КЛАСТЕРНАЯ МОДЕЛЬ ЗАЩИТЫ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Сундеев П. В.[1]

DOI: 10.21681/2311-3456-2025-4-2-8

Цель исследования: *разработать модель защиты информации для анализа конструктивной безопасности архитектуры распределенного реестра с учетом политики разграничения доступа и квантовой угрозы.*

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

Результат исследования: *разработана расширенная модель защиты информации с полным перекрытием для систем распределенного реестра с учетом влияния квантовой угрозы, которая позволяет оценивать конструктивную защиту, проводить формальный статический или динамический анализ безопасности архитектуры.*

Научная новизна: *на основе методов теории модульно-кластерных сетей разработана расширенная модель защиты информации с полным перекрытием для анализа конструктивной безопасности распределенного реестра за счет кластерной декомпозиции архитектуры и информационных взаимодействий, учета эффективности средств защиты информации. Показаны системные критерии оценки конструктивной защиты.*

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

Введение

При разработке систем распределенного реестра (DLTS) необходим анализ конструктивной безопасности архитектуры [1–3]. Особенностью технологии распределенного реестра (DLT) является конструктивная защита на основе криптографии и децентрализации информационного взаимодействия[2]. Сложная топология распределенного информационного взаимодействия, появление эффективных методов взлома криптографии с неидеальной стойкостью и увеличение скорости вычислений создают риск нарушения безопасности транзакций [4–9]. Для анализа безопасности архитектуры DLTS необходима формальная модель защиты, в которой учтены все существенные свойства, применимы критерии для оценки конструктивной защиты с формальным доказательством безопасности архитектуры, имеется возможность учета политики доступа и эффективности средств защиты информации.

Известна теоретическая модель защиты информации с полным перекрытием, которая строится из предположения о необходимости контроля каждого возможного воздействия по схеме «угроза (v) – защита (d) – объект (o)». Для построения модели необходимо определить множества угроз V, средств D и объектов O защиты, а также взаимосвязи между ними. В развитии модели предлагалось ввести в нее множество уязвимостей $\overline{V}$, определяемого подмножеством декартова произведения $T \times O$, и множество барьеров – путей осуществления угроз безопасности, перекрытых средствами защиты, и определяемого декартовым произведением $\overline{V} \times M$.

Практическое применение теоретической модели для распределенных систем со сложной политикой разграничения доступа и динамичной топологией информационного взаимодействия, которая характерна для систем с «открытой» архитектурой, ограничено достоверностью модели защиты из-за проблем с определением элементов указанных множеств и поиском опасных траекторий информационного процесса, а также отсутствием метода оценки их соответствия декларируемой политике доступа. При этом граф состояний системы может иметь большую размерность. Сложность его анализа может соответствовать классу NP-полных задач, поэтому формальная модель защиты должна обеспечивать редукцию графа состояний системы.

Задача моделирования защиты информации

В формальных моделях доступа информационное взаимодействие субъектов и объектов регулируется правилами политики разграничения доступа, которая обеспечивается конструктивно топологией архитектуры системы и средствами защиты, компенсирующими ее уязвимости. Поэтому модель защиты – это, по сути, статическая или динамическая модель собственно информационной системы с включенными в нее элементами, моделирующими источники внешних и внутренних угроз, а также конструктивные и дополнительные элементы защиты информации.

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

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

Пусть задана система распределённого реестра W и ее информационное окружение V. Физические и логические модули M_N^W и $M_{N^*}^V$, которые имеют выделенное функциональное значение при реализации информационного взаимодействия (средства защиты, субъекты и объекты доступа, способные реализовать информационные примитивы), являются элементами множеств W и V. Вместе они составляют множество вершин графа $G(M_{N+N^*},R_M)$, где $N+N^*$ – число вершин графа, и R_M – множество дуг, которые обозначают информационные взаимосвязи между модулями.

