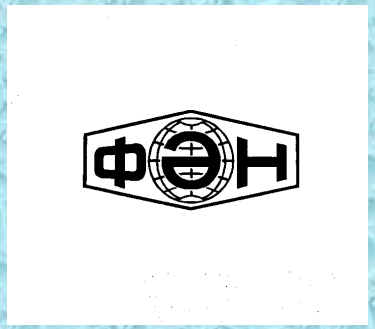
АКАДЕМИЯ НАУК РЕСПУБЛИКИ ТАТАРСТАН

В.А. РАЙХЛИН, И.С. ВЕРШИНИН,
Р.Ш. МИНЯЗЕВ, Р.Ф. ГИБАДУЛЛИН

КОНСТРУКТИВНОЕ МОДЕЛИРОВАНИЕ СИСТЕМ ИНФОРМАТИКИ

Под редакцией В.А. Райхлина



Академия наук РТ
Казань 2016

Прошло более 10 лет после выхода моей первой книги по КМС [***Райхлин В.А.*** Конструктивное моделирование систем, **2005**]. За эти годы нами получено немало новых интересных результатов по ***цифровым автоматам, параллельным СУБД и ассоциативной защите данных,*** что определяет предметную направленность наших исследований в настоящее время. Они заменили бóльшую часть прикладного материала ранее опубликованной книги, хотя ***методология КМС осталась неизменной.***

СТРУКТУРА МОНОГРАФИИ

Часть 1. Методология КМС

Раздел I – показываются ***истоки*** направления (синтез ***искусственных линий*** во взаимосвязи с вопросами реализации) и польза эвристики при построении математической модели. Но если такая модель найдена, то дальнейшие исследования проводятся строго дедуктивно с привлечением эксперимента.

Раздел II – обсуждается ***методология*** и связь КМС с *эволюционизмом* и *искусственным интеллектом*. Уточняется ***концепция неформальной модели синтеза*** с иллюстрацией ее отдельных положений на ряде моделей.

Часть 2. Неформально заданные цифровые автоматы

Раздел III. ***Элементы теории и моделирование процессов «ручного» синтеза*** (объектное определение и неполностью структурированная модель).

Раздел IV. ***Автоматизация процесса синтеза*** (фреймовая модель и построение интерактивной системы синтеза).

Раздел V. ***Вопросы реализации и программное моделирование*** (реализуемость и интерактивная генерации таких моделей).

Часть 3. Параллельные СУБД консервативного типа

Раздел VI. ***Моделирование кластеров консервативных БД с позиций КМС*** (принятый план обработки запросов, внешнее моделирование, модель выбора конфигураций, генетический алгоритм).

Раздел VII. ***СУБД Clusterix*** **как инструмент исследований** (функциональная характеристика, компоненты программной системы, измерительная подсистема, претрансляция запросов).

Раздел VIII. ***Результаты*** **исследований** (масштабируемость; вопросы самоорганизации; за гранью масштабируемости; мультикластеризация; перспективы развития).

Часть 4. Элементы ассоциативной стеганографии

Раздел IX. ***Введение в ассоциативную защиту объектов картографии*** (предлагаемая стратегия защиты; позиции КМС; базовый алгоритм маскирования и его свойства; возможности анализа защищенных сцен картографии).

Раздел X. ***Достижимая стойкость и помехоустойчивость ассоциативной защиты*** (анализ всевозможных атак; устойчивость к помехам дезинформации и случайным помехам).

Раздел XI. ***СУБД защищенных картографических сцен*** (принципы организации; разработанные прототипы; результаты тестирования).

В исследованиях, рассмотренных в разделах III–XI, в разное время принимали участие: кандидат наук **А.В. Морозов** и магистр **К.А. Фадеев** – разработчики интерактивных систем синтеза и программного моделирования цифровых автоматов; кандидат наук **Е.В. Абрамов**, магистры **Д.О. Шагеев, А.В. Попов, Н.А. Ильин** и **В.В. Куревин**, инженер **В.Р. Вагин** – создатели первой версии СУБД *Clusterix*; аспирант **Р.К. Классен** – энтузиаст новых исследований по параллельным СУБД; ассистент **С.В. Пыстогов** – разработчик ассоциативно-защищенных полнообъектных СУБД картографии. **Их вклад в практику КМС безусловен.**

ОБСУЖДЕНИЕ МЕТОДОЛОГИИ

ПОСЫЛКИ КОНСТРУКТИВИЗМА

Всякий, кто занимается вопросами синтеза в условиях неопределенности (иначе нет проблемы), является сознательным либо стихийным конструктивистом.

В основе конструктивизма – симбиоз, точнее – взаимодополнительность теории и эксперимента. До середины 80-х годов прошлого века господствовала парадигма первенства теории над экспериментом. С этим никогда не были согласны передовые ученые. ***Натурный, вычислительный либо умозрительный эксперимент – источник открытий***. Знаменитый философ и математик 17 века Рене Декарт (Картезиус) утверждал: ***«все вокруг познается лишь опытом и исследованиями»***. 11 теорем великого Пьера Ферма – это ***заметки к «Арифметике» Диофанта***. Как считал Норберт Винер, ***теоремы сначала открываются и лишь затем доказываются***.

Конструктивное моделирование систем занимается вопросами синтеза сложных систем в условиях неполноты информации. ***Недостаток информации восполняется открытиями по результатам эксперимента***, которые не поддаются строгому доказательству.

Надо иметь мужество декларировать эти открытия как конструктивные закономерности и брать их за основу развития перспективных теорий с серьезными приложениями.

Близкую точку зрения имели известные конструктивисты прошлого века академики Н.Н. Семенов (творец теории цепных реакций) и П.К. Анохин (творец конструктивной теории функциональных систем):

« … Опыт есть единственный непреложный аргумент, и как бы ни было удивительно то, что он нам говорит, – мы обязаны ему верить и строить новые теории применительно к тому, что мы видим, не смущаясь противоречиями со старым и привычным».

