МЕТОД ОЦЕНКИ ВЫПОЛНЕНИЯ НОРМАТИВНЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ

Сундеев П.В.[1]

Ключевые слова: *политика доступа, модель доступа, кластерная модель защиты, конструктивная защита.*

Аннотация

Цель: *разработать метод формальной оценки выполнения нормативных требований к защите информации в национальных распределенных реестрах и иных критических информационных системах.*

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

Результаты исследования: *разработан метод оценки выполнения нормативных требований к защите информации с формальным доказательством реализации политики доступа и мер защиты средствами конструктивной защиты архитектуры.*

Научная новизна: *научная новизна заключается в применении оригинального метода модульно-кластерного анализа защиты информационной архитектуры для формальной оценки выполнения нормативных требований к защите информации с использованием кластерной модели защиты информации с полным перекрытием. Достоверность оценки достигается построением модели защиты, точность которой обеспечивается формальным описанием политики доступа кластерами мультиграфа информационной системы и декомпозицией информационных связей на уровни взаимодействия, через которые реализуются функции защиты информации, а также формальным анализом безопасности состояний системы в машине логического вывода. Строгость доказательства безопасности архитектуры соответствует строгости математического аппарата логического вывода.*

Практическая значимость: *результаты исследований могут быть использованы для разработки стандартов формальной оценки выполнения нормативных требований к защите информации, анализа и разработки политик управления доступом для распределенных реестров и иных критических информационных систем с доказанным уровнем конструктивной защиты архитектуры, использованием формальных методов оценки выполнения нормативных требований в правоприменительной практике.*

DOI: 10.24412/1994-1404-2025-4-4-15

Введение

Наличие нормативных требований к защите информации предполагает проверку реализации установленных для информационной системы мер защиты. Для некоторых категорий информации и информационных систем установлена уголовная или административная ответственность, например, по статье 274.1 УК РФ за нарушение требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры или по статье 13.11 КоАП РФ за нарушение требований к защите персональных данных. С целью минимизации регуляторных рисков выполнение установленных мер защиты контролируется оператором информационной системы и уполномоченным органом при проведении государственного контроля. Доказательства выполнения нормативных требований к защите информации могут быть запрошены для принятия судебных решений. Проверка реализации организационных и технических мер защиты в некритичной информационной системе или в случае простой политики доступа может проводиться экспертными методами и тестированием функционала защиты. В случае критичности системы или на-

[1] ***Сундеев Павел Викторович,*** *доктор технических наук, главный инженер-исследователь, Научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: 0009-0005-8442-8921.*

E-mail: sundeev.pv@talantiuspeh.ru

личия сложной структуры информационных потоков с разными категориями информации и субъектов информационных отношений для проверки выполнения технических мер защиты целесообразно использовать формальный анализ защиты с верификацией выполнения политики доступа и реализации конструктивной защиты информации.

Оценку рисков, связанных с информационным взаимодействием, должен проводить собственник информации — юридическое или физическое лицо. Однако, законодательством РФ не предусмотрено понятие «собственник информации» в буквальной трактовке. Имеется понятие «обладатель информации», который может не быть собственником, например, субъектом персональных данных, но иметь законные основания на ее использование и защиту. Используемая правовая конструкция ограничивает право собственника на управление доступом и защиту информации. Например, юридическое лицо не может воспрепятствовать передаче своей коммерческой тайны, а физическое лицо — своих персональных данных, если законом предусмотрена передача иному лицу. «Собственник информации» может установить политику доступа и применять меры защиты информации, только если они не противоречат законодательству. Например, существуют ограничения на использование средств криптографической защиты информации для физических лиц или иностранных средств защиты информации на значимых объектах критической информационной инфраструктуры. При этом преобладающая часть информации относится к категории ограниченного доступа, защита которой регулируется законодательством Российской Федерации. В указанных случаях оценка рисков, связанных с информационным взаимодействием, определение политики доступа и выбор мер защиты проводятся обладателем информации на основании нормативных документов, в которых уже установлены категории информации с учетом ее ценности, ограничения по доступу для разных категорий субъектов к разным категориям объектов, определены организационные и технические меры защиты информации для категорий значимости объектов, классов или уровней защищенности информации или систем.

Технические меры защиты обеспечивают выполнение политики доступа за счет использования средств защиты, которые реализуют функции управления доступом и компенсируют конструктивные недостатки архитектуры с целью блокирования несанкционированного доступа в обход системы управления доступом. Существуют формальные методы оценки эффективности средств защиты информации, модели разграничения доступа, методы построения и анализа объектно-ориентированных моделей защиты информационных систем или моделей основанных на сетях Петри для динамического анализа процесса защиты, и другие [1-4]. Они позволяют анализировать отдельные свойства защиты, однако ограничены в формальном представлении всех специфических свойств существенных для проверки выполнения требований к защите информации, которые должны быть одновременно представлены в одной модели и оцениваться в комплексе.

В статье предложен метод оценки выполнения нормативных требований к защите информации с формальным доказательством реализации политики доступа выделенными и встроенными в архитектуру средствами конструктивной защиты. Достоверность метода оценки достигается использованием кластерной модели защиты, точность которой обеспечивается представлением политики доступа кластерами мультиграфа модели защиты информационной системы и декомпозицией информационных связей на уровни взаимодействия, через которые реализуются функции защиты информации, учетом в модели информационного окружения системы, а также формальным анализом состояний системы в машине логического вывода. Строгость доказательства безопасности архитектуры соответствует строгости математического аппарата логического вывода.

Концепция оценки выполнения нормативных требований к защите

В информационной системе реализуется политика доступа, в которой установлены правила, права и уровни доступа к информации для разных категорий субъектов и объектов (далее — векторы доступа), что позволяет управлять информационными потоками при взаимодействии внутри системы и с внешними субъектами и объектами. Политика доступа может быть простой, например, когда все субъекты одной системы имеют одинаковые права доступа ко всем объектам. В этом случае политикой будут ограничены только внешние взаимодействия. Однако, как правило, информационная система имеет объекты с разной оценкой рисков, к которым необходимо разграничивать доступ внешних и внутренних субъектов, назначать им разные полномочия по обработке информации, и исключить доступ для субъектов, которые их не имеют. В общем случае политика управления доступом устанавливает векторы доступа между идентифицированными субъектами и объектами, которые обозначают физические и логические информационные сущности, содержащие информацию или запрашивающие к ней доступ. Политика доступа разделяет субъекты и объекты с разным уровнем доступа на группы. Используемые в практике политики доступа строятся на основе формальных моделей разграничения доступа, имеющих теоретическое обоснование, например, мандатной, дискреционной, ролевой [2,3]. Архитектура может иметь недостатки (уязвимости), через которые возможны информацион-

[2] ГОСТ Р 59453.1—2021 Защита информации. Формальная модель управления доступом. Часть 1. Общие положения.

