ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ РАСПРЕДЕЛЕННОГО РЕЕСТРА В УСЛОВИЯХ ПОЯВЛЕНИЯ НОВОЙ КВАНТОВОЙ УГРОЗЫ

Сундеев П. В.[1]

DOI: 10.21681/2311-3456-2025-3-83-89

Цель исследования: *предложить подход к формальному анализу функциональной устойчивости или стабильности систем распределенного реестра для критических приложений в условиях появления новой квантовой угрозы.*

Методы исследования: *объектно-ориентированный анализ и синтез сложных систем, системный анализ, теория модульно-кластерных сетей, теория графов, теория матриц, математическая логика.*

Результаты исследования: *показано влияние безопасности архитектуры и политики доступа на функциональную стабильность распределенного реестра в условиях квантовой угрозы, предложена концепция и постановка задачи анализа безопасности архитектуры распределенного реестра в терминах теории модульно-кластерных сетей, подход к синтезу архитектуры с доказанными свойствами безопасности.*

Научная новизна: *применение теории модульно-кластерных сетей к анализу функциональной стабильности систем распределенного реестра в аспекте безопасности с учетом влияния квантовой угрозы.*

Ключевые слова: *модульно-кластерная сеть, системный анализ, безопасность.*

Введение

Технология распределенного реестра (DLT – Distributed ledger technologies) имеет децентрализованную архитектуру и предназначена для безопасного взаимодействия недоверенных субъектов на основе процедуры консенсуса без участия посредников [1–4]. В частных случаях централизованной или гибридной архитектуры предусмотрены администраторы и посредники, что позволяет контролировать систему, но создает дополнительные риски для участников взаимодействия. Национальные распределенные реестры могут попадать под действие законодательства о критической информационной инфраструктуре [5]. В условиях конкурентной среды на функциональную стабильность критической системы, кроме свойств надежности, производительности, функциональности и т.д., влияет безопасность, нарушение которой может быть целью внешних нарушителей, взаимодействующих субъектов и администраторов. Особенность архитектуры DLT – конструктивная реализация принципа «Secure by Design» на основе криптографии. Однако перспектива резкого увеличения скорости вычислений при появлении промышленных квантовых компьютеров создает неприемлемый для критических приложений риск компрометации неидеальной криптографии [6]. Поэтому для обеспечения доверия к системам распределенного реестра (DLTS – DLT System) необходимо формально оценивать безопасность архитектуры с учетом стойкости криптографии к квантовой угрозе.

В статье предложен системный подход к анализу архитектуры DLTS с формальным доказательством безопасности в условиях квантовой угрозы на основе методов теории модульно-кластерных сетей (МК-сетей) [7].

Особенности защиты информации в DLT

Функциональную стабильность в аспекте безопасности обеспечивают:

- политика разграничения доступа (ACP – Access Control Policy);
- конструктивная безопасность архитектуры (SBD – Secure By Design);
- надежность средств реализации ACP (MAC – Means of Access Control);
- безопасная обработка данных (SDP – Secure Data Processing).

При анализе безопасности архитектуры существенны первые три фактора.

ACP должен установить «собственник информации» с учетом собственной оценки ущерба из-за нарушения безопасности информации. Однако в законодательстве отсутствует понятие «собственник информации». Легитимно более широкое понятие «обладатель информации» [8], которое включает иные категории субъектов информационных отношений, имеющих правомерный доступ к информации. В условиях конкурентной среды и критичности системы такие субъекты должны включаться в модель угроз как потенциальные нарушители. Архитектура систем реализующих ACP в парадигме «обладатель информации», опасна для собственника из-за доступа к информации посредников, администраторов

1 Сундеев Павел Викторович, доктор технических наук, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: sundeev.pv@talantiuspeh.ru

и т.п. Архитектура DLT в «классическом» исполнении конструктивно включает функционал защиты, который не позволяет вносить изменения в данные, переданные и зарегистрированные в реестре, что обеспечивает доверие участников к их целостности в условиях отсутствия доверия друг к другу. При этом актуальна угроза конфиденциальности [9].