Н.Н. Семенов

« … Реальные системные закономерности могут быть почерпнуты и разработаны только на основе конкретного материала по исследуемому явлению. … Этот материал и должен стать основой формализации».

П.К. Анохин

Академик П.К. Анохин писал о необходимости передачи молодому поколению ученых истории возникновения той или иной плодотворной идеи:

«**А.Эйнштейн**, говоря об истории науки, часто подчеркивал, что “***только идеи имеют непреходящую ценность***”, и очень часто сетовал, что ученые мало заботятся о написании “истории идей”… ***Трудности творческого процесса не видны обычно в конечных результатах и поэтому для науки навсегда исчезает их познавательный и воспита-тельный смысл…»***

ПОЧЕМУ ТАК? – не всегда простой вопрос. При объяснении того или иного явления многие ученые и преподаватели как ***нечто очевидное*** нередко используют когда-то и кем-то высказанные **гипотезы** ***(постулаты)***, которые отнюдь «не лежат на поверхности». Сами они об этом часто забывают. Критически мыслящему человеку иногда бывает **нелегко принять на веру подобные установки**. Это вносит серьезные трудности в образовательный процесс и определяет ***необходимость развития научной методологии и ее усвоения не только молодым поколением***.

Достаточно давно, в ходе исследований по ***искусственным линиям*** у меня возникла убежденность в том, что предложенный конструктивный метод дает решения, близкие к ***глобальному оптимуму.*** Для базовых структур ограниченной сложности это было установлено достаточно строго. Однако с ростом размерности доказательство оптимальности становилось неразрешимой задачей. Надо было искать какой-то особый подход к обоснованию.

Найденный подход состоял в ***постулировании*** сходимости отображающих числовых последовательностей к некоторой эталонной во введенных метрических пространствах. Так родилась идея построения ***неформальных моделей синтеза*** как динамически ***эволюционирующих*** образований. ***В дальнейшем концептуально аналогичные подходы были успешно применены к синтезу ряда других объектов информатики.***

Ретроспективный анализ логики этих исследований позволил предложить концепцию ***конструктивного моделирования систем*** как методологическую основу одноименного научного направления.

КОНСТРУКТИВНОЕ МОДЕЛИРОВАНИЕ

Можно выделить 3 начала конструктивного моделирования систем:

1. Считается, что синтезируемое устройство моделирует поведение некоторой ***гипотетической системы***.

2. Полагается необходимой ***декларация постулатов*** для обоснования, в меру накопленных знаний, адекватности найденного метода решаемой задаче.

3. Признается «бесконечность систем объяснений и их неизбежная незавершенность,т.е. ***открытость*** для дальнейших объяснений».

Конструктивное моделирование систем ассоциируется с познанием своеобразной «вселенной» (п.1,3). Процесс такого познания бесконечен. ***В таком процессе правомерно использование общей методологии естественных наук (прежде всего, – физики), которая базируется на введении постулатов.***

Наиболее критичен п.2 – о необходимости введения постулатов (получения при синтезе ответов не только на вопросы **ГДЕ?** и **КАК?**, но и на вопрос **ПОЧЕМУ?** так).

Вот, например, мнение Дж. фон Неймана : *«Точные науки не объясняют, они редко даже обсуждают явления и, в основном, предлагают модели. … Смысл [моделей как некоторых абстракций – В.Р.] … состоит исключительно в том, что они должны «работать».* Да, модель обязана «работать». Все другое дискуссионно. Мы согласны с философом Е.П. Никитиным в том, что ***«объяснение – одна из важнейших функций науки»***.

Введение постулатов преследует две цели:

1) ***решение частной задачи моделирования*** (построения релевантной математической модели);
2) ***разработка конструктивного метода***, адекватного решаемой задаче синтеза.

Все постулаты содержат элементы модальности и определяют только ***направление поиска решения***, оставляя свободу выбора метода в рамках этого направления.

Выверенная система постулатов допускает избыточность. Внутренние противоречия этой системы либо ее недостаточность могут быть установлены только по мере накопления новых фактов. Именно поэтому *система постулатов должна быть открыта для корректив.*

Для развития конструктивных подходов в точных науках обычно вводятся некоторые ***определения и ограничения***. Полученный в итоге метод – всего лишь один из многих возможных. Оценка его адекватности несколько аморфна: ***«можно и так»***.

При введениии постулатов оценка адекватности становится более категоричной: ***в меру накопленных знаний и модальности методов постулируемого направления, «надо только так!»***. Это – вполне приемлемый мотив.

Сформулированная концепция S-моделирования представляет собой попытку возможной детерминации (систематизации) интуитивно разделяемой многими ***системной методологии синтеза.***

Не секрет, что многие методы сначала открываются, и лишь затем делаются попытки их обоснования. Все введенные понятия и принципы сформировались в итоге поиска приемлемого пути общенаучного обоснования таких методов.

КОНЦЕПЦИЯ S- МОДЕЛИРОВАНИЯ

Концепция формулирует общий методологический подход к синтезу в условиях неполноты информации. Она представляет собой ряд атрибутно-классификационных определений. Вводит типы S-моделей (S – от Synthesis), показывает этапы и приемы их построения. Основные положения концепции:

- ***Система*** – нечто единое целое, бесконечно познаваемое и объясняемое, заданное своим оператором назначения.
- ***S-модель системы***, или модель процесса синтеза – конструктивный метод получения множества представлений некоторой ***гипотетической системы***.
- ***Постулаты*** – обоснованные декларации свойств множества представлений гипотетической системы как объяснительные посылки к построению модели. ***Система постулатов открыта для корректив*** (пример табл. 1).

Таблица 1. Иллюстрация процесса пополнения (корректировки) системы постулатов.

