УДК 681.5

В.С. ХАРЧЕНКО

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

ПАРАДИГМЫ И ПРИНЦИПЫ ГАРАНТОСПОСОБНЫХ ВЫЧИСЛЕНИЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Анализируются таксономические, методологические и технологические аспекты гарантоспособных вычислений. Обсуждается парадигма "гарантоспособных систем из негарантоспособных компонент" и ее применение для различных приложений: от естественно надежных кристаллов до сложных инфраструктур. Анализируются принципы и методы оценки и обеспечения гарантоспособности, реализации многоверсионности и мультиреконфигурации при создании гарантоспособных систем. Обобщаются примеры применения парадигмы при разработке систем на программируемой логике, web-систем и др.

Ключевые слова: *гарантоспособность, компьютерные системы, инфраструктура, надежный кристалл, многоверсионность.*

Введение

Растущая зависимость общества, окружающей среды, социально-технических систем от информационных технологий (ИТ) проявляется в двух противоречивых тенденциях. С одной стороны, динамично расширяется набор ИТ-продуктов и услуг, ставших неотъемлемой частью жизни социума, а с другой, - растут риски, сопровождающие процесс ускоряющейся зависимости функциональности, надежности и безопасности аварийно опасных систем, критических инфраструктур с интенсивным использованием ИТ от качества решений, получаемых и реализуемых с помощью этих технологий.

Данная зависимость и возрастание рисков, связанных с ИТ, проявляется в таких, казалось бы разных областях как атомная энергетика и ракетно-космическая техника, не только в схожести причин отдельных аварийных ситуаций или предпосылок к ним, а и статистических данных об отказах, приведших к возникновению таких ситуаций [1-4].

Авария ракеты-носителя «Ариан-5» была обусловлена недостаточной верификацией программного модуля системы навигации, который был перенесен в новый проект после многократного использования в предыдущих проектах. Аналогичные причины возможного отказа имели место в системе автоматического регулирования турбин АЭС, которые были обнаружены в процессе испытаний и могли бы привести к инциденту в процессе дальнейшей эксплуатации [2]. Каждая пятая авария ракетно-космических комплексов в 1990-2000-е годы связана с отказами компьютерных систем (КС) управления [3]. Такая тенденция сохраняется и в последующем десятилетии. Схожие данные характерны для АЭС за последние 15 лет, также примерно 20% отказов оборудования приходится на долю информационно-управляющих систем (ИУС) [4].

Возросшая зависимость надежности и безопасности технических комплексов критического применения (ККП) от ИУС нормативно закреплена в стандартах ISO/IEC посредством понятия «функциональная безопасность», определяющего «вклад» ИУС в безопасность комплекса в целом. Несмотря на колоссальные затраты, направленные на повышение их информационной безопасности, все более уязвимыми становятся КС и сети бизнес-критических инфраструктур для несанкционированного доступа. Известны случаи проникновения в компьютерные коммуникации космических аппаратов, ставившие под угрозу управляемость и безопасность специальных систем, многочисленные факты взлома банковских систем, приведших к материальным потерям. С другой стороны, к таким же материальным потерям приводят сбои и отказы КС.

Следовательно, можно сделать выводы о том, что:

– проблема надежности, информационной и функциональной безопасности КС ККП, объединяемых понятием «гарантоспособность» [5 – 7], становится все актуальнее;

– внедрение новых компьютерных технологий должно сопровождаться анализом и выработкой адекватных мер парирования возможных рисков;

– характеристики аппаратных и программных компонент, используемых для создания КС ККП, не обеспечивают требуемые надежность и безопасность, что обусловливает необходимость реализации адекватных системных концепций и решений;

– задачи обеспечения заданных показателей гарантоспособности (надежности и безопасности) должны решаться совместно.

Цель данной работы – краткий обзор и анализ путей решения проблем в области создания гарантоспособных компьютерных систем (КС) и гарантоспособных вычислений (dependable computing) в целом. Эта работа является естественным развитием идей, представленных в [5], и результатов последующих исследований [6 – 16], проводившихся в последние годы на кафедре компьютерных систем и сетей Национального аэрокосмического университета «ХАИ» и научно-техническом центре гарантоспособных компьютерных систем, сервисов и технологий (DESSERT-центре www.stc-dessert.com).

Данная работа имеет обзорный характер. Учитывая ограниченный объем, принят конспективный стиль изложения без детального анализа результатов и полного реферирования списка публикаций.

1. Таксономия

Термин «гарантоспособность» пока не получил толкования в национальной нормативной базе, хотя и используется в течение последних 15-20 лет, наполняясь новым содержанием. После публикации работ [5 – 7], обсуждения различных аспектов гарантоспособности в Украине на 1-3-й Международных конференциях «Гарантоспособные системы, сервисы и технологии» (DESSERT'06-08 http://www.stc-dessert.com/conf2008/) в рамках реализации Национальной космической программы специалистами кафедры и Сертификационного центра АСУ (Госкомцеткачества ГК ЯРУ) по заказу НКАУ подготовлен отраслевой стандарт «Гарантоздатність програмно-технічних комплексів космічних систем». В этом стандарте обобщены эти результаты с учетом специфики требований к космическим системам.

