узел облачной блокчейн-платформы, как было показано ранее, функционирует на $N_{\text{ур}}$ уровнях, которые могут быть одновременно подвержены гибридным атакам. Вероятность компрометации узла зависит от вероятности успеха гибридной атаки, включающей классическую и квантовую составляющие:

$$P_{\text{компр.узла}} = 1 - (1 - P_{\text{компр.кл}})(1 - P_{\text{компр.кв}}). \tag{3}$$

Успешность квантовой атаки зависит от применяемого алгоритма (Шора или Гровера), количества кубитов квантового компьютера атакующего и длины ключа, являющейся параметром противодействия такой атаке. Тогда вероятность компрометации узла в результате квантовой атаки может быть определена как

$$P_{\text{компр.кв}} = 1 - ((1 - P_{\text{Шора}})(1 - P_{\text{Гровера}}))^{N_{\text{ур}}}. \tag{4}$$

Вероятности $P_{\text{Шора}}$ и $P_{\text{Гровера}}$ с учетом оценок, полученных в работе [30], можно приближенно оценить как

$$P_{\text{Шора}} = 1 - \left(1 - e^{\frac{-2n_{\text{ключа}}}{Q}\frac{n_{\text{ключа}}^3 t_{\text{gate}}}{t_{\text{ког}}}}\right)^{N_{\text{попыток}}}, \tag{5}$$

$$P_{\text{Гровера}} = 1 - \left(1 - e^{\frac{-n_{\text{ключа}}}{Q}\frac{\pi}{4}\frac{2^{n_{\text{ключа}}/2} t_{\text{gate}}}{t_{\text{ког}}}}\right)^{N_{\text{попыток}}}. \tag{6}$$

Следует отметить, что данные оценки не учитывают многокубитные корреляции, коррекцию ошибок и возможность продления времени когерентности с использованием логических кубитов. Последнее сильно зависит от типа применяемого квантового компьютера. Например, применение сверхпроводникового квантового компьютера на базе кубитов-трансмонов позволяет достичь времени когерентности $t_{\text{ког}}$ = 0,5 мс [31], а применение квантового компьютера на базе фотонов в микроволновых резонаторах – $t_{\text{ког}}$ = 34 мс [32]. В дальнейшем для оценки будем использовать время когерентности порядка $t_{\text{ког}} \simeq 10^{-2}$ с. На рис. 4 представлены оценки вероятностей успеха квантовых атак (5) и (6) с использованием алгоритмов Шора и Гровера при различном количестве кубитов, длине ключа и допустимом количестве попыток.

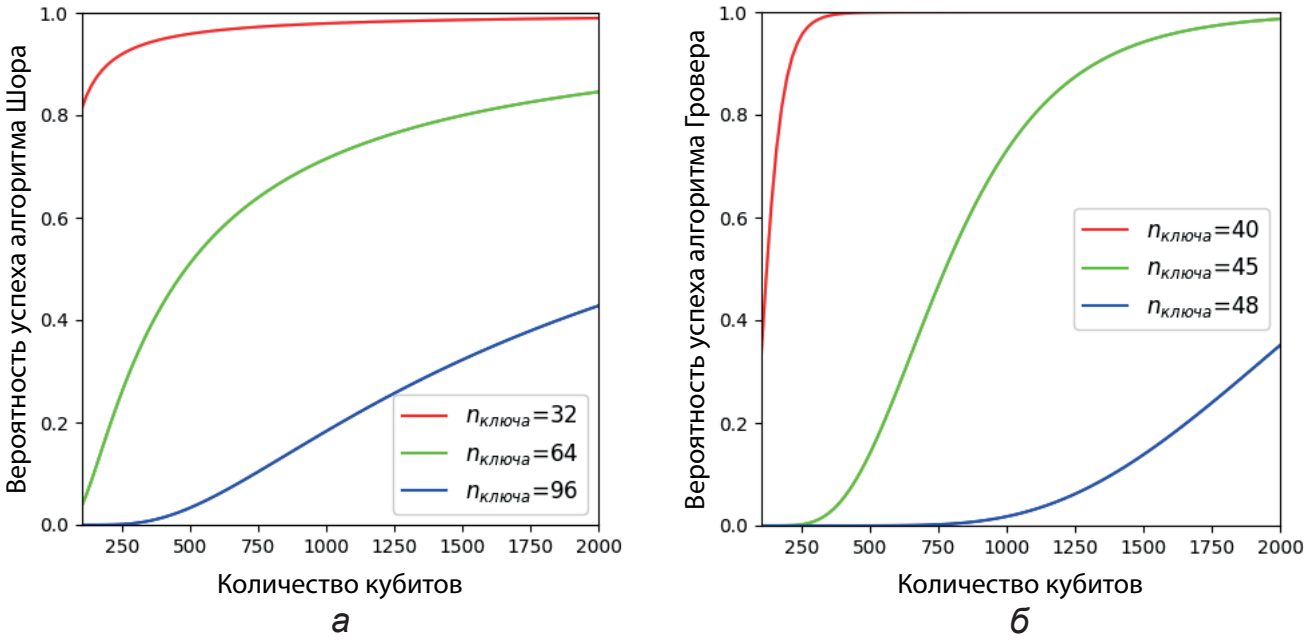

Рис. 4. Вероятности успеха квантовых атак с использованием: а – алгоритма Шора; б – алгоритма Гровера

Классические атаки на облачные блокчейн-платформы осуществляются путем отправки вредоносных входных данных, обработка которых приводит к нарушению семантики вычислений (появлению аномального состояния программы, не соответствующего ожидаемому или заданному эталонной моделью). Вероятность компрометации узла вследствие классической атаки зависит от его способности противодействовать таким атакам, не допуская нарушений семантики, и оперативно восстанавливать штатное функционирование при их возникновении, сохраняя при этом работоспособное (устойчивое) состояние. Данный показатель с учетом [33] может быть определен как

$$P_{\text{компр.кл}} = 1 - ((P_{\text{прот}} + (1 - P_{\text{прот}})P_{\text{восст}})P_{\text{раб}})^{N_{\text{ур}}}. \quad (7)$$

