УДК 004.052

В.С. ХАРЧЕНКО

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ГАРАНТОСПОСОБНОСТЬ И ГАРАНТОСПОСОБНЫЕ СИСТЕМЫ: ЭЛЕМЕНТЫ МЕТОДОЛОГИИ

Проведен анализ комплекса проблем, связанных с развитием теории и практики гарантоспособных компьютерных систем (КС). Уточнены основные понятия и структура свойства гарантоспособности. Сформулированы базовые парадигмы и принципы обеспечения гарантоспособности КС. Проанализированы наиболее важные задачи, связанные с разработкой гарантоспособных КС (ГКС).

компьютерные системы, гарантоспособность, надёжность, безопасность, многоверсионность, web-сервисы, информационно-техническое состояние, управление гарантоспособностью

Введение. О кризисе теории надёжности КС

Человечество становится всё более зависимым от объёма, доступности и качества услуг, предоставляемых динамично развивающимися компьютерными технологиями (КТ). Эта зависимость распространяется на различные, казалось бы, совершенно не связанные области: коммерция и финансы, коммуникации и транспорт, энергетика и космос. Важнейшей составляющей такой зависимости является уровень надёжности и безопасности сервисов и систем, базирующихся или полностью реализуемых с использованием КТ. Это обусловлено тем, что недостаточный уровень надёжности и безопасности компьютерных систем (КС) приводит либо к материальным потерям, снижению конкурентоспособности и сужению сегментов рынка для коммерческих (бизнес-критических) приложений, либо к более серьёзным последствиям, связанным с гибелью людей, экологическими катастрофами и т.д. для КС критического применения. За более чем полвека после появления первых компьютеров теория надёжности сформировалась как классическая наука и хорошо развилась применительно к техническим системам. Арсенал методов и средств оценки и обеспечения надёжности прошёл всестороннюю апробацию и продолжает совершенствоваться по мере внедрения новых КТ. В то же время развитие теории надёжности применительно к программным средствам, сетевым технологиям и web-системам идёт недостаточно эффективно.

Это, на наш взгляд, обусловлено несколькими причинами. Во-первых, классическая теория надёжности, её методы не могут описать и дать адекватные оценки объектам, работоспособность которых нарушается не только вследствие отказов физической природы, а из-за проектных ошибок, информационных воздействий и др. Более того, для таких объектов трудно определить само понятие отказа и детерминировать множество его причин. Во-вторых, разработка систем с интенсивным использованием программного обеспечения, сетевых и web-технологий ведётся людьми иной инженерной философии, базирующейся, по-прежнему, на подходах к разработке и анализу результатов скорее как искусству, а не как строгой науке. Сохраняется ориентация на качественные, а не количественные инструментарии оценки, не укладывающиеся в «прокрустово ложе» строгих математических методов. Такая ситуация в теории надёжности КС сложилась в последние десятилетия несмотря на то, что всё большую долю в причинах отказов компьютерных систем составляют дефекты программных средств, перегрузки сетей и несанкционированные информационные воздействия. Она усугубляется ещё и тем,

что вопросы надёжности и информационной безопасности КС в течение многих лет рассматривались разными специалистами с использованием не связанных методов и технологий.

Отражением поиска путей преодоления этого кризиса стало появление в англоязычной литературе и наполнение новым содержанием термина “dependability”, имеющим более широкие рамки чем «надёжность», которому он соответствует [1, 2]. Поэтому логичнее было бы пользоваться иным русскоязычным термином, который может объединить свойства классической надёжности (безотказность, ремонтопригодность, долговечность и сохраняемость) и безопасности, прежде всего информационной. Таким может стать термин «гарантоспособность» (надёжность в широком смысле).

Анализ литературы. Цель работы

Различные аспекты гарантоспособности, принципы построения и реализации гарантоспособных КС, как надёжных и безопасных систем, детально исследовались на протяжении последних двух десятилетий. Ключевой работой можно считать специальный выпуск журнала IEEE “Trans. On Computers” в 1986 г., под редакцией A.Avizienis и J.-C. Laprie [1], которыми был сформулирован принцип “dependable computing” (гарантоспособных вычислений) как вычислений, устойчивых к отказам аппаратных средств и программных средств, т.е. к отказам, обусловленным проявлением их дефектов, внесенных при разработке и не выявленных при тестировании. Несмотря на то, что к этому времени уже существовали проекты, в первую очередь, в компьютеризированных аэрокосмических системах , которые в той или иной мере обеспечивали такую устойчивость, эта работа в методическом отношении инициировала развитие подходов, направленных на преодоление дуализма в инструментариях оценивания и гарантирования требуемой надежности по линиям «аппаратные - программные средства», «процессы разработки - продукты», «физические дефекты - дефекты проектирования». Такой дуализм существовал в теории надёжности КС [2] и не ликвидирован в полной мере до сих пор.

В том же году J. Dobson и B. Randell опубликовали работу [3], где определено понятие “secure fault tolerance” (безопасная отказоустойчивость), предложили принцип её реализации для различных КС, положив таким образом начало устранению дуализма по линии «надёжность (отказоустойчивость) - информационная безопасность».

Спустя восемнадцать лет A. Avizienis, J.-C. Laprie, B. Raudell и C. Landweher в [4] (базовой статье первого номера начавшего издаваться специального журнала IEEE “Trans. On Dependable and Secure Computing”) обобщили результаты и зафиксировали итоги развития гарантоспособных (как надёжных и безопасных) вычислений, определив достаточно полную и сбалансированную систему понятий и таксономических схем. К этому времени ‘dependability” как гарантоспособность («расширенная» надежность) была уже определена в том или ином виде в ряде стандартов, технических отчётов и монографий [5 – 7]. В русско- и украиноязычной литературе предпринимались две попытки легализовать ввести и стандартизовать термин «гарантоспособность». Первая из них – после выхода журнала [1], переведенного на русский язык, не оказалась удачной и ограничилась публикацией нескольких работ [8 – 10], в которых гарантоспособность определялась как свойство комплексной устойчивости к отказам аппаратных и программных средств, достигаемой благодаря использованию принципа многоверсионности. Вторая попытка, базирующаяся на работе [4], а точнее её более раннем варианте [7], сделана в [11 – 13], где дан эволюционный и содержательный анализ развития парадигм, методов и средств реализации гарантоспособных систем.

