УДК 681.3

АВТОМАТИЗАЦИЯ АНАЛИЗА ФУНКЦИОНАЛЬНОЙ СТАБИЛЬНОСТИ КРИТИЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Сундеев П.В. – к. т. н.
Краснодарский военный институт

При создании и реконфигурации информационных систем, используемых в критичных приложениях, трудноразрешимой проблемой является доказательство функциональной стабильности (ФС) информационной архитектуры. В работе рассматривается подход к формализации описания процессов и состояний информационной системы с целью автоматизации логического поиска траекторий информационного процесса, приводящих систему в функционально нестабильные состояния.

Формальная постановка задачи анализа функциональной стабильности критичных информационных систем

Целью анализа ФС критичной информационной системы (КИС) является выявление некоторых свойств объектов, определяющих безопасность состояния системы. Под объектами здесь понимаются элементы информационной архитектуры: функциональные модули, носители информации, файлы и другие материальные или абстрактные информационные объекты, состояния которых характеризуют состояния системы и ход информационного процесса.

Пусть заданы множество Q объектов и некоторое свойство этого множества. Свойство v для некоторого объекта x может быть задано предикатом $P_v(x)$, определенным как функция на множестве Q со значениями «истинно» (И) и «ложно» (Л) $P_v : Q?\{И, Л\}$.

Если Q – множество модификаций объекта, q_o – модификация безопасного объекта, q_i – модификация небезопасного объекта, v – свойство «быть безопасным», то $P_v(q_o)$ = И, $P_v(q_i)$ = Л для всех $q_i \in Q$. Множество Q разбивается предикатом P_v на два подмножества: $Q_v = \{q_o\}$ – безопасный объект и $\overline{Q}_v = \{q_1, q_2, ..., q_n\}$ – небезопасные объекты.

При этом справедливо

$$Q = Q_v \mathbf{U} \overline{Q}_v, \quad Q_v \mathbf{I} \overline{Q}_v = \varnothing. \qquad (1)$$

Таким образом, вычислением значения истинности предиката $P_v(x)$ решается задача анализа безопасности некоторого объекта x.

Если свойство v рассматривать как некоторое сочетание других свойств объекта x, выраженных предикатами $P_{V_1}(x), P_{V_2}(x), \mathbf{K}$, то значение предиката $P_v(x)$ может быть найдено вычислением значения предикатов $P_{V_1}(x), P_{V_2}(x), \mathbf{K}$ и затем определением истинности $P_V(x)$ путем приложения операции следования вида

$$F(P_{V_1}(x), P_{V_2}(x), \mathbf{K}) \to P_v(x). \qquad (2)$$

Каждое свойство v_i также может быть представлено через совокупность других свойств объекта. Применение некоторых операций логики к начальному множеству предложений, составляющему модель объекта x, и получение некоторого предложения этого же языка, являющегося формальным выражением свойства v, составляет процесс вычисления предиката $P_v(x)$. Задача анализа решается путем вычисления значения предиката $P_i(x)$, который принимает истинное значение, если объект x является i-й модификацией q_i, и значение «ложно» – в противном случае.

Таким образом, представление логического компонента алгоритма анализа безопасности в виде формальных операций логического следования на множестве предложений языка задания объекта анализа позволяет рассматривать процесс анализа ФС как многоуровневый управляемый ло-

гический вывод некоторого выражения этого языка, который находится в ходе построения эксперимента.

Решение задачи анализа функциональной стабильности КИС

Решение прямой задачи анализа ФС КИС состоит в определении отсутствия траекторий, проводящих систему в опасные состояния, при установлении конкретных типов информационных отношений между информационными объектами.

Общая последовательность описания ситуации и доказательства ФС КИС в указанном смысле содержит несколько этапов.

1. Классификация, определение и описание свойств типовых информационных объектов предметной области и информационных отношений между ними на содержательном уровне.

2. Описание информационных объектов и отношений в виде аксиом и теорем на языке стандартной логики исчисления предикатов первого порядка.

