МЕТОДИКА СИНТЕЗА КВАНТОВО-УСТОЙЧИВЫХ БЛОКЧЕЙН-ПЛАТФОРМ С КИБЕРИММУНИТЕТОМ

Балябин А. А.[1], Петренко С. А.[2]

DOI: 10.21681/2311-3456-2025-4-46-54

Цель исследования: *разработка методики параметрического синтеза киберустойчивых блокчейн-экосистем и платформ «Экономики данных» Российской Федерации с кибериммунитетом в условиях новой квантовой угрозы.*

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

Полученные результаты: *проведено исследование существующих подходов к обеспечению квантовой устойчивости блокчейн-платформ с кибериммунитетом; сформулирована гипотеза о возможности обеспечения требуемой киберустойчивости блокчейн-платформ с кибериммунитетом в условиях квантовых атак; разработана методика параметрического синтеза квантово-устойчивых блокчейн-экосистем и платформ «Экономики данных» Российской Федерации с кибериммунитетом с использованием методов теории подобия; проведены экспериментальные исследования методики, результаты которых позволили подтвердить выдвинутую гипотезу.*

Научная новизна: *предложенная методика отличается от существующих тем, что во вновь разработанную методику введены новые группы формальных операций для каждого уровня функционирования блокчейн-платформ с кибериммунитетом по оцениванию необходимого и достаточного значений параметров нейтрализующих воздействий с использованием методов теории подобия, а также критерий, позволяющий установить существование решения для заданных значений требуемых показателей киберустойчивости и временных показателей функционирования блокчейн-платформы.*

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

Введение

Технологии распределенного реестра (DLT) активно развиваются и находят широкое применение в различных сферах, таких как финансовые услуги, цепочки поставок, здравоохранение и государственное управление. Они обеспечивают безопасность, прозрачность и децентрализацию данных, позволяя создавать системы, в которых участники могут проверять и записывать информацию без необходимости в доверенном центре. Основным примером реализации таких технологий является блокчейн, лежащий в основе криптовалют [1].

На базе блокчейн создаются новые технологии: смарт-контракты, токены (ERC-20), децентрализованные финансы (DeFi), децентрализованные приложения (dApps) и другие. Технологии распределенного реестра активно применяются при создании систем интернета вещей (IoT) [2], облачных платформ [3], систем Индустрии 4.0 [4]. Ведутся исследования по созданию интероперабельных блокчейн-экосистем [5] и децентрализованной сети Интернет (Web3) [6].

В Российской Федерации технологии распределенного реестра играют важную роль в реализации национального проекта «Экономика данных», позволяя создавать блокчейн-экосистемы и платформы, цифровые валюты, системы налогообложения, голосования и иные защищенные системы хранения и обработки данных, являющихся важнейшим активом в цифровой экономике [7].

Внедрение новых технологических решений неизбежно приводит к усложнению ландшафта киберугроз и возникновению новых, ранее неизвестных типов воздействий. Например, технологии искусственного интеллекта (AI) сегодня зачастую применяются для выявления недостатков систем защиты и планирования наступательных кибероперации [8, 9]. Одним из новейших вызовов безопасности блокчейн-экосистем и платформ является проблема обеспечения их киберустойчивости в условиях развития квантовых вычислений [10–12].

Свойства конфиденциальности, целостности и невозможности отказа от авторства, характерные для блокчейн-платформ, обеспечиваются криптостойкостью алгоритмов, которая в свою очередь зависит от вычислительной сложности задач факторизации и дискретного логарифмирования. Применение квантовых алгоритмов Шора и Гровера позволяет ускорить решение этих задач и создает угрозу киберустойчивости блокчейн-платформ [13, 14].

1 Балябин Артём Алексеевич, младший научный сотрудник, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. 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.org/0000- 0003-0644-1731. E mail: Petrenko.SA@talantiuspeh.ru