Вероятность успешного противодействия узла классической атаке обратна вероятности пропуска такой атаки и возникновения модификации вычислений. Пропуск атаки возможен, если она произошла на участке программы, защищенном механизмами кибериммунитета, но не была обнаружена (событие S_1), либо если она произошла на незащищенном участке программы (событие S_2):

$$P_{\text{прот}} = 1 - P_{\text{мод}}\,(P(S_1) + P(S_2)). \quad (8)$$

Здесь $P(S_1)$ и $P(S_2)$ могут быть определены соответственно как

$$P(S_1) = (k_{\text{вред}}\,(1 - P_{\text{обн}}))(k_{\text{покр}}\,(1 - P_{\text{обн}})), \quad (9)$$

$$P(S_2) = k_{\text{вред}}\,(1 - P_{\text{обн}})(1 - k_{\text{покр}}), \quad (10)$$

тогда, подставив (9) и (10) в формулу (8) и преобразовав, получим:

$$P_{\text{прот}} = 1 - P_{\text{мод}}\,k_{\text{вред}}\,(1 - P_{\text{обн}})(1 - k_{\text{покр}}\,P_{\text{обн}}). \quad (11)$$

Вероятность восстановления штатного функционирования узла облачной блокчейн-платформы напрямую зависит от вероятности обнаружения нарушения. Предположим, что все обнаруженные нарушения восстанавливаются одним из способов (возврат к предыдущему устойчивому состояния, перезапуск), известные нарушения обнаруживаются всегда, а ранее неизвестные – с вероятностью p, тогда вероятность обнаружения и восстановления можно определить как

$$P_{\text{восст}} = P_{\text{обн}} = k_{\text{изв}}1 + (1 - k_{\text{изв}})p. \quad (12)$$

Одним из показателей устойчивости функционирования узла облачной блокчейн-платформы в условиях классических атак является также вероятность его нахождения в работоспособном состоянии в произвольный момент времени. Данный показатель по смыслу схож с коэффициентом готовности и может быть определен как

$$P_{\text{раб}} = \frac{T_{\text{ср.атак}}}{T_{\text{ср.атак}} + T_{\text{ср.восст}}}. \quad (13)$$

Здесь $T_{\text{ср.атак}}$ характеризует среднюю продолжительность функционирования узла между пропусками атак и может быть определена как отношение времени вычислений с учетом контроля семантики за $n_{\text{ц}}$ циклов к ожидаемому количеству пропусков атак за это время:

$$T_{\text{ср.атак}} = \frac{n_{\text{ц}}\,(T_{\text{выч}} + T_{\text{обн}})}{n_{\text{ц}}\,(1 - P_{\text{прот}})} = \frac{T_{\text{выч}} + T_{\text{обн}}}{1 - P_{\text{прот}}}, \quad (14)$$

а $T_{\text{ср.восст}}$ в отличие от абсолютного времени, необходимого для восстановления $T_{\text{восст}}$, учитывает

ожидаемое количество успешных восстановлений за $n_ц$ циклов:

$$T_{ср.восст} = \frac{n_ц\, T_{восст}}{n_ц\, P_{восст}} = \frac{T_{восст}}{P_{восст}}. \quad (15)$$

Общее время выполнения программного цикла на узле облачной блокчейн-платформы, включая непосредственно вычисления, обнаружение нарушений и восстановление, может быть определено как:

$$T_{цикла} = T_{выч} + T_{обн} + T_{восст}, \quad (16)$$

где $T_{выч}$ и $T_{восст}$ зависят от параметров программы и могут быть определены как время выполнения вычислительных инструкций во всех линейных блоках с учетом количества параметров и время перезаписи полного образа программы в памяти (время выполнения операций чтения-записи) соответственно:

$$T_{выч} = kmnt_0, \quad (17)$$

$$T_{восст} = 2kmnt_0. \quad (18)$$

Время, затрачиваемое на обнаружение нарушений в течение программного цикла, зависит от применяемой для контроля семантики эталонной модели программы. Например, в работе [34] показано, что при применении аппарата теории подобия и размерностей время обнаружения нарушений определяется как

$$T_{обн} = k_{покр}\left(k\frac{m(m-1)}{2}(2n-1) + kmn\right)t_0. \quad (19)$$

С учетом введенных обозначений и формальных отношений можно сформулировать метод обеспечения устойчивости облачных блокчейн-платформ в условиях гибридных квантово-классических атак.

Входные данные метода:

- параметры облачной блокчейн-платформы;
- параметры гибридных атак (квантовых – Q и классических – $k_{вред}$);
- текущие параметры противодействия (длина ключа $n_{ключа}$, коэффициент покрытия кибериммунитета $k_{покр}$);
- требования к показателям устойчивости (вероятности компрометации $P^{тр}_{компр}$ и времени выполнения программного цикла на узле блокчейн $T^{тр}_{цикла}$.

Выходные данные метода:

- значения показателей устойчивости функционирования облачной блокчейн-платформы;
- вывод о достижении или невозможности достижения требуемой устойчивости.