Цель данной работы – анализ терминологических, методологических и теоретических аспектов развития гарантоспособных компьютерных систем.

Статья включает описание основных понятий, связанных с гарантоспособностью и гарантоспособными системами (разделы 1, 2), анализ задач и принципов обеспечения гарантоспособности (разделы 3, 4), методов ее оценки (раздел 5).

1. Базовые понятия и таксономии

1.1. Гарантоспособность и её свойства

Свойство гарантоспособности далее рассматривается применительно к КС различного типа, включая, в первую очередь, компьютерные сети, системы распределённой обработки информации, web-системы и др. Ключевые понятия гарантоспособных КС базируются на результатах анализа работы [4] и имеют дискуссионный характер. Состояния, события и свойства определяются в терминах услуг, предоставляемых КС. С учётом этого можно говорить о КС как сервис-ориентированных компьютерных системах (СОКС).

Гарантоспособность - это способность КС предоставлять требуемые услуги, которым можно оправданно доверять. Гарантоспособность является комплексным свойством, включающим (рис. 1):

– *безотказность* (reliability) – свойство непрерывно предоставлять корректные (требуемые) услуги;

– *готовность* (availability) – свойство доступности ресурсов КС для предоставления требуемых услуг;

– *живучесть* (survivability) – свойство минимизировать снижение и сохранять в приемлемых пределах объём и качество предоставляемых услуг при отказах;

– *функциональная безопасность* (safety) – свойство исключать или минимизировать вредные (катастрофические) последствия при отказах для пользователей, других систем или окружающей среды;

– *целостность* (integrity) – свойство исключать непредусмотренные изменения системы и предоставляемых услуг;

– *конфиденциальность* (confidentiality) – свойство препятствовать неавторизованному доступу к информации об услугах;

– *достоверность* (high confidence) – свойство правильно оценивать корректность предоставляемых услуг, т.е. определять степень доверия к услуге;

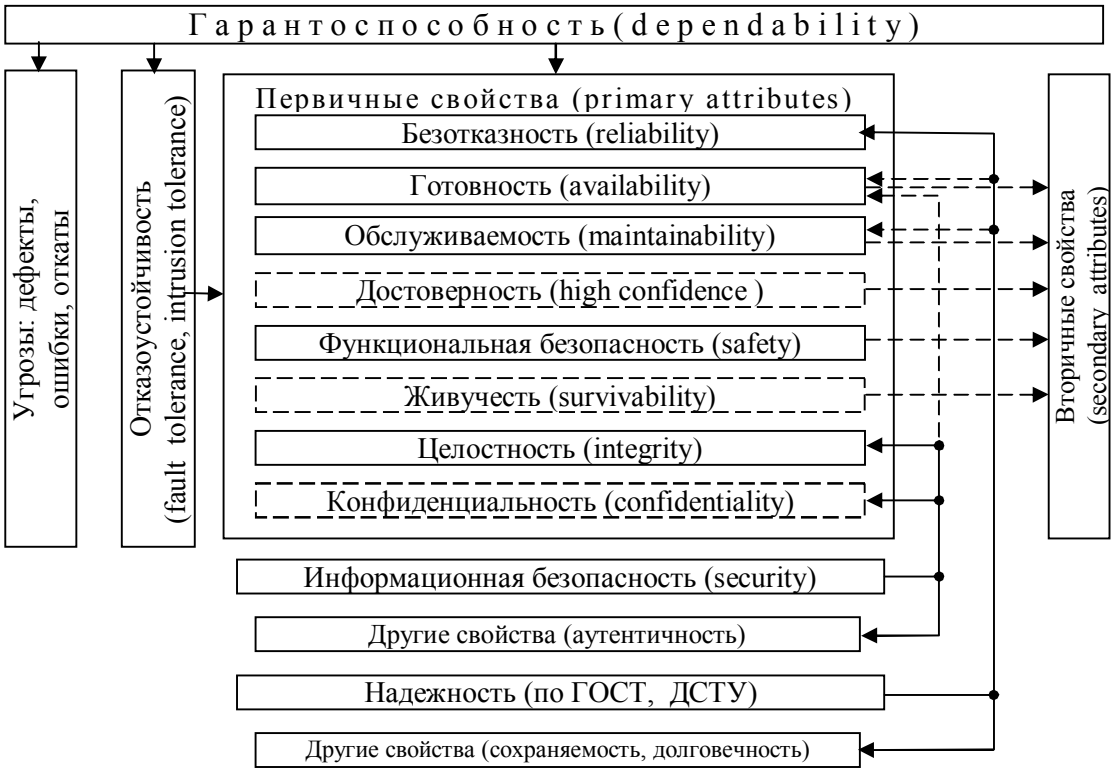

Рис. 1. Структура и взаимосвязь свойств гарантоспособности

– *обслуживаемость* (maintainability) – свойство приспособленности к модификациям и ремонту.

Рассмотренные свойства, составляющие гарантоспособность, являются первичными. Для каждого из них могут быть определены вторичные свойства. Например, для обслуживаемости такими могут являться ремонтопригодность (repairability), контролепригодность (chekability) и др. При этом вторичные и последующие свойства могут быть общими для различных первичных свойств, что является следствием их неполной «ортогональности».

Сопоставительный анализ приведенной выше таксономии свойств (рис. 1) с аналогичной таксономической схемой [4] показывает следующее.

1. В определение гарантоспособности включён термин «требуемые», т.е. специфицированные услуги, поскольку без этого размываются границы свойства.

2. По нашему мнению, включение свойств конфиденциальности и живучести как составляющих гарантоспособности зависит от назначения и специфики использования КС. Если не допускается доступ к информации об услугах, предоставляемых системой, то гарантоспособность должна включать конфиденциальность как обязательное свойство. Если допускается деградация (снижение) объема и качества предоставляемых услуг, то живучесть для таких КС должна рассматриваться как часть гарантоспособности. Кроме того, в данной работе в число первичных свойств включена достоверность, поскольку ею определяется одно из ключевых слов в формулировке гарантоспособности («...оправданно доверять»).

