

Федеральное государственное бюджетное учреждение науки  
Институт проблем управления им. В.А. Трапезникова  
РОССИЙСКОЙ АКАДЕМИИ НАУК

**В.С. Викторова, Н.В. Лубков, А.С. Степанянц**

**АНАЛИЗ НАДЕЖНОСТИ  
ОТКАЗОУСТОЙЧИВЫХ  
УПРАВЛЯЮЩИХ  
ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ**

Москва  
ИПУ РАН  
2016

УДК 681.019.3  
ББК 3965-021.1  
А351

**Викторова В.С.** Анализ надежности отказоустойчивых вычислительных систем/ В.С. Викторова, Н.В. Лубков, А.С. Степанянц. – М.: ИПУ РАН, 2016. – 117 с.

Обобщены результаты теоретических и практических работ авторов в области проектного анализа надежности бортовых отказоустойчивых управляющих вычислительных систем. При разработке и исследовании моделей сделан акцент на специфике “надежного поведения” вычислительной техники – возможности возникновения сбоев и алгоритмической обработке неисправностей. Процесс возникновения неисправностей и последующей деградации технической структуры ОУВС исследуется с привлечением логико-вероятностных и марковских моделей.

Проведены параметрические исследования влияния несовершенства средств контроля (неабсолютная полнота контроля, отказы контроля) на работоспособность ОУВС, позволяющие обосновано выдвигать требования к контролю.

Предназначена для научных работников, инженеров и аспирантов, занимающихся анализом и обеспечением надежности вычислительных систем.

*Рецензенты: д.т.н. Каравай М.Ф., д.т.н. Лебедев В.Г.*

*Утверждено к печати Редакционным советом Института.*

*Текст воспроизводится в виде, утвержденном  
Редакционным советом Института*

ISBN 978-5-91450-134-8

 **ИНСТИТУТ  
ПРОБЛЕМ  
УПРАВЛЕНИЯ** 2013

## ОГЛАВЛЕНИЕ

<b>ПРЕДИСЛОВИЕ</b> .....	<b>5</b>
<b>1. СПЕЦИАЛИЗИРОВАННЫЕ МОДЕЛИ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ИССЛЕДОВАНИЯ НАДЕЖНОСТИ ОТКАЗОУСТОЙЧИВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ</b> .....	<b>8</b>
1.1. Унифицированная марковская модель анализа надежности отказоустойчивых вычислительных систем.....	9
1.2. Исследование приемов укрупнения состояний в моделях надежности ОУВС .....	19
<b>2. РАЗРАБОТКА ФРАГМЕНТОВ МОДЕЛИ НАДЕЖНОСТИ ОУВС</b> .....	<b>28</b>
2.1. Модель стохастического поведения сбоя во времени .....	28
2.1.1. Приемы описания временных характеристик сбоя .....	28
2.1.2. Моделирование поведения сбоя .....	30
2.1.3. Оценка эффективности методов парирования сбоя .....	31
2.2. Сравнение эффективности методов восстановления типа повторения операций .....	35
2.3. Параметрический анализ надежности встроенных средств контроля .....	36
2.3.1. Модели нерезервированных невосстанавливаемых систем с подсистемой контроля.....	37
2.3.2. Модели нерезервированных восстанавливаемых систем с подсистемой контроля.....	46
2.3.3. Модели резервированных систем с подсистемой контроля .....	51
<b>3. АНАЛИЗ НАДЕЖНОСТИ ОУВС МЕТОДОМ АГРЕГИРОВАНИЯ МАРКОВСКИХ МОДЕЛЕЙ</b> .....	<b>56</b>
3.1. Факторы модели надежности ОУВС .....	57
3.2. Модель обработки неисправностей.....	58
3.3. Модель деградации технической структуры ОУВС .....	61
<b>4. АНАЛИЗ НАДЕЖНОСТИ ОУВС МЕТОДОМ АГРЕГИРОВАНИЯ ЛОГИКО-ВЕРОЯТНОСТНЫХ И МАРКОВСКИХ МОДЕЛЕЙ</b> .....	<b>65</b>

4.1.	Описание функционирования и структурно-надежностный анализ ОУВС .....	66
4.2.	Построение агрегированной модели надежности ОУВС .....	70
4.3.	Методы расчета показателей надежности на деревьях отказов ОУВС .....	89
4.4.	Модели надежности элементов с учетом сбоев .....	102
4.4.1.	Анализ надежности устройств связи, работающих в режиме обмена .....	104
4.4.2.	Анализ надежности устройств связи, работающих в режиме согласования.....	106
4.4.3.	Анализ надежности УС, работающих в двух режимах .....	110
4.4.4.	Анализ надежности вычислительной машины .....	111
4.5.	Результаты анализа ОУВС .....	112
<b>5.</b>	<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>114</b>
	<b>ЛИТЕРАТУРА.....</b>	<b>116</b>

## ПРЕДИСЛОВИЕ

Вычислительные машины уже давно используются для выполнения управляющих функций на объектах повышенной критичности (космических, военных, промышленных), что является причиной предъявления жестких требований к надежности их функционирования. Разрабатываются и внедряются проекты управляющих вычислительных систем (УВС), высокая надежность которых достигается как за счет использования качественной элементной базы, так и за счет введения избыточности [1-16]. Избыточные УВС, использующие контроль, резервирование и специальные процедуры обработки неисправностей, получили название отказоустойчивых управляющих вычислительных систем (ОУВС). Анализ надежности ОУВС является достаточно сложной задачей из-за необходимости учета большого количества факторов, характеризующих как свойство управляющей системы, так и особенности вычислительного процесса. Естественный путь преодоления этих трудностей состоит в разработке моделей работоспособности этих систем, учитывающих наличие развитой системы контроля неисправностей, способность к изменению структуры при возникновении нарушений функционирования отдельных ее элементов, процедуры восстановления вычислительного процесса и др. Однако построить универсальную модель надежности ОУВС, рассчитанную на многообразие применяемых методов обеспечения работоспособности и многочисленные варианты архитектурных решений, не представляется возможным, а построение набора частных моделей работоспособности ОУВС не решит поставленной задачи из-за ограниченности такого набора. В данной книге предлагается процедура построения моделей надежности отказоустойчивых вычислительных систем и детально рассматриваются основные элементы этих моделей, соответствующие архитектурным решениям и организации средств обеспечения работоспособности. Описываются способы агрегирования элементов моделей в общую модель надежности ОУВС.

Книга состоит из четырех разделов.

В первом разделе выполнен обзор специализированных моделей и программного обеспечения анализа надежности ОУВС. Приведен результат критического анализа некоторых приемов описания

надежностного поведения ОУВС, которые были предложены в пионерских работах по созданию унифицированной модели надежности ОУВС – ARIES. Эти приемы в явном и неявном виде применяются как отечественными, так и зарубежными специалистами и в настоящее время, поэтому ограничить области их корректного применения представляется полезным.

Во втором разделе проведены исследования процессов возникновения ошибок и восстановления вычислительного процесса после сбоя. Получены вероятностные характеристики сложных событий этого процесса, необходимые для вычисления показателей, оценивающих успешность завершения восстановления вычислительного процесса методом повторения фрагментов программ после обнаружения ошибки. Особенностью модели является предположение о неэкспоненциальном распределении длительности существования сбоя в ОУВС. Проведен анализ свойств средств обнаружения неисправностей. Исследованы зависимости вероятностей возникновения аварийных и штатных отказов систем от параметров полноты и безотказности встроенного контроля. Влияние свойств контроля на показатели надежности оценено для систем с различной степенью резервирования и восстановления.

В третьем разделе описан подход к декомпозиции надежностного поведения ОУВС на медленные и быстрые процессы. К медленным относятся процессы возникновения отказов и сбоев элементов ОУВС. Быстрые процессы связаны с процедурами обработки этих неисправностей. Предложена дискретная марковская модель обработки неисправностей с разделением состояний отказ и сбой и учетом возможности возникновения вторичных неисправностей в процессе восстановления нормального хода вычислительного процесса, нарушенного сбоями. Описана техника интеграции модели обработки неисправностей в непрерывную марковскую модель деградации технической структуры ОУВС. Работа методов декомпозиции и интеграции продемонстрирована на примере анализа надежности отказоустойчивого трехмашинного вычислительного комплекса.

В четвертом разделе предложен метод моделирования деградации работоспособности резервированных отказоустойчивых управляющих вычислительных систем, основанный на структурно-логической декомпозиции. Декомпозиция заключается в выделении пол-

ной группы несовместных событий работоспособности /неработоспособности вычислительных машин и устройств сетей связи с объектом и межмашинного согласования. Для оценки характеристик надежности частей системы, выделяемых при декомпозиции, использована комбинация логико-вероятностных методов деревьев отказов и марковского моделирования. Описано применение метода при моделировании “надежностного поведения” ОУВС с частотным и последовательностным критериями признания сбоивших компонентов отказавшими. Представлены результаты анализа обобщенного дерева отказов ОУВС, каждое базовое событие которого раскрывается вложенным деревом, марковским графом, комбинаторной моделью.

# 1. СПЕЦИАЛИЗИРОВАННЫЕ МОДЕЛИ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ИССЛЕДОВАНИЯ НАДЕЖНОСТИ ОТКАЗОУСТОЙЧИВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Для оценки эффективности проектных решений по обеспечению отказоустойчивости управляющих вычислительных систем были разработаны специализированные модели и программные средства анализа надежности - ADVISER, ARIES, CAST, CARE, GRAMP, HARP, SHARPE, SURF [17-22]. Хотя эти программы к настоящему времени морально устарели (в основном с программисткой точки зрения), многие реализованные в них идеи и подходы нашли свое воплощение и дальнейшее развитие в современном универсальном ПО анализа надежности [23-26].

В этих программах впервые были воплощены:

- идея агрегирования марковских и логико-вероятностных моделей и впервые были реализованы начальные формы динамических деревьев отказов [27, 28], в которых вероятности “срабатывания” динамических вершин ненагруженного резервирования (SPARE GATE) и последовательности (SEQUENCE ENFORCING GATE) рассчитывались на марковских моделях;
- декомпозиция надежного поведения системы на медленные (возникновение неисправностей) и быстрые (обработка неисправностей) процессы; причем, сложная многоэтапная процедура обработки неисправностей исследовалась с привлечением статистического моделирования, а в качестве формального описания этапов привлекались расширенные сети Петри [29-31];
- графическое задание модели надежности пользователем в виде деревьев отказов, которые затем автоматически преобразовывались в марковские цепи.

Наиболее известной и цитируемой отечественными специалистами является унифицированная модель и программа ARIES [32]. Исследования по синтезу и анализу отказоустойчивых систем планомерно развиваются и в настоящее время. Ежегодно проводится международная конференция по гарантоспособным системам и сетям (International Conference on Dependable Systems and Networks

(<http://www.dsn.org>)), образовавшаяся в результате слияния симпозиума IEEE по отказоустойчивым вычислениям (Fault-Tolerant Computing (FTCS)) и конференции IFIP по гарантоспособным вычислениям в критичных приложениях (Conference on Dependable Computing for Critical Applications (DCCA)). В нашей стране в настоящее время вновь наблюдается повышение интереса специалистов по вычислительной технике и надежности к проблеме синтеза и анализа надежности отказоустойчивых вычислительных систем [33, 34]. Однако отсутствие у нас планомерных работ в данной области в 90-е годы не позволило критически осмыслить модели надежности ОУВС. В данной книге приведен результат критического анализа модели надежности программы ARIES и выявлены некоторые ошибочные приемы по укрупнению состояний и агрегированию моделей. Модель надежности программы ARIES была выбрана потому, что именно она явилась обобщением большинства моделей надежности ОУВС, разработанных в США, и послужила катализатором к разработке подобных себе моделей в нашей стране.

### **1.1. Унифицированная марковская модель анализа надежности отказоустойчивых вычислительных систем**

ARIES [17, 32] рассматривает ОУВС как последовательное соединение подсистем, каждая из которых определяется тремя структурными параметрами  $N$  (число рабочих элементов),  $S$  (число резервных элементов),  $D$  (число разрешенных деградаций рабочей (активной) конфигурации). Например, при  $N = 2$ ,  $S = 1$ ,  $D = 1$  имеем подсистему с двумя параллельно работающими элементами и одним, находящимся в холодном резерве. ARIES допускает исследование как восстанавливаемых (с произвольным числом ремонтных бригад), так и невосстанавливаемых (замкнутых) ОУВС. Рабочие элементы подсистем подвержены возникновению, как постоянных отказов, так и сбоев, в резервных элементах могут возникать только постоянные отказы.

В ARIES предполагаются неидеальными операции контроля и подключения резерва, а также мероприятия по восстановлению сбившихся элементов, что учитывается с помощью специального параметра модели – покрытия, представляющего собой условную вероятность парирования системой неисправности при условии, что она произошла.

В модели приняты три условия перехода подсистемы в отказ – истощение ее ресурсов; возникновение необнаруживаемой или невосстанавливаемой неисправности рабочих элементов; подключение неисправного резерва, вместо отказавшего рабочего элемента.

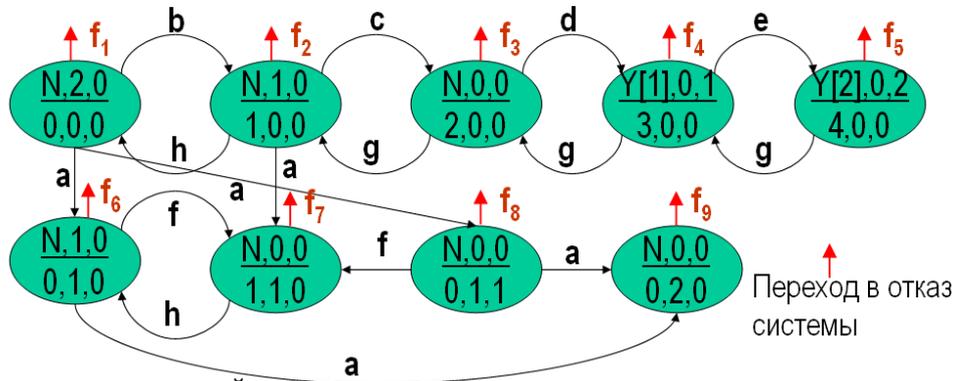
Графовая интерпретация модели надежности представлена на рис.1.1. Состояния  $N,S-i$  ( $i = 0, \dots, S-i$ ) есть состояния полной активной конфигурации и наличия  $S-i$  элемента холодного резерва. Состояния  $\overline{N},S-i$  есть состояния полной активной конфигурации и наличия необнаруженной неисправности у  $S-i+1$  – го резервного элемента. Переходы из состояний  $N,S-i+1$  в состояния  $N,S-i$  происходят при возникновении обнаруживаемых и восстанавливаемых неисправностей рабочих элементов или при возникновении обнаруживаемых неисправностей резервных элементов. Состояние  $N-j,0$  соответствует истощенному холодному резерву и  $j$  обнаруженным отказам рабочих элементов ( $j = 0, \dots, D$ ). Стратегия восстановления по постоянным отказам, принятая в модели, представлена на схеме рис.1.2.

Исследование надежности ОУВС проводится в рамках ARIES на базе однородных марковских процессов с непрерывным временем и дискретным множеством состояний, порождающих систему дифференциальных уравнений

$$P'(t) = P(t) \cdot \Lambda(t), \quad (1.1)$$

где  $\Lambda(t)$  – инфинитезимальная  $n \times n$  матрица с элементами  $\lambda_{ij}(t)$ , являющимися интенсивностями переходов из состояния  $i$  в состояние  $j$ . При допущении об экспоненциальном распределении времени пребывания в состояниях, сделанном в ARIES

$$P'(t) = P(t) \cdot \Lambda. \quad (1.2)$$



Кодировка состояний:

$\underline{A, P, K}$     A – число рабочих модулей;  
                   P – число доступных резервных модулей;  
 $\underline{Q, R, B}$     K – число деградаций, которые произошли в системе;  
                   Q – количество ремонтируемых модулей;  
                   R – количество отказавших резервных модулей, не подлежащих ремонту  
                   B – количество заблокированных резервных модулей

$$\begin{array}{llll}
 \mathbf{a} = (1 - \mathbf{C}d)\theta & \mathbf{d} = \mathbf{N}\mathbf{C}\mathbf{Y}[1]\lambda & \mathbf{h} = \mu & \mathbf{f}_1 = \mathbf{f}_2 = \mathbf{f}_6 = \mathbf{f}_7 = \mathbf{f}_8 = \mathbf{N}(1 - \mathbf{C}\mathbf{a})\lambda \\
 \mathbf{b} = \mathbf{N}\mathbf{C}\mathbf{a}\lambda + 2\mathbf{C}d\theta & \mathbf{e} = \mathbf{Y}[1]\mathbf{C}\mathbf{Y}[2]\lambda & & \mathbf{f}_3 = \mathbf{N}(1 - \mathbf{C}\mathbf{Y}[1])\lambda & \mathbf{f}_5 = \mathbf{Y}[2]\lambda \\
 \mathbf{c} = \mathbf{N}\mathbf{C}\mathbf{a}\lambda + \mathbf{C}d\theta & \mathbf{f} = \mathbf{C}d\theta & \mathbf{g} = 2\mu & \mathbf{f}_4 = \mathbf{N}(1 - \mathbf{C}\mathbf{Y}[2])\lambda & \mathbf{f}_9 = \mathbf{N}\lambda
 \end{array}$$

Рис. 1.1. Марковский граф модели надежности ARIES (количество резервных элементов = 2, количество разрешенных деградаций = 2, число ремонтных бригад = 2)