Элементы таксономии. Под *гарантоспособностью* (ГС) понимается комплексное свойство системы предоставлять требуемые услуги, которым можно оправданно доверять. Таксономическая схема ГС включает следующие элементы: *угрозы и воздействия* на систему, которые могут привести к негативному (непредусмотренному) изменению ее состояния и характеристик; *механизмы парирования* этих угроз (отказоустойчивости и отказобезопасности); *первичные* и производные от них индивидуальные и общие *вторичные свойства*, отражающие различные аспекты ГС. Кроме того, важным элементом такосономической схемы является понятие информационно-технического состояния, позволяющего объединить аспекты функциональной и информационной безопасности.

Свойства. К числу первичных свойств ГС в общем случае относятся следующие: *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; *обслуживаемость* (maintainability) – свойство приспособленности к модификациям и ремонту.

К числу вторичных свойств могут быть отнесены, например, для обслуживаемости – ремонтопригодность (repairability), контролепригодность (checkability, testability), для живучести – стойкость (stability, resistance) и т.д. Профиль первичных и вторичных свойств зависит от конкретного типа КС и может включать часть свойств.

Угрозы. К числу угроз относятся, прежде всего, дефекты и вызываемые ими отказы и сбои. Различают три основные группы дефектов [5]: *дефекты разработки* (ДР) (development faults); *физические дефекты* (ДФ) (physical faults) (аппаратных средств, возникающие вследствие естественных причин, например, старения элементов); *дефекты взаимодействия* (ДВ) (interaction faults) (вследствие внешних несанкционированных вмешательств или информационных атак, ошибок обслуживающего персонала, экстремальных воздействий физического характера).

Каждому из дефектов соответствуют свои «патологические» цепочки:

– *для ДР*: ошибочные действия или решения при проектировании системы, разработке программных средств приводят к внесению дефекта, который проявляется при использовании КС в определенных условиях и вызывает ошибку в вычислительном процессе. Это вызывает сбой или отказ системы;

– *для ДФ*: вследствие естественных (внутренних) причин возникает дефект аппаратных средств, вызывающий ошибку вычислительного процесса, сбой или отказ;

– *для ДВ*: вследствие внешних воздействий появляется дефект (нарушение информационной или технической составляющей состояния системы), который вызывает ошибку вычислительного процесса и далее сбой или отказ КС, либо несанкционированно становятся доступными для внешней системы или искажаются данные, циркулирующие или хранящиеся в системе.

Информационно-техническое состояние (ИТС). Под *ИТС* следует понимать совокупность свойств и признаков как технического, так и информационного характера, присущих системе в определенный момент времени. Эта совокупность может быть специфицирована в более широком контексте, чем техническое состояние, и определять критерии классификации состояний КС (ИУС).

В контексте ИТС множество состояний (исправных-неисправных, работоспособных-частично работоспособных-неработоспособных, безопасных-потенциально опасных-опасных или критических) рассматривается с учетом того, что переходы между ними осуществляются как вследствие ДФ, ДП, так и из-за ДВ. Если такие дефекты вызовут или искажение информации, или несанкционированный доступ к ней (что не допускается по условиям ее использования согласно техническому заданию), это можно толковать как переход системы в неисправное, неработоспособное или опасное состояние в зависимости от масштаба последствий такого перехода. Отметим, что необходимость комплексного рассмотрения состояний ИУС подтверждается тем, что наличие одних дефектов создают условия для возникновения других. Наиболее характерной является такая зависимость между ДП программных средств и ДВ информационного типа, поскольку ДП могут становиться причиной так называемых уязвимостей (vulnerability) программных компонент, которые используются для нарушения целостности и безопасности КС.

Профиль гарантоспособности. *Гарантоспособная КС* (ГКС*)* – это система, обладающая полным или частичным набором первичных свойств, составляющих ГС. О гарантоспособности и ГКС имеет смысл говорить тогда, когда системе присущи как традиционные надежностные свойства (безотказность, готовность), так и свойства функциональной и информационной (целостность, конфиденциальность) безопасности. *Профиль гарантоспособности* (набор необходимых свойств и их показателям) определяется исходя из требований к системе.

2. Парадигмы

Эволюционный анализ парадигм, методов и средств обеспечения гарантоспособности и ее свойств дан в [6, 7].

В процессе анализа выявляются и формализуются этапы развития систем и парадигм. Элементами анализа являются: типы компонент, из которых складывается система; собственно система (уровень ее сложности); свойства компонент и систем в целом (от безотказности до гарантоспособности); базовый механизм, методы и средства обеспечения системных свойств.

Начальная парадигма сформулирована *в 50-е годы* Джоном фон Нейманом 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).

В *60 – 70-е годы* она видоизменилась в виде реализации активной отказоустойчивости: «*надежная (отказоустойчивая) система из ненадежных компонент с контролем и реконфигурацией при отказах*». Компонентами являлись МИС и СИС 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 формируется принцип многоверсионного проектирования и создания 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 (конец XX – начало XXI века) привело к обобщению этой парадигмы с учетом расширившейся таксономии гарантоспособности КС.

