УДК 681.32.019

Г.С. ТЕСЛЕР

РЕШЕНИЕ ПРОБЛЕМЫ ГАРАНТОСПОСОБНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ В АСПЕКТЕ БАЗИСОВ КОМПЬЮТЕРНОЙ НАУКИ

Abstract: *The methods and means of element-technological, information, program-algorithmical and organization basises in deciding the problem of dependability of CS are considered. The particular attention was paid to system-cybernetic approach in deciding this problem. Among considered means for providing dependability CS there are used the following: regular and crisis controlling, monitoring resources and information flours, functional doubling, net interconnection between components CS and others.*
Key words: *dependability, reliability, availability, integrity, technology, computer system.*

Анотація: *Розглянуто методи та засобі елементно-технологічного, інформаційного, програмно-алгоритмічного і організаційного базисів у вирішенні проблеми гарантоздатності КС. Особливу увагу приділено системно-кібернетичному підходу у вирішенні цієї проблеми. Серед розглянутих засобів для забезпечення гарантоздатності КС використовуються такі: штатне і кризисне керування, моніторинг ресурсів та інформаційних потоків, функціональне дублювання, мережева взаємодія між компонентами КС і багато інших.*
Ключові слова: *гарантоздатність, відмовостійкість, готовність, цілісність, технологія, комп'ютерна система, надійність.*

Аннотация: *Рассмотрены методы и средства элементно-технологического, информационного, программно-алгоритмического и организационного базисов в решении проблемы гарантоспособности КС. Особое внимание уделено системно-кибернетическому подходу в решении этой проблемы. Среди рассмотренных средств для обеспечения гарантоспособности КС используются следующие: штатное и кризисное управление, мониторинг ресурсов и информационных потоков, функциональное дублирование, сетевое взаимодействие между компонентами КС и многие другие.*
Ключевые слова: *гарантоспособность, отказоустойчивость, готовность, целостность, технология, компьютерная система, надежность.*

1. Введение

В связи с тем, что современное развитие направлено на создание информационного общества, а затем общества знаний [1], поэтому все большее значение приобретает надежность и ее обобщение – гарантоспособность компьютерных систем (КС). Этот процесс приводит к тому, что КС широко используются в различных областях народного хозяйства, в технике, науке, медицине, банковском деле, автоматизации технологических и других процессов и т.д., которые требуют достоверности получаемой информации.

В свою очередь, понятие гарантоспособности появилось как результат некоторой интеграции таких понятий, как надежность, отказоустойчивость, функциональная безопасность, обслуживаемость и т.д. С этой точки зрения гарантоспособность КС эквивалентна системной (функциональной) надежности. Но надежность только косвенно определяет термин гарантоспособности. Потребителя услуг КС мало интересует надежность КС. Это интересует специалистов, а потребителя интересует, насколько он получит от КС достоверные результаты и насколько устойчив процесс работы КС для непрерывного получения результатов. Проблема получения недостоверных результатов КС усугубляется тем, что практически большинство КС

ISSN 1028-9763. Математичні машини і системи, 2008, № 4

связаны между собой Интернетом, позволяющим другим КС использовать недостоверную информацию (естественно, не зная об этом). В ряде случаев это может привести к катастрофическим последствиям. Особо это опасно в критических областях использования КС. Более подробно данные проблемы рассматриваются в работе [2, 3]. Именно в связи с широким использованием КС и Интернета во всех областях информационного общества решение проблем гарантоспособности является наиболее актуальным и важным в настоящее время.

Существуют различные подходы к решению данных проблем. Более подробно остановимся на них в последующих разделах работы.

Отличительной чертой настоящей работы является взгляд на решение этих проблем на основе базисов компьютерной науки.

Однако рассмотрению базисов компьютерной науки должен предшествовать системно-кибернетический подход к процессам, протекающим в системах вообще и КС, в частности. При решении проблемы создания отказоустойчивых КС на передний план выдвигаются различные технологии, обобщенная диагностика (мониторинг), адаптивность, целенаправленность, многопроцессорность и надежность (устойчивость) функционирования. Так, для обеспечения гарантоспособности необходимо рассматривать технологичность элементной базы, технологию программирования, технологию вычислений, информационные (компьютерные) технологии и т.д.

2. Гарантоспособность

Следуя работам [4, 5], дадим несколько понятий термину гарантоспособность.

Исходное определение гарантоспособности прежде всего исходило из того, что система предоставляет обслуживание, которому можно доверять.

Альтернативное понятие определяет гарантоспособность как способность избегать отказов обслуживания более частых и более серьезных, чем это приемлемо.

И, наконец, гарантоспособность воспринимается как синтетическое понятие, которое объединяет следующие показатели:

– готовность, т.е. готовность к правильному обслуживанию;

– безотказность, т.е. непрерывность (постоянство) правильного обслуживания;

– функциональная безопасность, т.е. отсутствие катастрофических последствий для пользователей и окружающей среды;

– целостность, т.е. отсутствие некорректных изменений системы;

