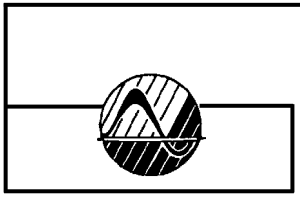

УДК 004.415:681.3

ЭВОЛЮЦИОННО-КОМПОНЕНТНАЯ МОДЕЛЬ И КОНФИГУРАЦИОННАЯ ОЦЕНКА НАДЕЖНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

А.Д. Герасименко
(Конструкторское бюро АСУ НПО «Радий», Кировоград)

Предложена эволюционно-компонентная модель информационно-управляющих систем, позволяющая учесть и оценить весь спектр изменений программно-аппаратных компонент OTS (Off The Shelf), включая оценку надежности и безопасности.

эволюционно-компонентная модель, конфигурационная оценка, надежность, информационно-управляющие системы

Постановка проблемы. Современная парадигма разработки компьютерных информационно-управляющих систем (ИУС), аппаратных средств (АС) и программного обеспечения (ПО), в том числе и для систем критического применения, характеризуется тем, что ИУС не разрабатывается «с нуля», а включают в себя многочисленные готовые компоненты. Такого рода готовые продукты получили название OTS (Off-The-Shelf), т.е. продукции «с полки» [1].

Применение OTS-компонентов может повысить общее качество ИУС, а также их надежность и безопасность. Данные преимущества объясняются тем, что OTS-компоненты уже прошли апробацию и известен опыт их использования. В то же время закрытый код и отсутствие информации о процессе разработки ПО затрудняют оценку OTS элементов при их использовании в ИУС критического применения. Это, в свою очередь, создает проблемы при экспертизе и независимой верификации в процессе нормативного регулирования и лицензирования.

Анализ литературы. Следует отметить, что, несмотря на широкое использование OTS-компонент в современных ИУС и важность задачи и важность оценки надежности и безопасности таких компонент, в известной

литературе отсутствуют комплексные исследования, посвященные данному вопросу. Исследования в области OTS-компонент компьютерных ИУС носят, как правило, фрагментарный характер и посвящены решению отдельных практических вопросов: в [2, 3] предложен подход к оценке применимости использования коммерческого программного обеспечения (ПО) в ИУС критического применения; в [4 – 6] рассмотрены экономические аспекты применения OTS-компонент ИУС; в [7] предложена технология применения программных OTS-компонент, позволяющая ограничить использование избыточных функций; в [1, 8] разработана классификация программно-аппаратных OTS-компонент и предложен подход к оценке их надежности и безопасности; в [9, 10] предложены методики тестирования программных и аппаратных OTS-компонент в составе ИУС.

Проведенный анализ публикаций показал, что в известных работах:

– в основном рассматриваются вопросы использования коммерческих OTS-компонент и недостаточное внимание уделено использованию компонент, которые были ранее созданы самими разработчиками ИУС;

– отсутствует комплексный подход к оценке и аппаратных, и программных OTS-компонент;

– в математическом аппарате оценки OTS-компонент практически не используются методы системного анализа, в частности, методы объектно-ориентированного анализа [11], наиболее адекватные исследуемой области.

Целью статьи является разработка модели ИУС, позволяющей учесть и оценить весь спектр изменений программно-аппаратных компонентов OTS (Off The Shelf), включая оценку надежности и безопасности.

Общий подход к разработке эволюционно-компонентной модели ИУС. Проведем анализ эволюции программно-аппаратных компонентов OTS, входящих в состав ИУС. При этом под эволюцией ИУС подразумевается ее развитие путем последовательных изменений программно-аппаратных компонент в процессе деятельности фирмы разработчика. Существуют следующие причины изменений (модификаций) компонентов ИУС:

– модификации, связанные с изменением функциональных возможностей, в том числе, и с выпуском принципиально новых типов ИУС;

– модификации, связанные с устранением замечаний заказчиков, в том числе, и с устранением дефектов разработки;

– модификации, связанные с изменением элементной базы и используемых инструментальных средств разработки;

– модификации, связанные с оптимизацией структуры и функционирования (характеристик) ИУС.

Следует отметить, что в общем случае внесение изменений может быть вызвано несколькими причинами. Кроме того, в ряде случаев между некоторыми из указанных выше причин может не существовать четких границ. Например, в случае выявления дефектов разработки модификации

будут связаны и с их устранением, и с изменением элементной базы.

