УДК 681.321

ЭВОЛЮЦИЯ ФОН-НЕЙМАНОВСКОЙ ПАРАДИГМЫ: ГАРАНТОСПОСОБНЫЕ СИСТЕМЫ ИЗ НЕГАРАНТОСПОСОБНЫХ КОМПОНЕНТ

д.т.н., проф. В.С. Харченко

Проведен эволюционный анализ развития парадигм, методов и средств обеспечения надежности компьютерных систем. Дана характеристика четырех этапов такой эволюции. Проанализировано соотношение между свойствами гарантоспособности и надежности в традиционном понимании.

Введение. Анализ проблемы надежности компьютерных систем. Обеспечение надежности компонентов и систем на их основе является одной из наиболее важных задач компьютерной и программной инженерии. Это связано с возрастанием влияния компьютерных технологий на надежность и безопасность компьютеризированных комплексов для критических (АЭС, аэрокосмические комплексы, транспортные коммуникации) и бизнес-критических (банковские системы, е-коммерция) приложений. Сейчас недостаточно рассматривать безотказность таких систем вне среды, в которой они функционируют, и последствий отказов их компонент, решая задачу обеспечения надежности в традиционной постановке. Необходимость формулировки задач в более широком контексте диктуется масштабностью систем, неопределенностью характеристик компонент, их распределенным характером и динамизмом, агрессивностью среды, в которой функционируют системы, сложностью формулировки понятия отказа.

Вопросы оценки и обеспечения надежности компьютерных систем и их компонент на различных этапах их эволюции рассматривались в ряде ключевых работ [1 – 6].

Цель данной статьи – конспективный анализ эволюции задач и принципов обеспечения надежности сложных компьютерных систем и технологий, исходя из базовой парадигмы, сформулированной в начале 60-х годов Джоном фон-Нейманом. С одной стороны, можно говорить о развитии этой парадигмы, если опираться на ее узкую формулировку "надежное устройство из ненадежных (небезотказных) реле", с другой, – о детализации парадигмы, считая, что ее расширенная формулировка "надежный организм из ненадежных компонент" дает универсальную схему решения существующих и будущих проблем.

Проведенный анализ, естественно, не претендует на полноту, поскольку эта проблема в целом очень объемна и многоаспектна. В огра-

© д.т.н., проф. В.С. Харченко, 2004

ниченных рамках статьи ставится задача выделить ключевые факторы эволюции с учетом последних этапов развития компьютерных технологий. Идея такой статьи вынашивалась давно, и решение об ее написании сформировалось окончательно после знакомства с этапной, на наш взгляд, работой ведущих специалистов в этой области А. Авиженисом, Ж.-К. Лапри и Б. Рэнделом [6]. Предварительная версия статьи опубликована в [7]. Поставленная задача не может быть полно решена вне терминологического контекста, однако, далее вопросы терминологии будут затрагиваться минимально и касаются только анализа соотношения понятий «гарантоспособность» и «надежность».

Аспекты эволюции. Эволюционный анализ развития проблемы надежности компьютерных систем и технологий проводится в нескольких аспектах (рис. 1):

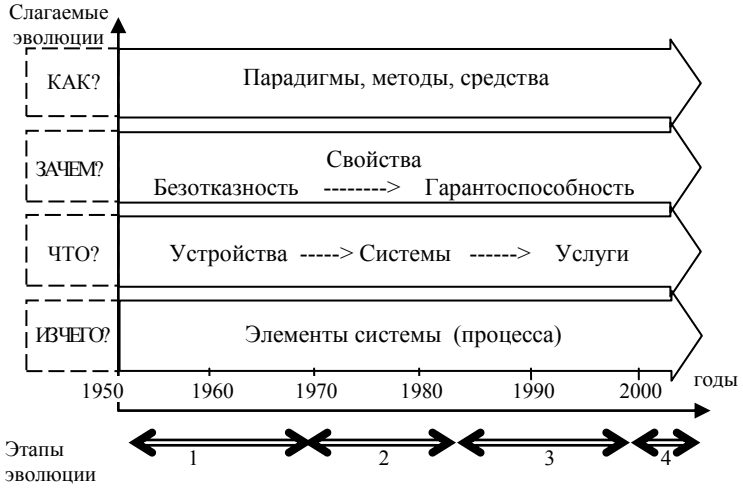

Рис. 1. Структура эволюции в области надежности компьютерных систем и технологий

− изменения элементов (компонент), из которых синтезируются (интегрируются) системы (*из чего (?) состоят системы*);

− изменения самих систем, которые являются объектом синтеза и обеспечения надежности (*что(?) синтезируется*);

− изменения номенклатуры и содержания свойств элементов и систем, которые рассматриваются и должны обеспечиваться (*зачем (?), из-за каких свойств, составляющих надежность (с учетом эволюции самого понятия надежности), применяются те или иные методы и средства*);

− изменения базовых принципов, методов и средств обеспечения требуемых свойств систем (*как (?) обеспечивается надежность систем*).