Для анализа безопасной архитектуры DLTS формальная модель защиты информации должна включать и обеспечивать:

- разделение субъектов и объектов доступа M_N^W и $M_{N^*}^V$ на непересекающиеся подмножества, для которых установлены разные политики доступа;
- средства ограничения или управления доступом (защиты информации) $D(M_D^W \subset M_N^W)$, которые обеспечивают разделение множества вершин графа G на непересекающиеся подмножества;
- информационные связи R_M между средствами защиты, субъектами и объектами, которые реализуют информационный процесс и существенны для управления доступом к объектам защиты;
- критерии для оценки конструктивной защиты архитектуры DLTS;
- редукцию порождающего графа состояний системы W и ее окружения V для снижения размерности области поиска опасных состояний;
- формальную верификацию безопасности архитектуры DLTS.

Кластерная модель защиты

В расширенной кластерной модели защиты информации с полным перекрытием проблема точности формальной модели решается определением субъектов и объектов доступа в качестве функциональных информационных модулей и декомпозицией информационных взаимодействий между ними на физические (F), синтаксические (L) и семантические (S) отношения с учетом их функциональных свойств, существенных для защиты информации, на основе методов теории модульно-кластерных сетей [11] с последующей оценкой безопасности статичной или динамичной топологии системы и эффективности средств защиты. Граф $G(M_{N+N^*},R_M)$ преобразуется в мультиграф $G^{FLS}(M_{N+N^*},R_M^{FLS})$. В мультиграфе G^{FLS} к множеству дуг R_M^{FLS} относятся только кратные дуги вида $\{r_{ij}^F \cup r_{ij}^L \cup r_{ij}^S\} \subseteq R_M^{FLS}$. Состав дуг мультиграфа определяется наличием входных и выходных интерфейсов модулей, обеспечивающих реализацию информационных примитивов через FLS-отношения, которые имеют иерархическую зависимость вида $r^F \longrightarrow r^L \longrightarrow r^S$. Состав вершин и дуг мультиграфа может меняться при наличии условий для информационного взаимодействия модулей по правилу «если взаимодействие возможно, то оно реализуется». Некратные FLS-дуги включаются в мультиграф при анализе угроз безопасности информации.

Все субъекты и объекты распределяются по кластерам K^W в соответствии с правами доступа, установленными политикой разграничения доступа, с учетом топологии системы. Внешние источники угроз из множества $M_{N^*}^V$ выделяются в отдельные кластеры K^V. Одному кластеру могут принадлежать только «доверенные» субъекты и объекты с одинаковым уровнем доступа. Субъекты доступа из других кластеров рассматриваются как потенциальные источники угроз. Распределение вершин $M_{N^*}^V$ и M_N^W по кластерам, которые являются источниками внешних и внутренних угроз, позволяет использовать модель защиты в качестве модели угроз. В DLTS, которые предназначены для взаимодействия недоверенных субъектов в конкурентной среде, каждый субъект может быть выделен в отдельный кластер. Одинаковые правила доступа для объектов и субъектов позволяют редуцировать граф состояний системы и свести сложность задачи поиска опасных состояний к разрешимости за полиномиальное время.

На рис. 1 представлена расширенная кластерная модель защиты информации с полным перекрытием. В качестве объекта защиты рассматривается кластер K_2^W системы W. К множеству угроз V для кластера K_2^W отнесены внешние нарушители из кластера K_3^V и внутренние субъекты из кластера K_1^W системы W, для которых установлена иная политика доступа.

Возможные информационные взаимодействия R^{FLS} между модулями представлены кратными дугами. Декомпозиция позволяет определить средства (функции) защиты из множества D^{FLS}, которые обеспечивают конструктивную безопасность и реализуют меры защиты на одном или нескольких уровнях FLS-отношений. Например, на синтаксическом уровне L конструктивно реализована криптографическая защита DLT, на F и L уровнях обеспечиваться конструктивная защита с использованием технологии квантового распределения ключей, на S уровне реализуется механизм авторизации.