Шаг 1. Выбор начальных значений длины криптографического ключа $n_{ключа}$ и коэффициента покрытия кибериммунитета $k_{покр}$ так, чтобы

$$P_{компр.кв}(n_{ключа}) \longrightarrow \min \text{ и } P_{компр.кл}(k_{покр}) \longrightarrow \min.$$

Шаг 2. Оценка максимально допустимого значения коэффициента покрытия кибериммунитета $k^{max}_{покр}$ на основе заданного требования к времени выполнения программного цикла на узле блокчейн $T^{тр}_{цикла}$. Данную оценку можно получить, подставив выражения (17)–(19) в (16) и решив неравенство $T_{цикла}(k_{покр}) \leq T^{тр}_{цикла}$ относительно $k_{покр}$:

$$k^{max}_{покр} = \frac{T^{тр}_{цикла} - 3kmnt_0}{\left(k\frac{m(m-1)}{2}(2n-1) + kmn\right)t_0}. \quad (20)$$

Шаг 3. Выбор текущего значения $k_{покр} \in [0, k^{max}_{покр}]$, минимизирующего вероятность успеха классической атаки при ограничении на время выполнения программного цикла, и переконфигурация кибериммунной системы защиты для контроля семантики вычислений с учетом нового коэффициента покрытия.

Шаг 4. Оценка текущей вероятности компрометации узла облачной блокчейн-платформы $P_{компр.узла}$ в условиях гибридных атак на основе формулы (3). Отметим, что при выборе достаточно большого значения $n_{ключа}$ вероятность успеха квантовой атаки будет пренебрежимо мала по сравнению с аналогичной вероятностью для классической атаки $P_{компр.кв} \ll P_{компр.кл}$. Однако увеличение длины ключа является временной мерой и может привести к существенному росту вычислительной сложности и времени функционирования блокчейн-платформы. Для эффективного противодействия квантовым атакам следует применять постквантовые криптографические алгоритмы.

Шаг 5. Оценка текущей вероятности компрометации облачной блокчейн-платформы $P_{компр}$ на основе формулы (1). Если $P_{компр} \leq P^{тр}_{компр}$, то требуемая устойчивость облачной блокчейн-платформы в условиях гибридных квантово-классических атак считается достигнутой. Иначе, при $k_{покр} < k^{max}_{покр}$ следует вернуться к шагу 3 и выполнить переконфигурацию кибериммунной системы защиты, увеличив долю контролируемых линейных блоков программ. Если же $k_{покр} = k^{max}_{покр}$, то считается, что в текущих условиях невозможно обеспечить требуемую устойчивость функционирования облачной блокчейн-платформы и необходимо принятие дополнительных мер защиты.

Общая схема предложенного метода представлена на рис. 5.

Условием возможности обеспечения требуемой устойчивости облачной блокчейн-платформы по показателю вероятности компрометации при ограничении на время выполнения программного цикла на узле блокчейн является существование таких значений $n_{ключа}$ и $k_{покр}$, что

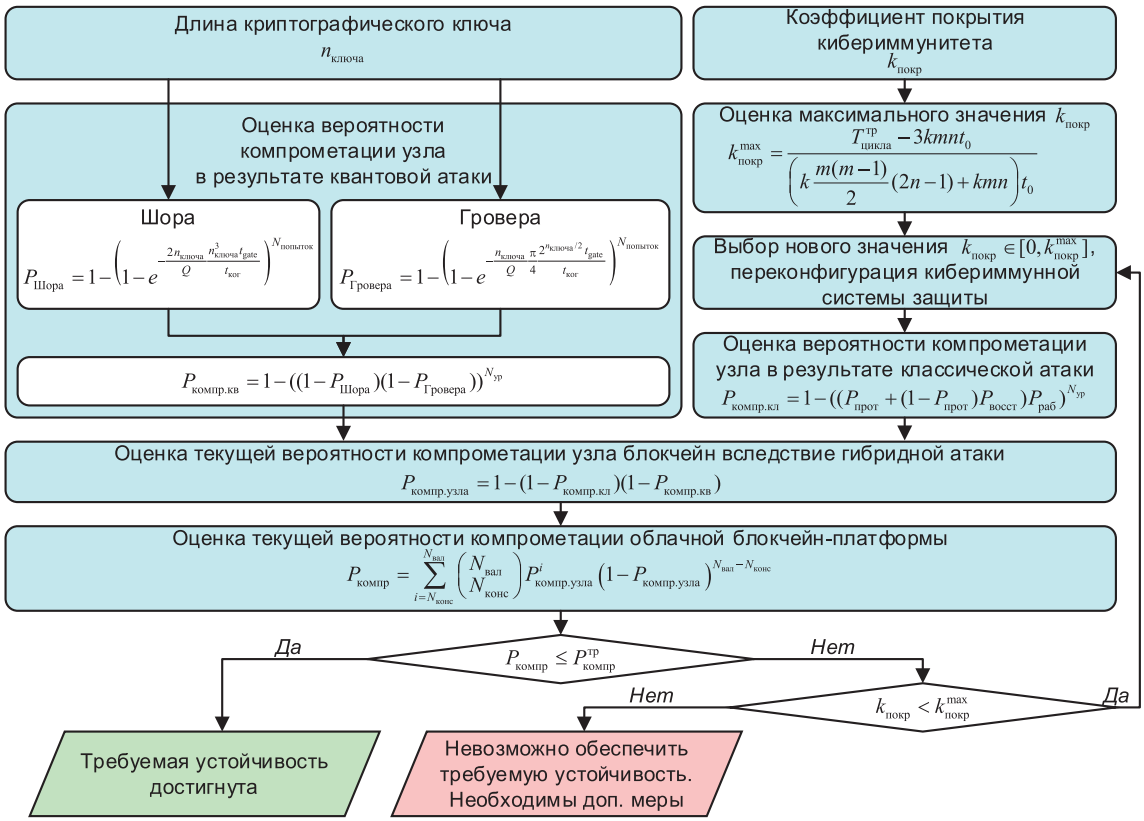

Рис. 5. Схема метода обеспечения устойчивости облачных блокчейн-платформ в условиях гибридных квантово-классических атак

$$\exists n_{ключа}, k_{покр} : \begin{cases} P_{компр}(n_{ключа}, k_{покр}) \le P_{компр}^{тр} \\ T_{цикла}(n_{ключа}, k_{покр}) \le T_{цикла}^{тр} \end{cases}. \quad (21)$$

4. Исследование метода обеспечения устойчивости облачных блокчейн-платформ

Для проверки выдвинутой гипотезы проведем экспериментальное исследование разработанного метода. Целью эксперимента является определение влияния параметров гибридных атак, а именно количества кубитов и доли вредоносных входных данных, на вероятность компрометации узла облачной блокчейн-платформы, а также определение возможностей обеспечения требуемой устойчивости функционирования облачной блокчейн-платформы за счет применения разработанного метода.