Таким образом, эволюционирование в рассматриваемой проблеме

осуществляется в многомерном пространстве: «*элементы, свойства элементов» – «системы, свойства систем» – « методы и средства».*

Этапы эволюции. За последние пятьдесят лет можно выделить несколько этапов эволюции парадигм синтеза и других аспектов развития компьютерных систем и технологий в контексте обеспечения их надежности.

1. Первый этап – 50 – 60-е годы: *синтез надежных (безотказных) устройств из ненадежных элементов*. Побудительный мотив: ***безотказность*** *элементов недостаточна – что делать?* ***Резервирование*** *все решит?*

Элементами систем являются реле, транзисторы и микросхемы малой степени интеграции; синтезируемыми системами – релейные и цифровые устройства. Рассматриваемые свойства для элементов и систем определяются парой: недостаточная безотказность элементов – требуемая безотказность систем. Основной метод решения задачи – параллельное резервирование для простейших радиоэлектронных элементов без использования специальных восстанавливающих органов или мажоритарное резервирование с обычным мажоритарным органом без применения встроенных или внешних средств контроля каналов. В таких системах требуемая безотказность обеспечивалась только за счет избыточности каналов, т.е. реализовывалась *пассивная отказоустойчивость*. В эти годы фактически применялся только один тип избыточности – структурная избыточность.

В теоретическом плане базовыми явились работы Дж. фон-Неймана, К. Шеннона, У. Пирса, А. Половко, С. Доманицкого и др.

2. Второй этап – 70 – 80-е годы*: синтез отказоустойчивых устройств и систем из ненадежных аппаратных компонент.* Побудительный мотив: ***отказы неизбежны;*** *как обеспечить требуемую надежность и улучшить эффективность резервирования?*

С учетом признания неизбежности отказов компонент изменяются подходы к синтезу систем с требуемой надежностью. Элементами систем являются микросхемы малой, средней и большой степени интеграции; синтезируемыми системами – сложные цифровые устройства, компьютеры и компьютерные системы. Пара рассматриваемых свойств осталась неизменной: недостаточная безотказность элементов – требуемая безотказность (отказоустойчивость) систем. Основные методы решения задачи – различные типы резервирования – структурное, информационное, временное. При этом использовались специальные средства оперативного контроля, диагностирования, реконфигурации и восстановления вычислительного или управляющего процесса. Это позволило реализовать идею так называемой *активной отказоустойчивости*, которая обеспечила более эффективное использование средств. Она дополнялась разработкой методов повышения контролепригодности компонент, из которых создается система, что позволяло минимизировать вне-

канальные средства поддержки отказоустойчивости.

Важными вехами в этой области явились труды А. Авижениса, Т. Андерсона, П. Пархоменко, Е. Согомоняна, И. Шубинского и др.

3. Третий этап – 80 – 90-е годы: *синтез отказоустойчивых (дефектоустойчивых) систем из ненадежных аппаратных и программных средств.* Побудительный мотив: *отказы аппаратных средств и* ***дефекты программных средств неизбежны;*** *как построить системы, устойчивые к* ***обоим*** *типам отказов?*

Элементы – аппаратные и программные компоненты; системы – компьютерные системы и сети. Новые подходы – N-версионное программирование и многоверсионное проектирование, объединяемые в концепцию многоверсионных систем, позволившую рассматривать устойчивость к отказам этих компонент с единых позиций, распространив исходную идею на этап применения. Формируются теоретические основы многоверсионных систем, включая их функционально-компонентные и автоматные модели, методы введения и оценки диверсности, базовые архитектуры и технологии. В конце 80-х годов начинает развиваться параллельная парадигма, расширяющая спектр рассматриваемых свойств: *синтез надежных и безопасных систем из ненадежных и небезопасных компонент.* Побудительный мотив: *как обеспечить* ***безопасность систем*** *(в смысле* ***safety,*** *т.е. отсутствия катастрофических последствий отказов, и в смысле* ***security,*** *т.е. защищенности информации) при* ***недостаточной*** *безотказности и защищенности компонент?*