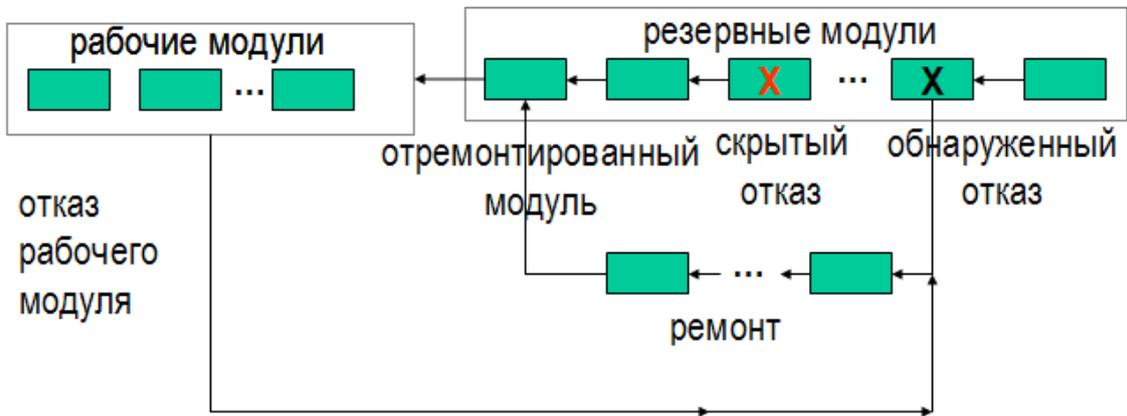


Рис. 1.2. Модель ARIES. Стратегия восстановления по постоянным отказам

Предлагается аналитическое решение (1.2) с использованием интерполяционной формулы Лагранжа-Сильвестра

$$P(t) = \sum_{i=0}^{n-1} e^{\sigma_i t} \left( \prod_{\substack{j=0 \\ j \neq i}}^{n-1} \frac{\Lambda - \sigma_j I}{\sigma_i - \sigma_j} \right) \cdot P(0), \quad (1.3)$$

где  $\sigma_i, \sigma_j$  – собственные значения матрицы  $\Lambda$ , нахождение которых существенно упрощено для невосстанавливаемых систем (в этом случае  $\Lambda$  – треугольная матрица с собственными значениями, лежащими на главной диагонали). Показатель вероятности безотказной работы исследуемой ОУВС вычисляется суммированием вероятностей пребывания во всех работоспособных состояниях

$$R(t) = \sum_{i=1}^{n-1} P_i(t). \quad (1.4)$$

В ARIES, вероятно впервые, была разработана и агрегирована в основную модель (рис.1.1) модель обработки неисправностей, учитывающая специфику именно ОУВС (рис.1.3), в частности, специальные программно-аппаратно реализуемые процедуры обработки сбоев (повтор команд, операций ввода-вывода, программ, перезагрузки системы). В условиях отсутствия точных исходных данных по частоте возникновения и длительности сбоев было принято допущение об экспоненциальном характере этих случайных величин с параметрами  $\tau$  и  $\vartheta$  соответственно. Все неисправности (постоянные отказы и сбои) подразделялись на два класса некатастрофические (принципиально восстанавливаемые) и катастрофические (наносящие столь большой вред, что восстановление от них невозможно). Это деление нашло свое отражение в ведении в модель обработки специального параметра “восстанавливаемости” –  $r$  ( $0 \leq r \leq 1$ ), являющегося условной вероятностью того, что произошедшая неисправность – некатастрофическая. Процесс восстановления от сбоев описывался тройкой параметров  $(n, T, E)$ , где  $n$  – число этапов восстановления,  $T = (T[1], \dots, T[n])$  – вектор длительностей каждого этапа,  $E = (E[1], \dots, E[n])$  – вектор эффективности этапов восстановления. Были выделены три возможных исхода восстановления от сбоев: успешное завершение восстановления (“покрытие сбоев”), переход на проце-

дуры восстановления от постоянных отказов, отказ системы. Соответствующие условные вероятности этих исходов определялись следующим образом:

$C_T = \mathbf{Prob}$ (процедуры восстановления от сбоев успешно завершены/неисправность возникла) =  $\mathbf{Prob}$ (возникшая неисправность есть некатастрофический сбой  $\cap$  сбой как физическое явление закончил свое существование до завершения процесса восстановления  $\cap$  по крайней мере одна из процедур восстановления оказалась эффективной  $\cap$  аппаратура, реализующая восстановление, исправна);

$L_T = \mathbf{Prob}$ (переход на процедуры восстановления от постоянных отказов/неисправность возникла) =  $\mathbf{Prob}$ ((возникшая неисправность есть некатастрофический сбой  $\cap$  (сбой как физическое явление не закончил свое существование до завершения процесса восстановления  $\cup$  ни одна из процедур восстановления не оказалась эффективной))  $\cup$  (возникшая неисправность есть некатастрофический отказ))  $\cap$  аппаратура, реализующая восстановление, исправна);

$F_T = \mathbf{Prob}$ (отказ системы/неисправность возникла) =  $\mathbf{Prob}$ (возникла катастрофическая неисправность  $\cup$  аппаратура, реализующая восстановление, неисправна).

Модель обработки неисправностей показана на рис. 1.3.

Она представляет собой конечную марковскую цепь с переходными вероятностями, вычисляемыми по формулам:

$$PR_i = \alpha e^{-\rho T[i]} \cdot E_i \cdot PV[i], \quad (1.5)$$

где  $\alpha$  – доля сбоев в общем потоке неисправностей;  $\rho$  – интенсивность неисправностей восстанавливающего оборудования;  $PV[i]$  есть вероятность завершения сбоя до начала выполнения  $i$ -го этапа восстановления

( $PV[i] = 1 - e^{-\sum_{j=0}^{i-1} \frac{T_j}{g}}$ ).

$$PE_i = e^{-\rho T[i]} (\alpha(1 - E[i]PV[i]) + (1 - \alpha)) \quad (1.6)$$

$$PF_i = 1 - e^{-\rho T[i]}. \quad (1.7)$$

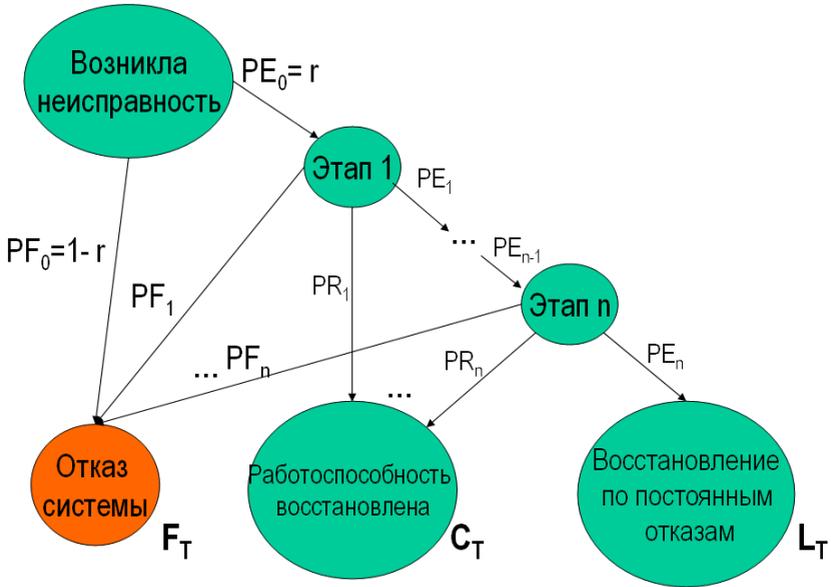


Рис. 1.3. Модель ARIES. Процедура обработки неисправностей

Тогда, вероятность попадания системы в состояние “Отказ системы” во время процесса восстановления

$$F_T = \sum_{i=1}^n PF_i \prod_{j=0}^{i-1} PE_j + 1 - r. \quad (1.8)$$

Вероятность успешного завершения процесса восстановления от сбоев

$$C_T = \sum_{i=1}^n PR_i \prod_{j=0}^{i-1} PE_j. \quad (1.9)$$

Вероятность перехода на процедуры восстановления от постоянных отказов

$$L_T = \prod_{i=0}^n PE_i . \quad (1.10)$$

Очевидно  $F_T + L_T + C_T = 1$ .

При агрегации модели обработки неисправностей в основную модель был учтен тот факт, что время обработки пренебрежимо малая величина по сравнению со средним временем между возникновением отказов элементов ОУВС. В связи с этим процедура восстановления как от сбоев, так и от постоянных отказов (переключение на резерв) полагались мгновенными. Факторы восстановления работоспособности, нарушаемой сбоями, и попадание в состояние соответствующее отказу ОУВС из-за неисправностей восстанавливающей аппаратуры или катастрофической неисправности учитывались соответствующей “развесовкой” интенсивностей неисправностей рабочих элементов ОУВС. Таким образом, для каждого состояния вводилась корректировка интенсивностей. Так, например, при безотказном резерве интенсивности перехода из состояния  $N, S$  в состояние  $N, S-1$  ( $\Lambda$ ) и состояние, соответствующее отказу ОУВС ( $\Lambda_f$ ) для исходной модели вычисляются по (1.11), а с учетом процедур обработки сбоев по (1.12):

$$\begin{aligned} \Lambda &= C_a N(\lambda + \tau) \\ \Lambda_f &= (1 - C_a) N(\lambda + \tau) . \end{aligned} \quad (1.11)$$

$$\begin{aligned} \Lambda &= C_a L_T N(\lambda + \tau) \\ \Lambda_f &= ((1 - C_a) L_T + F_T) N(\lambda + \tau) , \end{aligned} \quad (1.12)$$

здесь  $C_a$  – “покрытие” по постоянным отказам;  $\lambda$  – интенсивность отказов;  $\tau$  – интенсивность сбоев.

ARIES безусловно заслуживает высокую оценку, особенно как модель, в которой впервые были учтены специфичные для отказоустойчивых вычислительных систем процедуры восстановления работоспособности. Наряду с достоинствами в модели присутствует ряд неточностей и некорректных предположений. Некоторые из них были уже обсуждены и вызвали определенную полемику в печати. Так, в известном обзоре [35] обсуждается корректность применения

формулы Лагранжа-Сильвестра (1.3) для решения системы (1.2) и отмечается, что применение (1.3) возможно лишь в случае отсутствия кратных собственных значений матрицы  $\Lambda$ . Здесь же был приведен пример ОУВС тривиальной структуры (2,1,1), порождающий матрицу интенсивностей с кратными собственными значениями. Кроме того, указывалось, что, несмотря на элегантность записи, (1.3) требует для своей реализации  $O(n^5)$  вычислительных операций, в то время как классическая процедура

$$P(t) = \sum_{i=0}^{n-1} e^{\sigma_i t} a_i v_i; P(0) = \sum_{i=0}^{n-1} a_i v_i; v_i - \text{собственный вектор для}$$

собственного значения  $\delta_i$ ) требует только  $O(n^4)$ . Первое замечание для случая невозстанавливаемых систем было снято в [36], где доказывалась диагоналируемость  $\Lambda$  для всех невозстанавливаемых ОУВС, моделируемых ARIES, а, следовательно, корректность применения (1.3). Второе замечание осталось без ответа. К сожалению, с критической точки зрения ни в отечественной, ни в зарубежной литературе не обсуждалась трактовка надежностного поведения и способы укрупнения состояний, реализованные в ARIES. Рассмотрим эти вопросы подробнее.

1. Положение о том, что ОУВС есть последовательное соединение подсистем редко выполняется на практике. Часто система проектируется таким образом, что в ней присутствуют общие элементы для нескольких подсистем или ОУВС в целом, например, источники питания. Такое положение препятствует проведению раздельного анализа подсистем, требует рассмотрения системы в целом, что порождает сложные модели надежности, ни только не укладывающиеся в схему гибридного резервирования, но и вообще не допускающие никакой унификации надежностного поведения ни на системном, ни на подсистемном уровне.
2. В ARIES приняты 2 слишком пессимистических предположения о непосредственном переходе подсистемы в отказ. *Первое* связано с подключением неисправного резервного элемента (см. рис. 1.2). Например, в подсистеме с рабочими элементами, объединенными в мажоритарную структуру  $M$  из  $N$ , и  $S$  резервными элементами по логике ARIES при отказе хотя бы одного рабочего элемента и подключении на его место неисправного резерва под-

система сразу же попадает в состояние отказа. В действительности при числе отказавших рабочих элементов от 1 до  $N-M-1$  и даже всех неисправных резервах, подключаемых на их место, эти неисправности должны маскироваться мажоритарной структурой. Второе предположение связано с неисправностями оборудования, участвующего в восстановлении после сбоев – отказ любой единицы такого оборудования во время восстановления есть отказ подсистемы. В условиях высокой степени резервирования, как правило, реализованной в ОУВС, одиночный отказ как специализированного восстанавливающего оборудования, так и штатных средств системы, участвующих в восстановлении, не может непосредственно привести к отказу системы.

3. Наряду с введением пессимистических предположений, касающихся неисправностей восстанавливающего оборудования, обсужденных выше, в ARIES вводится слишком оптимистичное предположение об отсутствии неисправностей всех остальных элементов во время восстановления от сбоев. Предположение остается в силе даже при примерном равенстве интенсивностей неисправностей всех элементов системы. Понятно, что введение подобных предположений, существенно упрощающих надежное поведение ОУВС, и дает возможность строить унифицированные модели. Однако лишь при определенных (возможно и соответствующих реальности) значениях параметров системы они не исказят истинное значение показателей надежности, например, при малом суммарном времени восстановления от сбоев. Исследование соотношений параметров системы, при которых верны вводимые допущения, ни в ARIES, ни в последующих моделях не проводятся.
4. В модели обработки неисправностей, принятой в ARIES, проведено укрупнение состояний сбоя и отказа элемента. После попадания в укрупненное состояние процесс восстановления развивается двояким образом в зависимости от вида неисправности (сбой/отказ) (см. 1.5÷1.7). Полученные затем вероятности исходов процесса восстановления (см. 1.8÷1.10) используются для корректировки интенсивностей суммарного потока неисправностей ОУВС (1.11, 1.12). Укрупнение состояний сбоя и отказа в одно нарушает условие укрупнения, требующее равенства переходных вероятностей для укрупняемых состояний. Достаточно

сказать, что вероятность восстановления работоспособности после  $i$ -го этапа восстановления  $PR_i$  для состояния “Отказ системы” всегда равна нулю. Поэтому правильным является построение отдельных моделей процесса обработки неисправностей для случая сбоев и отказов, вычисления по этим моделям вероятностей исходов восстановления ( $L_{TO}$ ,  $F_{TO}$ ) (для отказов), ( $L_{TC}$ ,  $C_{TC}$ ,  $F_{TC}$ ) (для сбоев), а затем проведение отдельной корректировки соответствующих интенсивностей:

$$\Lambda = C_a N (L_{TO} \lambda + L_{TC} \tau) \quad (1.13)$$

$$\Lambda_f = ((1 - C_a) L_{TO} + F_{TO}) N \lambda + ((1 - C_a) L_{TC} + F_{TC}) N \tau. \quad (1.14)$$

5. Также необходимо сделать следующее замечание. В выражении 1.1 присутствует зависящая от  $t$  матрица  $\Lambda(t)$ . То есть, речь идет о неоднородном марковском процессе. Необходимо отметить, что учет неэкспоненциальных распределений для различных факторов, элементов системы, приводящий к неоднородным марковским процессам, по существу невозможен. Лишь в специально подобранных примерах (можно сказать учебных) возможен учет неэкспоненциальности в марковских моделях надежности, да и то для какого-нибудь одного фактора. Поэтому правильной “работающей” математической моделью является только однородный марковский процесс, т.е. выражение 1.2.

## 1.2. Исследование приемов укрупнения состояний в моделях надежности ОУВС

Для того, чтобы исследовать в какой степени некорректное укрупнение искажает значение показателей надежности ОУВС рассмотрим простой пример дублированной системы ( $N=2$ ) с идеальным контролем. При возникновении неисправности одного из элементов исправный пытается его восстановить по схеме рис. 1.2. Значение параметров процедуры обработки взято из [36], где  $n = 6$ ,  $r = 0.999$ ,  $T = [0.01, 0.02, 0.03, 0.04, 0.05, 0.08]$ ,  $E = [0, 0.1, 0.2, 0.5, 0.7, 0.01]$ . При неуспехе всех этапов восстановления после сбоев исправный элемент отключается из активной конфигурации с  $C_a = 1$ . Граф переходов системы представлен на рис. 1.4.

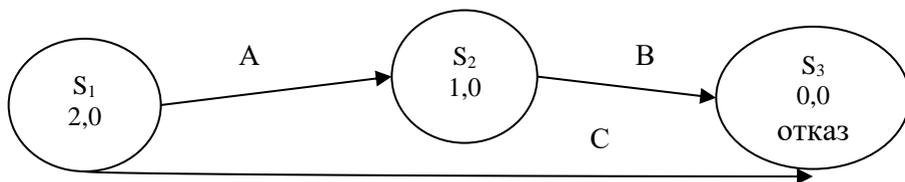


Рис. 1.4. Граф переходов дублированной ОУВС.

Интенсивности переходов А и С между состояниями 1 и 2 вычисляются по (1.11) и (1.12) соответственно, если в модели обработки неисправностей осуществлено укрупнение состояний сбой и отказ, или по (1.13) и (1.14) для точной модели без укрупнения.  $B = \lambda + \tau$ . Вероятность безотказной работы системы определяется выражением

$$P(t) = P_1(t) + P_2(t) = \frac{A}{A + C - B} e^{-Bt} + \frac{C - B}{A + C - B} e^{-(A+C)t}. \quad (1.15)$$

Вероятность отказа равна

$$Q(t) = 1 - P(t). \quad (1.16)$$

Относительная ошибка, возникающая при вычислении вероятности отказа системы при укрупнении состояний отказ и сбой в модели обработки неисправностей, равна

$$\Delta Q(t) = \frac{Q(t) - Q_{\text{укр.}}(t)}{Q(t)}, \quad (1.17)$$

где  $Q(t)$  – точное значение вероятности отказа системы (без укрупнения);  $Q_{\text{укр.}}(t)$  – приближенное значение (сбой и отказ укрупнены в одно состояние).

На рис. 1.5. представлена диаграмма зависимости  $\Delta Q(t) \cdot 100\%$  от  $\alpha$ . Каждый столбец соответствует фиксированному значению параметра  $\alpha$ . Если в системе присутствует только один тип неисправностей ( $\alpha = 0$  – отказы;  $\alpha = 1$  – сбой), то, очевидно, точное значение ве-

роятности отказа совпадает с приближенным. При отличных от граничных значениях  $\alpha$  относительная ошибка возрастает, принимая значение близкое к 26%.

На рис.1.6 представлена диаграмма зависимости  $\Delta Q(t) \cdot 100\%$  от параметра  $\vartheta$ . Нетрудно видеть, что чем меньше средняя длительность сбоя, тем больше ошибка. Это объясняется тем, что чем меньше  $\vartheta$ , тем в большей степени (с точки зрения вероятностных характеристик) различаются укрупняемые состояния сбоя и отказа.

