КРИТЕРИИ И ПОКАЗАТЕЛИ КОНСТРУКТИВНОЙ ЗАЩИТЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Сундеев П. В.[1]

DOI: 10.21681/2311-3456-2025-5-103-108

Цель исследования: *исследовать проблему формальных критериев и показателей для оценки конструктивной защиты информационных систем с учетом особенностей архитектуры распределенного реестра в условиях квантовой угрозы, предложить подход к формированию критериев конструктивной защиты, позволяющих автоматизировать анализ и синтез безопасной архитектуры.*

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

Результат исследования: *предложен подход к формированию системы критериев и показателей конструктивной защиты архитектуры информационной системы на основе кластерной модели защиты с полным перекрытием, представленной в виде кластерного мультиграфа модульно-кластерной сети, и анализа ее топологии. Оценка безопасности архитектуры по критериям конструктивной защиты заключается в формальном анализе наличия или отсутствия определенных типов вершин и дуг кластерного мультиграфа. Показатель непрерывности конструктивной защиты для оценки безопасности траекторий информационного процесса основан на сравнении весов помеченных вершин, обозначающих модули защиты, с установленным значением. Показана применимость критериев конструктивной защиты к оценке технологии распределённого реестра.*

Научная новизна: *разработан новый подход к формированию формальных критериев и показателей конструктивной защиты информационных систем на основе кластерной модели защиты с полным перекрытием в терминах теории модульно-кластерных сетей.*

Ключевые слова: *модульно-кластерная сеть, квантовая угроза, защита информации.*

Введение

При разработке защищенных информационных систем необходимо оценивать безопасность архитектуры, программного кода, учитывать политику доступа [1–4]. Критериями безопасности архитектуры, как правило, являются требования к защите информации и их реализации, установленные стандартами[2] и нормативными актами, которые не формальны и не позволяют доказывать безопасность архитектуры. Формальные показатели эффективности средств защиты информации, например, защиты от побочных электромагнитных излучений, стойкости криптографии, безопасности программного кода и т.д. применимы к оценке элементов, но не позволяют оценить безопасность архитектуры системы. В случае критических систем оценка должна быть формальной, чтобы минимизировать риск нарушения безопасности информации с неприемлемым ущербом. Технология распределенного реестра (DLT) используется в национальных блокчейн-экосистемах, критических приложениях в финансовой, медицинской и других сферах деятельности. Из-за нарушения безопасности информации может быть нанесен неприемлемый ущерб. Поэтому обеспечение конструктивной защиты архитектуры является непременным условием безопасности систем распределенного реестра (DLTS). Особенностью конструктивной безопасности «классической» архитектуры DLT является конструктивная защита, которая обеспечивается децентрализованной топологией информационного взаимодействия недоверенных субъектов и криптографией[3]. Масштабное использование криптографии с неидеальной стойкостью создает высокий риск компрометации из-за «квантовой угрозы», связанной с появлением эффективных методов атаки на ключевые системы, и квантовых компьютеров с высокой скоростью вычислений [5–9].

Система критериев конструктивной защиты позволяет оценивать безопасность архитектуры по результатам анализа топологии мультиграфа, который является информационной моделью системы с учетом ее защиты. В зависимости от постановки задачи при оценке безопасности может проверяться наличие или отсутствие определенных типов вершин, дуг и их веса. Применение формальных

1 Сундеев Павел Викторович, доктор технических наук, главный инженер-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Адрес: Россия, 354340, Краснодарский край, Федеральная территория «Сириус», пгт Сириус, проспект Олимпийский, д.1., ORCID: 0009-0005-8442-8921, E-mail: sundeev.pv@talantiuspeh.ru

2 ГОСТ Р 72118-2025 «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки».

3 Recommendation ITU-T X.1410 (03/2023), Distributed ledger technology (DLT) security. Security architecture of data sharing management based on the distributed ledger technology.

критериев позволяет автоматизировать процесс оценки конструктивной защиты информационной системы и улучшить ее достоверность.

Концепция оценки конструктивной защиты

Термин «конструктивная защита» информационной системы может трактоваться в узком смысле, когда обработка информации технологически невозможна без использования функций защиты, и в широком смысле, когда к ней относят дополнительные функции (средства) защиты, которые компенсируют отсутствующие функции защиты и уязвимости архитектуры. Примерами конструктивной защиты могут быть технология квантового распределения ключей, биометрическая аутентификация, DLT.

