SECTION 4. Computer science, computer engineering and automation.

Victor Aleksandrovich Melent'ev
Philosophy Doctor, Senior research associate
Institute of Semiconductor Physics Siberian Branch RAS, Russia
melva@isp.nsc.ru

RELIABILITY OF ELEMENTS OF THE COMPUTING SYSTEM AND ITS FAULT TOLERANCE

Abstract: *The system is given by a set of essential functions, and by a graph setting the environment for realization of these functions, and by the adequacy predicate establishing conditions of correspondence of the system graph to the set of the essential functions. This formal model allows to investigate tolerance of the system to the failures to be specified by the flow which is caused by a arbitrary factors, including and nonrandom. The flow of failures is assigned by a configuration space of the failed elements. Here a maximum value of the failure multiplicity is determined by the sum of a ceil value of the expectation of the number of a failed elementary machines (EM) and by the prescribed tolerance margin. The expectation is calculated subject to the workload of the system and to the distribution efficiency of this workload. The tolerance margin satisfies to acceptance criteria and allows for deviations of the real conditions of the system elements' functioning from the normative ones.*

***Key words*:** elements reliability of computing systems, fault tolerance of system, fault multiplicity, system graph.

Citation: Melent'ev VA (2014) RELIABILITY OF ELEMENTS OF THE COMPUTING SYSTEM AND ITS FAULT TOLERANCE. ISJ Theoretical & Applied Science 9 (17): 34-45. doi: http://dx.doi.org/10.15863/TAS.2014.09.17.6

УДК 519.17: 681.3

НАДЕЖНОСТЬ ЭЛЕМЕНТОВ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ И ЕЕ ОТКАЗОУСТОЙЧИВОСТЬ [1]

Аннотация: *Система задана множеством существенных функций, графом, устанавливающим среду для реализации этих функций, и предикатом адекватности, ставящим условия соответствия графа системы множеству существенных функций. Такая формальная модель позволяет исследовать устойчивость системы к отказам, заданным потоком, обусловленным не только случайными факторами. Поток отказов определен пространством конфигураций отказавших элементов, где максимальное значение кратности отказов определяется суммой округляемого вверх математического ожидания числа отказавших элементарных машин (ЭМ) и заданного запаса устойчивости. Математическое ожидание рассчитывается с учетом загрузки системы и эффективности ее распределения. Запас устойчивости соответствует требованиям Заказчика и учитывает отклонения реальных условий эксплуатации элементов системы от нормативных.*

Ключевые слова: *надежность элементов вычислительных систем, отказоустойчивость системы, кратность отказов, граф системы.*

[1] Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект 14-07-00169а)

Система задана множеством существенных функций, графом, устанавливающим среду для реализации этих функций, и предикатом адекватности, ставящим условия соответствия графа системы множеству существенных функций. Такая формальная модель позволяет исследовать устойчивость системы к отказам, заданным потоком, обусловленным не только случайными факторами. Поток отказов определен пространством конфигураций отказавших элементов, где максимальное значение кратности отказов определяется суммой округляемого вверх математического ожидания числа отказавших элементарных машин (ЭМ) и заданного запаса устойчивости. Математическое ожидание рассчитывается с учетом загрузки системы и эффективности ее распределения. Запас устойчивости соответствует требованиям Заказчика и учитывает отклонения реальных условий эксплуатации элементов системы от нормативных.

1. Введение.

Известно, что работа даже в штатных режимах сопровождается значительными температурными перепадами, зависящими от загрузки системы и от наличия и эффективности средств балансирования нагрузки ее элементов, от суточных и сезонных температурных циклов и наличия средств их нейтрализации и т.п. Влияние же на работоспособность системы внешних разрушающих факторов, в особенности, искусственного происхождения, не может быть учтено анализом совокупной надежности ее элементов в принципе. Кроме того, численные оценки надежности различных архитектурных вариантов сложных систем, состоящих из большого числа элементов, как правило, настолько близки, что сопоставление этих вариантов не выявляет между ними существенной разницы.

Ориентация на высокие надежностные характеристики элементов системы в силу вероятностной природы этих характеристик и недостаточной их достоверности в реальных условиях эксплуатации не исключает возможности отказов системы и соответствующих им катастрофических последствий. Надежностный подход несет в себе опасное заблуждение о возможности создания систем с непрерывной готовностью путем совершенствования технологических и методико-испытательских приемов получения высоконадежных компонентов в сочетании с их многократным резервированием и, таким образом, отвлекает от решения проблемы отказов, зависящих от совокупной системной организации компонентов, от интенсивности и условий использования, от наличия или отсутствия внешних факторов, направленных на разрушение системы, и, соответственно, от наличия или отсутствия противодействующих этим фактором средств.