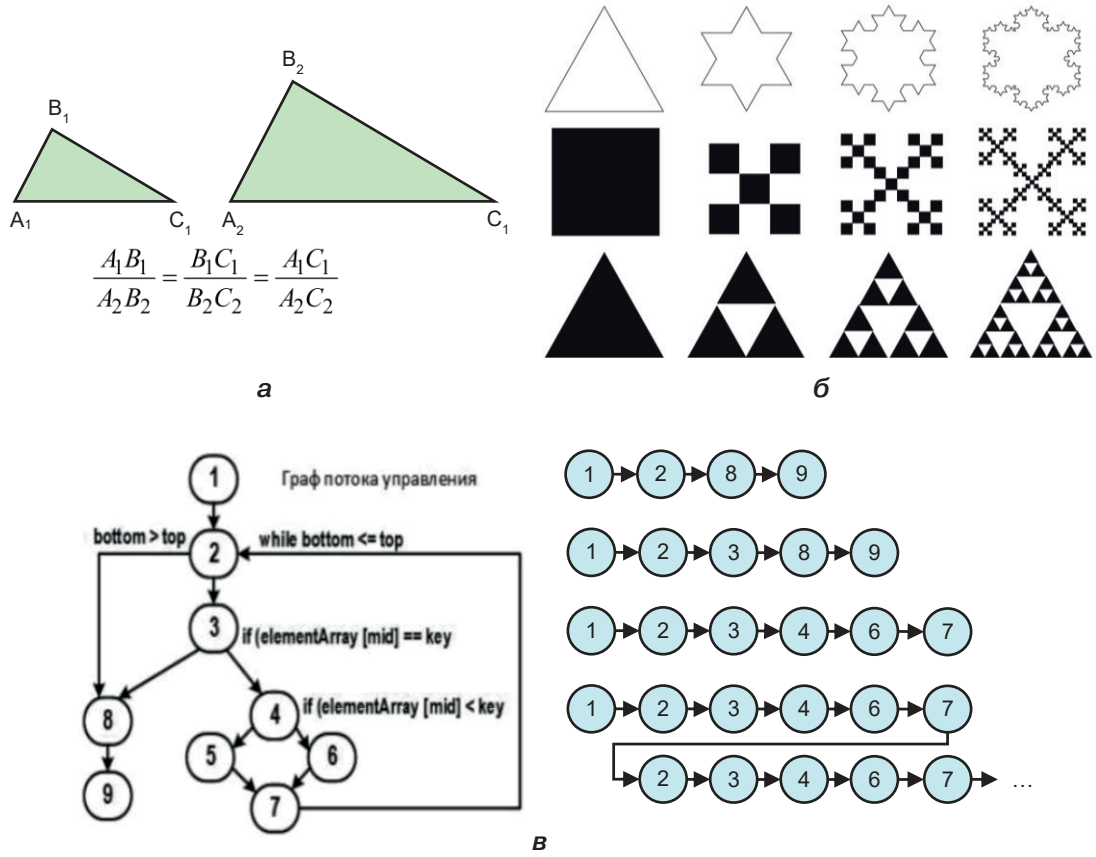

Рис. 1. Подобие и самоподобие:
а – геометрических фигур; б – фракталов; в – программных реализаций

Одним из возможных подходов к обеспечению киберустойчивости блокчейн-платформ является наделение их свойством кибериммунитета, то есть способностью обнаруживать аномалии, вызванные известными и ранее неизвестными воздействиями, противодействовать им и восстанавливать штатное функционирование [15, 16].

В ряде исследований предлагаются различные реализации методов кибериммунной защиты. Например, в работе [17] предлагается обеспечивать киберустойчивость информационных систем путем синтеза упреждающего поведения систем защиты. В работе [18] предлагается обеспечивать устойчивость киберфизических систем на основе динамической реконфигурации и гомеостаза. В работе [19] для решения схожих задач рассматривается возможность применения различных методов, в том числе гибридных, включая нейронные, иммунные и нейронечеткие.

Аномалии функционирования системы связаны с отклонением ее текущего состояния от некоторого штатного (киберустойчивого) состояния под воздействием внешних дестабилизирующих факторов. Одним из перспективных подходов к решению задач обнаружения аномалий и восстановления в рамках кибериммунного подхода является применение методов теории подобия и размерностей [20]. На рис. 1 представлены некоторые примеры проявления подобия и самоподобия.

В настоящем исследовании учитываются новейшие вызовы, связанные с ростом квантовых угроз, и предлагается методика параметрического синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом с использованием методов теории подобия и размерностей.

1. Постановка задачи исследования

Дано: L – блокчейн-платформа с кибериммунитетом, функционирующая на четырех уровнях, так что $L = \{L_i | i \in [1,4]\}$; $X = \{X_i | i \in [1,4]\}$ – множество входных данных; $Y = \{Y_i | i \in [1,4]\}$ – множество выходных данных; $E = \{E_i | i \in [1,4]\}$ – множество параметров среды; $A = \{A_i | i \in [1,4]\}$ – множество параметров дестабилизирующих воздействий; $D = \{D_i | i \in [1,4]\}$ – множество параметров нейтрализующих воздействий; $R = \{R_i | i \in [1,4]\}$ – множество показателей киберустойчивости; $T = \{T_i | i \in [1,4]\}$ – множество временных показателей функционирования.

Необходимо: разработать методику M параметрического синтеза квантово-устойчивых блокчейн-

платформ, для которых обеспечиваются требуемые значения $R_1^{тр},...,R_4^{тр}$ показателей киберустойчивости $R_1,...,R_4$ ($\forall R_i \geq R_i^{тр}$, $R_i \in R$, $i = 1..4$) и значения $T_1^{тр},...,T_4^{тр}$ временных показателей функционирования $T_1,...,T_4$ ($\forall T_i \leq T_i^{тр}$, $T_i \in T$, $i = 1..4$) в условиях квантовых дестабилизирующих воздействий A.

Формальная постановка научной задачи: найти

$$M{:}<L,X,Y,E,A,D,R,T> \longrightarrow <D,R,T>$$
$$D = \{D_i\}$$
$$R = \{R_i\}, R_i \geq R_i^{тр}$$
$$T = \{T_i\}, T_i \leq T_i^{тр}$$
$$i \in [1,4] \qquad (1)$$

при ограничениях $A_i \in [A_{i\min}, A_{i\max}]$, $A_i \in A \subseteq A_{доп}$, $i = 1..4$; $D_i \in [D_{i\min}, D_{i\max}]$, $D_i \in D \subseteq D_{доп}$, $i = 1..4$.