Критерии конструктивной защиты информационной системы разработаны на основе положений теории модульно-кластерных сетей (МК-сеть) с использованием кластерной модели защиты информации с полным перекрытием [10]. В терминах МК-сетей конструктивная защита информации рассматривается как архитектурные ограничения топологии информационного взаимодействия, а также функции защиты, которые реализуют управление доступом и компенсируют недостатки архитектуры с целью ограничения несанкционированного взаимодействия. Формальным критерием или показателем конструктивной защиты в терминах теории МК-сетей может быть оценка наличия, отсутствия и свойств элементов топологии кластерного мультиграфа (вершин, дуг и их весов), которые влияют на доступ субъектов к объектам.

Для формальной оценки безопасности информационная система и ее окружение представляются в виде объектно-ориентированной модели в терминах теории МК-сетей, в которых используется декомпозиция информационных взаимодействий на физические (F), синтаксические (L) и семантические (S) отношения между модулями [10]. Если объектно-ориентированную информационную модель Q представить в виде графа, то элементы множеств M_N и R_M^{FLS} будут составлять множество вершин кластерного мультиграфа $G^{FLS}(M_N,R_M^{FLS})$, где N – число вершин, и R_M^{FLS} – множество дуг, которые обозначают информационные связи между вершинами, обозначающими физические и логические модули, имеющие функциональное значение в процессах обработки и защиты информации. При этом множество дуг R_M^{FLS} состоит из подмножеств внутренних дуг инцидентных вершинам одного кластера R^K и подмножества внешних дуг инцидентных вершинам из разных кластеров $R^{\bar{K}}$, таких что $R^K \cap R^{\bar{K}} = \emptyset$. Таким образом, модульно-кластерная сеть представляет собой FLS-мультиграф $G^{FLS}(M_N,R_M^{FLS})$, вершины которого обозначают 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 возможна реализация информационных FLS-отношений.

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

Утверждение 1. Любые две вершины $\{m_i,m_j\}$ мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ являются смежными, если и только если в остовных 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. Если любые две вершины $\{m_i,m_j\}$ графа $G^{FLS}(M_N,R_M^{FLS})$, обозначающие модули МК-сети, смежные, то возможно информационное взаимодействие между этими модулями.

Утверждение 3. Путь P_{ij}^{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 P_{ij}^F, P_{ij}^L, P_{ij}^S между этими вершинами в остовных FLS-подграфах.

Критериями распределения вершин по кластерам являются одинаковые для них внешние правила доступа, установленные в эталонной кластерной матрице, которые в свою очередь определяются принадлежностью модуля к системе W, окружению V или средствам защиты D, а также правилами разграничения доступа и системными критериями конструктивной защиты.

Политика доступа разбивает систему на множество кластеров $K = \{K^W,K^V,K^D\}$. Для вершин одного кластера установлены общие правила доступа, то есть взаимодействие не ограничено. Для вершин разных кластеров установлены разные правила доступа, то есть взаимодействие ограничено или запрещено. Возможна вложенность кластеров с иерархическими правилами доступа. Если правила выполняются для произвольной пары вершин $\{m_i,m_j\}$ и отсутствует путь P_{ij}^{FLS} между вершинами разных кластеров мультиграфа, между которыми политикой доступа запрещено взаимодействие, то архитектура безопасна. При этом политика доступа должна разрешать взаимодействие с модулями подмножества M_d^D, обозначающими модули защиты из кластеров подмножества K^D, через которые осуществляется управление доступом и в соответствии с политикой может быть создана дуга в остовном F, L или S подграфе для образования полной FLS-дуги.