[3] ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом.

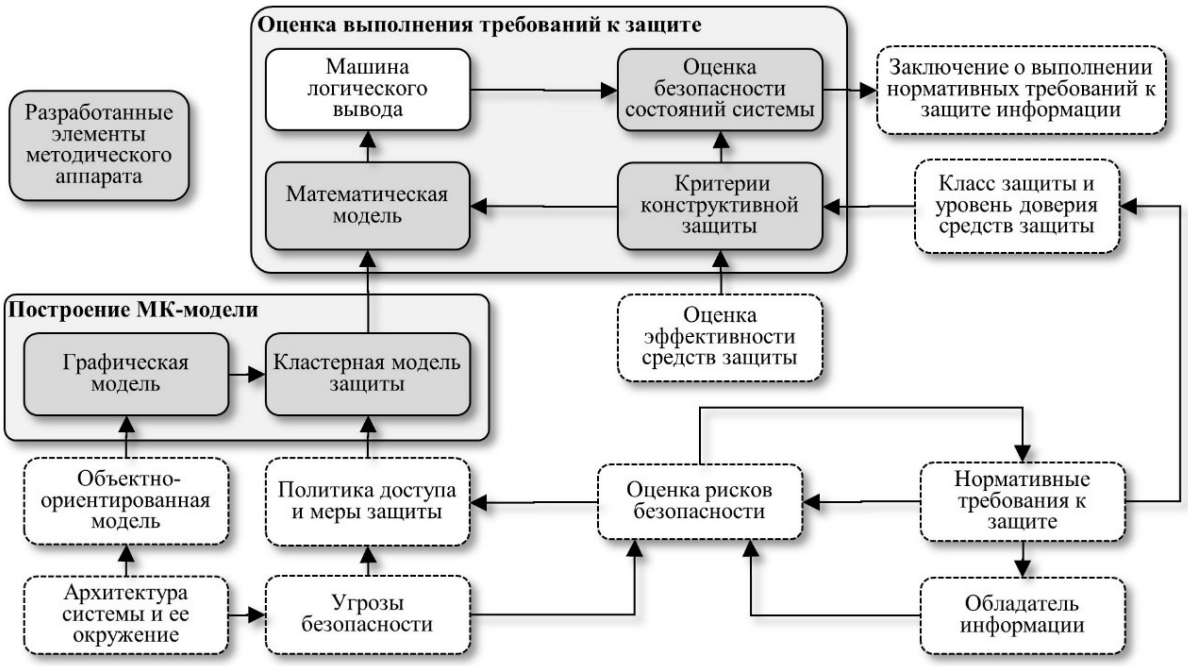

Рис. 1. Структура методического аппарата оценки выполнения нормативных требований к защите информации

ные связи, не санкционированные политикой доступа. Необходимо исключить несанкционированное взаимодействие субъектов и объектов информационной системы с субъектами и объектами информационного окружения, не имеющими прав доступа. Топология возможных информационных связей определяется архитектурой системы и конструктивными средствами защиты, которые используются для управления информационными потоками в соответствии с политикой доступа.

С целью обеспечения точности модели защиты и достоверности оценки в общем случае необходимо учитывать в политике доступа и проверять возможность установления информационных связей между идентифицированными субъектами и объектами системы, а также связей с информационным окружением, субъекты и объекты которого не идентифицированы. Для компенсации недостатков архитектуры и управления доступом используются средства защиты информации. В случае наличия нормативных требований необходимо оценивать наличие, класс защиты и уровень доверия средств защиты информации.

Концепция метода формальной оценки выполнения нормативных требований к защите информации основывается на использовании расширенной модели защиты информации с полным перекрытием[4], в которой средства защиты контролируют все информационные связи и разрешают только связи допустимые политикой доступа [5]. Для оценки выполнения нормативных требований на формальной модели защиты проверяется гипотеза об отсутствии опасных состояний системы, если топология информационных потоков не нарушает декларируемую политику доступа. Точность расширенной модели защиты информации обеспечивается представлением групповой политики доступа кластерами мультиграфа информационной системы и декомпозицией информационных связей на уровни взаимодействия, через которые реализуются меры защиты информации, формальным поиском опасных состояний системы в машине логического вывода определяемых наличием или отсутствием помеченных вершин и дуг мультиграфа, которые определяются политикой доступа и критериями конструктивной защиты, а также оценкой наличия средств защиты установленного класса защиты и уровня доверия. Достоверность оценки зависит от полноты описания исходной информационной модели системы. Строгость доказательства безопасности архитектуры соответствует строгости математического аппарата логического вывода.

Методический аппарат оценки выполнения нормативных требований

Для оценки выполнения нормативных требований к защите информации используются существующие и новые методы и модели (рис. 1). Графическая модель информационной системы формируется на основе объектно-ориентированной модели системы и ее окружения. Политика управления доступом и меры защиты информации, реализующие эту политику, установлены нормативными документами и определяются обладателем информации с учетом категорий обрабатываемой информации, угроз безопасности и особенностей архитектуры. Требования к составу, классу защиты

[4] Хоффман Л.Дж. Современные методы защиты информации // Пер. с англ. М.: Советское радио, 1980. 264 с.

и уровню доверия средств защиты информации также устанавливаются нормативными документами. Разработанными элементами методического аппарата оценки выполнения нормативных требований к защите являются метод построения модульно-кластерной модели (МК-модели) информационной системы и метод оценки выполнения нормативных требований к защите.

Метод построения МК-модели заключается в формировании кластерной модели защиты информации на основе графической модели информационной архитектуры, в которой учтены декларируемая политика доступа и средства защиты информации. Исходной для формирования графической модели является объектно-ориентированная модель архитектуры системы и ее информационного окружения, которая строится по известной методике объектно-ориентированного анализа сложных систем с применением функциональной декомпозиции объектов на физические и логические модули в соответствии с методами теории модульно-кластерных сетей [6, 7]. Объектно-ориентированная модель может быть представлена в нотации UML с использованием программных CASE-средств для объектно-ориентированного моделирования, например, Rational Rose.