Эти парадигмы сформировали необходимость введения свойства “dependability”(гарантоспособность или надежность в «широком смысле», включающая безотказность, готовность, безопасность – “security” и ”safety”, живучесть). В русскоязычной литературе термин «гарантоспособность» появился в 1986 году после перевода специального выпуска журнала IEEE Transaction on Computers [8], а несколько позже в работе [9]. Другими линиями развития свойств, поддерживающих их реализацию, стали, на наш взгляд:

− *контролепригодность – тестопригодность – дигностируемость – реконфигуропригодность*. Введение в рассмотрение последнего из свойств явилось своеобразным ответом на развитие, в частности, СБИС-технологий, позволявших создавать матричные многопроцессорные структуры на одном кристалле [10];

− *отказоустойчивость – дефектоустойчивость*. Термин «дефектоустойчивость» стал некоторой альтернативой термину «отказоустойчивость» и учитывал специфику отказов, обусловленных дефектами программных средств, не выявленных при тестировании и проявляющихся при применении систем и таким образом более точно отражал свойство

систем функционировать правильно в условиях аномалий (дефектов) как аппаратных, так и программных компонент. Это свойство позволяет с единых методологических позиций рассматривать способность систем обнаруживать, локализовать и парировать последствия дефектов аппаратных (ДАС) и программных средств (ДПС), дефектов проектирования, производства и эксплуатации. В частности, в [9] было доказано ряд важных утверждений, касающихся свойств дефектоустойчивых систем, среди которых ключевыми явились утверждения о том, что система, обладающая свойством ДПС-устойчивости, является ДАС-устойчивой, а введение версионной избыточности в дублированных структурах может обеспечивать их ДАС-устойчивость без наличия встроенных средств контроля каналов благодаря ассиметричному поведению различных версий.

– *отказоустойчивость – отказобезопасность*. Первый термин не указывает на характер отказов, которые парирует система, и их последствия. Что касается термина «отказобезопасность», то он позволял детализировать составляющие свойства безопасности (safety) для критических приложений [11].

Следует подчеркнуть, что фактор надежности программных средств сыграл (и играет сейчас [12]) важнейшую роль в утверждении гарантоспособности как ключевого элемента эволюционирования.

Наиболее серьезные результаты на этом этапе были получены А. Авиженисом, Ж.-К. Лапри, Б. Литлвудом, М. Лью, Б. Рэнделом, А. Романкевичем и др.

4. Четвертый этап – 2000-е годы: *синтез гарантоспособных систем из негарантоспособных компонент.* Побудительный мотив: *как обеспечить* ***гарантоспособность систем и услуг*** *при* ***недостаточной*** *гарантоспособности компонент(элементов, систем* ***и процессов)?***

Элементы – компьютеры, кластерные субсистемы, web-компоненты; системы – распределенные образования (сети, web-системы). Формируется понятийный аппарат гарантоспособных систем. Их компонентами являются элементы, характеризуемые векторными показателями безотказности, готовности, безопасности. Концепция многоверсионности, применявшаяся ранее только как методология для уменьшения проектных ошибок, расширяется, объединяя триаду «многоверсионные системы, технологии, проекты» [13]. Следует подчеркнуть, что парадигма «гарантоспособная система из негерантноспособных компонент», впервые сформулированная в [14, 15], действительно является этапной, поскольку развивает исходную идею фон-Наймана к современным системам и задачам. В настоящее время проводятся работы, связанные с анализом задач и принципов синтеза гарантоспособных web-систем с использованием концепции многоверсионности, а также его применения для повышения отдельных составляющих гарантоспособности, для которых он раннее не ис-

пользовался, а именно безопасности (security) [15].

О свойстве гарантоспособности. Анализ работы [6], в которой детально описаны основные понятия в области гарантоспособности, позволяет выделить следующие наиболее важные аспекты:

− компьютерная система характеризуется пятью основными свойствами – функциональностью (functionality), удобством использования или практичностью (usability), производительностью (performance), стоимостью (cost) и гарантоспособностью (dependability);

− гарантоспособность – это способность компьютерной системы гарантированно предоставлять набор услуг (сервисов). При этом понятие отказа формулируется исходя из корректности и полноты сервисов, предоставляемых пользователю;

− в свою очередь, гарантоспособность включает свойства готовности (availability, готовности предоставления корректного сервиса), безотказности (reliability, продолжительности корректного сервиса), безопасности (safety, отсутствия катастрофических последствий для пользователей и окружающей среды), конфиденциальности (confidentiality, отсутствия неавторизированного доступа к информации), целостности (integrity, отсутствия недопустимого или непредусмотренного изменения состояния системы) и обслуживаемости (maintainability**,** приспособленности к ремонту и модификации);

− живучесть (survivability или performability) не внесена в гарантоспособность, а рассматривается как отдельное свойство. Соотношение между ними анализируется в приложениях к работе [6] с учетом разных подходов к определению самого свойства живучести;

− отказоустойчивость (fault-tolerance) определяется как средство поддержания гарантоспособности и его составляющих.

Таким образом, анализируя соотношение между надежностью и гарантоспособностью, отметим следующее. Надежности, понимаемой в соответствии с действующими в Украине и бывшем СССР стандартами и включающей безотказность, ремонтопригодность, сохраняемость и долговечность (надежности в узком смысле), не соответствует термин «dependability» как более широкий (без учета свойств сохраняемости и долговечности, редко используемых в компьютерных системах). Поэтому для перевода термина «dependability», строго говоря, не может использоваться термин «надежность», поскольку ему соответствует «надежность в широком смысле» или «гарантоспособность».

Следует сказать, что свойства, входящие в гарантоспособность, тесно связаны между собой. Это иллюстрирует табл. 1, в которой показаны позитивные и негативные аспекты влияния реализации свойства безопасности (security) на другие составляющие гарантоспособности.

Таблица 1

Влияние свойства безопасности (security)
на другие составляющие гарантоспособности

Аспекты соотношения безопасности (security) и других составляющих гарантоспособности	Другие свойства гарантоспособности			
	Готовность (availability)	Безотказность (reliability)	Безопасность (safety)	Обслуживаемость (maintainability)
Позитивные аспекты	Применение средств обеспечения безопасности уменьшает время неготовности компьютерной системы из-за умышленных отказов (malicious failure)	Применение средств обеспечения безопасности увеличивает вероятность безотказной работы компьютерной системы (с учетом умышленных отказов)	Применение средств обеспечения безопасности уменьшает вероятность перехода компьютерной системы в критическое состояние вследствие умышленных отказов	
Негативные аспекты	Применение средств обеспечения безопасности требует дополнительных временных ресурсов для поддержания функций безопасности	Увеличение сложности компьютерной системы из-за введения дополнительных программно-аппаратных средств обеспечения безопасности может привести к снижению безотказности		Применение средств обеспечения безопасности приводит к увеличению сложности и стоимости обслуживания системы в целом

Выводы. За последние полвека происходила многоэтапная эволюция парадигм, принципов, методов и средств, связанных с надежностью компьютерных систем. На основе анализа различных факторов, решаемых задач, свойств элементов и систем выделены четыре этапа такой эволюции. Ключевым на последних этапах эволюции является вопрос расширения содержания понятия надежности, нашедшего свое отражение в появлении англоязычного термина «dependability», который может быть переведен как «гарантоспособность» или «надежность в широком смысле». Поскольку в настоящее время существует определенная асимметрия в номенклатуре и содержании свойств, связанных с надежностью

(гарантоспособностью), целесообразно проведение гармонизации национальных и международных стандартов, которая бы учла этот аспект. В научных исследованиях представляет несомненный интерес изучение взаимного влияния различных составляющих гарантоспособности для их комплексной оценки и обеспечения.

Необходимо сделать еще один вывод, касающийся эволюции надежности компьютерных систем. В качестве элементов (компонент), влияющих на надежность (гарантоспособность) систем, должны рассматриваться не только аппаратные и программные средства как продукты, из которых она создается, а и процессы ее создания. В этом случае и сама система должна рассматриваться как проект, объединяющий продукты и процессы [16]. Такой интегративный подход должен применяться и с учетом изменений, происходящих в элементной базе, которая все более интеллектуализируется за счет внедрения технологий, основанных на IP-ядрах, и создания отказо(дефекто)устойчивых платформ на кристалле [17].