Рис.1.7 демонстрирует поведение точной и приближенной функций вероятности отказа от времени. Некорректность использования приближенной функции усугубляется тем, что она является оценкой снизу показателей типа вероятности отказа. Графики построены при значениях параметров системы, взятых из [36]:  $\lambda + \tau = 10^{-4}$  1/ч.;  $\rho = 10^{-4}$  1/ч.

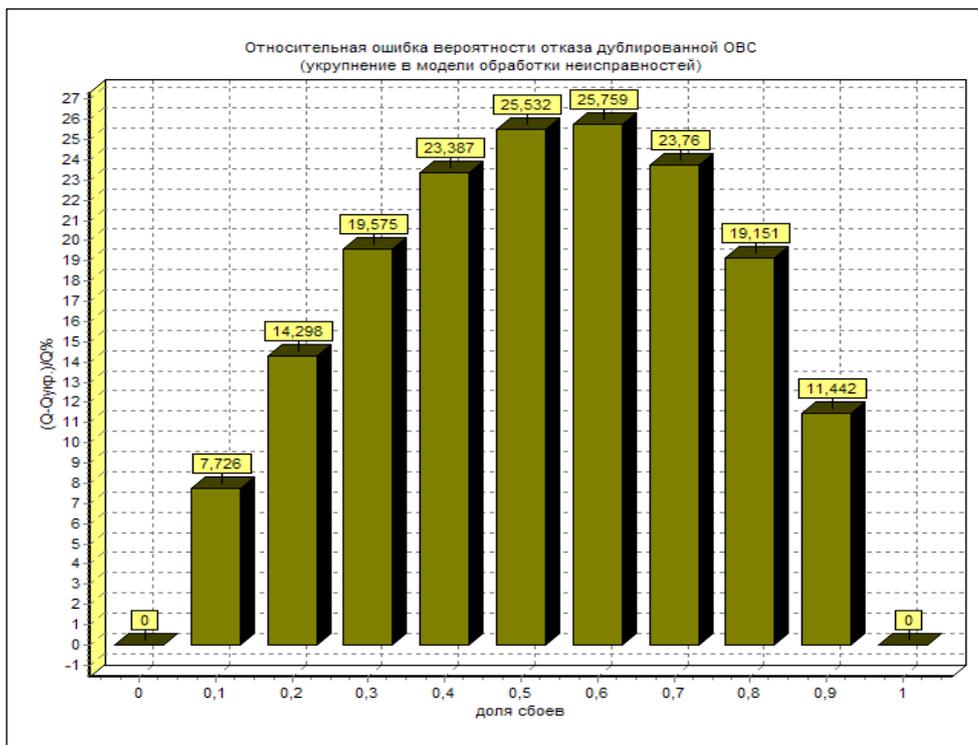


Рис. 1.5. Зависимость ошибки вычисления вероятности отказа от параметра доля сбоев.

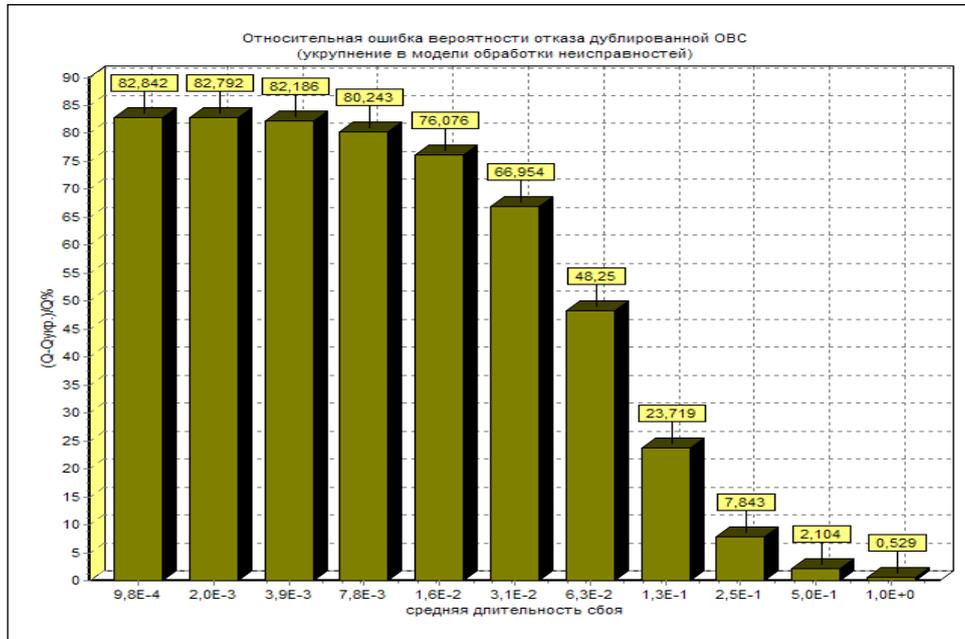


Рис. 1.6. Зависимость ошибки вычисления вероятности отказа от параметра средняя длительность сбоя.

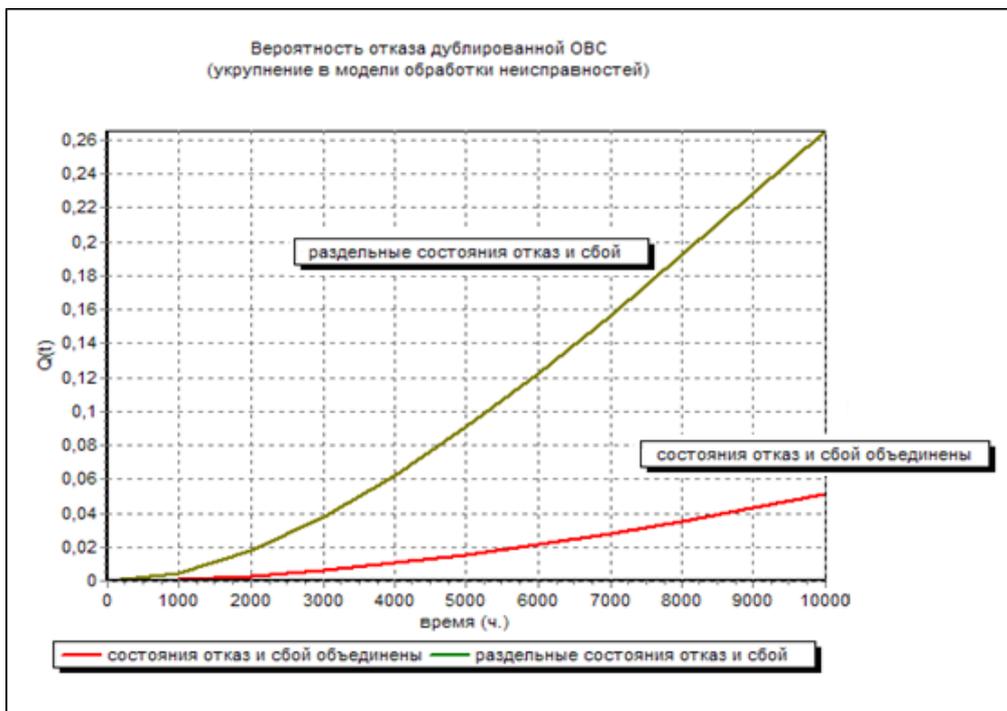


Рис. 1.7. Вероятность отказа дублированной ОУВС с парированием сбоев

В ARIES описанное укрупнение было применено в модели обработки неисправностей (рис. 1.3), поэтому оно хотя и привело к погрешностям вычисления показателей надежности на основной модели, описывающей процесс возникновения неисправностей элементов ОУВС (рис. 1.1), эти погрешности не носили столь катастрофический характер, как в последующих моделях, перенявших идею подобного укрупнения и использовавших ее именно в основных моделях. Например, если следовать этой технике укрупнения, то граф переходов (рис. 1.8,а) преобразуется объединением состояний отказ и сбой в граф (рис. 1.8,б).

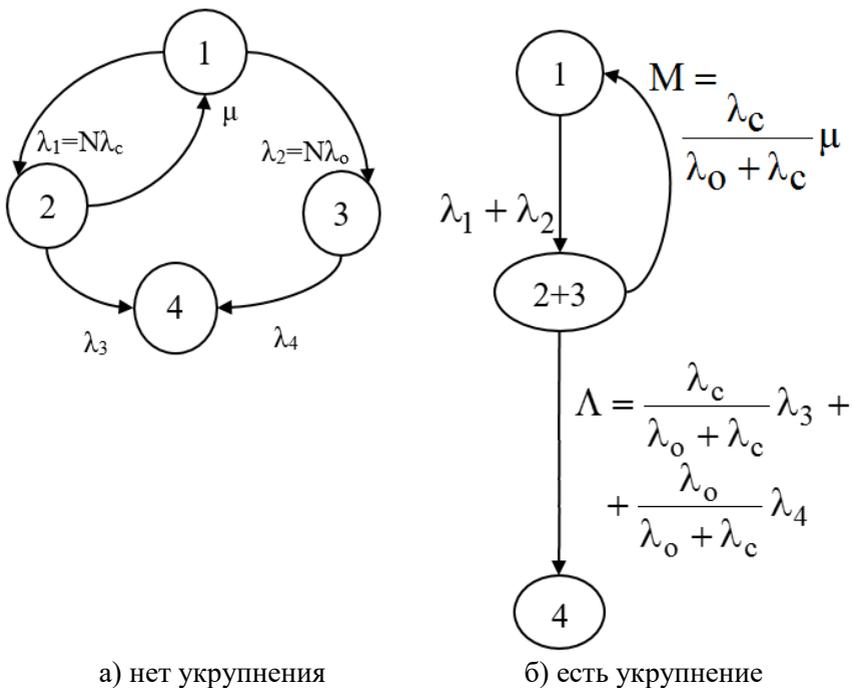


Рис. 1.8. Марковский граф возникновения неисправностей

Функция распределения и вероятности пребывания в состояниях 1, 2, 3 имеют вид:

$$F(t) = 1 - \sum_{i=1}^3 P_i(t); \quad (1.18)$$

$$\begin{aligned} P_1(t) &= \frac{\lambda_1 + \lambda_2 + x_2}{x_2 - x_1} e^{x_1(t)} - \frac{\lambda_1 + \lambda_2 + x_1}{x_2 - x_1} e^{x_2(t)}; \\ P_2(t) &= \frac{(\lambda_1 + \lambda_2 + x_1)(\lambda_1 + \lambda_2 + x_2)}{(x_2 - x_1)\mu} (e^{x_1(t)} - e^{x_2(t)}); \\ P_3(t) &= \frac{(\lambda_1 + \lambda_2 + x_2)\lambda_2}{(x_2 - x_1)(\lambda_4 + x_1)} e^{x_1(t)} + \frac{(\lambda_1 + \lambda_2 + x_2)\lambda_2}{(x_2 - x_1)(\lambda_4 + x_2)} e^{x_2(t)} \\ &\quad - \frac{(\lambda_1 + \lambda_2 + \lambda_4 + x_1 + x_2)\lambda_2}{(\lambda_4 + x_1)(\lambda_4 + x_2)} e^{-\lambda_4(t)}. \end{aligned} \quad (1.19)$$

$$x_{1,2} = \frac{-(\lambda_1 + \lambda_2 + \lambda_3 + \mu) \pm \sqrt{(\lambda_1 + \lambda_2 + \lambda_3 + \mu)^2 - 4(\lambda_1\lambda_3 + \lambda_2\lambda_3 + \lambda_2\mu)}}{2}.$$

Функция распределения для укрупненного графа

$$\begin{aligned} F_Y(t) &= 1 - (P_1(t) + P_{2+3}(t)) = 1 + \frac{x_2}{x_1 - x_2} e^{x_1(t)} - \frac{x_1}{x_1 - x_2} e^{x_2(t)}; \\ x_{1,2} &= \frac{-(\lambda_1 + \lambda_2 + \Lambda + M) \pm \sqrt{(\lambda_1 + \lambda_2 + \Lambda + M)^2 - 4(\lambda_1 + \lambda_2)\Lambda}}{2}. \end{aligned} \quad (1.20)$$

На рис. 1.9 даны графики функций  $F(t)$  и  $F_Y(t)$ . Из приведенных графиков видно, что в то время как точное значение функции распределения изменяется на интервале (0 – 10000 ч) от 0 до 1, приближенное значение изменяется от 0 до 0,008. То есть укрупнение существенно различных состояний (сбой, из которого есть возврат в исходное состояние; отказ, из которого принципиально отсутствует возврат в исходное состояние) порождает недопустимую погрешность. При варьировании параметров системы ( $\lambda_c, \lambda_o, \lambda_3, \lambda_4$ ) в диапазоне  $10^{-2} \div 10^{-7}$  1/ч величина погрешности практически остается нечувствительной к изменениям параметров системы. Проведенные исследования позволяют сделать вывод о недопустимости подобного укрупнения.

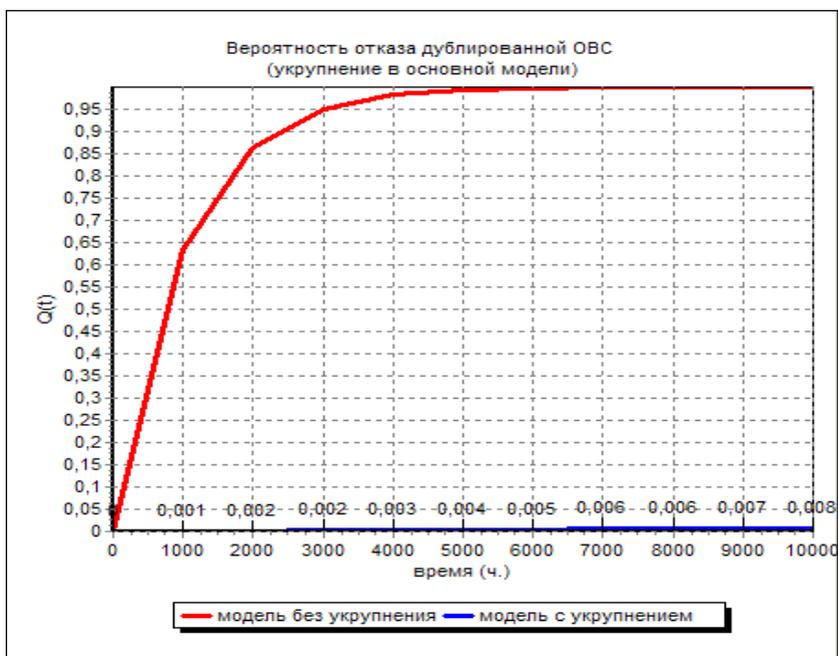


Рис. 1.9. Вероятность отказа дублированной ОУВС (укрупнение в основной модели)

## 2. РАЗРАБОТКА ФРАГМЕНТОВ МОДЕЛИ НАДЕЖНОСТИ ОУВС

### 2.1. Модель стохастического поведения сбоя во времени

Сбоем будем называть событие, состоящее во временной утрате работоспособности ОУВС и характеризующееся возникновением ошибки при выполнении тестов, управляющих приложений, задач (процессов) операционной системы. Сбои являются характерным явлением, свойственным интегральным схемам, комплектирующим функциональные блоки ОУВС, и составляют большинство в общем потоке неисправностей. Интенсивность возникновения сбоев в несколько порядков превышает величину интенсивности возникновения постоянных отказов ( $\sim 10^{-4}1/\text{ч}$  и  $\sim 10^{-7}1/\text{ч}$  для серийно выпускаемых микропроцессорных кристаллов). Создание новейших технологий и методов повышения выхода годных СБИС позволяет предполагать усугубление имеющегося разрыва и, как следствие, выделение сбоев в преобладающий фактор, определяющий надежность ОУВС. Выделяют два основных источника случайных сбоев – ионизирующее излучение и электромагнитные помехи.

#### 2.1.1. Приемы описания временных характеристик сбоя

Обычно предполагают, что поток внешних возмущающих событий, приводящих к возникновению сбоя, носит Пуассоновский характер. Следовательно, случайные интервалы времени между моментами появления сбоев описываются экспоненциальным распределением. Большинство сбоев вызывается короткими импульсными помехами, поэтому используемое допущение об экспоненциальном характере случайной длительности сбоя достаточно неестественно по ряду причин. В частности, в связи с большой дисперсией экспоненциального распределения и предположением о независимости оставшейся длительности сбоя от предыдущего времени его существования в системе как физического явления. Поэтому для описания случайной длительности сбоев более корректным является привлечение неэкспоненциальных распределений. Неэкспоненциальность нарушает предположение о марковских свойствах надежностного поведения ОУВС, возмущаемого появлением сбоев, и затрудняет его аналитические исследования.

Существуют методы приближенного моделирования распределений произвольного вида с помощью экспоненциального. Методы основаны на замене состояния системы, время пребывания в котором подчиняется неэкспоненциальному закону, каскадом последовательно соединенных “экспоненциальных” состояний. Случайное время пребывания в каждом из состояний каскада подчиняется экспоненциальному закону; интенсивность переходов между этими состояниями постоянна. С привлечением этих методов случайный процесс возникновения и пребывания сбой в ОУВС, как физического явления, может быть описан марковским процессом и исследован стандартным образом.

Проведем замену состояния системы, время пребывания в котором распределено неэкспоненциальным образом, на каскад последовательно соединенных  $k$  состояний. Случайные времена  $T_1, T_2, \dots, T_k$ , соответствующие временам нахождения системы в состояниях каскада, распределены экспоненциально с параметрами  $\mu_1, \mu_2, \dots, \mu_k$  соответственно.