Безопасная архитектура предполагает наличие в ней МАС, реализующих АСР. Состав функций защиты в DLTS зависит от конфигурации архитектуры и организации процесса обработки данных с учетом актуальных угроз безопасности информации и может включать идентификацию и аутентификацию субъектов и объектов доступа, авторизацию, шифрование, физическую защиту носителей и т.д., наличие и надежность которых необходимо учитывать при формальном анализе [3,4]. При анализе безопасности архитектуры DLT необходимо учитывать надежность МАС, в частности, учитывать риск компрометации неидеальной криптографии, которая является основой конструктивной безопасности архитектуры, в условиях квантовой угрозы.

Концепция анализа безопасности архитектуры DLT методами МК-сетей

Для формального анализа архитектура DLT представляется в виде объектно-ориентированной информационной модели в терминах теории МК-сетей [7]. «Классическая» архитектура DLT [1] представляет собой МК-сеть в виде полного ациклического маркированного регулярного ориентированного мультиграфа $G^{FLS}(M_N,R_M^{FLS})$, вершины которого обозначают функциональные модули M_P (P – число модулей) и модули защиты M_D (D – число МАС), где $M_P \cup M_D = M_N$ и $M_P \cap M_D = \varnothing$, а дуги R_M^{FLS} обозначают физические (F), синтаксические (L) и семантические (S) FLS интерфейсы модулей, которые определяют возможность информационных отношений между модулями.

Определение 1. Модульно-кластерная сеть – это FLS мультиграф $G^{FLS}(M_N,R_Q^{FLS})$, вершинами которого являются функционально-информационные модули $M_N = \{m_1, m, \ldots, m_n\}$, где N – их число, а дуги $R_M^{FLS} = \{R^F \cup R^L \cup R^S\}$ (где $R^F = \{r_x^F\}$, $R^L = \{r_y^L\}$, $R^S = \{r_z^S\}$) определяются наличием у модулей FLS-интерфейсов, через которые устанавливаются функционально-информационные отношения.

Мультиграф $G^{FLS}(M_N,R_M^{FLS})$ состоит из F, L и S остовных подграфов (или просто FLS-подграфов), у которых вершины совпадают и соответствуют множеству $M_N = \{m_1, m, \ldots, m_n\}$, а инцидентные им дуги различаются и определяются соответственно множествами $R^F = \{r_x^F\}$, $R^L = \{r_y^L\}$, $R^S = \{r_z^S\}$, отражающими FLS отношения между модулями.

Упрощенный фрагмент мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ и его декомпозиция на остовные FLS подграфы представлены на (рис. 1).

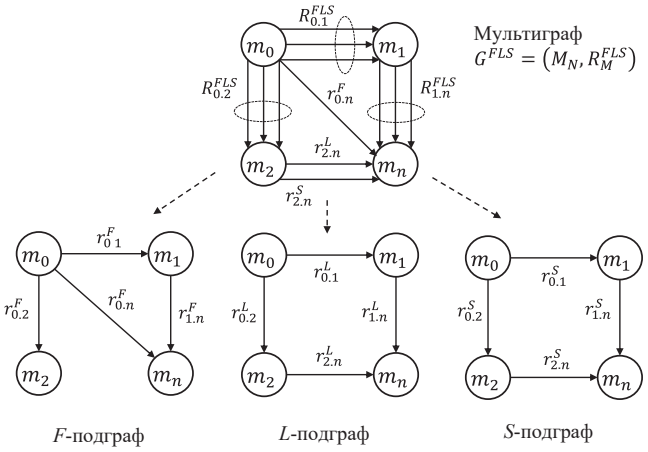

Рис. 1. Фрагмент мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ МК-сети и его декомпозиция на остовные FLS-подграфы

Фрагмент мультиграфа на рис. 1 содержит два пути $P_{0.2}^{FLS} = \{R_{0,2}^{FLS}\}$ и $P_{0.n}^{FLS} = \{R_{0,1}^{FLS}, P_{1.n}^{FLS}\}$, по которым возможна реализация информационного процесса.

