УДК 681.3(075)

А. Н. Буточнов[1], В. В. Августовский[1], В. Н. Цыцарев[2]
[1]Институт проблем регистрации информации НАН Украины
ул. Н. Шпака, 2, 03113 Киев, Украина
[2]Национальный университет им. Т. Шевченко

Оценка надежности многофункциональных программно-технических комплексов

Предложены методика и алгоритмы расчета приближенных значений показателей надежности (средней наработки на отказ и среднего времени восстановления) многофункциональных программно-технических комплексов, позволяющие учесть как отказы технических устройств, так и отказы, порождаемые ошибками в программах.

Ключевые слова: *надежность, показатели надежности, методики расчета, многофункциональные системы, высоконадежные системы, программные ошибки.*

Постановка задачи

В настоящее время для решения задач управления в различных предметных областях широко применяются информационные и информационно-управляющие системы (ИС), выполняющие множество различных функций по сбору, обработке, передаче и отображению информации в режиме реального времени. Основой таких систем является программно-технический комплекс (ПТК), который представляет собой сложную вычислительную систему, являющуюся объединением комплекса технических средств (КТС) и программного обеспечения (ПО), реализующих все функции ИС.

Обычно различают два вида ПО: *системное и прикладное*. К *системному ПО* относятся операционные системы, СУБД, драйверы, обеспечивающие работу устройств, и др. *Прикладное ПО* — это множество программ, решающих функциональные задачи системы. В статье рассматривается только прикладное ПО, так как вероятность ошибки прикладного ПО из-за его недостаточного тестирования значительно выше, чем вероятность ошибки системного ПО.

КТС включает в себя множество технических устройств (ТУ), как правило, объединенных общей локальной вычислительной сетью, обеспечивающих решение функциональных задач системы. Элементами КТС являются компьютеры различного назначения (серверы, рабочие станции), хранилища информации, источ-

© А. Н. Буточнов, В. В. Августовский, В. Н. Цыцарев

ники бесперебойного питания, принтеры, плоттеры, сканеры, информационные доски, модемы, маршрутизаторы, коммутаторы, кабельные соединения и т.п.

В процессе функционирования ИС решается (одновременно или в определенной последовательности) несколько информационных задач, различных по важности, по требуемым ресурсам, по продолжительности решения. Каждую отдельную задачу, которая решается в данной ИС, будем называть *функцией* ИС. Потребность в выполнении тех или иных функций определяется внешней средой ИС — случайным потоком входных заявок на выполнение различных функций.

Функция может «отказать» (не выполняться) в момент поступления заявки, если в этот момент произойдет отказ ТУ, которое используется при выполнении функции, или в случае, если на вход программы, реализующей функцию, поступили данные, при которых проявилась скрытая ошибка в программе.

В данной статье предлагается методика оценки надежности многофункциональных ПТК с учетом возможных отказов ТУ и отказов, порождаемых ошибками в ПО. Рассматриваются основные подходы и алгоритмы расчета, на которых строится методика.

Формализация описания функциональной структуры ИС

Предполагается, что каждая функция ИС реализуется отдельной программой (процессом, потоком), которая может быть запущена или остановлена при вызове или завершении выполнения функции.

Все функции можно разделить на *внутренние* и *внешние* (выходные). *Внутренние функции* обеспечивают выполнение каких-либо других функций системы. *Внешние функции* определяют результат функционирования ИС, потребляемый конечным пользователем.

Связи между функциями понимаются в том смысле, что программа одной функции в качестве входных данных использует результаты, полученные в результате выполнения программы другой функции. В этом случае можно говорить, что одна функция обеспечивает выполнение другой функции. Такой подход позволяет ввести понятие функциональной структуры ИС.

Функциональную структуру ИС формально будем представлять графом $\boldsymbol{G} = \langle \boldsymbol{F}, \boldsymbol{V} \rangle$, где $\boldsymbol{F}$ — множество вершин графа, отождествляемых с отдельными функциями, а $\boldsymbol{V}$ — множество дуг, соединяющих вершины и указывающих направление связи. Предполагается, что циклы в графе отсутствуют. Структура программ определяется таким образом, что все реально существующие обратные связи (циклы) локализованы внутри одной программы.