Подмена понятий отказоустойчивости и живучести системы понятием совокупной надежности ее элементов усугубляется, как правило, абстрагированием от информационно-логической структуры системы и от конфигураций возникающих в ней отказов. Правомерность такого упрощенного подхода к исследованию отказоустойчивости систем с менее чем 100%-й избыточностью представляется весьма сомнительной. Подобную примитивизацию можно считать приемлемой лишь при исследовании надежности полностью резервированной системы, коэффициент избыточности которой тождественен допускаемой в системе кратности отказов, т.е. для систем, допускающих повышение их готовности за счет пропорционального снижения эффективности. Тем не менее, в [1, с. 358], например, потенциальная живучесть вычислительной системы оценивается отношением математического ожидания числа исправных элементарных ее машин к общему их числу. При этом считается, что избыточное число ЭМ в системе не превышает «десятичного логарифма числа составляющих ЭМ». Не обсуждая здесь вопросы достоверности используемой в этой работе экспоненциальной модели надежности ЭМ, отметим, что система там считается работоспособной, если число N исправных машин в ней (безотносительно к их связанности) не менее числа n. Заметим, что истинное значение

математического ожидания числа исправных ЭМ *в работоспособной системе*, никак не тождественно математическому ожиданию общего их числа. В действительности оно определяется средним значением числа ЭМ *в множестве их работоспособных конфигураций*, характеризуемых наличием в каждой из них компоненты связности с числом вершин в ней, не меньшим числа *n*. То есть, истинное значение искомого математического ожидания необходимо определять произведением среднего числа исправных ЭМ на условную вероятность соответствия их совокупности требованиям связности. Значение этой вероятности определяется отношением числа конфигураций, сохраняющих заданное число *n* связных ЭМ, к общему числу конфигураций. Оно равно единице (т.е. условную вероятность можно не принимать во внимание) только в единственном случае: если структура системы полносвязна. К примеру, для кольцевой структуры ВС при $N=100$, $n=95$ и при наличии двух отказавших ЭМ условная вероятность сохранения в системе компоненты связности с числом вершин, не меньшим *n*, составляет всего лишь $2(N-n)/(N-1)$, или 10,5%; такая система обладает не 98%-й потенциальной живучестью (без учета структуры), а составляет всего лишь 9,75% от нее. Из примера видно, что достоверность подобных моделей, исключающих из рассмотрения структурную составляющую архитектуры отказоустойчивой системы, тем сомнительнее, чем более структура системы отличается от полного графа. Игнорирование же при этом состава функциональных подсистем, каждая из которых, как правило, предъявляет специфические требования к структуре сети связи, ограничивает применимость рассмотренного подхода пустым множеством реально действующих систем.

Отказоустойчивость системы заключается в эффективном противодействии распространению на нее последствий некоторого числа отказов ее компонентов в любом их сочетании и независимо от их происхождения, будь они случайными или обусловленными. В работе [2, с. 1215-1218] показано, что показатели надежности отдельных ЭМ системы, полученные путем статистической обработки результатов их автономных испытаний, не соответствуют реальным режимам их эксплуатации в составе системы, что потоки отказов составляющих систему ЭМ не являются пуассоновскими и зависят от режимов и времени их предшествующей эксплуатации. В работе показано, что полное время работы ЭМ в составе системы коррелированно реальной загруженностью последней и может быть приведено к нормативным режимам функционирования. При этом коэффициенты масштабирования времени и интенсивности отказов ЭМ определяются функцией плотности вероятности распределения ее состояний, которая соответствует качеству общесистемных алгоритмов организации функционирования системы, в частности, алгоритмов выравнивания ее нагрузки. Предложена обобщенная модель отказоустойчивой системы, устанавливающая взаимосвязь функциональной и структурной компонент системы с условиями, определяющими ее работоспособность в потоке отказов произвольного происхождения.

2. Моделирование надежности элементов вычислительных систем.

Основанием для использования модели простейшего потока отказов в исследованиях надежности ЭВМ, состоящей из сотен и тысяч дискретных элементов, является центральная предельная теорема, согласно которой сумма большого числа независимых потоков с любыми законами распределения приближается к простейшему потоку с ростом числа слагаемых потоков. В настоящее же время, когда состав ЭМ существенно изменился и исчисляется теперь лишь единицами БИС (процессор, память, коммутатор), закон больших чисел не может быть применен, поток отказов не может быть безоговорочно принят простейшим, а используемый в качестве исходной посылки при выведении формул надежности ВС постулат об экспоненциальном характере функции надежности элементарной машины является ошибочным.

Ненадежность элементарной машины в составе ВС обусловлена не только внутренними свойствами используемых интегральных микросхем (ИМС) (качеством технологических процессов производства и испытаний, конструктивными недостатками, необратимостью накапливаемых в процессе эксплуатации дефектов и т.п.), но и свойствами системы в целом (эффективностью используемых алгоритмов выравнивания загрузки, эффективностью системы охлаждения или защиты и т.д.). Очевидно, что математическое ожидание числа отказавших элементов системы, рассчитанное без учета неизбежных в процессе эксплуатации отклонений элементов системы от нормативных режимов их функционирования, обусловленных например, случайным характером потока поступающих в систему заданий и несовершенством алгоритмов их распределения, не является вполне достоверным, если существует корреляционная связь между этими отклонениями и показателями надежности элементов.

Наличие такой корреляционной связи давно осознано ведущими производителями микросхемотехники, отказавшимися от неадекватного реалиям эксплуатации представления потока отказов пуассоновской моделью, основанной на допущении ординарности, стационарности и отсутствии последействия. Тем не менее, применение этой модели в теоретических исследованиях надежности компонентов вычислительных систем по-прежнему преобладает. Общепринятыми при этом значениями интенсивности λ отказов высоконадежных электронных компонентов в нормативных условиях их эксплуатации считают значения от 10^{-6} до 10^{-9} час$^{-1}$, устройства с более низкими значениями относят к сверхвысоконадежным. Значение λ, как правило, считают при этом неизменным, а величину средней наработки до отказа T определяют обратной λ величиной: $T = \lambda^{-1}$. Получаемые таким образом теоретические значения среднего времени T наработки до отказа для высоконадежных ИМС составляют от 10^6 до 10^9 часов (114-114155 лет) [3, с. 22].

Между тем, практика эксплуатации, как отдельных электронных компонентов, так и их совокупностей (в частности, в составе компьютеров) указывает на существенные различия в фактических значениях T и λ^{-1}, обусловленных наличием в потоке отказов деградационной составляющей. Приведем в этой связи весьма показательный пример, взятый из [4, с. 6]. Если в группе из 500 000 человек в возрасте 25 лет в течение года умрет 625 человек, то с учетом эксплуатационного ресурса такой группы, составляющего 500 000 человеко-лет, интенсивность отказов составит $1{,}25 \cdot 10^{-9}$ год$^{-1}$. Значение, обратное этой интенсивности и равное 800 годам, превышает среднюю продолжительность ($T \cong 70 \div 80$ лет) человеческой жизни более чем в 10 раз. Из примера видно, что отождествление среднего времени T наработки до отказа с величиной λ^{-1} учитывает лишь случайную составляющую общего числа отказов и игнорирует обусловленную накопительными процессами деградации (износа) детерминированную его часть. В общем же случае справедливо $0 < T \le \lambda^{-1}$. Очевидно, что равенство $T = \lambda^{-1}$ выполняется лишь при отсутствии или ничтожности в сравнении со случайными отказами отказов деградационных; если же $T < \lambda^{-1}$, то поток отказов нестационарен и зависит от предыстории эксплуатации устройства, а функция вероятности его безотказной работы отличается от экспоненциальной.

Принятые для полупроводниковых приборов сверхнизкие значения интенсивности потока случайных отказов, не позволяют проводить надежностные испытания в течение сотен и тысяч лет, соответствующих этим значениям, тем более что реальные сроки эксплуатации этих изделий, определяемые их моральным износом, на порядки меньше. Так как достоверность статистических исследований определяется репрезентативностью соответствующей выборки, то и размеры, соответствующие столь малому числу событий (отказов) в процессе испытаний, существенно превышают размеры партий выпускаемых

изделий и также не могут быть достигнуты. Трудоемкость полноценных испытаний усугубляется необходимостью охвата всего вероятностного пространства состояний испытуемых объектов, обусловленного ожидаемыми эксплуатационными температурным и вольтамперным диапазонами и соответствующими им временными циклами. В разрешение этой проблемы ГОСТ 27.002-89 (Надежность в технике…) предусматривает использование «экстраполированных показателей, определяемых на основании результатов расчетов, испытаний и (или) эксплуатационных данных путем экстраполирования на другую продолжительность эксплуатации и другие условия эксплуатации».

Ведущие мировые производители добиваются сокращения времени испытаний изделий микросхемотехники до значений, существенно меньших их реальной долговечности, применением методики ускоренных испытаний HAST (Highly Accelerated Stress Test). Основным приемом при этом является форсирование режимов, основанное на введении факторов, ускоряющих физико-химические процессы старения и деградации ИМС [5, с. 5]. Результаты таких испытаний экстраполируют на нормативные режимы посредством использования моделей, учитывающих сложность испытуемых объектов и технологических процессов их изготовления, виды дефектов и соотношения между ними, разницу температур и напряжений между испытаниями и нормативными режимами. Заметим, что сам факт использования методик форсированных испытаний и последующей экстраполяции получаемых при этом результатов на заданные режимы эксплуатации приборов указывает на коррелированность показателей интенсивности отказов и средней наработки до отказа от режимов эксплуатации, – и это нельзя не учитывать в оценках надежности реальных устройств.

Выбор модели потока отказов производят, как правило, по результатам исследований физических процессов, приводящих к отказу. Как показано в [6, с, 37; 7, с. 194], отказы ИМС хорошо описываются распределениями, имеющими конкретную физическую интерпретацию. Там же дан сравнительный анализ вероятностно-физических моделей отказов и перечислены наиболее распространенные деградационные процессы в ИМС. Так как этими процессами являются химическая реакция, диффузия, электромиграция носителей и электрокоррозия, то в основе большинства их моделей лежит уравнение Аррениуса, устанавливающее связь между скоростью этих процессов и температурой [8, с. 1]. В соответствии с этим уравнением скорость химических и физических процессов, лежащих в основе отказа ИМС при средних значениях энергии активации $E_a = 0{,}7 \div 0{,}8$ эВ, удваивается с повышением ее температуры на каждые $10^{\circ}\mathrm{C}$. Отметим также, что одним из способов удовлетворения всегда актуальному требованию повышения быстродействия является увеличение энергии активации, снижающее флуктуационную составляющую сигнала, но увеличивающее при этом коэффициент K_y ускорения процесса старения ИМС и соответствующим образом снижающее ее долговечность. Так, например, если фактор ускорения при температуре $40^{\circ}\mathrm{C}$ принят равным единице, то увеличение E_a до 1,3 эВ в совокупности с повышением температуры до $100^{\circ}\mathrm{C}$, может вызвать снижение долговечности примерно в 5000 раз [3, с. 24], что существенно больше, чем $K_y = 2^6$ при $E_a = 0{,}7 \div 0{,}8$ Эв.

Используемые в исследованиях надежности изделий микросхемотехники модели отличаются выбором закона распределения отказов, соответствующего типу преобладающего в испытуемом приборе деградационного процесса с присущим этому прибору значением энергии активации [8, с. 2], технологическим процессом изготовления, количеством в нем $p-n$ переходов и т.п. В то же время все модели сходятся в том, что показатели надежности коррелированны временем и режимами предшествующей эксплуатации, а между средней наработкой до отказа T и интенсивностью отказов λ изделия существует зависимость более сложная, чем обратная. В работе [5, с. 7], например,

показано, что если в качестве модели отказов ИМС используется не экспоненциальное, а двухпараметрическое диффузионное DN-распределение, соответствующее немонотонному марковскому процессу, то рассчитанные по результатам ускоренных испытаний оценки надежности имеют не более чем 10%-ю погрешность. Данная там же сравнительная оценка показателей средней наработки до отказа для экспоненциального распределения и для DN-распределения, показывает, что для большинства технологических процессов изготовления ИМС средняя наработка до их отказа, полученная из экспоненциального распределения, завышена в сравнении с DN-распределением в 70-520 раз.

Многие ведущие фирмы – изготовители микросхем (Siemens AG, Analog Devices (ADI), Atmel, Xilinx) используют в оценках надежности χ^2 -распределение и оценивают [9, с. 46] экспериментальную интенсивность отказов по формуле:

$$\lambda = \frac{\chi^2(P,v)}{2N\,\Delta t\,K_y}\cdot 10^9.$$

Здесь P — доверительная вероятность (0,5–0,95), связанная с уровнем значимости (Confidence Level – CL) соотношением $(1-CL/100)$, фирмы Atmel и ADI в своих расчётах уровень значимости закладывают $CL = 60\% \div 90\%$; $v = (2n+2)$, где n – количество отказавших ИС; N – общее число испытуемых ИС; K_y – обобщённый коэффициент ускорения; Δt – время испытаний. Из этой формулы видно, что экстраполяция результатов испытаний на другие температурные режимы производится с учетом приведённого к этим режимам времени испытаний (эквивалентных приборо-часов) – $t_э = N\,\Delta t\,K_y$.

Заметим, что независимо от выбора закона экстраполяции (экспоненциальное, вейбулловское, логнормальное, DN-, χ^2- или другие распределения) текущее значение интенсивности λ отказов прибора определяется не текущим временем t его эксплуатации, а эквивалентным его значением $t_э$, причем $K_у(-\Delta t^\circ\mathrm{C}) = K_у^{-1}(\Delta t^\circ\mathrm{C})$, где $\Delta t^\circ\mathrm{C} = t^\circ\mathrm{C} - t_н{}^\circ\mathrm{C}$ – отклонение от нормативной температуры $t_н{}^\circ\mathrm{C}$ прибора. Инвариантность времени $t_э$ законам и параметрам распределения показателей надежности, соответствующим различным (по технологии изготовления, сложности, видам преобладающих деградационных дефектов и т.п.) типам ИМС, позволяет абстрагироваться от этих законов при определении приведенного к нормативным режимам времени эксплуатации и соответствующей отклонениям от этих режимов интенсивности отказов.

Определим множество состояний прибора в течение времени t его эксплуатации как непрерывное в диапазоне рабочих температур $t_0{}^\circ\mathrm{C} \le t^\circ\mathrm{C} < t_{\max}$; здесь $t_0{}^\circ\mathrm{C}$ – температура окружающей среды, $t_{\max}{}^\circ\mathrm{C}$ – максимальное значение температуры прибора, при котором произойдет отказ либо отключение прибора при наличии средств защиты. Если плотность вероятностей состояний прибора в этом температурном диапазоне за время t определить функцией $f(t^\circ\mathrm{C})$, причем $\int_{t_0{}^\circ\mathrm{C}}^{t_{\max}{}^\circ\mathrm{C}} f(t^\circ\mathrm{C})\,dt^\circ\mathrm{C} = 1$, то полное приведенное к номинальной температуре время $t_э$ эксплуатации прибора, соответствующее времени t эксплуатации в динамике его функционирования определится с учетом среднего на заданном температурном диапазоне значения $K_у$:

$$t_э = tK_у = t\cdot \int_{t_0{}^\circ\mathrm{C}}^{t_{\max}{}^\circ\mathrm{C}} K_у(t^\circ\mathrm{C})\cdot f(t^\circ\mathrm{C})\,dt^\circ\mathrm{C}.$$

Аналогично этому среднее значение интенсивности отказов λ в заданном температурном диапазоне и при заданной функции $f\left(t^{\circ}\mathrm{C}\right)$ плотности вероятности распределения температур определим из

$$\lambda = \lambda_{\text{н}} K_{\text{у}} = \lambda_{\text{н}} \cdot \int_{t_0{}^{\circ}\mathrm{C}}^{t_{\max}{}^{\circ}\mathrm{C}} K_{\text{у}}\left(t^{\circ}\mathrm{C}\right) \cdot f\left(t^{\circ}\mathrm{C}\right) dt^{\circ}\mathrm{C}.$$

Здесь $\lambda_{\text{н}}$ – среднее значение интенсивности отказов прибора при эксплуатации его в нормативном режиме.

Заметим, что распространенное на практике ошибочное представление об отсутствии зависимости среднего значения интенсивности отказов и срока службы прибора от интенсивности его эксплуатации за предшествующий период основано на утверждении о балансе температурных отклонений $\pm\Delta t^{\circ}\mathrm{C}$ в обе стороны от номинальной температуры $t_{\text{н}}{}^{\circ}\mathrm{C}$. Согласно этому утверждению периодам перегрузки прибора соответствуют такие же по длительности и модулю периоды их недогрузки: $t\left(\Delta t^{\circ}\mathrm{C}\right) = t\left(-\Delta t^{\circ}\mathrm{C}\right)$. Согласившись с утверждением о балансе температурных отклонений, функцию плотности вероятности отклонения температуры $\Delta t^{\circ}\mathrm{C}$ прибора от нормативной температуры $t_{\text{н}}{}^{\circ}\mathrm{C}$ будем считать симметричной: $f\left(x\right) = f\left(-x\right)$, $0 \le x \le t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}$, $t_{\text{н}}{}^{\circ}\mathrm{C} - t_0{}^{\circ}\mathrm{C} = t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}$. Учитывая $K_{\text{у}}\left(x\right) = K_{\text{у}}{}^{-1}\left(x\right)$, получим:

$$t_{\text{э}} = t \cdot \int_{t_{\text{н}}{}^{\circ}\mathrm{C} - t_0{}^{\circ}\mathrm{C}}^{t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}} K_{\text{у}}\left(x\right) \cdot f\left(x\right) dx = t\left(\int_0^{t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}} K_{\text{у}}{}^{-1}\left(x\right) \cdot f\left(x\right) dx + \int_0^{t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}} K_{\text{у}}\left(x\right) \cdot f\left(x\right) dx \right) =$$

$$= t \cdot \int_0^{t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}} \frac{K_{\text{у}}{}^{2}\left(x\right) + 1}{K_{\text{у}}\left(x\right)} f\left(x\right) dx.$$

$$\lambda = \lambda_{\text{н}} \cdot \int_0^{t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}} \frac{K_{\text{у}}{}^{2}\left(x\right) + 1}{K_{\text{у}}\left(x\right)} \cdot f\left(x\right) dx.$$

Из $K_{\text{у}}\left(0\right) = 1$, $1 \le K_{\text{у}}\left(x\right) \le K_{\text{у}}\left(t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}\right)$ и из того, что, как показано выше, $K_{\text{у}}\left(t_{\max}{}^{\circ}\mathrm{C} - t_{\text{н}}{}^{\circ}\mathrm{C}\right) >> 1$ ясно, что приведенное полное время $t_{\text{э}}$ эксплуатации и среднее значение интенсивности λ отказов существенно превышают соответственно время t и нормативную интенсивность $\lambda_{\text{н}}$, и что эти превышения определяются эксплуатацией прибора в высокотемпературных, режимах.

Итак, показатели надежности отдельных ЭМ вычислительных систем определяются режимами их эксплуатации. Режимы эти существенно коррелированны потоком и трудоемкостью поступающих в систему заданий, а также эффективностью алгоритмов планирования и выравнивания нагрузки, направленных на максимальное использование всех компонентов системы и на максимальную их загрузку. Именно поэтому в анализе надежности ВС и составляющих ее ЭМ не следует абстрагироваться ни от суммарной загрузки системы, ни от используемых в ее распределении средств. Отметим в связи с этим, что нам не доводилось встречать исследований, направленных на поиск алгоритмов, ограничивающих эффективность использования системы нормативными режимами, соответствующими надежностным испытаниям ее компонентов, т.е. алгоритмов, искусственно занижающих эффективность как самой системы, так и ее элементов.

3. Моделирование отказоустойчивости системы

В отличие от надежности, являющейся вероятностной характеристикой системы и производной от соответствующих среднестатистических свойств и способов объединения используемых для ее построения аппаратных средств, отказоустойчивость и живучесть присущи системе благодаря ее архитектуре (функциональной, структурной, алгоритмической и т.п. организации), нацеленной на сохранение ею способности реализации в реальном времени и с определенным качеством необходимого минимума функций, достаточного для получения определенного техническими требованиями результата при возникновении любого отказа или их группы в пределах заданной кратности и независимо от вероятности появления таковых.

Исходя из этого, систему S зададим множеством $F=\{F_i\}$ обязательных (существенных) функций F_i, определяющим функциональную целостность системы, графом $G(V,E)$, задающим среду для реализации этих функций, и предикатом адекватности $\mathrm{H}=\bigcap\eta_i$, устанавливающим условия соответствия графа G множеству F функций [10, с. 92]. Здесь V – множество вершин графа (модулей системы), а E – множество ребер (межмодульных связей системы). Предикат $\eta_i(F_i,G,G_i)$ (далее просто $\eta_i(G)$) определен на дискретном множестве $\{0,1\}$ и равен единице тогда и только тогда, когда в множестве подграфов графа G найдется хотя бы один подграф G_i, удовлетворяющий условиям реализации на нем функции F_i. Предикат H системы S определяет формальные условия соответствия структуры системы в целом реализуемому на ней с необходимым качеством заданному множеству F существенных функций: $\mathrm{H}=1$, если $\forall F_i\in F\ \exists G_i \mid \eta_i(F_i,G,G_i)=1$. Добавив к этим компонентам описание ожидаемого в процессе эксплуатации потока Ф отказов, получим описание моделей системы $S=S(F,G,\mathrm{H},\Phi)$ и ее подсистем $S_i=S_i(F_i,G_i,\eta_i,\Phi)$. В общем случае отказы модулей системы и связей между ними (вершин и ребер графа) различны по природе, соответственно различны законы и параметры их распределения, поэтому разделим поток Ф на составляющие, воздействующие на вершины – Φ_v и на ребра – Φ_e графа G: $\Phi(G)=G'(\Phi_v(V),\Phi_e(E))$. Далее для сокращения выкладок учитываем наиболее деструктивную и наиболее вероятную в практике эксплуатации вычислительных систем часть потока отказов $\Phi_v(V)$, полагая $\Phi_e(E)=0$ и $\Phi(G)=\Phi_v(V)$.

Пусть функциональная подсистема $S_i=S_i(F_i,G_i,\eta_i,\Phi)$ подвержена воздействию на систему S потока отказов Ф и задана функцией $F_i\subseteq F$; предикат η_i при этом обусловливает выбор подграфа $G_i(V_i,E_i)\subseteq G$ возможностью реализации заданной функции F_i на подмножествах составляющих граф $G'(V',E')$ исправных вершин $V_i'\subseteq\Phi(V)=V'$ и исправных ребер $E_i'\subseteq\Phi(E)=E'$. Равенство $\eta_i(G_i')=1$ указывает на адекватность дефектного подграфа $G_i'=\Phi(G_i)$ требованиям, заданным предикатом η_i. Оно равносильно равенству $F_i\cap\eta_i(G_i')=F_i$ и описывает случай автономной отказоустойчивости подсистемы, достигаемой за счет ее внутренних ресурсов. Менее жестким в достижении отказоустойчивости является равенство $\eta_i(G')=1$, или $F_i\cap\eta_i(\Phi(G))=F_i$, – в этом случае подсистема ориентирована на сохранение ею работоспособности путем использования не только своих внутренних ресурсов, но и ресурсов системы в целом. Отказоустойчивость системы в целом достигается делегированием этого свойства каждой из существенных функциональных подсистем:

$\mathrm{H}(\Phi(G))=1$ при $\bigcap_1^{|F|}(\eta_i(G_i')\cup\eta_i(G'))=1$, отсюда $F\bigcap\mathrm{H}(\Phi(G))=\{F_i\bigcap\eta_i(\Phi(G))\}=\{F_i\}$. Несомненно, что в состав существенных подсистем отказоустойчивой ВС должны быть включены системообразующая, контрольно-диагностическая и реконфигурационная подсистемы, утилитарность которых ясна из их названий. Кратность допускаемых в этих подсистемах отказов (не приводящих к потере ими работоспособности), должна быть не меньшей кратности, допускаемой в наиболее отказоустойчивой прикладной подсистеме из числа существенных [11, с. 148].

Каждая из существенных функций с учетом возможных дефектных конфигураций системы может быть реализована множеством способов, зависящих от алгоритмической, программной и аппаратурной ее реализации: $F_i=\{f_i\bigcap\{A_i(p_i,h_i)\}\}\subseteq F$. Единство связанных условиями взаимной адекватности компонент: алгоритмической A_i – как способа реализации, программной p_i – как средства и аппаратной h_i – как среды реализации функции F_i, указывает на резервы повышения отказоустойчивости подсистемы путем расширения границ взаимной адекватности ее компонент, т.е. путем использования таких алгоритмов и реализующих их программ и технических средств, которые в комплексе обеспечивают устойчивость подсистемы S_i к отказам заданной кратности. Функциональная компонента f_i каждой подсистемы S_i сочетает в себе алгоритм A_i реализации функции f_i и конкретизирующие его программную p_i и аппаратурную h_i составляющие. Последняя входит в состав связанного множества модулей, поставленных в соответствие вершинам V_i и ребрам E_i подграфа $G_i(V_i,E_i)$ графа G системы S. Данный абзац направлен на осознание того факта, что в общем случае любая из функций $F_i\subseteq F$ может быть реализована не единственным, а некоторым множеством способов, рассчитанных на диапазон возможной деградации аппаратных средств. Это указывает на возможности повышения отказоустойчивости ВС посредством максимального использования потенциальных возможностей ее структуры путем введения большей алгоритмической и программной избыточности.

Анализ отказоустойчивости заключается в оценке степени сохранения системой существенных для ее пользователей утилитарных качеств в полиномиальном множестве конфигураций заданного числа l отказавших в ней элементов. Модели такой системы и ее подсистем опишем следующим образом:

$$S=S\left(F,G,\mathrm{H},l=\{0,...,l_{\max}\}\right),\ S_i=S_i\left(F_i,G_i,\eta_i,l=\{0,...,l_{\max}\}\right).$$

Здесь $l_{\max}$ – максимальное значение кратности одновременно присутствующих в системе отказов в течение планируемого срока ее эксплуатации, коррелированного ее загруженностью и внешними условиями. Определим это значение суммой округленного вверх математического ожидания $M(l)$ числа отказавших элементарных машин (ЭМ) и заданного запаса δl устойчивости: $l_{\max}=\lceil M(l)\rceil+\delta l$. Запас устойчивости может быть задан приращением δl или соответствующим этому приращению коэффициентом и соответствует критическим требованиям Заказчика. Введение запаса предупреждает отказ системы в экстремальных условиях эксплуатации ее элементов, например, при воздействии пиковых значений радиационного фона, при пиковой загрузке системы, при наличии направленных извне разрушающих факторов и т.п.