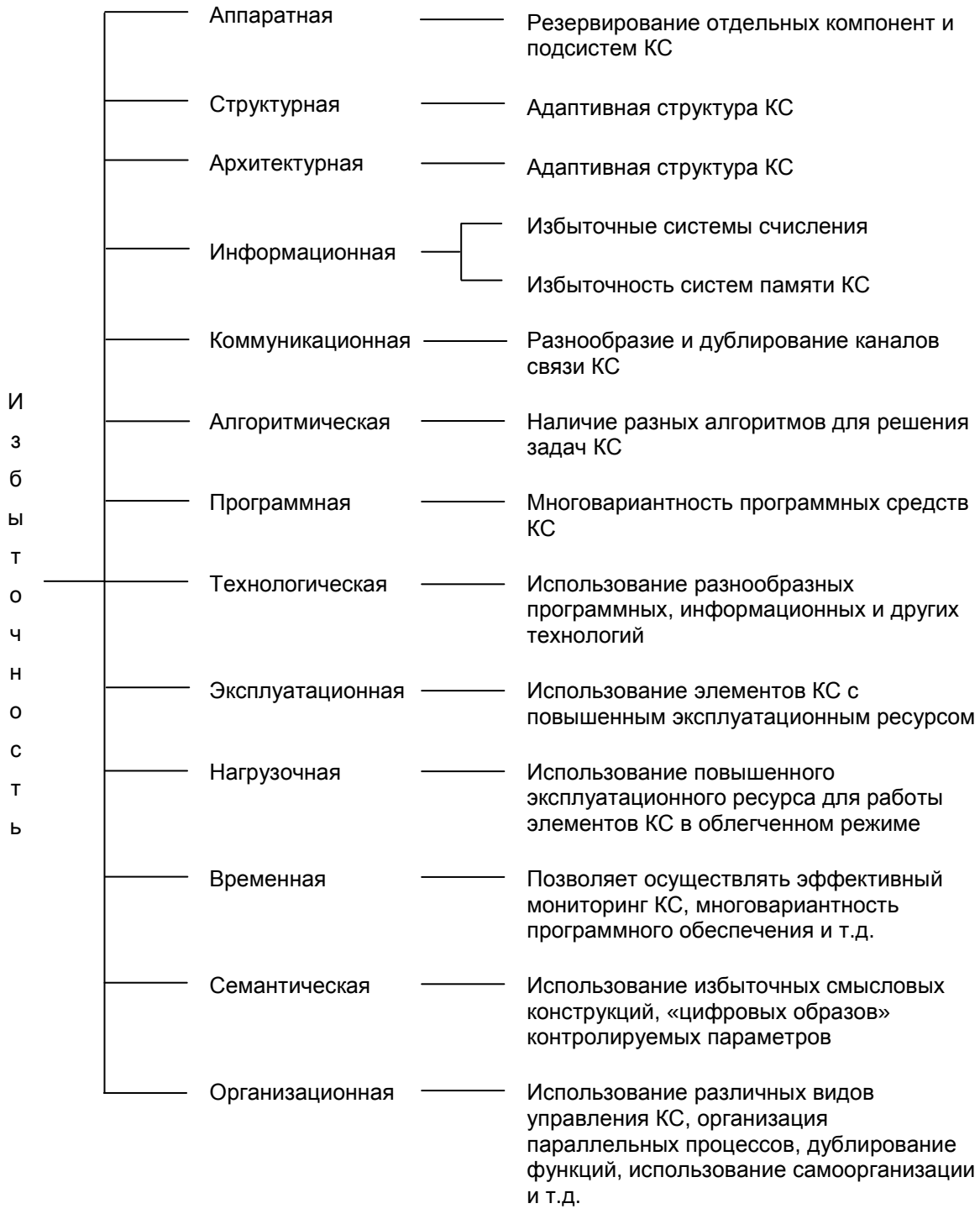
– обслуживаемость, способность подвергаться модификациям и ремонту либо автоматической замене отказавших компонент системы, а также устойчивость работы.

Но гарантоспособность будет не вполне полной, если она не будет дополнена требованием безопасности системы, т.е. возможности противостоять внешним угрозам и, прежде всего, несанкционированному проникновению в систему.

Как утверждается в работах [4, 5], ключевой предпосылкой гарантоспособности для больших систем является отказоустойчивость. Но это только необходимое условие. Достаточным условием достижения гарантоспособности системы является удовлетворение всех без исключения показателей, приведенных в синтетическом определении отказоустойчивости. Напомним, что, в

свою очередь, необходимым условием при построении отказоустойчивых систем является наличие и широкое использование различных видов избыточности.

На рис. 1 приведены различные виды избыточности, которые могут быть использованы при создании гарантоспособных КС.



В [6] считается, что гарантоспособная КС (ГКС) – это система, обладающая полным или частичным набором первичных свойств, составляющих гарантоспособность. При этом под первичными свойствами понимается безотказность, готовность, обслуживаемость, достоверность,

функциональная безопасность, живучесть, целостность, конфиденциальность, а также можно добавить информационную безопасность, аутентичность, надежность, сохраняемость, долговечность и т.д.

В [2] отмечается, что гарантоспособность в конечном итоге является средством (технологией), гарантирующим достоверность получения информации от КС в результате ее преобразования, хранения и передачи, невзирая на наличие внешних и внутренних возмущений, воздействующих на работу КС. Но получение достоверной информации связано с надежной работой всех компонент КС и достоверной входной информацией. С другой стороны, необходимым условием гарантоспособности является ее устойчивая работа, позволяющая адекватно реагировать на все внутренние и внешние возмущения. Наряду с понятием устойчивости КС, в [2] рассматривается расширенное понятие работоспособности относительно КС.

Продолжая эту мысль, под гарантоспособностью КС можно воспринимать способность КС правильно и устойчиво работать как в штатном режиме ее функционирования, так и в нештатном (критическом) режиме путем сохранения рабочих характеристик всех необходимых компонент системы, влияющих на выполнение поставленных перед КС заданий.

Гарантоспособность как функциональная (системная) надежность основывается на устойчивой работе всех компонент компьютерной системы (технических и программных), математического обеспечения (методы и алгоритмы), информационного, а также их правильной работы, невзирая на возникшие сбои и отказы, связанные с внутренними и внешними причинами, что обеспечивает гарантоспособность вычислений и полученных от ГКС услуг.

Гарантоспособность является дальнейшим естественным развитием отказоустойчивости и живучести компьютерных систем, которые широко используют все виды избыточности, мониторинга состояния КС и механизмов парирования последствий возникших в КС сбоев, а также противодействия внешним и внутренним попыткам нарушения (искажения) правильности работы и функционирования КС и ее информационных составляющих.

Важное значение для ГКС имеет обеспечение гарантоспособных вычислений, наличие входных и выходных фильтров, исключающих искажение входной и выходной информации.

В качестве оценки гарантоспособности в [6] предлагаются два вида оценок:

– векторные, представляющие собой набор показателей, которые оценивают отдельные свойства гарантоспособности (безотказность, готовность, целостность) либо устойчивость к различным типам дефектов;

– скалярные, с помощью которых дается обобщенная оценка.