Для анализа изменений (эволюции) программно-аппаратных OTS-компонент предлагается эволюционно-компонентная модель ИУС [12, 13], которая базируется на ***функционально-компонентном подходе*** к анализу эволюции ИУС и формировании множества вариантов эволюции; ***разработке модели*** поэтапных изменений ИУС; ***метрическом подходе*** к оценке функционально-компонентных изменений ИУС.

Проанализируем множество вариантов эволюции ИУС. Варианты эволюции ИУС определяются маркетинговой политикой предприятия и наличием рынков сбыта продукции. Разработанные системы могут тиражироваться в виде поставочных комплектов, которые могут несколько отличаться друг от друга вследствие изменений требований заказчика, а также вследствие других эволюционных изменений, вызванных доработками, развитием технологий, элементной базы.

Специфическим видом комплектов являются диверсные комплекты ИУС, которые позволяют повысить их безопасность и надежность за счет введения версионной избыточности [14]. Версионная избыточность реализуется путем одновременного использования нескольких комплектов ИУС, разработанных с применением различных программно-аппаратных решений. Кроме того, могут быть разработаны принципиально новые типы ИУС, в той или иной степени отличающиеся от существующих образцов.

Таким образом, целесообразно выделить следующие три варианта эволюции ИУС: 1) разработка очередного поставочного комплекта ИУС; 2) разработка диверсного комплекта ИУС; 3) разработка нового типа (комплекта) ИУС.

Функционально-компонентный подход к анализу эволюции ИУС. Варианты эволюции ИУС определяются изменениями двух взаимосвязанных составляющих: 1) набора функций, реализуемых программно-аппаратными компонентами ИУС; 2) набора программно-аппаратных компонент.

В практике создания ИУС новые системы, как правило, не разрабатываются «с нуля», а опираются на уже существующие программно-аппаратные решения, которые, в свою очередь, реализуют определенный набор функций. Поэтому, в большинстве случаев целесообразно говорить об OTS-подходе к разработке ИУС. Тогда при анализе изменений следует зафиксировать предыдущую версию ИУС, как некую отправную точку, а для следующей версии ИУС проанализировать изменения относительно предыдущей версии ИУС. Между функциональной и компонентной составляющими существует определенная корреляция. Однако, степень функциональных изменений (исходя из уточненного назначения ИУС и решаемых задач) и компонентных изменений (исходя из применяемых программно-аппаратных средств и технологий), а также их взаимозависимость определяются множеством различных факторов и

должны быть проанализированы для каждого конкретного случая.

Таким образом, функционально-компонентный подход к анализу эволюции ИУС заключается в построении траектории эволюции ИУС в пространстве «функции–компоненты».

Данный подход иллюстрируется рис. 1. Пространство «функции-компоненты» задается соответствующими осями. Начало координат представляет собой некоторую зафиксированную версию ИУС. Поскольку в общем случае возможно сокращение как функциональности ИУС, так и набора компонент, будем считать, оси пространства «функции-компоненты» имеют отрицательную составляющую. Для каждого варианта реализации ИУС имеем как изменения в функциональности ΔФ, так и изменения в составе компонент ΔК. ΔФ и ΔК могут быть определены с использованием специальных метрик. Таким образом, изменения для каждого варианта реализации ИУС могут быть описаны вектором эволюции ИУС **ΔФК**, который характеризуется модулем $|\mathbf{\Delta\Phi K}| = \sqrt{\Delta\Phi^2 + \Delta K^2}$ и углом отклонения от оси К $\varphi = \text{arctg}\,(\Delta\Phi / \Delta K)$. Длина вектора $|\mathbf{\Delta\Phi K}|$ определяет степень изменений, внесенных в ИУС, угол φ – соотношение между функциональными и компонентными изменениями ИУС. Вектор в целом полностью определяет траекторию эволюции ИУС. Таким образом, рис. 1 представляет собой геометрическую интерпретацию функционально-компонентного подхода к анализу эволюции ИУС.

Рис. 1. Геометрическая интерпретация функционально-компонентного подхода к анализу эволюции ИУС

На рис. 1 представлены три возможных варианта эволюции ИУС: $\mathbf{\Delta\Phi K_1}$ – разработка очередного поставочного комплекта ИУС; $\mathbf{\Delta\Phi K_2}$ – разработка диверсного комплекта ИУС; $\mathbf{\Delta\Phi K_3}$ – разработка нового типа ИУС.