Преобразование Лапласа плотности вероятности величины  $T_i$  равно

$$\mathcal{L}\{f(t_i); s\} = \int_0^{\infty} f(t_i) e^{-st_i} dt_i = \frac{\mu_i}{\mu_i + s}, \quad i=1, 2, \dots, k. \quad (2.1)$$

Пусть неотрицательная случайная величина  $T$  ( $T = T_1 + T_2 + \dots + T_k$ ) представляет собой суммарное время пребывания в состояниях каскада, а следовательно, и время пребывания в исходном состоянии. Преобразование Лапласа плотности случайной величины  $T$  равно

$$\mathcal{L}\{f(t); s\} = \prod_{i=1}^k \int_0^{\infty} f(t_i) e^{-st_i} dt_i = \prod_{i=1}^k \frac{\mu_i}{\mu_i + s}. \quad (2.2)$$

Результат применения обратного преобразования к (2.2)

$$f(t) = \sum_{i=1}^k A_i \mu_i e^{-\mu_i t}, \quad \text{где } A_i = \prod_{j \neq i} \frac{\mu_j}{\mu_j - \mu_i} \quad (2.3)$$

Если каждое состояние каскада имеет идентичное распределение с параметрами  $\mu_1 = \mu_2 = \dots = \mu_k = \rho = k\mu$ , то (2.3) преобразуется к виду

$$f(t) = \frac{k\mu}{(k-1)!} (k\mu t)^{k-1} e^{-k\mu t}. \quad (2.4)$$

Распределение с плотностью вида (2.4) носит название распределения Эрланга  $k$ -го порядка с математическим ожиданием

$$M[T] = \frac{k}{\rho}, \text{ дисперсией } D[T] = \frac{k}{\rho^2} \text{ и коэффициентом вариации } r,$$

меньшим единицы:  $r = \frac{\sqrt{D[T]}}{M[T]} = \frac{1}{\sqrt{k}}$ . Коэффициент вариации опре-

деляет степень разброса случайной величины относительно ее математического ожидания. Для экспоненциального распределения  $r = 1$ . Применяв распределение Эрланга, мы уменьшаем этот разброс, что уместно при описании “времени жизни” сбоя. Кроме того, с помощью (2.4) можно моделировать произвольные распределения с  $r < 1$ . Соответствующим выбором параметров  $\rho$  и  $k$  достигается равенство их математических ожиданий и дисперсий.

### 2.1.2. Моделирование поведения сбоя

Модель поведения сбоя во времени описывает следующие этапы. В случайный момент времени  $T_0$ , распределенный по экспоненциальному закону с параметром  $\lambda$ , ОУВС подвергается воздействию внешних возмущений (ионизирующее излучение, электромагнитные помехи), вызывающие сбой ее работы. Сбой, как физическое явление (кратковременное искажение выходного сигнала пораженного блока ОУВС) присутствует в системе короткий промежуток времени  $T_1$ , распределенный неэкспоненциально. По истечении времени  $T_1$  сбой “оканчивает” свое существование в системе (заканчивается действие возмущающей импульсной помехи). Аппаратура ОУВС продолжает работать в соответствии с техническими требованиями, однако последствия появления сбоя, записанная в память ложная информация, могут еще долго нарушать нормальный ход вычислительного процесса и порождать искаженные управляющие воздействия. Графовая интерпретация поведения сбоя во времени представлена на рис. 2.1а. На рис. 2.1б представлена модификация исходной модели (рис. 2.1а) путем замены состояния  $S$ , время пребывания в котором описывается неэкспоненциальной функцией распределения  $G(t)$ , на каскад последовательно соединенных состояний  $S_1, S_2,$

...,  $S_k$  с экспоненциально распределенными с параметром  $k\mu$  временами пребывания.

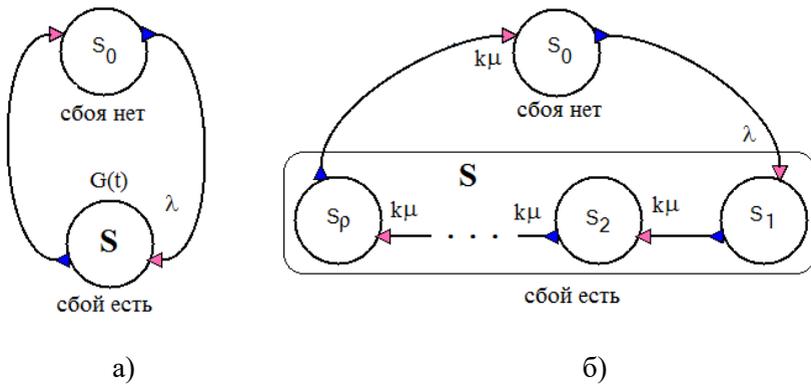


Рис. 2.1. Модель “времени жизни” сбоя в ОУВС

### 2.1.3. Оценка эффективности методов парирования сбоя

Для оценки успешности завершения системного метода борьбы со сбоями (например, повторение операций) и проведение сравнительного анализа эффективности различных модификаций этого метода (например, по временным критериям) требуется знание аналитических выражений для вероятностей следующих событий:

- $P_0(t)$  - вероятность отсутствия сбоя на интервале  $(0, t)$ ;
- $P(t)$  - вероятность отсутствия сбоя, как физического явления, в момент времени  $t$ ;
- $P(T, t)$  - вероятность отсутствия сбоя, как физического явления, в момент времени  $t$ , если в интервале  $(0, T)$  ( $T < t$ ) произошел хотя бы один сбой.

Необходимость знания этих выражений объясняется тем, что для успешного завершения повтора фрагментов вычислений должно осуществиться следующее сложное событие: сбой, зафиксированный контролем на интервале  $(0, T)$ , должен “уйти” из системы, как физическое явление, к моменту запуска повтора  $t$ ; в течении времени выполнения повтора сбой должны отсутствовать в системе.

Для экспоненциальной модели времени жизни сбоя, когда время его возникновения и пребывания в системе распределено экспоненциально с параметрами  $\lambda$  и  $\mu$  соответственно, эти вероятности связаны соотношением

$$P(T, t) = P(t) - P_0(T)P(t - T), \quad (2.5)$$

$$\text{где } P_0(T) = e^{-\lambda T}; P(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t}.$$

Представляет интерес определение этих вероятностей для описанной выше модели временного поведения сбоя с учетом снятия ограничений на экспоненциальный характер времени его существования.

Отметим

$$P(t) = 1 - \sum_{i=1}^k P_i(t), \quad (2.6)$$

где  $P_i(t)$  – вероятность пребывания в  $i$ -м состоянии каскада  $S_1, S_2, \dots, S_k$  (см. рис. 2.1б).

Ввиду краткости “жизни сбоя” предположим, что за рассматриваемый промежуток времен попасть в каждое из состояний каскада можно только один раз. Для вывода выражения для  $P_1(t)$  рассмотрим три случайных события, которые должны иметь место на интервале  $(0, t)$  для того, чтобы система, описанная моделью на рис. 2.1б, находилась в состоянии  $S_1$ . Первое событие заключается в отсутствии сбоя на интервале  $t_1 \in [0, t]$ ; вероятность этого события есть  $e^{-\lambda t_1}$ . Второе соответствует возникновению сбоя в интервале времени  $[t_1, t_1 + dt_1]$ ; вероятность этого события  $\approx \lambda dt_1$ . Третье соответствует тому, что система не выйдет из состояния  $S_1$  в оставшийся интервал времени  $[t_1 + dt_1, t]$ ; вероятность этого события  $e^{-k\mu(t - t_1 - dt_1)}$ .

$$\text{Тогда } P_1(t) = \int_{t_1=0}^{t_1=t} e^{-\lambda t_1} e^{-k\mu(t - t_1 - dt_1)} \lambda dt_1 \text{ и, сделав необходимые}$$

преобразования и пренебрегая членами  $e^{-k\mu dt_1}$ , получаем

$$P_1(t) = \frac{\lambda}{k\mu - \lambda} \left( e^{-\lambda t} - e^{-k\mu t} \right). \quad (2.7)$$

Вероятность пребывания во втором состоянии каскада  $S_2$

$$\begin{aligned} P_2(t) &= \int_{t_2=0}^{t_2=t} \int_{t_1=0}^{t_1=t_2} \lambda e^{-\lambda t_1} e^{-k\mu(t_2-t_1)} \mu e^{-k\mu(t-t_2)} dt_1 dt_2 = \\ &= \frac{k\mu}{k\mu - \lambda} P_1(t) - \lambda e^{-k\mu t} \frac{k\mu t}{k\mu - \lambda}. \end{aligned} \quad (2.8)$$

Вероятность пребывания в  $k$ -м состоянии каскада  $S_k$

$$P_k(t) = \frac{k\mu}{k\mu - \lambda} P_{k-1}(t) - \lambda e^{-k\mu t} \frac{(k\mu t)^{k-1}}{(k\mu - \lambda)(k-1)!}. \quad (2.9)$$

Прежде, чем находить выражения для  $P(T, t)$ , сделаем некоторые предварительные замечания.  $P(t, T)$  есть вероятность отсутствия сбоя в момент времени  $t$ , в то время как в интервале  $(0, T)$  произошел хотя бы один сбой. Поэтому для нахождения  $P(T, t)$  надо проинтегрировать на интервале  $(0, T)$  произведение плотности вероятности возникновения сбоя и вероятности отсутствия сбоя в момент времени  $t$ , определенную, исходя из предположения о наличии сбоя в начальный момент времени ( $\bar{P}(t)$ ).

$$P(T, t) = \int_0^T f(\tau) \bar{P}(t - \tau) d\tau. \quad (2.10)$$

Вероятность отсутствия сбоя в системе в момент времени  $t$  (состояние  $S_0$  на рис. 2.1б) при начальном состоянии  $S_1$  определяется  $k$ -кратным интегралом вида

$$\begin{aligned} \bar{P}(t) = P(S_0 / \text{при начале из } S_1) &= \int_0^t k\mu dt_k \int_0^{t_k} k\mu dt_{k-1} \dots \int_0^{t_2} e^{-k\mu t_1} e^{-k\mu(t_2-t_1)} \dots \\ &e^{-k\mu(t_k-t_{k-1})} e^{-\lambda(t-t_k)} k\mu dt_1. \end{aligned}$$

Сделаем необходимые преобразования, получаем

$$\bar{P}(t) = \frac{e^{-\lambda t} (k\mu)^k}{(k-1)!} \int_0^t t_k^{k-1} e^{-(k\mu-\lambda)t_k} dt_k \quad (2.11)$$

Окончательное выражение для  $\bar{P}(t)$  имеет вид

$$\bar{P}(t) = (k\mu)^k e^{-\lambda t} \left[ \frac{1}{(k\mu-\lambda)^k} - e^{-t(k\mu-\lambda)} \sum_{i=0}^{k-1} \frac{t^i}{i!(k\mu-\lambda)^{k-1}} \right] \quad (2.12)$$

Подставив выражение для  $\bar{P}(t)$  в (2.10), сделав замену переменных и соответственно изменив пределы интегрирования, получаем окончательное выражение для вероятности отсутствия сбоя в момент времени  $t$ , в то время как в интервале  $(0, T)$  ( $T < t$ ) произошел хотя бы один сбой. Выражение получено при предположении о пуассоновском характере потока сбоев и случайной длительности сбоя, распределенной по закону Эрланга с параметрами  $k$  и  $\rho = k\mu$ .

$$P(T, t) = (k\mu)^k \lambda e^{-\lambda t} \left[ \frac{T}{(k\mu-\lambda)^k} + \sum_{i=1}^k \frac{1}{(k\mu-\lambda)^{k-i+1}} [\mathfrak{R}(t) - \mathfrak{R}(t-T)] \right], \quad (2.13)$$

где  $\mathfrak{R}(t) = e^{-t(k\mu-\lambda)} \sum_{j=0}^i \frac{t^j}{j!(k\mu-\lambda)^{i-j}}$ .

Рассмотренный метод, используемый для оценки вероятности пребывания сбоя в выделенном состоянии каскада, основывается на многократном интегрировании плотностей распределений случайных времен пребывания в состояниях каскада, предшествующих выделенному. Метод носит приближенный характер. Суть приближения метода заключается в учете лишь однократного прохождения по состояниям каскада. При моделировании поведения сбоя рассматриваются лишь короткие временные интервалы, что является интуитивным подтверждением возможности использования метода.

## 2.2. Сравнение эффективности методов восстановления типа повторения операций

Полученные в предыдущих разделах выражения для определения вероятности отсутствия сбоя в заданный момент времени при различных начальных условиях (отсутствия сбоя  $\left( P_{00}(t) \right)$ , наличия сбоя  $\left( \bar{P}_{00}(t) \right)$ , наличие сбоя на интервале выполнения фрагмента программы  $\left( \bar{P}_{00}(T, t) \right)$  могут быть применены при оценке эффективности стратегий восстановления вычислительного процесса типа повторения операций. Используя эти выражения, можно определить вероятность успешного завершения выделенного этапа повторов ( $i$ -й повтор команды, откат на контрольную точку и т.д.):

$$\begin{aligned}
 & P(\text{успех } i\text{-го этапа восстановления}) = \\
 & \left[ \bar{P}_{00}(T, t_{\text{beg}i}, \lambda_{\text{сб}}, \mu) \cdot P_0(t_{\text{beg}i}, \lambda_{\text{отк}}) - \right. \\
 & \left. \sum_{k=1}^{i-1} P(\text{успех } k\text{-го этапа восстановления}) \cdot P_{00}(\Delta t_i^k, \lambda_{\text{сб}}, \mu) \cdot \right. \\
 & \left. P_0(\Delta t_i^k, \lambda_{\text{отк}}) \right] \cdot P_0(\lambda, t_{\text{rbi}}), \quad \text{где } \lambda = \lambda_{\text{сб}} + \lambda_{\text{отк}}.
 \end{aligned} \tag{2.14}$$

Здесь первое произведение, стоящее в квадратных скобках, есть вероятность отсутствия как постоянного отказа, так и сбоя, произошедшего в интервале времени выполнения фрагмента программы ( $T$ ), на момент начала выполнения процедуры восстановления  $t_{\text{beg}i}$ . Для выделения события успеха восстановления именно на  $i$ -м этапе из первого произведения, стоящего в квадратных скобках, вычитается вероятность успешного завершения всех предыдущих процедур восстановления. Множитель скобок есть вероятность отсутствия неисправностей любого типа во время выполнения  $i$ -го восстановления ( $t_{\text{rbi}}$ ).  $\Delta t_i^k$  - разность времен между  $i$ -м и  $k$ -м этапами восстановления.

На основе выражения (2.14) возможно конструирование показателей эффективности восстановления (например, среднее время успешного завершения восстановления вычислительного процесса ОУВС, нарушаемого возникновением сбоев), а, следовательно, и осуществления сравнительного анализа различных стратегий восстановления типа повторения операций. Среднее время успешного завершения вычислительного процесса ОУВС определяется как

$$T = \sum_{i=1}^n T_i \cdot P_i, \quad (2.15)$$

где  $T_i$  – время реализации соответствующего этапа восстановления;  $P_i$  – вероятность его успешного завершения.

### **2.3. Параметрический анализ надежности встроенных средств контроля**

В реализации процедур автоматического восстановления ОУВС принимают участие средства встроенного оперативного контроля. Встроенный контроль выполняет функции контроля без перерыва в решении задач управления. Встроенный контроль характеризуется временем запаздывания в обнаружении ошибок, долей обнаруживаемых ошибок (полнотой контроля), степенью влияния отказов своих элементов на вычислительный процесс ОУВС. Известно, что полнота контроля влияет практически на все показатели надежности технических систем [37, 38]. Только при полноте контроля, близкой к единице, реализуются все возможности дополнительных мероприятий и средств, направленных на повышение надежности. Однако, для достижения таких значений полноты контроля, система контроля ОУВС требует вложения определенного объема технических средств, которые в свою очередь могут отказывать и тем самым влиять на уровень надежности системы. Представляет интерес зависимость полноты контроля, обеспечиваемой подсистемой контроля ОУВС, от надежности технических средств (ТС) контроля в различных моделях ОУВС с контролем и влияние их на основные показатели надежности ОУВС. Исследуемые модели работоспособности представлены графом переходов марковской модели вычислительной системы.

### 2.3.1. Модели нерезервированных невозстанавливаемых систем с подсистемой контроля

Будем различать два типа отказа системы – аварийный (“тяжелый”) останов (А), обусловленный неконтролируемым отказом системы, и остановка вычислительного процесса (О), вызванная контролируемым отказом системы или отключением системы по ложному сигналу подсистемы контроля.

Система характеризуется интенсивностью отказов  $\lambda$ , интенсивность отказов средств контроля составляет  $\beta$  часть от  $\lambda - \beta\lambda$ . Полнота контроля технических средств –  $\eta$ . Средства контроля имеют отказы двух типов: несрабатывание, доля которых  $\alpha$ , и ложное срабатывание, доля которых  $1-\alpha$ . Основная задача средств контроля состоит в уменьшении числа аварийных остановок вычислительного процесса при сохранении или некотором снижении безотказности.

а). Система (вычислительный модуль системы) имеет контролируемую часть  $\eta\lambda$ , подсистема контроля (средства аппаратного контроля) не контролируется. Отказы средств контроля типа несрабатывание и ложное срабатывание несовместны. Критерий аварии – неконтролируемый отказ системы. Граф переходов такой системы приведен на рис. 2.2. Здесь состояния 1, 2 – работоспособные, 3 – неработоспособное с отказом типа останов, 4 – неработоспособное с отказом типа авария.

Проведены расчеты  $P(\theta)$ ,  $P_o(\theta)$ ,  $P_a(\theta)$ , где  $\theta = \lambda t$ , при различных значениях  $\alpha$ ,  $\beta$  и  $\eta$ . На графиках рис. 2.3. приведены кривые  $P$  (вероятность безотказной работы – ВБР),  $P_o$ ,  $P_a$  для  $\theta = 0.5$  и  $\alpha = 0.5$ . Вероятность безотказной работы  $P = P_1 + P_2$  в этом случае не зависит от полноты контроля  $\eta$  и уменьшается с ростом объема технических средств контроля  $\beta$  и доли ложных срабатываний ( $1-\alpha$ ) в потоке отказов СК. Из графиков видно, что полнота контроля  $\eta$  изменяет соотношение  $P_o$  и  $P_a$ . Характерно, что при некоторых значениях  $\eta$  ( $\eta=\alpha$ )  $P_a$  не зависит от надежности СК (от  $\beta$ ), а при полном контроле ( $\eta=1$ ) остается возможность отказа типа А. В этом проявляется ненадежность средств контроля.

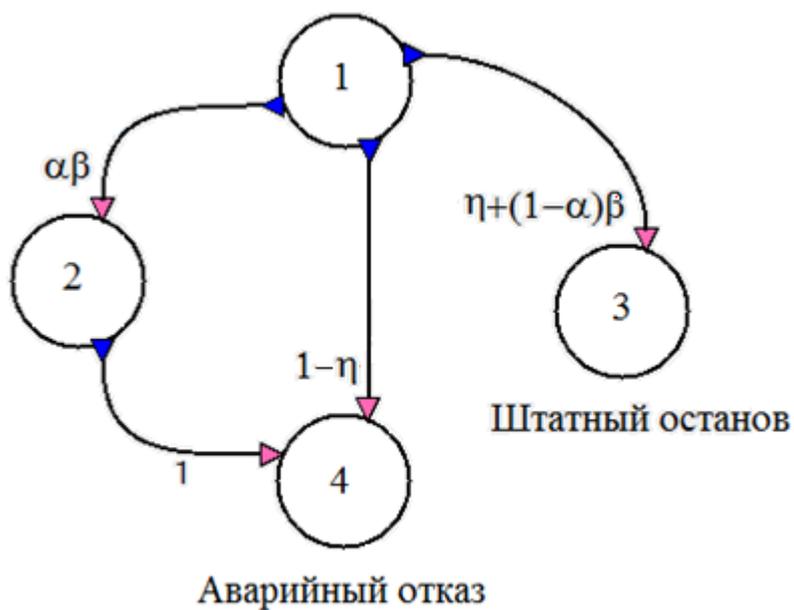


Рис. 2.2. Граф переходов нерезервированной невосстанавливаемой системы (случай а).

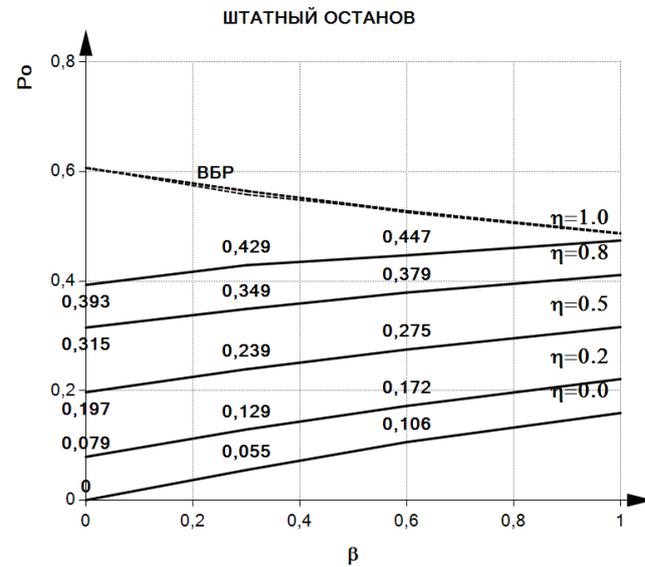
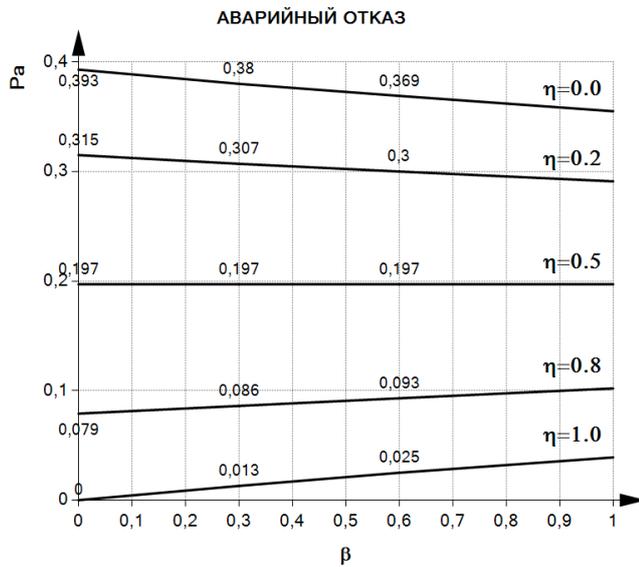


Рис. 2.3. Параметрический анализ (случай а).

б). В этом случае, аналогичном а), СК, как и основные средства, контролируется с полнотой  $\eta$ , а неконтролируемая часть СК имеет отказы двух типов. Критерий аварии тот же, что и в а), критерий остановки – контролируемый отказ системы и СК, ложное срабатывание неконтролируемой части СК. Граф переходов приведен на рис.2.4. На графиках (рис.2.5) приведены значения  $P_a$  и  $P_o$  при  $\theta = 0.5$  и  $\alpha = 0.5$ . При  $\beta = 0$  и (или)  $\eta = 0$  вероятность безотказной работы  $P$  одинакова с предыдущим случаем, при других значениях  $\beta$  и  $\eta$  – уменьшается за счет более быстрого числа остановок по сравнению с убыванием числа аварий. Здесь также имеет место независимость  $P_a$  от  $\beta$ , но она наступает при  $\eta = 1$  и соответствует безаварийному режиму работы ( $P_a = 0$ ).

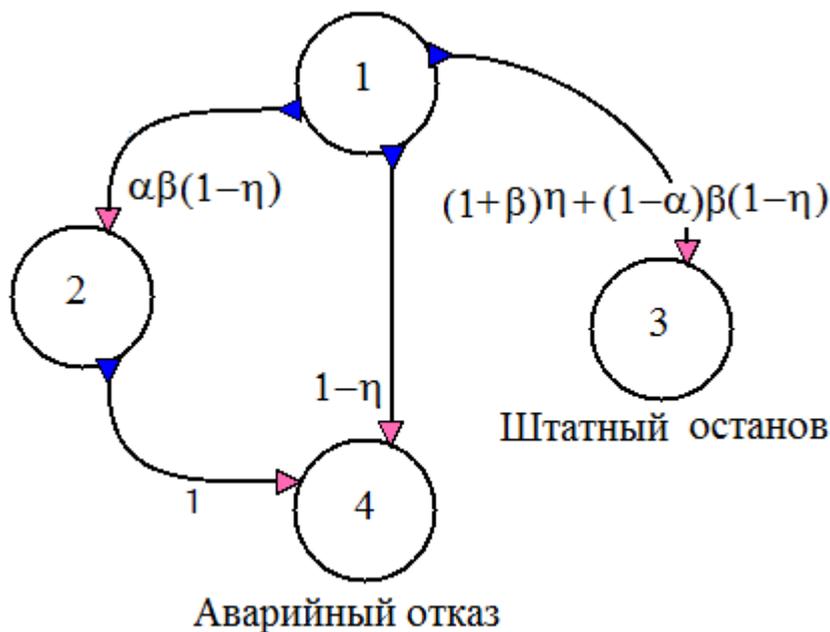


Рис. 2.4. Граф переходов нерезервированной невосстанавливаемой системы (случай б).

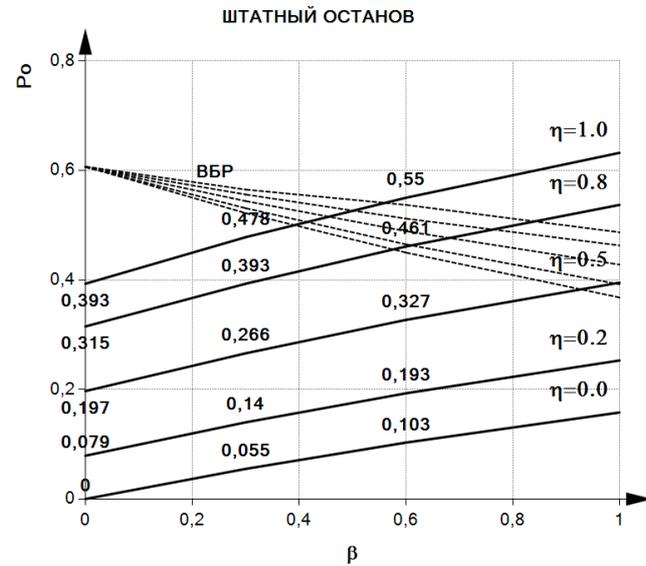
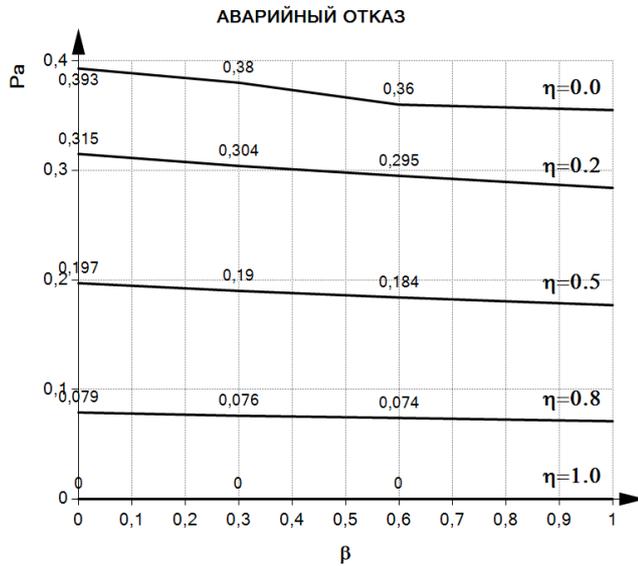


Рис. 2.5. Параметрический анализ (случай б).

в). Если предположить в случае б) возможность появления ложного срабатывания или контролируемого отказа СК после возникновения в них скрытого отказа (отказа типа несрабатывания), получим следующую модель работоспособности системы (рис. 2.6). Кривые  $P_a(\theta)$  и  $P_o(\theta)$  при  $\theta = \lambda t = 0.5$  и  $\alpha = 0.5$  приведены на рис. 2.7. По сравнению с предыдущими случаями здесь получен некоторый выигрыш в показателе  $P_a$ , но ухудшились показатели  $P$  и  $P_o$ .

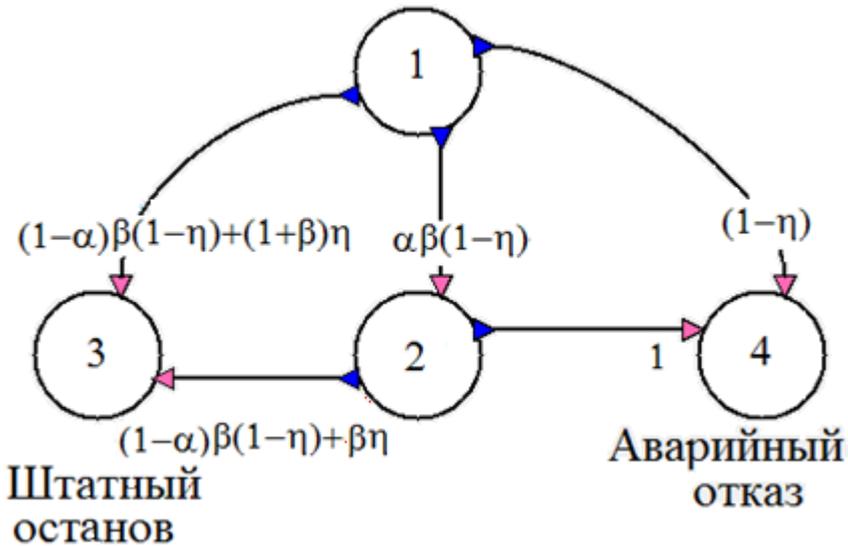


Рис. 2.6. Граф переходов нерезервированной невосстанавливаемой системы (случай в)

г). Ранее было принято, что контролируемый отказ СК ведет к отказу системы. Но можно использовать и другой алгоритм – ОУВС продолжает работу, если установлено, что отказ произошел в средствах контроля (рис.2.8). Такая стратегия улучшает показатели  $P$  и  $P_o$ , но несколько ухудшает значение  $P_a$  (рис.2.9). Имеется значение полноты контроля, при которой величина  $P_a$  и  $P_o$  не зависит от объема СК ( $\beta$ ). Для  $P_a$  это происходит при  $\eta \approx 0.345$ , для  $P_o$  при  $\eta = 0.7$  ( $\theta = \lambda t = 0.5$  и  $\alpha = 0.5$ ). Как и в случае а), здесь даже при полном контроле ( $\eta = 1$ ) остается возможность аварийного отказа системы.

Сравнение вариантов а)-г) по показателям  $P(\theta)$ ,  $P_o(\theta)$ ,  $P_a(\theta)$  при  $\theta = 0.5$  и  $\alpha = 0.5$  и различных значений  $\beta$  приведено в таблице 2.1, где

> означает “больше”. Выбор допустимых значений  $\beta$  и  $\eta$  в системе определяется требуемым соотношением  $P_0$  и  $P_a$ , которое устанавливается при рассмотрении модели более высокого уровня, учитывающей потери от отказов каждого типа.

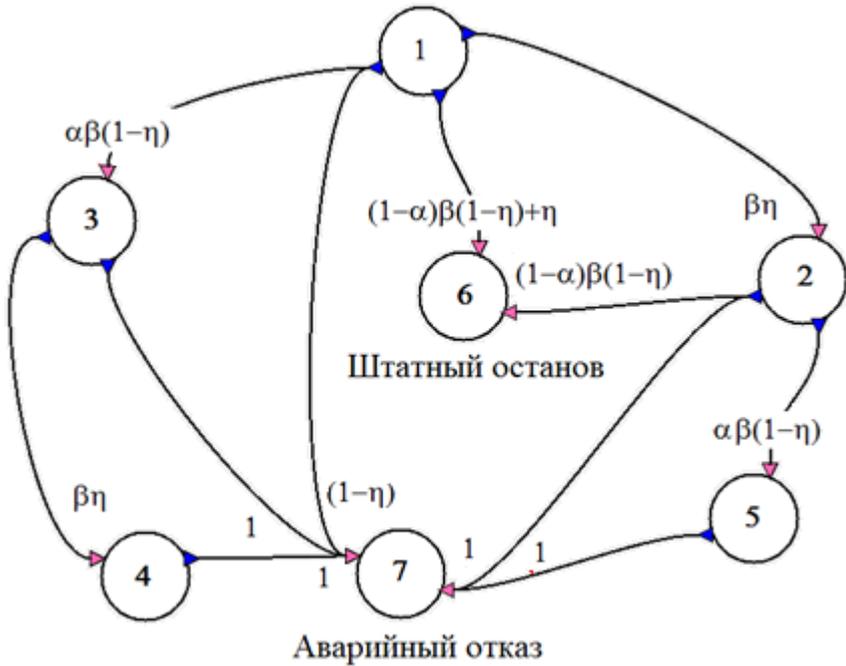


Рис.2.8. Граф переходов нерезервированной невозстанавливаемой системы (случай г).

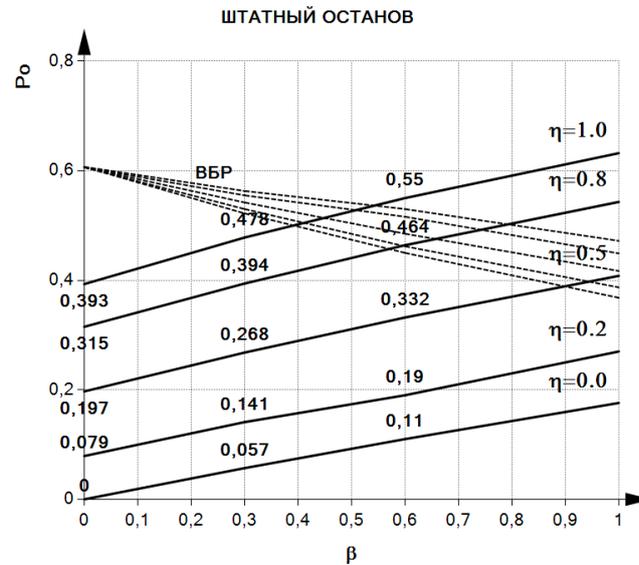
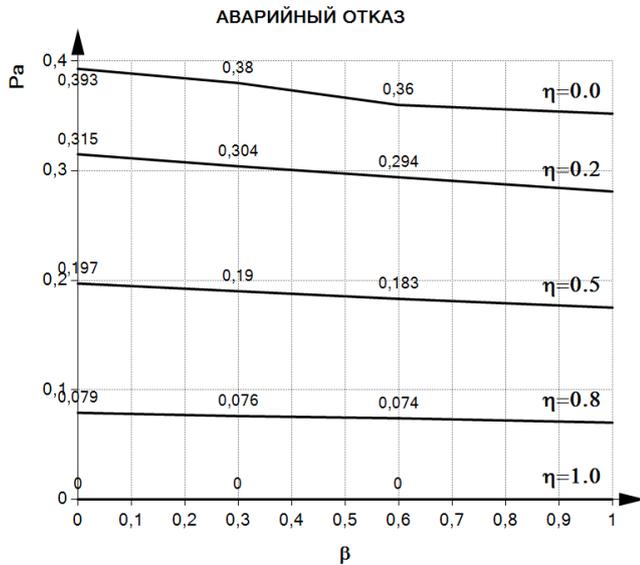


Рис.2.7. Параметрический анализ (случай в).

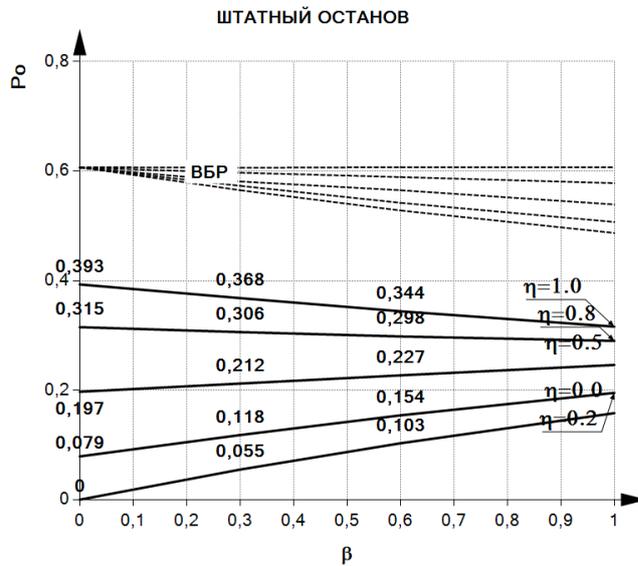
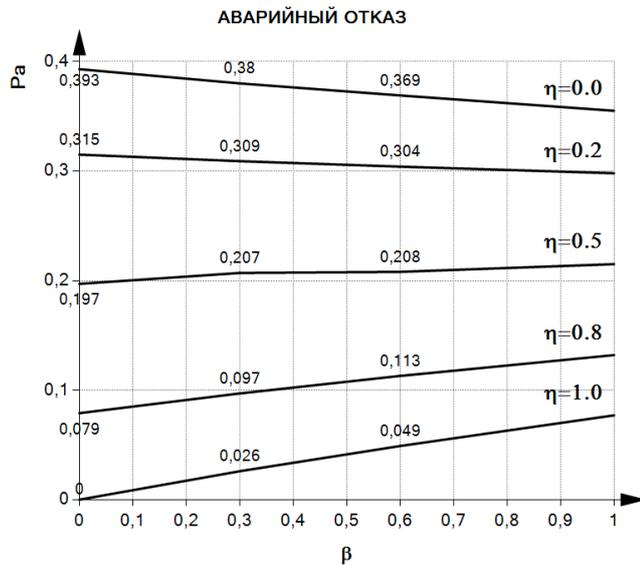


Рис.2.9. Параметрический анализ (случай г).