Гипотетическая система	Развитие системы постулируемых свойств	Динамика представлений
Нечто, на чем человеку удобно сидеть	гладкая поверхность	бревно
	небольшие размеры	«чурбак»
	легкость переноски	табурет
	наличие опоры для спины	первый стул
	— — —	— — —

- ***S-моделирование системы*** – итеративный процесс поиска и разработки конструктивного метода (рис. 1).

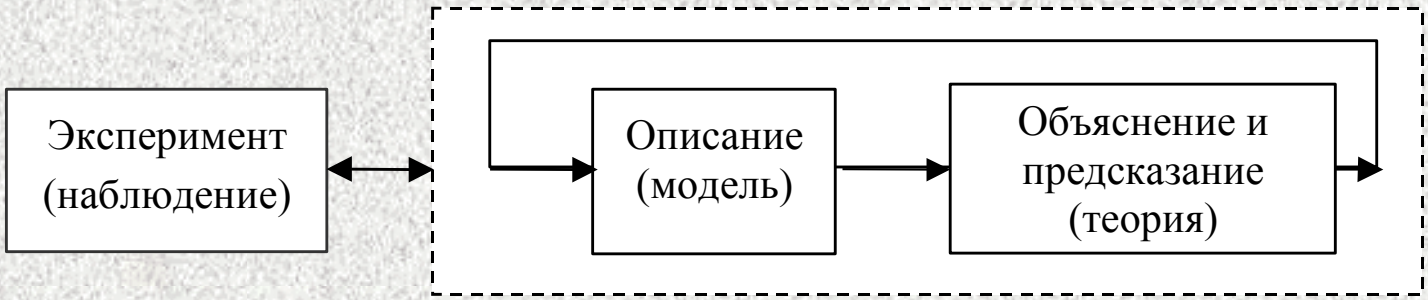


Рис. 1. Иллюстрация процесса *S*-моделирования.

- ***Устойчивая основа S-модели*** – ее компонента, не меняющаяся в процессе S-моделирования.

- ***Частная задача S-моделирования*** – поиск релевантной математической модели, т.е. ассоциированного с объектом синтеза множества и отношений на нем (подмножеств, областей) с постулированными свойствами.

- ***Унитарная S-модель (US-модель)*** – интегрированное описание системы, удовлетворяющее принятой системе постулатов.

- ***Иерархическая S-модель (IS-модель)*** – множество представлений иерархической системы. Каждый уровень иерархии рассматривается отдельно в симбиозе каждого представления.

Определение модели системы как конструктивного метода вполне корректно с позиций системного анализа, который допускает широкую трактовку понятия модели как любого целесообразного представления системы.

Разработка конструктивного метода при неполноте информации рассматривается как моделирование процесса синтеза.

Математическая модель входит в состав модели процесса как релевантное описание (фреймовое, логическое, алгебраическое или др.) ***подмножеств (областей) с постулируемыми свойствами.***

В выделенной области тем или иным методом (алгоритмом) ***ищется решение задачи синтеза.***

Введение постулатов обосновывает найденный метод, делает его адекватным решаемой задаче, определяет процедуру синтеза.

Виды постулатов:

1) ***законы природы (мировой опыт)*** – не доказуемы, но постоянно проявляются и безусловно принимаются всеми;

2) ***экспериментальные закономерности*** – не строго индуктивны, что является источником сомнений. Их преодолевают использованием аксиомы знания модальной логики: ***«Что известно, то верно»***;

3) ***умозрительно введенные постулаты.*** Их невозможно проверить опытом, нельзя и опровергнуть (например, постулаты церкви). Но они «работают».

ГДЕ «копать»? ПОЧЕМУ именно здесь? КАК это делать?

Получение ответов на эти кардинальные вопросы синтеза является предметом конструктивного моделирования систем как научного направления.

ИНВЕРСИЯ ПОНЯТИЙ МОДЕЛИ И ТЕОРИИ

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПО Д. ГИЛЬБЕРТУ

– ***формальная аксиоматическая система как математическая модель некоторой содержательной математической теории.*** Это совокупность абстрактных объектов, в которой представлены правила оперирования множеством символов в сугубо синтаксической трактовке.

Формальная система определена, если

1) задан конечный алфавит (конечное множество символов);
2) определена процедура построение формул (слов);
3) выделено некоторое множество слов, называемых аксиомами;
4) задано конечное множество правил вывода, которые позволяют получать новые теоремы из аксиом и ранее доказанных теорем.

Интерпретация – распространение исходных положений формальной системы на реальный мир. Она придает смысл каждому символу системы и устанавливает взаимооднозначное соответствие между этими символами и реальными объектами.

Теоремы формальной системы, будучи интерпретированы, становятся утверждениями в обычном смысле слова, и тогда можно говорить об их истинности или ложности. Одна и та же формальная система может служить моделью различных конкретных ситуаций.

Обоснованием модели считается ее непротиворечивость, т.е. невозможность доказательства в ней двух противоположных теорем.

Цель моделирования – повышение строгости математических построений и доказательство общих теорем для множества интерпретаций.

Изменение цели ***(моделирование системы как «черного ящика»)*** приводит к взаимной инверсии понятий модели и теории.

ПОЗИЦИЯ Ю.А. ШРЕЙДЕРА

Модель ***M***, или реляционная система определяется как множество M с заданным на нем набором отношений $\{r_1,\ldots,r_n\}$, свойства которых определены тем или иным способом.

k–местным отношением на множестве M называется совокупность упорядоченных наборов (кортежей) из *k* элементов множества M вида $\langle x_1, x_2,\ldots,x_k\rangle$.

Сигнатурой модели называется набор названий отношений (набор имен-символов) в этой модели. Так, модель $M = \langle M \{r_1, \ldots, r_n\}\rangle$ имеет сигнатуру $\Omega = \langle R_1, \ldots, R_n\rangle$, если $\alpha(R_i) = r_i$ для любого $i \in \{\overline{1,n}\}$. Здесь α – отображение, которое сопоставляет каждому имени отношения R_i из сигнатуры Ω отношение r_i.