Таким образом, кластерная структура системы Q определяется на множествах модулей $M_N=\{M_w^W,M_v^V,M_d^D\}$ информационной системы W и ее окружения V, множествах FLS-отношений $R_M^{FLS} = \{R^F,R^L,R^S\}$ и кластеров $K_Q = \{K^W,K^V,K^D\}$,

$$G_Q^{FLS}(M_N,R_M^{FLS}) \equiv$$
$$\equiv \begin{cases} M_N = \{M_w^W,M_v^V,M_d^D\} | \{M_w^W \cap M_v^V \cap M_d^D\} = \emptyset; \\ R_M^{FLS} = \{R_W^{FLS};R_V^{FLS};R_D^{FLS};R_{W^*}^{FLS};R_{V^*}^{FLS};R_{D^*}^{FLS}\}; \\ K_Q = \{K^W,K^V,K^D\} | \{K^W \cap K^V \cap K^D\} = \emptyset; \end{cases} \quad (1)$$

где $\{R_W^{FLS};R_V^{FLS};R_D^{FLS};R_{W^*}^{FLS};R_{V^*}^{FLS};R_{D^*}^{FLS}\}$ – подмножества полных внутренних $\{R_W^{FLS};R_V^{FLS};R_D^{FLS}\}$ и внешних $\{R_{W^*}^{FLS};R_{V^*}^{FLS};R_{D^*}^{FLS}\}$ FLS-дуг кластеров $\{K^W,K^V,K^D\}$.

Системные критерии конструктивной защиты определяют наличие или отсутствие вершин или дуг внутри и между кластерными подмножествами K_Q мультиграфа $G^{FLS}(M_N,R_M^{FLS})$, что указывает на наличие или отсутствие пути P_{ij}^{FLS} между любыми произвольными вершинами $\{m_i,m_j\}$ из кластерных подмножеств K^W и K^V или разных кластеров подмножества K^W. Для разных топологий и уровней защиты может использоваться один или несколько критериев конструктивной защиты. При выборе критериев должны учитываться топология информационного взаимодействия, уровни защиты и доверия, которые необходимо обеспечить для конкретной системы, а также используемые технологии обработки и защиты информации.

Формальные критерии и показатели конструктивной защиты

Рассмотрены критерии и показатели конструктивной защиты для наиболее распространённых случаев.

Критерий 1. Если все внешние дуги $R_{W^*}^{FLS}$ кластера K^W инцидентны вершинам из кластера K^D, то конструктивно архитектура системы безопасна.

В этом случае кластеры K^W и K^V не имеют смежных вершин. Критерий актуален для информационных систем с единой политикой для всех собственных субъектов и объектов доступа. Соответственно, оценка конструктивной защиты архитектуры проводится поиском полных FLS-дуг между вершинами кластеров K^W и K^V. Критерий актуален для случая периметровой защиты при отсутствии разделения прав доступа между субъектами внутри системы.

Более сильный критерий 2 конструктивной защиты учитывает внутренние угрозы, связанные с разными политиками доступа для разных кластеров системы W.

Критерий 2. Если все внутренние R_W^{FLS} и внешние $R_{W^*}^{FLS}$ дуги кластеров $\{K_1^W,K_2^W,...,K_N^W\} \subseteq K^W$ инцидентны вершинам из кластеров K^D, то конструктивно архитектура системы безопасна.

Критерий актуален для случая групповых политик, когда в информационной системе установлены одинаковые правила доступа в выделенных группах субъектов и объектов доступа.

Для взаимодействия недоверенных субъектов актуален критерий конструктивной защиты, предусматривающий возможность взаимодействия только через средства защиты. В случае однотипной политики доступа для всех субъектов, например, в «классической» архитектуре DLT, все вершины становятся кластерами, что приводит к трактовке критерия 1.

Критерий 3. Если каждый кластер $\{K_1^W,K_2^W,...,K_N^W\} \subseteq K^W$ имеет только одну вершину и внешние дуги $R_{W^*}^{FLS}$ кластеров K^W инцидентны вершинам из кластеров K^D, то конструктивно архитектура системы безопасна.

Оценка конструктивной защиты архитектуры по критерию 3 заключается в проверке отсутствия полных FLS-дуг между вершинами кластеров $K_1^W,K_2^W,...,K_N^W$ и с вершинами из K^V, наличия только одной вершины в каждомкластере K^W и наличия у него FLS-дуги с вершиной из кластера K^D.

Следующий критерий безопасности актуален для критических информационных систем с необходимостью обеспечения относительно высокого уровня доверия. В этом случае в каждый кластер $K_1^W,K_2^W,...,K_N^W$ включаются кластеры K^D или вершины из подмножества M_d^D, которые обозначают функции (средства) защиты информации. Критерий применим, когда каждый субъект имеет собственные «доверенные» средства защиты информации и может управлять доступом к своим объектам в кластере без участия посредников.