Дальнейшее эволюционирование фон-Неймановсой парадигмы происходит с учетом эволюционирования систем, компонент, из которых они складываются, свойств компонент и систем, связанных не только с надежностью (гарантоспособностью), а и с другими свойствами – функциональностью, производительностью и др.

Благодарности. Данная работа выполнялась автором в рамках проекта «On Developing a General Approach to Analysis and Synthesis of Multiversion Software Systems and Applying it in Emerging Application Domains», поддержанного грантом Британского Королевского научного общества RS 15114, 2003-2004. Автор благодарен также участникам научно-технического семинара «КриКТехС» (*http://k503.xai.edu.ua*), на котором обсуждалась проблематика этой статьи, что, безусловно, способствовало улучшению ее качества.

ЛИТЕРАТУРА

1. *Майерс Г. Надежность программных средств. – М.: Мир, 1980. – 360 с.*
2. *Основы технической диагностики. В 2-х частях / Под ред. П.П. Пархоменко. – М.: Энергоатомиздат, 1977. – 265 с.; 1984. – 238 с.*
3. *Лонгботтом Р. Надежность вычислительных систем. – М.: Энергоатомиздат, 1985. – 228 с.*
4. *Согмонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. – М.: Радио и связь, 1989. – 208 с.*
5. *Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучих вычислительных систем. – К.: Наук. думка, 1990. – 184 с.*
6. *Avižienis A., Lapri J-C., Randel B. Fundamental Concepts of Dependability, UCLA CSD Report no.010028, LAAS Report no.01-145, Newcastle University*

Report no. CS-TR-739, 2002, 20 p.

7. *Харченко В.С. От безотказности электронных устройств к гарантоспособности web-систем: эволюция парадигм, методов и средств // Контрольно-измерительные приборы и автоматика. – 2004. – № 9. – С. 4 – 9.*
8. *Avižienis A., Lapri J-C.Dependable Computing: from Concepts to design Diversity? // IEE Transactions on Computers. – 1985. – V. 74. – P. 8 – 21.*
9. *Харченко В.С., Паршин В.В. Многоальтернативные системы и обеспечение гарантоспособности. Препринт №321. – Х.: Институт проблем машиностроения АН Украины, 1989. – 33 с.*
10. *A Reconfigurability of Fault-Tolerant Systems: The Measures, Algorithms and Modeling Technique / V.S. Kharchenko, V.V. Gostishchev, N.P. Blagodarny, V.A. Melnikov // Зарубежная радиоэлектроника. – 2002. – № 5. – С. 62 – 72.*
11. *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.*
12. *Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ «ХАІ». – 2003. – Вип. 3. – С. 135 – 149.*
13. *Многоверсионные системы, технологии и проекты / Под ред. В.С. Харченко. – Х.: Мин. образования и науки Украины. – 2003. – 528 с.*
14. *Gorbenko A., Kharchenko V., Popov P., Romanovsky A., Boyarchuk A. Dependable Web-services out of undependable Web-components. Technical Report. – University of Newcastle-upon-Tyne, Greaf Britaine, NAU "KhAJ", Ukraine, 2004. – 36 p.*
15. *Kharchenko V., Popov P., Romanovsky A. On Dependability of Composite Web Services with Components Upgraded Online // Proceedings of DSN 2004 Workshop on Architecting Dependable Systems. – Florence, Italy. – 2004, 30 June. – P. 14 – 20.*
16. *Kharchenko V.S. Multiversion Information Technologies and Reliable Projects // Матеріали Міжнародної конференції з управління "Автоматика-2001". – Одеса, Україна. – 2001. – Т. 2. – С. 135 – 136.*
17. *Харченко В.С., Тарасенко В.В., Ушаков А.А. Встроенные отказоустойчивые цифровіе системі с программируемой логикой. Учебное пособие. – Х.: Мин. образования и науки Украины. – 2004. – 188 с.*

Поступила 20.07.2004

***ХАРЧЕНКО Вячеслав Сергеевич**, доктор техн. наук, профессор, заведующий кафедрой компьютерных систем и сетей НАКУ им. Н.Е. Жуковского "ХАИ". Область научных интересов – надежность, живучесть и безопасность компьютерных систем критического применения, технологии их проектирования, моделирования и экспертизы.*

E-mail: V.Kharchenko@khai.edu.