Надежность, том 18, №4, 2018
Оригинальная статья
DOI: 10.21683/1729-2646-2018-18-4-3-9

Адаптивная гарантоспособность информационных систем управления

Игорь Б. Шубинский, *АО «НИИАС», Москва, Россия*
Алексей М. Замышляев, *АО «НИИАС», Москва, Россия*
Любиша Р. Папич, *Исследовательский центр по управлению качеством и надежностью (DQM), Приевор, Сербия*

Игорь Б. Шубинский

Алексей М. Замышляев

Любиша Р. Папич

Резюме. *В статье рассматривается надежность информационной системы управления с позиции способности предоставлять требуемые услуги, которым можно оправданно доверять, т.е. ее гарантоспособность. Предполагается, что система функционирует без участия операторов. Задача состоит в обеспечении гарантоспособности мультимодульной системы управления в условиях воздействия на результаты решения задач отказов, сбоев и ошибок в решении задач вычислительными модулями (ВМ) системы. Применение традиционных методов обеспечения отказоустойчивости не обеспечивает желаемого эффекта, поскольку даже при бесконечной структурной избыточности, но при реальных возможностях оперативного обнаружения отказов или сбоев ВМ, гарантоспособность системы значительно ниже ожидаемой. В статье предложены и оценены способы адаптивной гарантоспособности. Назначение их состоит в реализации наблюдаемости систем управления при ограниченных возможностях контроля работоспособности составных ВМ и в достижения требуемых уровней гарантоспособности информационных систем управления в условиях незначительного резерва времени и структурной избыточности. Эти цели достигаются путем активного (и автоматического) переназначения имеющихся вычислительных ресурсов для оперативной обработки информации. Способы адаптивной грантоспособности позволяют без остановки вычислительных процессов при решении реальных задач осуществлять своевременное автоматическое обнаружение и устранение отказов, сбоев ВМ и ошибок в решении предусмотренных задач путем оперативной локализации неисправных модулей и последующей автоматической реконфигурации системы с выводом из процесса функционирования отказавших модулей.*

Ключевые слова: *вычислительные модули, гарантоспособность, адаптивная защита, отказы, сбои, ошибки в решении предусмотренных задач, автоматическая реконфигурация системы, контроль, допустимое время перерыва в работе, временная избыточность, циклы и такты защиты.*

Формат цитирования: *Шубинский И.Б., Замышляев А.М., Папич Л.Р. Адаптивная гарантоспособность информационных систем управления // Надежность. 2018. Т. 18, № 4. С. 3-9. DOI: 10.21683/1729-2646-2018-18-4-3-9*

1. Введение

1.1. Гарантоспособность информационных систем управления

Обеспечение надежности информационной техники находится в центре внимания всех специалистов, кто напрямую или косвенно связан с ее разработкой, производством и эксплуатацией. За все годы развития цифровой техники интенсивность отказов элементной базы уменьшилась на шесть порядков. В составе информационной системы тысячи таких цифровых элементов, каждый из которых представляет собой программно-аппаратные устройства, выполняющее множество различных функций.

Теперь уже центральной проблемой обеспечения надежности информационной системы становится безошибочное выполнение предусмотренных в системе функциональных задач, которые технически реализуются с помощью информационных процессов. Актуальность этой проблемы обусловлена тем, что частота ошибок в работе информационной системы и связанных с ними функциональных отказов значительно превышает частоту отказов цифровой техники, а сами функциональные отказы могут быть критичными для окружающей среды и объектов управления [1, 2 и др.].

В связи с этим ряд исследователей исходят из того, что необходимо изучать надежность выполнения информационных технологий как способность информационной системы поставлять обслуживание, которому можно доверять. *Обслуживание,* поставляемое системой, представляет ее свойства или поведение в том виде, в котором это воспринимается *пользователем*. В трактовке авторов данной работы обслуживание, которому можно доверять, расценивается как *общая надежность* [3].

В указанной работе [3] применены следующие понятия:

правильное или корректное обслуживание осуществляется, когда обслуживание реализует функцию (функции) системы;

отказ системы – событие отклонения осуществляемого обслуживания от правильного обслуживания, т.е.

отказ – это переход от правильного обслуживания к *неправильному обслуживанию*, когда не осуществляется функция системы.

Развитие данного подхода нашло отражение в материалах исследований рабочей группы WG 10.4 Международной Федерации (IFIP WG-10.4) по обработке информации [4]. Однако вместо термина «общая надежность» специалисты этой рабочей группы вводят термин *«гарантоспособность»*, которая в указанной работе рассматривается как «достоверность вычислительной системы, способной предоставлять требуемые услуги, которым можно *оправданно* доверять». Услуга – вид деятельности, работ, в процессе которых не создается новый материально-вещественный продукт, но изменяется качество уже имеющегося ранее созданного продукта. Само оказание услуги создает желаемый результат [5]. В явном виде гарантоспособность – это свойство *обслуживания* и зависит от характера использования системы.

1.2. Ограниченные возможности традиционных методов обеспечения гарантоспособности систем управления

Обслуживание пользователя с заданным уровнем гарантии качества осуществляется с помощью технической системы и представляет собой действие, процесс, необходимые для реализации функции по оказанию данной услуги. Здесь подразумевается сочетание аппаратной части, программного обеспечения и человека-оператора информационной системы. В дальнейшем полагаем, что система управления автоматически без участия человека-оператора выполняет заданные функции. Следовательно, для обеспечения высокого уровня гарантоспособности системы необходимо предварительно добиться еще более высокого уровня надежности и аппаратуры (изделия) и составных программных средств. Продукция (изделие) – это предмет или набор предметов, изготовляемых на предприятии. Классическая (структурная) теория надежности исследовала процессы отказов и восстановлений *продукции* (системы, элемента). В работах [1, 6] показано, что даже при сколь угодно большой избыточности не представляется возможным достичь высокого уровня надежности изделий. Исследована модель надежности резервированного объекта с раздельным резервированием в составе одного основного и бесконечного количества резервных однотипных устройств. Приняты следующие предпосылки:

• Время жизни компонентов имеет случайный характер и описывается распределением срока службы, которое удовлетворяет условиям:

- времена выхода из строя каждого из резервированных компонентов статистически не зависят друг от друга;

- у всех резервированных компонентов одинаковое экспоненциальное распределение срока службы компонентов непрерывно, дифференцируемо, и имеет ограниченное среднее.

• Система этих случайных величин представляет собой простой процесс восстановления.

• Средства контроля и коммутации на резервные устройства идеально надежны.

• Время переключения на резерв пренебрежимо мало.

При данных предпосылках предельная вероятность безотказной работы резервированной группы определяется в виде $P_{\Pi}(t) \le \sum_{n=0}^{\infty} P(n,t) \cdot \gamma^n$, где $P(n,t)$ – распределение результирующего числа интервалов времени между заменами отказавшего устройства данного объекта, который до момента отказа выполнял функции основного элемента; $\gamma = P\{\nu \le \tau_{д}\} = \int_0^{\tau_{д}} f_{\nu}(t)dt = F_{\nu}(\tau_{д})$ – вероятность правильного и своевременного обнаружения отказа и переключения на резерв, ν – случайное время существования отказа устройства, $\tau_{д}$ – допустимое время перерыва в работе системы (для систем управления это время сопоставимо с длительностью цикла управления); $f_{\nu}(t)$ – функция плотности времени существования отказа в системе.

При указанных предпосылках в работе [7] установлено, что среднее время до отказа резервированного объекта с раздельным резервированием в составе одного основного и бесконечного количества резервных однотипных устройств не превышает уровня, определяемого формулой (1) в предположении простейшего потока отказов или сбоев устройств

$$T_{СП} \le 1/\lambda(1-\gamma) \qquad (1)$$

где λ – интенсивность отказов одного устройства.

В работе [7] установлено, что можно ожидать повышения средней наработки до отказа исходного устройства за счет многократного резервирования с восстановлением не более чем в 2…10 раз даже при очень высокой вероятности правильного и своевременного обнаружения отказа и переключения на резерв $0{,}8 < \gamma \le 0{,}9$.

Если учесть, что программное обеспечение системы управления также реализуется с отказами и чаще с ошибками [8, 9, 10 и др.], то рассчитывать на достижение высокого уровня гарантоспособности системы за счет традиционных методов не приходится даже при очень больших затратах на введение в систему избыточности.

2. Постановка задачи адаптивной гарантоспособности

Требуется обеспечить заданный высокий уровень гарантоспособности информационной системы управления ***без введения больших объемов*** структурной, временной, функциональной и т.д. избыточности, на основе:

- управления гарантоспособностью по результатам оценки ***правильности*** выполнения в системе предусмотренных задач системы, а не по частоте отказов и интенсивности восстановления после них;

- использования ***естественной*** временной избыточности, которая сохраняется во многих системах в пределах цикла управления;

- адаптации системы к ошибочным результатам выполнения предусмотренных задач с помощью динамической перестройки системы и обеспечения параллельного выполнения задач с потактным сравнением результатов;

- ***приоритетного*** обслуживания наиболее важных задач с целью обеспечения их более высокого уровня гарантоспособности.

Идеи и принципы адаптивной гарантоспособности имеют много общего с концепцией активной защиты (АЗ), которая изложена нами в работе [11]. Они кратко состоят в следующем:

- длительности всех циклов обработки информации разделяются на определенные постоянные или случайные интервалы времени, которые в дальнейшем будем называть тактами, в пределах каждого из которых реализуется предусмотренное множество программных модулей и формируются контрольные точки;

- все множество составных вычислительных модулей (ВМ) информационной системы подразделяется на два составных множества: вычислительная среда – множество, состоящее из m однотипных основных ВМ; защитная среда – множество из $k \le m$ однотипных ВМ избыточных относительно решаемых задач;

- динамическая реконфигурация модулей системы управления производится через такты для организации параллельной обработки информации;

- потактное виртуальное резервирование путем параллельного решения предусмотренных всех m задач на основных ВМ при наличии хотя бы одного исправного избыточного ВМ;

- минимальная конфигурация системы должно содержать не менее $m = 2$ основных и одного избыточного ВМ для выявления ошибочного результата в решаемой задаче, классификации неисправностей и обнаружения их местонахождения;

- синтез адаптивной гарантоспособности (АГ) основывается на выборе такого значения длительности τ такта, при котором в течение допустимого времени перерыва в работе ошибка в результате решения задачи должна с заданным уровнем гарантии быть выявлена и устранена путем локализации ВМ – источника ошибки и перекоммутации его с избыточным исправным ВМ.

3. Организация систем с адаптивной гарантоспособностью

Для практической реализации идей и способов организации АГ могут быть предложены различные дисциплины. В рамках данной статьи рассматриваются две дисциплины: ***Д1*** и ***Д2***.

Д1. Система с рестартом на один такт, содержащая m основных и один контролирующий ВМ, контроль неприоритетный, переназначение модулей не предусмотрено. В случае сбоя одного из пары ВМ выполняется повторный счет с прежними операндами. Совпадение результатов в очередном такте исключает возможность отказа модулей, сбой устранен, обновляется контрольная точка по задаче первого ВМ в i-ом цикле защиты. Если сбой ВМ обнаружен собственными средствами контроля, то естественно обновляется контрольная точка по данным первого основного ВМ. Случай отказа одного из пары ВМ обнаруживается с помощью рестарта на один такт АЗ. Если при решении одного и того же участка задачи в течение двух тактов результаты работы пары однотипных ВМ дважды не совпали, то контрольная точка не обновляется до выполнения совместной работы контролирующего ВМ с очередным основным (в данном примере третьим ВМ). В случае совпадения результатов работы этой последней пары принимается решение об отказе предыдущего основного ВМ (в данном примере второго), обновляется контрольная точка для второго ВМ по данным контролирующего модуля, который теперь выполняет функции второго основного ВМ. Если же в трех смежных тактах защиты результаты не совпали, то принимается решение об отказе контролирующего ВМ и система некоторое время в случае отсутствия исправного избыточного модуля может работать без защиты

Таким образом, относительно дисциплины ***Д1*** параметры A, b и x_y характеризуются следующим: количество тактов в цикле защиты $A = m$; количество тактов принятия решения об отказе или сбое основного ВМ $b = 2$; количество тактов, затрачиваемых на восстановление вычислительного процесса с последней контрольной точки $x_y \le m+2$.

Д2. Система с рестартом и переназначением ВМ, содержащая m основных и один контролирующий модуль. Организация обнаружения и устранения неисправностей такая же, как и в дисциплине ***Д1.*** *Переназначение ВМ* необходимо для сокращения цикла защиты в условиях, когда количество основных ВМ существенно больше числа избыточных модулей. Суть переназначения заключается в том, что в определенных тактах перераспределяются ВМ между вычислительной и защитной средами. За определенными модулями защитной среды на время такта закрепляются функции основных модулей и наоборот. В результате этого устраняется недостаток, присущий способам фиксации контролирующих ВМ, когда модули вычислительной среды контролируются значительно реже, чем модуль защитной среды. Действительно, во всех случаях фиксации модули защитной среды в пределах цикла АЗ участвуют во всех парах контролируемых ВМ, тогда как модули вычислительной среды – только в одной паре, либо несколько чаще, если в каждом такте защиты образуются две и более пары ВМ.

Таким образом, относительно дисциплины ***Д2*** параметры A, b и x_y следующие: $A = \mathrm{int}\left(\frac{m+1}{2}\right)$, $b = 2$, $x_y = \mathrm{int}\left(\frac{m+5}{2}\right)$.

Организация ***приоритетного контроля*** способности системы управления правильно решать предусмотренные задачи позволяет существенно повысить уровень ее гарантоспособности относительно приоритетных задач. Приоритетный контроль организуется на основе переназначения ВМ. Однако при этом преследуется другая цель. Если при переназначении модулей решалась задача уравнять частоту контролей основных и избыточных ВМ, то при приоритетном контроле решается задача увеличения частоты контролей наиболее значимых с точки зрения решаемых задач модулей.

Проиллюстрируем возможности построения систем с двумя отмеченными в качестве приоритетных модулями (таблица 1). Предполагается, что первый отмеченный модуль (нулевой приоритет) контролируется в цикле АЗ с заданной наибольшей частотой, второй (первый приоритет) – с повышенной частотой, но меньшей, чем модуль нулевого приоритета. Остальные ВМ в этой же системе контролируются с одинаковой, но пониженной относительно приоритетных модулей частотой. Пусть $m = 7$, $k = 1$ ($m + k = 8$), нулевой приоритет отводится модулю 2, а первый приоритет – модулю 5. Поставим условие, чтобы в цикле АГ модуль 2 контролировался в четырех тактах, модуль 5 – в двух тактах, а остальные модули 1, 3, 4, 6, 7 и 8 – в одном такте. Решение этой задачи приведено в таблице 1.

Получены следующие результаты. Цикл АГ равен $A = 6$ тактам, четыре раза переназначаются ВМ, модуль 2 контролируется в двух тактах из трех соседних, а модуль 5 контролируется через два такта. Длительность цикла АГ возросла по сравнению с равномерным переназначением ВМ в 1,5 раза, поскольку в том варианте длительность цикла равнялась бы $A = (m + k)/2k = 4$. Это естественно, так как сокращение интервалов времени между контролями одних ВМ возможно за счет увеличения времени между контролями неприоритетных ВМ. В решении таких задач АЗ должен быть применен разумный компромисс. Это в полной мере относится и к выбору способа фиксации или переназначения ВМ. В первом случае проще управление АГ, во втором случае короче цикл управления. Переназначение ВМ предпочтительнее при очень малых величинах допустимого времени перерыва в работе, хотя при этом несколько сложнее управление АГ. При менее жестких временах ограничениях следует стремиться к реализации АГ на основе фиксации контролирующих ВМ.

4. Эффективность способов адаптивной гарантоспособности систем управления

Эффективность адаптивной гарантоспособности оценивается с помощью показателя вероятности успешной адаптации информационной системы управления к отказам, сбоям, программным ошибкам. Успешная адаптация будет в том случае, если в результате действий, предусмотренных алгоритмами защиты, длительность существования указанных неисправностей меньше или равна допустимой величине, что позволяет устранить ошибочные результаты в управлении. Здесь под допустимой величиной подразумевается цикл управления, т.е. время, в течение которого обнаружение и устранение неисправности в системе не приведет к ошибочному очередному управлению. Поскольку время устранения для каждой дисциплины защиты составляет постоянное количество тактов АГ, то достаточно ограничиться сравнением длительности обнаружения неисправности с допустимым временем обнаружения.

Оценку эффективности адаптивной гарантоспособности проведем для следующих типовых условий организации защиты.

Задачи обработки информации разделены на равные части (такты) τ, причем длительность такта много меньше длительности задачи. Задачи решаются через случайные интервалы времени υ_2, однако длительности решения задач υ_1 много больше длительности пауз, т.е. $\upsilon_1 >> \upsilon_2$. Это позволяет разделить задачу на такты защиты (например, для общности – такты случайной длительности). Кроме того, учитывается, что допустимое время перерыва в работе системы – постоянная величина $\tau_д$. Предполагается, что отсутствуют одновременные отказы или сбои проверяемого в текущем такте рабочего и контролируемого ВМ. Длительность такта определяется длительностью выполнения в пределах такта группы функционально законченных программных модулей. Поскольку все ВМ, на которых выполняются программные модули, однотипны, то порядок распределения программных модулей по тактам работы ВМ является общим для всех ВМ. Это позволяет принять одинаковыми распределения $F_\upsilon(t)$ длительности тактов для всех ВМ.

Требуется установить вероятность успешной адаптации системы к отказам:

Таблица 1

Номер такта	Номера основных ВМ	Номер контролирующего ВМ	Пары контролируемых ВМ	Переназначаемые ВМ	Частота контролей ВМ		
					2	5	1, 3, 4, 6, 7, 8
1	1 8 3 4 5 6 7	2	**2**–7	8–2			
2	1 8 3 4 5 6 7	2	**2**–3	8–2			
3	1 2 3 4 5 6 7	8	8–**5**	-			
4	8 2 3 4 5 6 7	1	1–**2**	8–1	**4**	**2**	**1**
5	1 2 3 8 5 6 7	4	4–**2**	8–4			
6	1 2 3 4 8 6 7	5	**5**–6	8–5			

$$\beta = P\{\nu \le \tau_{Д} - t_{у}\} = \int_{0}^{\tau_{Д}-t_{у}} f_{\nu}(t)dt, \qquad (2)$$

где $f_{\nu}(t)$ – функция плотности времени ν существования скрытого отказа в системе.

Для нахождения функции плотности $f_{\nu}(t)$ и вероятности успешной адаптации к отказам β в целом используются следующие параметры:

• функции распределения и характеристики временных интервалов защиты – длительности тактов, допустимого времени перерыва в работе системы и времени устранения обнаруженного отказа ($\tau_{Д}$ и $t_{у}$ соответственно);

• параметры принятой дисциплины АЗ: $A, b, t, x_{у} = t_{у}/\tau$.

Время подключения контролирующего ВМ к очередному основному слагается из случайной длительности такта υ и времени ожидания ψ от момента завершения параллельной работы с предыдущим ВМ до момента начала следующего такта работы очередного ВМ. Причем, $\psi \le \upsilon$ и во время ожидания осуществляется загрузка памяти контролирующего ВМ командами и операндами очередного основного модуля.

Для нахождения функции плотности времени ν предварительно установим функцию плотности суммарного времени ψ + υ. В изображении Лапласа она имеет вид

$$f_{\xi}(s) = \phi_{\psi}(s) * f_{\upsilon}(s),$$

где $\phi_{\psi}(s)$ – изображение плотности распределения времени ожидания ψ, а $f_{\upsilon}(s)$ – изображение плотности распределения длительности такта АЗ.

Пусть от момента возникновения скрытого отказа ВМ до момента подключения к нему контролирующего ВМ прошло x тактов. Тогда условная вероятность того, что $x < X$, где $X = 0, 1, \ldots, A, \ldots$, может быть найдена с помощью соответствующего преобразования Лапласа

$$f_{x}(s) = [f_{\xi}(s)]^{x}.$$

Вследствие равновероятной возможности отказа любого из ВМ, которые не защищены в данном такте, можно полагать, что целочисленная случайная величина x равномерно распределена в диапазоне чисел 1, 2, …, A–1. Отсюда плотность распределения количества тактов существования неисправности в системе определяется с помощью выражения:

$$f(x) = \sum_{i=1}^{A-1} \frac{\delta(x-i)}{A-1}, \qquad (3)$$

где δ(x) есть дельта функция от параметра x.

Общая длительность существования отказа до его обнаружения представляет собой сумму времени x(υ+ψ) и времени b(υ+ψ) от момента обнаружения факта неисправности до локализации отказавшего ВМ в соответствии с выбранной дисциплиной АЗ.

Функция плотности случайной величины x(υ+ψ)=θ в изображении Лапласа представляется следующим образом по формуле полной вероятности:

$$f_{\theta}(s) = \sum_{i=1}^{A-1} \frac{1}{A-1} \left(f_{\xi}(s)\right)^{i}.$$

Функция плотности случайной величины $(x+b)\cdot(\upsilon+\psi)$ в изображении Лапласа вычисляется в виде

$$f_{\nu}(s) = f_{\theta}(s) * (f_{\upsilon}(s))^{b} = \frac{1}{A-1} \sum_{i=1}^{A-1} \left(f_{\xi}(s)\right)^{i+b} \qquad (4)$$

Следующий шаг в определении вероятности успешной адаптации к отказам системы с рассматриваемой организацией АЗ состоит в том, чтобы в полученном выше выражении раскрыть функцию $f_{\xi}(s)$, которая в изображении Лапласа есть функция плотности суммы длительности такта и времени задержки в подключении контролирующего ВМ к основному в пределах такта ($\xi = \upsilon + \psi \le 2\upsilon$).

Ориентируясь на экспериментальные данные [2], примем распределения случайных длительностей тактов υ в виде распределения Эрланга a-го порядка с функцией плотности $f_{\upsilon}(t) = \frac{\rho(\rho \cdot t)^{a}}{a!} e^{-\rho \cdot t}$, которые в изображении Лапласа имеют следующий вид:

$$f_{\upsilon}(s) = \left(\frac{\rho}{\rho + s}\right)^{a+1},$$

где ρ – параметр распределения Эрланга (количество событий в единицу времени).

Согласно работе [12] функция плотности времени ожидания ψ (в нашем случае время подключения контролирующего к основному) в изображении Лапласа имеет следующий вид:

$$\phi_{\psi}(s) = \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right].$$

Следовательно, в формуле (4) функция плотности $f_{\xi}(s)$ равна

$$f_{\xi}(s) = f_{\upsilon}(s) \cdot \phi_{\psi}(s) = \left(\frac{\rho}{\rho + s}\right)^{a+1} \cdot \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right].$$

Подставляя данное выражение в формулу (3.4), находим

$$f_{\nu}(s) = \frac{1}{A-1} \sum_{i=1}^{A-1} \left\{\left(\frac{\rho}{\rho + s}\right)^{a+1} \frac{\rho}{(a+1)s}\left[1 - \left(\frac{\rho}{\rho + s}\right)^{a+1}\right]\right\}^{i+b}.$$

Переходя от изображения к оригиналу при постоянной величине допустимого времени перерыва в работе и воспользовавшись формулой (3), определяем вероятность успешной адаптации системы с АГ к отказам

$$\beta = 1 - \frac{e^{-(a+1)\cdot x_{Д}^{*}}}{A-1} \sum_{i=1}^{A-1} \left(\frac{1}{a+1}\right)^{i+b} \sum_{|\bar{n}|=i+b} \frac{(i+b)!}{\bar{n}!} \cdot \sum_{k=0}^{\eta} \frac{\left((a+1)x_{Д}^{*}\right)^{k}}{k!}, \qquad (5)$$