Пара $\langle M, \alpha\rangle$ называется моделью в сигнатуре Ω. Это определение модели эквивалентно предыдущему.

Пусть формула Φ_i представляет высказывание о свойствах отношения с именем R_i безотносительно к базовому множеству M, а потому и к отображению $\alpha(R_i)$.

Теорией T называется множество формул $\{\Phi_i\}$ в сигнатуре $\Omega = \{R_i\}$ вместе с набором $\{\rho\}$ правил вывода в той же сигнатуре (например, сугубо продукционных типа ПОСЫЛКА $\rightarrow$ СЛЕДСТВИЕ), т.е. кортеж $T = \langle\Omega, \{\Phi\}, \{\rho\}\rangle$. Если правила вывода специально не оговариваются, то $T = \langle\Omega, \{\Phi\}\rangle$. Формулы Φ, входящие в определение теории *T*, называются аксиомами этой теории. Сами по себе они не истинны и не ложны, ибо базовое множество в теории отсутствует.

В модели М есть все, что есть в теории, и добавляется базовое множество М. Иными словами, ***модель – реализация теории***.

Модель ***М*** называется реализацией теории ***Т***, если:

1) сигнатура модели совпадает с сигнатурой теории;

2) после интерпретации каждого имени отношения в теории как одноименного отношения в модели каждая аксиома теории становится истинным высказыванием, т.е. выполняется для данной модели.

Таким образом, в рассматриваемой версии понятий, которая берется далее за основу, **ТЕОРИЯ** – это перечень названий отношений и свойств этих отношений, а **МОДЕЛЬ** – множество, на котором заданы соответствующие отношения и выполнены требуемые свойства.

При этом считается правомерным говорить как о формальных (формальные системы), так и о не вполне формализованных теориях и даже о неформальных (язык которых не определен).

Пример 2. Некто направляется в престижный клуб. Швейцар интересуется наличием у него «фульки». Что это такое? – Нечто тонкое, изящное, сделанное со вкусом и в то же время весомое и строгое. Такова теория «фульки». Она неформальна. Возможные модели: трубка с инкрустацией, портсигар, кошелек с деньгами и др.

СВЯЗЬ S-МОДЕЛЕЙ С ПОЗИЦИЕЙ ШРЕЙДЕРА

S-модель рассматривается как множество реализаций гипотетической системы с разным качеством моделирования либо как множество интерпретаций некоторой формально-подобной системы, построенной в процессе моделирования (пример – далее). ***В таком смысле сама модель является динамической развивающейся системой.*** Рост качества либо каждая новая интерпретация достигаются всегда с высокой эффективностью. Каждая найденная реализация (интерпретация) – это некоторое состояние модели.

Для характеристики множества реализаций (интерпретаций) системы воспользуемся понятием каркаса, введенным в для описания систем. Это кортеж $K = \langle\langle M,\alpha\rangle, \Omega_2, A\rangle$, где $\langle M,\alpha\rangle$ – модель в сигнатуре Ω_1; Ω_2 – сигнатура, в которой нет общих с Ω_1 имен отношений; A – аксиоматика в сигнатуре $\Omega = \Omega_1 \cup \Omega_2$. Модель-состоянием каркаса M_k называется одно из представлений $\langle M,\beta\rangle$ в сигнатуре Ω. Множество $\{M_k\}$ отвечает пониманию *S*-модели. При этом $\langle M,\alpha\rangle$ является как бы «тканью» (основой), на которую постепенно наносится «рисунок» – отношения из сигнатуры Ω_2.

Если найденное конструктивное описание системы определяет полное множество состояний модели, такая модель называется *устойчивой, или гомеостатичной.* Этот случай достаточно редок и возможен только для US-моделей. Чаще поиск очередного состояния модели представляет всякий раз самостоятельную задачу.

Системный гомеостаз – это способность системы сохранять динамическое равновесие (находиться в области функциональной устойчивости) при переходе от одного состояния к другому. В данном случае устойчивость понимается в смысле детерминированности перехода к новой эффективной реализации системы.

Элемент ⟨M,α⟩ – устойчивый конструктивный «муляж», требующий «оживления», чтобы стать одной из реализаций системы. Этот элемент неизменен для любых реализаций. Он присутствует в любой модели как следствие базовой идеи, сообщает модели некоторую устойчивость. Это значительно облегчает процесс S-моделирования.

Такая интегрированная основа выявляется согласно принятым постулатам и мировым тенденциям в данной прикладной области.

ОСОБЕННОСТИ S-МОДЕЛИ

Математически, S-модель трактуется как множество, на котором заданы соответствующие отношения (области в пространствах параметров) и выполнены требуемые свойства этих отношений.

Изначально не известно ни то, ни другое, ни третье. Все находится во взаимосвязи в едином процессе S-моделирования.В силу объективной неопределенности, при построении S-модели необходимо использовать ***эвристику***, что свойственно только естественному интеллекту. ***Полученная модель неформальна.*** *Но если она найдена, то дальнейшее исследование проводится строго дедуктивно.*

Конечной целью S-моделирования является разработка теоретически обоснованного конструктивного метода, т.е. процедуры синтеза. Эта процедура формируется путем модельных исследований ***(разработка S-модели),*** в ходе которых оптимизируются значения параметров в области, устанавливаются оценки достижимого качества моделирования и эффективности на множестве состояний модели.

Построение S-модели и ее исследование неразделимы, ибо са-ма модель находится в результате исследований как основы введения постулатов. Характерная черта S-моделирования – его итеративность.

Понятие устройства отождествляется с методом его синтеза. *Если устройство – это модель, то естественно задаться вопросом: какими свойствами оно должно обладать, чтобы моделирование было наиболее эффективным.* Иными словами, чтобы требуемое качество моделирования (воспроизведения функций системы) достигалось при минимальных аппаратных затратах или при заданной сложности устройства обеспечивалось наилучшее качество.