Критерий 4. Если каждый кластер $K_1^W,K_2^W,...,K_N^W$ имеет вершины из подмножества M_d^D и внешние дуги $R_{W^*}^{FLS}$ каждого кластера инцидентны только этим вершинам кластера, то конструктивно архитектура системы безопасна.

На практике чаще встречаются гибридные схемы с встроенными в K^W и дополнительными средствами защиты из подмножества M_d^D, для оценки которых необходимо использовать несколько критериев.

Для всех критериев средства защиты из подмножества M_d^D должны иметь установленный уровень доверия, выбор которого зависит от оценки рисков. Уровень доверия может учитываться в весах вершин.

При использовании критериев конструктивной защиты анализ безопасности топологии архитектуры сводится к поиску вершин, которые должны отсутствовать или присутствовать в МК-модели системы, и в оценке смежности определенных типов вершин мультиграфа. В систему критериев могут быть включены требования к наличию, смежности и месту размещения в мультиграфе вершин, обозначающих модули с определенными функциями защиты. Сравнение значений весов определенных типов вершин мультиграфа с установленным знамением, является показателем уровня защиты.

Высокий уровень конструктивной защиты в узкой трактовке термина дает использование функций

защиты технологически не отделимых от процедур обработки информации. Например, такими технологиями являются квантовое распределение ключей и биометрическая аутентификация. Формально в мультиграфе такие свойства могут задаваться объединением функций защиты в один кластер средств защиты, например, K^{FL}, а также весами дуг, на одном или более уровней FLS-отношений, рассчитанных по внешним методикам.

Показателем эффективности элементов защиты являются веса вершин или дуг мультиграфа. Если значение весов вершин из подмножества M_d^D принадлежащих пути P_{ij}^{FLS} между произвольной парой вершин $\{m_i, m_j\}$ в FLS-мультиграфе $G^{FLS}(M_N, R_M^{FLS})$ не ниже установленного значения, то конструктивно архитектура системы безопасна.

Значение веса, например, для средств криптографической защиты DLT может быть задано значением показателя стойкости криптографии с учетом «квантовой угрозы» [6–9]. При заданных значениях весов вершин оценка проводится сравнением веса каждой вершины с установленным значением с учетом требуемого уровня защиты.

Для учета надежности функций защиты в оценке безопасности архитектуры вершинам мультиграфа из подмножества M_d^D присваиваются нормированные весовые коэффициенты, характеризующие надежность защиты на основе внешних данных

$$D = |d_1^{(k)}, d_2^{(k)}, \ldots, d_n^{(k)}|. \quad (2)$$

Каждой d-ой вершине приписывается вес, 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 классом защиты и уровнем доверия к средству защиты или расчетным значением, например, стойкости криптографии к атакам с использованием квантового суперкомпьютера с высокой скоростью вычислений. Например, компания IBM анонсировала технологический прорыв в обработке ошибок и создание промышленного квантового компьютера на 200 логических кубитов к 2029 году [12, 13], что приближает горизонт реализации «квантовой» угрозы для широко используемых информационных систем, в которых применяется асимметричная или не стойкая симметричная криптография. В системах, для которых криптография является основой конструктивной защиты, например, для национальных распределенных реестров, разработка надежных постквантовых криптографических алгоритмов становится приоритетной задачей [14].

Кластерная модель защиты позволяет продемонстрировать использование системных критериев для оценки конструктивной защиты архитектуры на FLS-уровнях информационных отношений. На рис. 1 пример а) демонстрирует неконтролируемое взаимодействие $R_{v.w}^{FLS}$ модулей v_z и w_y из кластеров K_3^V и K_2^W, что по критерию 1 оценивается как угроза безопасности.