Один из вариантов скалярного показателя представляет собой вероятность оказания услуги КС.

Другой вариант скалярной оценки основывается на метрическом подходе, использующем детализирующую модель гарантоспособности как иерархии первичных и вторичных свойств, а также их характеристик, определяемых набором метрик. Последние оцениваются экспериментальным путем или вычисляются на основе измеряемых параметров системы. Далее получают свертку метрик.

3. Системно-кибернетический подход при решении задач гарантоспособности КС

В рамках этого раздела работы рассмотрим возможность перенесения некоторых функций человека в КС. Это оправдано тем, что человек, как и многие объекты живой природы, достаточно хорошо оснащен механизмами, позволяющими ему поддерживать жизненно важные параметры и процессы на уровне их стабилизации, что позволяет ему функционировать в необходимых пределах.

Как отмечается в работах [7–10], взаимодействие человека с окружающим его миром, а также его автономное функционирование взаимно обусловлены и осуществляются в пределах следующих функций: инстинктивной, двигательной, эмоциональной и интеллектуальной.

Так, например, инстинктивная функция человека в мыслительном процессе проявляется как необходимость принятия решений, связанных с проблемами личной безопасности, создания благоприятных условий существования, удаления отходов по мере необходимости, и т.д.

В кибернетических системах, каковыми являются КС, эти функции могут включать следующее:

– мониторинг окружающего пространства в реальном времени (параметрических сигналов, значений функций, хода протекания процессов и т.д.);

– анализ ситуации, связанной с состоянием контролируемой сложной системы (КС и ее элементов), на основе данных мониторинга для оперативного реагирования, т.е. выполняется функция самосохранения КС;

– формирование ассоциативных связей внутри текущей информации мониторинга, записываемой в память КС и ее компонент;

– управление ассоциативными связями между данными мониторинга в текущей ситуации и признаками подобия прошлых ситуаций;

– кризисное управление при восстановлении утраченных функций.

Таким образом, «инстинктивная» функция КС в основном состоит в следующем: мониторинге деятельности (работа, функционирование и т.д.); мониторинге всех видов ресурсов системы, мониторинге внешнего пространства системы (в тех случаях, когда это необходимо); анализе текущих ситуаций; осуществлении ситуационного управления в нормальном режиме для предотвращения угроз работы системы в соответствии с ее регламентом и переходу к кризисному управлению в случае перехода угрозы в реальное состояние.

Аналогично вышеизложенному можно интерпретировать двигательные, эмоциональные и интеллектуальные функции человека, которые могут быть внесены в КС для обеспечения ее гарантоспособности.

Двигательная функция человека обусловлена необходимостью управлять двигательной активностью человека (пространственной ориентацией, координацией движений, планированием и организацией деятельности). Для КС, которые работают в подвижных объектах, практически все двигательные функции человека должны в той или иной степени присутствовать. А в обычных системах должна присутствовать функция планирования и организации деятельности внутри КС для предотвращения возникновения угрозы нормального функционирования и ее ликвидации в случае возникновения.

Таким образом, двигательная функция разума обеспечивает уточнение внешней обстановки (в нашем случае – внутренней обстановки), выработку акта воли, организацию пространства, ресурсов и деятельности.

При этом двигательный разум непосредственно взаимодействует с интеллектуальным, что выражается в возможности проектирования соответствующих рациональных технологий действий, а также организации выполнения необходимых проектов и планов.

Интеллектуальная функция разума человека может осуществлять входной (выходной) контроль (в нашем случае входные и выходные информационные фильтры КС), нормоконтроль (контроль правильности работы системы), планирование (формирование замысла будущего действия).

Нормоконтроль в КС во многих случаях осуществляется на основе оценки нахождения значений параметров, ограничений, которые определяются регламентом работы системы.

Эмоциональная функция разума человека обеспечивает моделирование возможностей, выработку стратегий поведения и коррекцию ограничений действий. Но эмоциональный разум работает на основе информации, полученной от органов чувств.

Для КС необходимо ввести комплексные анализаторы информации, циркулирующей в системе управления. При этом «эмоциональная реакция в системе управления КС свидетельствует о наличии в системе внутреннего дисбаланса функций, который требует принятия решений либо о коррекции выполняемых функций компонентами системы, либо о коррекции полей ограничений, а в некоторых случаях и коррекции исходной целевой функции системы.

Помимо этого, для моделирования возможностей системы в целом и ее компонент с целью обеспечения высокого уровня их гарантоспособности используются прогнозные модели возможности возникновения угроз.

Полученные результаты моделирования непосредственно используются системой управления для принятия необходимых действий в случае необходимости.

Для правильного понимания, как обеспечить гарантоспособность КС, целесообразно обеспечить баланс (гармонию) протекания шести процессов, происходящих в системе [10, 11]. При этом баланс данных процессов происходит путем стимуляции одних процессов и сдерживания других, в зависимости от выбранной цели, стратегии и тактики процесса управления.

Основным требованием к объекту вообще и КС, в частности, является обеспечение его функционирования по предназначению с сохранением его штатной работы и организации, а также рациональное использование имеющихся наличных ресурсов.

Функционирование любого активного объекта обеспечивается наличием следующих шести процессов:

● Процесс переработки ресурсов и получения продукции. Управляющая информация. Управляющая информация, начиная от цели, последовательно декомпозируется на функции, планы и т.д. вплоть до команд и сигналов. В нашем случае целью является обеспечение гарантоспособности КС.

● Процесс роста. В этом процессе управляющая информация обеспечивает организацию ресурсов объекта в структурные единицы. Активность управляющей информации позволяет

выполнять ресурсный потенциал структурных элементов объекта. Эта информация также позволяет сбалансировать процессы организации активного объекта, обеспечивая сохранение возможности функционирования объекта по предназначению в штатном режиме.

● Процесс саморазрушения, т.е. происходит отклонение работы отдельных элементов системы от штатного режима, что приводит к отклонению работы от предназначения, если не будут приняты специальные меры. Природа этого процесса связана, с одной стороны, с процессами деградации элементов объекта под влиянием времени, внешних и внутренних условий их работы, а, с другой стороны, процесс деградации объекта связан с тем, что управляющая и другие виды информации, идущие к структурным единицам объекта и от них, искажается. Этому процессу противостоит процесс управления безопасностью на основе ситуационного управления.