Она формулируется как парадигма «*гарантоспособных систем из негарантоспособных компонент* (dependable systems out of undependable components)» (DS/UDC)) [6 – 10].

Далее можно говорить об этапе, связанном с развитием концепции инфраструктур или «системы систем». Для него парадигма может модернизироваться к виду «*гарантоспособные инфраструктуры из негарантоспособных систем* (dependable infrastructures out of undependable systems)» (DI/UDS))

3. Принципы

При обеспечении гарантоспособности необходимо отказ рассматривать в контексте ИТС, и выделять принципы, позволяющие улучшать как надежность, так и безопасность КС.

3.1. Отказоустойчивость и отказобезопасность

Отказоустойчивость является базовым механизмом обеспечения гарантоспособности.

Операционный цикл отказоустойчивости. Отказоустойчивость основана на реализации в полном или усеченном виде цепочки действий (операций), образующих операционный цикл [7]: *прогнозирование* (fault forecasting, F_f) возможности появления (проявления) дефекта и возникновения отказа вследствие этого дефекта; *предупреждение* (fault prevention) появления (проявления) дефекта и возникновения отказа; *обнаружение* (fault detection) появления (проявления) дефекта, ошибки вычислений, отказа; *идентификация* (fault diagnosis) причины, вида и места дефекта (отказа); *парирование* (fault-tolerance) последствия дефекта и возникновения отказа путем *отключения* (fault insulations) отказавших элементов и/или *изоляции* искаженной информации и *реконфигурацию* структуры (архитектуры) за счет блокирования отказавшего компонента из конфигурации и замены работоспособным; *восстановление* вычислительного процесса (fault recovery).

Операционный цикл имеет свои особенности и составляющие для разных дефектов и для некоторых первичных свойств гарантоспособности. В последнее время развивается подход, названный *"self-healing"*, когда фактически к циклу отказоустойчивости добавляются операции, связанные с ремонтом («самолечением») системы с использованием внешних и внутренних ресурсов.

Особенности цикла отказобезопасности. Для систем, важных для безопасности, одной из таких составляющих является отказобезопасность. Она представляет собой механизм парирования отказов, которые могут привести к переходу системы в опасные состояния, либо минимизации последствий такого перехода.

Другими словами, отказобезопасность является одним из механизмов обеспечения функциональной безопасности подобно тому, как отказоустойчивость является механизмом обеспечения надежности и гарантоспособности в целом.

По аналогии могут быть определены понятия устойчивости к дефектам взаимодействия, информационным вторжениям (intrusion-tolerance), а также к физическим воздействиям, когда используются либо специальные физические средства защиты, либо архитектурные решения.

3.2. Многоверсионность и многоверсионные вычисления

Сущность и задачи. Сущность многоверсионности (МВ) как принципа обеспечения ГС – использование *различных продуктовых* (аппаратно-программных) и *процессных средств* для реализации идентичных функций с целью:

а) *создания КС, устойчивых к ДФ и ДР*, благодаря снижению вероятности отказа по общей причине из-за применения в резервных каналах системы различных программно-аппаратных версий (многоверсионных систем (МВС));

б) *повышения полноты и достоверности верификации* программного обеспечения и КС в целом благодаря использованию диверсных независимых процессов и средств проектирования и тестирования и снижению рисков не выявленных дефектов;

в) *улучшения информационной безопасности (*целостности и конфиденциальности) применением многоверсионной цифровой подписи, блочной криптозащиты, адаптивного выбора диверсных конфигураций web-серверов, ОС, БД [11].

При разработке должны быть решены задачи (а при анализе и экспертизе оценены результаты решения): *обоснованности применения (неприменения) МВ* как средства обеспечения ГС; *выбора вида версионной избыточности* и вариантов архитектур МВС; определения *реальной степени МВ* и возможных *негативных последствий* использования диверсности.

Модели МВС. Теоретико-множественная модель МВС S описывается входным X и выходным алфавитами Z, множествами выполняемых функций F, настроек выбора C, версий реализации V и формирования выходных данных U по результатам выполнения версий $v_i \in V$. Существуют автоматные модели, описывающие МВС с общей и раздельной, полной и частичной диверсностью [12]. Для оценки степени диверсности и характеристик МВС в целом используются метрические и вероятностные методы.

В том случае, когда в МВС применяется несколько различных видов версионной избыточности (например, кристаллы от разных производителей и разные алгоритмы и инструментальные средства проектирования), то модель S дополняется множеством этих видов E и правилом R их назначения для версий. В этом случае говорят о мультидиверсных системах.

Многоверсионный жизненный цикл. Разработка технологий проектирования и верификации ГКС требует уточнения моделей жизненного цикла (МЖЦ). По аналогии со стандартными МЖЦ разработки ПО и ИУС, ЖЦ функциональной безопасности предложена модель *жизненного цикла ГС или ГКС*. Если обеспечивается за счет диверсности, то в основу такой модели может быть положена модель *многоверсионного жизненного цикла* [6,8], базирующаяся на операциях генерации и выбора версий

на различных этапах и при реализации различных процессов.