Как показано в разделе 2, текущее значение интенсивности λ отказов отдельных ЭМ следует определять исходя из приведенного к номинальным режимам времени $t_э$, учитывающего функции их загрузки в процессе эксплуатации вычислительной системы и соответствующие ей неизбежность отклонений от нормативных режимов и ускорение

деградации. Нами уже отмечалось также, что состав ЭМ в настоящее время ограничен набором всего лишь нескольких ИМС (процессор, память, коммутатор). Это не позволяет распространить на ЭМ действие центральной предельной теоремы и считать поток отказов в ней простейшим, тем более что модели потоков отказов разнотипных ИМС различаются между собой типами преобладающих дефектов, ускорениями их проявлений от режимов, вкладами каждой из ИМС в общее число отказов ЭМ и т.д. Хотя исследования в части надежности ЭМ пока что не актуализированы их нынешней архитектурой, но многочисленные форумы пользователей указывают на процессор, как на наиболее подверженную отказам часть ПК при превышении его нормативных эксплуатационных режимов притом, что даже использование многоядерных архитектур не спасает процессор от общего перегрева при интенсивном его использовании. Учитывая это, а также то, что основная часть загрузки ЭМ выпадает прежде всего на процессор, примем его здесь за основной компонент, режимы и соответствующая им интенсивность отказов которого определяются его загруженностью. Если считать распределение температур процессора в процессе его эксплуатации нормальным с соответствующей этому распределению функцией плотности

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}},$$

то сдвиг μ эксцесса этой функции от нормативной температуры $t_{\text{н}}{}^{\circ}\text{C}$ в пределах $0^{\circ}\text{C}<\mu\le t_{\max}{}^{\circ}\text{C}-t_{\text{н}}{}^{\circ}\text{C}$ определяется, очевидно, загрузкой $K_{\text{з}}$ процессора и перепадами (сезонными и суточными) температуры $t_{0^{\circ}\text{C}}$ окружающей среды: $\mu=f\left(K_{\text{з}},t_{0^{\circ}\text{C}}\right)$, а стандартное отклонение σ – качеством алгоритмов выравнивания нагрузки, трудоемкостью и рангом решаемых на ВС задач и т.п. Несомненно при этом, что увеличение загрузки существенно увеличивает (в сравнении с $\mu=0^{\circ}\text{C}$) средние значения эквивалентного времени эксплуатации и интенсивности отказов каждой из составляющих систему ЭМ при соответствующем снижении среднего времени наработки до отказа.

В обеспечение данной модели инструментальными средствами анализа отказоустойчивости в работе [11, с. 147] введено формальное определение толерантности графа как степени сохранения определенных предикатом свойств в множестве подграфов, получаемых при элиминации заданного числа его элементов. С помощью этого определения формализованы понятия свойств и показателей структурной отказоустойчивости, структурной живучести и структурной надежности системы и ее функциональных подсистем, показаны взаимосвязи этих показателей и их различия в полномочности. Эффективность реализации предложенной модели в значительной степени определяется эффективностью аппарата исследования графов, что связано с переборным характером большинства решаемых при этом задач. В основе решения таких задач лежит работа со структурными описаниями [12, с. 168; 13, с. 696], содержащими в явном виде не только информацию, достаточную для построения графа системы, но и некоторую информацию о свойствах этого графа, что исключает необходимость полного перебора при сопоставлении структур при изначальной организации функциональных подсистем и их реконфигурации при выявлении отказавших элементов.

Предложенная выше формальная модель является обобщенной как в смысле учета ею утилитарных качеств (функциональности) системы и адекватности этим качествам реализующей их среды (структурного и конфигурационного соответствия), так и в смысле применимости ее к исследованиям отказоустойчивости системы, деградирующей при воздействии на нее потока отказов произвольного происхождения (случайных и детерминированных) с любыми законами и параметрами распределения. Границы применимости любой модели определяются широтой охватываемого ею пространства и

наличием эффективных инструментальных средств. В связи с этим отметим, что, несмотря на универсальность и возможности описания предложенной моделью самых общих случаев и подходов, она не исключает детализации важных для исследователя аспектов посредством абстрагирования от несущественной в таких случаях специфики (например, от некоторых архитектурных особенностей, конфигурации технических средств, структуры связей и протоколов взаимодействия, характеристик потока отказов элементов системы). Это позволяет при необходимости искусственно сузить рамки, выделяя в вероятностном пространстве возможных состояний системы только исследуемые.

4. Заключение

В работе показана неправомочность использования экспоненциальной модели для оценки надежности ЭМ и недостоверность основанной на ней модели надежности вычислительной системы. Увеличение степени интеграции составляющих ЭМ компонентов и связанное с этим уменьшение их числа препятствует использованию закона больших чисел в представлении потока отказов, воздействующего на ограниченное множество элементов, пуассоновской моделью. Неадекватность экспоненциальной модели надежности ЭМ, обусловлена также нестационарностью потока и наличием корреляционной зависимости показателей надежности элементов от режимов и времени предшествующей их эксплуатации. Нестационарность потока отказов подтверждена многочисленными теоретическими и практическими исследованиями и обусловлена необратимостью накапливаемых с течением времени деградационных процессов. Изменения скорости этих процессов от режимов эксплуатации ИМС, составляющих основу элементарных машин вычислительной системы, подтверждается стандартизацией использования форсированных режимов в практике определения показателей надежности интегральных микросхем. Случайный характер поступающих в систему заданий, их трудоемкость и требуемая ресурсоемкость, эффективность используемых в системе средств распределения нагрузки по элементам, наличие сезонных (суточных) изменений температурного фона, – все это определяет нестационарность температурных режимов работы ЭМ и, как следствие, нестационарность и зависимость потока отказов от предыстории эксплуатации системы и ее элементов.