Зададим начальные значения параметров: $N_{вал}$ = 10000, k = 1000, m = 5, n = 2 – как практически возможные параметры облачных блокчейн-платформ; $N_{ур}$ =4, $k_{изв}$ =0,4, $P_{мод}$ = 0,75, p = 0,875 – на основе результатов исследования облачных платформ с кибериммунитетом [33, 34]; b = 0,51, t_{gate} = 10^{-7}, $t_{ког}$ = 10^{-2} – на основе принятых в настоящей работе допущений.

На рис. 6 представлены результаты исследования зависимости вероятности компрометации узла вследствие квантовой и классической атак от длины криптографического ключа и коэффициента покрытия кибериммунитета соответственно, полученные на основе формул (4) и (7).

Как видно на рис. 6а, увеличение длины криптографического ключа $n_{ключа}$ затрудняет осуществление квантовой атаки с применением алгоритмов Шора и Гровера даже при наличии у атакующего квантового компьютера с достаточно большим количеством кубитов (Q = 1000 и более). Так, например, при использовании 256-битного ключа в криптосистеме AES вычислительная сложность перебора с помощью алгоритма Гровера составит $O(2^{128})$, что делает практически невозможной ее компрометацию за разумное время при текущих ограничениях квантовых вычислений. На рис. 6б видно, что увеличение доли линейных блоков программ, для которых выполняется контроль семантики вычислений, определяемой коэффициентом покрытия кибериммунитета $k_{покр}$, положительно влияет на способность узла блокчейн противодействовать классическим атакам и снижает вероятность его компрометации. Таким образом, увеличение значений $n_{ключа}$ и $k_{покр}$ повышает устойчивость функционирования узла облачной блокчейн-платформы в условиях гибридных атак.

Пусть теперь требуется обеспечить общую вероятность компрометации облачной блокчейн-платформы

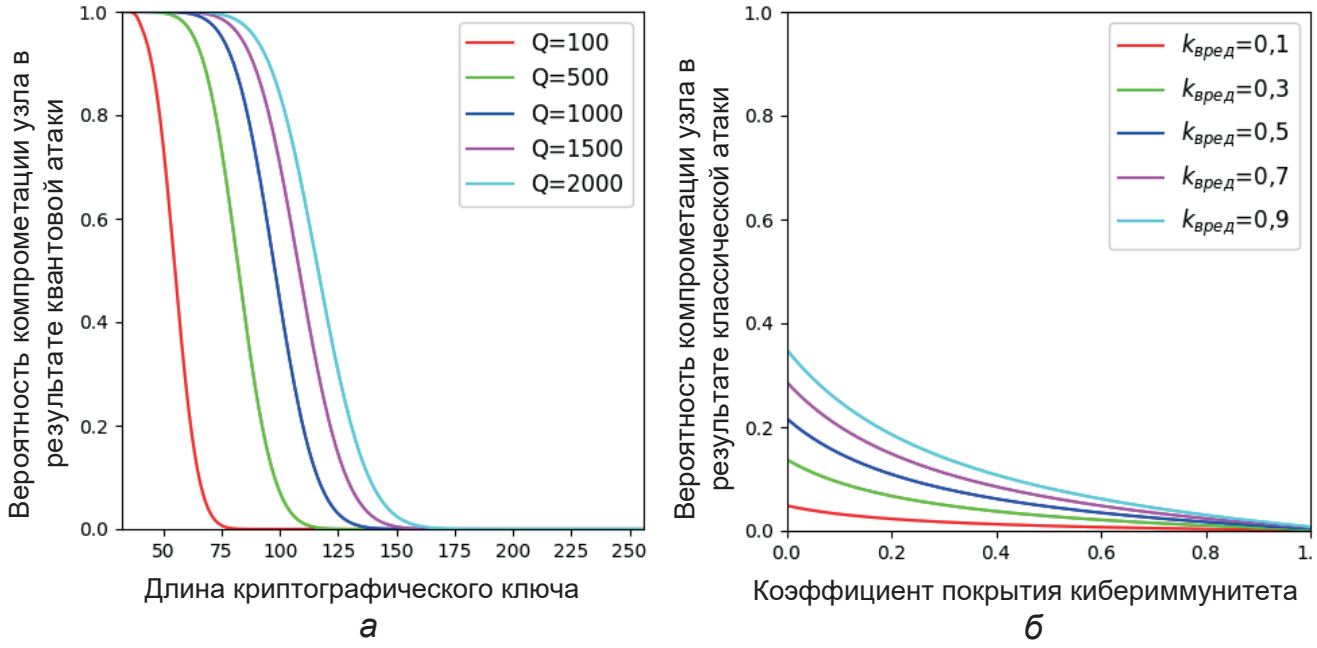

Рис. 6. Вероятность компрометации узла: а – вследствие квантовой атаки; б – вследствие классической атаки

не выше $P^{тр}_{компр}$ = 0,05 и время выполнения программного цикла на узле блокчейн не более $T^{тр}_{цикла}$ = = 45000 ед. времени. На рис. 7 представлены результаты исследования вероятности компрометации облачной блокчейн-платформы в условиях гибридных квантово-классических атак при применении разработанного метода, полученные на основе формулы (1).