Закон «отрицания отрицания» для МВС. Существуют интересные закономерности в эволюции самих МВС. Одна из них иллюстрируется реализацией принципа МВ в ИУС АЭС, в развитии которого можно выделить три этапа [12]:

1) 80-е годы – переход от аппаратно-реализованных комплектов систем к схеме, когда один комплект (primary system) реализовывался аппаратно, на жесткой логике, а второй (secondary system) в виде программного решения на микропроцессорах (МП); такой подход к разработке являлся переходным, а вторичные комплекты использовались, чаще всего, в телеметрическом режиме;

2) 90-е годы – разработка первого и второго комплектов на идентичных или разных МП с использованием разных языков программирования (разработка фирмой Westinghause систем аварийной защиты на основе МП Intel и Motorola с использованием языков C++ и Ada) или использование сигнальной диверсности с последующей обработкой информации на идентичных МП (примером таких систем является программно-технический комплекс Teleperm XS, разработанный компанией Siemens);

3) 2000-е годы – использование программируемых логических интегральных схем (ПЛИС) для разработки обоих комплектов; при этом применяются кристаллы от разных производителей, различные технологии изготовления, языки описания аппаратуры и т.д.; уникальный ПТК и многоверсионные системы безопасности на основе ПЛИС разработаны и внедрены на АЭС Украины и Болгарии НПП «Радий».

Анализ эволюции принципа диверсности является отражением диалектического закона *«отрицания отрицания»*, поскольку пройден цикл из двух переходов: двухфазного «отрицания» двухкомплектных (недиверсных) систем на жесткой логике (HW и HW) диверсными системами с использованием программной реализации на МП (SW1 и SW2); последующего «отрицания» двухкомплектных диверсных систем (SW1 и SW2) системами с диверсными комплектами на ПЛИС (ПЛИС1 и ПЛИС2), т.е. фактически комплектами на жесткой логике, «зашиваемой» в кристалл, хотя и с использованием специальных программных средств САПР.

Возможен еще один вариант реализации МВС, когда первый и второй комплекты реализуются с использованием МП и ПЛИС соответственно, однако, он может быть более сложен из-за проблем с верификацией комплекта на МП и неудобен в эксплуатации. Возможен путь, когда используются диверсные ПЛИС-проекты, базирующиеся на разных вариантах реализации технологии «мягких процессоров (soft processors)», при которой функции системы «зашиваются» в кристалл в виде многоверсионных процессорных IP-ядер. Такой шаг фактически следует рассматривать как первую фазу следующего цикла «отрицания».

Генетические алгоритмы (ГА) для синтеза версий. Применительно к ПЛИС разработан подход, альтернативный САПР-ориентированному подход. Он базируется на использовании аппарата ГА для синтеза версий МВС. В этом случае версии *синтезируются в виде модели «черного ящика»*. Тогда МВС состоит либо из версий, синтезированных с использованием ГА (*внутренняя диверсификация*), либо из версий, полученных с использованием стандартных САПР и ГА (*внешняя диверсификация*) [13]. При этом реализуется еще один вариант парадигмы DS/UDC, поскольку проектные решения могут иметь специфицированный и управляемый уровни гарантоспособности.

Выбор многоверсионной технологии. Широкий спектр вариантов реализации принципа диверсности привел к появлению и формализации понятия *многоверсионной технологии* (МВТ). МВТ фиксирует кортеж элементов – вариантов выбора видов версионной избыточности по N этапам жизненного цикла и числа соответствующих версий. Задача выбора сформулирована и решается как оптимизационная задача поиска путей в биполярном N-уровневом графе по критерию «диверсность (надежность-безопасность) – стоимость» [12]. Основные проблемы при этом – построение графа исходя из возможных видов диверсности и их совместимости, а также вычисление метрик диверсности по этапам ЖЦ.

3.3. ЗМ-концепция и динамическая мультиреконфигурация

Принцип МВ дополняется принципами *многопараметрической адаптации* (МА) и *многоуровневой управляемой деградации* (МД), объединяемыми в концепцию ЗМ [6].

Многопараметрическая адаптация. МА состоит в организации *нескольких программно-аппаратно реализуемых контуров управления реконфигурацией* с учетом видов дефектов, числа и номенклатуры отказавших компонент. Известны методы порогово-версионной, порогово-ярусной, пространственно-структурной адаптации и др., реализуемые в КС и ПЛИС-ориентированных системах.

Многоступенчатая управляемая деградация. МД состоит в *перераспределении избыточных и неизбыточных мобильных ресурсов и коррекции, при необходимости, целей функционирования* для минимизации объемов деградации и рисков перехода в опасные ИТС. Механизмы деградации реализуются,

когда профиль ГС включает живучесть, а ГКС допускает ухудшение характеристик при отказах.