Показано, что текущие значения интенсивности отказов и времени наработки до первого отказа элементов системы определяются не текущим временем их эксплуатации, а полным, приведенным к нормативным их температурным режимам, временем. Это время существенно превышает текущее значение времени эксплуатации элемента и масштабировано коэффициентом ускорения деградационных процессов, определяемым интегралом от произведения функций форсирования и плотности вероятности распределения рабочих температур. Показано, что сдвиг функции плотности вероятности распределения рабочих температур коррелирован загруженностью системы в целом и эффективностью используемых в ней средств распределения нагрузки, что очевидным образом определяет ухудшение показателей надежности элементов системы с ростом ее загруженности и эффективности использования. Вскрыта необходимость разработки моделей надежности вычислительной системы и входящих в ее состав ЭМ в соответствии с предложенным в работе подходом.

Представленная в работе формальная модель отказоустойчивой системы впервые объединяет функциональную и структурную ее компоненты с условиями взаимной адекватности этих компонент в потоке отказов произвольного происхождения. Отсутствие в модели ограничений на используемые при построении систем структуры, на законы и параметры распределения отказов или их совокупностей определяет обобщенный характер предложенной модели. Границы применимости любой модели определяются как возможностями описания самых общих случаев и подходов, так и возможностью

искусственного сужения рамок рассмотрения путем выделения в вероятностном пространстве возможных состояний системы только исследуемых состояний. В этом смысле предложенная модель является универсальной и позволяет детализировать важные для исследователя аспекты посредством абстрагирования от несущественной в некоторых случаях специфики (например, от некоторых архитектурных особенностей, конфигурации технических средств, структуры связей и протоколов взаимодействия, характеристик потока отказов элементов системы).

References:

1. Khoroshevskiy VG (2005) Arhitektura vyichislitelnyih sistem. Moscow, Izdatelstvo MGTU im. Baumana.
2. Melentiev VA (2008) Modelirovanie sistem, ustoychivyih k otkazam zadannoy kratnosti. Trudyi VII Mezhdunarodnoy konferentsii «Identifikatsiya sistem i zadachi upravleniya» SICPRO ‘08. Moscow, Institut problem upravleniya im. V.A. Trapeznikova RAN, pp.1210-1223.
3. Gorlov MI, Strogonov AV (2000) Gerontologiya kremnievyih integralnyih shem. ChipNews. No.3, Ch. 1, pp. 22-25.
4. Wendy Torell. Victor Avelar Mean Time Between Failure: Explanation and Standards. White Paper No. 78 American Power Conversion Corp. Available: http://www.apcmedia.com/salestools/VAVR-5WGTSB_R0_EN.pdf
5. Romanov V (2005) Kolichestvennaya otsenka nadezhnosti integralnyh mikroshem s uchetom matematicheskoy modeli otkazov. Nadezhnost i kontrol kachestva, No. 4, pp. 4-7.
6. Azarskov VN, Strelnikov VP (2004) Nadezhnost sistem upravleniya i avtomatiki. Uchebnoe posobie. K.: NAU.
7. Strelnikov VP (2004) Otsenka resursa izdeliy elektronnoy tehniki. MatematichnI mashini I sistemi, No. 2, pp. 186-195.
8. Feduhin AV (2005) Otsenka i issledovanie kazhuscheysya energii aktivatsii izdeliy elektronnoy tehniki. "Sistemotehnika", MIEM, No. 3. Setevoy elektronnyiy nauchnyiy zhurnal. Available: http://systech.miem.edu.ru/uslov.html.
9. Strogonov A (2002) Dolgovechnost integralnyih shem i proizvodstvennyie metodyi ee prognozirovaniya. ChipNews, No.6, pp. 44-49.
10. Melentiev VA (2004) Novyiy podhod k modelirovaniyu otkazoustoychivyih sistem. Avtometriya, No.4, pp. 88-105.
11. Melentiev VA (2004) Tolerantnost grafov i strukturnaya otkazoustoychivost vyichislitelnyih sistem. Vestnik Tomskogo gosudarstvennogo universiteta, ser. "Matematika, kibernetika, informatika", No.9(I), pp. 144-150.
12. Melentiev VA (2005) Formalnyiy podhod k issledovaniyu struktur vyichislitelnyih sistem. Vestnik Tomskogo gosudarstvennogo universiteta, ser. "Matematika, kibernetika, informatika", No.14, pp. 167-172.
13. Melentiev VA (2004) Formalnyie osnovyi skobochnyih obrazov v teorii grafov. II Mezhdunarodnaya konferentsiya "Parallelnyie vychisleniya i zadachi upravleniya", PACO 2004, 4-6 oct 2004, Institut problem upravleniya im. V.A. Trapeznikova RAN. Trudyi konferentsii. Moscow, pp. 694-706.