Гипотеза исследования: применение теории подобия и размерностей для реализации кибериммунной защиты блокчейн-платформ позволяет обеспечить требуемую их киберустойчивость в условиях квантовых атак.

2. Методика синтеза квантово-устойчивых блокчейн-платформ

Блокчейн-платформу с кибериммунитетом можно представить в виде системы из четырех взаимоувязанных уровней: криптографических алгоритмов, алгоритмов консенсуса, смарт-контрактов и децентрализованных приложений. На каждом уровне на систему оказываются квантовые дестабилизирующие воздействия, приводящие к возникновению аномалий. Противодействие квантовым атакам осуществляется на основе метода кибериммунной защиты, предназначенного для нейтрализации дестабилизирующих воздействий и обеспечения требуемой киберустойчивости блокчейн-платформы.

Методика параметрического синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом заключается в поиске значений параметров нейтрализующих воздействий D, обеспечивающих выполнение требований к показателям киберустойчивости R и временным показателям функционирования T на каждом уровне блокчейн-платформы при заданных параметрах воздействий A. Схема предлагаемой методики для i-го уровня блокчейн-платформы приведена на рис. 2.

Определим теперь аналитические выражения для синтеза необходимого и достаточного значений параметров нейтрализующих воздействий для каждого уровня блокчейн-платформы.

2.1. Синтез параметра для уровня криптографических алгоритмов

Показатель киберустойчивости блокчейн-платформы для уровня криптографических алгоритмов определяется как:

$$R_1 = 1 - w_1 q_1 \geq R_i^{тр}, \qquad (2)$$

где q_1 – параметр воздействия, определяющий вероятность синтеза блока атакующим быстрее остальной сети; w_1 – параметр нейтрализующего воздействия, определяющий коэффициент доверия к узлу.

Временной показатель функционирования блокчейн-платформы для уровня криптографических алгоритмов может быть определен как время, затрачиваемое на проверку подобия транзакций, включенных в блок:

$$T_1 = \lfloor (1 - w_1)N \rfloor n \log_2 n \leq T_1^{тр}, \qquad (3)$$

где N – количество блоков в блокчейн; n – количество транзакций в блоке.

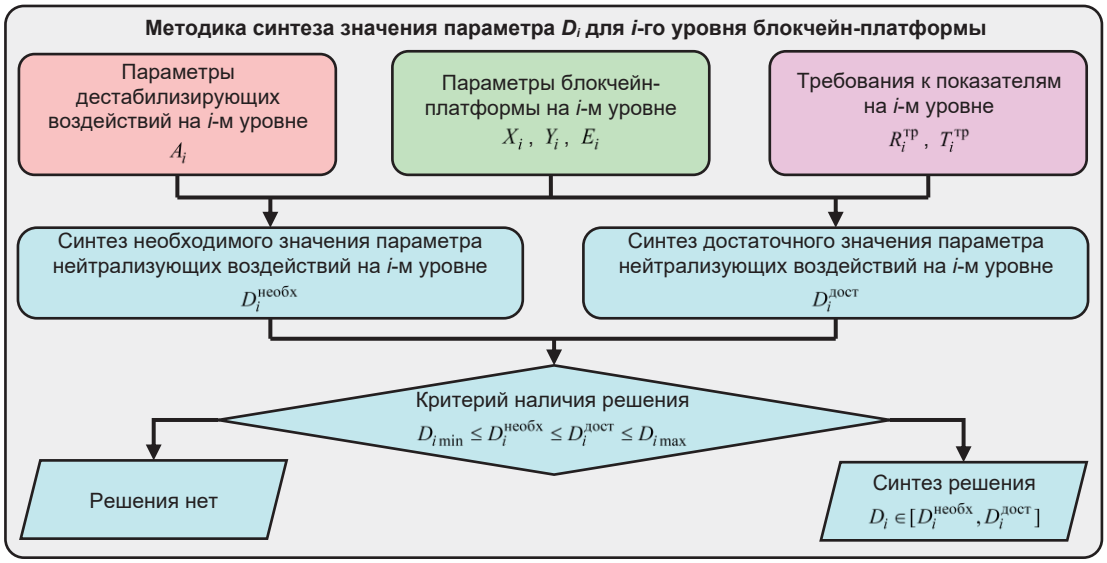

Рис. 2. Схема методики для i-го уровня блокчейн-платформы

При выполнении условия подобия хэш-сумма блока будет равна хэш-сумме вершины дерева Меркла. Здесь $nlog_2n$ характеризует сложность построения дерева Меркла для определения целостности блока, таким образом при снижении коэффициента доверия к узлу потребуется более глубокая проверка на предмет наличия аномалий связанных транзакций в более ранних блоках, что приведет к росту времени вычислений.