3. Гарантоспособность и информационная безопасность (security) имеют общие свойства (целостность и конфиденциальность) и специфические. Для безопасности - это, например, аутентичность. Включение в работе [4] готовности в число таких свойств, на наш взгляд, не является оправданным, так как оно имеет самостоятельный характер, хотя и зависит определенным образом от уровня информационной безопасности. Кроме того, свойство готовности не рассматривалось в ГОСТах и ДСТУ как первичное свойство надежности и могло представляться в их рамках как совокупность свойств безотказности и ремонтопригодности.

4. В [4] отказоустойчивость (fault tolerance) не рассматривается в отличие от [1] как свойство, составляющее гарантоспособность, а определяется как механизм, средство, поддерживающее другие свойства гарантоспособности. Такой подход к трактовке отказоустойчивости оправдан, поскольку с помощью рассмотренных средств может обеспечиваться (повышаться) и безотказность, и готовность, и безопасность, и живучесть.

1.2. Дефекты, ошибки, отказы. Модель состояний

Важной частью таксономии гарантоспособности [4] являются угрозы (threats), которые могут привести к непредоставлению услуг (рис. 1). При этом речь идёт, прежде всего, о дефектах или неисправностях (faults), которые имеют место вследствие различных причин.

В конечном итоге множество дефектов, классифицируемое по многим признакам, делится на три большие группы [14]: дефекты разработки (ДР) (development faults), физические дефекты (ДФ) (physical faults) и дефекты взаимодействия (ДВ) (interaction faults). Первые из них характерны, в первую очередь, для программных средств и проявляются при определённых условиях (входных данных), вторые – характерны для аппаратных средств и возникают вследствие естественных причин (например, старения элементов), третьи – являются следствием внешних воздействий (несанкционированных вмешательств или информационных атак, ошибок обслуживающего персонала, экстремальных воздействий физического характера, которые могут привести к кратным отказам аппаратных средств.

Дефекты являются причиной отказов КС. Отказы для СОКС имеют свою классификацию дефектов, определяемую, прежде всего, их последствиями. Цепочка событий, которые имеют место для различных дефектов такова [2, 4, 14]:

а) для ДР: *ошибочные* действия или решения при проектировании системы приводит к внесению *дефекта* в ее проект, который проявляется при использовании КС при определенных условиях и приводит к *ошибке* в вычислительном процессе, что вызывает *сбой* или *отказ* системы (в предоставлении услуги);

б) для ДФ: вследствие *естественных (внутренних) причин* возникает *дефект*, который приводит к *ошибке* в вычислительном процессе, приводящей к *сбою* или *отказу*;

в) для ДВ: вследствие внешних *воздействий* информационного, физического или иного характера появляется *дефект*, который вызывает *ошибку* вычислительного процесса и далее *сбой* или *отказ* КС.

Гарантоспособная система, в общем случае, имеет (рис. 2) множества работоспособных (и безопасных) состояний $MS_{РБС}$, частично работоспособных (и безопасных) состояний $MS^{i}_{ЧРБС}$, $i = \overline{1,d}$ (d – число допустимых уровней деградации) и полностью неработоспособных состояний $MS_{ПНРС}$. Если $d > 1$, можно говорить о свойстве живучести рассматриваемой системы. В состав $MS_{ПНРС}$ входят множества неработоспособных, но безопасных состояний $MS_{ФБС}$ и опасных состояний $MS_{ФОС}$. При этом последнее множество $MS_{ФОС}$ рассматривается как множество функционально опасных (аварийных) состояний, а множества $MS_{РБС}$ и $MS_{ЧРБС}$ объединяют состояния функционально безопасные. Что касается информационной безопасности, то она может обеспечиваться частично для множеств $MS_{ЧРБС}$. С учетом возможных типов отказов из-за ДР, ДФ и ДВ система из исходного исправного состояния S_0 переходит в состояния (подмножества состояний) $S_{ДР}$, $S_{ДФ}$ и $S_{ДВ}$ соответственно. Если эти дефекты возникают, но не обнаруживаются, система переходит в состояния (подмножества состояний) $S'_{ДР}$, $S'_{ДФ}$ и $S'_{ДВ}$.

При обнаружении дефектов и их парировании (устранении) система переходит в исправное состояние S0 в случае, если это не связано с включением резервных (использованием не пополняемых) ресурсов (аппаратных, программных) и таким образом остается в пространстве состояний множества MS РБС1. Это множество может включать и другие состояния, например, связанные с профилактикой, обновлением системы и т.д. (на рис. 2 не показаны).

Переход системы из состояний множества MS РБС1 в состояния множества MS РБСj, $j = \overline{2,n}$ вызвано уменьшением запаса ресурсов при сохранении в полном объеме ее функциональности. В случае пополнения ресурсов возможны обратные переходы. При невозможности сохранения полной функциональности системы (уровня основных характеристик) после возникновения новых дефектов ДР, ДФ или ДВ происходит переход в состояния из мно-