Кластерная модель защиты является расширением графической модели системы за счет определения в ней политики доступа, которая обеспечивается архитектурой и средствами защиты информации. Графическая МК-модель системы — это мультиграф, вершины которого обозначают модули объектно-ориентированной модели, а дуги — возможные физические (*F*), синтаксические (*L*) и семантические (*S*) отношения между ними. Кластерная модель защиты информации — это *FLS*-мультиграф информационный системы, в котором имеются вершины, обозначающие средства (функции) защиты информации, и определены кластеры объединяющие вершины с одинаковым вектором доступа в соответствии с политикой доступа. Функционал средств защиты задается в модели *FLS*-интерфейсами модулей, а класс защиты и уровень доверия — весами вершин (дуг) мультиграфа, обозначающих средства защиты, если они определены в нормативных и технических документах, или иными методами оценки эффективности средств защиты. Например, для средств криптографической защиты информации может быть задана стойкость криптографического алгоритма к квантовой угрозе.

С целью формализации и автоматизации процесса анализа защиты в случае сложной архитектуры или критичности системы из графической модели может быть сформирована математическая модель системы в терминах логики предикатов первого порядка, которая позволяет проводить итеративный поиск опасных состояний системы с доказательством результатов анализа в машине логического вывода. Оценка выполнения нормативных требований к защите информации сводится к поиску и сравнительному анализу структуры вершин, дуг и значений их весов. Статические или динамические состояния информационной модели системы сравниваются с кластерной структурой, которая задается политикой доступа и критериями конструктивной защиты. Веса вершин (дуг), обозначающих средства (функции) защиты, сравниваются со значениями, установленными нормативными документами, или с расчетными значениями.

Модель защиты для оценки нормативных требований

Применительно к решаемой задаче модель защиты для оценки нормативных требований — это статическая или динамическая модель информационной системы, в которой определены политика доступа с уникальными субъектами и объектами доступа или их классами, топология возможных информационных связей между ними с правилами переходов состояний для моделирования динамики информационного процесса, потенциальные источники внешних и внутренних угроз, средства защиты информации, реализующие управление доступом и компенсирующие недостатки архитектуры.

Модель защиты для оценки требований формируется из модели информационной системы *X* и ее окружения *Y*, которая с целью формального анализа представлена в виде объектно-ориентированной модели системы *Z* в терминах теории МК-сетей [5-7]. Проблема точности формальной модели решается определением внешних и внутренних субъектов и объектов доступа в качестве функциональных физических и логических информационных модулей, разнесением всех субъектов и объектов по кластерам в соответствии с политикой доступа, применением для оценки безопасности архитектуры критериев конструктивной защиты, декомпозицией информационных взаимодействий на *FLS*-отношения с учетом функциональных свойств модулей существенных для защиты информации на основе методов теории модульно-кластерных сетей [6], что позволяет оценивать безопасность топологии информационных потоков допускаемых архитектурой и эффективность защиты относительно декларируемой политики доступа. На (рис. 2) показана концептуальная модель взаимодействия системы *X* и ее окружения (системы) *Y* с декомпозиций информационных связей на *FLS*-отношения, обозначены классы мер защиты, которые могут быть реализованы на *F*, *L* или *S* уровне информационного взаимодействия.

Если объектно-ориентированную информационную модель системы *Z* представить в виде графа МК-сети, то элементы множества M_N 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 модулями. При этом множество дуг R_M^{FLS} состоит из подмножеств внутренних дуг инцидентных вершинам из одного кластера R^K и подмножества

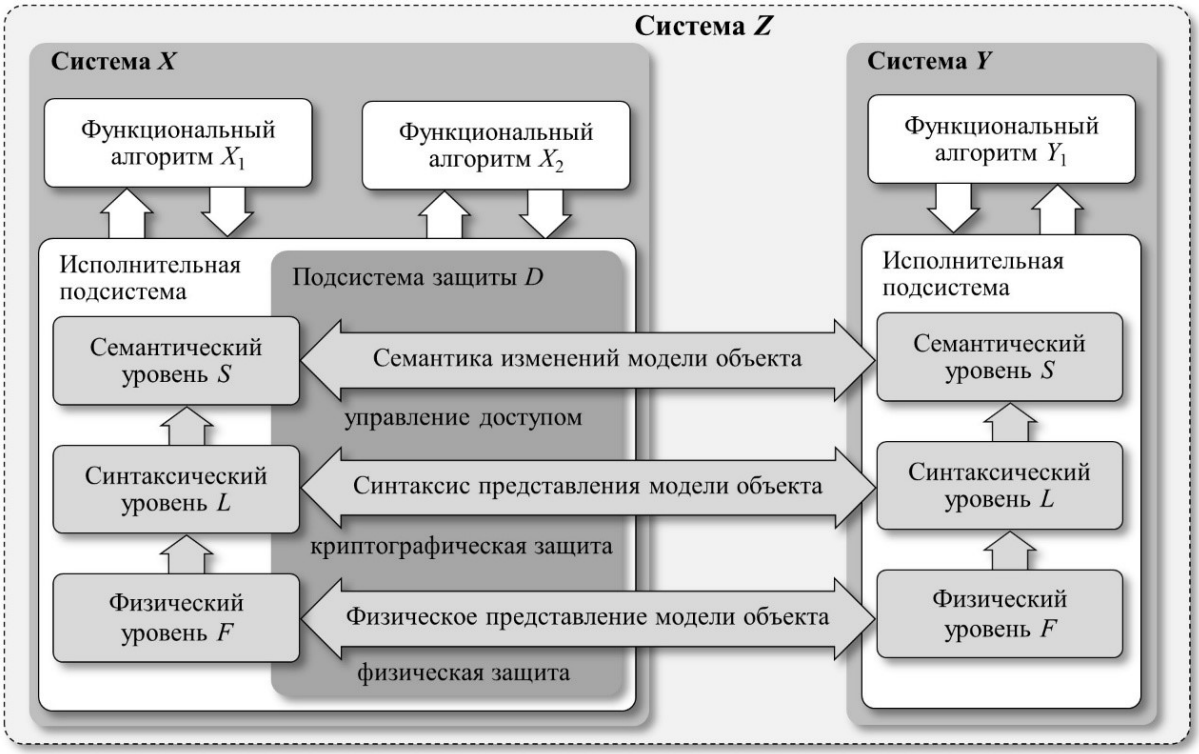

Рис. 2. FLS-модель информационного взаимодействия системы X и ее окружения Y

внешних дуг инцидентных вершинам из разных кластеров $R^{\bar{K}}$, таких что $R^K \cap R^{\bar{K}} = \emptyset$.