Для удобства будем полагать, что $D_1 = 1 - w_1$, тогда выражения для необходимого и достаточного значений параметра нейтрализующих воздействий на 1-м уровне блокчейн с учетом (2) и (3) можно записать как:

$$D_1^{\text{необх}} = 1 - (1 - R_1^{\text{тр}})/q_1$$
$$D_1^{\text{дост}} = T_1^{\text{тр}} /(Nnlogn). \quad (4)$$

2.2. Синтез параметра для уровня алгоритмов консенсуса

Показатель киберустойчивости блокчейн-платформы для уровня алгоритмов консенсуса определяется как:

$$R_2 = \sum_{k=0}^{z_2} \frac{\lambda^k e^{-\lambda}}{k!}(1 - (\lambda/z_2)^{z_2-k}) \geq R_2^{\text{тр}}, \quad (5)$$

где $\lambda = z_2 w_2 q_2 / (1 - w_2 q_2)$ – математическое ожидание длины цепочки блоков, сгенерированной атакующим; z_2 – количество блоков, на которое вредоносная цепочка должна быть длиннее для принятия ее в качестве основной; q_2 – параметр, определяющий вероятность синтеза блока атакующим быстрее остальной сети; w_2 – параметр нейтрализующего воздействия, определяющий коэффициент доверия к узлу.

Пусть требуется, чтобы цепочка атакующего была на 1 блок длиннее для принятия ее в качестве основной, то есть $z_2 = 1$. Тогда, упрощая выражение (5), получим:

$$R_2 = e^{-\lambda}(1 - \lambda) \geq R_2^{\text{тр}}. \quad (6)$$

Поскольку неравенство (6) содержит линейную и экспоненциальную зависимости от искомого параметра, его аналитическое решение затруднительно. Однако, выражение с экспонентой можно разложить в ряд Маклорена:

$$e^{-\lambda} = 1 - \lambda + \frac{(-\lambda^2)}{2!} + \frac{(-\lambda^3)}{3!} + \ldots . \quad (7)$$

Поскольку $\lambda \in [0,1]$ при $z_2 = 1$, то возможно провести аппроксимацию $e^{-\lambda} \approx 1 - \lambda$. Тогда неравенство (6) примет вид:

$$R_2 = (\lambda^2 - 2\lambda + 1) \geq R_2^{\text{тр}}. \quad (8)$$

Решая квадратичное неравенство (8) относительно λ с учетом допустимых значений, получим:

$$\lambda \leq 1 - \sqrt{R_2^{\text{тр}}}. \quad (9)$$

Тогда с учетом (5):

$$w_2 q_2 / (1 - w_2 q_2) \leq 1 - \sqrt{R_2^{\text{тр}}}, \quad (10)$$

что выполняется только в случае:

$$w_2 \leq \min\left(1, \frac{1 - \sqrt{R_2^{\text{тр}}}}{q_2 (2 - \sqrt{R_2^{\text{тр}}})}\right). \quad (11)$$

Временной показатель функционирования блокчейн-платформы для уровня алгоритмов консенсуса может быть определен как время, затрачиваемое на достижение консенсуса валидаторами:

$$T_2 = bV + (1 - w_2)(1 - b - e)V \leq T_2^{\text{тр}}, \quad (12)$$

где b – минимальное количество валидаторов, необходимое для подтверждения корректности цепочки блоков при коэффициенте доверия к узлу, создавшему цепочку $w_2 = 1$, $b \in [0,1]$; V – общее количество валидаторов в блокчейн; e – допустимая погрешность валидации (допустимое количество валидаторов, не подтверждающих корректность блока), $e < 1 - b$.

При снижении доверия к узлу, создающему цепочку блоков, для достижения консенсуса потребуется большее количество валидаторов, что увеличивает временные затраты на согласование. Будем полагать, что $D_2 = 1 - w_2$, тогда выражения для необходимого и достаточного значений параметра нейтрализующих воздействий на 2-м уровне блокчейн с учетом (11) и (12) можно записать как:

$$D_2^{\text{необх}} = \max\left(0{,}1 - \frac{1 - \sqrt{R_2^{\text{тр}}}}{q_2 (2 - \sqrt{R_2^{\text{тр}}})}\right),$$
$$D_2^{\text{дост}} = \frac{T_2^{\text{тр}} - bV}{(1 - b - e)V}. \quad (13)$$

2.3. Синтез параметра для уровня смарт-контрактов

Показатель киберустойчивости блокчейн-платформы для уровня смарт-контрактов определяется как:

$$R_3 = R_2 \frac{1}{n_3} \sum_{i=1}^{n_3} \left(1 - \frac{\#X_{3i}^- - \#D_{3i}}{\#X_{3i}}\right) k_{\text{покр}} \geq R_3^{\text{тр}}, \quad (14)$$

где R_2 – показатель киберустойчивости уровня алгоритмов консенсуса; n_3 – количество смарт-контрактов; $\#X_{3i}$ – мощность множества входных данных i-го смарт-контракта; $\#X_{3i}^-$ – мощность подмножества вредоносных входных данных i-го смарт-контракта, $X_{3i}^- \subset X_{3i}$; $\#D_{3i}$ – мощность множества выявленных и заблокированных вредоносных входных данных i-го смарт-контракта, $\#D_{3i} \leq \#X_{3i}^-$; $k_{\text{покр}}$ – коэффициент покрытия операций смарт-контракта проверками подобия, $k_{\text{покр}} \in [0,1]$.