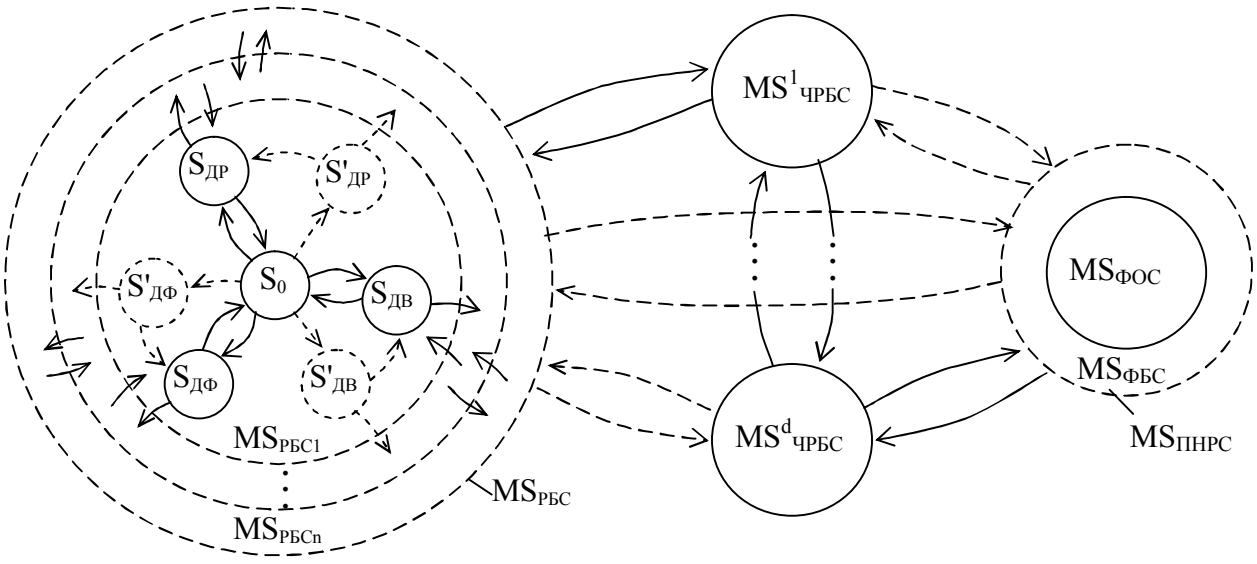

Рис. 2. Модель состояний гарантоспособной системы

жеств MS^i ЧРБС. Структура пространства состояний этих множеств аналогична структуре MS РБС. Далее могут осуществляться переходы в состояния $S_v \in MS$ ПНРС(MS ФОС). Пунктиром обозначены менее вероятные переходы, которые могут иметь место при кратных (однородных и неоднородных) дефектах или при пополнении ресурсов, обеспечивающем восстановление (переход) на несколько уровней «вверх».

Данная модель состояний и переходов является обобщением модели отказобезопасных систем [15, 16], поскольку учитывает аспекты как функциональной, так и информационной безопасности.

2. Гарантоспособные системы: эволюция парадигм

Гарантоспособная КС (ГКС) – это система, обладающая полным или частичным набором первичных свойств, составляющих гарантоспособность. При этом о ГКС имеет смысл говорить тогда, когда системе присущи как традиционные надежностные свойства (НС – безотказность, готовность), так и свойства информационной безопасности (ИБС – целостность, конфиденциальность). Гарантоспособность КС может обеспечиваться на основе традиционных для улучшения составляющих её свойств подходов. Как НС, так и ИБС повышаются путем: улучшения свойств компонент КС; организации контроля уровня свойств и восстановления работоспособного (защищенного) состояния при отказах, вызванных ДР, ДФ и ДВ; использования избыточности – различных методов резервирования компонент. Последнее из направлений является наиболее мощным, а иногда и единственным путем обеспечения, прежде всего, НС, а иногда и ИБС (агрегатирования методов криптозащиты).

Эволюционный анализ парадигм, методов и средств обеспечения гарантоспособности и ее свойств дан в [11, 12]. Начальная парадигма сформулирована в 50-е годы Джоном фон Нейманом [17] как «надежная (безотказная) система из ненадежных (небезотказных) элементов» (reliable system out of unreliable elements) (RS/URE). Системой в этом случае являлись релейно-контактные или простейшие цифровые устройства, а базовым механизмом – параллельное или мажоритарное резервирование (пассивная отказоустойчивость).

Далее, в 60 – 70-е годы она видоизменилась в направлении реализации активной отказоустойчивости: «надежная (отказоустойчивая) система из ненадежных компонент с контролем и реконфигурацией при отказах». Компонентами являлись уже интегральные микросхемы малой и средней интеграции и устройства на их основе, системами – компьютеры и КС.

80 – 90-е годы связаны с развитием парадигмы «надежные (отказоустойчивые) системы из ненадежных аппаратных и программных компонент», которая отражала возрастание веса программных средств как фактора ненадежности. В это время развился принцип многоверсионного проектирования и реализации КС, устойчивых к отказам, вызванных как ДФ, так и ДР. Параллельно была сформулирована парадигма «надежные и безопасные (secure) системы из ненадежных и небезопасных компонент».

Развитие Internet-технологий и СОКС (конец XX – начало XXI века) привело к обобщению этой парадигмы с учётом формирования концептуальной базы гарантоспособности КС [4, 7]. Впервые её формулировка «гарантоспособные системы из негарантоспособных компонент (dependable systems out of undependable components)" (DS/UDC)) дана в [17]. Затем она получила обоснование и содержательное наполнение применительно к СОКС и другим приложениям в [13, 18 – 20].

Следует отметить, что, во-первых, парадигма DS/UDC является следующим шагом к формулировке «хорошая система из плохих компонент (good system out of bad components)" (GS/BC) и её вариациям типа «быстродействующая система из медленных компонент» (многопроцессорные КС, системы распределённой обработки); во-вторых, приведенные формулировки парадигм RS/URE, DS/UDC,

GB/BC носят радикальный характер и более корректными должны быть следующие «системы (устройства) с требуемой надёжностью (безотказностью) из недостаточно надёжных (безотказных) элементов», «системы с достаточной гарантоспособностью из недостаточно гарантоспособных компонент» или «системы с требуемыми (лучшими) характеристиками» из компонент с недостаточными (худшими) характеристиками»; в-третьих, поскольку гарантоспособность КС (прежде всего, программных средств) зависит не только от продуктов разработки, а и процессов их создания (проектирования, тестирования и др.), то рассмотренные формулировки могут быть спроецированы и на процессы жизненного цикла КС. Важность такого подхода подтверждается применением многоверсионных технологий при разработке КС и реализацией концепции многоверсионного проекта в целом [21].

3. Задачи обеспечения гарантоспособности

Первичные свойства гарантоспособности тесно связаны между собой. Анализ их взаимовлияния представлен в [12, 13] в виде квадратной матрицы, столбцы и строки которой соответствуют свойствам гарантоспособности, а клетки (i, j) - вариантам изменения j-го свойства при улучшении (ухудшении) i-го свойства. Эта взаимозависимость носит противоречивый характер. Например, повышение свойств информационной безопасности (целостности, конфиденциальности) приводит, с одной стороны, к повышению готовности благодаря уменьшению вероятности успешных атак, которые могут вызвать останов КС для её восстановления, а с другой, – к дополнительным затратам времени на проведение профилактических работ (обновление программных средств и защитных функций), что может потребовать останова системы, и, следовательно, вызвать потери готовности. Это является дополнительным доказательством необходимости комплексного решения задач обеспечения гарантоспособности. К их числу могут быть отнесены следующие.