Знание указанных свойств позволит доопределить задачу синтеза и найти адекватный метод. Эти свойства могут быть выявлены в динамике моделирования в виде постулатов-аксиом теории, утверждающих достаточно проверенные идеи. Процесс *S*-моделирования рассматривается как многошаговый итеративный процесс, в котором взаимодополнительно проявляются как объяснительные посылки (теория), так и сам конструктивный метод (модель). Найденные в этом процессе аксиомы приобретают сугубо содержательный смысл. Поэтому точнее называть их постулатами.

Модель и теория становятся столь трудно разделимы, что их противопоставление теряет смысл. ***Это характерно для системотехники в целом.*** Здесь наиболее правомерно *интегрированное понятие модели-теории*. Процесс ее построения является творческим, т.е. неформальным в своей основе. **Эвристика играет решающую роль.**

Синтез – это процесс. Под процессом в кибернетике понимается последовательная смена состояний некоторого объекта или этапов решения некоторой задачи. Поэтому модель процесса необходимо включает *«модельную процедуру»*, а реализация *S*-модели дает *конструктивный метод*. Отсюда название – *конструктивное моделирование*. Для сравнительно несложных заданий построение *S*-модели подразумевает разработку *«ручной процедуры»* синтеза. Обычно это не требует полной структуризации знаний.

Формирование *«машинной процедуры»* автоматизированного синтеза связано с привлечением методов искусственного интеллекта (*AI* – Artificial Intelligence). Частично структурированная *S*-модель трансформируется в *AIS*-модель *(модель синтеза, адаптированная к искусственному интеллекту)* как совокупность структур знаний и данных, над которой определяется искомая процедура.

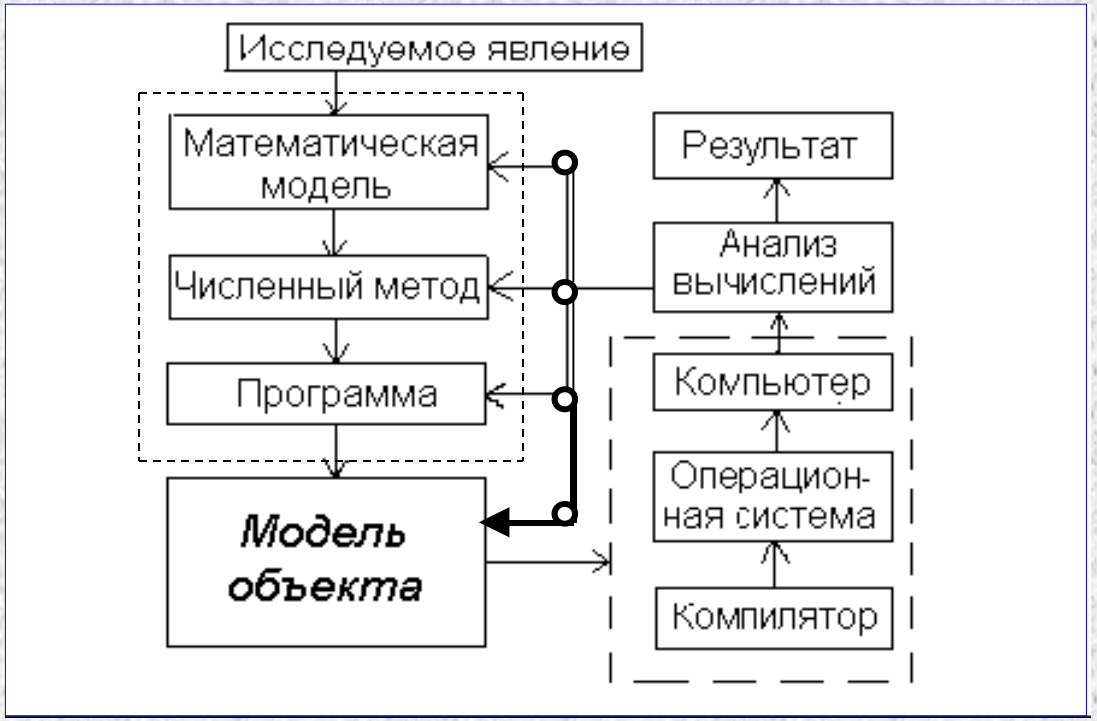
Еще одной задачей является выбор *инструментальных средств* и разработка их *интерфейса* с построенной *AIS*-моделью. Соответствующая программная система есть не что иное, как *интерпретатор экспертной системы синтеза*.

Процесс построения иерархических моделей наиболее сложен. ***Разница между внешней и внутренней IS-моделями та же, что между стратегией и тактикой.***

Выработка обоснованной **стратегической линии** в условиях недостаточности априорной информации происходит итеративно с привлечением элементов внутреннего моделирования. При этом ***главная роль отводится систематике накопленных знаний и модельному эксперименту.***

Процесс IS-моделирования включает *анализ результатов* ***вычислительного эксперимента*** над ***близкой к натурной программной моделью*** синтезируемого объекта.

Эксперимент проводится по схеме, показанной на рисунке. Под «Исследуемым явлением» подразумевается исследование *свойств синтезируемого объекта*. Часть схемы – «математическая модель, численный метод, программа» – относится к процедуре, *реализуемой на программной модели*. Другая ее часть – «компилятор, ОС, компьютер» – символизирует *используемую платформу*.



Разрабатываемую ***программную модель объекта*** приходится непрерывно корректировать по промежуточным результатам эксперимента. Такая коррекция связана всякий раз со значительными трудозатратами.

ПРОЦЕССЫ РАЗРАБОТКИ ПРОГРАММНОЙ МОДЕЛИ И ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА, ПРОВОДИМОГО ПО ЭТОЙ СХЕМЕ, НЕРАЗДЕЛИМЫ.