При заданных параметрах облачной блокчейн-платформы и требовании к времени выполнения программного цикла на узлах блокчейн максимально допустимое значение коэффициента покрытия киберимунитета, вычисленное на основе (20), составило $k^{max}_{покр}$ = 0,375. Для случаев, представленных на рис. 7а, применение разработанного метода позволяет обеспечить требуемую устойчивость

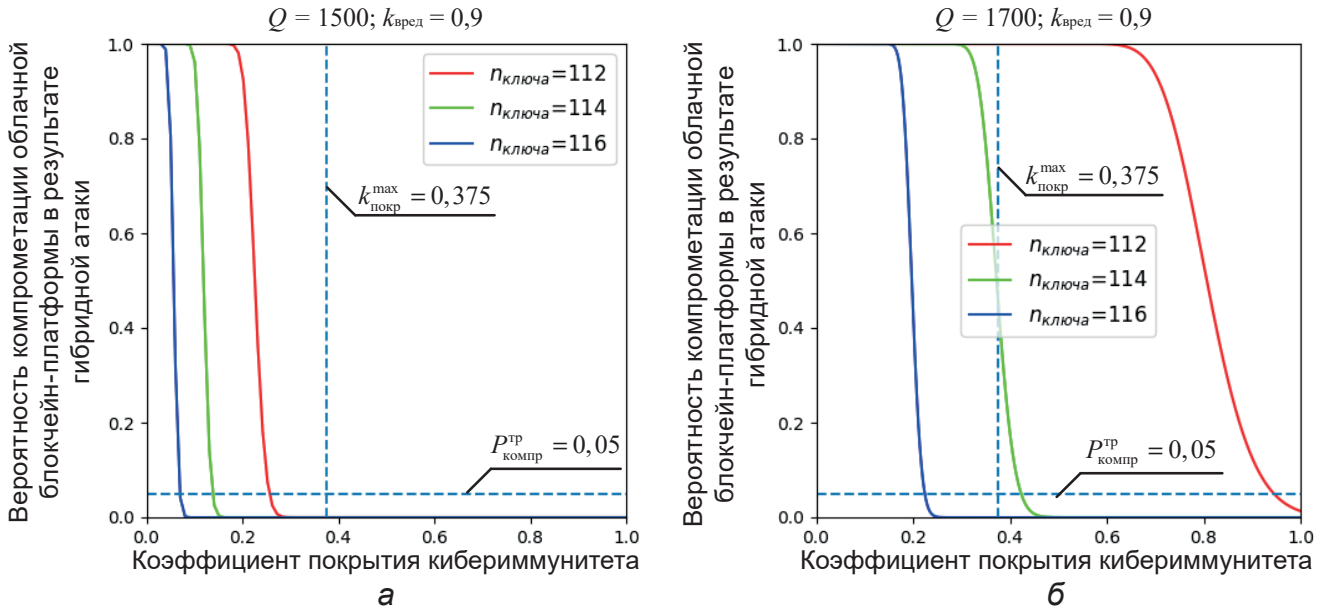

Рис. 7. Вероятность компрометации облачной блокчейн-платформы вследствие гибридных квантово-классических атак: а – при наличии возможности обеспечения требуемой устойчивости; б – при отсутствии возможности обеспечения требуемой устойчивости

функционирования облачной блокчейн-платформы в условиях гибридных атак за счет варьирования $k_{\text{покр}}$ в диапазоне $[0, k_{\text{покр}}^{\max}]$. Однако при увеличении количества кубитов, доступных атакующему, до $Q = 1700$ обеспечение требуемой устойчивости в соответствии и условием (21) становится возможным лишь при $n_{\text{ключа}} = 116$ (рис. 7б), в остальных же случаях необходимо применение дополнительных мер защиты.

Таким образом, результаты экспериментальных исследований согласуются с теоретическими выводами, а значит выдвинутую гипотезу о том, что применение разработанного метода позволяет обеспечить требуемую устойчивость функционирования облачных блокчейн-платформ в условиях гибридных квантово-классических атак, можно считать подтвержденной.

Выводы

В работе предложен метод обеспечения устойчивости облачных блокчейн-платформ на основе кибериммунитета, позволяющий обеспечивать требования к показателю вероятности компрометации при ограничении на время выполнения программного цикла узла блокчейн за счет варьирования длины криптографического ключа и коэффициента покрытия кибериммунитета. Сформулирована и экспериментально подтверждена гипотеза о том, что применение данного метода позволяет обеспечить требуемую устойчивость функционирования облачных блокчейн-платформ в условиях гибридных квантово-классических атак.

Достоверность исследования подтверждается согласованностью результатов эксперимента с теоретическими выводами, а также непротиворечивостью полученных результатов с известными работами в предметной области.

К направлениям дальнейших исследований можно отнести следующее:

- исследование возможностей применения методов искусственного интеллекта и машинного обучения для оптимального управления параметрами противодействия квантово-классическим атакам;
- исследование возможностей применения иных математических аппаратов для контроля семантики вычислений на узлах блокчейн (лямбда-исчисления; троек Хоара; схем Ляпунова, Лаврова, Ершова, Янова, Летичевского; темпоральных логик; систем алгоритмических алгебр и других);
- разработка научно-обоснованных рекомендаций по созданию и внедрению технических и технологических решений для обеспечения требуемой устойчивости функционирования облачных блокчейн-экосистем и платформ «Экономики данных» Российской Федерации в условиях гибридных квантово-классических атак.

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 №23-03 от 27.09.2024 г.).