Декомпозиция элементов множества дуг $R_M \longrightarrow R_M^{FLS}$ расширяет классическое понятие «смежности» вершин мультиграфа.

Утверждение 1. Любые две вершины $\{m_i, m_j\}$ мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ являются смежными, если и только если в FLS-подграфах между этими вершинами существует хотя бы одно подмножество кратных дуг вида $\{r_{i,j}^F, r_{i,j}^L, r_{i,j}^S\}$, которое называется полной FLS-дугой.

Утверждение 2. Информационное взаимодействие между любыми двумя модулями МК-сети возможно, если обозначающие их вершины $\{m_i, m_j\}$ графа $G^{FLS}(M_N,R_M^{FLS})$ смежные.

Утверждение 3. Путь P^{FLS} между произвольной парой вершин $\{m_i, m_j\}$ в FLS мультиграфе $G^{FLS}(M_N,R_M^{FLS})$ существует, если и только если существуют пути между этими вершинами в FLS-подграфах смежности.

Переход состояний МК-сети происходит только при наличии инцидентных дуг между смежными вершинами на всех трех уровнях взаимодействия (полная FLS дуга) активной траектории процесса при совпадении соответствующих индексов входных и выходных интерфейсов модулей. Семантика решающих правил определяется типовыми информационными примитивами [9] и может быть дополнена функционалом элементов DLT [1–4]. В децентрализованной «классической» схеме архитектуры DLT правила АСР являются однотипными для всех вершин.

В критических системах АСР и архитектура должны реализовать модель защиты с «полным перекрытием». Расширенный вариант модели защиты с полным перекрытием образует пятидольный ориентированный граф (рис. 2) на основе декомпозиции множества информационных взаимодействий

R_M на подмножества $\{R^F \cup R^L \cup R^S\}$ R_M^{FLS} *FLS*-отношений, реализующих фазы информационного взаимодействия в соответствии с парадигмой трехуровневого информационного взаимодействия [10], которые реализуются МАС из множества M_D.

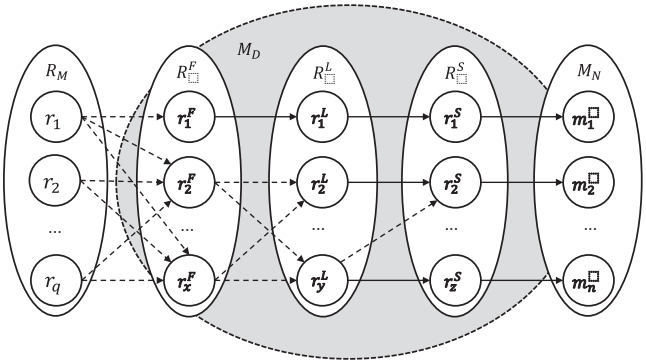

Рис. 2. Отображение множества информационных взаимодействий R_M на множество модулей M_N через множество M_D средств разграничения доступа и подмножества $\{R^F \cup R^L \cup R^S\}R_M^{FLS}$ FLS-отношений

В расширенной модели защиты с полным перекрытием множество вершин M_N, где N – число всех вершин мультиграфа G^{FLS}, разбивается правилами АСР на кластерные подмножества модулей обработки данных M_K (K – число кластеров), такие что $M_1 \cap M_2 \cap M_k = \emptyset$ и $M_1 \cup M_2 \cup M_k = M_K$, и M_D – подмножество МАС (D – число МАС), где $M_K \cap M_D = \emptyset$ и $M_K \cup M_D = M_N$. Кластерные ограничения отражаются на графе отсутствием полных *FLS* дуг между любыми элементами из разных подмножеств M_K. Мультиграф G^{FLS} является разновидностью цветной сети Петри [11], в которой *FLS*-маркеры имеют иерархическую зависимость и срабатывают в последовательности $R^F \longrightarrow R^L \longrightarrow R^S$ при совпадении согласованных выходных и входных индексов (цветов), которые определяют семантику переходов.