● Процесс самообучения, изменения природы либо приобретение новых функций. Этот процесс связан с тем, что структурные единицы объекта инициируют изменение состава ресурсов с целью приобретения новых функций. В процесс самообучения входит порождение новых стратегий функционирования объекта, что является штатной функцией органа управления объектом. В пределах компенсации объекта процесс самообучения позволяет изменять выполняемые функции на самом объекте, а также вырабатывать требования об изменении функций к метасистеме при взаимодействии с другими объектами.

● Процесс самоорганизации и «исцеление» объекта. Этот процесс направлен на восстановление нарушенных функций, в частности, возникших в результате процесса саморазрушения. При этом исполнительные средства объекта, самоорганизуясь в структурную иерархию, восстанавливают управляемость и работу по предназначению объекта. Свойство самоорганизации в этом случае связано с необходимостью обеспечения структурных единиц объекта к самосохранению либо исцелению в случае возникновения угроз объекту в нарушении работы по предназначению. При этом происходит переход к кризисному управлению объектом, обеспечивающим ликвидацию очага, вызвавшего кризис, и восстановление функции объекта в полном либо частичном объеме за счет имеющихся либо привлечения новых ресурсов.

● Процесс мониторинга и интегрирования ресурсов в соответствии с регламентом функционирования объекта. При этом исполнительные средства объекта генерируют (порождают) информацию об исполнении полученных заданий, состоянии структуры и ресурсов объекта. Данная информация анализируется и структурируется в соответствующей структурной единице объекта, где она складируется, и на ее основе строятся действия, непосредственно направленные на ликвидацию возникших угроз с учетом прогноза состояний функционирования объекта по предназначению.

В качестве исходных элементов этих процессов берутся: управляющая информация, структура объекта и ресурсы. Шесть процессов представляют собой шесть комбинаций целевого взаимодействия данных элементов. При этом необходимо ответить на следующие вопросы: Что воздействует? На что воздействует? В какой среде происходит воздействие?

Все шесть процессов, воспринятые во времени и динамике, представляют собой функционирование сложной системы.

Управление какой-либо деятельностью объекта сводится к поддержанию баланса между результатами описанных выше шести процессов путем сдерживания одних и стимулирования других в зависимости от выбранной стратегии управления.

В случае выхода одного или нескольких процессов за рамки регламента функционирования процесса, при необходимости осуществляется переход от штатного к ситуационному (кризисному) управлению объектом.

Читатель может легко самостоятельно интерпретировать эти шесть процессов в рамках создания гарантоспособных и отказоустойчивых КС.

Описание функционирования сложной системы в виде этих шести процессов является одной из теоретических основ построения теории создания гарантоспособных КС.

Целесообразно дополнить описанные выше шесть процессов иерархией структуризации информации в активном объекте.

С точки зрения системно-кибернетического подхода [10] и закономерностей трансформации информации в циклах управления сложными системами, активный объект существует на следующих уровнях:

– нулевой уровень – это целевая функция активного объекта в терминах его предназначения, которая вырабатывается на более высоком уровне (метауровне) по отношению к объекту (системе);

– первый уровень – это перечень функций объекта с обоснованием необходимости его создания и ограничениями, которые налагает на функционирование целевая функция объекта;

– второй уровень – это структурная организация существования и функционирования объекта, включая документы (инструкции и т.д.) и/или процессы, обеспечивающие жизненный цикл функционирования объекта в соответствии с регламентом, а также процесс самообучения (для приобретения новых качеств, функций и возможностей адаптации к внешним и внутренним воздействиям);

– третий уровень – это порождение командно-сигнальной информации и ее использование в практической реализации целевой функции объекта, включая возможности восстановления утраченных функций либо ресурсов с использованием результатов мониторинга для обеспечения безопасности и работоспособности объекта.

В нашем случае под объектом понимается КС, а под целевой функцией – обеспечение гарантоспособности КС.

Необходимо отметить, что гарантоспособность на основе использования функционально-информационных блоков требует системного подхода как с точки зрения выделения функций системы по иерархии, так и с точки зрения выделения целей и подцелей. Помимо этого, должны быть обеспечены:

– системная согласованность по целям, задачам, ресурсам и необходимым результатам работы системы, а также обеспечение ее гарантоспособности при наличии отказов и сбоев;

– взаимная согласованность целей, задач, ресурсов и ожидаемых результатов управления работоспособностью системы;

– своевременное обнаружение, гарантированное распознавание и системное диагностирование факторов и ситуаций, приводящих к отказам, сбоям и выдаче неправильных результатов вычислительной системы;

– оперативное прогнозирование, достоверное оценивание нештатных и критических ситуаций;

– своевременное формирование, оперативная реализация решений управления гарантоспособностью в процессе предотвращения нештатных и критических ситуаций.

4. Роль базисов компьютерной науки в решении проблемы гарантоспособности

Впервые роль базисов вычислительной техники была рассмотрена автором в работе [12] при решении проблемы производительности, хотя в научно-технических отчетах они рассматривались автором в начале 90-х годов прошлого столетия. На значении этих базисов мы останавливались и в работе [13] при решении проблемы отказоустойчивости КС.

В настоящей работе базисы рассматриваются в аспекте решения проблемы отказоустойчивости КС. Но при этом необходимо учитывать, что отказоустойчивость является неотъемлемой частью проблемы гарантоспособности.

Под термином базис в настоящей работе понимается набор средств, методов, ресурсов и технологий, составляющих основу производства информационного продукта, вырабатываемого КС.

Элементно-технологический базис был известен еще до введения автором остальных базисов. Он составляет основу построения hardware и во многом зависит от технологий изготовления технических средств КС. Если раньше элементный базис составляли элементы, из которых строились процессы и другие компоненты КС, то теперь основу элементно-технологического базиса составляют СБИС. При решении проблемы гарантоспособности важнейшими являются следующие показатели: высокая надежность, производительность, готовность, экономичность, наличие внутреннего мониторинга и т.д.