В примере б) показана блокировка связи между модулями v_z и w_y кластеров K_3^V и K_2^W средством защиты семантического уровня $d_s^{K_S^D}$ из подмножества

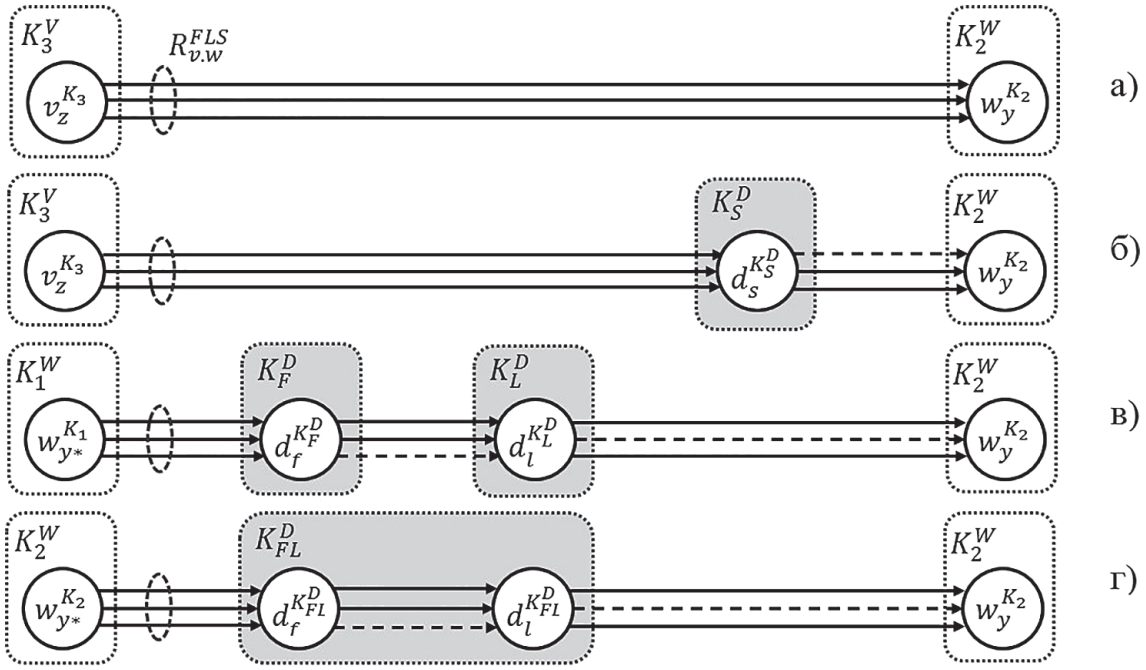

Рис. 1. Критерии конструктивной защиты архитектуры

M_d^D, например, средством разграничения доступа. В примере в) показано взаимодействие модулей $w_{y^*}^{K_1}$ и $w_y^{K_2}$ из кластеров K_1^W и K_2^W контролируемое средствами защиты физического $d_f^{K_F^D}$ и синтаксического $d_l^{K_L^D}$ уровней, например, средством физической защиты периметра и средством шифрования. Пример г) демонстрирует защиту взаимодействия модулей w_y и w_{y^*} из одного кластера K_2^W через средство, которое реализует конструктивную защиту в узкой трактовке термина на физическом $d_1^{K_1^F}$ и синтаксическом уровнях $d_1^{K_1^L}$, например, средство квантового распределения ключей.

Выводы

Предложен подход к формированию формальных критериев и показателей конструктивной защиты архитектуры информационных систем, которые сформированы на основе кластерной модели защиты в терминах теории МК-сетей. Критерии конструктивной защиты позволяют проводить формальный анализ FLS-мультиграфа, который является моделью информационной архитектуры, с учетом топологии информационного взаимодействия и политики доступа, оценивать непрерывность уровня защиты для траекторий информационного процесса сравнением нормированных весов средств защиты информации с установленным уровнем защиты.

Оценка конструктивной защиты архитектуры информационной системы обеспечивается формальным анализом наличия или отсутствия вершин и дуг мультиграфа. Критерии конструктивной защиты инвариантны к широкому классу задач оценки безопасности архитектуры и вариантов топологии информационного взаимодействия, могут быть использованы при разработке стандартов конструктивной безопасности информационных систем, создании систем с «иммунной защитой». Результаты исследований позволяют разработать систему критериев конструктивной защиты для решения проблемы оценки безопасности, автоматизации анализа и синтеза DLTS с доказательством уровня безопасности с применением аппарата математической логики.