Каждой дуге $\upsilon_{ij} = \langle f_i, f_j \rangle \in \boldsymbol{V}$ ставится в соответствие *коэффициент влияния* ν_{ij}, величина которого характеризует *силу влияния* функции f_i на функцию f_j ($f_i, f_j \in \boldsymbol{F}$), $\nu_{ij} \in (0, 1]$. Если $\nu_{ij} = 1$, то функция f_j может выполняться только при условии успешного выполнения функции f_i. При $\nu_{ij} = 0$ функция f_j не зависит от функции f_i, и это, по сути, эквивалентно тому, что соответствующая дуга υ_{ij} на графе $\boldsymbol{G}$ отсутствует.

При $0 < \nu_{ij} < 1$ функция f_j может в некоторых случаях выполняться независи-

мо от функции f_i. Величину v_{ij} можно интерпретировать как относительную долю случаев, когда отказ функции f_i приводит к отказу функции f_j. Величина v_{ij} может быть определена приближенно методом экспертных оценок. На рис. 1 показан пример графа ***G***.

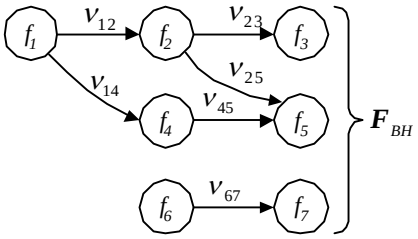


Рис. 1. Пример графа функциональной структуры ИС (граф ***G***)

Функции могут существенно различаться по их важности (по «вкладу», который они вносят в эффективность функционирования ИС). Степень важности функции f_i будем оценивать *коэффициентом относительной важности* w_i. Величину коэффициента w_i можно интерпретировать как относительный ущерб, который понесет система в случае отказа функции f_i. Для внешних функций ($f_i \in \boldsymbol{F}_{BH}$) значения w_i могут быть определены методом парных сравнений [1, 2], при этом значения w_i лежат в интервале [0, 1] и удовлетворяют условию $\sum_{f_i \in \boldsymbol{F}_{BH}} w_i = 1$.

Для всех остальных (внутренних) функций ($f_i \notin \boldsymbol{F}_{BH}$) коэффициенты относительной важности определяются по формуле:

$$w_i = \sum_{f_j \in \boldsymbol{F}_i} v_{ij} w_j \,, \qquad (1)$$

где $\boldsymbol{F}_i$ — множество функций, для которых функция f_i является непосредственно обеспечивающей ($f_k \in \boldsymbol{F}_i$, если существует дуга $\upsilon_{ik} = \langle f_i, f_k \rangle$).

Расчеты по формуле (1) начинаются с функций, непосредственно обеспечивающих выходные функции. Затем последовательно рассчитываются коэффициенты для всех остальных внутренних функций.

Формализация описания надежностной структуры КТС ИС

Надежностную структуру КТС ИС будем представлять структурной схемой надежности (ССН) [3, 4]. Для формализованного представления ССН будем использовать структуру данных — *дерево вложенности* ***D*** **= ⟨*S, R*⟩**, где ***S*** — множество вершин, каждая из которых представляет отдельный фрагмент общей ССН, а ***R*** — множество дуг, обозначающих переходы от элементов (фрагментов) ССН более высоких уровней к элементам более низких уровней вложенности.