Литература

1. Mourtzis D., Angelopoulos J., Panopoulos N. Blockchain Integration in the Era of Industrial Metaverse // Applied Sciences. 2023. Vol. 13. No. 3. P. 1353. DOI: 10.3390/app13031353.
2. Марков А. С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1(53). С. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Gai K., Guo J., Zhu L., Yu S. Blockchain Meets Cloud Computing: A Survey // IEEE Communications Surveys & Tutorials. 2020. Vol. 22. No. 3. Pp. 2009–2030. DOI: 10.1109/COMST.2020.2989392.
4. Khanna A., Sah A., Bolshev V., Burgio A., et al. Blockchain–Cloud Integration: A Survey // Sensors. 2022. No. 22(14). P. 5238. DOI: 10.3390/s22145238.
5. Петренко А. С., Ломако А. Г., Петренко С. А. Анализ современного состояния исследований проблемы квантовой устойчивости блокчейна. Часть 1 // Защита информации. Инсайд. 2023. № 3(111). С. 38–46.
6. 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.
7. Балябин А. А., Петренко С. А., Костюков А. Д. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ // Защита информации. Инсайд. 2024. № 5(119). С. 26–34.
8. Fernandez-Carames T. M., Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks // IEEE Access. 2020. Vol. 8. Pp. 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
9. Shahid F., Khan A. Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers // Future Generation Computer Systems. 2020. Vol. 111. Pp. 241–253. DOI: 10.1016/j.future.2020.04.042.
10. Sahin M. S., Akleylek S. A survey of quantum secure group signature schemes: Lattice-based approach // Journal of Information Security and Applications. 2023. Vol. 73. P. 103432. DOI: 10.1016/j.jisa.2023.103432.
11. Москвин В. С., Богатырев В. А. Постквантовые алгоритмы электронной цифровой подписи и их использование в распределенном реестре // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 47–53. DOI: 10.36724/2409-5419-2022-14-4-47-53.

12. Yang Z., Salman T., Jain R., Pietro R. D. Decentralization Using Quantum Blockchain: A Theoretical Analysis // IEEE Transactions on Quantum Engineering. 2020. Vol. 3. Pp. 1–16. DOI: 10.1109/TQE.2022.3207111.
13. Li Q., Wu J., Quan J., Shi J., Zhang S. Efficient Quantum Blockchain With a Consensus Mechanism QDPoS // IEEE Transactions on Information Forensics and Security. 2022. Vol. 17. Pp. 3264–3276. DOI: 10.1109/TIFS.2022.3203316.
14. Wen X. J., Chen Y. Z., Fan X. C., Zhang W., et al. Blockchain consensus mechanism based on quantum zero-knowledge proof // Optics and Laser Technology. 2022. Vol. 147. P. 107693. DOI: 10.1016/j.optlastec.2021.107693.
15. Sun X., Kulicki P., Sopek M. Multi-Party Quantum Byzantine Agreement without Entanglement // Entropy. 2020. Vol. 22. No. 10. P. 1152. DOI: 10.3390/e22101152.
16. Singh S., Rajput N. K., Rathi V. K., Pandey H. M., et al. Securing Blockchain Transactions Using Quantum Teleportation and Quantum Digital Signature // Neural Processing Letters. 2023. Vol. 55. Pp. 3827–3842. DOI: 10.1007/s11063-020-10272-1.
17. Wang W., Yu Y., Du L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm // Scientific Reports. 2022. Vol. 12. No. 1. DOI: 10.1038/s41598-022-12412-0.
18. Петренко А. С., Петренко С. А., Костюков А. Д. Эталонная модель блокчейн-платформы // Защита информации. Инсайд. 2022. № 4(106). С. 34–44.
19. 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.
20. Балябин А. А., Петренко С. А. О создании киберустойчивых облачных платформ управления киберфизическими объектами в условиях роста угроз безопасности // Защита информации. Инсайд. 2025. № 4(124). С. 20–30.
21. Зегжда Д. П., Александрова Е. Б., Калинин М. О., Марков А. С. и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Научно-техническое издательство «Горячая линия-Телеком». 2021. 560 с.
22. Андрушкевич Д. В., Бирюков Д. Н., Тимашов П. В. Порождение сценариев предотвращения компьютерных атак на основе логико-онтологического подхода // Труды Военно-космической академии имени А. Ф. Можайского. 2021. № 677. С. 118–134.
23. Шелухин О. И., Рыбаков С. Ю., Ванюшина А. В. Влияние фрактальной размерности на качество классификации компьютерных атак методами машинного обучения // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 1. С. 57–64. DOI: 10.36724/2409-5419-2023-15-1-57-64.
24. Aljuaid W. H., Alshamrani S. S. A deep learning approach for intrusion detection systems in cloud computing environments // Applied sciences. 2024. Vol. 14. No. 13. P. 5381. DOI: 10.3390/app14135381.
25. Новикова Е. С., Котенко И. В., Мелешко А. В., Израилов К. Е. Обнаружение вторжений на основе федеративного обучения: архитектура системы и эксперименты // Вопросы кибербезопасности. 2023. № 6(58). С. 50–66. DOI: 10.21681/2311-3456-2023-6-50-66.
26. Шамсутдинов Р. Р., Васильев В. И., Вульфин А. М. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем // Системная инженерия и информационные технологии. 2024. Т. 6. № 4(19). С. 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14.
27. Балябин А. А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5(119). С. 35–44.
28. Балябин А. А., Петренко С. А., Костюков А. Д. Метод восстановления облачных и пограничных вычислений на основе кибериммунитета // Защита информации. Инсайд. 2022. № 6(108). С. 26–31.
29. Wrieden J. K., Vassilakis V. G. An Analysis of the Threats Posed by Botnet Malware Targeting Vulnerable Cryptocurrency Miners // 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), Paris, France. 2023. Pp. 82–87. DOI: 10.1109/ICUFN57995.2023.10201027.
30. Петренко А. С. Метод анализа квантовой устойчивости национальных блокчейн-экосистем и платформ // Защита информации. Инсайд. 2025. № 2(122). С. 18–27.
31. Tuokkola, M., Sunada, Y., Kivijärvi, H. et al. Methods to achieve near-millisecond energy relaxation and dephasing times for a superconducting transmon qubit // Nature Communications. 2025. Vol. 16, 5421. DOI: 10.1038/s41467-025-61126-0.
32. Milul O., Guttel B., Goldblatt U., Hazanov S., et al. Superconducting cavity qubit with tens of milliseconds single-photon coherence time // PRX Quantum. 2023. Vol. 4. No. 3. 030336. DOI: 10.1103/PRXQuantum.4.030336.
33. Балябин А. А., Петренко С. А. Модель самовосстановление киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE'25 : Сборник трудов IX Международной научно-технической конференции, Иннополис. 2025. С. 76–91.
34. Балябин А. А., Петренко С. А. Методика самовосстановления киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE'25 : Сборник трудов IX Международной научно-технической конференции, Иннополис. 2025. С. 103–114.