Определение. Модульно-кластерная сеть — это *FLS*-мультиграф $G^{FLS}(M_N, R_M^{FLS})$, вершинами которого являются функционально-информационные модули $M_N = \{m_1, m, \ldots, m_N\}$, где *N* их число, дуги $R_M^{FLS} = \{R^F \cup R^L \cup R^S\}$, где $R^F = \{r_M^F\}$, $R^L = \{r_M^L\}$, $R^S = \{r_M^S\}$, определяются наличием у модулей *FLS*-интерфейсов, через которые потенциально могут быть установлены функционально-информационные отношения, кластеры K^Z объединяют вершины, которые могут быть смежными только в соответствии с политикой доступа, установленной для соответствующих модулей из M_N.

В мультиграфе G^{FLS} к множеству дуг R_M^{FLS} относятся только кратные дуги вида $\{r_{ij}^F \cup r_{ij}^L \cup r_{ij}^S\} \subseteq R_{ij}^{FLS}$, где $r_{ij}^F \neq 0, r_{ij}^L \neq 0, r_{ij}^S \neq 0$. Состав дуг мультиграфа определяется наличием парных исходящих и входящих интерфейсов модулей, обеспечивающих возможность реализации информационных примитивов через *FLS*-отношения, которые имеют иерархическую зависимость вида $r^F \to r^L \to r^S$. В динамической модели состав вершин и дуг мультиграфа может меняться при наличии условий для информационного взаимодействия модулей по правилу «если взаимодействие возможно, то оно реализуется».

Мультиграф $G^{FLS}(M_N, R_M^{FLS})$ состоит из *F*, *L* и *S* остовных подграфов, у которых вершины совпадают и соответствуют множеству $M_N = \{m_1, m, \ldots, m_N\}$, а инцидентные им дуги различаются и определяются соответственно подмножествами $R^F = \{r_f^F\}$, $R^L = \{r_l^L\}$, $R^S = \{r_s^S\}$, отражающими *FLS*-отношения между модулями.

Декомпозиция дуг $R_M \to R_M^{FLS} \supseteq \{R^F \cup R^L \cup R^S\}$ расширяет понятие «смежности» вершин мультиграфа $G^{FLS}(M_N, R_M^{FLS})$.

Правило 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.

Правило 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.

Правило 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 *FLS*-подграфах смежности.

Расширенное понятие «смежности» вершин мультиграфа позволяет формализовать анализ информационных связей между модулями с учетом наличия в архитектуре функций (средств) защиты информации на разных *FLS*-уровнях взаимодействия, которые должны быть формально представлены в модели защиты информации.

В кластерной модели защиты информации отмеченные вершины мультиграфа группируются в кластеры, которые определяются политикой доступа и конструктивной защитой.

Пусть заданы:

Z — система состоящая из множества элементов (модулей) $M_N = \{M_x^X, M_y^Y, M_d^D\}$;

X — подмножество множества *Z*, состоящее из элементов (модулей) M_x^X, обозначающих субъекты и объекты доступа;

Y — подмножество множества *Z*, состоящее из элементов (модулей) M_y^Y, обозначающих внешние по отношению к информационной системе *X* субъекты и объекты доступа;

D — подмножество множества *Z*, состоящее из элементов M_d^D, обозначающих конструктивные и дополнительные функции (средства) защиты, которые управляют доступом в системе *Z*, где $M_d^D = \{M_Z^D, M_X^D, M_Y^D\} = \{M^F, M^L, M^S\}$;

M_X^D — подмножество средств защиты системы *X*;

M_Y^D — подмножество средств защиты системы *Y*;

M_Z^D — подмножество средств защиты системы *Z*;

M^F — подмножество средств защиты физического уровня *F*;

M^L — подмножество средств защиты синтаксического уровня *L*;

M^S — подмножество средств защиты семантического уровня *S*;

K^Z — множество кластеров системы *Z*, $K^Z = \{K^X, K^Y, K^D\}$;

K^X — подмножество кластеров системы, включающих модули $M_x^X \subseteq X$;

K^Y — подмножество кластеров окружения, включающих внешние модули $M_y^Y \subseteq Y$;

K^D — подмножество кластеров защиты, включающих модули M_d^D;

R_M^{FLS} — множество информационных отношений между $M_N = \{M_x^X, M_y^Y, M_d^D\}$.

Элементы подмножеств *X*, *Y* и *D* распределены по кластерам в соответствии с политикой доступа, так что $K^Z = K^X \cup K^Y \cup K^D$ и $K_1 \cap K_2 \cap \ldots \cap K_k = \emptyset$, где (*k* — общее количество кластеров).

Критерием распределения вершин по кластерам является одинаковый для соответствующих модулей вектор доступа, который установлен политикой доступа и зафиксирован в эталонной кластерной *FLS*-матрице K^{FLS} — квадратной бинарной матрице, проиндексированной номерами вершин мультиграфа $G^{FLS}(M_N, R_M^{FLS})$. Логическое значение «1» в ячейках матрицы K^{FLS} проставляется только если между модулями разрешено информационное взаимодействие в соответствии с политикой доступа. Политика доступа устанавливается внешним процессом в соответствии с выбранной формальной моделью разграничения доступа, например, мандатной, дискреционной, ролевой, с учетом уровня риска взаимодействия, связанного с ценностью информации, разным уровнем доверия между элементами системы *X*, окружения *Y* и защиты *D*, и критериями конструктивной защиты. Во многих случаях политика доступа установлена нормативными документами, например, для персональных данных, государственных информационных ресурсов, объектов критической информационной инфраструктуры и т. д. Вектор доступа указывает на наличие разрешения и условия доступа субъекта или группы субъектов к объекту или группе объектов, то есть определяет возможные действия исполнительной подсистемы с объектом доступа на семантическом уровне отношений, например, для систем UNIX — «*r*» (чтение), «*w*» (запись), «*x*» (выполнение), или более общие для информационных систем разных типов — «*g*» (создание), «*m*» (модификация), «*d*» (уничтожение), «*c*» (копирование), «*x*» (выполнение), «*k*» (хранение), «*t*» (перевод) и т. п.

Все субъекты и объекты распределяются по кластерам K^Z в соответствии с политикой доступа. Для внешних субъектов и объектов или их классов из подмножества M_y^Y также должны быть установлены векторы доступа, например, «нулевой вектор» при запрете взаимодействия. Модули из подмножества M_y^Y определяются как внешние источники угроз, соответствующие вершины выделяются в отдельные кластеры K^Y. К одному кластеру могут относиться только субъекты и объекты с одинаковым уровнем доступа. Субъекты доступа из других кластеров рассматриваются как потенциальные источники угроз. В системах, которые предназначены для взаимодействия недоверенных субъектов в конкурентной среде, каждый пользователь может быть выделен в отдельный кластер. Наличие одинаковых векторов доступа для типовых субъектов и объектов позволяет редуцировать граф состояний системы и свести сложность задачи поиска опасных состояний к разрешимости за полиномиальное время.