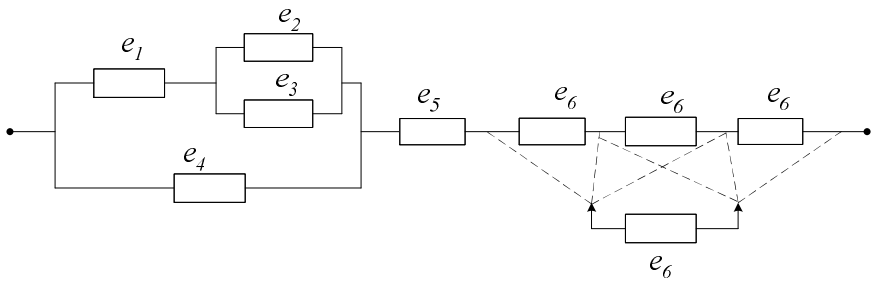
Каждую *i*-ю вершину *u*-го уровня вложенности будем представлять в виде:

$$s_i^u = \left\langle ts_i^u, P_i^u, M_i^u \right\rangle,$$

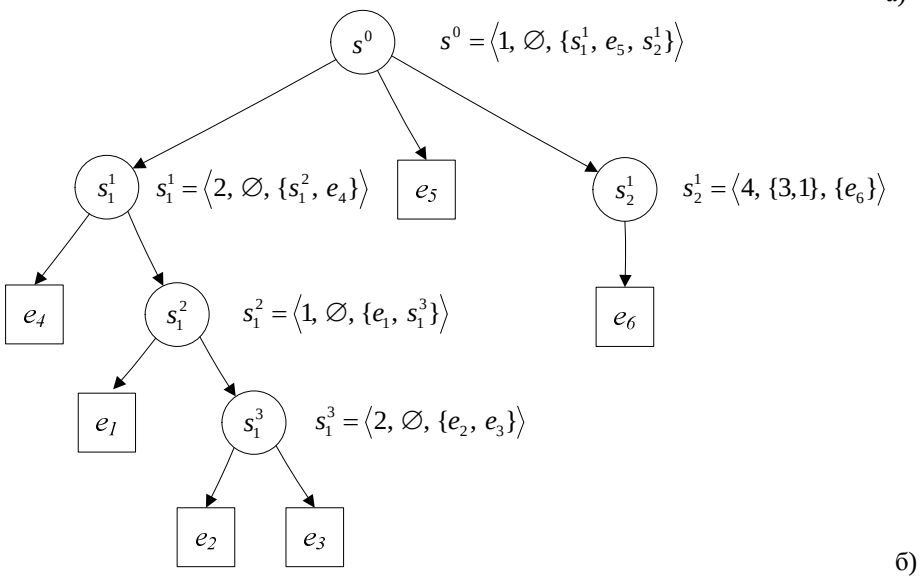
где ts_i^u — признак типа структуры, которая представляется вершиной s_i^u. Признак ts_i^u может принимать значения: 1 — последовательное соединение элементов; 2 — параллельное соединение; 3 — нагруженное резервирование (однотипные элементы); 4 — ненагруженное резервирование (однотипные элементы) и т.п.;

P_i^u — множество числовых параметров, характеризующих структуру s_i^u. Так, если $ts_i^u = 3$ или $ts_i^u = 4$, то $P_i^u = \{k, n\}$, где k — число основных элементов, а n — число резервных элементов в резервированной группе, которая задается структурой s_i^u. При $ts_i^u = 1$ или $ts_i^u = 2$ множество P_i^u пусто;

$M_i^u = \{s_j^{u+1}\}$ — множество структур (вершин) s_j^{u+1} уровня $(u + 1)$, являющихся элементами структуры s_i^u. Если s_i^u является структурой нижнего уровня, то элементами множества M_i^u являются комплектующие элементы КТС $e_j \in E$ (E — множество всех комплектующих элементов КТС). В этом случае $M_i^u = \{e_1, e_2, ...\}$. В общем случае множество M_i^u может включать как структуры $(u + 1)$-го уровня вложенности, так и комплектующие элементы $e_j \in E$, т.е. $M_i^u = \{s_1^{u+1}, s_2^{u+1}, ..., e_k, ...\}$. На рис. 2 приведен пример ССН КТС (рис. 2,а) и соответствующее ей дерево ***D*** (рис. 2,б) вложенности структур ***S***.



а)



б)

Рис. 2. Пример ССН КТС и дерева вложенности структур (дерево ***D***)

В данном примере структура s^0 представляется последовательным соединением (t_s = 1) элементов множества $M_1^1 = \{s_1^1, e_5, s_2^1\}$, в котором s_1^1 и s_2^1 — структуры уровня u = 1, e_5 — комплектующий элемент.