СИСТЕМЫ ИНФОРМАТИКИ

СИНТЕЗ АВТОМАТОВ ПО НЕФОРМАЛЬНОМУ ЗАДАНИЮ

В данном случае *(последовательностный алфавитный)* оператор системы задан тройкой {X, Z, L}, где L – отображение множества входных слов в алфавите X во множество выходных слов в алфавите Z. По условию *отображение автоматно*, т.е. существует абстрактный автомат определенного вида, не обязательно конечный. Оператор системы не формализован, т.е. язык задания достаточно широк. Область определения отображения бесконечна. *Длина входной последовательности не ограничена*. Это требует введения в процедуру абстрактного синтеза конечного автомата *элементов эвристики*.

Частную задачу моделирования решает

Теорема. Если автомат Мили синтезирован таким образом, что переход в любое его состояние s^k (k – номер такта) происходит только при одном значении выхода z^k, то каждое состояние автомата может быть специфицировано некоторой группой элементов события, отмеченного соответствующим значением выхода.

Это позволяет в конечном итоге ввести

Постулат (объектное определение автомата). Абстрактный автомат обладает следующими свойствами.

1. Это объект, определенный перечнем внутренних состояний и указанием порядка следования между выделенными состояниями на множестве ***изменений входа*** (x^{k-1} - x^k). При этом каждому полному состоянию автомата (x^k, s^{k-1}) отвечает свое значение выхода.

2. Внутреннее состояние автомата – объект, специфицированный кортежем <x^{k-1} – x^k, z^k, ИНДЕКС>. Этот кортеж определяет условия перехода в данное состояние. Компоненты атрибута ИНДЕКС представляют *значения параметров согласно заданию*.

Необходимость учета именно изменения входа (а не только его конечного значения) ***принципиальна. Элемент эвристики скрыт в определении атрибута*** **ИНДЕКС.**

Введенный постулат принят за основу построения соответствующей US–модели, множество состояний которой определено ее применением ко множеству конкретных задач. *Такая модель частично устойчива, ибо содержит элементы эвристики.*

Сформулированный постулат определяет устойчивую основу *S*-модели *(язык спецификации состояний)* как некоторую ***формально-подобную*** систему:

1) задан алфавит как множество символов **V, Z, I** : {V (var x = $x^{k-1} - x^k$), Z (z^k), I (ИНДЕКС)};
2) определен допустимый вид формул: $\Phi = < V, I, Z >$;
3) имеется одна аксиома начального состояния $\Phi_0 = <-, I_0, ->$, если это состояние названо;
4) рекурсивно обозначены правила вывода: $\Phi_i , V_j \supset \Phi_r , r = r (i, j)$. Эта запись читается так: если автомат находится в состоянии Φ_i , то под действием изменения входа V_j он переходит в состояние Φ_r. При этом r зависит как от i, так и от j.

В отличие от строго формальной эта система не допускает каких-либо манипуляций символами, ибо ИНДЕКС и правила вывода в ней *только обозначены* и всякий раз уникальны. Поэтому она является всего лишь *формально-подобной устойчивой основой моделирования* **⟨M,α⟩**, по-отдельности интерпретируемой для каждой задачи.

Тем не менее, на ее основе ***развит подход к синтезу автомата по неформальному заданию.*** В данном случае множество состояний *US*-модели определено его применением ко множеству конкретных задач.

ВНЕШНЕЕ МОДЕЛИРОВАНИЕ КЛАСТЕРОВ КОНСЕРВАТИВНЫХ БД

Гипотетическая система. Ее назначение (оператор системы) – обслуживание потока запросов к консервативной базе данных в реальном времени по схеме «клиент – сервер».

Цель моделирования – достижение возможно высокого качества представления этой системы на платформе вычислительных кластеров при заданном числе процессоров N.

Задача внешнего моделирования – выяснить, какой должна быть архитектура консервативной СУБД на этой платформе.

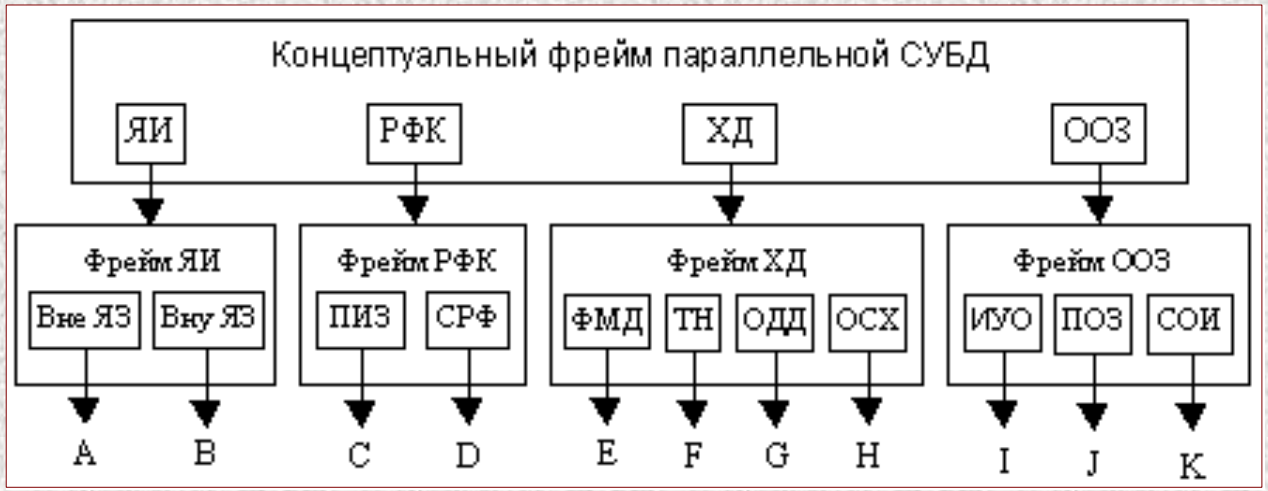
Выделяются следующие *уровни иерархии*:

- Языковый интерфейс.
- Стратегия распределения функций между компонентами.
- Физический уровень (уровень хранения данных).
- Организация обработки запросов.