Дополнением к процессам управляемой деградации являются процессы многоступенчатого восстановления посредством перераспределения локальных и системных ресурсов и реализации принципа «технического каннибализма».

Мультиреконфигурация. Активная отказоустойчивость, концепция 3М и ее принципы поддерживаются процедурами динамической реконфигурации. ПЛИС-технологии предоставляют возможность динамической *мультиреконфигурации*, включающей реконфигурацию алгоритмов, функциональных и надежностных архитектур. При этом реконфигурация реализуется в физическом и информационном пространстве и во времени исходя из фактического и прогнозируемого состояния кристалла с учетом среды, в которой функционирует система, путем формирования и имплементации оптимальной архитектуры по критерию «гарантоспособность – объем и качество выполнения функций».

3.4. Естественно-гарантоспособные кристаллы

Благодаря реализации указанных принципов при построении систем на кристалле (SoC) может быть реализована и развита концепция естественно-надежных компьютеров. В этом случае можно говорить о *естественно-гарантоспособных кристаллах* (ЕГК) или naturally dependable SoC, когда ГС реализуется «снизу (физический уровень) – вверх (архитектурный уровень)».

Уровни реализации естественной гарантоспособности для ЕГК. Идея ЕГК может реализовываться *на молекулярном уровне* (нанотехнологии), *уровне программно доступных логических ячеек*, *уровне типовых элементов библиотек* функциональных и HDL-описания (создания библиотек отказоустойчивых компонент), *уровне резервированных каналов* и *перезагружаемых конфигураций*. Для обеспечения информационной безопасности как составляющей ГС необходимы свои схема декомпозиции по уровням и множество используемых методов и средств.

Системы из специфицированных частично-работоспособных компонент. Использование ГА-подхода ограничивается большими временными затратами при точной реализации сложных проектов. Поскольку на каждом шаге выполнения ГА-синтеза может фиксироваться набор входных сигналов $X_h \subset X$, при котором версия работает верно, предложено осуществлять многократную генерацию ГА-версий с учетом возможных ресурсных ограничений, чтобы обеспечить выполнение условия $X_{h1} \cup X_{h2} \cup \ldots \cup X_{hk} = X$.

Другими словами, в этом случае система компонуется из специфицированных частично корректных версий. Обобщением этого метода является синтез *систем с устанавливаемым уровнем отказоустойчивости из специфицированных частично корректных и частично определенных версий* [13].

3.5. Управление гарантоспособностью

Обобщение понятия ИТС КС и ИУС предоставляет возможности формирования расширенного множества стратегий технического (информационно-технического) обслуживания и управления состоянием по планово-предупредительным и гибким схемам. Целесообразен переход от *концепции управления надежностью (готовностью) по фактическому техническому состоянию к концепции управления гарантоспособностью по фактическому ИТС* [6, 7].

Сущность концепции заключается в том, что: обслуживание технических и программно-технических средств с целью профилактических целей и выявления скрытых отказов вследствие ДФ и прогнозируемых или выявленных ДР, а также обслуживание (проверка и модернизация) средств информационной безопасности (и живучести) с учетом ДВ проводятся не в фиксированные - плановые моменты времени, а *согласно фактическому ИТС*;

– моменты времени, продолжительность и объем мероприятий по обслуживанию *зависят от контролируемого уровня гарантоспособности*.

Стратегии управления. Множество возможных стратегий управления классифицируется по двум основным признакам: *степени и порядку совмещения профилактических или ремонтных мероприятий* по снижению рисков, обусловленных ДФ, ДР и ДВ; *составляющим гарантоспособности* и соответствующим показателям этих составляющих, их комбинациям или ГС в целом. Стратегии управления ГС реализуются средства, которые обеспечивают: *оперативный контроль* ИТС, его технической и информационной составляющих; *прогнозирование изменения* ИТС и оценку показателей ГС с учетом результатов мониторинга и с использованием специальных математических моделей; *определение момента, номенклатуры и объема профилактических мероприятий* согласно требованиям к ГС, ее текущего и прогнозируемого значений; *реализацию принятых решений* и оценку их влияния на фактический уровень ГС.

С учетом сущности ИТС рассматривается *политика управления гарантоспособностью* может и должна рассматриваться как *обобщение политики информационной безопасности КС*..

Масштабирование диверсности и гарантоспособности. Управление гарантоспо-собностью

может осуществляться путем разработки *платформ*, позволяющих получать проектные решения с *масштабируемым уровнем ГС*. Наличие графа МВТ позволяет также масштабировать и степень диверсности в ГКС. Примером таких решений является платформа «Радий» [12], которая используется для создания ИУС АЭС и обеспечивает масштабирование: *характеристик выполняемых функций* путем изменения количества и типов исполнительных механизмов, приемников информации и входных сигналов, а также технологических алгоритмов; *обеспечиваемого уровня гарантоспособности* за счет варьирования числа резервных каналов и ярусов (участков резервирования) и набора процедур контроля, диагностирования и реконфигурации при отказах, вызванных разными причинами (ДФ, ДП, ДВ); *типов и глубины диверсности* с использованием унифицированного множества вариантов процессно-продуктной версионной избыточности и алгоритмов выбора МВТ в зависимости от типа системы и предъявляемых требований.