Вектор $\mathbf{\Delta\Phi K_1}$ имеет минимальный модуль, поскольку при тиражировании поставочных комплектов ИУС имеем минимальные изменения и функциональной, и компонентной составляющей. При разработке диверсного комплекта вектор эволюции ИУС $\mathbf{\Delta\Phi K_2}$ совпадает с осью K ($\varphi_2 = 0$), поскольку функциональность ИУС не меняется, а все изменения обуславливаются изменениями программно-аппаратных компонент. Изменения компонентной составляющей ΔK_2 в данном случае будут наибольшими, поскольку задачей создания диверсных комплектов ИУС является именно реализация максимальных изменений программно-аппаратных компонент с целью снижения вероятности отказов по общей причине. Максимальную длину (модуль) вектор эволюции ИУС $\mathbf{\Delta\Phi K_3}$ будет иметь при разработке нового типа ИУС. Что касается угла φ, то в общем случае нельзя заранее утверждать, когда его величина будет больше: при разработке очередного поставочного комплекта ИУС (φ_1) или при разработке нового типа ИУС (φ_3).

Функционально-компонентная модель ИУС. Разработанная геометрическая интерпретация пространства «функции–компоненты» является общей. В действительности и функции, и компоненты ИУС имеют сложную иерархическую структуру.

Таким образом, в пространстве «функции-компоненты» имеем иерархическую структуру осей, что, в свою очередь, приводит к иерархической структуре пространственного представления. Поэтому, размерность эволюционно-компонентной модели при детальном описании эволюции реальных ИУС значительно возрастает. Для решения задачи описания пространства «функции-компоненты» необходима более подробная функционально-компонентная модель ИУС.

Проанализируем программно-аппаратную структуру компонентов ИУС. Конструктивно ИУС представляет собой набор блоков, объединенных в составе шкафов. В состав блоков могут входить процессоры, реализующие комплекс программ. Отметим, что функции ИУС, которые традиционно реализовывались посредством ПО, последнее время все чаще передаются устройствам на базе программируемых логических интегральных схем (ПЛИС). ПЛИС представляют собой симбиоз аппаратных средств и ПО: физически аппаратная реализация разрабатывается и верифицируется программными методами и в программной среде [13]. В рамках рассматриваемой модели проект ПЛИС и его составляющие целесообразно рассматривать по аналогии с программными компонентами.

Таким образом, программно-аппаратные компоненты ИУС представляют собой конструктивы (шкафы и блоки), которые включают в себя как аппаратные средства (АС), так и ПО.

АС блока состоят из функциональных узлов. Функциональные узлы состоят из схемотехнических элементов, фиксированная комбинация которых составляет элементную базу ИУС. Элементная база представляет собой основу построения ИУС. В составе функциональных узлов блока только процессоры, как правило, содержат ПО. В свою очередь, ПО процессоров состоит из программных модулей. С точки зрения изменяемости компонент среди модулей целесообразно выделить библиотеку, которая может переходить из проекта в проект без изменений. Остальные модули является изменяемыми, и степень изменений зависит от конкретного типа ИУС. Проект ПЛИС, являющийся аналогом ПО микропроцессора, также включает в свой состав модули.

Модули ПО и модули ПЛИС включают набор алгоритмов, через которые непосредственно реализуются подфункции ИУС. Алгоритмы настраиваются на выполнение конкретных функций и подфункций при помощи констант и параметров. Аналогом программных алгоритмов в проектах ПЛИС являются так называемые IP-Cores (Intellectual Property Cores – ядра с интеллектуальными свойствами). Такие ядра (алгоритмы), с одной стороны, универсальны и надежно повторяемы, а с другой, - параметрически настраиваемы под конкретный проект.

Описанная выше программно-аппаратная структура ИУС может быть представлена в виде восьмиуровневого графа, имеющего форму дерева (рис. 2). Графовая модель компонентов ИУС позволяет четко определить структурные уровни АС и ПО, а также разграничить АС и ПО ИУС.

Реализация функций ИУС осуществляется путем разработки различного рода программно-аппаратных компонент. Поэтому, может быть сделан вывод о том, что наличие типовой структуры выполняемых функций приводит к наличию в составе ИУС типовых функциональных подсистем и их составных частей. Шкаф, включающий АС и ПО, реализует все множество функций ИУС. В составе ИУС функциональные подсистемы обычно реализуются в виде блоков. Один блок может выполнять одну или несколько функций ИУС.