1. *Создание гарантоспособных Web-сервисов*, работающих в условиях отказов аппаратных средств (вследствие ДФ), программных средств (вследствие ДР) и отказов, обусловленных ДВ (атаками и экстремальными воздействиями). При этом в качестве компонентной базы используются коммерческие COTS (Commercial-Of-The- Shelf)- продукты, включая ранее разработанные целевые сервисы, объединяемые в вертикально и горизонтально композируемые Web-сервисы [18, 20, 22, 23] с помощью инструментальных платформ (контейнеров). В этом случае в полном объеме реализуется парадигма DS/UDC, поскольку речь идет о создании СОКС с требуемой (повышенной) гарантоспособностью из компонент – целевых сервисов с недостаточным ее уровнем. Возможна также реализация более общей парадигмы GS/BC, поскольку может достигаться улучшение не только гарантоспособности, но и реактивности, благодаря превышению выигрыша от получения информации от наиболее быстрого сервиса над потерями времени на интегрирование (обработку информации) от целевых сервисов (задержки среды Middleware).

В формализованном виде эта задача может быть представлена следующим образом.

Задача анализа. СОКС W объединяет множество целевых сервисов W_k, $k = 1, \ldots, K$), каждый из которых характеризуется вектором частных показателей показателем гарантоспособности $\Gamma_k = \{\Gamma_{kl}\}$, $l = 1, \ldots, L$, L – число показателей свойств гарантоспособности. Определить значение показателя гарантоспособности системы $W - \Gamma_W$.

Задача синтеза. Существует множество целевых сервисов $M_W = \{Wr\}$, $r = 1, \ldots, R$ с однотипной функциональностью и известными показателями Γ_r. Синтезировать СОКС W^*, объединяющую подмножество целевых сервисов $\Delta W \subset M_W$, такую что уровень гарантоспособности Γ_{W^*} будет не ниже требуемого $\Gamma_{тр}$ (максимальной), а затраты – минимальными (не более допустимых). В данной задаче могут дополнительно задаваться требования или ограничения по другим характеристикам (временным, функциональным).

2. *Оптимизация обслуживания гарантоспособных компьютерных систем* (*сетей*). Существует ряд задач, связанных с максимизацией показателей готовности обслуживаемых КС на основе выбора оптимальной периодичности и объема технического обслуживания с учетом отказов вследствие ДФ [24]. Эта задача нашла также свое экспериментальное решение для некоторых классов КС с учетом дефектов программных средств (ДР) [25]. Влияние внешних воздействий (дефектов ДВ) позволяет сформулировать задачу выбора (поиска) оптимальной стратегии обслуживания гарантоспособных КС с учетом всего множества дефектов. Другими словами, речь идет об оптимизации обслуживания компьютерной сети по показателю готовности как с точки зрения технического состояния (поддержки безотказности аппаратных и программных средств), так и с точки зрения ее информационного состояния (поддержания информационной безопасности путем обновления программных средств и модернизации средств защиты).

Для КС с планово–предупредительной системой профилактического обслуживания (жесткая стратегия, *Str*1), фиксированными объемами V_{rel}, V_{sec} и продолжительностями проведения технического τ_{rel} и информационного τ_{sec} обслуживания возможны два основных типа стратегий с раздельным *Str*1,*P* и общим *Str*1,*O* обслуживанием. В первом случае, с периодичностями T_{rel} и T_{sec} проводятся раздельное техническое и информационное обслуживание КС. Во втором случае проводится совместное обслуживание с периодичностью T_{dep}, продолжительность которого $\tau_{dep} \le \tau_{rel} + \tau_{sec}$. Задача, таким образом, сводится к поиску оптимальных T_{rel} и T_{sec} для стратегии *Str*1,*P* и T_{dep} для стратегии *Str*1,*O*.

Альтернативой стратегии *Str*1 является стратегия гибкого управления по техническому состоянию *Str*2 [24], в которой периодичность и объем обслуживания не являются фиксированными, а зависят от фактических значений показателей надежности (безотказности) и потерь (выигрыша) в готовности при проведении обслуживания и устранении неисправностей. Для КС можно перейти от концепции управления по фактическому техническому состоянию (ФТС) к концепции интегрированного управления по фактическому техническому и информационному состоянию (ФТИС) или управлению гарантоспособностью по ФТИС. При использовании гибких стратегий обслуживания *Str*2, объем, продолжительность и периодичность (или момент начала) обслуживания являются оптимизируемыми показателями. Очевидно, что в этом случае также возможны две субстратегии с раздельными и смешанным обслуживанием *Str*2,*P* и *Str*2,*O*.

4. Принципы обеспечения и разработки гарантоспособности

4.1 Механизмы отказоустойчивости

В соответствии с таксономией [4] и её модификацией, иллюстрируемой рис. 1, отказоустойчивость является базовым механизмом (средством) обеспечения гарантоспособности. Он основан на реализации в полном, или усеченном виде цепочки действий (операций): *прогнозирование* (fault forecasting, F_f) возможности появления (проявления) дефекта и возникновения отказа вледствие этого дефекта; *предупреждение* (fault prevention, F_p) появления (проявления) дефекта и возникновения отказа; *обнаружение* (fault detection, F_d) появления (проявления) дефекта, ошибки вычислений, отказа; *идентификация* (fault diagnosis, F_i) причины, вида и места дефекта (отказа); *парирование* (fault tolerance, F_t) последствия дефекта и возникновения отказа. Последнее действие может включать: реконфигурацию (fault removal, F_r) структуры (архитектуры) путем исключения отказавшего компонента из конфигурации, замены работоспособным и восстановление вычислительного процесса (fault recovery, F_c).

Каждый из методов обеспечения отказоустойчивости может быть препарирован исходя из наличия и особенностей реализации элементов множества $M_F = \{F_f, F_p, F_d, F_i, F_t, F_r, F_c\}$. Например (табл. 1), обычное

мажоритарное резервирование (2 из 3) обеспечивает отказоустойчивость посредством операции F_t (символ), адаптивное мажоритарное резервирование (АМР) – посредством операций F_d (обнаружение факта отказа второго канала), F_i (идентификации работоспособного канала), F_t (парирования последствий отказа первого, а затем и второго канала), F_r (реконфигурации структуры из мажоритарной в одноканальную конфигурацию), и, при необходимости, F_c (восстановления информации после прерывания).