Задача анализа заключается в поиске состояний системы, нарушающих декларируемую политику, и в оценке уровня защиты для каждого пути по критерию отсутствия «слабого звена», т.е. вершин или дуг с весами ниже установленного значения. Статический анализ проводится на мультиграфе G^{FLS} проверкой гипотез о достижимости модулей при установленных кластерных ограничениях и позволяет оценить безопасность исходного состояния системы. Динамический анализ позволяет оценить безопасность состояний системы для всех траекторий информационной процесса при изменении состава вершин и дуг мультиграфа G^{FLS} в результате применения решающих правил управляемого логического вывода. Результаты проверки достижимости модулей отражаются в квадратной матрице достижимости модулей $A^Д = [a_{ij}]$ мультиграфа G^{FLS}, элементы которой строятся по правилу:

$$a_{ij} = \begin{cases} 1, \text{ если из вершины } i \text{ к вершине } j \text{ имеется путь } P_{ij}^{FLS}; \\ 0, \text{ если из вершины } i \text{ к вершине } j \text{ путь } P_{ij}^{FLS} \text{ отсутствует.} \end{cases} \quad (1)$$

Формальным критерием безопасности архитектуры является отсутствие пути P_{ij}^{FLS} между любыми произвольными вершинами из разных кластерных подмножеств M_K, который не содержит хотя бы одной вершины из подмножества M_D. Отсутствие пути доказывается сравнением значений каждой позиции кластерной матрицы $A^K = [a_{ij}]$, сформированной по правилам АСР с позицией в матрице достижимости $A^Д = [a_{ij}]$, которая формируется в результате логического вывода. Если матрицы равны, то формальные правила АСР выполняются и конфигурация архитектуры DLT безопасна. Для критических систем может быть установлен более строгий критерий безопасности – все полные *FLS*-дуги между любыми вершинами подмножества M_K должны быть инциденты хотя бы одной вершине из подмножества M_D. Этот случай актуален, например, для политики с «нулевым доверием» (Zero Trust), если каждое взаимодействие между любыми модулями осуществляется через процедуры безопасности.

Квантовая угроза для технологий распределенного реестра

Функции защиты могут быть реализованы МАС на физическом F, синтаксическом L или семантическом S уровнях информационного взаимодействия [7]. Для учета надежности МАС в оценке безопасности архитектуры DLT вершинам мультиграфа из множества M_D присваиваются нормированные весовые коэффициенты, характеризующие надежность защиты на основе внешних данных

$$V = |v_1^{(k)}, v_2^{(k)}, \ldots, v_n^{(k)}|. \quad (2)$$

Каждой v-ой вершине приписывается вес $V_v^{(k)}$, где k – функция веса.

Непрерывность уровня защиты оценивается сравнением значений весовых коэффициентов помеченных вершин графа для каждого пути относительно нормированного заданного значения, которое может быть установлено, например, классом защиты и уровнем доверия к средству защиты, или расчетным значением, например, стойкости криптографии к атакам с использованием квантового суперкомпьютера с высокой скоростью операций. Например, для функций шифрования и аутентификации, которые являются конструктивной основой безопасности архитектуры DLT, может быть задана оценка стойкости или вероятности компрометации криптографии. Для DLT оценка надежности криптографии является принципиальной. Публичные оценки скорости вычислений существующих квантовых компьютеров пока

не достигли области риска компрометации криптографии DLT, например, 13x106 кубит для взлома 256-битного ключа Bitcoin [6]. Однако анонсируется создание более производительных промышленных квантовых компьютеров, возможно скрытие информации об их наличии, разрабатываются эффективные методы атак на неидеальную криптографию при существующей скорости вычислений.

Снижение риска возможно, например, за счет использования постквантовой и идеальной криптографии, технологии квантового распределения ключей (QKD – Quantum Key Distribution). В частности, имеются рекомендации об использовании двойной длины ключа в симметричных блочных алгоритмах [6]. Усиление стойкости асимметричной криптографии за счет повышения сложности математических вычислений в предположении отсутствия эффективных методов обратного преобразования не дает гарантии конструктивной безопасности архитектуры DLT, что предполагает поиск альтернативной организации архитектуры для критических приложений.