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. Antipov I. S., Arustamyan S. S., Ganichev A. A. Markov A. S. et al. Intelligent Fuzzing Method for Aviation Information Systems as Part of the Secure Software Development Cycle. Russian engineering research. 45, 685–690 (2025). DOI: 10.3103/S1068798X25700728.
2. Ищукова Е. А. О влиянии криптографической стойкости функций хеширования на устойчивость современных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 3(67). С. 63-71. DOI: 10.21681/2311-3456-2025-3-63-71.
3. Markov A. S., Varenitca V. V., Arustamyan S. S. Topical issues in the implementation of secure software development processes. В сборнике: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. 2023. С. 48–53.
4. Наседкин П. Н. Оценка состояния комплексной системы защиты информации на основе онтологий / П. Н. Наседкин, Л. В. Аршинский // Информационные и математические технологии в науке и управлении. 2023. № 1(29). С. 158–177. – DOI:10.38028/ESI.2023.29.1.014.
5. Балябин А. А., Петренко С. А. Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. № 3(67). С. 72–82. DOI: 10.21681/2311-3456-2025-3-72-82.
6. Petrenko A. S., Petrenko S. A. Basic Algorithms Quantum Cryptanalysis // Вопросы кибербезопасности. 2023. No. 1(53). P. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115.
7. Petrenko A. S. Applied Quantum Cryptanalysis (scientific monograph). River Publishers. (2023). 256 p. ISBN 9788770227933. DOI: 10.1201/9781003392873.
8. 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.
9. Battarbee C., Kahrobaei D., Perret L., Shahandashti S. F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures. In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023. (2023). Lecture Notes in Computer Science. V. 14154. P. 113–138. Springer, Cham. DOI: 10.1007/978-3-031-40003-2_5.
10. Li L., Lu X., Wang K. Hash-based signature revisited. (2022). Cybersecurity. V. 5. Article no. 13. DOI:10.1186/s42400-022-00117-w.
11. Сундеев П. В. Функциональная стабильность распределенного реестра в условиях появления новой квантовой угрозы // Вопросы кибербезопасности. 2025. № 3(67). С. 83–89. DOI: 10.21681/2311-3456-2025-3-83-89.
12. Tristan Muller, Thomas Alexander, Michael E. Beverland, Markus Buhler, Blake R. Johnson, Thilo Maurer, Drew Vandeth. Improved belief propagation is sufficient for real-time decoding of quantum memory. IBM Quantum. (Dated: June 11, 2025). DOI: 10.48550/arXiv.2506.01779.
13. Theodore J. Yoder1, Eddie Schoute1, Patrick Rall1, Emily Pritchett1, Jay M. Gambetta1, Andrew W. Cross1, Malcolm Carroll1, and Michael E. Beverland. Tour de gross: A modular quantum computer based on bivariate bicycle codes. IBM Quantum. (Dated: June 03, 2025). DOI: 10.48550/arXiv.2506.03094.
14. Skiba V. Yu., Petrenko S. A., Gnidko K. O., Petrenko A. S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security. Computing, Telecommunication and Control, 2025, Vol. 18, No. 2, pp. 56–73.

CRITERIA AND INDICATORS FOR CONSTRUCTIVE PROTECTION OF THE DISTRIBUTED REGISTRY

Sundeev P. V.[4]

Keywords: *modular cluster network, quantum threat, information protection.*

The purpose of the study: *to investigate the problem of formal criteria and indicators for evaluating the constructive protection of information systems, taking into account the features of the architecture of a distributed registry in the context of a quantum threat, to propose an approach to the formation of criteria for constructive protection that automate the analysis and synthesis of secure architecture.*

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

Research result: *an approach to the formation of a system of criteria and indicators for constructive protection of an information system architecture based on a cluster protection model with complete overlap, presented as a cluster multigraph of a modular cluster network, and an analysis of its topology is proposed. The assessment of architecture security according to the criteria of constructive protection consists in a formal analysis of the presence or absence of certain types of vertices and arcs of a cluster multigraph. The continuity indicator of constructive protection for assessing the safety of information process trajectories is based on comparing the weights of the marked vertices indicating the protection modules with the set value. The applicability of constructive protection criteria to the evaluation of distributed registry technology is shown.*