METHOD OF ENSURING CYBER RESISTANCE BLOCKCHAIN PLATFORMS BASED ON CYBER IMMUNITY

Balyabin A. A.[3], Petrenko S. A.[4]

Keywords: *threats to information security, quantum threats to security, blockchain ecosystems and platforms, cybersecurity, cyber resilience, methods of analysis and synthesis of quantum-resistant blockchain.*

Purpose of the research: *ensuring the resilience of cloud blockchain ecosystems and platforms of the 'Data Economy' of the Russian Federation based on cyber immunity in the face of hybrid quantum-classical attacks.*

3 Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology. Sirius Federal Territory, Russia. ORCID 0009-0006-3949-154X, E-mail: Balyabin.AA@talantiuspeh.ru
4 Sergei A. Petrenko, Dr.Sc. (of Tech.) (Grand Doctor, Full Professor), Team Leader, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology. Sirius Federal Territory, Russia. ORCID 0000-0003-0644-1731. E-mail: Petrenko.SA@talantiuspeh.ru

Methods of the research: *methods of system analysis, methods of probability theory and mathematical statistics, methods of the theory of stability of complex systems.*

Results of the research: *the analysis of research in the subject area has demonstrated that existing methods for ensuring the resilience of various information and computing systems consider either classical or quantum threats and do not fully ensure the resilience of cloud blockchain platforms under hybrid attacks characterized by the presence of both threat types. To resolve this problematic situation, an objective has been set to develop a novel method for ensuring the resilience of cloud blockchain platforms based on cyber immunity, and a hypothesis has been formulated regarding the feasibility of achieving the research goal through the application of this method.*

A method for ensuring the resilience of cloud blockchain platforms based on cyber immunity under hybrid quantum-classical attacks has been developed, enabling compliance with the compromise-probability requirements under constraints on the execution time of a blockchain node's program cycle by varying the cryptographic key length and the cyber immunity coverage coefficient.

A study of the developed method has demonstrated the capability to achieve the required resilience of cloud blockchain platforms under hybrid quantum-classical attacks, and the conditions for the existence of a solution have been determined, thereby confirming the formulated hypothesis.

Scientific novelty: *the developed method is the first to take into account new conditions such as hybrid attacks on cloud blockchain platforms, which are formally described through newly introduced parameters of the number of quantum computer qubits available to the attacker and the proportion of malicious input data. Furthermore, the application of this method for the first time imbues cloud blockchain platforms with a new emergent property of cyber immunity, which consists of the ability to detect known and previously unknown attacks aimed at violating the semantics of computations, counter them, and restore normal operation if violations occur*

References

1. Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain Integration in the Era of Industrial Metaverse. Applied Sciences, 13, 3, 1353. DOI: 10.3390/app13031353.
2. Markov, A. S. (2023). Important milestones in open source software security. Cybersecurity issues, 1(53), 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
3. Gai, K., Guo, J., Zhu, L., & Yu, S. (2020). Blockchain Meets Cloud Computing: A Survey. IEEE Communications Surveys & Tutorials, 22, 3, 2009–2030. DOI: 10.1109/COMST.2020.2989392.
4. Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasinski, M. (2022). Blockchain–Cloud Integration: A Survey. Sensors, 22(14), 5238. DOI: 10.3390/s22145238.
5. Petrenko, A. S., Lomako, A. G., & Petrenko, S. A. (2023). Analysis of the Current State of Research Blockchain Quantum Resilience Problems. Part 1. Zaŝita informacii. Inside, 3(111), 38–46.
6. Petrenko, S. A., & Balyabin A. A. (2025). Model of quantum threats to national blockchain ecosystems and platforms. Cybersecurity issues, 1(65), 7–17. DOI: 10.21681/2311-3456-2025-1-7-17.
7. Balyabin, A. A., Petrenko, S. A., & Kostyukov, A. D. (2024). Model of security threats and cyber resistance of cloud platforms of the critical IT infrastructure of the Russian Federation. Zaŝita informacii. Inside, 5(119), 26–34.
8. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8, 21091–21116. DOI: 10.1109/ACCESS.2020.2968985.
9. Shahid, F., & Khan, A. (2020). Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers. Future Generation Computer Systems, 111, 241–253. DOI: 10.1016/j.future.2020.04.042.
10. Sahin, M. S., & Akleylek, S. (2023). A survey of quantum secure group signature schemes: Lattice-based approach. Information Security Applications, 73, 103432. DOI: 10.1016/j.jisa.2023.103432.
11. Moskvin, V. S., & Bogatyrev, V. A. (2022). Post-quantum digital signing algorithms and their application in distributed registry. High technologies in Earth space research, 14, 4, 47–53. DOI: 10.36724/2409-5419-2022-14-4-47-53.
12. Yang, Z., Salman, T., Jain, R., & Pietro, R.D. (2020). Decentralization Using Quantum Blockchain: A Theoretical Analysis. IEEE Transactions on Quantum Engineering, 3, 1–16. DOI: 10.1109/TQE.2022.3207111.
13. Li, Q., Wu, J., Quan, J., Shi, J., & Zhang, S. (2022). Efficient Quantum Blockchain With a Consensus Mechanism QDPoS. IEEE Transactions on Information Forensics and Security, 17, 3264–3276. DOI: 10.1109/TIFS.2022.3203316.
14. Wen, X. J., Chen, Y. Z., Fan, X. C., Zhang, W., Yi, Z. Z., & Fang, J. B. (2022). Blockchain consensus mechanism based on quantum zero-knowledge proof. Optics and Laser Technology, 147, 107693. DOI: 10.1016/j.optlastec.2021.107693.
15. Sun, X., Kulicki, P., & Sopek, M. (2020). Multi-Party Quantum Byzantine Agreement without Entanglement. Entropy, 22, 10, 1152. DOI: 10.3390/e22101152.
16. Singh, S., Rajput, N. K., Rathi, V. K., Pandey, H. M., Jaiswal, A. K., & Tiwari, P. (2023). Securing Blockchain Transactions Using Quantum Teleportation and Quantum Digital Signature. Neural Processing Letters, 55, 3827–3842. DOI: 10.1007/s11063-020-10272-1.
17. Wang, W., Yu, Y., & Du, L. (2022). Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Scientific Reports, 12, 1, 1. DOI: 10.1038/s41598-022-12412-0.
18. Petrenko, A. S., Petrenko, S. A., & Kostyukov, A. D. (2022). The perfect model of the blockchain platform. Zaŝita informacii. Inside, 4(106), 34–44.
19. Petrenko, A. S., & Petrenko, S. A. (2022). Quantum resilience estimation method blockchain. Cybersecurity issues, 3(49), 2–22. DOI 10.21681/2311-3456-2022-3-2-22.
20. Balyabin A. A., & Petrenko S. A. (2025). On the creation of cyberresilient cloud platforms for managing cyber-physical objects in the context of growing security threats. Zaŝita informacii. Inside, 4(124), 20–30.