В формальном описании кластерной модели защиты с полным перекрытием множество вершин M_{N+N^*}, где $N+N^*$ – число всех вершин мультиграфа G^{FLS}, разбивается политикой доступа на кластерные подмножества субъектов и объектов доступа (модулей) K_K ($K = 1, \ldots, k$ – число кластеров), такие что $K_1 \cap \ldots \cap K_k = \emptyset$ и $K_1 \cup \ldots \cup K_k = K_K$, и K_D – кластерные подмножества, состоящие из элементов множества $D^{FLS} = \{d_f^F, d_l^L, d_s^S\}$ средств защиты, и $K_K \cap K^D = \emptyset$.

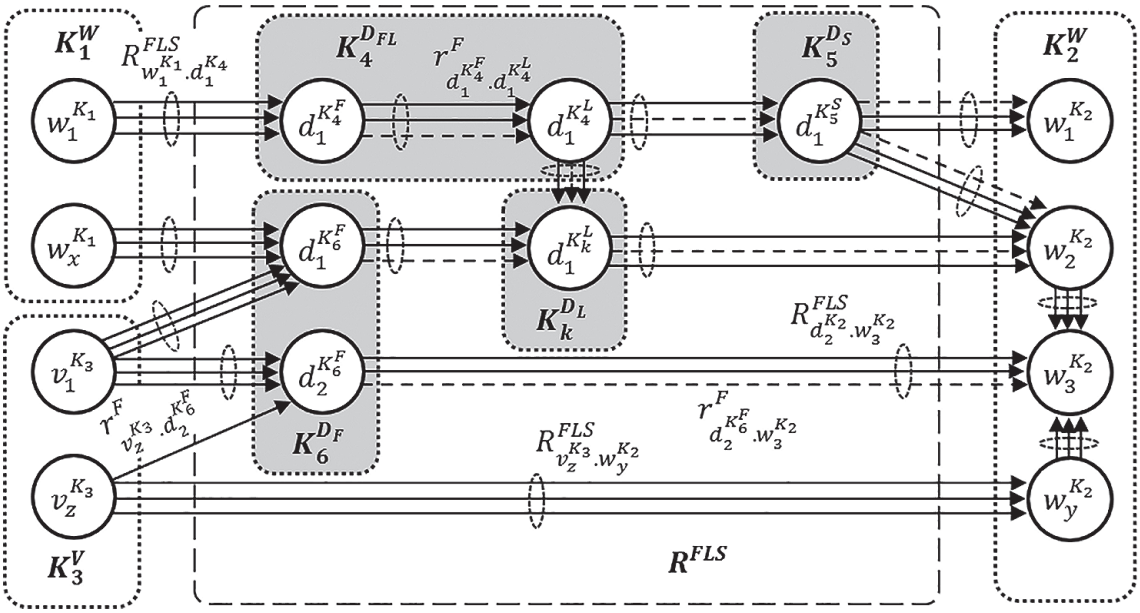

Рис. 1. Кластерная модель защиты информации

Декомпозиция дуг $R \longrightarrow R_M^{FLS}\{R^F \cup R^L \cup R^S\}$ в кластерной модели защиты расширяет понятие «смежности» вершин графа. Если все вершины и дуги составляют мультиграф $G^{FLS}(M_N,R_M^{FLS})$, то любые две его вершины $\{m_i,m_j\}$ являются смежными, только если в остовных FLS-подграфах между этими вершинами существует хотя бы одно подмножество кратных дуг вида $R_{i,j}^{FLS} = \{r_{i,j}^F,r_{i,j}^L,r_{i,j}^S\}$, которое называется полной FLS-дугой. Взаимодействие между любыми двумя модулями возможно, если обозначающие их вершины $\{m_i,m_j\}$ мультиграфа $G^{FLS}(M_N,R_M^{FLS})$ смежные. Путь $P_{i,j}^{FLS}$ между произвольной парой вершин $\{m_i,m_j\}$ в мультиграфе $G^{FLS}(M_N,R_M^{FLS})$ существует, если существуют пути между этими вершинами в FLS-подграфах смежности.