Таблица 1

Анализ методов обеспечения отказоустойчивости

Методы обеспечения отказоустойчивости	Операции						
	F_f	F_p	F_d	F_i	F_t	F_r	F_c
Мажоритарное резервирование (2 из 3)	-	-	-	-	+	-	-
Адаптивное мажоритарное резервирование (2 из 3 > 1 из 1)	-	-	+	+	+	+	±
Адаптивное мажоритарное резервирование с рейтингованием каналов	+	±	+	±	+	±	±

Максимально полной может быть процедура обеспечения отказоустойчивости при реализации АМР с рейтингованием каналов – учетом числа ошибок в процессе функционирования, которое позволяет парировать (F_t), а в некоторых случаях (символ) и предупреждать (F_p) возникновение отказов. Такой метод может реализовываться, например, в СОКС, объединяющих целевые сервисы с помощью специальной среды взаимодействия Middleware, механизмов рейтингования и обработки исключений [22, 23, 26].

Необходимо подчеркнуть, что механизмы отказоустойчивости в гарантоспособных системах должны быть инвариантны по отношению к типам дефектов, вызывающих отказы. Появившийся термин “intrusion tolerance” (устойчивость к “вторжениям”, т.е. к отказам, обусловленным дефектами взаимодействия) и получающий все более широкое распространение в англоязычной литературе является отражением не только автономности, но и важности свойств информационной безопасности (и живучести) в составе гарантоспособности. В то же время представляется целесообразным разработка унифицированных процедур анализа вида и последствий отказов, учитывающих как ДФ и ДР, ТАК и ДВ в рамках технологии FME(C)A [27].

4.2. Принцип диверсности (многоверсионности)

Учитывая различную природу дефектов ДР, ДФ, ДВ и последствий, вызываемых ими отказов, средства, реализующие операции из множества M_F, для них могут быть раздельными. Другими словами, ГКС в этом случае будет иметь три подсистемы, выполняющие функции $F_i \in M_F$ для каждого из типов дефектов WFДФ, WFДР и WFДВ, соответственно (рис. 3, а). Интегрированными могут быть средства реализации функции восстановления информации WFC.

Очевидно, что раздельная реализация подсистем приводит к большим затратам программно-аппаратных средств, что делает подсистему обеспечения гарантоспособности сложной, а следовательно, недостаточно надежной. Таким образом, важно иметь концептуальные подходы, которые бы позволили комплексно решать проблемы обнаружения и парирования отказов, вызванных физическими дефектами аппаратных средств, дефектами проектирования программных средств и внешними воздействиями информационного и иного характера.

Один из таких мощных подходов базируется на *принципе диверсности* (*многоверсионности*). Использование этого принципа позволило на первом этапе решить задачи создания КС, устойчивых к ДФ и ДР, благодаря тому, что снижается вероятность отказа по общей причине вследствие дефектов программных средств из-за применения в резервных каналах системы различных программных версий [1, 2].

Далее оказалось, что использование диверсности позволяет улучшить и свойства информационной безопасности (целостности и конфиденциальности) [29,30]. В частности, теоретически и эксперименталь-

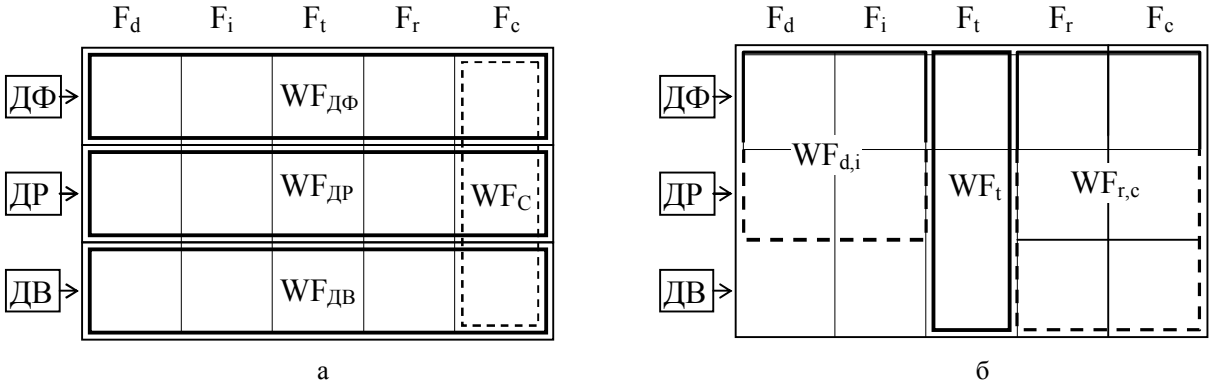

Рис. 3 . Варианты реализации функций отказоустойчивости в одно- (а) и многоверсионной (б) ГКС

но доказана эффективность реализации двухверсионной цифровой подписи, многоверсионной блочной криптозащиты. Кроме того, использование диверсности открывает большие возможности для повышения безопасности СОКС благодаря введению механизмов адаптивного выбора диверсных конфигураций web-серверов, операционных систем и приложений с учетом накопления и динамичного обновления информации об уязвимости различных типов компонент на этих уровнях относительно различных типов атак [28, 30, 31]. Таким образом, можно говорить о реальной осуществимости интегрированных систем обеспечения гарантоспособности не только по дефектам ДФ и ДР, что уже используется на практике, а и по дефектам ДВ (рис. 3, б). Для СОКС при использовании принципа диверсности объединяются средства выполнения операций F_t (подсистема W_{Ft}) и возможно частичное или полное объединение средств для выполнения операций F_d, F_i (подсистема *WFd,i*) и F_r, F_c (подсистема *WFr,c*).

Принцип многоверсионности (МВ) может эффективно дополняться принципами *многопараметрической адаптации* (МА) *и многоуровневой управляемой деградации* (МД) в единой концепции, получившей название 3М [32]. МА предполагает организацию нескольких программно реализуемых и аппаратно поддерживаемых контуров управления реконфигурацией с учетом видов и числа отказавших компонент, а МД – перераспределение избыточных и неизбыточных, но мобильных ресурсов (и коррекцию, при необходимости, целей функционирования) для минимизации объемов деградации.