Для оценки будем считать, что множества X_{3i}, X_{3i}^- и D_{3i} для всех смарт-контрактов одинаковы. В процессе функционирования блокчейн-платформы

происходит накопление образцов вредоносных входных данных и снижается вероятность возникновения нарушения. Тогда выражение для предельной киберустойчивости блокчейн-платформы с учетом (14) примет вид:

$$R_3 = R_2\, k_{\text{покр}} \geq R_3^{\text{тр}}. \quad (15)$$

Временной показатель функционирования блокчейн-платформы для уровня смарт-контрактов может быть определен как время, затрачиваемое на выполнение смарт-контрактов с учетом проверки подобия маршрутов выполнения допустимым маршрутам:

$$T_3 = n_3 \left(kmn + k_{\text{покр}}\, k \frac{m(m-1)}{2}(2n-1) \right) \leq T_3^{\text{тр}}, \quad (16)$$

где k – количество линейных блоков операций в смарт-контракте; m – количество операций в блоке; n – количество параметров в операции.

Параметром нейтрализующих воздействий на данном уровне можно считать коэффициент покрытия операций смарт-контрактов проверками подобия $D_3 = k_{\text{покр}}$. Тогда выражения для необходимого и достаточного значений параметра нейтрализующих воздействий на 3-м уровне блокчейн с учетом (15) и (16) можно записать как:

$$D_3^{\text{необх}} = R_3^{\text{тр}}/R_2$$
$$D_3^{\text{дост}} = \frac{2(T_3^{\text{тр}} / n_3 - kmn)}{km(m-1)(2n-1)}. \quad (17)$$

2.4. Синтез параметра для уровня децентрализованных приложений

Показатель киберустойчивости блокчейн-платформы для уровня децентрализованных приложений определяется как:

$$R_4 = R_3 \frac{1}{n_4} \sum_{i=1}^{n_4} \left(1 - \frac{\#X_{4i}^- - \#D_{4i}}{\#X_{4i}} \frac{1}{l_i} \sum_{r=1}^{l_i} P_{3ir}^a \right) k_{\text{покр}}, \quad (18)$$

где R_3 – показатель киберустойчивости уровня смарт-контрактов; n_4 – количество dApps; $\#X_{4i}$ – мощность множества входных данных i-го dApp; $\#X_{4i}^-$ – мощность подмножества вредоносных входных данных i-го dApp, $X_{4i}^- \subset X_{4i}$; $\#D_{4i}$ – мощность множества выявленных и заблокированных вредоносных входных данных i-го dApp, $\#D_{4i} \leq \#X_{4i}^-$; l_i – количество смарт-контрактов в i-м dApp; P_{3ir}^a – вероятность возникновения нарушения в r-м смарт-контракте i-го dApp; $k_{\text{покр}}$ – коэффициент покрытия операций в децентрализованных приложениях проверками подобия.

Аналогично уровню смарт-контрактов в процессе функционирования блокчейн-платформы происходит накопление образцов вредоносных входных данных децентрализованных приложений, поэтому выражение для предельной киберустойчивости можно записать как:

$$R_4 = R_3\, k_{\text{покр}} \geq R_4^{\text{тр}}. \quad (19)$$

Временной показатель функционирования блокчейн-платформы для уровня децентрализованных приложений может быть определен как время, затрачиваемое на выполнение dApps с учетом проверки подобия последовательностей операций допустимым последовательностям:

$$T_4 = n_4 \frac{l}{n_3} T_3 (1 + k_{\text{покр}}) \leq T_4^{\text{тр}}, \quad (20)$$

где l – количество смарт-контрактов, исполняемых в рамках каждого децентрализованного приложения.

Параметром нейтрализующих воздействий на данном уровне можно считать коэффициент покрытия операций децентрализованных приложений проверками подобия $D_4 = k_{\text{покр}}$. Тогда выражения для необходимого и достаточного значений параметра нейтрализующих воздействий на 4-м уровне блокчейн с учетом (19) и (20) можно записать как:

$$D_4^{\text{необх}} = R_4^{\text{тр}} / R_3$$
$$D_4^{\text{дост}} = \frac{T_4^{\text{тр}}\, n_3}{n_4\, l T_3} - 1. \quad (21)$$

Исследуем теперь возможности параметрического синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом при управлении параметрами нейтрализующих воздействий с помощью предложенной методики в условиях квантовых атак.

3. Исследование квантовой устойчивости блокчейн-платформ

Для параметрического синтеза квантово-устойчивой блокчейн-платформы необходимо найти значения параметров нейтрализующих воздействий D, обеспечивающие требуемые значения показателей киберустойчивости и временных показателей функционирования блокчейн. Такие параметры с учетом (4), (13), (17), (21) должны удовлетворять условию:

$$D_i^{\text{необх}} \leq D_i \leq D_i^{\text{дост}},\ i = 1..4. \quad (22)$$

На рис. 3 представлены графики зависимости показателей киберустойчивости и временных показателей функционирования блокчейн-платформы от параметров нейтрализующих воздействий на каждом уровне. Как видно, функции требуемых показателей функционирования блокчейн-платформ являются монотонно возрастающими. Сформулируем утверждение относительно существования решения задачи параметрического синтеза квантово-устойчивой блокчейн-платформы.