4. Оценка

При создании ЕГК и ГКС в целом одной из наиболее сложных является проблема оценки показателей ГС.

Учитывая комплексность ГС, для его оценки могут использоваться два типа показателей: векторные, т.е. набор показателей, оценивающих отдельные свойства ГС и устойчивость к ДФ, ДР, ДВ) и *скалярные*, с помощью которых дается обобщенная оценка гарантоспособности.

Скалярная оценка может быть дана с использованием мультипликативного показателя, представляющего собой произведение вероятностей успешного выполнения операций, образующих цикл отказоустойчивости по разным дефектам [7].

4.1. Метрико-вероятностные методы

Одной из наиболее сложных является проблема оценки надежности и ГС программных средств. Она осложняется *отсутствием достоверной и упорядоченной информации о дефектах, выявляемых при тестировании*.

Метрические методы. Для оценки ГС программных средств используются метрические методы, основанные на вычислении метрик, непосредственно или косвенно характеризующих надежность, безопасность и ГС в целом. В этом случае формируется иерархическая модель свойства, определяется множество метрик, параметров для их вычисления, утилит или методик для их получения, а затем после их измерения осуществляется разработка и свертка результатов в соответствии с *иерархией радиальных метрических диаграмм и выбранной процедурой свертки*. Основная проблема – получение детальной и корректной иерархии, а также полной информации о параметрах.

Метрический метод применяется также при *детерминированной оценке* показателей контроля, диагностирования и отказоустойчивости МВС при одиночных и кратных отказах аппаратных и программных средств.

Вероятностные методы. При наличии нормализованных трендов дефектов, полученных по результатам тестирования, включая процедуры, основанные на проектно-ориентированном засеве дефектов, оценка ГС может быть выполнена с помощью вероятностных моделей (моделей роста надежности – SRGM). Для этого используется база данных типовых моделей и *метод их комплексирования и выбора, основанный на анализе матриц допущений*. Метрическая и вероятностная процедуры оценки могут дополнять друг друга, повышая достоверность оценивания в целом [14].

Многофрагментные марковские модели (МФМ). Для случая восстанавливаемых ГКС проблема оценки усложняется, поскольку необходимо учитывать параметры как процессов отказов, так и процессов восстановлений. Ее решение возможно с использованием одного из классов *вложенных марковских цепей* – МФМ. Они позволяют структурировать множества состояний системы *с учетом изменения параметров потоков отказов и восстановлений* и описать поведение ГКС в рамках марковских моделей. МФМ могут позволять исследовать разные свойства одно- и многоверсионных ГКС и оптимизировать параметры стратегий управления ГС (п.4.5.2).

Имитационное моделирование (ИМ). Во многих случаях оценка ГКС невозможна без ИМ. Это касается ситуаций, когда необходимо учитывать *различные законы распределения параметров отказов вследствие ДФ, ДП, ДВ*. Для ПЛИС актуальной является задача учета параметров множественных (кластерных) отказов ячеек и связей в кристалле. Она решается с использованием специальных средств генерации кластеров и оценки вариантов архитектур с учетом реального размещения проекта в кристалле и взаимного расположения резервных каналов. Они позволили отработать *метод структурно-пространственной адаптации* систем на программируемой логике, когда выбор отказоустойчивой конфигурации и ее размещение в ПЛИС зависит от информации об отказавших частях кристалла и характера внешних воздействий [15].

4.2. Формальные методы

Общая характеристика. Для разработки и оценки ГС находят применение специальная группа методов, получивших в англоязычной литературе статус «формальных». К ним относятся методы, основанные как на классических процедурах вероятностного анализа, теории марковских случайных процессов, так и на частично формализованных процедурах, в частности, FME(C)A, FTA, HAZOP и др.

Что касается формальных методов разработки программного обеспечения и КС, то здесь активно развиваются методы, базирующиеся на *формальных языках представления спецификаций* (B-, EventB-, Z-нотации и др.), так называемом *Model-checking подходе*, *риск-ориентированные методы*. В контексте ГС эти подходы позволяют усовершенствовать методы оценки гарантоспособности сложных систем и технологии разработки ГКС.

Модификации FMECA-анализа. В [11] табличный метод, позволяющий выполнять качественный анализ видов и последствий отказов, их вероятности и критичности (оценку надежности и функциональной безопасности), был развит в направлении *возможности оценки информационной безопасности*. Затем он был модернизирован в соответствии с таксономической схемой (п.2.1), в результате чего строка FME(C)A-таблицы стала содержать столбцы типов физических и информационных воздействий, вид, причину и форму проявления отказов, вызванных ДФ, ДП, ДВ, вероятность, тяжесть и продолжительность ликвидации последствий отказов и возможные средства снижения рисков отказов. Такая *расширенная FME(C)A-таблица* дополняется многомерной *матрицей критичности* и *процедурой оптимизации обеспечения ГС по критерию «критичность-стоимость»*.