4.3. Жизненный цикл гарантоспособности систем

Различные проектные решения гарантоспособных систем должны обеспечивать требуемый уровень свойств надежности и безопасности. Разработка конкретных технологий проектирования и верификации ГКС, учитывая сложность и комплексность задачи, требует уточнения моделей жизненного цикла. По аналогии со стандартизованной общей моделью жизненного цикла функциональной безопасности (или функционально безопасных) программного обеспечения и информационно-управляющих систем (safety life cycle), проанализированных в [33, 34] имеет смысл разработать модель *жизненного цикла гарантоспособных систем* (dependable system life cycle).

Если гарантоспособность системы и ее ПО обеспечивается за счет диверсности, то в основу такой модели может быть положена модель *многоверсионного жизненного цикла* [35], базирующаяся на операциях генерации и выбора версий на различных этапах и при реализации различных процессов.

5. Об оценке гарантоспособности

Учитывая комплексный характер гарантоспособности как сложного свойства для его оценки могут использоваться два типа показателей: векторные, которые представляют собой набор показателей,

оценивающих либо отдельные свойства гарантоспособности (безотказность, готовность, целостность) либо устойчивость к различным типам дефектов (ДФ, ДР, ДВ); скалярные, с помощью которых дается обобщенная оценка.

Простейший вариант скалярного показателя представляет собой *вероятность представления услуги* СОКС, P_{dep}, которая при определенных допущениях (независимости дефектов разных типов) может быть вычислена как произведение вероятностей отсутствия (парирования) дефектов из множества M_D = {ДФ, ДР, ДВ}. Далее эти вероятности могут быть вычислены с учетом вероятностей успешного выполнения всех операций из множества M_F (и допущения о независимости отказов соответствующих средств). Тогда

$$P_{dep} = \prod_{i:\, D_i \in M_D} \prod_{j:\, F_j \in M_F} P_{ij} ,$$

где P_{ij} – вероятность успешного выполнения операции F_j для дефектов типа D_i.

Для более точной оценки требуется детально проанализировать множество состояний и переходов между ними на базе общей модели (рис. 2) для конкретных приложений, используя аппарат теории марковских или полумарковских процессов.

Скалярная оценка может быть получена также на основе *метрического подхода*, при котором строится максимально детализированная модель гарантоспособности как иерархии первичных, вторичных свойств, их характеристик, определяемых набором метрик, оцениваемых экспертным путем или вычисляемых на основе измеряемых параметров системы. Далее может быть выполнена свертка метрик, поддерживаемая и визуализируемая с помощью радиальных метрических диаграмм [36].

Заключение. От кризиса к развитию

Проблемы, возникшие в теории надежности компьютерных систем, по существу, являются следствием динамичных изменений в КТ, не нашедших адекватного отражения, прежде всего, в ее понятийной базе и методах оценки. Кроме того, параллельное развитие родственных дисциплин – теории функциональной и, особенно, информационной безопасности не способствовало интегративным процессам в силу их самодостаточности. Однако, дальнейшее сохранение параллелизма существенно ограничивает возможности поиска эффективных решений (cost-effective decisions) для широкого класса КС, в частности, сервис-ориентированных, где отказ (невыполнение функций) может быть вызван всем спектром дефектов (ДФ, ДР, ДВ). Поэтому целесообразно, на наш взгляд, сохраняя полную автономность указанных теорий, развивать их интеграцию в рамках теории гарантоспособных систем. Это позволит ликвидировать как внутренний дуализм теории надежности КС (аппаратные и программные средства, процессы и продукты), так и внешний дуализм по линии «надежность и безопасность».

Как и для всякой междисциплинарной теории, число нерешенных проблем в области ГКС существенно превышает число решенных. Во-первых, требует своего развития и совершенствования понятийная база. Здесь, одним из ключевых представляется вопрос об информационно-техническом состоянии, которое может уточнить понятие отказа как события, связанного с потерей работоспособности вследствие ДФ, ДР, ДВ и сформировать множество стратегий управления гарантоспособностью. Кроме того, целесообразно рассмотреть вопрос о развитии национальной нормативной базы, связанной с гарантоспособностью КС. Во-вторых, важным направлением исследований является разработка методов оценки гарантоспособности. При этом следует учитывать расширение множества возможных ошибок по идентификации состояния гарантоспособной системы. При анализе возможных отказов целесообразно использовать единые F(I)MEA-методики, учитывающие все аспекты отказо- и атакоустойчивости (fault- и intrusion-tolerance) [27]. Поскольку практическое воплощение и тиражирование СОКС на основе web-

технологий заметно опережает теоретические исследования, весьма актуальным представляется развитие методов экспериментального оценивания с использованием как существующих средств и технологий, так и их модернизированных аналогов. В-третьих, своего дальнейшего совершенствования требуют конкретные методики обеспечения гарантоспособности КС и ее свойств в рамках принципа многоверсионности и других базовых принципов, которые позволяют получить комплексные решения в пространстве множеств операций M_F обеспечения устойчивости к различным дефектам.

При разработке технологий проектировании ГКС целесообразно базироваться на модели жизненного цикла гарантоспособности, объединяющей процессы и специальные решения по ее обеспечению и верификации.