Таблица 2.1. Сравнение вариантов нерезервированных, невосстанавливаемых подсистем ОУВС.

	P	Pa	Po
0	4=1=2>3	3<1=2=4	3>1=2=4
0.4	4>1>2>3	3<2<1<4	3>2>1>4
0.9	4>1>2>3	3<2<1<4	3>2>1>4
1.0	4>1>2=3	3=2<1<4	2=3>1>4

### 2.3.2. Модели нерезервированных восстанавливаемых систем с подсистемой контроля

Рассматривается система типа а), в которой при отказе контролируемой части проводится восстановление с интенсивностью  $\mu$ . При отказе неконтролируемой части система попадает в состояние со скрытым отказом. Если во время пребывания в системе скрытого отказа происходит контролируемый отказ, то система полностью восстанавливается с интенсивностью  $\mu$ . После отказа контроля типа ложное срабатывание система восстанавливается, при несрабатывании средств контроля ОУВС отказывает. Граф работоспособности системы приведен на рис. 2.10. Состояния 1, 2 – работоспособные, 3, 6 – неработоспособные.

Графики функции готовности  $K(\theta)$  при  $\theta = 1$ ,  $\alpha = 0.5$  для различных значений  $\eta$  и  $\beta$  показаны на рис. 2.11. Значения  $K(\theta)$  не зависят от надежности средств контроля (от  $\beta$ ) при полноте контроля  $\eta \approx 0$ . При полноте контроля  $\eta \rightarrow 1$  влияние надежности СК на показатели надежности ОУВС становится ощутимым. Так, если при абсолютно надежных СК, составляющих 30% от всей аппаратуры ОУВС,  $K(1) = 0.9$  обеспечивается при  $\eta = 0.85$ , то учет их надежности потребует повышения  $\eta$  до величины 0.93. Здесь же можно определить необходимую эффективность дополнительных средств, вкладываемых в СК. Если достигнуто  $K(1) = 0.85$  при  $\beta = 0.35$  и  $\eta = 0.85$ , то получить  $K(1) = 0.9$  можно при увеличении  $\eta$  до 1 за счет  $\Delta\beta \leq 0.22$ , или при  $\eta \geq 0.95$  за счет  $\Delta\beta = 0.03$ . Приведенная взаимосвязь  $\beta$  и  $\eta$  зависит от величины  $K(\theta)$  при выбранном значении  $\theta$  и от  $\theta$ . Это объясняется неодинаковым влиянием  $\eta$  и  $\beta$  на форму функции  $K(\theta)$ . На рис. 2.12

приведены функции неготовности для различных сочетаний значений параметров  $\eta$  и  $\beta$ . Эквивалентность структур наступает при определенном значении наработки  $\theta$ .

Влияние надежности и полноты контроля на другие показатели рассмотрим на модели системы, представленной на рис. 2.13. Как и в предыдущем случае, после контролируемого отказа система восстанавливается с интенсивностью  $\mu_p$ . Кроме того, проводится техническое обслуживание системы с интенсивностью  $\mu_0$ , во время которого происходит полное восстановление системы, если в ней были скрытые отказы. Оценивались среднее время восстановления системы  $T_v$  и коэффициент готовности  $K_r$  при  $\mu_p = 1$ ,  $\mu_p/\lambda = 10^3$ ,  $\mu_p/\mu_0 = 720$  (ежемесячное обслуживание) и различных значениях  $\beta$  и  $\eta$ . Результаты показаны на графике рис. 2.14. Значения показателей  $T_v$  и  $K_r$  в сильной степени зависят от полноты контроля, а при  $\eta$  близких к 1 – и от надежности средств контроля  $\beta$ . На рис.2.14 приведены графики, отражающие взаимосвязь  $\beta$  и  $\eta$  при различных значениях коэффициента готовности. По графику можно определить: предельное значение  $K_r$  при известных значениях  $\beta$  и соответствующих им значениях  $\eta$ ; допустимые затраты аппаратуры для обеспечения величины  $\eta$ , необходимой для выполнения задания по  $K_r$ ; приращение полноты контроля  $\Delta\eta$ , обеспечивающее выигрыш в  $K_r$  при дополнительных затратах  $\Delta\beta$ .

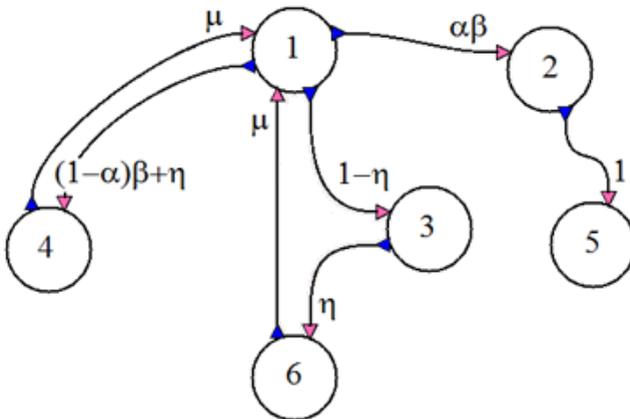


Рис. 2.10. Граф переходов нерезервированной восстанавливаемой системы.

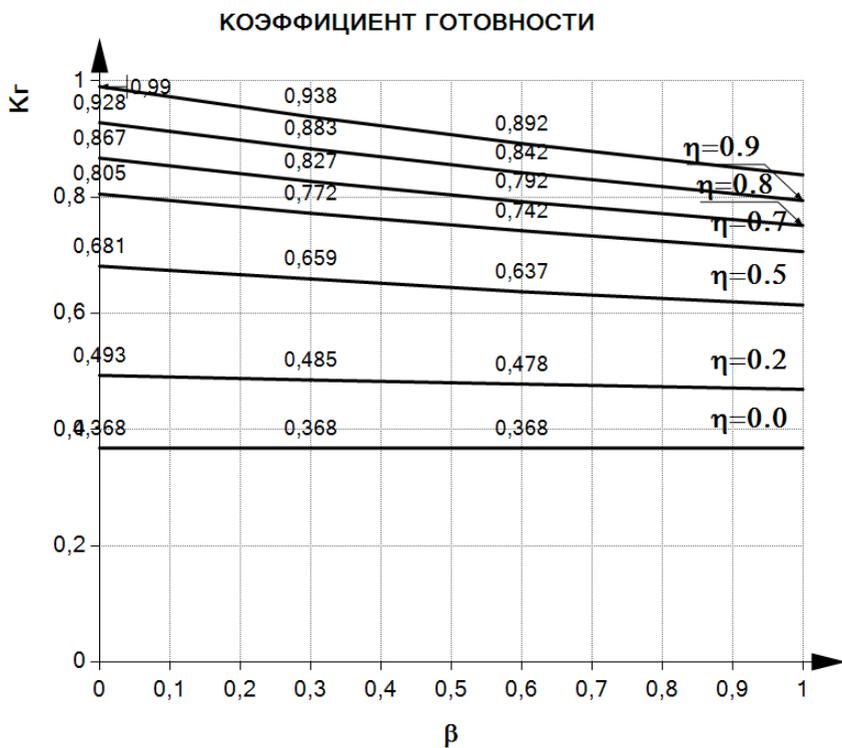


Рис. 2.11. Параметрический анализ готовности нерезервированной восстанавливаемой системы.

### Коэффициент простоя (t=1 ч.)

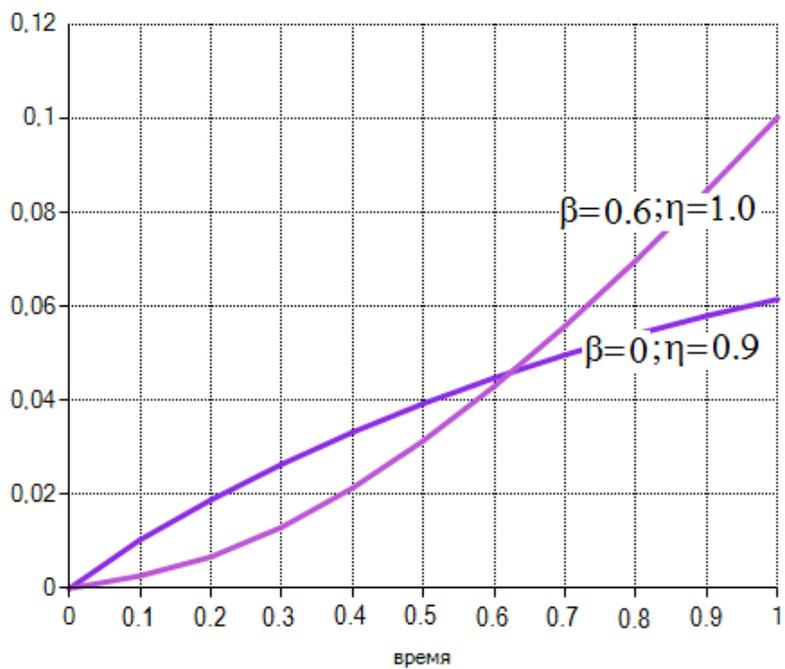


Рис. 2.12. Функция неготовности.

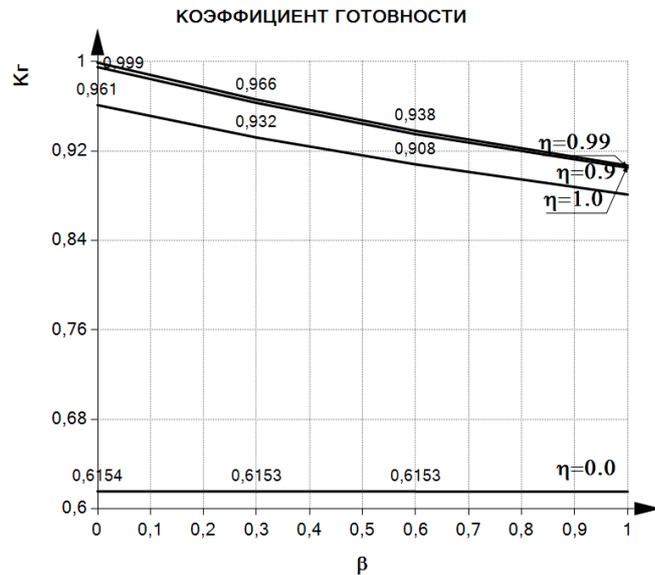
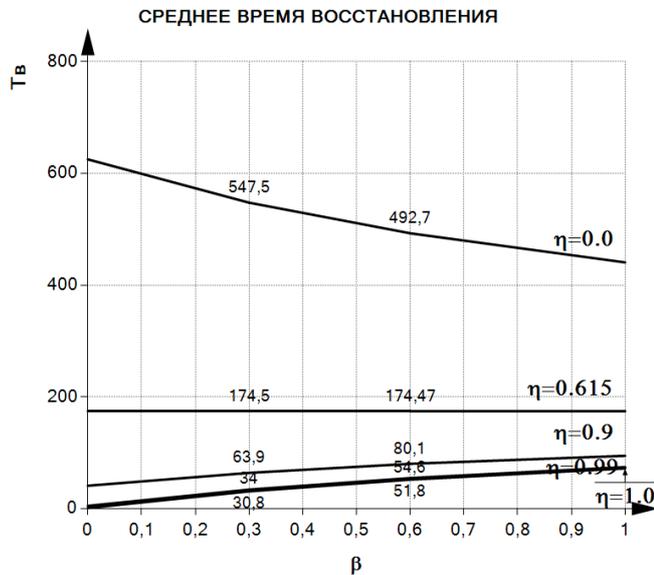


Рис. 2.14. Параметрический анализ готовности системы с восстановлением и периодическим обслуживанием.

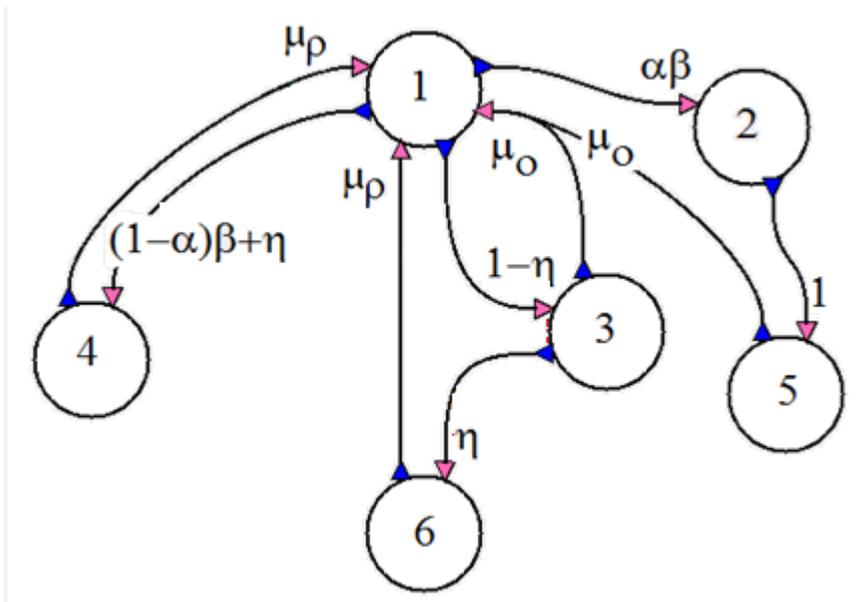


Рис. 2.13. Граф переходов нерезервированной восстанавливаемой системы с периодическим обслуживанием.

### 2.3.3. Модели резервированных систем с подсистемой контроля

Рассматриваемая дублированная система с подсистемой контроля. Подсистема контроля имеет два типа отказов – несрабатывание и ложное срабатывание. Система работает до последнего работоспособного элемента. При контролируемом отказе элементы ОУВС восстанавливаются, при неконтролируемом остаются в состоянии со скрытым отказом. Граф переходов системы приведен на рис. 2.15. Здесь: состояние 1 – исправное; 2 – оба элемента ОУВС работоспособны, в подсистеме контроля отказ типа несрабатывание; состояния 3-7 работоспособны при одном отказавшем элементе ОУВС и различных состояниях подсистемы контроля; состояние 8 – остановка вычислительного процесса из-за ложного срабатывания контроля; состояние 9 – отказ системы. Последние два состояния неработоспособные.



надежности на заданную величину. Как и в нерезервированном случае (2.3.2), здесь выводы и соотношения  $\beta$  и  $\eta$  справедливы для определенного интервала времени  $\theta$ .

Отказы типа ложное срабатывание в средствах контроля ( $\alpha \neq 1$ ) ухудшают показатели безотказности, что подтверждается графиками рис. 2.17, построенными для  $\alpha = 0.5$ .

Рассмотренные модели просты и выявляют достаточно сильную связь свойств средств контроля. Возможно это связь полноты контроля и надежности средств контроля будет менее явна на фоне многочисленных факторов, действующих в более сложных моделях систем. Однако пренебрегать зависимостью полноты контроля от надежности средств контроля при анализе работоспособности ОУВС недопустимо. И если отказы СК типа несрабатывание снижают полноту контроля ОУВС, то отказы типа ложное срабатывание непосредственно влияют на безотказность вычислительного модуля, приводя к дополнительным прерываниям вычислительного процесса.

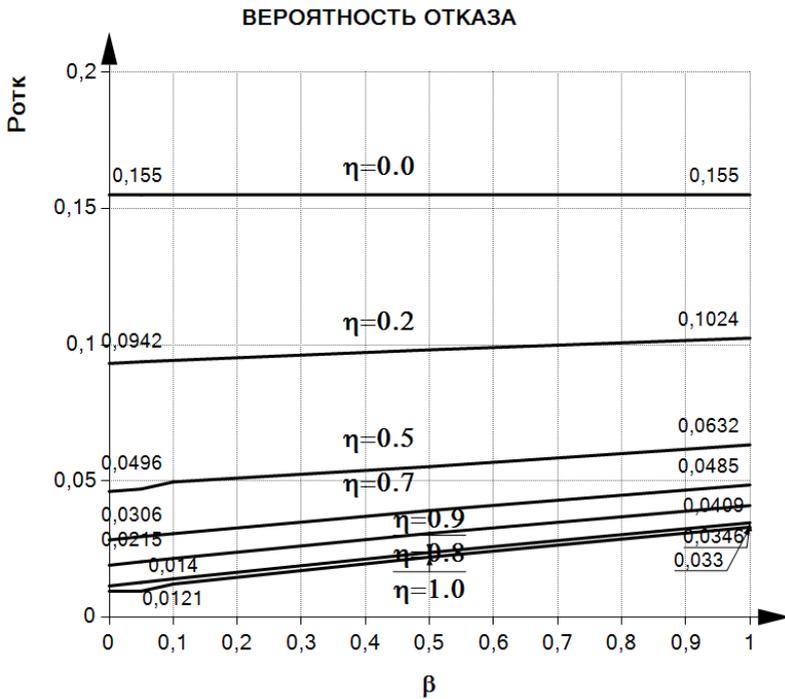


Рис. 2.16. Параметрический анализ резервированной системы с восстановлением ( $\alpha = 1$ ).

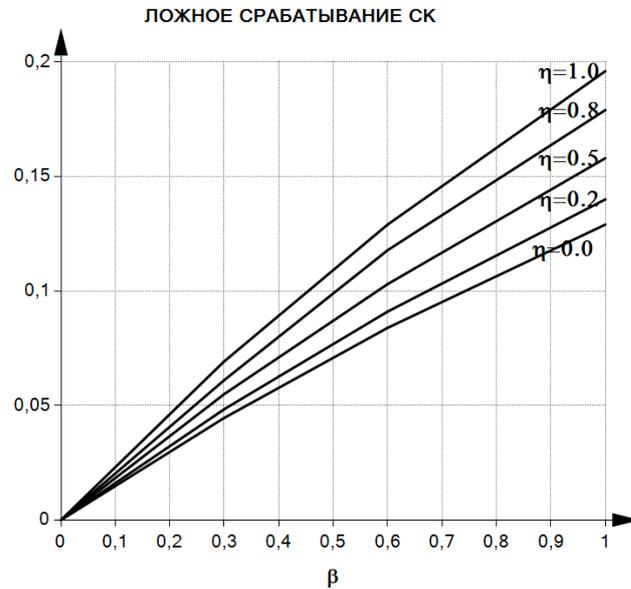
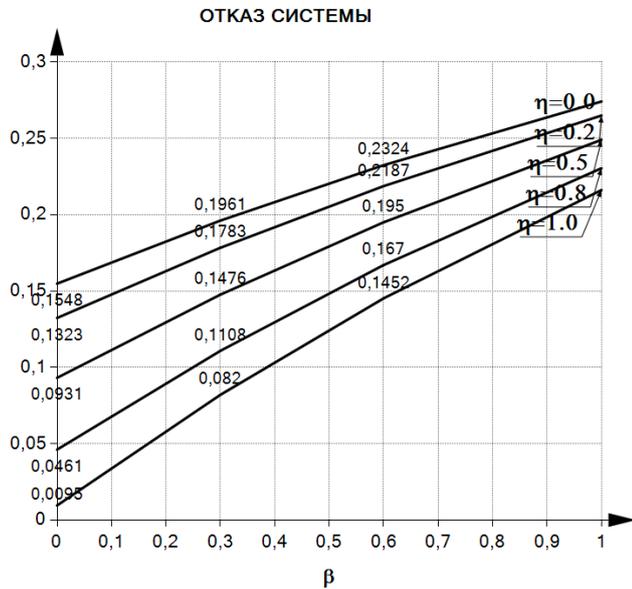


Рис. 2.17. Параметрический анализ резервированной системы с восстановлением ( $\alpha = 0.5$ ).

### 3. АНАЛИЗ НАДЕЖНОСТИ ОУВС МЕТОДОМ АГРЕГИРОВАНИЯ МАРКОВСКИХ МОДЕЛЕЙ

В первом разделе настоящей книги были рассмотрены однородные ОУВС, т.е. системы, состоящие из резервированных подсистем с одинаковой технической структурой и с однотипной реакцией элементов на возникшую неисправность. Однородность поведения и технической структуры системы снижает размерность моделей и позволяет решить задачу анализа надежности, оставаясь в рамках марковских моделей без привлечения логико-вероятностного моделирования [39, 40]. Общий подход к моделированию надежности однородных ОУВС основывался на раздельном построении марковских моделей обработки неисправностей и моделей деградации технической структуры ОУВС. Используемые приемы агрегирования марковских моделей основывались на укрупнении состояний сбой и отказ в одно состояние и корректировки интенсивностей выхода из укрупненного состояния с учетом успешности завершения процедур парирования сбоев. В разделе 1.2 был проведен анализ результатов расчетов показателей надежности на моделях с укрупнением и было показано, что укрупнение существенно различных состояний (сбой, из которого есть возврат в исходное состояние; отказ, из которого принципиально отсутствует возврат в исходное состояние) порождает значительную относительную погрешность вычисления. Некорректность использования подобного укрупнения усугубляется тем, что при вычислении такого показателя как вероятность отказа оно дает оценку снизу. Для дублированной ОУВС, для которой возможно получение аналитического решения марковской модели надежности, были рассмотрены следующие случаи: (1) укрупнение проводится при моделировании быстрых процессов обработки неисправностей; (2) укрупнение проводится при моделировании медленных процессов деградации технической структуры ОУВС. Сравнение значений показателя вероятности отказа, полученных на точной модели без укрупнения состояний сбой и отказ и на моделях (1) и (2), позволило выявить два параметра, в наибольшей степени влияющих на погрешность вычисления – доля сбоев и средняя длительность сбоя. В зависимости от изменения параметра доля сбоев относительная ошибка вычисления вероятности отказа в модели (1) изменялась от 0

до 25%. При уменьшении средней длительности сбоя модель (1) порождала ошибки от 0 до 80%. Верхняя граница относительной ошибки, порождаемой моделью (2), приближалась к 100%.

В данном разделе будет предложена свободная от выявленных недостатков агрегированная модель надежности ОУВС, в которой медленный процесс деградации технической структуры описывается марковским процессом с непрерывным временем, а быстрый процесс обработки неисправностей – дискретной марковской цепью. Техника интеграции модели обработки неисправностей в общесистемную модель надежности, основывается на раздельном рассмотрении событий возникновения постоянных отказов и сбоев.

Работа агрегированной модели будет продемонстрирована на примере анализа отказоустойчивой вычислительной системы, представляющей собой резервированную структуру из трех полносвязных машин. Отдельная вычислительная машина (ВМ) состоит из базовой части (БЧ), адаптера связи с абонентом (А), приемо-передатчика межмашинного обмена (П/П).

### **3.1. Факторы модели надежности ОУВС**

Критерием отказа анализируемой ОУВС является невозможность правильной работы не менее, чем по двум (из трех) каналам связи с абонентом внешней среды.

Факторами, учитываемыми при построении модели надежности, явились:

- возможность возникновения двух типов неисправностей – постоянных отказов и сбоев
- отсутствие восстановления работоспособности ОУВС, нарушенной возникновением постоянных отказов
- наличие резервирования (троирование) базовых и периферийных частей
- введение специальных процедур обработки сбоев базовых частей машин
- наличие видов отказов (например, пробой по питанию) элементов небазовой части ОУВС (адаптер, приемник-передатчик), которые могут привести к неисправности базовой части

Исследование «надежностного поведения» ОУВС с учетом специальных процедур обработки сбоев выполняется на марковских моделях надежности.

Процедура обработки неисправностей рассматривается как последовательность  $k$  программных попыток восстановления нормального хода вычислительного процесса ((перезапись памяти, повторы сегментов программ, откаты на контрольные точки...)). Предполагается, что неуспех  $i$ -ой попытки восстановления может быть вызван тремя факторами

- длительность сбоя (как физического явления) превышает длительность  $i$ -ой попытки восстановления
- за время выполнения  $i$ -ой попытки восстановления произошел повторный сбой восстанавливаемой базовой части ОУВС
- за время выполнения  $i$ -ой попытки восстановления произошел сбой или отказ других частей ОУВС

Кроме того, предполагается, что часть отказов и сбоев может носить катастрофический характер (система переходит в отказ, минуя деградацию).

Общий подход к моделированию заключается в раздельном построении моделей обработки неисправностей и моделей деградации технической структуры ОУВС. На модели обработки неисправностей рассчитываются вероятности успеха и неуспеха восстановления по сбоям, с помощью которых корректируются интенсивности переходов модели деградации технической структуры.

### **3.2. Модель обработки неисправностей**

Модель обработки неисправностей, возникающих в ОУВС, представляет собой дискретный марковский процесс, показанный на графе, приведенном на рис. 3.1. Дискретность времени процесса определяется тем, что переход в состояния выполнения  $i$ -ой процедуры восстановления, успешного или неуспешного завершения восстановления возможен лишь в строго определенных моменты времени, определяемые протоколом отказа-сбоеустойчивого обмена данными базовых частей ОУВС. Возможная реализация такого протокола описана в [4, 5].

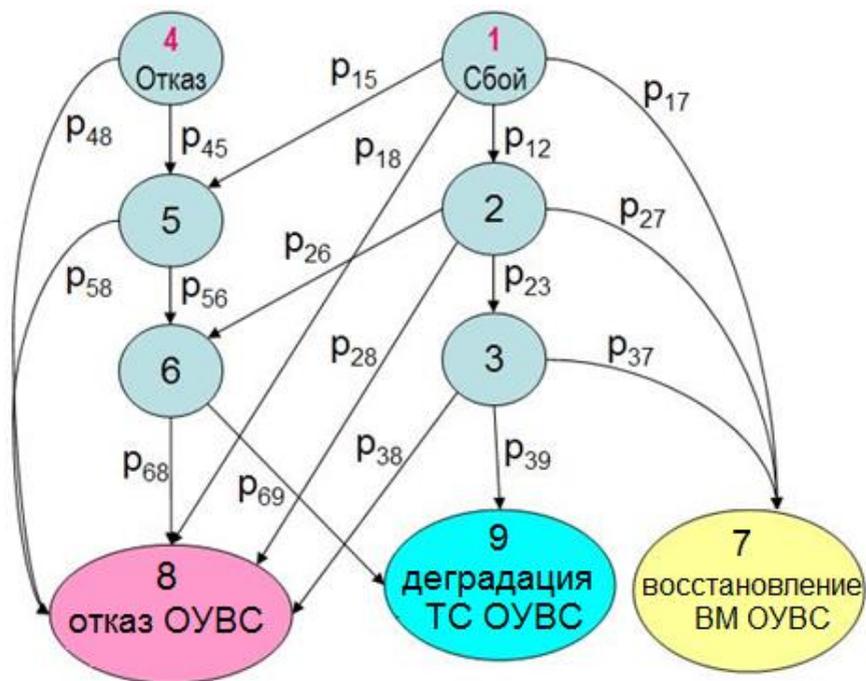


Рис. 3.1. Марковский граф процесса обработки неисправностей ОУВС ( $k = 3$ )

Состояния 2 и 5 графа соответствуют неуспешному завершению первой попытки программного восстановления по сбоям. Состояния 3 и 6 – неуспеху второй попытки. Всего в системе реализовано три попытки восстановления. Состояние 7 – успех программного восстановления сбившейся вычислительной машины. Состояние 8 – отказ системы в целом, который происходит по вине возникновения катастрофических неисправностей и (или) неисправностей, возникающих во время проведения восстановления. Состояние 9 – отключение (блокировка) сбившихся (отказавших) частей ОУВС ввиду неуспеха программных восстановительных операций.

Элементы матрицы переходов  $P$  находятся из следующих соотношений:

$$\begin{aligned}
p_{12} &= q_B, p_{15} = q_{\text{отк}}, p_{17} = p_B, p_{18} = q_{\text{ко}} \\
p_{23} &= q_B, p_{26} = q_{\text{отк}}, p_{27} = p_B, p_{28} = q_{\text{ко}} \\
p_{37} &= p_B, p_{38} = q_{\text{ко}}, p_{39} = q_B + q_{\text{отк}} \\
p_{45} &= 1 - q_{\text{ко}}^0, p_{48} = q_{\text{ко}}^0 \\
p_{56} &= 1 - q_{\text{ко}}^0, p_{58} = q_{\text{ко}}^0 \\
p_{69} &= 1 - q_{\text{ко}}^0, p_{68} = q_{\text{ко}}^0
\end{aligned} \tag{3.1}$$

Вероятность успешного восстановления по сбоям:

$$p_B = p_{\text{нс}} p_2 (1 - q_{\text{отк}}) (1 - p_t) (1 - q_{\text{сб}}), \tag{3.2}$$

Где  $p_2 = e^{-2(\lambda_{\text{сб}} + \lambda_{\text{б}} + \lambda_{\text{нб}})\tau}$  - вероятность отсутствия сбоя или отказа с двумя другими машинами,

$\lambda_{\text{сб}}$  - интенсивность отказов базовой части ОУВС,

$\lambda_{\text{нб}}$  - интенсивность отказов небазовой части ОВС,

$p_{\text{нс}}$  - условная вероятность возникновения некатастрофического сбоя,

$p_{\text{но}}$  - условная вероятность возникновения некатастрофического отказа,

$p_t = e^{-\tau/\sigma}$  - вероятность того, что длительность сбоя ( $\sigma$ ) превышает время одной попытки восстановления ( $\tau$ ),

$q_{\text{сб}} = 1 - e^{-\lambda_{\text{сб}}\tau}$  - вероятность повторного сбоя машины во время ее восстановления,

$q_{\text{отк}} = 1 - e^{-(\lambda_{\text{б}} + \lambda_{\text{нб}})\tau}$  - вероятность отказа машины во время ее восстановления.

Вероятность неуспеха восстановления по сбоям:

$$q_B = p_{\text{нс}} p_2 (1 - q_{\text{отк}}) ((1 - p_t) q_{\text{сб}} + p_t) \tag{3.3}$$

Вероятность перехода в отказ во время восстановления:

$$q_{\text{ко}} = 1 - p_{\text{нс}} + p_{\text{нс}} (1 - p_2) \tag{3.4}$$

Вероятность перехода в отказ системы во время бессмысленного восстановления по сбоям машины, в которой на самом деле произошел постоянный отказ

$$q_{\text{ко}}^0 = 1 - P_{\text{но}} P_2 \quad (3.5)$$

Переходная матрица  $P$  и вектор начальных условий  $p(0)$  позволяют вычислить распределение финальных вероятностей за  $n$  шагов, как  $[0, 0, 0, 0, 0, 0, p_7(n), p_8(n), p_9(n)] = p(0)P^n$ . Причем, если  $p(0) = [1, 0, 0, 0, 0, 0, 0, 0, 0]$ , т.е. моделируется событие возникновения постоянного отказа, то при  $n \geq 3$   $p_7(n) = 0$ ,  $p_8(n) = P_{\text{F}}$ ,  $p_9(n) = P_{\text{D}}$ . Если рассматривается возникновение сбоя, то  $p(0) = [0, 0, 0, 1, 0, 0, 0, 0, 0]$  и при  $n \geq 3$   $p_7(n) = P_{\text{r}}$ ,  $p_8(n) = P_{\text{f}}$ ,  $p_9(n) = P_{\text{d}}$ . Таким образом, минуя укрупнения состояний сбой и отказ, получены коэффициенты, корректирующие интенсивности переходов непрерывной марковской модели надежности ОУВС. Для вычисления распределения вероятностей финальных состояний дискретного марковского процесса была создана специализированная программа анализа эффективности процедур восстановления по сбоям.

### 3.3. Модель деградации технической структуры ОУВС

Модель деградации представляет собой непрерывный марковский процесс с дискретным множеством состояний, показанный на графе, приведенном на рис. 3.2

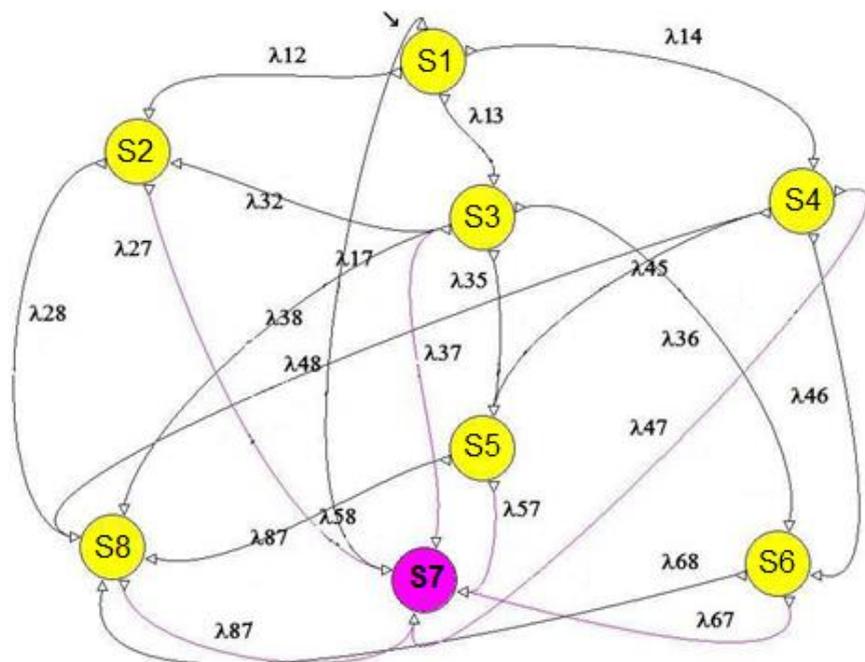


Рис. 3.2 Марковский граф деградации технической структуры ОУВС

Состояния Марковской модели:

S1 – система исправна

S2 – работают две машины, одна заблокирована

S3 – работают три машины, но у одной из машин отказала 1 межмашинная связь

S4 – работают три машины, но у одной отказала связь с абонентом

S5 – работают две машины на 2 канала связи с абонентом

S6 – работают две машины на 2 канала связи с абонентом

S7 – отказ СК

S8 – одна машина работает, вторая – “подслушивает” и транслирует связь с абонентом

Интенсивности переходов марковской модели:

$$\begin{aligned}
\lambda_{12} &= 3\lambda_{\Sigma}P_D + 3\lambda_{\text{сб}}, & \lambda_{13} &= 6\lambda_{\text{pp}}, & \lambda_{14} &= 3\lambda_a, \\
\lambda_{17} &= 3\lambda_{\Sigma}P_F + 3\lambda_{\text{сб}}P_f \\
\lambda_{27} &= 2(\lambda_{\Sigma} + \lambda_a + \lambda_{\text{pp}} + \gamma\lambda_{\text{сб}}), \\
\lambda_{23} &= 2 \cdot (1 - \gamma)\lambda_{\text{сб}} \\
\lambda_{32} &= \lambda_{\Sigma}P_D + 2\lambda_{\text{pp}} + \lambda_a + \lambda_{\text{сб}}P_D, & \lambda_{36} &= \lambda_a, \\
\lambda_{37} &= \lambda_{\Sigma} + \gamma\lambda_{\text{сб}} + \lambda_{\Sigma}P_f + \lambda_{\text{сб}}P_f, & \lambda_{38} &= (1 - \gamma)\lambda_{\text{сб}} \quad , \quad (3.6) \\
\lambda_{45} &= 4\lambda_{\text{pp}} + \lambda_{\Sigma}P_D, & \lambda_{46} &= 2\lambda_{\text{pp}}, \\
\lambda_{47} &= 2(\lambda_{\Sigma} + \lambda_a + \gamma\lambda_{\text{сб}}) + \lambda_{\Sigma}P_f, & \lambda_{48} &= 2 \cdot (1 - \gamma)\lambda_{\text{сб}} \\
\lambda_{57} &= 2(\lambda_{\Sigma} + \lambda_a + \lambda_{\text{pp}} + \gamma\lambda_{\text{сб}}), & \lambda_{58} &= 2 \cdot (1 - \gamma)\lambda_{\text{сб}} \\
\lambda_{67} &= 3(\lambda_{\Sigma} + \gamma\lambda_{\text{сб}}) + 4\lambda_{\text{pp}} + 2\lambda_a, & \lambda_{68} &= 3 \cdot (1 - \gamma)\lambda_{\text{сб}} \\
\lambda_{87} &= 2(\lambda_{\Sigma} + \lambda_a + \lambda_{\text{pp}} + \lambda_{\text{сб}})
\end{aligned}$$

где  $\lambda_{\Sigma} = \lambda_{\text{сб}} + \lambda_{\text{нб}}$ ;  $\lambda_{\text{pp}}$  – интенсивность отказов прямо-передатчика;  $\lambda_a$  – интенсивность отказов адаптера,  $(1 - \gamma)$  – доля отказов небазовой части, приводящей к отказу базовой.