Политика доступа должна разделять систему *Z* на множество кластеров $K^Z = \{K^X, K^Y, K^D\}$. Для вершин одного кластера установлен общий вектор доступа, то есть взаимодействие не ограничено. Для вершин разных кластеров установлены разные векторы доступа, то есть взаимодействие запрещено или ограничено условиями, но потенциально возможно. Возможна вложенность кластеров с иерархическими уровнями доступа. Если политика выполняется для всех произвольных пар вершин $\{m_i, m_i\}$ из разных кластеров, то есть отсутствуют пути P_{ij}^{FLS} между вершинами из разных кластеров *FLS*-мультиграфа, между которыми политикой доступа запрещено взаимодействие, то архитектура безопасна при условии эффективности средств защиты не ниже установленного значения. В оценке эффективности защиты может учитываться класс защиты и уровень доверия средства защиты информации в зависимости от принадлежности его к подмножеству M_Z^D, M_X^D или M_Y^D. Политика доступа должна предусматривать возможность взаимодействия с доверенными модулями подмножества M^D, обозначающими функции (средства) защиты информации, 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 *Z* определяется на множестве модулей $M_N = \{M_x^X, M_y^Y, M_d^D\}$ информационной системы *X* и ее окружения *Y*, множествах *FLS*-отношений $R_M^{FLS} = \{R^F, R^L, R^S\}$ и кластеров $K^Z = \{K^X, K^Y, K^D\}$

$$G_Z^{FLS}(M_N, R_M^{FLS}) \equiv \begin{cases} M_N = \{M_x^X, M_y^Y, M_d^D\} | \{M_x^X \cap M_y^Y \cap M_d^D\} = \emptyset; \\ R_M^{FLS} = \{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}; \\ K^Z = \{K^X, K^Y, K^D\} | \{K^X \cap K^Y \cap K^D\} = \emptyset; \end{cases} \quad (1)$$

где $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ — подмножества полных внутренних $\{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}\}$ и внешних $\{R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$ *FLS*-дуг кластеров $\{K^X, K^Y, K^D\}$.

Кластерная модель защиты сложной информационной системы является расширением модели защиты информации с полным перекрытием и имеет большой размер. В [5] представлен пример фрагмента кластерной модели защиты. Для оценки выполнения нормативных требований к защите информации в критических системах из модульно-кластерного *FLS*-мультиграфа графической модели защиты формируется математическая кластерная модель защиты информации, которая должна обеспечить итеративный поиск и оценку безопасности состояний системы в машине логического вывода.

Формальная постановка задачи оценки нормативных требований к защите

Целью оценки выполнения нормативных требований к защите является выявление некоторых свойств объекта анализа. Под объектом анализа здесь понимаются физические и логические функциональные модули, которые составляют информационную архитектуру системы и ее окружения, являются субъектами и объектами доступа, а под свойствами объекта анализа — функционально-информационные связи между ними, которые определяют возможные траектории информационного процесса и безопасность состояний системы в дискретные моменты времени. Безопасность состояния системы заключается в отсутствии связей, нарушающих декларируемую политику доступа. Дополнительной задачей является оценка соответствия средств защиты заданному классу защиты и уровню доверия, если средство защиты информации сертифицировано, или значению уровня защиты, рассчитанному по внешним методикам, если сертификация не является нормативным требованием.

Пусть конечное множество элементов $M_N = \{m_1, m_2, \dots, m_n\}$ (где N их число) составляют систему *Z*. Каждый элемент *m* обладает свойствами r_m^{FLS} из конечного множества свойств $R_M^{FLS} = \{R^F, R^L, R^S\} = \{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$, 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 *Z* 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 *Z*. 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 $\overline{\Psi}$ системы *Z*. 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)

$$P_r: \Psi \to \{\text{И}, \text{Л}\}. \quad (2)$$

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

$$\Psi = \Psi_r \cup \overline{\Psi}_r, \Psi_r \cap \overline{\Psi}_r = \emptyset. \quad (3)$$

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 $P_{r_1}(x), P_{r_2}(x), \dots$, то вычисление значения предиката $P_r(x)$ может быть проведено вычислением значения предикатов $P_{r_1}(x), P_{r_2}(x), \dots$ и затем определением истинности $P_r(x)$ путем приложения операции следования вида

$$F(P_{r_1}(x), P_{r_2}(x), \dots) \to P_r(x) \quad (4)$$

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 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 оценки выполнения нормативных требований к защите информации заключается в:

– формировании множества вершин $M_N = \{M_x^X, M_y^Y, M_d^D\}$;

– формировании множества дуг $R_M^{FLS} = \{R_{XY}^{FLS}; R_{YD}^{FLS}; R_{DX}^{FLS}; R_{\overline{XY}}^{FLS}; R_{\overline{YD}}^{FLS}; R_{\overline{DX}}^{FLS}\}$;

– формировании множества кластеров $K^Z = \{K^X, K^Y, K^D\}$;

– поиске элементов и доказательства полноты множества $\overline{\Psi}_r = \{\psi_1, \psi_2, \dots, \psi_e\}$, где $\overline{\Psi}_r = f\{M_N, R_M^{FLS}\}$, для оценки его пустоты ($\overline{\Psi}_r = \emptyset$);

– оценке соответствия нормированных весов элементов подмножества M_y^D, и в случае использования элементов подмножеств M_z^D и M_Y^D, установленному значению.

Метод анализа модели для оценки выполнения нормативных требований

Оценка выполнения нормативных требований к защите информации на МК-модели архитектуры информационной системы заключается в анализе соответствия топологии *FLS*-мультиграфа декларируемой политике доступа с учетом оценки соответствия эффективности средств защиты нормированному уровню, определяемому по внешним методикам. Например, для функций защиты синтаксического уровня *L* может использоваться оценка класса защиты и уровня доверия сертифицированного средства криптографической защиты информации или стойкости криптографии, которая является особенностью конструктивной защиты распределенных реестров[5], если сертификация не является обязательным требованием.

Начальное состояние модели определяется наличием у модулей типовых для исследуемого объекта исходящих и входящих *FLS*-интерфейсов, которые определяют их функционально-информационные свойства. Типовые исходящие и входящие *FLS*-интерфейсы двух модулей определяют наличие дуг в *F*, *L* или *S* остовных подграфах между представляющими их вершинами мультиграфа G^{FLS}. При наличии кратных дуг *F*, *L* или *S* в остовных подграфах между двумя вершинами в матрице смежности мультиграфа G^{FLS} фиксируется полная *FLS*-дуга. Свойства вершин и дуг мультиграфа G^{FLS} задаются подматрицами *FLS*-интерфейсов, которые полностью определяют функционально-структурные свойства модулей относительно других модулей архитектуры

$$F_{(ij)}^I = \left\| f_{(i^{\text{исх.}}, j^{\text{вх.}})}^I \right\|; L_{(ij)}^I = \left\| l_{(i^{\text{исх.}}, j^{\text{вх.}})}^I \right\|; \quad S_{(ij)}^I = \left\| s_{(i^{\text{исх.}}, j^{\text{вх.}})}^I \right\| \qquad (5)$$

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 ($i, j = 1, N$; *N* — максимальный номер вершины).

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 исходящих и входящих интерфейсов каждого модуля. Совпадение индексов отмеченных исходящих и входящих *FLS*-интерфейсов указывает на наличие дуги в соответствующем остовном *FLS*-подграфе. Наличие значений «1» в одинаковых позициях *FLS*-матриц указывает на то, что вершины являются смежными в соответствии с правилом 1.

Оценка топологии проводится перемножением значений в позициях бинарной квадратной *FLS*-матрицы достижимости вершин *FLS*-мультиграфа $G^{FLS}(M_N, R_M^{FLS})$ с эталонной бинарной квадратной кластерной *FLS*-матрицей, которая содержит сведения о разрешенных политикой доступа и критериями конструктивной защиты полных *FLS*-дугах. Логическое умножение бинарных матриц одного размера реализовано с помощью логических операций между элементами матриц. В отличие от традиционного матричного умножения, где элементы результирующей матрицы представляют собой скалярное произведение строк и столбцов, бинарное умножение использует логические операции, что позволяет получить матрицу, которая удовлетворяет условиям булевой логики.

В соответствии с правилом 3 в матрице достижимости вершин 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 *FLS*-подграфах смежности. *FLS*-матрица достижимости мультиграфа $G^{FLS}(M_N, R_M^{FLS})$ получается логическим пошаговым перемножением элементов остовных квадратных бинарных *F*, *L* и *S* матриц смежности. Результирующая матрица будет содержать сведения о наличии путей P_{ij}^{FLS} между всеми вершинами.

Матрица смежности A^{FLS} вершин мультиграфа G^{FLS} формируется последовательным логическим перемножением значений в ячейках *F*, *L* и *S* подматриц смежности A^F, A^L и A^S в одинаковых позициях. Поэтому в матрице смежности вершин A^{FLS} мультиграфа G^{FLS} значение «1» имеется только если значение «1» имеется в этой же позиции в каждой из *F*, *L* и *S* подматриц смежности вершин, то есть имеется полная *FLS*-дуга в мультиграфе G^{FLS}.

Матрица смежности $\mathrm{A}^{FLS} = (a_{ij})$ мультиграфа $G^{FLS}(M_N, R_M^{FLS})$, где $a_{ij} = 1 \Leftrightarrow (i,j) \in \mathrm{A}^{FLS}$, содержит информацию о всех путях длины 1 (дугах).

Для поиска путей длины 2 находится композиция отношения A^{FLS} с самим собой

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

$$A^{FLS^2} = \left(a_{ij}^2\right)_{n\times n} = \left(\sum_k a_{ik}a_{ki}\right) = \left(\left(a_{i1} \wedge a_{1j}\right) \vee \ldots \vee \left(a_{in} \wedge a_{nj}\right)\right), \quad (6)$$

где ∨ — конъюнкция и ∧ — дизъюнкция.

После нахождения матриц A^{FLS^K} для всех $k, 1 \le k \le n-1$ будут иметься сведения о всех путях длины от 1 до *n*-1. Квадратным бинарным *FLS*-матрицам смежности A^F, A^L и A^S соответствует матрица достижимости R^{FLS}

$$R^{FLS}(G) = E \vee A^{FLS} \vee A^{FLS^2} \vee \ldots \vee A^{FLS^{n-1}} = \left(a_{ij}^*\right)_{n\times n} = \left(a_{ij} \vee a_{ij}^2 \vee \ldots \vee a_{ij}^{n-1}\right) \quad (7)$$

где E — единичная матрица.

Результаты проверки достижимости модулей отражаются в квадратной матрице достижимости вершин $R^{FLS}(G)$ графа G^{FLS}, элементы которой заполняются по правилу

$$a_{ij} = \begin{cases} 1, \text{если из вершины } i \text{ к вершине } j \text{ имеется путь } P_{ij}^{FLS}; \\ 0, \text{если из вершины } i \text{ к вершине } j \text{ путь } P_{ij}^{FLS} \text{ отсутствует.} \end{cases} \quad (8)$$

Формальным критерием безопасности архитектуры является отсутствие пути P_{ij}^{FLS} между любыми произвольными вершинами из разных кластеров, который нарушает политику доступа, то есть наличие пути не предусмотрено эталонной кластерной матрицей. Условие проверяется сравнением значений каждой позиции эталонной кластерной матрицы $K(G) = [a_{ij}]$ сформированной по правилам политики доступа с той же позицией в матрице достижимости $R(G) = [a_{ij}]$, значения в ячейках которой формируются в результате эксперимента. Применима теорема Кантора-Бернштейна. Если множество ненулевых элементов матрицы $K(G) = [a_{ij}]$ равномощно или больше мощности множества ненулевых элементов матрицы $R(G) = [a_{ij}]$, то есть $|K(G)| \ge |R(G)|$, то в мультиграфе G^{FLS} отсутствуют пути P_{ij}^{FLS}, приводящие систему *Z* в опасные состояния, формальные правила политики доступа выполняются и архитектура системы безопасна.

Таким образом, формально доказательство выполнения нормативных требований к защите информации в системе может проводиться на основе проверки гипотез об инцидентности дуг вершинам из других кластеров.