3. Исключение кванторов общности и существования и преобразование аксиом на расширенный язык клауз Хорна, содержащих не более одного заключения.

4. Поиск минимального конечного подмножества дизъюнктов для Эрбрановского универсума методом резолюций с целью уменьшения размерности области поиска доказательств.

5. Описание предложений на языке логического программирования.

6. Автоматизированный поиск решения с использованием нисходящего вывода и семантического метода, демонстрирующих несовместимость множества клауз при помощи того, что ни одна интерпретация не делает все клаузы истинными.

Модель состояний модулей

Выбранный уровень рассмотрения системы предполагает определение и формализацию отношений между функциональными модулями, возни-

кающих в ходе решения задач по обработке информации. Внутренний механизм функционирования модулей, связанный с прохождением и обработкой информационных сигналов, на данном уровне рассмотрения системы значения не имеет. Для конкретного модуля не важно, в интересах какой задачи выполняется некоторая информационная процедура из числа допустимых операций. С позиции управления информационным процессом важным является вопрос о способности модуля взаимодействовать с другими модулями при данном состоянии системы. Способность модуля к взаимодействию полностью зависит от его состояния, определяемого рядом факторов, которые в данном случае будут иметь качественный смысл.

Анализ особенностей использования и функционирования базовых типов модулей информационных систем позволяет ввести в рассмотрение совокупность формальных высказываний

$$\Im^M = \left\{ \Im_k^M \middle| k \in N^\Phi \right\}, \qquad (3)$$

которые определяются как элементарные формальные высказывания (ЭФВ). Каждое ЭФВ описывает либо одно из нескольких специфических условий нахождения модуля в состоянии S_k^M, либо полное условие нахождения модуля в этом состоянии. Все ЭФВ являются функциями времени в смысле истинности $\Im_k^M$ на момент наступления некоторого события t_n^H.

В рамках предлагаемого подхода ЭФВ описывают состав интерфейсов конкретных модулей и могут быть получены из результатов объектно-ориентированного анализа системы. Описание состояний модулей является статическим представлением системы, которое необходимо дополнить описанием правил переходов состояний, отражающих перемещения модулей по зонам доступа и изменения в составе модулей и их свойств.

Формальное описание процессов функционирования

Сущность любой информационной системы заключается в обеспечении информационного взаимодействия объектов на физическом, синтакси-

ческом и семантическом уровнях [1, 2]. Функции безопасности могут осуществляться на одном и более уровнях и заключаются в регулировании доступа к объектам со стороны внешней среды и активных объектов системы.

Для проведения формального анализа состояний и оценки ФС информационной архитектуры необходимо:

сформулировать формальные признаки опасных состояний системы из множества $\tilde{S}^{O}$, при которых возможна дестабилизация системы;

сформулировать формальные признаки безопасных состояний системы из множества $\tilde{S}^{Б}$, при которых система считается функционально стабильной;

задать начальное, безопасное состояние системы из множества $\tilde{S}^{H}$;

сформулировать формальные правила переходов системы из одного состояния в другое в ходе информационного процесса $S_x \to S_y$;

доказать методом относительно полного перебора состояний, что траектория информационного процесса не приводит систему к опасным состояниям, или необходимо найти эти состояния, что докажет функциональную нестабильность архитектуры системы.

Начальное состояние системы S^{H} считается безопасным, если все объекты O^{W} системы W находятся в разрешенных для них информационной политикой зонах доступа Z_c^{C}, Z_l^{L}, Z_f^{F}, определенных на соответствующих трех уровнях информационного взаимодействия. Объекты контроля ФС $O^{ФС}\,\hat{I}\,O^{W}$, реализующие функции контроля доступа и изоляции зон, имеют статус «активный» $O^{ФС}\,\hat{I}\,O^{a}$, и в системе отсутствуют информационные объекты O^{H} с недекларированными информационными функциями. Это состояние описывается формулой

$$\forall n\left[S_n^{H} \subset \tilde{S}_m^{Б}\right] \Leftrightarrow \forall f \forall l \forall c\ \left[\tilde{O}^{W} \in \tilde{Z}_f^{F}, \tilde{Z}_l^{L}, \tilde{Z}_c^{C} \wedge \tilde{O}^{ФС} \in \tilde{O}^{a} \wedge \tilde{O}^{H} \notin \tilde{Z}_f^{F}, \tilde{Z}_l^{L}, \tilde{Z}_c^{C}\right], \qquad (4)$$