Для повышения надежности работы элементов чрезвычайно важно улучшение эксплуатационных характеристик элементов не только за счет передовых технологий их изготовления, но и за счет использования понижения эксплуатационной частоты их работы (уменьшает температурный режим и используются элементы, способные работать на более высокой частоте, а также, в случае недогруженности, имеют возможность отключать неработающие элементы и переходить в режим «ожидания»). Помимо этого, важно использовать возможности выдачи сигналов о возникновении угроз на более высокий уровень, а в некоторых случаях парировать отказы за счет использования других базисов на микроуровне.

Информационный базис представляет собой совокупность средств и методов, связанных с представлением, переработкой, хранением и передачей информации, а также обеспечением ее целостности. При этом важно, в каком виде представлены информация, объемы запоминаемой информации и время доступа к ней, скорости и объемы информации, передаваемой по каналам связи и перерабатываемой активными элементами КС. Сюда относится не только информация, подлежащая обработке, но и программная информация.

Следует знать, что информационный базис играет ключевую роль в решении проблемы гарантоспособности. Прежде всего, он определяет систему счисления обрабатывающих элементов, входящих в КС. Использование кодирования информации с обнаружением и исправлением ошибок или доведение возникших ошибок до ошибок, соответствующих единице последнего разряда (например, двоично-пятеричный код, циклические коды и т.п.), способствуют появлению архитектуры системы NonStop, которая обеспечивает быстрое проявление неисправностей и соответствует тому принципу, что каждая компонента КС либо функционирует правильно, либо немедленно останавливается.

Как уже отмечалось выше, информационный базис включает получение, передачу, трансформацию, хранение, структурирование и выдачу информации КС. Сюда относятся и базы данных разных типов, а также входная и выходная информация машинных алгоритмов.

Для обеспечения гарантоспособности КС важную роль должны играть входные и выходные информационные фильтры, обеспечивающие отсев неправдоподобных данных на входе и выходе как обрабатывающих компонент, так и самих КС. Эти фильтры являются чрезвычайно важными в связи с тем, что КС обладает свойством увеличения неопределенности выходной информации, если входная информация является даже частично неопределенной. Отметим, что обеспечение достаточного уровня гарантоспособности КС, с точки зрения информационного базиса, обеспечивается в каждой из компонент КС своими средствами с согласованием с общей стратегией обеспечения гарантоспособности КС в целом.

Программно-алгоритмический базис включает в свой состав все компоненты software, т.е. системное и прикладное программное обеспечение КС, а также алгоритмы, методы, схемы счета, функциональные преобразования информации, решающие правила, модели вычислительных процессов, стандартные и определяемые функции, выражения, цепочки операторов, макросов и т.д. входного языка КС. Таким образом, этот базис включает в себя все компоненты, составляющие основу создания и реализации вычислительного процесса КС. Помимо этого, рассматриваемый базис в качестве своих инструментов содержит технологии программирования и технологии вычислений, которые являются чрезвычайно важными для обеспечения гарантоспособных вычислений. Технология вычислений непосредственно связана с обеспечением численной устойчивости методов (алгоритмов) при решении прикладных задач.

Гарантоспособность программного обеспечения во многих случаях использует идею многовариантности [14, 15]. Безусловно, для решения проблемы гарантоспособности программно-алгоритмический базис должен эффективно взаимодействовать с другими базисами компьютерной науки. Это, прежде всего, относится к организационному базису, который должен принимать активное участие в организации появления сигналов об угрозах, их локализации и, по возможности, их ликвидации. Особо важно участие этого базиса в управлении вычислительным процессом и переходе к ситуационному (кризисному) управлению, в случае превращения угрозы в реальность, и возвращение вычислительного процесса в нормальное состояние, если это возможно.

При осуществлении этих процессов, в основном, участвует средний уровень иерархии данного базиса.

Организационный базис связывает воедино все процессы, происходящие в системе, и тесно связанные с архитектурой и структурой КС, а также системным программным обеспечением. Он же должен организовать взаимодействие между элементами и уровнями КС, синхронизацию их работы, обеспечить мониторинг состояния системы и восстановление правильности работы в случае возникновения различных видов дефектов, выявленных при мониторинге, за счет использования различных видов избыточности, имеющихся в КС; эффективный вычислительный процесс внутри машины и информационное и физическое взаимодействие как с внутрисистемными компонентами, так и с внешней по отношению к КС средой, и т.п.

Наиболее эффективной, с точки зрения организационного базиса, является адаптивная КС с программируемой структурой и архитектурой, основанная на магистрально-сетевом взаимодействии. Отметим, что организационный базис играет большую роль в рестарте процессов в случае возникновения внештатных (кризисных) ситуаций и организации процессов управления. Это чрезвычайно важно для обеспечения гарантоспособных вычислений. При этом важно управление процессами на локальном (микро), промежуточном и глобальном уровнях. Сегодняшние безотказные КС, в основном, базируются на методах дублирования компонент и сравнения получаемых результатов. Хотя, если следовать логике живой природы, необходимо перейти от простого дублирования к дублированию функций и иметь интеллектуальные средства для обнаружения дефектов и их парирования.

Современный организационный базис для обеспечения гарантоспособности должен использовать адаптивные многоконтурные сетевые архитектуры, NonStop структуры обрабатывающих элементов, дублирование функций, а не элементов, как это делается в настоящее время, организацию мониторинга всех компонент КС, выявление и прогнозирование угроз и устранение их в случае реализации, осуществление реорганизации КС при необходимости противодействовать внутренним и внешним угрозам, оценивание достоверности получаемой выходной информации, а также слежение за прохождением информации внутри системы и нахождение ее в заданных диапазонах и многое другое.

Организационный базис должен реализовать правильное выполнение шести процессов на соответствующих уровнях иерархии КС, как это описано в разд. 3.