B-нотации и разработка МВС. Формальный метод, основанный на B-нотации, позволяет при разработке спецификации учесть и реализовать затем процедуры отказоустойчивости. Кроме того, существуют средства, генерирующие исполнительный код с языка B. Следовательно, такой метод может давать возможность *расширения множества многоверсионных технологий разработки и верификации*.

Например, при использовании ПЛИС версии МВС могут разрабатываться с использованием языка описания аппаратуры *VHDL*, Java-ориентированного языка *JHDL*, а также технологии *BHDL*, позволяющей получать HDL-код непосредственно с B-нотации. Такие методы могут значительно повысить качество независимой верификации ГКС.

5. Перспективы

Очередным этапом развития концепции гарантоспособности, судя по анализу публикаций, проектов последних лет в области информационных технологий, финансируемых Европейским союзом в рамках программ FP-6, FP-7, может стать разработка так называемых "*Resilient Systems and Infrastructures*" (RSI). Фактически речь идет о расширении спектра свойств систем и их объединений и более широкой трактовки их устойчивости к внешним и внутренним «вызовам» [10].

Гарантоспособные инфраструктуры или «системы систем». Анализ причин крупнейших аварий (коллапса регионального кластера энергетической системы США, аварий космических систем Arian, SeaLaunch и др.), которые были связаны и с несовершенством КС, позволил прийти к выводу, что необходим комплексный подход, позволяющий лучше учесть интерфейс и взаимовлияние компьютерной ИУС и объекта контроля и управления (технической или организационно-технической системы). Для этого была сформулирована *концепция гарантоспособной инфраструктуры* или *«системы систем»*. Такой инфраструктурный подход используется как для движения «вверх» – к объединению КС и объектов, так и «вниз» – для реализации внутрикристальных IP-ядер, IP-инфраструктур (IIP) и многоверсионных IIP.

Расширение таксономии гарантоспособности. Множество факторов, рассматриваемых в рамках RSI-подхода, должно включать изменение требований к системе и изменение среды (внешней системы), в которой функционирует система. Механизмом, поддерживающим устойчивость к таким дополнительным вызовам, может быть *механизм управляемой эволюции*, а свойство, которое расширяет ГС – *способность к эволюции (evolvability)*. При этом отказоустойчивость является частным случаем такого механизма. Для реализации управляемой эволюции необходимо разработать по аналогии с отказоустойчивостью ее операционный цикл, в котором дефекты должны рассматриваться как частный случай изменений. Создание устойчивых к изменениям – *эволюабельных систем и инфраструктур* должно опираться на *комопнентно-ориентированный подход* к проектированию, использование *динамически масштабируемых платформ*.

Заключение

Проблема гарантоспособности имеет общий характер для систем различной размерности. Гарантоспособные вычисления представляют научное направление, связанное с хранением и обработкой информации с повышенными требованиями к надежности и безопасности. В данной работе проведен обзор и краткий анализ проблем ГС, оценки и разработки ГКС, возможных методов их решений. Анализируемая проблема имеет общий характер и возможные пути решения – от создания ЕГК до разработки и реинжиниринга надежных и безопасных инфраструктур, от встроенных решений до распределенных систем, реализуемых с использованием сетевых и Интернет-технологий. Рассмотренные методы позиционированы в контексте парадигмы DS/UDC, которая является частным случаем более общей формулировки «хорошая система из плохих (недостаточно хороших) компонент» и имеет и другие вариации «быстродействующая система из медленных (недостаточно быстрых) процессоров», «точная система из неточных (недостаточно точных) измерителей» и т.д.

Среди базовых принципов, обеспечивающих ГС как комплексное свойство систем выполнять функции (услуги) с гарантированным качеством, несмотря на угрозы различной природы, следует выделить принципы многоверсионности и дополняющие его МА и МД. Они реализуются путем мультиреконфигурации архитектур, их физического размещения в пространстве, коррекции целей и функций, управления ГС по фактическому ИТС.

Дальнейшие исследования и разработки могут быть направлены на детализацию методов оценки и обеспечения ГС для различных приложений и развитие RSI-подхода.

Благодарности. Исследования в области ГКС проводились при выполнении НИР, финансируемых МОН Украины (темы № 104U003502, № 106U001071, 2002-2008), предприятиями НПП «Радий» и НТ СКБ «Полисвит», при поддержке гранта Royal Scientific Society (Великобритания, 2003-2004), а также в рамках проекта TEMPUS-MASTAC (2006-2009) по разработке образовательных программ по критическому аэрокосмическому компьютингу для магистров и аспирантов.

Литература

1. Айзенберг Я.Е. Сопоставление принципов обеспечения безопасности систем управления ракетоносителями и атомными электростанциями / Я.Е. Айзенберг, М.А. Ястребенецкий // Космічна наука та технологія. – 2002. – № 1. – С. 55-60.

2. Харченко В.С. Экспертная оценка безопасности OTS компонент информационных и управляющих систем АЭС / В.С. Харченко, В.В. Скляр, М.А. Ястребенецкий // Інформаційні технології в енергетиці. - Київ: ІПМЕ НАНУ, 2003. – С. 12-9.