В свою очередь, блоки состоят из функциональных узлов. Функциональные узлы выполняют подфункции, необходимые для реализации функции или группы функций ИУС. Таким образом, функции ИУС могут быть декомпозированы на составные подфункции. Структура подфункций может иметь несколько иерархических уровней. Структура функций ИУС определяются структурой ее аппаратно-программных компонент. Таким образом,

модель функций ИУС может быть представлена в виде древообразного графа, подобного графу, представленному на рис. 2. Граф функций ИУС является урезанным по сравнению с графом компонент ИУС, поскольку подфункции ИУС не приписываются нижним уровням аппаратных и программных компонент (уровни элементов и констант и параметров ПО).

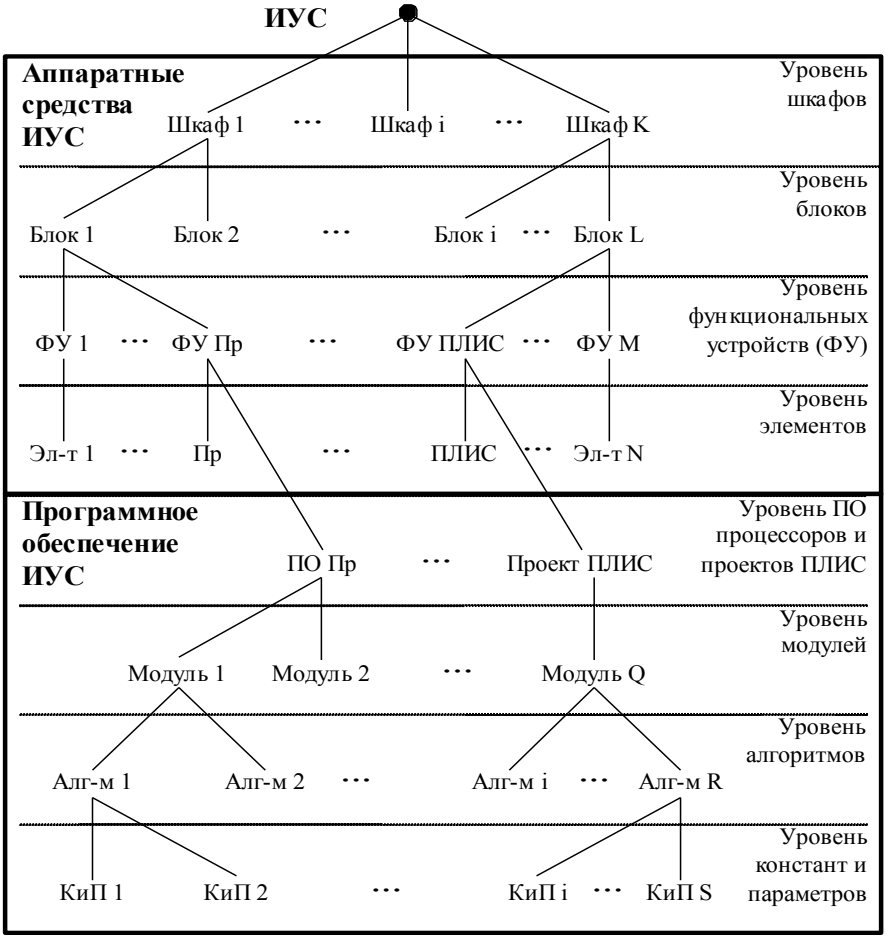

Рис. 2. Графовая модель структуры компонентов ИУС

Принципы оценки надежности ИУС при повторном использовании компонент. К современным ИУС критического использования для таких отраслей, как энергетика, транспорт и др., применяются жесткие требования по надежности [1 – 3]. Требования к надежности таких систем должны содержать: ***перечень функций***, для которых регламентируют пока-

затели надежности, первую очередь, показатели безотказности и ремонтопригодности; ***виды и критерии*** отказов для каждой функции; ***номенклатуру показателей*** безотказности и ремонтопригодности для каждой функции; ***значения показателей*** безотказности и ремонтопригодности.

Рассмотренный фрагмент требований к ИУС АЭС позволяет выявить ряд проблем, возникающих при оценке и демонстрации надежности ИУС:

– потребность в достоверных исходных данных;

– необходимость разработки и апробации методик оценки надежности;

– высокая точность расчетов при демонстрации значений показателей надежности близких к единице или к нулю;

– необходимость учета программной составляющей ИУС [5];

– выбор и/или разработка инструментальных средств (ИС);

– необходимость модификации расчетов надежности при частичных изменениях в тиражируемых ИУС.