Структура s_1^1 является параллельным соединением (t_s = 2) двух элементов: комплектующего элемента e_4 и структуры s_1^2. Структура s_1^2 является последовательным соединением (t_s = 1) элемента e_1 и структуры s_1^3. Структура s_1^3 представляет собой параллельное соединение элементов e_2 и e_3.

Структура s_2^1 — это резервированная группа, состоящая из трех последовательно соединенных однотипных элементов e_6 и одного резервного элемента того же типа (скользящий резерв).

Дерево вложенности ***D*** является удобным формализмом, используемым в алгоритмах расчета показателей надежности КТС.

Расчет показателей надежности КТС с учетом отказов технических устройств

В качестве базовых показателей надежности в методике приняты: T_0 — средняя наработка на отказ и T_B — среднее время восстановления. При расчетах базовых показателей принимаются следующие основные допущения:

— все отказы считаются независимыми;

— закон распределения времени между отказами элементов и закон распределения времени восстановления экспоненциальный.

С учетом того, что современные ТУ (элементы КТС) ИС имеют весьма высокий уровень безотказности, принятые допущения можно считать вполне приемлемыми. При получении результирующих оценок ПН они не приводят к большим ошибкам.

Исходной информацией для расчетов является:

— ССН КТС (или части КТС), представленная соответствующим деревом вложенности ***D***;

— данные о показателях надежности ТУ, накапливаемые в базе данных.

Значения показателей надежности T_{0i}^u и T_{Bi}^u для *i*-й подструктуры *u*-го уровня вложенности вычисляются с помощью процедуры $PN(s_i^u, T_{0i}^u, T_{Bi}^u)$, параметрами которой являются:

s_i^u — *i*-я подструктура (ССН) *u*-го уровня вложенности (вершина дерева ***D***);

T_{0i}^u и T_{Bi}^u — результаты, возвращаемые процедурой — показатели надежности части КТС, представленной структурой s_i^u.

Если в качестве параметра s_i^u задать корневую вершину дерева s^0, то в качестве результата процедура *PN* вернет значения T_0 и T_B для КТС в целом.

Вычисления показателей надежности производятся по известным формулам [3, 4]:

при $ts_i = 1$ (последовательное соединение):

$$T_{0i}^{u} = \left(\sum_{j} \frac{1}{T_{0ij}^{u+1}} \right)^{-1}, \; T_{Bi}^{u} = T_{0i}^{u} \sum_{j} \frac{T_{Bij}^{u+1}}{T_{0ij}^{u+1}}; \tag{2}$$

при $ts_i = 2$ (параллельное соединение):

$$T_{0i}^{u} = \left(\sum_{j} \frac{1}{T_{Bij}^{u+1}} \cdot \prod_{j} \frac{T_{Bij}^{u+1}}{T_{0ij}^{u+1}} \right)^{-1}, \; T_{Bi}^{u} = \left(\sum_{j} \frac{1}{T_{Bij}^{u+1}} \right)^{-1}, \tag{3}$$

где T_{0ij}^{u+1} и T_{Bij}^{u+1} — ПН j-го элемента $m_{ij} \in M_i^u$ (M_i^u — множество элементов, образующих структуру s_i^u). Индекс j принимает последовательные значения номеров элементов (комплектующих или подструктур, входящих в M_i^u);

при $ts_i = 3$ (скользящий нагруженный резерв):

$$T_{0i}^{u} = \left[\frac{k \cdot C_{n+k}^{k}}{T_{0i1}^{u+1}} \left(\frac{T_{Bi1}^{u+1}}{T_{0i1}^{u+1}} \right)^{n} \right]^{-1}, \; T_{Bi}^{u} = \left(\frac{n+1}{T_{Bi1}^{u+1}} \right)^{-1}; \tag{4}$$

при $ts_i = 4$ (скользящий ненагруженный резерв):

$$T_{0i}^{u} = \frac{n \cdot T_{0i1}^{u+1}}{k} \left(k \cdot \frac{T_{Bi1}^{u+1}}{T_{0i1}^{u+1}} \right)^{-n}; \; T_{Bi}^{u} = \left(\frac{n+1}{T_{Bi1}^{u+1}} \right)^{-1}, \tag{5}$$

где T_{0i1}^{u+1} и T_{Bi1}^{u+1} — показатели надежности элементов, входящих в резервированную группу, представленную структурой s_i^u (все элементы однотипные); k и n — число основных (соединенных последовательно) и резервных элементов в структуре s_i^u; C_{n+k}^{n} — число сочетаний из $n + k$ по k.

На рис. 3 представлена структурная схема алгоритма процедуры *PN*. Процедура реализует вычисление показателей надежности по формулам (2)–(5) для структуры s_i^u. Операторы 2, 3 и 9 образуют цикл, в котором производится перебор элементов множества M_i^u, входящих в структуру s_i^u. Если элемент является структурой s_j^{u+1} следующего (u + 1)-го уровня, то ПН T_{0ij}^{u+1} и T_{Bij}^{u+1} для нее определяются путем рекурсивного вызова процедуры *PN* (оператор 6). Если элемент является комплектующим элементом, то значения T_{0ij}^{u+1} и T_{Bij}^{u+1} определяются по информации о показателях надежности этого элемента (оператор 5).

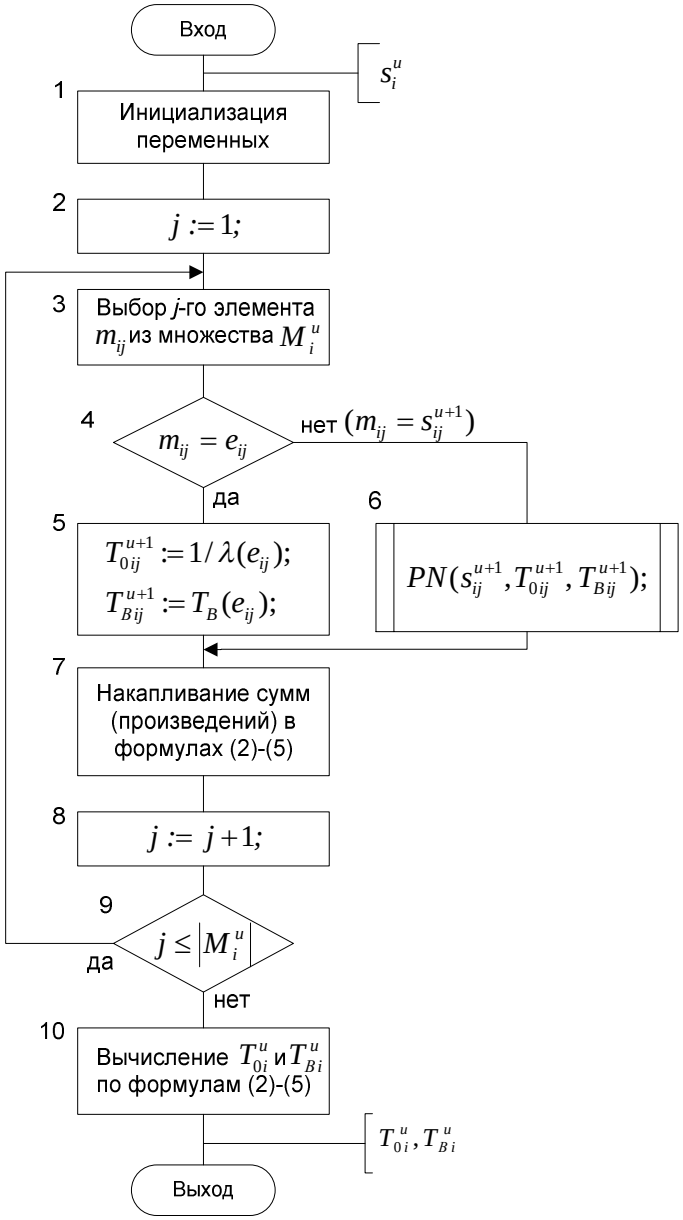


Рис. 3. Структурная схема алгоритма процедуры $PN(s_i^u, T_{0i}, T_{Bi})$

Расчет показателей надежности отдельной функции с учетом ошибок в программах

Успешное выполнение той или иной функции обеспечивается правильным исполнением программ, реализующих данную функцию. Отказ функции может произойти в том случае, если откажет какое-либо ТУ, используемое при исполнении программ функции, или в случае, если проявится ошибка в программе, которая ранее никогда не проявлялась (произойдет «отказ» программы).

С учетом допущения о том, что отказы ТУ и отказы программ являются независимыми и подчинены экспоненциальному закону распределения, интенсивность отказов *i*-й функции определим как сумму:

$$\lambda_i = \lambda_{КТС\,i} + \lambda_{ПО\,i}, \tag{6}$$

где $\lambda_{КТС\,i}$ и $\lambda_{ПО\,i}$ — интенсивности отказов соответственно части КТС, обеспечивающей выполнение программ *i*-й функции, и отказов, которые могут порождаться ошибками в этих программах.

Для определения $\lambda_{КТС\,i}$ строится ССН для *i*-й функции и соответствующее ей дерево вложенности $\boldsymbol{D}_i$, а затем используется рассмотренный выше алгоритм (процедура *PN*).

Известно, что отказы ПО имеют совершенно иную природу, чем отказы ТУ. Отказы ПО порождаются ошибками, оставшимися не устраненными после отладки программ, и могут проявляться (или не проявляться) на протяжении всего периода эксплуатации ПО. Не вдаваясь в проблемы и трудности, связанные с оценкой надежности ПО, воспользуемся упрощенной методикой, основанной на рекомендациях [5].

Согласно этой методике интенсивность отказов программ вычисляется по формуле:

$$\lambda_{ПО\,i} = \eta_{ПО\,i} \cdot P_{ПО\,i}, \tag{7}$$

где $\eta_{ПО\,i}$ — интенсивность вызовов программы, реализующей *i*-ю функцию, которая определяется как среднее число обращений к программе за некоторый малый промежуток времени, отнесенное к величине этого промежутка; $P_{ПО\,i}$ — вероятность того, что в программе *i*-й функции имеется ошибка, которая может проявиться в произвольный момент времени.

Для успешного выполнения отдельной *i*-й функции f_i в многофункциональном ПТК может потребоваться выполнение других, обеспечивающих ее функций (программ). Поэтому интенсивность $\lambda_{ПО\,i}$ должна вычисляться согласно выражению:

$$\lambda_{ПО\,i} = \eta_{ПО\,i} \cdot P_{ПО\,i} + \sum_{f_j \in \boldsymbol{F}_i^+} \lambda_{j/1,\ldots,j-1} \cdot \nu_{ji}, \tag{8}$$

где $\lambda_{j/1,\ldots,j-1}$ — условная интенсивность отказов функции f_j при условии, что функции $f_1, \ldots, f_{j-1}$ выполняются правильно; ν_{ji} — коэффициент влияния функции f_j на функцию f_i; $\boldsymbol{F}_i^+$ — множество функций, непосредственно обеспечивающих функцию f_i (все вершины, соответствующие функциям $f_j \in \boldsymbol{F}_i^+$, на графе $\boldsymbol{G}$ связаны дугами υ_{ji} с вершиной f_i).

На рис. 4 изображена структурная схема алгоритма процедуры-функции $LPO(f_i, s_i)$, которая в качестве основного результата возвращает значение интенсивности $\lambda_{ПО\,i}$, вычисленное согласно (8).