На рис. 1 полные дуги обозначены пунктирными овалами. Для примера показана неполная дуга вида $r^F_{v_z^{K_3}.d_2^{K_6^F}}$, которая указывает на наличие физического отношения, которое не позволяет реализовать информационное взаимодействие из-за отсутствия кратных дуг $r^L_{v_z^{K_3}.d_2^{K_6^F}}$ и $r^S_{v_z^{K_3}.d_2^{K_6^F}}$ в остовных L и S подграфах. Управляемые FLS средствами защиты кластерные ограничения показаны пунктирными дугами, которые появляются в составе полной дуги при реализации доступа соответственно на F, L или S уровне взаимодействия модулей. Таким образом, кластерная модель защиты представляет собой мультиграф, вершины которого соединяются кратными FLS-дугами, внутрикластерная связность и межкластерная разряженность максимальны. Возможны вырожденные варианты, когда внутрикластерная связность отсутствует и вершины становятся кластерами или когда все вершины являются элементами одного кластера. Некратные дуги включаются в модель для анализа «скрытых» угроз.

Анализ кластерной модели защиты

Цель анализа конструктивной защиты архитектуры DLTS – поиск траекторий информационного процесса, которые содержат полные и не полные дуги допускаемые топологией архитектуры, но не контролируемые средствами защиты, а также оценка минимального уровня эффективности защиты для траекторий информационного процесса. Неконтролируемые средствами защиты информационные взаимодействия между кластерами отображаются в модели полной дугой вида $R^{FLS}_{v_z^{K_3}.w_y^{K_2}}$ (рис. 1). При формальном анализе кластерной модели защиты проводится поиск полных FLS-дуг входящих в или выходящих из защищаемых кластеров, но не инцидентных вершинам множества средств защиты D^{FLS} из кластеров $K^F \cup K^L \cup K^S \subseteq K^D$. При анализе «скрытых» угроз дополнительно проводится поиск не полных F, L и S дуг.

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

В ходе анализа проводится поиск состояний системы, нарушающих политику доступа, и оценка

непрерывности уровня защиты для каждого пути поиск вершин с весами ниже установленного значения. При статическом анализе проверяется достижимость вершин мультиграфа G^{FLS}, что позволяет оценить безопасность конкретной топологии DLTS. Динамический анализ позволяет оценить безопасность состояний методом перебора траекторий информационного 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 вершин $B^{Д} = \|b_{ij}\|$ мультиграфа G^{FLS}, элементы которой заполняются по правилу

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

Критерием безопасности архитектуры является отсутствие пути P_{ij}^{FLS} между любыми произвольными вершинами из разных кластерных подмножеств K_K, который не содержит хотя бы одну вершину из множества D^{FLS}. Отсутствие пути проверяется сравнением значений каждой позиции кластерной матрицы $B^{К} = \|b_{ij}\|$ сформированной по правилам политики доступа и правилам конструктивной защиты (см. утверждения 1 и 2) с позицией в матрице достижимости $B^{Д} = \|b_{ij}\|$, которая формируется при анализе топологии.

Если при сравнении мощности множеств по теореме Кантора-Бернштейна мощность множества $|B^{К}|$ ненулевых элементов матрицы $B^{К} = \|b_{ij}\|$ равномощно или больше мощности множества $|B^{Д}|$ ненулевых элементов матрицы $B^{Д} = \|b_{ij}\|$, то формальные правила доступа выполняются и архитектура системы безопасна. Для национальных распределенных реестров и платформ может требоваться более высокий уровень защиты, когда любое взаимодействие проходит контроль доступа. В этом случае все полные FLS-дуги между любыми вершинами подмножеств K^W должны быть инциденты вершине из подмножеств K^D множества D^{FLS}. Все вершины становятся кластерами, реализуется политика с «нулевым доверием» и каждое взаимодействие проходит через контроль доступа. Полные дуги между вершинами одного кластера вида $R^{FLS}_{v_z^{K_3}, w_y^{K_2}}$ (рис. 1) запрещены, все дуги должны быть инцидентны вершинам, обозначающим средства защиты из множества D^{FLS}. Из этого следует определение конструктивно безопасной архитектуры информационной системы.