Эволюционно-компонентная модель ИУС является основой для разработки подхода к решению задачи конфигурационной оценки надежности ИУС. Общие принципы оценки надежности ИУС при повторном использовании компонент включают:

– использование типовой структуры функциональных подсистем ИУС (типовых блоков и типовых функциональных узлов);

– использование для оценки надежности ИУС иерархической модели, построение которой определяется структурной моделью функций и программно-аппаратных компонентов ИУС;

– конфигурационное управление многокомпонентной моделью надежности ИУС.

Выводы. Предложенная эволюционно-компонентная модель ИУС позволяет решать следующие практические задачи:

– реализовать процесс конфигурационного управления компонентами ИУС;

– фиксировать изменений в структуре и функциях ИУС;

– проводить анализ применимости готовых OTS компонент;

– выполнять конфигурационную оценку надежности ИУС;

– оценивать трудозатраты на разработку ИУС.

Полученные результаты были применены в конструкторском бюро АСУ НПО «Радий» при разработке ИУС, важных для безопасности АЭС.

ЛИТЕРАТУРА

1. *Харченко В.С., Скляр В.В., Кожемяченко В.Г. Классификация и профилирование OTS-продуктов для компьютерных систем управления // Системи обробки інформації. – Х.: ХВУ. – 2003. – Вип. 2. – С. 38 – 44.*

2. *Preckshot G., Scott J. A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications. NUREG/CR-6421. – Lawrence Livermore National Laboratory, 1995. – 33 p.*
3. *DeBusk B. Managing the Reliability of COTS-based Military Systems // Proceedings of the 44th Annual Reliability and Maintainability Symposium. – Anaheim (California, USA). – 1998. – P. 394 – 400.*
4. *IAEA TECDOC–1328. Solution for Cost Effective Assessment of Software Based Instrumentation and Control Systems in Nuclear Power Plant. – Vienna: International Atomic Energy Agency, 2002. – 131 p.*
5. *Харченко В.С., Харченко К.В. COTS- и CrOTS-подходы к повышению эффективности критических и коммерческих IT-проектов // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ. – 2002. – Вип. 2 (18). – С. 252 – 258.*
6. *McDermid J. The Cost of COTS // IEEE Transactions on Computer. – 1998. – V. 46, n 6. – P. 490 – 498.*
7. *Popov P., Riddle S., Romanovsky A., Strigini L. On Systematic Design of Protectors for Employing OTS Items // Proc. of the 27th Euromicro conference. – Warsaw, Poland. – 2001. – P. 22 – 29.*
8. *Харченко В.С., Скляр В.В., Ястребенецкий М.А. Экспертная оценка безопасности OTS компонент информационных и управляющих систем АЭС // Збірник наукових праць ІПМЕ ім. Г.Є. Пухова НАНУ. Спец. вип. "Інформаційні технології в енергетиці". – К.: ІПМЕ. – 2003. – С. 12 – 19.*
9. *Voas J. Maintaining Component-Based Systems // IEEE Transactions on Software. – 1998. – V. 24. – n 7. – P. 531 – 540.*
10. *Yu Y., Johnson B. A BBN Approach to Certifying the Reliability of COTS Software Systems // Proceedings of the 49th Annual Reliability and Maintainability Symposium. – Tampa (Florida, USA). – 2003. – P. 19 – 24.*
11. *Буч Г. Объектно-ориентированный анализ и проектирование с примерами приложений на C++. – М.: «Бином», 2000. – 560 с.*
12. *Herasimenko O., Sklyar V., Kharchenko V. An Evolutional-Component Model of Process Control System // Proceedings of the 2nd International Conference Advanced Computer Systems and Networks Design and Application "ACSN–2005". – Lviv (Ukraine). – 21 – 23 September 2005. – P. 123 – 126.*
13. *Kharchenko V., Lysenko I., Sklyar V., Herasimenko O. Safety and Reliability Assessment and Choice of the Redundant Structures of Control Safety Systems // Proceedings of IEEE East-West Design & Test Workshop (EWDTW'05). – Odessa (Ukraine). – 15 – 19 September 2005. – P. 212 – 218.*
14. *Харченко В.С., Жихарев В.Я., Илюшко В.М., Нечипорук Н.В. Многоверсионные системы, технологии, проекты. – Х.: НАКУ «ХАИ», 2003. – 486 с.*

Поступила 2.11.2005

Рецензент: доктор технических наук, профессор В.С. Харченко,
Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ».