



УДК 681.3

Г.С.ТЕСЛЕР

---

## КОНЦЕПЦИЯ СОЗДАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СРЕДСТВ С ВЫСОКИМ УРОВНЕМ ОТКАЗОУСТОЙЧИВОСТИ

### 1. Введение

Современный уровень развития вычислительных средств и широкое их внедрение во все области деятельности человека все более требуют создания вычислительных средств с высоким уровнем отказоустойчивости. Высокий уровень отказоустойчивости в принципе желателен для всех видов вычислительных средств, но это требует значительных дополнительных технических, программных, финансовых затрат. В связи с этим вычислительные средства с высоким уровнем отказоустойчивости применяются, главным образом, в критических областях, где отказ вычислительных средств приводит к тяжелым последствиям. В основном эти области можно характеризовать следующими тремя факторами:

– отказ вычислительных средств угрожает жизни людей и ведет к большим материальным потерям (транспортные средства различных видов, системы обороны, атомные электростанции, жизнеобеспечение лечебных учреждений и т.д.);

– отказ вычислительных средств влечет за собой тяжелые экономические последствия (автоматические и автоматизированные технологические процессы в промышленности и энергетике, системы связи, банковские системы и т.д.);

– отказ ведет к нарушению функционирования сложных технических объектов (необслуживаемые космические аппараты, подводные, надводные, воздушные и земные автономно функционирующие объекты и т.д.).

Этот перечень можно было бы продолжить, но и вышеприведенные примеры показывают актуальность и важность рассматриваемой области знаний.

Имеются различные определения понятия отказоустойчивости. Интегрируя их, можно дать следующее определение: отказоустойчивость – свойство вычислительной системы сохранять свою работоспособность и функциональные возможности в полном или умеренном объеме при наличии отказов и / или сбоев одной или нескольких компонент системы. Необходимым условием достижения отказоустойчивости является наличие в системе различных видов избыточности, процедур обнаружения и устранения возникших сбоев и отказов и соответствующей организации системы.

### 2. Постановка проблемы

В настоящее время достаточно хорошо изучены вопросы отказоустойчивости и живучести СВТ за счет использования их надежности, резервирования, методов и средств технического, диагностического обслуживания, их реконфигурации, технического обслуживания и ремонта [1,2]. Однако изучение отдельно друг от друга этих средств не приводит к существенному повышению надежности и отказоустойчивости сложных систем, каковыми являются современные вычислительные системы.

Данная проблема будет стоять еще более остро для СВТ уже ближайшего будущего. Поэтому для решения этой проблемы, безусловно, необходимо учесть весь богатый опыт, накопленный в данной области за предыдущие годы. Но для резкого прорыва в решении этой проблемы целесообразно учесть и весь опыт, накопленный природой в процессе эволюционного развития объектов живой природы вообще и человечества, в частности.

Такой подход связан, прежде всего, с обобщенным законом зеркального отображения [3,4] и тем, что в результате эволюции человек, как вершина этого процесса, достиг, с точки зрения, отказоустойчивости весьма ощутимых преимуществ перед сложными техническими системами. Это связано с тем, что одним из фундаментальных свойств биологических систем являются высокие надежность и отказоустойчивость, позволяющие им нормально функционировать, выживать и воспроизводиться. Это свойство биологических систем проявляется на всех уровнях иерархии биосферы, начиная с макромолекул и кончая популяцией. Именно поэтому биологические системы в процессе эволюционного развития достигли оптимального уровня совершенства, а это позволяет утверждать, что надежность и отказоустойчивость биологических систем гораздо выше, чем в любой сложности технической системы. При этом эти системы обладают:

- высокой надежностью, точностью и устойчивостью;
  - возможностью параллельной работы элементов (клеток) и более сложных образований;
  - резервированием на всех уровнях функционирования и управления;
  - дублированием регулирующих механизмов и исполнительных функций путем использования разнообразных рабочих процессов, многократного повторения информации и дублирования процесса передачи информации;
  - взаимным контролем протекающих процессов;
- вероятно - детерминированным взаимодействием на всех уровнях функционирования и управления;
- иерархичными уровнями управления и обработки информации;
  - параллельными, вертикальными и горизонтальными связями;
  - избыточностью элементов, структур и т.д.;
  - возможностью передачи функций отказавшей системы другой, исправно функционирующей;
  - осуществлением принципов целесообразности, рациональности, адаптивности, системной экономичности, отбора, самоорганизации типа "проб" и "ошибок", эволюционного развития и т.п.;
  - устойчивостью на основе динамического иерархического баланса и многими другими особенностями, механизмами и способами.

Помимо этого, на основе действия принципа смешанного экстремума [4] в процессе развития эволюционного развития биологических и антропогенных систем, наряду с их усложнением, наблюдается сочетание структурной и функциональной симметрии (дублирования) и асимметрии (отсутствие дублирования), а также универсальности (сложности) и специализации (простоты), способствующих уровню устойчивости и эффективности этих систем.

Кроме того, для обеспечения отказоустойчивости этих систем важное место занимает контроль правильности их функционирования. При этом контроль осуществляется, в основном, в точках бифуркации (разделения) протекающих в системе процессов. При этом осуществляется контроль попадания основных параметров процесса в заданный интервал, проверка на "вырождаемость" и т.д. В контроле как антропогенных, так и биологических систем, важную роль играет анализ информации о протекании процессов.

Рассмотрим способы и механизмы обеспечения надежности и отказоустойчивости биологических систем [5] на разных иерархических уровнях.

На уровне макромолекул надежность и отказоустойчивость обеспечиваются совместным действием механизмов редупликации макромолекул и мутаций.

На клеточном уровне и уровне одноклеточных организмов надежность обеспечивается за счет деления клеток и кроссинговера.

На уровне организма - путем размножения и рекомбинации хромосом.

На уровне популяции - использование генофонда вида и генотипов отдельных особей.

На уровне органов организма - за счет использования структурно-функционального резервирования клеток.

На уровне физиологических систем - путем взаимного перекрытия функций, выполняемых органами, и/или дублированием органов.

На уровне систем внутренней сферы - компенсаторные свойства систем для поддержания жизненно важных переменных за счет интенсификации работы других смежных систем.

На уровне мозга и взаимодействия с внешней средой - используется обучаемость для выработки стереотипного поведения.

На уровне отдельного организма - используются механизмы адаптации.

В биологических организмах действуют принципы самосохранения, целесообразности и адаптивности, которые направлены на сохранение биологического вида.

Обращает на себя внимание наличие избыточности состава живых структур, выполняющих ту или иную функцию. Такая избыточность живых структур не случайна.

Особо большое значение в биологических системах имеет информационное дублирование. Так, нарушение связи и управления в каком-либо звене чаще всего ведет только к временному нарушению определенной функции, которая затем восстанавливается посредством включения в работу обходных путей. Именно это говорит о необходимости достижения высокого уровня отказоустойчивости. Поэтому в вычислительных средствах необходимо использование сетевого взаимодействия и функционального дублирования.

Отметим, что избыточность в биологических системах осуществляется на вещественном, энергетическом и информационном уровнях. Помимо этого, свойство избыточности биологических систем лежит в основе механизмов адаптации и обучаемости. Учитывая закон зеркальной симметрии и вышеперечисленные свойства биологических систем в части устойчивости, целесообразно адаптировать их для вычислительных средств, обладающих повышенным уровнем отказоустойчивости.

### **3. Принципы создания высоконадежных отказоустойчивых вычислительных систем**

Учитывая обобщенный закон симметрии [4,5], отражающий адекватность и направленность эволюционного развития биологических объектов и средств вычислительной техники, можно сформулировать принципы создания отказоустойчивых вычислительных средств. При этом необходимо учесть, что любой общий закон, когда его хотят применить к какой-либо конкретной области знаний, приобретает свои характерные уточнения, характеризующие эту область применения. Учитывая вышеизложенное, основные принципы, которым должны отвечать вычислительные средства с высоким уровнем отказоустойчивости, состоят в следующем:

1. Преемственность способов, средств и механизмов, которые использовались для обеспечения отказоустойчивости.
2. Обеспечение достаточного уровня избыточности на уровне элементов, узлов, блоков и т.п.
3. Обеспечение достаточного уровня избыточности выполняемых функций.
4. Обеспечение достаточного уровня взаимного контроля правильности функционирования как отдельных частей вычислительной системы, так и системы в целом.
5. Обеспечение сетевого взаимодействия как внутреннего (параллельные работы), так и внешнего.

6. Обеспечение иерархичности уровня управления системы с использованием как горизонтальных, так и вертикальных связей.

7. Использование перспективной элементно-технологической базы для достижения высокой надежности и отказоустойчивости системы.

8. Обеспечение достаточного дублирования функций и процессов.

9. Создание эффективной структурно-функциональной организации процесса вычислений, обеспечивающей высокий уровень отказоустойчивости.

10. Обеспечение адаптации и адекватности вычислительной системы и окружающей среды по степени сложности и открытости к модернизации.

11. Обеспечение достаточного уровня надежности вычислительных средств с использованием динамического, иерархического баланса необходимых ресурсов.

12. Использование интеллектуального уровня контроля вычислительного процесса и управления для обеспечения высоких показателей уровня отказоустойчивости.

13. Обеспечение сочетания магистрального и сетевого взаимодействия как внутри, так и вне вычислительной системы.

14. Обеспечение эффективного контроля правильности функционирования вычислительных средств.

Обобщенный минимаксный критерий эффективности, удовлетворяющий вышеприведенным требованиям, может быть представлен в следующем виде [7]:

$$Z = \min_{y \in Y} \max_{x \in X} F(x, y),$$

где  $X = (x_1, x_2, \dots, x_n)$ ,  $Y = (y_1, y_2, \dots, y_m)$ .

В качестве  $x_1, x_2, \dots, x_n$  могут выступать следующие параметры:

$x_1$  - производительность;

$x_2$  - надежность;

$x_3$  - отказоустойчивость;

$x_4$  - количество и вид выполняемых функций;

$x_5$  - точность вычислений;

$x_6$  - пропускная способность каналов;

$x_7$  - емкость оперативной памяти;

$x_8$  - емкость долговременной памяти;

$x_9$  - характеристики загрузки компонентов системы;

$x_{10}$  - разрешающая способность дисплея;

$x_{11}$  - количество портов;

$x_{12}$  - характеристики условий эксплуатации и т.д.

В качестве  $y_1, y_2, \dots, y_m$  могут выступать следующие параметры:

- У<sub>1</sub> - стоимость вычислительных средств и/или ее компонент;
- У<sub>2</sub> - потребляемая мощность;
- У<sub>3</sub> - массо-габаритные характеристики;
- У<sub>4</sub> - время обработки прерываний;
- У<sub>5</sub> - величина коэффициента готовности к эксплуатации;
- У<sub>6</sub> - время выполнения основных операций;
- У<sub>7</sub> - время запаздывания;
- У<sub>8</sub> - время обнаружения сбоя и/или ошибки системы;
- У<sub>9</sub> - время исправления ошибки и т.д.

Как показано в работе [4], вычислительные средства с сетевым взаимодействием по форме наиболее адекватны биологическим системам в части надежности и устойчивости. Идеология сетевого взаимодействия внутри отказоустойчивых вычислительных средств необходима также и в связи с необходимостью создания разнообразных комбинаций элементов и функций системы. Благодаря этому появляются дополнительные возможности по обнаружению и парированию возникших в системе отказов и сбоев. Помимо этого, целесообразно использование перспективной элементно-технологической базы, основанной на молекулярных, квантовых и оптических технологиях [6]. Необходимо использовать семантические и функциональные уровни контроля и дублирования, а также вероятностно-детерминированные модули обнаружения и парирования сбоев и отказов на основе анализа текущих "образов" функционирования вычислительной системы.

Обращает на себя внимание то, что в ряде принципов присутствует термин "достаточный". Это обстоятельство и ряд других понятий тесно связаны с комплексным критерием эффективности. Такой критерий должен отвечать следующим требованиям:

- быть многофакторным [7];
- отвечать принципу смешанного экстремума [5];
- отвечать оптимизации Парето;
- отвечать принципу иерархического динамического баланса [8];
- основываться на игровых стратегиях поиска смешанного экстремума, вместо традиционно используемого детерминированного подхода использовать устойчивые и эффективные компромиссы [9].

#### **4. Роль базисов вычислительной техники и избыточности в решении проблемы отказоустойчивости**

Как видно из вышеизложенного, решение проблемы отказоустойчивости является достаточно сложным и многогранным. Понятно, что в одной статье нет возможности рассмотреть все факторы, влияющие на повышение уровня отказоустойчивости. Поэтому в данном разделе рассмотрим только достаточно важные, с нашей точки зрения, вопросы. Известно [10], что с точки зрения производительности, интенсификации процесса вычислений, адаптации к условиям применения и отказоустойчивости играют базисы вычислительной техники элементно-технологический, организационный, алгоритмический и информационный. В таблице 1 представлена связь базисов вычислительной техники с интенсификацией процесса вычислений, адаптацией к условиям применения, отказоустойчивостью и балансом требований, предъявляемых к средствам вычислительной техники.

Таблица 1

Базисы	Интенсификация процесса вычислений	Адаптация к условиям применения	Отказоустойчивость	Баланс требований
1	2	3	4	5
Элементно-технологический	Повышение частотных свойств, уменьшение энергопотребления. Использование конвейерной обработки	Возможность перехода в режим покоя для уменьшения нагрева БИС, потребляемой мощности и увеличения времени наработки на отказ. Понижение тактовой частоты по эффекту аналогично режиму покоя. Использование адаптивной архитектуры для увеличения загрузки устройств обработки информации и повышения коэффициента полезного действия компьютера. Механизмы обнаружения и парирования отказов и сбоев, реализованные аппаратно	Повышение надежности элементов и узлов как за счет использования современных технологий изготовления БИС, так и за счет использования передовых физико-биологических эффектов. Включение в компьютер аппаратных средств контроля и обнаружения и парирование отказов. Использование аппаратной, временной и других видов избыточности	Использование многокритериальных показателей эффективности с преобладанием наиболее важных для данного применения показателей (производительность, надежность, отказоустойчивость, стоимость, массогабариты и т. д.)
Организационный	Эффективная организация процесса вычислений. Уменьшение затрат различных видов ресурсов, включая и саму систему управления. Увеличение функциональных возможностей системы управления и, как следствие, всей вычислительной системы	Использование программируемой архитектуры и структуры. Использование RISC-архитектуры (адаптация к внутренним условиям применения); VLIW-архитектуры для оптимизации загрузки вычислительных средств. Использование идеи адаптации и сетевого взаимодействия для обеспечения саморазвития и решения интеллектуальных задач. Использование идей организации материального производства для выпуска массовой и индивидуальной продукции	Использование самоорганизации и различных видов избыточности для парирования возникших сбоев и отказов в технических средствах и программном обеспечении	Использование многокритериальных показателей эффективности. Устранение «узких мест» в вычислительном процессе
Информационный	Повышение пропускной способности каналов. Уменьшение цикла обращения к памяти. Увеличение объема всех видов памяти до таких размеров, чтобы она не была «узким местом» в процессе вычислений. Увеличение коэффициента полезного действия канала (уменьшение количества служебной информации, разумное ее сжатие, совмещение во времени передачи разнообразной информации, повышение надежности). Использование системы проблемно-ориентированных счислений	Широкое использование результатов прошлого труда (заранее рассчитанных таблиц, однократная их передача, широкое использование шаблонов, операций по умолчанию и т.д.). Использование укороченных данных (работа с инкрементной информацией). Использование переменной разрядности в процессе вычислений	Использование кодов с обнаружением и исправлением ошибок. Использование аппаратной, информационной, временной и других видов избыточности	Использование многокритериальных показателей эффективности

Особо необходимо остановиться на таком важном факторе организационного базиса, как возможность перестраиваемости структуры и архитектуры вычислительной системы. Это связано с тем, что отказоустойчивость и повышение производительности вычислительных средств в значительной степени зависят от возможности использования перестраиваемых либо комбинированных структур и архитектур. Благодаря такой динамичной перестраиваемости происходит адаптация вычислительной системы к внутренним и внешним условиям функционирования (сбоям, отказам, решаемым задачам и т.д.). Для маскирования возникших в

системе сбоев и отказов используются дублирование аппаратных средств, выполняемых функций и информационных средств. Наиболее удобным для реализации такого подхода являются обеспечение параллельных вычислений и сетевое взаимодействие, позволяющие наиболее эффективно использовать все виды имеющейся в системе избыточности. При этом весьма эффективным является подход, основанный на выявлении искажения информации в результате возникновения сбоя либо отказа.

Выше уже отмечалась та важная роль, какую играют вид и способы использования избыточности для повышения уровня отказоустойчивости. В табл. 2 приведены некоторые из таких подходов.

Таблица 2

№ п/п	Вид избыточности	Способ использования избыточности	Этапы, на которых используется данный вид избыточности	Конкретизация условий для использования данного вида избыточности
1	2	3	4	5
1	Аппаратная	Резервирование отдельных компонент системы и подсистем (горячее, холодное, комбинированное) - элементное, групповое	Разработка и комплексирование системы	Однородность компонент технических средств
2	Структурная	Построение структуры, позволяющей реконфигурацию системы или замещение отказавшего элемента	Разработка и комплексирование системы	Однородность структуры и средств обнаружения отказов и сбоев
3	Информационная	Использование кодов, алгоритмов для каналов связи и памяти для обнаружения и исправления ошибок; зеркальное отображение информации в разных блоках памяти и т.д.	Разработка системы	Избыточность производительности, объемов памяти и другой аппаратуры, а также разработка специальных программ
4	Алгоритмическая	Использование алгоритмического разнообразия и механизмов адаптации к условиям применения средств генерирования и контроля процесса вычислений	Разработка, модернизация и эксплуатация системы	Наличие глубоких и разнообразных специальных знаний о реализуемом классе алгоритмов и их свойствах
5	Программная	Аналогично алгоритмической избыточности с добавлением привязки к новой конфигурации вычислительных средств	Разработка, модернизация и эксплуатация системы	- " -
6	Функциональная	- " -	- " -	- " -
7	Нагрузочная	Использование технических и других средств в облегченном режиме, что позволяет повысить показатели их надежности	Разработка системы	Использование высокотехнологичных наукоемких элементов системы в облегченных режимах эксплуатации по сравнению с паспортными
8	Эксплуатационная (прогнозная, материалоёмкая, температурная, вибронагрузочная, радиационно-стойкая, энергетическая и т.д.)	Использование технических и других средств в облегченном режиме, что позволяет повысить показатели их надежности	Разработка системы	- " -
9	Надежностная	Позволяет уменьшить другие виды избыточности	- " -	- " -
10	Семантическая	Сравнение поточных «цифровых» образов контролируемых характеристик; использование избыточности, смысловых конструкций (подобно тому, как это делается в программировании – семантиче-	Разработка, модернизация и эксплуатация системы	Наличие технической и функциональной избыточности, параллельные вычисления и

		ская сеть, денотационная семантика, включающая оценочные функции и т.д.		сетевое взаимодействие
11	Вероятностная (статистическая)	Получение контролируемых характеристик как вероятностных (типа мат. ожидания, медианы, доверительного интервала и т.д.)	- " -	Наличие технической, алгоритмической и функциональной избыточности, параллельных вычислений, сетевого взаимодействия и/или соответствующей элементно-технологической базы, включая квантовые технологии

В работах [11-15] приведены другие подходы к решению проблемы надежности и отказоустойчивости.

### Выводы

1. На основе анализов средств и механизмов, которые обеспечивают высокую надежность и устойчивость биологических систем с учетом обобщенного закона зеркальной симметрии, разработаны базовые принципы построения вычислительных средств с высоким уровнем отказоустойчивости.
2. Предложен минимаксный критерий оценки эффективности вычислительных систем, который базируется на многокритериальном подходе и игровых стратегиях поиска оптимизма на основе использования эффективных и устойчивых компромиссов.
3. Показано, что наиболее эффективным способом достижения высокого уровня отказоустойчивости СВТ является использование широкого спектра видов избыточности и средств, заложенных в элементно-технологическом, организационном, информационном и алгоритмическом базисах.

### СПИСОК ЛИТЕРАТУРЫ

1. Державний стандарт України (ДСТУ) 2506-94. Відмовостійкість і живучість. Загальні технічні вимоги / Розробники: В.А.Романов, В.П.Стрельников, В.Д.Шпак та інш.
2. ДСТУ 2504-94. Відмовостійкість і живучість. Методи випробувань / Розробники В.А.Романов, В.П.Стрельников, П.С.Колчан.
3. Теслер Г.С. Перспективы развития вычислительных средств с сетевым взаимодействием //Математические машины и системы. -2001.- №1,2.- С. 3-11.
4. Теслер Г.С. Принципы смешанного экстремума как основа эволюционного развития вычислительных средств // Математические машины и системы. -2001.- №3,4 – С.7-9
5. Словарь по кибернетике / Под ред. В.С. Михалевича Киев: Гл. ред. УСЭ, 1989.- 751 с.
6. Затучная Ж. Назад, в будущее // Компьютерные ведомости .-№2.- С.21-28.
7. Теслер Г.С. Интенсификация процесса вычислений // Математические машины и системы. - 1999. - №2.- С. 25-37.
8. Теслер Г.С. Концепция построения постиндустриального информационного общества // Математические машины и системы. -2000.-№2,3 - С.185-194.
9. Моисеев Н.Н. Математика ставит эксперимент. – Москва: Наука, 1979.- 223 с.
10. Теслер Г.С. Место и роль алгоритмического базиса в решении проблемы производительности // Математические машины и системы. -1997. №1.- С. 25-33.
11. Погребинский С.Б., Стрельников В.П. Проектирование и надежность многопроцессорных ЭВМ. - Москва: Радио и связь,1988.-168 с.
12. Литвинский И.Е. Обеспечение безотказности персональных ЭВМ. - М. Радио и связь, 1993. - 208 с.
13. Кокс Д.Р., Смит В.Л. Теория восстановления.- Москва: Сов. радио, 1967. - 298 с.
14. Вульман И.Д. Повышение надежности и эффективности РЭА на основе использования избыточности с проведением восстановительного контроля // Надежность и контроль качества. - 1991. -№11. -С.34-40.
15. Смирнов Н.И., Широков Б.Б. Оценка безотказности интегральных микросхем. - Москва: Радио и связь, 1983.- 104 с.