Но для этого необходимо еще, помимо вышеописанного, наличие в КС интеллектуального центра в виде экспертной системы, работающей в режиме реального времени, для обеспечения прогноза происходящих событий, их анализа для принятия необходимых решений, а также самообучения и саморазвития КС.

Как видно из вышеизложенного, ни один из базисов компьютерной науки не в состоянии в одиночку решить проблему гарантоспособности КС. Это связано с тем, что проблема создания гарантоспособности КС является комплексной и поэтому для ее решения необходимо использовать все базисы. Но при этом между базисами могут возникнуть противоречия, которые могут быть решены на основе принципа смешанного экстремума [1, 16].

На рис. 2 приведены средства, которые можно использовать при создании гарантоспособных КС в рамках рассмотренных выше базисов.

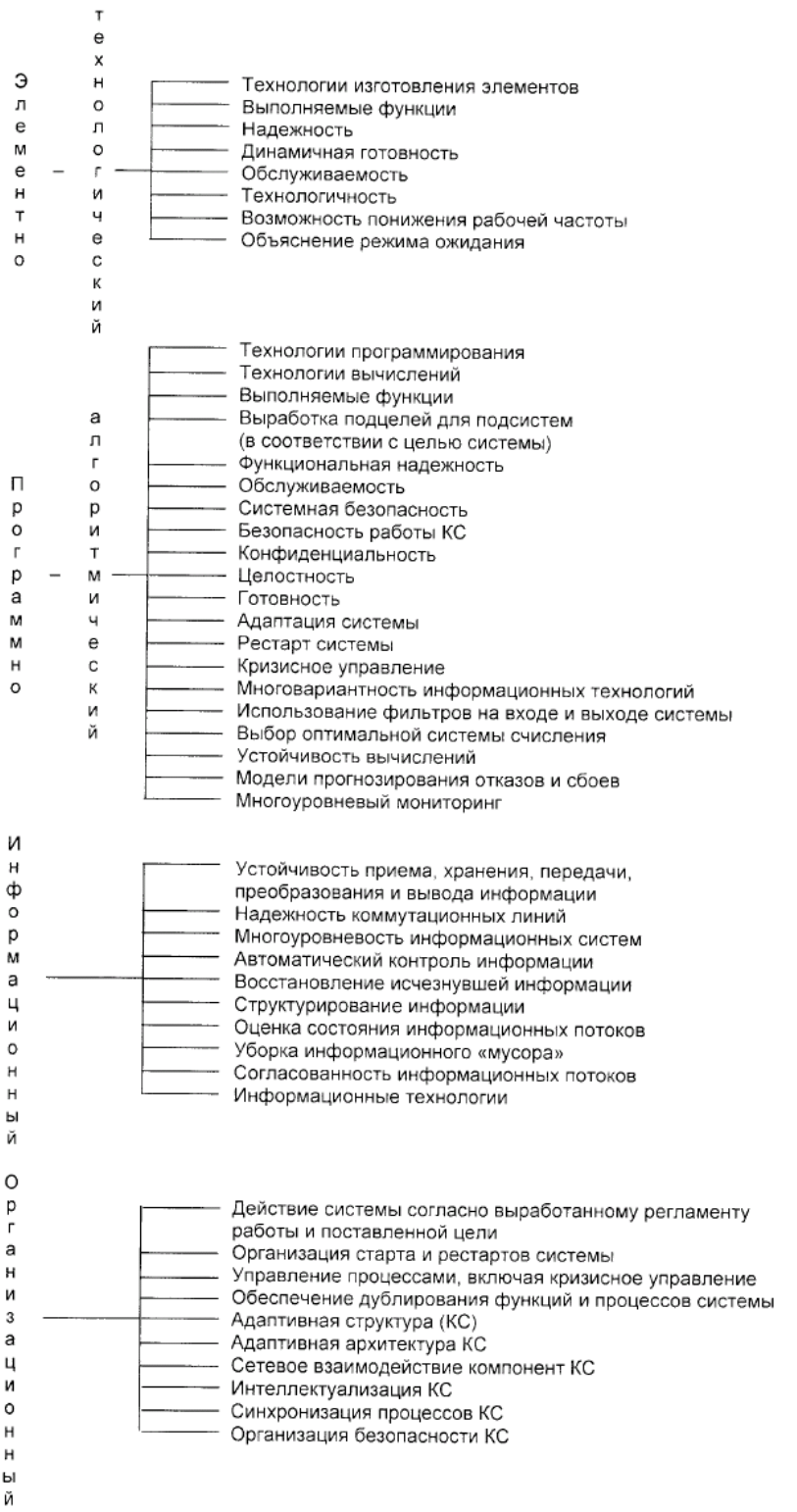


Рис. 2. Роль базисов компьютерной науки в решении задач гарантоспособности

5. Средства для построения гарантоспособных КС

Надежные компьютеры являются ключевыми элементами для создания отказоустойчивых и гарантоспособных КС для работы в сфере розничной торговли, финансов, телефонной коммутации и т.д.Одной из наиболее известных в мире фирм, как отмечается в работе [17], является компания

Tandem. Системы Tandem NonStop базируются на реализации многопроцессорной обработки и модели распределенной памяти.

Для обеспечения восстановления после сбоев аппаратуры и ошибок программного обеспечения эти системы используют механизм передачи сообщений между процессными парами. База данных NonStop SQL, в основе архитектуры которой лежит модель системы без разделения, позволяет в ряде случаев достичь линейной масштабируемости от количества используемых в КС процессоров.

Однако в системе Integrity компании Integrity используются методы аппаратной избыточности, основанные на трехкратном резервировании с мажоритарным клапаном. Это не совсем оптимальное решение, но оно обеспечивает продолжение непрерывной работы в условиях реализации угроз.

Более передовой является архитектура NonStop с сетевым взаимодействием между компонентами КС.

Отметим, что системы, имеющие центральный процессор, выполняют сравнение выходов дублированных взаимосинхронизированных микропроцессоров. Ответственность после обнаружения неисправности в аппаратуре возлагается на программное обеспечение. Однако сравнение может выполнять не только процессорный элемент, но и вычислительная сеть, разумеется, если такая имеется в структуре КС. Она же может осуществлять и коммутацию как сообщение пакетов и т.д., так и соединение элементов, включая периферийные устройства между собой.