Статический анализ проводится на мультиграфе G^{FLS} проверкой гипотез о достижимости модулей при установленных кластерных ограничениях, которые определены политикой доступа, что позволяет оценить безопасность исходного состояния системы *Z*. Этого достаточно для формальной оценки выполнения нормативных требований к защите информации для класса или уровня защищенности системы с установленными мерами защиты информации. Вывод о выполнении нормативного требования делается на основании наличия вершин, имеющих определенный функционал защиты, и замыкании на них путей между вершинами, которые проходят через помеченные вершины. Могут быть заданы последовательности вершин, через которые должны проходить траектории информационного процесса. Например, в большинстве случаев входящая дуга должна быть инцидентна вершине, которая обозначает средство аутентификации и, затем, должна быть дуга к вершине, обозначающей средство авторизации.

Оценка выполнения требований к используемым средствам защиты информации проводится сравнением значений весовых коэффициентов вершин графа из подмножества M_X^D средств защиты системы *X*.

$$M_X^D = \left|m_1^{(g)}, m_2^{(g)}, \ldots, m_n^{(g)}\right|. \quad (9)$$

Каждой вершине приписывается вес $m_n^{(g)}$, где *g* — функция веса, которая может обозначить класс защиты и уровень доверия для сертифицированных средств защиты информации или нормированную оценку эффективности средства защиты, рассчитанную по внешней методике для несертифицированных средств защиты. Например, в технологии распределенного реестра реализована конструктивная защита на основе криптографии и децентрализации информационного взаимодействия [8]. Поэтому для криптографических функций шифрования, аутентификации, хеширования, консенсуса, электронной подписи, которые являются основой конструктивной защиты DLT, может быть задана оценка стойкости криптографии. В случае «квантовой угрозы», связанной с появлением промышленных квантовых компьютеров и эффективных квантовых алгоритмов решения сложных вычислительных задач, позволяющих скомпрометировать асимметричную криптографию или не идеальную симметричную криптографию, например, алгоритмы Шора и Гровера [9–11], оценка стойкости должна корректироваться.

В случае использования внешних средств защиты информации, например, арендованных, необходимо также оценивать вершины из подмножества M_Z^D средств защиты системы *Z* и, возможно, из подмножества M_Y^D окружения *Y*.

Значение веса у одной или нескольких вершин ниже заданного класса, уровня или установленного значения указывает на невыполнение нормативного требования.

В критических системах может проводиться оценка эффективности установленных нормативных требований к защите информации с использованием динамического анализа, который позволяет оценить безопасность состояний системы для всех траекторий информационного процесса при изменении состава вершин и дуг мультиграфа G^{FLS} в результате применения решающих правил управляемого логического

вывода, реализующих процедуры обработки и защиты информации, которые могут быть дополнены специфическим функционалом конкретной технологии. 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 парных исходящих и входящих *FLS*-интерфейсов модулей.

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 эталонной кластерной *FLS*-модели), то состояние безопасное. Соответственно, если отношения запрещены (отсутствуют в эталонной кластерной *FLS*-модели), то состояние опасное. Строгость доказательства соответствует строгости математического аппарата логического вывода.

В методе анализа МК-сети мультиграф описывается предложениями математической логики, к которым применяются процедуры логического вывода, обеспечивающие поиск и анализ состояний модели. Доказательство безопасности архитектуры обеспечивается управляемым перебором состояний в ходе реализации последовательности процедур логического вывода при построении графа состояний системы и оцениванием на каждом шаге безопасности последнего порожденного состояния (рис. 3).

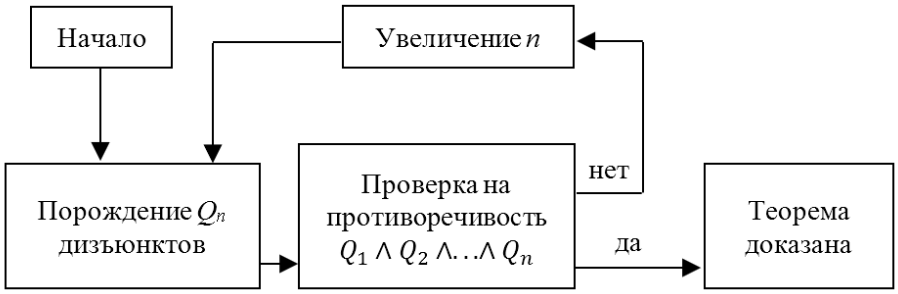

Рис. 3. Схема доказательства отсутствия опасных состояний архитектуры

Проверка безопасности состояния заключается в установлении всех возможных *FLS*-отношений между модулями, которые изменялись на последнем шаге, и проверке их принадлежности подмножеству разрешенных для этих модулей кластерных *FLS*-отношений. Логический вывод является строго формальным процессом, что обеспечивает доказательство соответствия архитектуры системе функционально-структурных ограничений при условии корректности исходных данных.

Выводы

Применение модульно-кластерного анализа позволяет строить модель защиты информационной системы с точностью описания архитектуры достаточной для оценки выполнения нормативных технических требований к защите информации. Сравнение кластерной структуры мультиграфа с матрицей достижимости вершин показывает наличие или отсутствие вершин и дуг, не соответствующих нормативным требованиям к защите информации, установленным для определенных классов или уровней защищенности информационных систем при декларируемой политике доступа. Динамический анализ мультиграфа может использоваться для решения обратной задачи оценки несоответствия мер защиты информации, установленных нормативными документами, политике доступа, а также для доказательства выполнения нормативных требований в критических системах с оценкой безопасности всех состояний системы в машине логического вывода.

Результаты исследований могут быть использованы для разработки стандартов формальной оценки выполнения нормативных требований к защите информации, анализа и разработки политик доступа для национальных распределенных реестров и иных критических информационных систем с доказанным уровнем конструктивной защиты архитектуры. При динамическом анализе методический аппарат может применяться для оценки эффективности формальных моделей разграничения доступа и их реализации в политике управления доступом конкретной информационной системы.

Перспективным направлением является применение технологии искусственного интеллекта для сбора и анализа данных при построении исходной информационной модели системы в терминах кластерной модели защиты и формирования заключений о выполнении нормативных требований к защите информации по результатам эксперимента.

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).