На каждом уровне возможен альтернативный выбор решений.

ФРЕЙМОВОЕ ПРЕДСТАВЛЕНИЕ

Процесс внешнего моделирования сводится к решению указанных альтернатив согласно ***фреймовой модели этого процесса*:**



На верхнем уровне иерархии размещаются фреймы языкового интерфейса (ЯИ), распределения функций между компонентами (РФК), хранения данных (ХД), организации обработки запросов (ООЗ). Далее идут дочерние фреймы: к ЯИ – выбора типа внешнего и внутреннего языка; к РФК – выбора стратегии параллельного исполнения запросов и способа распределения функций; к ХД – выбора физической модели данных, типа накопителя, метода доступа к данным и структуры хранения; к ООЗ – выбора между одно- и двухуровневой обработкой, плана обработки и среды обмена. По стрелкам A, B, …, K следуют возможные альтернативы выбора решений для фреймов Вне ЯЗ, Вну ЯЗ, …, СОИ.

УСТОЙЧИВАЯ АРХИТЕКТУРНО-ФУНКЦИОНАЛЬНАЯ ОСНОВА

Пусть в перечень условий, при которых решается задача внешнего моделирования, включены (по умолчанию) условия отсутствия коллизий при межпроцессорных обменах (синхронный мониторинг), предпочтений среди альтернатив в ФМД и ОСХ, возможной простоты реализации исполнительного уровня (использование на этом уровне инструментальной СУБД MySQL).

Тогда, с учетом мирового опыта построения машин баз данных, UNIX-кластеров, тенденций использования перспективных инструментальных (SQL, LINUX, MPI) и сетевых средств при минимуме программных доработок, постулированного плана обработки по схеме «Select – Project – Join», получаем систему правил как элементов неформальной теории параллельных СУБД консервативного типа. Эта система формирует интегрированный

Постулат 1.2. *Устойчивая архитектурная основа кластеров консервативных баз данных определена продукцией*

A, B, C, D, E, F, G, H ⊃ W.

Здесь:

W – искомая архитектура кластера консервативных баз данных;

A – внешний язык запросов – SQL;

B – ***внутренний язык запросов*** – MySQL;

C – общая стратегия обработки запросов: ***множество процессоров на один запрос***;

D – используются одноканальные жесткие диски (НМД) с плавающими головками;

E – ***база данных распределяется*** между несколькими НМД с применением механизма ***хеширования***;

F – имеются ***нижний*** (операции Input, Select, Project) и ***верхний*** (операции Join, Sort) уровни обработки;

G – ***план обработки запроса регулярен***. Исходный SQL-запрос расщепляется на MySQL-фрагменты исполнительных уровней;

H – используется стратегия MPP с обменом сообщениями, реализуемая на базе стандартных скоростных сетей с коммутатором в операционной среде Linux.

Введенный постулат полностью решает внешние альтернативы для фреймов ЯИ, РФК, ХД, ООЗ и определяет тем самым ***устойчивую архитектурную основу IS-модели в целом.***

Согласно постулату, кластер консервативных баз данных включает: Host ЭВМ, процессоры I/O_r и $Join_j$. Host ЭВМ реализует функции мониторинга и претрансляции запросов. Общее число физических процессоров в кластере (включая Host) $N=2n+1$, $n=1, 2,\ldots$

Верхний исполнительный уровень образуют процессоры $Join_j$ (выполняют операции *join, project*) числом p. ***Нижний*** – процессоры I/O_r (операции *input, select, project*) числом $q=h-p$, где $h=N-1=2n$.

База данных распределена в дисковом пространстве I/O_r путем хеширования записей отношений по основному ключу. Меняя значение p при неизменном h, получаем ряд ***конфигураций*** кластера.

Разработка программной модели параллельной СУБД консервативного типа и исследование ее поведения при различных n, k=q/p, объемах БД и параметрах потока запросов является предметом внутреннего S-моделирования.

АССОЦИАТИВНАЯ СТЕГОЗАЩИТА ДАННЫХ КАРТОГРАФИИ

ЗАДАЧА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ГИС формулируется следующим образом. Задан блок закодированных тематических карт. Заголовок блока: <ИМЯ_ТЕМЫ>. Имя карты: <ГЛОБАЛЬНЫЕ_КООРДИНАТЫ_КАДРА>. Кадр отображает участок определенных размеров на карте местности. Тематическая карта формируется как отношение с кортежами: <ИМЯ_ОБЪЕКТА><ЛОКАЛЬНЫЕ_КООРДИНАТЫ_ОБЪЕКТА>.

По условию мощности множеств имен и градаций значений координат не превышают величины γ , что допускает единообразное кодирование имен и координат словом длины $k \geq \log^{\gamma}$ в ***алфавите почтовых индексов*** при сохранении семантических особенностей кодов разных уровней. Любая из 10 букв этого алфавита представлена ***двоичными матрицами эталона и маски*** размерами $m \times n$ бит, где m – число столбцов, n – число строк матриц.

После рандомизации получается множество тематических *стегокарт*, которое составляет ***защищенную картографическую базу данных***. Роль ***базы знаний – стегоключа*** выполняет соответствующий ***набор масок.*** Знание ключа необходимо для идентификации стегокарт и раскрытия их содержимого. Требуется найти **МЕТОД ЗАЩИТЫ КАРТОГРАФИЧЕСКИХ ДАННЫХ, УРОВЕНЬ СТОЙКОСТИ КОТОРОГО НЕ НИЖЕ ДОКАЗУЕМОГО.**

Гипотетическая система. Предполагается, что факт передачи стеганограмм противнику известен, но нельзя допустить их несанкционированное распознавание. Соответственно за гипотетическую систему в данной задаче принимается идеальная система картографической защиты со свойством ***безусловной стойкости*** *(совершенной секретности)* по **Шеннону**.