где $\bar{n}! = n_0! n_1! \ldots \cdot n_a!$; $|\bar{n}| = n_0 + n_1 + \ldots + n_a$; $x_{Д}^{*} = \tau_{Д}^{*}/\tau$; $t_{Д}^{*} = \tau_{Д} - t_{у}$;

$$\eta = (a+2)(i+b) + \sum_{j=1}^{a} j n_j + 1.$$

В частном случае $a = 0$ (экспоненциальное распределение длительности такта) имеет место следующее выражение вероятности успешной адаптации системы к отказам $\beta = 1 - \frac{e^{-x_д^*}}{\_A-1} \sum_{i=1}^{A-1} \sum_{k=0}^{2(i+b)+1} \frac{(x_д^*)^k}{k!}$, поскольку в этом случае $\bar{n}! = 1$, а $|n| = 0$.

С помощью выражения (5) проанализируем зависимости вероятности успешной адаптации системы с АЗ от допустимого количества тактов перерыва в работе, числа m основных модулей и применительно к рассмотренным ранее дисциплинам ***Д1*** и ***Д2***.

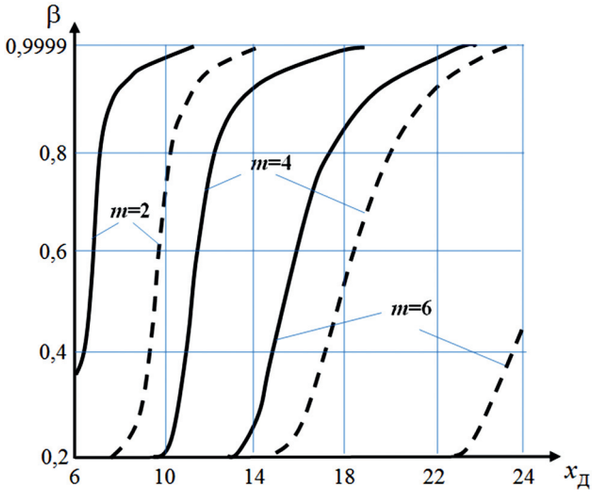

Рисунок 1 – Зависимости вероятности успешной адаптации системы со случайными тактами защиты к отказам в зависимости от допустимого количества $x_д$ тактов защиты и от числа m основных ВМ

На рисунке 1 показаны зависимости $\beta = f(x_д)$ при $a \geq 2$ применительно к дисциплинам ***Д2*** (сплошные линии) и ***Д1*** (пунктирные линии). Начиная со второго порядка распределения Эрланга длительности такта и выше результаты этих зависимостей практически совпадают. Они свидетельствуют о том, что наибольшей скоростью адаптации к отказу ВМ обладают дисциплины, аналогичные ***Д2***. Эти дисциплины примерно на несколько тактов быстрее реагируют на ошибки в результатах решения задач, чем дисциплины класса ***Д1***. Преимущества отмеченных дисциплин повышаются по мере увеличения количества основных вычислительных модулей.

Вместе с тем, АГ со случайной длительностью тактов значительно инерционнее, чем АГ с тактами постоянной длительности. Так, даже при минимальном для АГ количестве основных модулей $m = 2$ время обнаружения и устранения отказа ВМ увеличивается в 1,5–2 раза. Поскольку для многих архитектур систем управления и вычислительных процессов в них не представляется возможным организовать АГ с постоянными тактами, то целесообразно изыскивать дополнительные возможности в повышении скорости адаптации систем с АГ к отказам составных ВМ. Такая возможность, например, имеет место при применении также встроенного контроля основных ВМ, с помощью которого в системах с АГ возможно оперативнее обнаруживать и устранять неисправности ВМ.