Рассмотрим более подробно архитектуру NonStop, являющуюся одним из значимых компонентов гарантоспособности КС.

Архитектура NonStop [17] предполагает объединение двух и более процессов при помощи дублированной высокоскоростной межпроцессорной шины. В качестве такой шины может быть использована оптоволоконная сеть межпроцессорного обмена.

Все аппаратные компоненты системы NonStop основываются на принципе «быстрого проявления неисправностей», в соответствии с которым каждый компонент системы должен либо функционировать правильно, либо немедленно остановиться, что в противном случае позволяет остановить распространение искаженной информации. Современные конструкции для обнаружения ошибок в основном полагаются на методы дублирования и сравнения. Но существуют и другие подобные методы (аппаратные и программные). Однако восстановление нормальной работы КС после обнаружения неисправности в основном возлагается на программное обеспечение, хотя в ряде случаев возникает необходимость использовать и аппаратные средства.

Дальнейшее развитие этой архитектуры связано с использованием дублированной локальной вычислительной сети. Базовым элементом ее является маршрутизатор. В типовой конфигурации системы большинство ее узлов имеют двухпортовые интерфейсы. При этом выявление неисправного узла возлагается на саму сеть.

Для восстановления после сбоев аппаратуры и ошибок программного обеспечения эти системы используют механизмы передачи сообщений между процессорными парами.

В работе [18, 19] рассматриваются другие подходы построения отказоустойчивых бортовых комплексов. Среди них – одноканальные структуры с автоматом контроля и восстановления; многоканальные резервированные структуры; многоканальные структуры с автоматом межканального обмена; программного контроля и восстановления информации в каналах; многоканальные структуры с аппаратным мажоритированием входной и выходной информации каналов; многоканальные многоярусные структуры с аппаратным мажоритированием сигналов каждого функционального узла бортового комплекса, а также проведен их анализ. Некоторые из рассмотренных подходов и механизмов могут быть использованы в перспективной сетевой NonStop архитектуре, идеология которой наиболее полно отвечает требованиям к построению гарантоспособных систем.

Важной задачей осуществления эффективной отказоустойчивости является предупреждение распространения ошибки на работу исправных компонент КС. Сказанное выше наиболее наглядно видно, когда один из компонентов КС передает ошибочную информацию другим компонентам, использующим эту информацию.

До недавнего времени для решения этой проблемы в основном использовались механизмы троирования компонент с мажоритарным клапаном (механизм совпадения двух компонент из трех). В настоящее время, например, для создания отказоустойчивых серверов, используется нонстопная (NonStop) архитектура компоненты КС, которая не выдает ошибочную информацию в соседние компоненты за счет самоконтроля. В случае отказа этой компоненты, информация поступает от подобной компоненты, которая функционально дублирует первую. В качестве арбитра в этом случае выступает вычислительная сеть. Здесь мы наблюдаем сразу три эффекта: локализацию распространения ошибки, продолжение правильной работы системы и элемент сетевого взаимодействия между компонентами КС.

Для того, чтобы сама внутренняя вычислительная сеть не стала «ахиллесовой пятой» в решении проблемы отказоустойчивости, она также дублируется. Таким образом, вместо механизма «два из трех» используется механизм «один из двух» с сетевым взаимодействием.

В случае отказа и второй компоненты КС в рассматриваемом процессе можно использовать механизм функционального дублирования, т.е. передачи выполняемой функции другой компоненте, находящейся в другой паре, в виде дополнительной нагрузки и новой маршрутизации. Но для этого в КС должен быть интеллектуальный управляющий блок, который обязан поддерживать описанные выше механизмы. Во время переключения компонент КС для обеспечения непрерывной работы (для КС реального времени) необходимо воспользоваться прогнозными значениями параметров процессов, которые оперативно передаются в интеллектуальный управляющий блок КС. В случае появления случайного сбоя в системе можно использовать кратные вычисления, но для этого необходимо иметь определенный запас времени.

Характерными чертами гарантоспособности рассматриваемой КС являются следующие:

– использование всех видов избыточности;

– сетевое взаимодействие между компонентами системы;

– использование обобщенной готовности системы, позволяющей заменить отказавший компонент на исправный;

– использование обрабатывающих модулей системы, работающих в режиме NonStop;

– использование дублирования функций вместо простого дублирования элементов системы;

– наличие двух видов управления системой: штатного и кризисного (ситуационного);

– наличие системы мониторинга системы на всех уровнях ее работы;

– прогнозирование надежности работы элементов системы;

– наличие возможности реконфигурации системы;

– возможность отслеживания информационных потоков системы;

– отслеживание выхода параметров системы за установленные пределы и оперативное реагирование на выход за пределы установленного «коридора»;

– наличие средств оперативного реагирования системы на возникшие угрозы, обеспечивающие продолжение работы системы в штатном режиме;

– наличие интеллектуальных модулей в системе, позволяющих вырабатывать в реальном времени стратегию и тактику по обеспечению нормальной работы системы в случае возникновения угроз и обеспечивающих саморазвитие системы с учетом наличных ресурсов;

– возможность разрешения имеющихся противоречий на всех стадиях создания и эксплуатации системы на основе принципа смешанного экстремума;

– иметь средства управлять надежностью системы;

– необходимое условие сохранения целостности системы. На рис. 3 представлен основной набор средств, используемый для создания гарантоспособных КС.

В решении проблемы гарантоспособности КС важную роль играет обеспечение их готовности. При этом различают высокую готовность, которая минимизирует время планового и непланового времени простоя КС за счет быстрого восстановления работы системы после обнаружения неисправности, и непрерывную готовность, которая обеспечивает правильную работу системы и устраняет любое время простоя как плановое, так и неплановое. В нашем случае именно непрерывная (динамичная) готовность является наиболее предпочтительной. Но для осуществления непрерывной готовности необходимы избыточные аппаратные и программные средства, которые в ряде случаев можно использовать для распараллеливания необходимых работ, выполняемых КС, механизмы мониторинга элементов системы, парирования возникших угроз и отказов, а также возможность адекватного реагирования на текущее состояние. Дополнительным требованием к таким системам является отсутствие деградации системы в случае возникновения отказа.