Формальная постановка задачи анализа безопасности архитектуры DLTS

Пусть конечное множество элементов $M_N = \{m_1, m_2, ..., m_n\}$ (где N их число) составляет систему W, $M_K \cup M_D = M_N$ и $M_K \cap M_D = \emptyset$. Каждый элемент m обладает свойствами r_m^{FLS} из конечного множества свойств $R_M^{FLS} = \{R^F, R^L, R^S\}$, определенных на множестве M_N. Конкретный набор свойств всех элементов множества M_N, которые составляют подмножество $R_m^{FLS} \subset R_M^{FLS}$, определяет состояние ψ^t системы W в дискретный момент времени t. Множества M_N и R_M^{FLS} конечны, поэтому все состояния $\psi = f(M_N, R_M^{FLS}, t)$ принадлежат конечному множеству состояний Ψ системы W. Если в момент времени t между одной или несколькими парами модулей существуют бинарные отношения $\exists(m_i, m_j) \subset M_N$, которые на основании внешнего правила отнесены к подмножеству опасных, то состояние ψ^t относится к подмножеству опасных состояний $\bar{\Psi}$ системы W. Пусть задано множество Ψ объектов анализа и некоторое свойство r этого множества. Свойство r объекта анализа x может быть задано предикатом $P_r(x)$, определенным как функция на множестве Ψ со значениями «истина» (И) и «ложь» (Л)

$$P_r: \Psi \longrightarrow \{И, Л\}. \quad (3)$$

Если Ψ – множество состояний системы, ψ_i – безопасное состояние, ψ_j – опасное состояние, r – свойство «быть безопасным», то $P_r(\psi_i) = И$, $P_r(\psi_j) = Л$ для всех $\psi \in \Psi$. Множество Ψ разбивается предикатом P_r на два подмножества: $\Psi_r = \{\psi_1, \psi_2, ..., \psi_n\}$ – безопасные состояния системы, и $\bar{\Psi}_r = \{\psi_1, \psi_2, ..., \psi_e\}$ – опасные состояния системы. При этом справедливо

$$\Psi = \Psi_r \cup \bar{\Psi}_r, \Psi_r \cap \bar{\Psi}_r = \emptyset. \quad (4)$$

Вычислением значения истинности предиката $P_r(x)$ решается задача анализа безопасности некоторого объекта анализа x. Если свойство r рассматривать как сочетание других свойств объекта x, выраженных предикатами $P_{r_1}(x)$, $P_{r_2}(x)$, ..., то вычисление значения предиката $P_r(x)$ может быть проведено вычислением значения предикатов $P_{r_1}(x)$, $P_{r_2}(x)$, ... и затем определением истинности $P_r(x)$ путем приложения операции следования вида

$$F(P_{r_1}(x), P_{r_2}(x), ...) \longrightarrow P_r(x). \quad (5)$$

Применение некоторых операций логики к начальному множеству предложений, составляющему модель объекта x, и получение некоторого предложения этого же языка, являющегося формальным выражением свойства r, составляет процесс вычисления предиката $P_r(x)$. Каждое свойство r_j также может быть представлено через совокупность других свойств объекта. Задача анализа решается путем вычисления значения предиката $P_j(x)$, который принимает значение «истина», если объект x является j-ой модификацией ψ_j и значение «ложь» в противном случае. Представление логического компонента алгоритма анализа архитектуры DLTS в виде формальных операций логического следования на множестве предложений языка задания объекта анализа позволяет рассматривать процесс доказательства как многоуровневый управляемый логический вывод некоторого выражения этого языка, который отыскивается в ходе построения эксперимента.

Таким образом, в формальной постановке задача анализа безопасности архитектуры DLTS заключается в формировании множеств M_N и R_M^{FLS}, поиске элементов и доказательства полноты множества $\bar{\Psi}_r = \{\psi_1, \psi_2, ..., \psi_e\}$, где $\bar{\Psi}_r = f\{M_N, R_M^{FLS}\}$, для доказательства его пустоты ($\bar{\Psi}_r = \emptyset$), а также оценке соответствия весов $V_v^{(k)}$ элементов подмножества M_D установленному значению.