Утверждение 1. Если для заданных требуемых значений показателей $R_i^{\text{тр}}$, $D_i^{\text{тр}}$, $i = 1..4$ существует решение D_i, $i = 1..4$, то оно лежит в отрезке $[D_i^{\text{необх}}, D_i^{\text{дост}}]$.

Доказательство. Доказательство данного утверждения вытекает из требований критерия наличия решения в соответствии с методикой параметрического синтеза:

$$D_{i\,\min} \leq D_i^{\text{необх}} \leq D_i^{\text{дост}} \leq D_{i\,\max}, \quad (23)$$

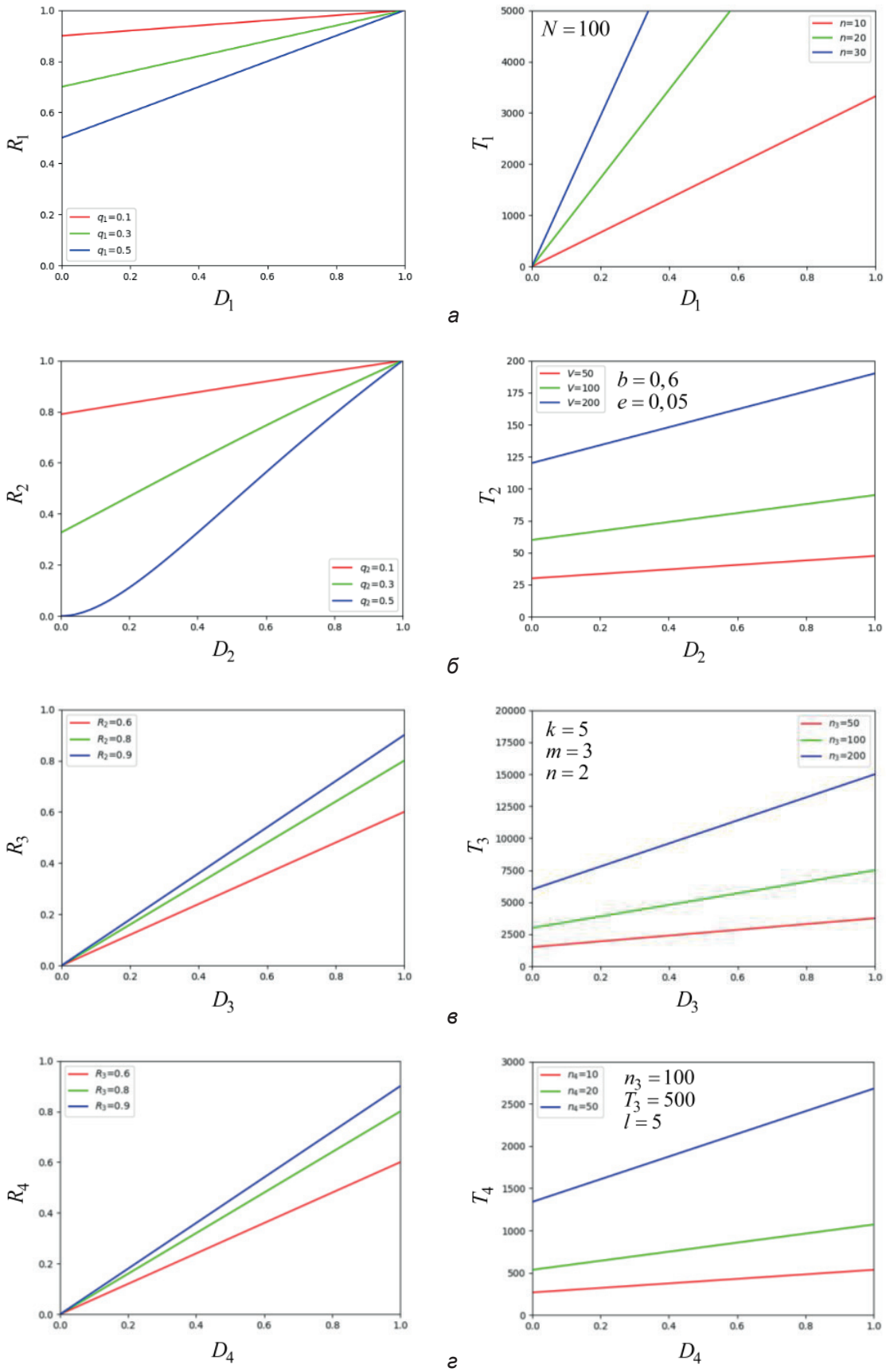

Рис. 3. Результаты исследования показателей киберустойчивости и временных показателей функционирования блокчейн-платформ на уровнях: а – криптографических алгоритмов; б – алгоритмов консенсуса; в – смарт-контрактов; г – децентрализованных приложений

а также того, что функции требуемых показателей являются непрерывно возрастающими на всем промежутке $D_i \in [0,1]$, $i = 1..4$. Таким образом, если решение существует, то оно принадлежит отрезку $[D_i^{\text{необх}}, D_i^{\text{дост}}]$, $i = 1..4$.

Ч.т.д.

Таким образом, результаты проведенных исследований позволяют *подтвердить* выдвинутую гипотезу.

Выводы

В настоящем исследовании поставлена задача разработки методики параметрического синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом. Выдвинута гипотеза о возможности обеспечения требуемой киберустойчивости блокчейн-платформ. Разработана методика параметрического синтеза блокчейн-платформ с кибериммунитетом, отличающаяся от существующих введением новых групп формальных операций по оцениванию необходимого и достаточного значений параметров нейтрализующих воздействий для обеспечения требуемых значений показателей киберустойчивости и временных показателей функционирования блокчейн-платформ с использованием методов теории подобия.

В результате исследований определены аналитические выражения для необходимого и достаточного значений параметра нейтрализующих воздействий D_i, $i = 1..4$ на каждом уровне блокчейн-платформы, а также экспериментально установлено, что выбор значения параметра из отрезка $[D_i^{\text{необх}}, D_i^{\text{дост}}]$, $i = 1..4$ позволяет обеспечить требуемые значения показателей функционирования блокчейн-платформ с кибериммунитетом в условиях квантовых атак. Таким образом, результаты экспериментов позволили подтвердить выдвинутую гипотезу.

В дальнейшем результаты исследования могут быть использованы при разработке киберустойчивых блокчейн-экосистем и платформ «Экономики данных» Российской Федерации в условиях новой квантовой угрозы.

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. Nguyen D. C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
3. 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.
4. 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.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.
6. Zhu Q., Loke S. W., Trujillo-Rasua R., Jiang F., Xiang Y. Applications of Distributed Ledger Technologies to the Internet of Things: A Survey // ACM Comput. Surv. 2019. Vol. 52. No. 6. P. 120:1–120:34. DOI: 10.1145/3359982.
7. Петренко А. С. Квантово-устойчивый блокчейн: научная монография // Санкт-Петербург : Питер, 2023. 384 с.
8. Петренко С. А. Киберустойчивость Индустрии 4.0: научная монография // «Издательский Дом «Афина». 2020. 256 с.
9. Маркова С. В. Выявления уязвимостей в децентрализованных информационных системах на основе смарт-контрактов с помощью методов обработки больших данных // Фундаментальные исследования. 2022. № 9. С. 47–53.
10. 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.
11. Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H. -N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
12. 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.
13. Петренко А. С., Романченко А. М. Перспективный метод криптоанализа на основе алгоритма Шора // Защита информации. Инсайд. 2020. № 2 (92). С. 17–23.
14. Петренко А. С., Петренко С. А. Basic Algorithms Quantum Cryptanalysis (Основные алгоритмы квантового криптоанализа) // Вопросы кибербезопасности. 2023. №1 (53). С. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.
15. Балябин, А. А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5 (119). С. 35–44.
16. 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.

17. 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.
18. Зегжда Д. П., Александрова Е. Б., Калинин М. О. и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам // Москва : Научно-техническое издательство «Горячая линия-Телеком». 2021. 560 с.
19. Петренко С. А. Кибериммунология // Санкт-Петербург : Афина. 2021. 239 с.
20. Балябин А. А., Петренко С. А. Методика кибериммунной защиты цифровых сервисов «ГосТех» с использованием теории подобия и размерностей // The 2023 Symposium on Cybersecurity of the Digital Economy – CDE'23 : Сборник трудов VII международной научно-технической конференции, Иннополис, 11-12 апреля 2023 года. Иннополис: Университет Иннополис. 2024. С. 85–90.

METHODOLOGY FOR SYNTHESIZING QUANTUM-RESISTANT BLOCKCHAIN PLATFORMS WITH CYBER-IMMUNITY

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

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

Purpose of the research: *development of a methodology for the parametric synthesis of cyber-resilient blockchain ecosystems and platforms of the 'Data Economy' of the Russian Federation with cyber-immunity under the new quantum threat.*

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

Result of the research: *an study of existing approaches to ensuring quantum resilience of blockchain platforms with cyber-immunity has been conducted; a hypothesis regarding the possibility of ensuring the required cyber-resilience of blockchain platforms with cyber-immunity under quantum attacks has been formulated; a methodology for the parametric synthesis of quantum-resilient blockchain ecosystems and platforms of the 'Data Economy' of the Russian Federation with cyber-immunity has been developed using similarity theory methods; experimental studies of the methodology have been carried out, the results of which confirmed the proposed hypothesis.*

Scientific novelty: *the proposed methodology differs from existing ones in that it introduces new groups of formal operations for each level of blockchain platforms with cyber-immunity functionality, aimed at evaluating the necessary and sufficient values of neutralizing impact parameters using similarity theory methods. Additionally, it includes a criterion that allows establishing the existence of a solution for the given values of required cyber-resilience and time performance indicators of the blockchain platform.*

The results were obtained with the financial support of the project «Technologies for countering previously unknown quantum cyber threats», implemented within the framework of the state program of the «Sirius» Federal Territory «Scientific and technological development of the «Sirius» Federal Territory (Agreement No. 23-03 dated September 27, 2024).