Для обеспечения высокой готовности КС необходимо обеспечить, прежде всего, защиту наиболее важной части системы – данных, а также диагностику в режиме on-line, изоляцию неверного процесса, сетевую организацию коммуникаций и т.д.

Рис. 3. Дерево гарантоспособности и безопасности

Помимо этого, целесообразно ввести контроль наличия информации и параметров потоков информации во всех частях вычислительной системы и особенно на коммутаторе в случае использования системы с сетевым взаимодействием, программируемой структурой и архитектурой, включая индикаторы прохождения информации. Помимо этого, подобное необходимо осуществлять и для контроля функционально-информационных блоков.

Для обеспечения гарантоспособных вычислений следует:

– ввести входные и выходные фильтры на входе и выходе вычислительной системы и ее функционально-информационных блоков, отсекающих значения выходящих за пределы допустимых диапазонов значения данных, учета трендов и т.п.;

– провести исследования устойчивости вычислений как при разработке вычислительных алгоритмов, так и в ходе самих вычислений;

– осуществлять проверку соответствия полученных в результате вычислений данных необходимым путем их подстановки в исходные математические зависимости и оценки величин полученных невязок;

– осуществлять текущую оценку разных видов погрешностей как на этапе разработки алгоритмов, так и в ходе вычислений;

– широко использовать итерационные методы, в которых погрешность зависит в основном от погрешности последней итерации;

– использовать наряду с полными алгоритмами упрощенные алгоритмы, позволяющие осуществлять качественную оценку полученных вычислений;

– осуществлять расчет необходимых функциональных зависимостей с разной точностью для обнаружения скрытых неустойчивостей вычислений;

– бороться с возможностью «зависания» операционной системы, а в случае возникновения данной ситуации необходимо предусмотреть ее дублирование и т.д.

6. Выводы

Представленный в работе материал имеет как теоретическое, так и практическое значение при построении гарантоспособных КС.

Впервые и в отечественной, и зарубежной литературе показана важность решения проблемы гарантоспособности на основе базисов компьютерной науки. Это позволило увидеть, что при решении данной проблемы возникает необходимость оптимизировать противоречия, существующие между этими базисами.

И, наконец, системно-кибернетический подход совершенно в другом ракурсе позволил взглянуть на проблему гарантоспособности. Приведенные в работе подходы требуют дальнейшей детализации и конкретизации. В целом, проблема гарантоспособности КС настолько сложна, что вряд ли в ближайшее время предвидится ее полное решение.

СПИСОК ЛИТЕРАТУРЫ

1. Теслер Г.С. Новая кибернетика. – Киев: Логос, 2004. – 404 с.
2. Теслер Г.С. Концепция построения гарантоспособных систем // Математичні машини і системи. – 2006. – № 1. – С. 134 – 145.
3. Теслер Г.С. Концепция создания вычислительных средств с высоким уровнем отказоустойчивости // Математичні машини і системи. – 2002. – № 2. – С. 176 – 183.
4. Laprie J. et al. Fundamental concepts of dependability / J. Laprie, A. Avizienis, B. Randell // Technical Report: UCLACSD Report N 01-145, Newcastle university Report no. cs – TR – 739. – 2002. – 31 p.
5. Basic concepts and taxonomy of dependable and secure computing / A. Avizienes, J. Laprie, B. Randel et al. // IEEE Trans of dependable and secure computing. – 2004. – Vol.1, N 1. – P. 11 – 33.
6. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радіоелектронні і комп'ютерні системи. – 2006. – № 5 (17). – С. 7 – 19.

7. Косс В.А. Модель естественного интеллекта и пути реализации задач искусственного интеллекта // Математичні машини і системи. – 2006. – № 4. – С. 21 – 35.
8. Успенский П.Д. Психология возможной эволюции человека. – СПб.: Комплект, 1995. – 160 с.
9. Заннос С. Человеческие типы. – СПб.: Издательский дом «Весь», 2004. – С. 30 – 130.
10. Теслер Г.С., Косс В.А. Системно-кибернетический подход к анализу функций активных объектов для реализации в современных технологиях // Математичні машини і системи. – 2006. – № 2. – С. 3 – 13.
11. Колин Р. Теория небесных влияний. – СПб.: Издательство Чернышева, 1997. – 432 с.
12. Теслер Г.С. Место и роль алгоритмического базиса в решении проблемы производительности // Математические машины и системы. – 1997. – № 1. – С. 25 – 33.
13. Теслер Г.С. Концепция создания вычислительных средств с высоким уровнем отказоустойчивости // Математичні машини і системи. – 2006. – № 1. – С. 134 – 145.
14. Avizenis A. The N-version approach to fault tolerant software // IEEE Trans. Software engineering? – 1985. – December, Vol. SE – 11. – P. 1491 – 1501.
15. Харченко В.С., Паршин В.В. Многоверсионные системы и обеспечение гарантоспособности / В.С. Харченко, В.В. Паршин. – Харьков: ИП маш., 1989. – 33 с. – (Препринт № 321).
16. Теслер Г.С. Принцип смешанного экстремума как основа развития вычислительных средств // Математичні машини і системи. – 2002. – № 1. – С. 3 – 13.
17. Шнитман В.З., Кузнецов С.Д. Серверы корпоративных баз данных. Информационно-аналитические материалы Центра информационных технологий. – http//www.ivann.delta.msk.su.
18. Харченко В., Юрченко Ю. IOTS – подход: анализ вариантов структур отказоустойчивых бортовых комплексов при использовании электронных комплексов Industry. – http//www.cpm.ru.
19. Харченко В.С. и др. Реализация проектов отказоустойчивых бортовых компьютеров космических компонент Industry / В.С. Харченко, Ю.Б. Юрченко, Н.К. Байда // Технология приборостроения. – 2002. – № 1. – С. 74 – 80.

Стаття надійшла до редакції 04.01.2008