Доказательство безопасности состояний архитектуры DLTS

Для моделирования состояний системы FLS-подграфы задаются тремя взаимосвязанными квадратными бинарными FLS-матрицами

$$F = \|f_{i,j}\|; L = \|l_{i,j}\|; S = \|s_{i,j}\|, \quad (6)$$

где $i,j = 1, n$, n – максимальный номер вершины.

Свойства вершин и дуг мультиграфа задаются подматрицами FLS интерфейсов, которые полностью определяют функционально-структурные свойства модулей относительно других модулей архитектуры

$$F_{(ij)}^I = \|f_{(i^{вых.}\, j^{вх.})}^I\|; L_{(ij)}^I = \|l_{(i^{вых.}\, j^{вх.})}^I\|; S_{(ij)}^I = \|s_{(i^{вых.}\, j^{вх.})}^I\|, \quad (7)$$

где $F_{(ij)}^I$, $L_{(ij)}^I$, $S_{(ij)}^I$ – подматрицы смежных физических, синтаксических и семантических выходных для модулей m_i и входных для модулей m_j FLS интерфейсов.

Состояния системы являются результатом взаимодействия модулей на трех уровнях, поэтому необходимо генерировать согласованные FLS-матрицы смежности для каждого уровня информационного взаимодействия в соответствии с выражениями (6) и (7). Уровни взаимодействия представляются отдельными FLS-матрицами смежности, у которых строки и столбцы проиндексированы номерами модулей. Наличие значений, отличных от «0», в одинаковых позициях квадратных FLS-матриц указывает на то, что модули, номерами которых проиндексированы строки и столбцы, являются смежными вершинами.

Доказательство безопасности архитектуры обеспечивается управляемым перебором состояний в ходе построения FLS-мультиграфа состояний системы и определением на каждом шаге безопасности порожденного состояния. Проверка безопасности состояния заключается в установлении всех возможных отношений между модулями, которые изменялись на последнем шаге, и проверке их принадлежности подмножеству разрешенных отношений для этих модулей. Если отношения разрешены (присутствуют в кластерной FLS-модели), то состояние безопасное. Соответственно, если отношения запрещены (отсутствуют в кластерной FLS-модели), то состояние опасное. Строгость доказательства соответствует строгости математического аппарата логического вывода.

Подход к синтезу функционально стабильной архитектуры DLTS

Результаты оценки функционально-структурных свойств методами теории МК-сетей позволяют применять их для решения задачи структурно-функционального синтеза безопасной архитектуры DLTS, который заключается в итерационном процессе поиска опасных состояний и замыкании всех маршрутов между вершинами разных кластеров хотя бы на одну вершину подмножества M_D модулей MAC, а также замыкании всех входящих FLS-дуг на вершины со значением весового коэффициента не ниже установленного или замене модулей MAC из подмножества M_D.

Выводы

1. Применение методов теории МК-сетей, основанных на парадигме трехуровневого информационного FLS взаимодействия, позволяет моделировать и анализировать функционально-структурные свойства архитектуры DLT с формальным доказательством корректности результатов на основе управляемого логического вывода некоторого предложения формального языка математической логики.

2. Особенностью архитектуры DLT является однотипность FLS модулей, интерфейсов и кластеров ACP для всех (децентрализованная схема) или основного множества (централизованная и гибридная схемы) участников взаимодействия, что позволяет редуцировать граф состояний и аппроксимировать результаты на всю систему без потери достоверности оценок. Различия в схемах конфигурации архитектуры DLT могут учитываться в информационной модели, например, включением, кроме типовых модулей «потребитель» и «поставщик» данных, модулей «сервер хранения ключей», «сервер хранения данных», «управление обменом данными» и дополнительных FLS-интерфейсов [4]. В такой конфигурации возможен переход в опасное состояние через интерфейсы модулей, реализующих централизованные функции. При этом нарушается регулярность мультиграфа G^{FLS} и требуется корректировка исходной объектно-ориентированной информационной модели. Кроме того, в ACP с отсутствием доверия участников взаимодействия к централизованным модулям, их FLS интерфейсы формируют траектории процесса, которые всегда будут приводить систему в опасные состояния, например, из-за угрозы нарушения конфиденциальности транзакций и/или сведений об участниках взаимодействия. В этом случае для обеспечения корректности результатов логического вывода необходимо формировать ACP с исключением модулей с централизованными функциями из модели нарушителя безопасности и кластерных матриц. Целесообразно разработать модели угроз для типовых конфигураций архитектуры DLT с учетом особенностей ACP, архитектуры и квантовой угрозы.