3. Харченко В.С. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций / В.С. Харченко, В.В. Скляр, О.М. Тарасюк // Радіоелектронні і комп'ютерні системи. – 2003. – № 3. – С. 135-149.

4. Спектор Л.И. Нарушения в работе АЭС, вызванные системой управления технологическими процессами энергоблока / Л.И. Спектор, О.Н. Бутова, В.В. Инюшев, М.А. Ястребенецкий // Ядерная и радиационная безопасность. – 2004. – Т. 7, № 4. – С. 54-63.

5. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr. // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

6. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / Харченко В.С. // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 7-19.

7. Харченко В.С. Гарантоздатність комп'ю–терних систем: межа універсальності в контексті інформаційно-технічоного стану / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 8-16.

8. Kharchenko V.S. Multi-version Information Technologies and Development of Dependable Systems out of Undependable Components / V.S. Kharchenko, V.V. Sklyar, A.V. Volkovoy // Proc.of IEEE DepCoS Conference, Szklarska Poreba, Poland, June 14-16, 2007. – P. 18-24.

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

10. Kharchenko V. Dependable Computing Systems for Supporting Transformation of the Force Information Infrastructure / V. Kharchenko, V. Sklyar, O. Odaruschenko // Information & Security. – 2007. – Vol. 22. – P.75-91.

11. Gorbenko A F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring / A. Gorbenko, V. Kharchenko, O. Tarasyuk, A. Furmanov // LNCS 4157, Rigorous Development of Complex Fault-Tolerant Systems / M. Butler et al. (eds.). – Springer, 2006. – P. 153-168.

12. Kharchenko V.S. FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessment / V.S. Kharchenko, V.V. Sklyar (edits). - RPC "Radiy", National Aerospace University "KhAI", State STC on Nuclear and Radiation Safety, 2008. – 188 p.

13. Yakymets N. Fault-Tolerant Digital Systems Implemented with Partially Definite and Partially Cor-

rect Automata / N. Yakymets, V. Kharchenko // Proc. of 2nd Intern. Workshop on Engineering Fault Tolerant Systems, Dubrovnik, Croatia, September 4, 2007. – P. 32-37.

14. Основи надійності цифрових систем: підручник / Під ред. В.С. Харченка. – Харків: МОН України, ХАІ, 2004. – 475 с.

15. Ushakov A. Fault-tolerant Embedded PLD-systems: Structures, Simulation, Design Technologies / A. Ushakov, V. Kharchenko, V. Tarasenko // Proc. of the 12th Intern. Conf. Mixed Design of Integrated Circuits and Systems, Krakow, Poland, June 12-15, 2003. – P. 546-551.

16. Gorbenko A. Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability / A. Gorbenko, V. Kharchenko, A. Romanovsky // LNCS 5454, Methods, Models and Tools for Fault-Tolerance / M. Butler et al. (eds.). - Springer, 2009. – P. 324-342.

Поступила в редакцию 20.04.2009

Рецензент: д-р техн. наук, профессор, зав. кафедрой теоретической и прикладной информатики Г.Н. Жолткевич, Харковский национальный университет ім. В.Н. Каразина, Харьков, Украина.

ПАРАДИГМИ І ПРИНЦИПИ ГАРАНТОЗДАТНИХ ОБЧИСЛЕНЬ: СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ

В.С. Харченко

Аналізуються таксономічні, методологічні і технологічні аспекти гарантоздатних обчислень. Обговорюється парадигма "гарантоздатних систем з негарантоздатних компонент" та її використання для різних застосувань: від природно надійних кристалів до складних інфраструктур. Аналізуються принципи і методи оцінки і забезпечення гарантоздатності, реалізації багатоверсійності і мультиреконфігурації при створенні гарантоздатних систем. Узагальнюються приклади застосування означеної парадигми при розробленні систем на програмованій логіці, web-систем та інш.

Ключові слова: гарантоздатність, комп'ютерні системи, інфраструктура, природно гарантоздатний кристал, багатоверсійність.

PARADIGMS AND PRINSIPALS OF DEPENDABLE COMPUTING: STATE OF THE ART AND DEVELOPMENT PERSPECTIVS

V.S. Kharchenko

Taxonomical, methodological and technological aspects of dependable computing are analyzed. The paradigm of "dependable computing systems and IT- infrastructures out of undependable components" is discussed for different applications: from naturally dependable chips to complex IT-infrastructures. Principles and methods of dependability assessment and ensuring, means for multi-version and multi-reconfiguration used to develop dependable systems are reviewed. Examples of the paradigm application for PLD-based systems and web-systems are analyzed.

Key words: dependability, computer system, infrastructure, naturally dependable chip, multi-version.

Харченко Вячеслав Сергеевич – д-р техн. наук, профессор, заведующий кафедрой 503, Национальный аэрокосмический университет им. Н.Е.Жуковского «ХАИ», Украина, e-mail: V.Kharchenko@khai.edu, www.stc-dessert.com.