Литература

1. Avizienis A., Laprie J.-C. Dependable Computing: From Concepts to Application // IEEE Trans. on Computers. – 1986. – №74 (5). – P. 629-638.
2. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х.: МОУ, 1996. – 503 с.
3. Dobson I.E., Randell B. Building Reliable Secure Computing Systems out of Unreliable Insecure Components // Proc. of the IEEE Conference on Security and Privacy, Oakland, USA. – 1986. – P.187-193.
4. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol.1, № 1. – P. 11-33.
5. ITU-T. Terms and Definitions Related to QoS and Network Performance Including Dependability. Recommendations E800. – Geneva, 1994. – 65 p.
6. Соммервил И. Инженерия программного обеспечения. – СПб.: Вильямс, 2002. – 624 с.
7. Laprie J.-C., Avizienis A., Randell B. Fundamental Concepts of Dependability // Technical Report: UCLACSD Report no. 010028, LAAS Report no. 01-145, Newcastle University Report no.CS-TR-739. – 2002. – 31 p.
8. Харченко В.С., Паршин В.В. Многоверсионные системы и обеспечение гарантоспособности. – Препринт №321. – Х.: ИПмаш, 1989. – 33 с.
9. Харченко В.С. Исследование гарантоспособных структур УВС // Проектирование многомашинных комплексов реального времени. – М.: Знание.- 1990. – С.58-61.
10. Харченко В.С. Модели и свойства отказоустойчивых многоальтернативных систем // Автоматика и телемеханика. – 1992. – № 12. – С.140-147.
11. Харченко В.С. От безотказности электронных устройств к гарантоспособности web-систем // Контрольно-измерительные приборы и автоматика. – 2004. – № 9.- С.4-10.
12. Харченко В.С. Эволюция фон-неймановской парадигмы: гарантоспособные системы из негарантоспособных компонент // Системы обработки информации. – Х.: ХВУ, 2004. – № 8 (36). – С.11-19.
13. Харченко В.С. Гарантоздатність КС: проблеми та результати // Авіаційно-космічна техніка і технологія. – 2005. – № 7(23). – С.352-357.
14. Одарущенко О. Н. Поночовный Ю.Л., Одарущенко Е.Б. Терминологические аспекты теории надежности программных средств // Радиоэлектронные и компьютерные системы. – №2 (6). – С. 88-94.
15. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. – М.: Радио и связь, 1989.– 208 с.
16. Харченко В.С., Скляр В.В., Токарев В.И. Модели отказобезопасных структур цифровых систем контроля и управления // Системи обробки інформації. – Х.: ХВУ, 2003. – Вип. 4.– С. 200-205.
17. Фон-Неман Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент // Автоматы. – М.: ИЛ. - 1956. – С.68-139.
18. CS-TR: 863. Development of Dependable Web Services out of Undependable Web Components/ A. Gorbenko, V. Kharchenko, P. Popov, A. Romanovsky, A. Boyarchuk. School of Computing Science, University of Newcastle, Oct. 2004. – 36 p.

19. CS-TR: 879. Dependable Composite Web Services with Components Upgraded Outline: Solutions, Model and Implemenmtation / A. Gorbenko, V. Kharchenko, P. Popov, A. Romanovsky. School of Computing Science, University of Newcastle, Dec. 2004. – 25 p.

20. Gorbenko A., Kharchenko V., Popov P., Romanovsky A. Dependable Composite Web Services with Components Upgraded Online // In R. de Lemos et al. (Eds.): Architecting Dependable Systems III, LNCS 3549. Berlin, Heidelberg: Springer-Verlag. – 2005.– P. 92 – 121.

21. Харченко В.С. Многоверсионные системы, технологии и проекты. – Х.: НАКУ "ХАИ", Мин. образования и науки Украины. – 2003. – 528 с.

22. Инструментальная платформа для создания гарантоспособных композитных (нтегрированных) web-сервисов “INDECS” / В.С. Харченко, А.В. Горбенко и др // Труды Межд. Конф. "Информационные технологи в науке, производстве, образовании". – Х.: ХНУРЭ, 2005. – С. 35-37.

23. Coordinated Forward Error Recovery for Composite Web Services / F. Tartanoglu and s.o. // Proc. of the 22th Symposium on Reliable Distributed Systems (SRDS), Florence, Italy, 2003. – P. 167–176.

24. Волков Л.И. Управление эксплуатацией ЛК. – М.: Машиностроение, 1986. – 291 с.

25. Харченко В.С., Асидех Ф.А., Лисенко И.В. Марковские модели готовности восстанавливаемых STRATUS-систем // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 4. – С. 216-226.

26. Kharchenko V., Popov P., Romanovsky A. On Dependability of Composite Web Services with Components Upgraded Online // Proc. of Workshop on Architecting Dependable Systems (DSN 2004), Italy, 2004. – P. 14-20.

27. Gorbenko A.V., Kharchenko V.S., Tarasyuk O.M. FMEA-technique of Web Services Analysis and Dependability Ensuring // Proc. of the Workshop on Rigorous Engineering of Fault-Tolerant Systems (REFT’2005), Newcastle, UK, 2005. – P. 74–83.

28. Лысенко И.В., Халин М.В., Харченко В.С. Анализ и разработка методов и средств защиты информации с использованием многоверсионных технологий. – Отчет по НИР № 0104U003502 "Разработка научно-методических основ и информ. технологий оценки и обеспечения отказоустойчивости и безопасности компьютеризированных систем аэрокосмических комплексов критического применения" / Научн. рук. Харченко В.С. – НАКУ "ХАИ", 2003. – С.415-445.

29. Харченко В.С., Халин М. Многоверсионность для обеспечения конфиденциальности и целостности информации: модели и методы // Информационные технологии и системы. – К.: НАУ. – 2004, № 1. – С.45-50.

30. Garfinkel S., Spafford G. WebSecurity, Privacy, and Commerce. – Beijing, Cambridge, Farnham, Köln, Paris, Sebastopol’**,** Taipei, Tokio: Reilly. – 2002. – 756 p.

31. Харченко В.С., Фурманов А.А. Обеспечение устойчивости web-приложений к сетевым атакам с использованием диверсного подхода // Материалы 2-й НТК ХУ ПС. – Х.: МОУ, 2006. – С. 87.

32. Харченко В.С., Токарев В.И. Проектирование отказоустойчивых и живучих КС управления на основе концепции “3М” // Вісник Технологічного університету Поділля.– 2003. – №3. – С.29-32.

33. Информационно-управляющие системы АЭС: проблемы безопасности / М.А. Ястребенецкий, В.Н. Васильченко, В.С. Харченко и др. – К.: Техника, 2004. – 502 с.

34. Липаев В.В. Функциональная безопасность программного обеспечения. – М.: Синтег, 2005. – 224 с.

35. Волковой А.В., Скляр В.В., Харченко В.С. Метод формирования моделей многоверсионного жизненного цикла для программных проектов // ІКСЗТ. – 2004. – № 2 (46). – С. 40-44.

36. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: НАКУ "ХАИ". – 2004. – 159 с.

Поступила в редакцию 24.01.2006

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.