3. Для оценки надежности криптографии DLT в условиях квантовой угрозы необходимы исследования с натурными экспериментами, в том числе с использованием квантовых коммуникаций и технологии квантового распределения ключей. Целесообразно провести оценку риска компрометации хранимых в DLT данных со сроком конфиденциальности более 5 лет в случае достижения «квантового превосходства», а также исследовать применение в DLT:

- более стойкой симметричной криптографии для снижения риска компрометации DLT при резком достижении «квантового превосходства» и/или появлении эффективных методов взлома неидеальной криптографии;
- технологии QKD для генерации криптографических ключей;
- «постквантовой» ассиметричной криптографии для защиты транзакций в некритических DLTS.

Для реализации формального анализа и синтеза функционально стабильной архитектуры DLTS на основе методов теории МК-сетей целесообразно провести дополнительные исследования и разработки, в частности:

- исследовать влияние ACP, децентрализованных, централизованных и гибридных конфигураций архитектуры на безопасность DLTS;

- разработать технологию построения модульно-кластерной модели DLTS с использованием технологии искусственного интеллекта, специально обученного для решения задач моделирования информационных процессов;
- разработать технологию автоматизированного синтеза безопасной архитектуры DLTS-P (Protection) на основе анализа модульно-кластерной модели.

В целях проведения натурного моделирования, проверки научных гипотез и синтеза безопасной архитектуры DLT в условиях квантовой угрозы перспективным является создание межотраслевого кластера квантовых коммуникаций и искусственного интеллекта в Научно-технологическом университете «Сириус» в рамках этапа II «Вторая очередь пилотного проекта – расширение межуниверситетской квантовой сети – с 01.01.2025 г. по 31.12.2025 г.» [11], что позволит решить научные задачи и достичь синергетического эффекта при взаимодействии с экспертами профильных организаций и ВУЗов.

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. Recommendation ITU-T X.1400 (10/2020), Distributed ledger technology security. Terms and definitions for distributed ledger technology.
2. Recommendation ITU-T X.1402 (07/2020), Distributed ledger technology security. Security framework for distributed ledger technology.
3. Recommendation ITU-T X.1408 (10/2021), Distributed ledger technology (DLT) security. Security threats and requirements for data access and sharing based on the distributed ledger technology.
4. Recommendation ITU-T X.1410 (03/2023), Distributed ledger technology (DLT) security. Security architecture of data sharing management based on the distributed ledger technology.
5. Федеральный закон РФ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной структуры РФ».
6. Mark Webber, Vincent Elfving, Sebastian Weidt, Winfried K. Hensinger. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. AVS Quantum Sci. 4, 013801 (2022); doi: 10.1116/5.0073075.
7. Сундеев П. В. Модульно-кластерные сети: основы теории / П. В. Сундеев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2006. – № 22. – С. 31–52.
8. Федеральный закон РФ от 26.07.2007 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
9. Запечников С. В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций / С. В. Запечников // Безопасность информационных технологий. – 2020. – Т. 27, № 4. – С. 108–123. – DOI 10.26583/bit.2020.4.09.
10. Системный анализ функциональной стабильности критичных информационных систем / Симанков В. С., Сундеев П. В. / под науч. ред. В. С. Симанкова. КубГТУ, ИСТЭк. – Краснодар, 2004. – 204 с.
11. K. Jensen Coloured Petri nets: A high-level language for system design and analysis // Advances in Petri Nets 1990, ICATPN 1989, Lecture Notes in Computer Science.– vol. 483, Berlin–Heidelberg: Springer.– 1991.– ISBN 978-3-540-53863-9.– Pp. 342–416. https://doi.org/10.1007/3-540-53863-1_31.
12. Концепция создания, развития и эксплуатации Межуниверситетской квантовой сети (МУКС) Национальной исследовательской квантовой сети (НИКС) на 2024–2030 годы (утв. заместителем министра науки и высшего образования РФ 02.02.2024 года).