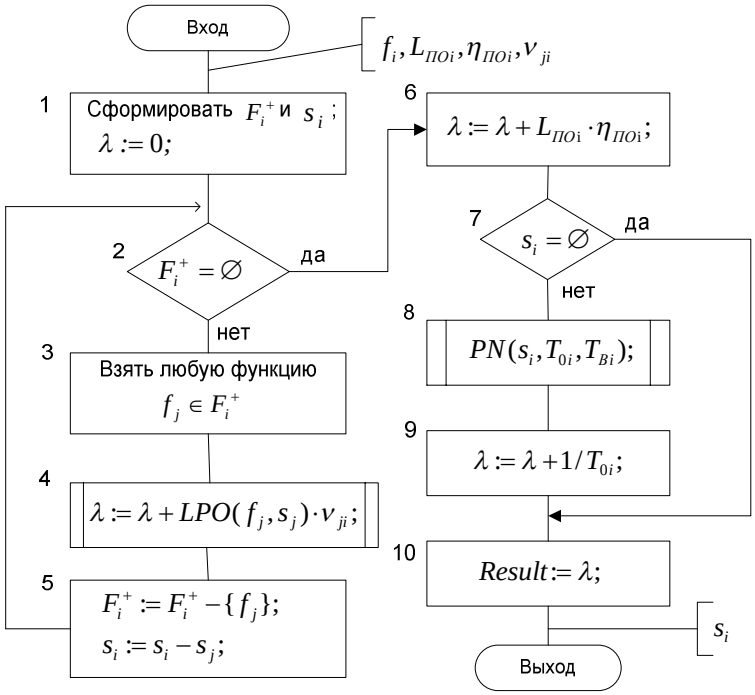


Рис. 4. Структурная схема алгоритма процедуры-функции $LPO(f_i, s_i)$

Кроме того, процедура возвращает (через параметр) указатель на структуру s_i, описывающую часть КТС, обеспечивающую выполнение функции f_i.

Работа алгоритма состоит в следующем. Оператор 1 выполняет подготовительные действия — создает и инициализирует используемые в процедуре вспомогательные объекты: F_i^+ — множество функций, выполнение которых является необходимым условием успешного выполнения функции f_i; s_i — структура, описывающая часть элементов КТС, которые участвуют в выполнении функции f_i; λ — переменная, в которой накапливается результирующее значение $\lambda_{ПО\,i}$.

Операторы 2, 3 и 5 образуют цикл, в котором производится последовательный выбор функций $f_j \in F_i^+$.

В операторе 4 вызывается (рекурсивно) функция *LPO* и ее результат суммируется в переменной λ. В качестве дополнительного результата функция *LPO* возвращает также указатель на объект s_j — структуру, описывающую часть элементов КТС, обеспечивающих выполнение функции f_j.

Оператор 5 выполняет следующие действия:

— из множества F_i^+ исключается функция, для которой уже проведены вычисления;

— из структуры s_i исключаются элементы КТС, надежность которых уже учтена при предыдущих расчетах.

После завершения цикла выполняется оператор 6, добавляющий в переменную λ составляющую интенсивности отказов, учитывающую программные ошиб-

ки. Если в структуре s_i остались элементы, отказы которых еще не учитывались, то выполняются операторы 8, 9. Оператор 8 вызывает процедуру *PN*, с помощью которой вычисляются показатели надежности части КТС, представленной структурой s_i. Оператор 9 добавляет в переменную λ составляющую интенсивности отказов элементов этой части КТС $\lambda_{KTCi}(s_i)$.

Накопленное значение интенсивности отказов λ оператор 10 присваивает переменной *Result* — возвращаемому значению функции *LPO*.

Результирующие значения средней наработки на отказ и среднего времени восстановления для функции f_i вычисляются по формулам:

$$T_{0i} = 1/\lambda_i,$$

$$T_{Bi} = (\lambda_{KTCi} \cdot T_{BKTCi} + \lambda_{ПОi} \cdot T_{BПОi}) / \lambda_i, \qquad (9)$$

где λ_{KTCi} и $\lambda_{ПОi}$ — составляющие интенсивности отказов функции f_i, входящие в (6); T_{BKTCi} — среднее время восстановления части КТС, обеспечивающей выполнение функции f_i (величина T_{BKTCi} получается с помощью процедуры *PN*); $T_{BПОi}$ — среднее время восстановления работоспособности функции f_i при программном отказе (это время обычно принимается равным времени перезагрузки сервера).