21. Zegzhda, D. P., Aleksandrova, E. B., Kalinin, M. O., Markov, A. S., Zhukov, I. Yu., Ivanov, D. V., Konoplev, A. S., Lavrova, D. S., Moskvin, D. A., Pavlenko, E. Yu., Poltavtseva, M. A., Shenets, N. N., Dakhnovich, A. D., & Krundyshev, V. M. (2021). Kiberbezopasnost' tsifrovoi industrii. Teoriya i praktika funktsional'noi ustoichivosti k kiberatakam. Moscow, Goryachaya liniya-Telekom Publ, 560 p.
22. Andrushkevich, D. V., Biryukov, D. N., & Timashov, P. V. (2021). Porozhdenie stsenariev predotvrashcheniya komp'yuternykh atak na osnove logiko-ontologicheskogo podkhoda. Trudy Voenno-kosmicheskoi akademii imeni A. F.Mozhaiskogo, 677, 118–134.
23. Sheluhin, O. I, Rybakov, S. Yu., & Vanyushina, A. V. (2023). Influence of fractal dimension on quality classification of computer attacks by machine learning methods. High technologies in Earth space research, 15, 1, 57–64. DOI: 10.36724/2409-5419-2023-15-1-57-64.
24. Aljuaid, W. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. Applied sciences, 14, 13, 5381. DOI: 10.3390/app14135381.
25. Novikova, E. S., Kotenko, I. V., Meleshko, A. V., & Izrailov, K. E. (2023). Federated learning based intrusion detection: system architecture and experiments. Cybersecurity issues, 6(58), 50–66. DOI: 10.21681/2311-3456-2023-6-50-66.
26. Shamsutdinov, R. R., Vasilyev, V. I., & Vulfin, A. M. (2024). Intelligent system for monitoring information security of the industrial internet of things using artificial immune systems mechanisms. System engineering and information technologies, 6, 4(19), 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14.
27. Balyabin, A. A. (2024). Model of the cloud platform of critical IT infrastructure of the Russian Federation under the conditions of information technology impacts. Zaŝita informacii. Inside, 5(119), 35–44.
28. Balyabin, A. A., Petrenko S. A., & Kostyukov A. D. (2022). Cloud and edge recovery method computing based on cyber immunity. Zaŝita informacii. Inside, 6(108), 26–31.
29. Wrieden, J. K., & Vassilakis, V. G. (2023). An Analysis of the Threats Posed by Botnet Malware Targeting Vulnerable Cryptocurrency Miners. 2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN), 82–87. DOI: 10.1109/ICUFN57995.2023.10201027.
30. Petrenko, A. S. (2025). Method for analyzing the quantum resilience of national blockchain ecosystems and platforms. Zaŝita informacii. Inside, 2(122), 18-27.
31. Tuokkola, M., Sunada, Y., Kivijarvi, H., Albanese, J., Gronberg, L., Kaikkonen, J. P., Vesterinen V., Govenius, J., & Mottonen, M. (2025). Methods to achieve near-millisecond energy relaxation and dephasing times for a superconducting transmon qubit. Nature Communications, 16, 5421. DOI: 10.1038/s41467-025-61126-0.
32. Milul, O., Guttel, B., Goldblatt, U., Hazanov, S., Joshi, L. M., Chausovsky, D., Kahn, N., Ciftyurek, E., Lafont, F., & Rosenblum, S. (2023). Superconducting cavity qubit with tens of milliseconds single-photon coherence time. PRX Quantum, 4, 3, 030336. DOI: 10.1103/PRXQuantum.4.030336.
33. Balyabin, A. A., & Petrenko S. A. (2025). Model' samovosstanovlenie kiberfizicheskikh sistem KII RF v usloviyakh kiberatak na osnove kiberimmuniteta. The 2025 Symposium on Cybersecurity of the Digital Economy – CDE'25 : Collected papers, 76–91.
34. Balyabin, A. A., & Petrenko S. A. (2025). Metodika samovosstanovleniya kiberfizicheskikh sistem KII RF v usloviyakh kiberatak na osnove kiberimmuniteta. The 2025 Symposium on Cybersecurity of the Digital Economy – CDE'25 : Collected papers, 103–114.