Scientific novelty: *a new approach to the formation of formal criteria and indicators for constructive protection of information systems based on a cluster protection model with complete overlap in terms of the theory of modular cluster networks has been developed.*

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. Antipov, I. S., Arustamyan, S. S., Ganichev, A. A., Markov, A. S. et al. Intelligent Fuzzing Method for Aviation Information Systems as Part of the Secure Software Development Cycle. (2025). Russian engineering research. No 45. P. 685–690. DOI: 10.3103/S1068798X25700728.
2. Ishchukova, E. A. On the influence of cryptographic stability of hashing functions on the stability of modern blockchain ecosystems and platforms. (2025). Voprosy Kiberbezopasnosti [Cybersecurity issue]. No 3 (67). P. 63-71. DOI: 10.21681/2311-3456-2025-3-63-71 (Russian Text).
3. Markov, A. S., Varenitca, V. V., Arustamyan, S. S. Topical issues in the implementation of secure software development processes. (2023). In the collection: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. P. 48–53.
4. Nasedkin, P. N. Assessment of the state of the integrated information security system based on ontologies. (2023). Informacionnye i matematicheskie tekhnologii v nauke i upravlenii. [Information and mathematical technologies in science and management]. No 1(29). P. 158–177. DOI:10.38028/ESI.2023.29.1.014 (Russian Text).
5. Balyabin, A. A., Petrenko, S. A. Model of a blockchain platform with cyber-immunity under quantum attacks. (2025). Voprosy Kiberbezopasnosti [Cybersecurity issue]. No 3(67). P. 72–82. DOI: 10.21681/2311-3456-2025-3-72-82 (Russian Text).
6. Petrenko, A. S., Petrenko, S. A. Basic Algorithms Quantum Cryptanalysis. (2023). Voprosy Kiberbezopasnosti [Cybersecurity issue]. No. 1(53), pp. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115 (Russian Text).
7. Petrenko, A. S. Applied Quantum Cryptanalysis (scientific monograph). (2023). River Publishers. 256 p. ISBN 9788770227933. DOI: 10.1201/9781003392873.
8. Webber, M., Elfving, V., Weidt, S., Hensinger, W. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. (2022). AVS Quantum Sci. 4, 013801. DOI: 10.1116/5.0073075.
9. Battarbee, C., Kahrobaei, D., Perret, L., Shahandashti, S. F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures. In: Johansson, T., Smith-Tone, D. (eds). (2023). Post-Quantum Cryptography. PQCrypto 2023. Lecture Notes in Computer Science. V. 14154. P. 113–138. Springer, Cham. DOI: 10.1007/978-3-031-40003-2_5.
10. Li, L., Lu, X., Wang, K. Hash-based signature revisited. (2022). Cybersecurity. V. 5. Article No. 13. DOI:10.1186/s42400-022-00117-w.
11. Sundeev, P. V. Functional stability of a distributed registry in the context of the emergence of a new quantum threat. (2025). Voprosy Kiberbezopasnosti [Cybersecurity issue]. No 3 (67). P. 83–89. DOI: 10.21681/2311-3456-2025-3-83-89 (Russian Text).
12. Muller, T., Alexander, T., Beverland, M., Buhler, M., Johnson, B., Maurer, T., Vandeth, D. Improved belief propagation is sufficient for real-time decoding of quantum memory. (2025). IBM Quantum. DOI: 10.48550/arXiv.2506.01779.
13. Yoder, T., Schoute, E., Rall, P., Pritchett, E., Gambetta, J., Cross, A., Carroll, M., Beverland, M. (2025). Tour de gross: A modular quantum computer based on bivariate bicycle codes. IBM Quantum. DOI: 10.48550/arXiv.2506.03094.
14. Skiba, V. Y., Petrenko, S. A., Gnidko, K. O., Petrenko, A. S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security. (2025). Computing, Telecommunication and Control. Vol. 18, No. 2, pp. 56–73.

4 Pavel V. Sundeev, Dr. Sc. (Technical), Chief researcher, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Address: Olimpiyskiy ave. b.1, Sirius, Sirius Federal Territory, Krasnodar region, Russia, 354340, ORCID: 0009-0005-8442-8921. E-mail: Sundeev.pv@talantiuspeh.ru