References

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. Nguyen D. C. et al. 6G Internet of Things: A Comprehensive Survey // IEEE Internet of Things Journal. 2022. Vol. 9. No. 1. Pp. 359–383. DOI: 10.1109/JIOT.2021.3103320.
3. Balyabin A. A., Petrenko S. A., Kostyukov A. D. Model' ugroz bezopasnosti i kiberustoychivosti oblachnykh platform KII RF // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 26–34.
4. Markov A. S. Vazhnaya vekha v bezopasnosti otkrytogo programmnogo obespecheniya // Voprosy kiberbezopasnosti. 2023. № 1 (53). Pp. 2–12. DOI: 10.21681/2311-3456-2023-1-2-12.
5. Chen C. et al. When Digital Economy Meets Web3.0: Applications and Challenges // IEEE Open Journal of the Computer Society. 2022. Vol. 3. Pp. 233–245. DOI: 10.1109/OJCS.2022.3217565.
6. Zhu Q., Loke S. W., Trujillo-Rasua R., Jiang F., Xiang Y. Applications of Distributed Ledger Technologies to the Internet of Things: A Survey // ACM Comput. Surv. 2019. Vol. 52. No. 6. P. 120:1–120:34. DOI: 10.1145/3359982.
7. Petrenko A. S. Kvantovo-ustoychivyy blokcheyn: nauchnaya monografiya. // Sankt-Peterburg : Piter, 2023. 384 p.
8. Petrenko S. A. Kiberustoychivost' Industrii 4.0: nauchnaya monografiya // «Izdatel'skiy Dom «Afina». 2020. 256 p.
9. Markova S. V. Vyyavleniya uyazvimostey v detsentralizovannykh informatsionnykh sistemakh na osnove smart-kontraktov s pomoshch'yu metodov obrabotki bol'shikh dannykh // Fundamental'nye issledovaniya. 2022. № 9. Pp. 47–53.

3 Artyom Balyabin, Junior Researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, E-mail: Balyabin.AA@talantiuspeh.ru

4 Sergei Petrenko, Dr.Sc. (in Tech.) (Grand Doctor, Full Professor), Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Orcid.org/0000- 0003-0644-1731, E-mail: Petrenko.SA@talantiuspeh.ru

10. Petrenko S. A., Balyabin A. A. Model' kvantovykh ugroz bezopasnosti informatsii dlya natsional'nykh blokcheyn-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. № 1(65). Pp. 7–17. DOI 10.21681/2311-3456-2025-1-7-17.
11. Kushwaha S. S., Joshi S., Singh D., Kaur M. Lee H. -N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Vol. 10. Pp. 6605–6621. DOI: 10.1109/ACCESS.2021.3140091.
12. 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.
13. Petrenko A. S., Romanchenko A. M. Perspektivnyy metod kriptoanaliza na osnove algoritma Shora // Zashchita informatsii. Insayd. 2020. № 2 (92). Pp. 17–23.
14. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. No. 1 (53). Pp. 100–115. DOI 10.21681/2311-3456-2023-1-100-115.
15. Balyabin A. A. Model' oblachnoy platformy KII RF s kiberimmunitetom v usloviyakh informatsionno-tekhnicheskikh vozdeystviy // Zashchita informatsii. Insayd. 2024. № 5 (119). Pp. 35–44.
16. Balyabin A. A., Petrenko S. A., Kostyukov A. D. Metod vosstanovleniya oblachnykh i pogranichnykh vychisleniy na osnove kiberimmuniteta // Zashchita informatsii. Insayd. 2022. № 6(108). Pp. 26–31.
17. Andrushkevich D. V., Biryukov D. N., Timashov P. V. Porozhdenie stsenariev predotvrashcheniya komp'yuternykh atak na osnove logiko-ontologicheskogo podkhoda // Trudy Voenno-kosmicheskoy akademii imeni A.F.Mozhayskogo. 2021. № 677. Pp. 118–134.
18. Zegzhda D. P., Aleksandrova E. B., Kalinin M. O. i dr. Kiberbezopasnost' tsifrovoy industrii. Teoriya i praktika funktsional'noy ustoychivosti k kiberatakam // Moskva : Nauchno-tekhnicheskoe izdatel'stvo «Goryachaya liniya-Telekom». 2021. 560 p.
19. Petrenko S. A. Kiberimmunologiya // Sankt-Peterburg : Afina. 2021. 239 p.
20. Balyabin A. A., Petrenko S. A. Metodika kiberimmunnoy zashchity tsifrovykh servisov «GosTekh» s ispol'zovaniem teorii podobiya i razmernostey // The 2023 Symposium on Cybersecurity of the Digital Economy – CDE'23 : Sbornik trudov VII mezhdunarodnoy nauchno-tekhnicheskoy konferentsii, Innopolis, 11-12 aprelya 2023 goda. Innopolis: Universitet Innopolis. 2024. Pp. 85–90.