Утверждение 1. Если все внешние дуги кластеров K^W инциденты вершинам из кластеров K^D средств защиты множества D^{FLS}, то конструктивно архитектура системы безопасна.

Для критических систем актуален более сильный критерий безопасности, который соответствует политике «нулевого доверия», учитывает внутренние угрозы и угрозы распределенной топологии.

Утверждение 2. Если все дуги кластеров K^W инциденты вершинам из кластеров K^D средств защиты множества D^{FLS}, то конструктивно архитектура системы безопасна.

Доказательство безопасности архитектуры DLTS при динамическом анализе обеспечивается управляемым перебором состояний в ходе построения FLS-мультиграфа и оценкой на каждом шаге безопасности порожденного состояния. Оценка безопасности состояния заключается в установлении всех возможных отношений между модулями, которые изменялись на последнем шаге, и проверке их принадлежности подмножеству разрешенных кластерных 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.

Кластерная модель позволяет использовать системные критерии для оценки конструктивной защиты архитектуры DLTS. На рис. 2 пример а) демонстрирует неконтролируемое взаимодействие $R^{FLS}_{v,w}$ модулей v_z и w_y из кластеров K_3 и K_2, что оценивается как угроза безопасности. В примере б) показано контролируемое средством защиты физического уровня d^F из подмножества D^{FLS} взаимодействие модулей v_z и w_y из кластеров K_3 и K_2. В примере в) показано взаимодействие модулей v_z и w_y из кластеров K_3 и K_2 контролируемое двумя средствами защиты синтаксического d^L и семантического d^S уровней. Пример г) демонстрирует контролируемое взаимодействие модулей w_y и w_{y^*} из одного кластера K_2 через средство защиты синтаксического уровня d^L. Контроль взаимодействия внутри кластера актуален для критических систем, например, для национальных распределенных блокчейн систем и платформ.

В общем случае при оценке конструктивной защиты архитектуры кластерная модель защиты позволяет учитывать топологию информационного взаимодействия на одном, двух или трех FLS-уровнях, а также эффективность системы защиты на основе сравнения весовых коэффициентов средств защиты.

Для учета эффективности средств защиты при анализе безопасности архитектуры вершинам графа из множества D^{FLS} присваиваются нормированные весовые коэффициенты, характеризующие надежность защиты на основе внешних оценок