FUNCTIONAL STABILITY OF A DISTRIBUTED REGISTRY IN THE CONTEXT OF A QUANTUM THREAT

Sundeev P. V.[2]

Keywords: *modular cluster network, system analysis, security.*

The purpose of the research: *to propose an approach to the formal analysis of the functional stability of distributed ledger systems for critical applications under conditions of quantum threat.*

Research methods: *object-oriented analysis and synthesis of complex systems, system analysis, theory of modular cluster networks, graph theory, matrix theory, mathematical logic.*

Research results: *the influence of architecture security and access policy on the functional stability of a distributed registry in the context of a quantum threat is shown, the concept and formulation of the problem of security analysis*

2 Pavel V. Sundeev, Doctor of Technical Sciences, Chief Research Engineer of the Scientific Center for Information Technologies and Artificial Intelligence of the Autonomous Educational Institution of Higher Education «Sirius University», Federal Territory «Sirius», Russia. E-mail: sundeev.pv@talantiuspeh.ru

of a distributed registry architecture in terms of the theory of modular cluster networks, an approach to the synthesis of architecture with proven security properties is proposed.

Scientific novelty: *application of the theory of modular cluster networks to the analysis of the functional stability of distributed registry systems in the aspect of security, taking into account the influence of the quantum threat.*

References

1. Recommendation ITU-T X.1400 (10/2020), Distributed ledger technology security. Terms and definitions for distributed ledger technology.
2. Recommendation ITU-T X.1402 (07/2020), Distributed ledger technology security. Security framework for distributed ledger technology.
3. Recommendation ITU-T X.1408 (10/2021), Distributed ledger technology (DLT) security. Security threats and requirements for data access and sharing based on the distributed ledger technology.
4. Recommendation ITU-T X.1410 (03/2023), Distributed ledger technology (DLT) security. Security architecture of data sharing management based on the distributed ledger technology.
5. Federal Law of the Russian Federation dated July 26, 2017 No. 187-ФЗ «On the security of the Critical Information Structure of the Russian Federation».
6. Mark Webber, Vincent Elfving, Sebastian Weidt, Winfried K. Hensinger. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. AVS Quantum Sci. 4, 013801 (2022); doi: 10.1116/5.0073075.
7. Sundeev P.V. Modular cluster networks: fundamentals of theory. KubGAU Scientific Journal [Electronic resource]. – Krasnodar: KubGAU, 2006. – № 22 (06). – The code of the Information Register is 0420600012\0132. Access mode: http://www.ej.kubagro.ru/2006/06/15.
8. Federal Law of the Russian Federation dated July 26, 2007 No. 149-ФЗ «On Information, Information Technologies and Information Protection».
9. Zapechnikov S.V. Distributed registry systems that ensure transaction confidentiality. Information Technology Security, [S.l.], v. 27, n. 4, pp. 108–123, 2020. ISSN 2074-7136.
10. System analysis of functional stability of critical information systems / Simankov V.S., Sundeev P.V. / under the scientific editorship of V.S. Simankov. KubSTU, ISTEk. Krasnodar, 2004. 204 p.
11. K. Jensen Coloured Petri nets: A high-level language for system design and analysis // Advances in Petri Nets 1990, ICATPN 1989, Lecture Notes in Computer Science. – vol. 483, Berlin – Heidelberg: Springer. – 1991. – ISBN 978-3-540-53863-9. – Pp.342–416. https://doi.org/10.1007/3-540-53863-1_31.
12. «The concept of creation, development and operation of the Interuniversity Quantum Network National Research Quantum Network (NICS) for 2024-2030» (approved by the Deputy Minister of Science and Higher Education of the Russian Federation on 02.02.2024).