5. Заключение

Ограниченные возможности резервирования, средств оперативного обнаружения отказов, сбоев, ошибок в выполнении информационных процессов, ограниченные возможности комплекса «аппаратура – программы» – все это вызывает необходимость в развитии нестандартных технологий обеспечения гарантоспособности информационных систем управления. Одной из них является предложенная в статье технология адаптивной гарантоспособности. Суть ее состоит в активном использовании естественной временной и структурной избыточности и в активном (и автоматическом) переназначении имеющихся вычислительных ресурсов не только для оперативной обработки информации, но и для реализации наблюдаемости системы при ограниченных средствах контроля. Адаптивная гарантоспособность предназначена для достижения требуемых уровней гарантоспособности информационных систем управления в условиях незначительного резерва времени, ограниченной эффективности средств обнаружения неисправностей составных вычислительных модулей, а также при условии, что объем избыточного оборудования не должен превышать объема основного оборудования. С помощью адаптивной защиты имеются реальные возможности добиться гораздо более высокого уровня гарантоспособности систем, чем с помощью традиционных методов резервирования. Технология адаптивной гарантоспособности позволяет в ограниченных временных условиях при решении реальных задач осуществлять своевременное автоматическое обнаружение и устранение отказов и сбойных ошибок путем оперативной локализации неисправных вычислительных модулей и последующей автоматической реконфигурации системы с выводом из процесса функционирования отказавших модулей. Вместе с тем, эта технология ориентирована на мультимодульные системы и недостаточно проработана для средств хранения и отображения информации, документирования, средств энергообеспечения информационных систем управления.

Библиографический список

1. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза [Текст] – М.: «Журнал Надежность», 2016. – 545с.

2. Кирпичников А.П., Васильев С.Н. Особенности современной микроэлектроники и вопросы построения систем управления высокой надежности и безопасности // Надежность (Dependability). – 2017. – Том 17, №3. – С. 10-16.

3. Avizienis A., Laprie J-C. and Randell B. Dependability of computer systems/ Fundamental concepts, terminology and examples. Technical report, LAAS – CNRS, October, 2000.

4. Rus I., Komi-Sirvio S., Costa P. Computer program with insurance of high reliability. Technical report, IFIP WG-10.4, March, 2008.

5. Борисов А.Б. Большой экономический словарь. – М.: Книжный мир, 2003. – 895 с.

6. Шебе Х., Шубинский И.Б. Предельная надежность структурного резервирования // Надежность (Dependability). – 2016. – Том 16, № 1. – С. 3-13.

7. Шубинский И.Б. Методы обеспечения функциональной надежности программ // Надежность (Dependability). – 2014. – № 4. – С. 87-101.

8. Потапов И.В. Проблематика в области надежности программных систем // Надежность (Dependability). – 2015. – № 1. – С. 57-61.

9. Шубинский И.Б., Шебе Х. Систематический подход к защите программного обеспечения от сбоев аппаратуры // Надежность (Dependability). – 2014. – №3. – С. 96-106.

10. Shubinsky I.B., Sheabe X. On the definition of functional reliability, Proceedings of the ESREL 2013, Safety, Reliability and Risk Analysis: Beyond the Horizon – Steenbergen et al. (Eds) 2014 Taylor & Francis Group, London, ISBN 978-1-138-00123-7, pp. 3021-3027.

11. Shubinskiy I.B. Adaptive fault tolerance in real-time information systems, Life Cycle Engineering and Management, ICDQM-2016, Prijevor, Serbia, 29-30 June 2016, pp. 3-14.

12. Гнеденко Б.В. Введение в теорию массового обслуживания [Текст] / Б.В. Гнеденко, И.Н. Коваленко. – Киев: Наука, 1963.

Сведения об авторах

Игорь Б. Шубинский – доктор технических наук, профессор, заместитель руководителя НТК АО «НИИАС», Москва, Россия, тел. +7 (495) 786-68-57, e-mail: igor-shubinsky@yandex.ru

Алексей М. Замышляев – доктор технических наук, заместитель Генерального директора АО «НИИАС», Москва, Россия, тел. +7 (495) 967-77-02, e-mail: A.Zamyshlaev@vniias.ru

Любиша Р. Папич – доктор технических наук, профессор, директор Исследовательского центра по управлению качеством и надёжностью (DQM), Приевор, Сербия

Поступила: 26.08.2018