где S_n^H – множество начальных состояний системы *W*;

$\tilde{S}_m^Б$ – множество безопасных состояний системы *W*;

$\tilde{O}^W$ – множество контролируемых информационных объектов системы *W*;

$\tilde{Z}_f^F, \tilde{Z}_l^L, \tilde{Z}_c^C$ – подмножества физических, синтаксических и семантических зон доступа;

$\tilde{O}^{ФС}$ – подмножество объектов системы *W*, реализующих функции контроля ФС;

$\tilde{O}^a$ – подмножество активных объектов системы на момент времени *t*;

$\tilde{O}^H$ – множество объектов с недекларированными информационными функциями, $\tilde{O}^H \subset \tilde{O}^W$.

Переход в другие состояния определяется возможностями активных объектов физически или логически перемещать себя и/или других объектов в другие зоны доступа. Способность активных объектов перемещать себя или другие объекты объясняется их взаимодействием *B* (O_x , O_y), что, в свою очередь, определяется тремя подмножествами пар (кортежами) открытых интерфейсов объекта и смежных объектов.

$$\forall x \forall y \; B_{x,y}(O_x, O_y) \Leftrightarrow \exists F \exists L \exists C \left\{ \left[F_{x,i}^{вых} = F_{y,i}^{вх} \wedge L_{x,i}^{вых} = L_{y,i}^{вх} \wedge C_{x,i}^{вых} = C_{y,i}^{вх} \right] \middle| (O_x, O_y) \in \tilde{Z}_f^F, \tilde{Z}_l^L, \tilde{Z}_c^C \right\}. \quad (5)$$

Каждое подмножество пар открытых интерфейсов соответствует уровню информационного взаимодействия.

Возможность физического взаимодействия устанавливается по схеме соединения объектов (наличием между ними каналов связи), совпадением используемых информационных параметров физических сигналов и наличием физических трансляторов, которые могут согласовать параметры взаимодействия (перемещать в пространстве носители информации, синхронизировать время и т. п.).

Возможность синтаксического взаимодействия объектов определяется наличием физического взаимодействия, совпадением алфавитов, лексики и синтаксиса языков или наличием трансляторов для приведения их в соответствие.

Возможность семантического взаимодействия объектов объясняется наличием физического и синтаксического взаимодействия, способностью объекта выполнять функции по управлению другими информационными объектами. Для анализа ФС интерес представляют семантические возможности объектов по обработке информации, т. е. способность объектов системы активизировать, копировать, перемещать, транслировать и т. д.

Устойчивый (возможно стандартный) набор способностей по физическому, синтаксическому или семантическому взаимодействию, существующих у объекта, называется соответственно физическим F, синтаксическим L или семантическим C открытым интерфейсом информационного объекта. Открытость интерфейса заключается в свободном доступе к нему соответствующих открытых интерфейсов других объектов при соблюдении необходимых условий. Все интерфейсы объектов системы могут быть сведены в перечне типовых интерфейсов системы отдельно по каждому уровню взаимодействия.

Правила описания переходных состояний

Подход к моделированию процессов обработки информации в сложных информационных системах на основе применения взаимосвязанного трехуровневого представления процессов позволяет выделить объективно существующие между ними взаимосвязи при анализе ФС информационной архитектуры КИС. Основными положениями такого подхода являются:

для адекватного моделирования процессов обработки информации необходимо одновременно и совместно рассматривать процессы изменения физических, синтаксических и семантических состояний информаци-

онных объектов, происходящих в системе функции обработки информации;

для описания процесса изменения состояния каждого из рассматриваемых объектов применяются адаптированные методы объектно-ориентированного анализа сложных систем, теории входящих потоков задач и теории состояний КИС;

для установления взаимосвязи между процессами вводятся логические условия пребывания каждого объекта в одном из его состояний в зависимости от состояний других объектов;

логические условия взаимосвязи процессов реализуются следующим образом: объект может находиться в заданном состоянии или изменять свое состояние в зависимости от заданных условий пребывания в соответствующем состоянии и от взаимодействия с другими взаимосвязанными объектами при нахождении их в заданном состоянии или при изменении этого состояния;

модель взаимосвязанного трехуровневого процесса обработки информации представляет собой множество взаимосвязанных логическими условиями информационного взаимодействия процессов, имеющих физическую, синтаксическую или семантическую природу;

модель представляется в виде трех взаимосвязанных, ориентированных графов, вершинами которых являются состояния физических, синтаксических или семантических процессов, а дуги – направленные переходы из одного состояния в другое.

Формальное состояние системы S_t^W в момент времени t определяется как отражение множества физических и абстрактных модулей $\tilde{M}^W$ системы W на множество контролируемых $\tilde{Z}^W$ и смежных с ними неконтролируемых зон доступа $\tilde{Z}^H$ всех уровней взаимодействия, а также множеством возможных отношений между активными абстрактными модулями $\tilde{M}_a^A$ и

остальными модулями системы, которые определяются кортежами парных интерфейсов модулей, находящихся в одной зоне в момент времени *t:*

$$S_t^W\left(\tilde{M}^W\right)\equiv\left\{\tilde{Z}^W,\ \tilde{Z}^H,\ \tilde{M}_a^A,\left(\tilde{F}_{x,i}^{вых}=\tilde{F}_{y,i}^{вх}\right),\left(\tilde{L}_{x,j}^{вых}=\tilde{L}_{y,j}^{вх}\right),\left(\tilde{C}_{x,k}^{вых}=\tilde{C}_{y,k}^{вх}\right)\middle|\ x\in\tilde{M}_a^A, y\in\tilde{M}^W\right\}, \quad (6)$$

где $S_t^W\left(\tilde{M}^W\right)$ – состояние системы W в момент времени t, состоящей из множества модулей $\tilde{M}^W$;

$\tilde{M}^W$ – множество физических и абстрактных модулей, идентифицированных в системе, $\tilde{M}^W\subset\tilde{Z}^W\vee\tilde{Z}^H$;

$\tilde{Z}^W$ – множество контролируемых зон системы;

$\tilde{Z}^H$ – множество смежных зон, неконтролируемых системой;

$\tilde{M}_a^A$ – подмножество активных абстрактных модулей системы W на момент времени t, $\tilde{M}_a^A\subset\tilde{M}^W$;

$\left(\tilde{F}_{x,i}^{вых}=\tilde{F}_{y,i}^{вх}\right),\left(\tilde{L}_{x,j}^{вых}=\tilde{L}_{y,j}^{вх}\right),\left(\tilde{C}_{x,k}^{вых}=\tilde{C}_{y,k}^{вх}\right)$ – кортежи парных интерфейсов модулей, находящихся в одной зоне.

В процессе функционирования система под воздействием разных событий может сохранять или изменять свое состояние. Для отображения динамики процесса функционирования кроме множества формул состояний системы необходимо иметь множество формул, описывающих переходы системы из одного состояния в другое.

В общем виде все возможные изменения или сохранения состояний системы определяются отображением

$$x^W : S^W \to S^W. \quad (7)$$

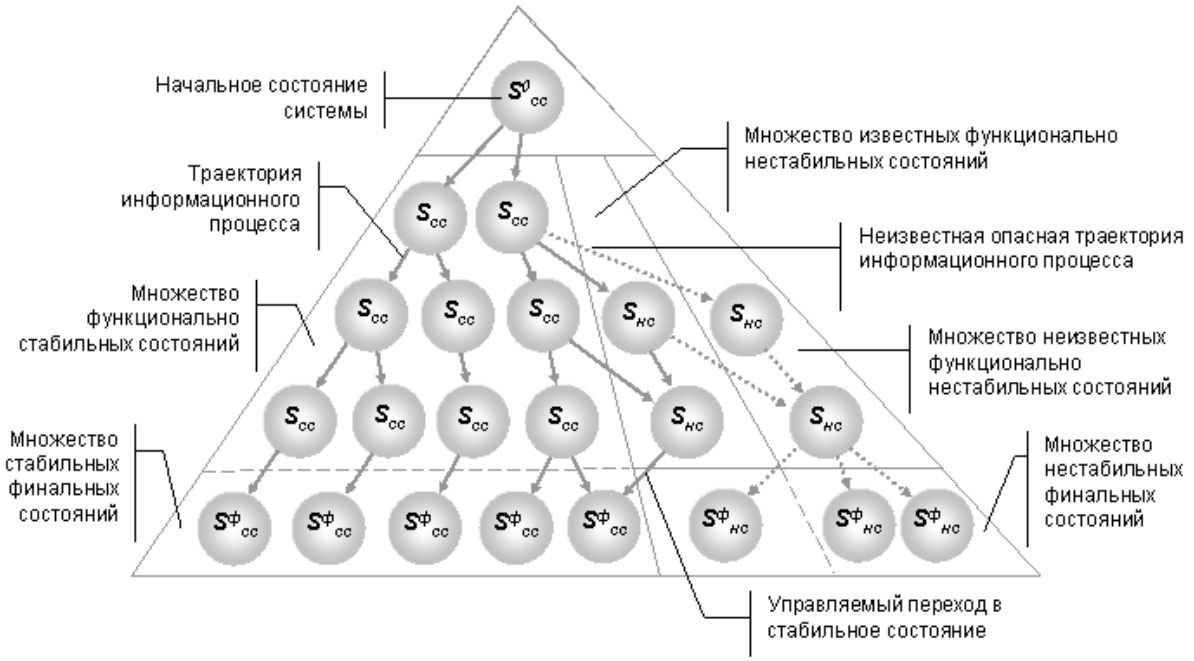
Для каждого состояния S_n^W можно указать правила x_n^W, позволяющие находить его образ $\tilde{x}_n^W\left(S_n^W\right)$ во множестве S^W. Упорядоченная последовательность правил x_n^W будет называться кортежем переходов. Кортеж переходов для S_n^W определяется как упорядоченная совокупность списков x_n^W,

содержащих информацию о причинах перехода, номерах состояний, к которым выполняются переходы, и условия каждого перехода.

Под сменой состояния системы здесь понимаются изменения в распределении или составе модулей относительно существующих зон доступа, а также информационных свойств модулей в результате потери или приобретения способности взаимодействовать через определенные открытые интерфейсы. Поэтому правила перехода состояний должны характеризовать условия и причины, при которых возможны указанные события.

Модель системы представляется в виде ориентированного графа, вершинами которого являются состояния процессов, а дуги – направленные переходы из одного состояния в другое, т. е. ее поведение, определяемое архитектурой системы и технологией обработки данных.

Точность отражения состояний КИС в модели определяется размерами множеств состояний системы и полнотой регистрируемых событий. Состояние системы будет воспроизводиться в модели приближенно из-за потери части информации. Однако и при этом условии размерность графа будет велика, а его вид заранее неизвестен (см. рисунок).



Граф возможных состояний модели КИС

Проблема, связанная со сложностью построения полного графа, может решаться с использованием принципа обучения и дообучения системы моделирования [3] или формализованных методик синтеза модели с последующим автоматизированным поиском траекторий, приводящих систему в опасные состояния [1, 2]. Наиболее эффективный способ моделирования и анализа функциональной стабильности КИС может заключаться в совместном использовании обоих принципов.

Правила формализованного описания моделей состояний состоят из правил описания условий взаимодействия информационных объектов (модулей) и правил переходов.

Аксиома 1. Если два модуля M_x и M_y находятся в одной физической зоне Z_f^F, и у них имеются парные физические интерфейсы $F_{x.k}^{вых} = F_{y.k}^{вх}$, то возможно их физическое взаимодействие I^F типа k:

$$\overline{F} \equiv \forall x \forall y\, I^F(M_x, M_y, k) \Leftrightarrow \exists k \exists f \left(F_{x.k}^{вых} = F_{y.k}^{вх} \middle| M_x, M_y \in Z_f^F\right), \qquad (8)$$

где $k=\overline{1,n}$ – порядковый номер физического интерфейса в перечне типовых физических интерфейсов системы.

Аксиома 2. Если два модуля M_x и M_y одновременно находятся в одной физической Z_f^F и одной синтаксической Z_l^L зонах, и у них имеются парные физические и синтаксические интерфейсы $F_{x.k}^{вых}=F_{y.k}^{вх}$ и $L_{x.h}^{вых}=L_{y.h}^{вх}$, то возможно их синтаксическое взаимодействие I^L типа h при условии выполнения k:

$$\overline{L}\equiv\forall x\forall y\, I^L\left(M_x,M_y,h\right)\Leftrightarrow\exists k\exists h\exists f\exists l\left(F_{x.k}^{вых}=F_{y.k}^{вх}\wedge L_{x.h}^{вых}=L_{y.h}^{вх}\,\middle|\, M_x,M_y\in Z_f^F,Z_l^L\right), \qquad (9)$$

где $h=\overline{1,m}$ – порядковый номер синтаксического интерфейса в перечне типовых синтаксических интерфейсов системы.

Аксиома 3. Если два модуля M_x и M_y одновременно находятся в одной физической Z_f^F, одной синтаксической Z_l^L и одной семантической Z_c^C зонах, и у них имеются парные физические, синтаксические и семантические интерфейсы $F_{x.k}^{вых}=F_{y.k}^{вх}$, $L_{x.h}^{вых}=L_{y.h}^{вх}$ и $C_{x.g}^{вых}=C_{y.g}^{вх}$, то возможно их семантическое взаимодействие I^C при условии выполнения k и h:

$$\overline{C}\equiv\forall x\forall y\, I^C\left(M_x,M_y,g\right)\Leftrightarrow$$
$$\Leftrightarrow\exists k\exists h\exists g\exists f\exists l\exists c\left(F_{x.k}^{вых}=F_{y.k}^{вх}\wedge L_{x.h}^{вых}=L_{y.h}^{вх}\wedge C_{x.g}^{вых}=C_{y.g}^{вх}\,\middle|\, M_x,M_y\in Z_f^F,Z_l^L,Z_c^C\right), \qquad (10)$$

где $g=\overline{1,p}$ – порядковый номер семантического интерфейса в перечне типовых семантических интерфейсов системы.

Правила формализованного описания переходов состояний системы заключаются в описании семантики возможных типов k, h и g информационных взаимодействий модулей на трех уровнях при выполнении аксиом 1, 2 и 3.

Аксиома 4. Семантика информационного взаимодействия на физическом уровне заключается в перемещении (трансляции) из физической зоны в смежную физическую зону $Z_f^F\rightarrow Z_{f.i}^F$ физического (носитель информации)

или абстрактного (алгоритм или данные) модуля $\mathrm{M}_{\mathrm{y}}^{A,F}$ под воздействием активного модуля $M_x^a \in \tilde{M}^{A,F}$ при выполнении условий $\bar{F}$ аксиомы 1.

Существует два типа физического взаимодействия:

- перемещение *m*-move (Π^{F}), при котором модуль $\mathrm{M}_{\mathrm{y}}^{A,F}$ оказывается в другой физической зоне $\mathrm{Z}_{\mathrm{f.i}}^{\mathrm{F}}$:

$$\bar{m} \equiv \forall x \forall y \, \Pi^{\mathrm{F}}\left(M_{\mathrm{x}}^{a}, \mathrm{M}_{\mathrm{y}}^{A,F}, \mathrm{Z}_{\mathrm{f}}^{\mathrm{F}} \to \mathrm{Z}_{\mathrm{f.i}}^{\mathrm{F}}\right) \Leftrightarrow \exists x \exists y \left(\bar{F}=1 \,\middle|\, \mathrm{M}_{x}^{\mathrm{a}} \in \tilde{\mathrm{M}}^{\mathrm{A,F}}\right); \qquad (11)$$

- копирование *c*-copy, т. е. размножение P^{F} модуля $\mathrm{M}_{\mathrm{y}}^{A,F}$ на 2, …, n таких же модулей и их перемещение Π^{F} в *f.i, …, f.j* зоны, при котором копии $\mathrm{M}_{\mathrm{y.1,\ldots,y.n}}^{A,F}$ модуля $\mathrm{M}_{\mathrm{y}}^{A,F}$ оказываются в других зонах $\mathrm{Z}_{\mathrm{f.i}}^{\mathrm{F}}, \ldots, \mathrm{Z}_{\mathrm{f.j}}^{\mathrm{F}}$. Эта операция обычно применяется к программным модулям

$$\begin{gathered}\bar{c} \equiv \forall x \forall y \, \mathrm{P}^{\mathrm{F}}\left(M_{\mathrm{x}}^{a}, \mathrm{M}_{\mathrm{y}}^{A,F} \to \mathrm{M}_{\mathrm{y.1,\ldots,n}}^{A,F} \,\middle|\, \mathrm{M}_{\mathrm{y}}^{A,F} = \mathrm{M}_{\mathrm{y.1,\ldots,n}}^{A,F}\right), \Pi^{F}\left(M_{\mathrm{x}}^{a}, \mathrm{M}_{\mathrm{y.1,\ldots,y.n}}^{A,F}, \mathrm{Z}_{\mathrm{f}}^{\mathrm{F}} \to \mathrm{Z}_{\mathrm{f.i,\ldots,f.j}}^{\mathrm{F}}\right) \Leftrightarrow \\ \Leftrightarrow \exists x \exists f \exists i \exists j \left(\bar{F}=1, \mathrm{M}_{x}^{\mathrm{a}} \in \tilde{\mathrm{M}}^{\mathrm{A,F}}, M_{y.1,\ldots,y.n}^{A,F} \in Z_{f.i,\ldots,f.j}^{F}\right).\end{gathered} \qquad (12)$$

Аксиома 5. Семантика информационного взаимодействия на синтаксическом уровне заключается в переводе синтаксиса *t*-translation абстрактного модуля M_y^A на другой язык, т. е. в перемещении Π^L его из одной синтаксической зоны в другую $\mathrm{Z}_{\mathrm{l}}^{\mathrm{L}} \to \mathrm{Z}_{\mathrm{l.i}}^{\mathrm{L}}$ под воздействием активного синтаксического модуля-транслятора T_x^L при выполнении условий $\bar{L}$ аксиомы 2.

$$\bar{t} \equiv \forall x \forall y \Pi^{\mathrm{L}}\left(T_{\mathrm{x}}^{L}, \mathrm{M}_{\mathrm{y}}^{\mathrm{A}}, \mathrm{Z}_{\mathrm{l}}^{\mathrm{L}} \to \mathrm{Z}_{\mathrm{l.i}}^{\mathrm{L}}\right) \Leftrightarrow \exists x \left(\bar{\mathrm{L}}=1, \mathrm{T}_{\mathrm{x}}^{\mathrm{L}} \in \tilde{\mathrm{M}}^{\mathrm{a}}\right). \qquad (13)$$

Аксиома 6. Информационное взаимодействие на семантическом уровне заключается в активизации *a*-action активным модулем-алгоритмом M_{x}^{a} другого абстрактного модуля-алгоритма, т. е. в передаче управления Π^C в виде ресурсов и параметров модулям-алгоритмам, способным совершать операции $\bar{g}$, $\bar{d}$, $\bar{a}$, $\bar{m}$, $\bar{c}$ и $\bar{t}$ при выполнении условий $\bar{C}$ аксиомы 3.

$$\bar{\mathrm{a}} \equiv \forall x \forall y \, \Pi^{\mathrm{C}}\left(M_{\mathrm{x}}^{a}, \mathrm{M}_{\mathrm{y}}^{\mathrm{A}}, \mathrm{Z}_{\mathrm{c}}^{\mathrm{C}} \to \mathrm{Z}_{\mathrm{c.i}}^{\mathrm{C}}\left(\bar{g} \vee \bar{d} \vee \bar{a} \vee \bar{m} \vee \bar{c} \vee \bar{t}\right)\right) \Leftrightarrow \exists x \left(\bar{C}=1, M_{x}^{a} \in \tilde{M}^{a}\right). \qquad (14)$$

Указанные операции определяют семантику возможностей модулей по исполнению следующих функций обработки информации на трех уровнях:

$\bar{g}$ – создание модуля, т. е. выделение носителя информации или его части под логическую структуру модуля и идентификация в системе новой структуры, соответственно, в качестве физического или абстрактного модуля;

$\bar{d}$ – уничтожение модуля, т. е. исключение носителя информации или логической структуры из системы;

$\bar{a}$ – активизация модуля, т. е. передача ему управления;

$\bar{m}$ – физическое перемещение модуля, т. е. перемещение носителя информации как физического объекта или логической структуры как абстрактного объекта из одного носителя информации в другой;

$\bar{c}$ – физическое копирование модулей, т. е. выделение носителя информации под копию модуля, идентификация этого носителя и перемещение структуры модуля на выделенный носитель (создание и перемещение);

$\bar{t}$ – синтаксическая трансляция абстрактных модулей, т. е. изменение синтаксиса или алфавита модуля без изменения семантики.

Для интерпретации на ЭВМ формальную модель удобно представить в виде логической программы, например, Пролог-программы. Главным компонентом языка Пролог является универсальный механизм решения задач, принцип действия которого основан на правиле резолюции. Правило резолюции оказывается особенно привлекательным при использовании для вычислений на ЭВМ, так как само по себе оно является полным множеством правил вывода для фразовой формы логики предикатов, т. е. применяя только одно это правило, можно вывести любое следствие из множества аксиом, представленных во фразовой форме. Для того чтобы воспользоваться этим механизмом, необходимо описать задачу при помощи фраз Хорна, выраженных на языке Пролог.

Генерация теорем и аксиом в виде формальных высказываний математической логики исчисления предикатов может осуществляться автоматически из объектных диаграмм и диаграмм классов на основе исходных данных о структуре ориентированного графа, свойствах его вершин и дуг, полученных на этапе объектно-ориентированного анализа КИС, при наличии совместимого с CASE-средством (например, Rational Rose) компилятора для языка типа Пролог или Лисп.

Создание научно-методического аппарата, объединяющего в рамках единой методологии основные положения теории ФС КИС, методы формализации состояний, автоматизации моделирования и поиска функционально нестабильных состояний с формальным доказательством отсутствия запрещенных траекторий, приводящих систему в опасные состояния, позволит проводить объективную оценку и гарантировать функциональную надежность информационных систем, используемых в критичных приложениях.

Список литературы

1. Симанков В.С., Сундеев П.В. Системный анализ функциональной стабильности критичных информационных систем: Монография / Под ред. В.С. Симанкова. Краснодар: Институт современных технологий и экономики, 2003. 132 с.

2. Сундеев П.В. Построение информационной модели функционирования обобщенной системы управления и обоснование фундаментальных принципов информационного взаимодействия сложных систем // Межвузовский сборник научных трудов. Краснодар: Краснодарский военный институт, 2000.

3. Пучков Н.В. Адекватность моделирования информационной среды при проектировании системы безопасности // Специальная техника средств связи. Системы, сети и технические средства конфиденциальной связи. 1999. Вып. 1.