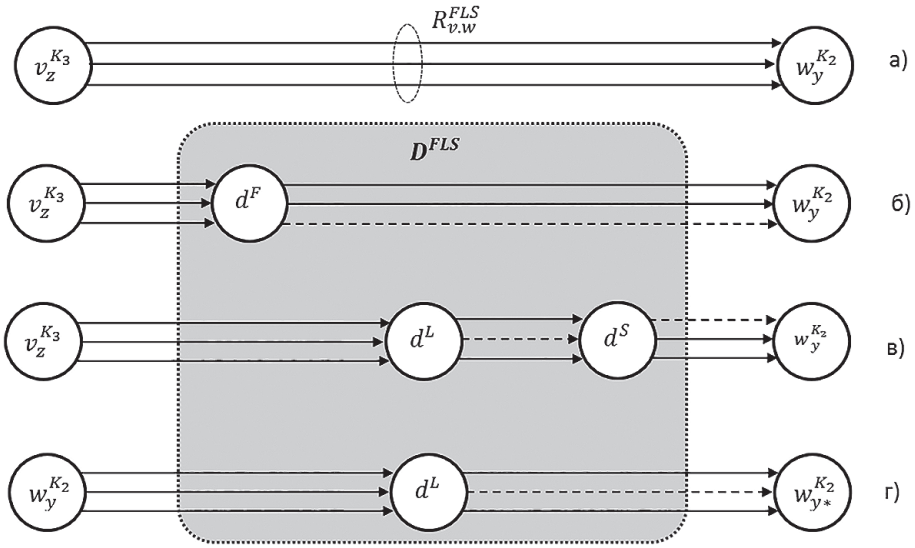

Рис. 2. Конструктивная защита архитектуры

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

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

Непрерывность уровня защиты оценивается сравнением значений весовых коэффициентов вершин графа для каждого пути относительно заданного нормированного значения. Например, для криптографических функций шифрования и аутентификации, которые являются основой конструктивной защиты DLTS, задается оценка стойкости криптографии к квантовой угрозе, связанной с появлением эффективных «квантовых» алгоритмов решения сложных вычислительных задач, позволяющих взломать асимметричную криптографию, и риском достижения «квантового превосходства» в скорости вычислений. Значение веса у вершины ниже заданного уровня указывает на угрозу безопасности.

Выводы

Кластерная модель защиты с полным перекрытием является инструментом анализа безопасности архитектуры DLTS со сложной архитектурой и политикой разграничения доступа. Модель позволяет оценивать безопасность архитектуры относительно декларируемой политики доступа, системных правил конструктивной защиты и оценок надежности средств защиты. Оценка конструктивной защиты на основе кластерной модели защиты позволяет принимать обоснованные решения при анализе и синтезе безопасной архитектуры DLTS. Криптографическая защита является основой конструктивной защиты DLT, для которой актуальна квантовая угроза. Кластерная модель защиты позволяет учитывать риск квантовой угрозы для DLTS при оценке эффективности средств защиты на основе внешних оценок стойкости криптографических алгоритмов [4–9].

Для проведения динамического анализа архитектуры с формальным доказательством ее безопасности кластерная модель защиты позволяет редуцировать граф состояний исследуемой системы за счет объектно-ориентированной декомпозиции системы на типовые функциональные модули методами теории модульно-кластерных сетей, что позволяет автоматизировать поиск опасных состояний без потери достоверности модели. Эвристики значительно сокращают размерность пространства поиска состояний. В реальных системах значительная часть (от 47 до 89 %) информационных объектов имеют однотипную функциональность и политику доступа, могут быть представлены в виде классов объектно-ориентированной модели. Эксперименты по моделированию показали возможность сокращения размерности порождающего графа состояний системы на 73 %, например, в случае «классической» архитектуры DLT, где все пользователи являются недоверенными субъектами и для них декларируется одинаковая политика доступа. Нижняя оценка мощности (3) определяется выбором только наилучших вариантов подграфов второго порядка в каждой частной резольвенте, что соответствует решению проблемы методами динамического программирования

$$N\_min = L \cdot R \cdot M^2 \cdot \frac{n^2}{t}, \quad (3)$$

где R - множество t-арных эвристических отношений над элементами порождающего графа G; M – мощность множества R; P - вектор параметров вершин графа с длиной L, равной количеству независимых переменных; n – мощность множества вершин порождающего графа G.