Расчет показателей надежности ПТК в целом

Поскольку ПТК — это многофункциональная система, трудным вопросом является определение понятия «отказ ПТК». Существуют различные подходы для решения этого вопроса, но их рассмотрение выходит за рамки данной статьи. Один из возможных подходов состоит в следующем.

На основе графа $\boldsymbol{G}$, представляющего функциональную структуру ПТК, определяется множество выходных (внешних) функций $\boldsymbol{F}_{ВН}$ ($\boldsymbol{F}_{ВН} \subseteq \boldsymbol{F}$). Выходными являются функции, вершины которых на графе $\boldsymbol{G}$ не имеют исходящих дуг. Для выходных функций $f_i \in \boldsymbol{F}_{ВН}$ определяются коэффициенты относительной важности w_i.

Далее определяется подмножество *критических функций* $\boldsymbol{F}^0_{ВН} \subseteq \boldsymbol{F}_{ВН}$, т.е. таких функций, отказ любой из которых приводит к недопустимому ухудшению уровня эффективности ИС. Например, с учетом известных коэффициентов относительной важности в подмножество $\boldsymbol{F}^0_{ВН}$ можно включить те функции, для которых выполняется условие: $w_i \geq w_i^0$, где w_i^0 — критическое (пороговое) значение коэффициента относительной важности, величина которого задается экспертом.

Введение подмножества критических функций $\boldsymbol{F}^0_{ВН}$ позволяет формализовать понятие «отказ ПТК». В этом случае можно считать, что отказ ПТК наступает тогда, когда откажет хотя бы одна из функций $f_i \in \boldsymbol{F}^0_{ВН}$.

Тогда показатели надежности ПТК можно рассчитать следующим образом:

$$T_{0\,ПТК} = \left(\sum_{f_i \in F^0_{ВН}} \frac{1}{T_{0i/1,\ldots,i-1}} \right)^{-1}, \tag{10}$$

$$T_{В\,ПТК} = \frac{1}{T_{0\,ПТК}} \sum_{f_i \in F^0_{ВН}} T_{0i/1,\ldots,i-1} \cdot T_{Bi}, \tag{11}$$

где $T_{0i/1,\ldots,i-1}$ — условная средняя наработка на отказ функции f_i при условии, что функции $f_1,\ldots, f_{i-1}$ выполняются безотказно; T_{Bi} — среднее время восстановления работоспособности функции f_i.

Алгоритм вычисления условной средней наработки на отказ $T_{0i/1,\ldots,i-1}$ подобен алгоритму вычисления условных интенсивностей отказов в процедуре *LPO*.

Выводы

Разработанная методика позволяет получать приближенные оценки показателей надежности многофункциональных программно-технических комплексов (ПТК) с учетом отказов технических устройств и отказов программного обеспечения, порождаемых ошибками в программах. При расчетах показателей надежности учитывается структурная избыточность технических средств (резервирование) и наличие связей между программами, реализующими различные функции ПТК. Расчеты производятся при допущениях об экспоненциальности распределений наработки до отказов и времени восстановления.

Для определения показателей надежности ПТК вводится понятие критического подмножества функций $\boldsymbol{F}^0_{ВН} \subseteq \boldsymbol{F}_{ВН}$, в которое включаются такие функции, отказы которых приводят к «отказу ПТК» в целом (к недопустимому снижению уровня эффективности).

Методика практически реализована средствами системы программирования Delphi для Windows.

1. *Дэвид Г.* Метод парных сравнений: Пер. с англ. — М.: Статистика, 1978.

2. *Тоценко В.Г.* Методы и системы поддержки принятия решений: алгоритмический подход. — К.: Наук. думка, 2002. — 382 с.

3. *Козлов Б.А., Ушаков И.А.* Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики. — М.: Советское радио, 1975. — 472 с.

4. *Черкесов Г.Н.* Надежность аппаратно-программных комплексов: Учеб. пособ. — СПб.: Питер, 2005. — 479 с.

5. ГОСТ 27.205-97. Надежность в технике. Проектная оценка надежности сложных систем с учетом технического и программного обеспечения и оперативного персонала.

Поступила в редакцию 31.08.2007