Литература

1. Язов Ю.К., Панфилов А.П. Составные сети Петри-Маркова со специальными условиями построения для моделирования угроз безопасности информации / Вопросы кибербезопасности. 2024. № 2(60). С. 53-65. DOI: 10.21681/2311-3456-2024-2-53-65.
2. Oleynik P.P., Salibekyan S.M. Model of security for object-oriented and object-attributed applications. Trudy ISP RAN/Proc. ISP RAS, vol. 28, issue 3, pp. 35-50. DOI: 10.15514/ISPRAS-2016-28-3.
3. Грибанова-Подкина М.Ю. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Вопросы безопасности. 2017. № 2. С. 25-34. DOI: 10.7256/2409-7543.2017.2.22065.
4. Devyanin P.N., Kuliamin V.V., Petrenko A.K., Khoroshilov A.V., Shchepetkov I.V. Integrating RBAC, MIC, and MLS in Verified Hierarchical Security Model for Operating System. Trudy ISP RAN/Proc. ISP RAS, vol. 32, issue 1, 2020. pp. 7-26.
5. Сундеев П.В. Кластерная модель защиты распределенного реестра // Вопросы кибербезопасности. 2025. № 4 (68). С.2-8. DOI: 10.21681/2311-3456-2025-4-2-8.
6. 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.
7. Сундеев П.В. Модульно-кластерные сети: основы теории. Научный журнал КубГАУ [Электронный ресурс]. Краснодар: КубГАУ, 2006. № 22 (06). Шифр Информрегистра: 0420600012\0132. URL: http://www.ej.kubagro.ru/2006/06/15.
8. 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.
9. Балябин А.А., Петренко С.А. Модель блокчейн-платформы с кибериммунитетом в условиях квантовых атак // Вопросы кибербезопасности. 2025. № 3 (67). сс. 72-82. DOI: 10.21681/2311-3456-2025-3-72-82.
10. Ищукова Е.А. Влияние криптографической стойкости функций хеширования на устойчивость современных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 3 (67). сс. 63-71. DOI: 10.21681/2311-3456-2025-3-63-71.
11. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3(49). С. 2—22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.

SECTION:
INFORMATION PROTECTION METHODS AND SYSTEMS

METHOD FOR ASSESSING COMPLIANCE WITH REGULATORY REQUIREMENTS FOR INFORMATION PROTECTION

***Sundeev P.V.*[6]**

Keywords: *access policy, access model, cluster protection model, constructive protection.*

Abstract

Objective: *to develop a method for formally assessing compliance with regulatory requirements for information protection in national distributed registries and other critical information systems.*

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

Research results: *a method has been developed to assess compliance with regulatory requirements for information protection with formal evidence of the implementation of access policies and protection measures by means of constructive architectural protection.*

Scientific novelty: *scientific novelty consists in the application of an original method of modular cluster analysis of information architecture protection for a formal assessment of compliance with regulatory requirements for information protection using a cluster model of information protection with complete overlap. The reliability of the assessment is achieved*

[6] ***Pavel V. Sundeev,*** *Dr.Sc. (Technology), Chief Research Engineer, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Russia. ORCID: 0009-0005-8442-8921.*
E-mail: sundeev.pv@talantiuspeh.ru

by building a protection model, the accuracy of which is ensured by a formal description of the access policy by multigraph clusters of the information system and the decomposition of information links into interaction levels through which information protection functions are implemented, as well as a formal analysis of the security of system states in the inference machine. The rigor of the architecture's security proof corresponds to the rigor of the mathematical apparatus of logical inference.

Practical significance: *the research results can be used to develop standards for the formal assessment of compliance with regulatory requirements for information security, analyze and develop access control policies for distributed registries and other critical information systems with a proven level of constructive architectural protection, using formal methods for assessing compliance with regulatory requirements in law enforcement practice.*

References

1. Iazov Iu.K., Panfilov A.P. Sostavnye seti Petri-Markova so spetsial'nymi usloviiami postroeniia dlia modelirovaniia ugroz bezopasnosti informatsii / Voprosy kiberbezopasnosti. 2024. No. 2(60). S. 53-65. DOI: 10.21681/2311-3456-2024-2-53-65.
2. Oleynik P.P., Salibekyan S.M. Model of security for object-oriented and object-attributed applications. Trudy ISP RAN/ Proc. ISP RAS, vol. 28, issue 3, pp. 35-50. DOI: 10.15514/ISPRAS-2016-28-3.
3. Gribanova-Podkina M.Iu. Postroenie modeli ugroz informatsionnoi bezopasnosti informatsionnoi sistemy s ispol'zovaniem metodologii ob"ektno-orientirovannogo proektirovaniia // Voprosy bezopasnosti. 2017. No. 2. S. 25-34. DOI: 10.7256/2409-7543.2017.2.22065.
4. Devyanin P.N., Kuliamin V.V., Petrenko A.K., Khoroshilov A.V., Shchepetkov I.V. Integrating RBAC, MIC, and MLS in Verified Hierarchical Security Model for Operating System. Trudy ISP RAN/Proc. ISP RAS, vol. 32, issue 1, 2020. pp. 7-26.
5. Sundeev P.V. Klasternaia model' zashchity raspredelennogo reestra // Voprosy kiberbezopasnosti. 2025. No. 4 (68). S.2-8. DOI: 10.21681/2311-3456-2025-4-2-8.
6. Sistemnyi analiz funktsional'noi stabil'nosti kritichnykh informatsionnykh sistem / Simankov V.S., Sundeev P.V. / pod nauch. red. V.S. Simankova. KubGTU, ISTEk. Krasnodar, 2004. 204 s.
7. Sundeev P.V. Modul'no-klasternye seti: osnovy teorii. Nauchnyi zhurnal KubGAU [Elektronnyi resurs]. Krasnodar: KubGAU, 2006. No. 22 (06). Shifr Informregistra: 0420600012\0132. URL: http://www.ej.kubagro.ru/2006/06/15.
8. Sundeev P.V. Funktsional'naia stabil'nost' raspredelennogo reestra v usloviiakh poiavleniia novoi kvantovoi ugrozy // Voprosy kiberbezopasnosti. 2025. No. 3 (67). S.83-89. DOI: 10.21681/2311-3456-2025-3-83-89.
9. Baliabin A.A., Petrenko S.A. Model' blokchein-platformy s kiberimmunitetom v usloviiakh kvantovykh atak // Voprosy kiberbezopasnosti. 2025. No. 3 (67). ss. 72-82. DOI: 10.21681/2311-3456-2025-3-72-82.
10. Ishchukova E.A. Vliianie kriptograficheskoi stoikosti funktsii kheshirovaniia na ustoichivost' sovremennykh blokchein-ekosistem i platform // Voprosy kiberbezopasnosti. 2025. No. 3 (67). ss. 63-71. DOI: 10.21681/2311-3456-2025-3-63-71.
11. Petrenko A.S., Petrenko S.A. Metod otsenivaniia kvantovoi ustoichivosti blokchein-platform // Voprosy kiberbezopasnosti. 2022. No. 3(49). S. 2—22. DOI 10.21681/2311-3456-2022-3-2-22. EDN: PFKKZC.