Таким образом:

1. Кластерная модель защиты информации с полным перекрытием, построенная с применением методов теории МК-сетей, позволяет проводить формальный анализ и оценивать безопасность архитектуры систем распределенного реестра.
2. Конструктивная безопасность архитектуры систем распределенного реестра может оцениваться по отсутствию внешних дуг у защищаемых кластеров, которые не инцидентны вершинам из кластера средств защиты информации. Для критических приложений условие безопасности может заключаться в оценке инцидентности всех дуг вершинам, обозначающим средства защиты информации.
3. Оценка эффективности средств защиты информации может заключаться в сравнении весов вершин, рассчитанных по внешним методикам. В частности, для систем распределенного реестра необходимо определять стойкость криптографических алгоритмов, используемых при аутентификации и шифровании.
4. Кластерную модель защиты информации можно использовать для моделирования угроз безопасности информации с учетом особенностей политики доступа, архитектуры и 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. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1(47). С. 2–9. DOI: 10.21681/2311-3456-2022-1-2-9.
2. Topical issues in the implementation of secure software development processes Markov A. S., Varenitca V. V., Arustamyan S. S. В сборнике: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. 2023. С. 48–53.
3. 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.
4. 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.
5. 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.
6. Petrenko A. S. Applied Quantum Cryptanalysis (scientific monograph). River Publishers. (2023). 256 p. ISBN 9788770227933. DOI: 10.1201/9781003392873.
7. 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.
8. 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.
9. Li L., Lu X., Wang K. Hash-based signature revisited. (2022). Cybersecurity. V. 5. Article No. 13. DOI:10.1186/s42400-022-00117-w.
10. 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.

CLUSTER MODEL OF DISTRIBUTED REGISTRY PROTECTION

Sundeev Pavel[3]

Keywords: *modular cluster network, quantum threat.*

The purpose of the study: *is to develop an information protection model for analyzing the constructive security of the distributed registry architecture, taking into account the access control policy and the quantum threat.*

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

Research result: *an extended information protection model with full overlap for distributed registry systems has been developed, taking into account the influence of the quantum threat, which allows evaluating constructive protection and conducting formal static or dynamic security analysis of the architecture.*

3 Pavel Sundeev, Dr.Sc. (Technical), Chief researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory Sirius University of Science and Technology. E-mail: sundeev.pv@talantiuspeh.ru

Scientific novelty: *based on the methods of the theory of modular cluster networks, an extended information protection model with full overlap has been developed to analyze the constructive security of a distributed registry due to the cluster decomposition of architecture and information interactions, taking into account the effectiveness of information security tools. The system criteria for evaluating constructive protection are shown.*

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. Markov A. S. Cybersecurity and Information Security as Nomenclature Bifurcation Scientific Specialties. (2022). Voprosy Kiberbezopasnosti [Cybersecurity issue]. № 1(47). P. 2–9 (Russian Text).
2. Topical issues in the implementation of secure software development processes Markov A. S., Varenitca V. V., Arustamyan S. S. In the collection: Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. (2023). IPSQDA-2023. P. 48–53.
3. 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]. № 3(67), c. 63–71. DOI: 10.21681/2311-3456-2025-3-63-71 (Russian Text).
4. Balyabin A. A., Petrenko S. A. Model of a blockchain platform with cyber-immunity under quantum attacks. (2025). Voprosy Kiberbezopasnosti [Cybersecurity issue]. № 3(67). P. 72–82. DOI: 10.21681/2311-3456-2025-3-72-82 (Russian Text).
5. Petrenko A. S., Petrenko S. A. Basic Algorithms Quantum Cryptanalysis. Voprosy Kiberbezopasnosti [Cybersecurity issue]. (2023). no. 1(53), pp. 100–115. DOI: 10.21681/2311-3456-2023-1-100-115 (Russian Text).
6. Petrenko A. S. Applied Quantum Cryptanalysis (scientific monograph). River Publishers. (2023). 256 p. ISBN 9788770227933. DOI: 10.1201/9781003392873.
7. 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.
8. 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.
9. Li L., Lu X., Wang K. Hash-based signature revisited. (2022). Cybersecurity. V. 5. Article no. 13. DOI:10.1186/s42400-022-00117-w.
10. Sundeev P. V. Functional stability of a distributed registry in the context of the emergence of a new quantum threat. (2025). Cybersecurity issue. № 3(67). P. 83–89. DOI: 10.21681/2311-3456-2025-3-83-89 (Russian Text).