Критерий Шеннона. Совершенная секретность определяется условием: ***для всех передаваемых сообщений их апостериорные вероятности должны быть равны априорным вероятностям независимо от величины этих последних.*** В таком случае перехват сообщения не дает противнику никакой иформации.

S-модель системы – искомое представление гипотетической системы – **практически стойкий способ стегозащиты**.

Устойчивая основа модели – предложенный **базовый алгоритм маскирования**. Использование в нем двумерно-ассоциативного механизма маскирования (*морфологическое ограничение)* определяет *множества* и *отношения.*

Множества. В данном случае ***S*-модель** определена на множестве наборов композиционных элементов <ЭТАЛОН><МАСКА>, компоненты которых суть бинарные матрицы одинаковых размеров mxn. Мощность любого набора равна мощности алфавита символов, используемых для представления имен объектов и их координат. При рассматриваемом десятичном кодировании она равна 10.

Отношения – полная совокупность наборов, удовлетворяющих условию *взаимной непокрываемости любой пары троичных эталонов*. Оно диктуется требованием однозначности санкционированного распознавания. *Достаточное условие такой непокрываемости – различие хотя бы в одном значащем элементе* x^{t}_{pq} *троичных матриц* X^{t1} *и* X^{t2}, $t1 \neq t2$. Элементы эталона X^{t}, не подлежащие маскированию, определены единичными компонентами *инверсной матрицы масок* $\overline{M}^{\,t} = \left|\overline{m}^{\,t}_{pq}\right|$ для этого эталона.

***S*-моделирование** – непрерывно продолжается. По имеющимся результатам сформулирована *система постулатов* как декларация свойств ***S*-модели**. Она положена в основу разработки *конструктивного метода* стегозащиты.

Постулат 1. *Генерируемый набор масок случаен. При этом для обеспечения «максимального число степеней свободы» в процессе рандомизации число единиц инверсной матрицы масок* $\overline{M}^{t}$ *для любого t-эталона должно быть близким к минимально возможному.*

Указанное число единиц определяется условием дихотомизации любой пары троичных эталонов в сгенерированном наборе по одному значащему (незамаскированному) биту.

Размеры mxn матриц кодовых символов должны быть *достаточными* для того, чтобы поиск подходящей рандомизации из условия требуемой стойкости занимал *приемлемое время*.

Постулат 2. *Если в итоге применения всевозможных ключей к любому стегокластеру получаем неединичное подмножество равноправдоподобных результатов распознавания, то использованный метод стегозащиты безусловно стоек* (логическая трактовка критерия Шеннона).

Постулат 3. *Достаточным условием удовлетворения требований постулата 2 является проведение такой рандомизации, что при полноте множества имен (координат)и ограниченном переборе ключей любой стегообъект (стегокоордината) представит все это множество.*

ЕЩЕ РАЗ -
О ПОСТУЛАТАХ !

О ПОСТУЛАТАХ

Характерной особенностью S-модели является постулирование свойств множества эффективных реализаций системы как основа теории и предпосылка разработки конструктивного метода. Введение постулатов – шаг весьма ответственный и многотрудный. Он целесообразен, только если разработка конструктивного метода на их основе показывает его ***перспективность для своего времени,*** а сам метод ***не укладывается в рамки существующей теории.***

Обычно требуемый детерминизм достигается при постановке задачи введением разного рода определений и ограничений. ***Постулаты делают то же самое, но декларируют это как закономерности,*** выявленные путем обобщения накопленного опыта или из специальных исследований, т.е. **нестрого индуктивно**. В силу последнего ***система постулатов как элементов объяснительной теории должна быть открытой.***

«Потенциальная бесконечность систем объяснений и их неизбежная незавершенность, т.е. открытость для дальнейших объяснений» – таков философский аспект правомерности корректив постулатов.

Ю.А. Шрейдер называет подобные элементы ***аксиомами*** *(«идеи, воплощаемые в моделях»).* Безусловно, наличие базовой идеи в творческом процессе необходимо. Однако ***содержательный смысл найденных закономерностей требует считать их постулатами.***

Выбор постулатов далеко не формален. *Они должны отвечать ключевым свойствам найденного метода («идеи, воплощаемые в моделях») и одновременно – быть адекватны предмету синтеза.* Последнее устанавливается нестрогой индукцией на основе наблюдаемых фактов либо умозрительно.

Двоякая природа постулата – источник сомнений в его адекватности. В строгом смысле, адекватность означает соответствие (релевантность) плюс достаточность. Говорить о достаточности постулата в условиях нестрогой индукции математически некорректно. Максимум, на что можно рассчитывать в данном случае, это – ***«хорошее» соответствие.***

Объяснить суть такого соответствия и почему только оно выводит нас за рамки **«еще одного метода среди множества других, ему подобных»**, очень непросто. Как писал известный математик **Пойа**, при нестрого индуктивном подходе **«то, что кажется достаточно правдоподобным одному, другому таковым совсем не представляется»**. ***Безусловно убедителен только мировой опыт.***

Мы полностью согласны с тем, что ***использование формальных аксиоматических систем в конкретных приложениях неконструктивно.*** Каждому явлению релевантна своя модель со своим математическим аппаратом. То и другое выявляется всякий раз неформально в результате серьезных исследований с использованием накопленного опыта.

Таков смысл «хорошего» соответствия, путь достижения которого показывает сформулированная концепция. **Глубокая внутренняя убежденность исследователя в своей правоте, достигаемая эффективность найденного метода** – немалая компенсация за возможную неудачу объяснения.

ПЛОХО, ЕСЛИ НЕТ ТОГО ИЛИ ДРУГОГО !