Осуществляя расчеты при варьировании параметров модели, можно исследовать многие аспекты надежности ОУВС. В частности, ответить на вопросы о том, какой вклад в общую ненадежность системы вносят сбои, насколько удастся повысить надежность ОУВС за счет введения специальных процедур обработки сбоев. Для ответа на эти вопросы были проведены расчеты, сведенные в таблицу 3.1. Расчеты выполнены для следующих значений параметров модели и интенсивностей отказов подсистем ОУВС: интенсивность отказов базовой части  $\lambda_{\text{сб}} = 4 \cdot 10^{-6}$ , интенсивность отказов небазовой части  $\lambda_{\text{нб}} = 0,6 \cdot 10^{-6}$ , интенсивность отказов прямо-передатчика  $\lambda_{\text{pp}} = 0,9 \cdot 10^{-6}$ , интенсивность отказов адаптера  $\lambda_a = 0,6 \cdot 10^{-6}$ , доля отказов небазовой части, не влияющей на отказы базовой  $\gamma = 0,3$ . Параметры процедуры восстановления по сбоям: число попыток восстановления  $k = 3$ , средняя длительность сбоя  $\sigma = 10$ мс, длительность одной попытки восстановления  $\tau = 20$ мс, интенсивность потока сбоев в 100 раз превышает интенсивность постоянных отказов ОУВС. Время функционирования системы 8760ч (1 год).

Расчеты проводились на программном обеспечении PTC Windchill Quality Solutions – WQS (прежнее название Relex). Расчеты интенсивностей отказов элементной базы подсистем ОУВС проводились по моделям MIL-HDBK-217 FN2 для коммерческого уровня изготовления и приемки в модуле прогнозирования безотказности (WQS Reliability Prediction). Вычисление показателей вероятности безотказной ОУВС было осуществлено в модуле марковского моделирования надежности (WQS Markov) [23-26].

Таблица 3.1. Результаты расчета показателей надежности ОУВС

Показатели	Вид расчета		
	Расчет по постоянным отказам без учета сбоев	Расчет по сбоям и постоянным отказам без учета специальных процедур обработки неисправностей	Расчет по сбоям и постоянным отказам с учетом специальных процедур обработки неисправностей
Вероятность безотказной работы	<b>0,992122</b>	<b>4,137050E-03</b>	<b>0,848385</b>
Вероятность отказа	<b>7,878300E-03</b>	<b>0,995863</b>	<b>0,151615</b>

Анализ отказоустойчивого трехмашинного вычислительного комплекса на предложенной модели подтверждает факт существенной зависимости надежности ОУВС от сбоев. Неучет в моделях надежности ОУВС сбоев приводит к получению необоснованно завышенных оценок показателей надежности. В тоже время, если в моделях надежности будут учитываться сбои, но не будет отражен факт просеивания потока сбоев введением специальных процедур восстановления, то будет получена недопустимо заниженная оценка надежности системы.

#### **4. АНАЛИЗ НАДЕЖНОСТИ ОУВС МЕТОДОМ АГРЕГИРОВАНИЯ ЛОГИКО-ВЕРОЯТНОСТНЫХ И МАРКОВСКИХ МОДЕЛЕЙ**

В процессе создания моделей надежности ОУВС возникает противоречие, связанное со стремлением наиболее полного учета факторов, определяющих надежность, с одной стороны, и необходимостью преодоления большой размерности, с другой стороны. Решением проблемы является проведение декомпозиции ОУВС, построение адекватных моделей выделенных частей и агрегирование полученных моделей, либо уже вычисленных показателей для частей системы в общесистемную модель или показатели. В предыдущем разделе анализ надежности трехмашинной системы был осуществлен с помощью агрегации марковских моделей. Ограничиться только марковскими моделями позволила невысокая структурная сложность системы. Если пространство “надежностных” состояний, характеризующихся различными сочетаниями отказавших и работоспособных элементов системы, имеет большую размерность, то разумным является сочетание логико-вероятностных и марковских моделей. Удачным выбором здесь является комбинация логико-вероятностных моделей деревьев отказов и марковского моделирования при сохранении мнемоники деревьев отказов. В деревья отказов внедряются динамические операторы (динамические вершины), учитывающие развитие процесса возникновения базовых событий во времени с помощью марковских моделей. Эти агрегированные модели называют динамическими деревьями отказов [27, 28]. В данном разделе будет рассмотрена отказоустойчивая вычислительная система со сложным “надежностным поведением”, в которой реализована постепенная деградация технической структуры и внедрены различные процедуры обработки неисправностей для различных частей системы. Для выполнения анализа надежности этой ОУВС будет построено обобщенное динамическое дерево отказов, каждое базовое событие которого раскрывается вложенным деревом, марковским графом, комбинаторной моделью.

#### **4.1. Описание функционирования и структурно-надежный анализ ОУВС**

Функциональная структура резервированной вычислительной системы, описанной в [4, 5, 9, 10], приведена на рис. 4.1. Каждая из вычислительных машин (ВМ) имеет по две тройки устройств связи (УС). Система обеспечивает прием информации из внешней среды и выдачу управляющих воздействий. В процессе функционирования системы при возникновении неисправностей (отказов элементов) она деградирует. Деградация происходит по сложной “траектории”, начальным состоянием является трехмашинная конфигурация, а конечным – состояния, соответствующие отказам системы. В процессе деградации система может принимать двухмашинную конфигурацию с блокировкой третьей ВМ и одномашинную, при которой одна ВМ осуществляет обмен с внешней средой, другая работает в режиме “подслушивания” (контроля) работающей, а третья заблокирована. Возможны два вида отказа системы в целом – отказ, при котором система выдает во внешнюю среду приоритетную команду безопасного останова (БО), и отказ, при котором не обеспечена выдача команды БО, и внешняя среда либо не воспринимает управляющих команд от системы, либо система выдает неверные команды. Отказ второго вида будет называться опасным отказом (ОО).

Верхние (по изображению на рис. 4.1) УС обеспечивают два режима работы системы – режим обмена с абонентскими устройствами (АУ) по мультиплексным каналам (МК) А, Б, В взаимодействия с внешней средой и режим межмашинного согласования. Нижние УС работают только в режиме межмашинного согласования. Верхние и нижние УС образуют по три МК обмена или согласования в соответствии с режимом работы системы (в МК входит по одному УС от каждой ВМ). Верхние МК составляют сеть обмена (СО), верхние и нижние – сеть согласования (СС). В режиме согласования верхние и нижние МК взаимно резервируют друг друга, образуя суммарно 6 каналов согласования. Отказ любого одного УС – отказ канала в режиме согласования.

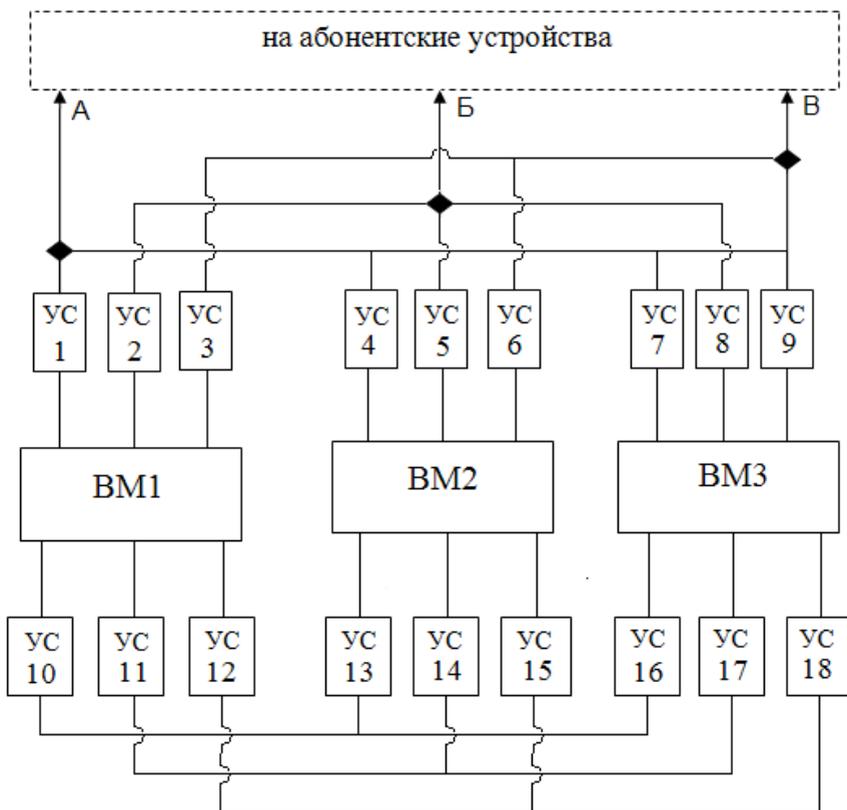


Рис.4.1. Функциональная структура трехмашинной ОУВС

С конфигурацией системы связано понятие полноты сети согласования – количество МК согласования, обеспечивающее конкретную конфигурацию. Для обеспечения полноты сети согласования необходимо

- в трехмашинной конфигурации – три полностью работоспособных МК
- в двухмашинной конфигурации – два полностью работоспособных МК
- в одномашинной конфигурации – один полностью работоспособный МК

Причем в двухмашинной и одномашинной конфигурациях каждый МК состоит только из двух УС, исключая УС первой заблокированной ВМ в трехмашинной конфигурации.

Недостаточность указанной полноты сети согласования приводит к переходу в режим с меньшим количеством ВМ – т.е. полнота сети согласования является одним из критериев деградации системы. Другой критерий деградации (отказа) системы обусловлен необеспечением минимум двух каналов обмена с АУ из трех (А, Б, В). Нарушение обмена с АУ связано с отказами УС обмена (верхних на рис. 4.1) и ВМ.

Для описания надежностного поведения всех УС принимается бинарная модель, т.е. каждый УС может находиться в двух состояниях – работоспособном и неработоспособном, причем состояние УС идентифицируется со 100% достоверностью. Каждая из ВМ описывается тремя состояниями – одним работоспособным и двумя неработоспособными, в соответствии с двумя выделенными видами отказов. Один вид назовем *благоприятным отказом* (этот отказ выявляется самой отказавшей ВМ и позволяет ей самоблокироваться и осуществлять режим “подслушивания”), другой – *неблагоприятным* (отказ, не позволяющий ВМ самоблокироваться). Неблагоприятный отказ одной из ВМ может как обнаруживаться, так и не обнаруживаться с помощью других ВМ. Любой первый отказ ВМ в трехмашинной конфигурации всегда выявляется и приводит к ее блокировке. В двухмашинной конфигурации любой отказ ВМ выявляется, но при неблагоприятном отказе осуществляется переход в безопасный останов, а при благоприятном в одномашинный режим. Из одномашинной конфигурации можно попасть в БО или в ОО в зависимости от вида отказов ВМ и набора технических состояний УС (работоспособности, неработоспособности). Таким образом, верхние УС каждого из МК в режиме обмена с точки зрения надежности резервируют друг друга, а сами МК образуют структуру “2 из 3”. Ранее указывалось, что при согласовании эти УС реализуют другую структуру. То, что одни и те же УС образуют различные структурные надежностные схемы (в зависимости от режима их использования – согласования или обмена) является одной из особенностей рассматриваемой вычислительной системы и *не позволяет привести ее надежностную структуру к комбинации последовательно-параллельных схем и мажоритарных схем вида “к из т”*.

Вторая особенность связана с необходимостью учета в некоторых ситуациях последовательности возникновения отказов, что обуславливается видами отказов ВМ и системы в целом.

И, наконец, третья особенность рассматриваемой системы заключается в использовании специальных алгоритмов восстановления вычислительного процесса, нарушенного сбоями, влияние которых на функционирование системы должно быть отражено в надежной модели.

Реакция системы на возникшую неисправность организована следующим образом. При нарушении нормального хода работы системы в результате отказа или сбоя ее структурного элемента (УС, ВМ) этот элемент программным путем исключается из конфигурации, соответствующей данному режиму работы системы (обмену, согласованию), и этот режим завершается с использованием резервных элементов. Исключенный элемент фиксируется. Решение о возможности дальнейшего использования исключенного элемента принимается на основе двух критериев.

Первый критерий (“частотный”): элемент признается отказавшим, если до конца интервала работы счетчика будет дополнительно зафиксировано ( $m_{кр1}-1$ ) нарушений функционирования у данного элемента. Второй критерий (“последовательностный”): элемент признается отказавшим, если после первого нарушения его функционирования нарушения будут происходить еще ( $m_{кр2}-1$ ) раз подряд.

Первый критерий применяется для УС, работающих в режиме обменов с внешней средой. Нарушение функционирования УС фиксируется в случае, если на одном цикле обменов ( $\Delta t_{об}$ ) возникает хотя бы одна неисправность.

Второй критерий применяется для УС, работающих в режиме согласования, и для ВМ. Нарушение функционирования ВМ фиксируется по результатам работы на интервале длиной  $\Delta t_{ВМ.}$ , для УС – при нарушении в одном цикле согласования ( $\Delta t_c$ ).

Таким образом, устройства связи, работающие в двух режимах (обмена, согласования), признаются отказавшими по любому из перечисленных двух критериев, сработавшему первым. Если критерий не “отрабатывает”, то накопленная информация по неисправностям “забывается”, т.е. если, например, по второму критерию произошло не более ( $m_{согл.кр.}-1$ ) сбоев подряд, при следующем согласовании сбоевшее устройство работало правильно, то начинается новый отсчет

критического числа  $m_{\text{согл.кр.}}$ . Аналогично с частотным критерием при наступлении нового интервала работы счетчика.

#### 4.2. Построение агрегированной модели надежности ОУВС

Для построения агрегированной модели надежности ОУВС выполним следующие действия:

1. В качестве основного блока ОУВС, отказы которого оказывают наиболее существенное влияние на надежностное поведение системы в целом, выделим трехмашинный блок ВМ. Причем, учтем, что каждая ВМ имеет два различных по последствиям неработоспособных состояния.
2. Построим обобщенное дерево отказов системы (ДО). Обобщенное ДО имеет пять ветвей, каждая из которых описывает возникновение несовместных событий, обусловленных разложением состояний блока ВМ на полную группу несовместных событий (4 события: 0, 1, 2, 3 отказавших ВМ). Причем событие, соответствующее трем работоспособным ВМ, разделено на два события (трехмашинный и двухмашинный режим работы). Это связано с возможностью возникновения отказов УС СО и СС, которые при трех исправных ВМ переведут систему в двухмашинный режим работы. Четвертая ветвь, соответствующая трем отказавшим ВМ, объединена через операцию И (AND) с отказами УС для отражения двух видов отказа системы в целом – БО и ОО, т.к. различные комбинации отказов элементов приведут и к различным видам отказа системы. Если отказы системы не дифференцировать по видам и интересоваться только безотказной работой (это соответствует объединению БО и ОО в одно состояние неработоспособности), то по четвертой ветви дерева без дополнительных логических связей с состояниями УС ОУВС переходит в отказ.
3. Исследуем временные режимы работы и процедуры обработки неисправностей ВМ, УС СО и СС, определяемые протоколом отказоустойчивого обмена. Построим комбинаторные и марковские модели отказов компонентов ОУВС, учитывающие “просеивание” потока сбоев. Выполним расчеты суммарных интенсивностей потока неисправностей компо-

нентов с учетом как постоянных отказов, так и сбоев, трактуемых по внедренным в систему критериям, как постоянный отказ.

4. Построим марковский граф переходов в пространстве состояний трехмашинного блока ВМ и определим вероятности пребывания в состояниях трехмашинной, двухмашинной, одномашинной работоспособных конфигурациях и состояниях безопасного останова и опасного отказа системы. Интенсивности переходов марковской модели определим с учетом расчетов по сбоям, двух видов отказов ВМ (благоприятном и неблагоприятном), неполноты контроля.
5. Построим “вложенные” ДО, моделирующие переход в отказ системы из-за отказов УС СО и СС для каждого несовместного состояния трехмашинного блока ВМ, на которых проведем расчеты вероятностей реализации соответствующих вершинных событий. Исходные надежностные параметры для базовых событий отказов УС определим с учетом частотного и последовательностного критериев признания сбоящего УС отказавшим.
6. На укрупненном ДО ОУВС проведем расчет показателей надежности ОУВС в целом. Исходные надежностные характеристики базовых событий укрупненного дерева определяются на основе расчетов распределения вероятностей по состояниям марковской модели блока ВМ (п.4) и показателей (коэффициент готовности и параметр потока отказов), вычисленных на вложенных деревьях (п.5).

Деревья отказов для исследуемой отказоустойчивой вычислительной системы приведены на рис. 4.2 – 4.12. На рис. 4.2 представлено обобщенное дерево отказов ОУВС. На последующих рисунках детализированы ветви дерева, изображенного на рис. 4.2. На рис. 4.3. представлен непосредственный переход из трехмашинной конфигурации в ОО. В связи с изменением структуры МК согласований при переходе из трехмашинной конфигурации в двухмашинную и далее в неработоспособные состояния (в трехмашинном режиме каждый МК согласования состоит из трех УС, по одному от каждой ВМ, а в двухмашинном – из двух УС, по одному от каждой из оставшихся ВМ) часть дерева с тремя работоспособными ВМ раскрыта последо-

вательно для упрощения формальных преобразований и расчета: сначала переход в двухмашинную конфигурацию (рис. 4.4), а затем из двухмашинной – в неработоспособные состояния (рис. 4.5). Дерево на рис. 4.5. также отражает и переход в отказы по второй ветви дерева, когда две ВМ работоспособны, а одна отказала. Далее рассматривается деградация из двухмашинной работоспособной конфигурации в отказ. На рис. 4.6, 4.7 (а и б) показаны деревья для случаев, когда работоспособна одна ВМ, а две отказали и когда все три ВМ отказали. В деревьях, представленных на рис. 4.5 – 4.7, в содержании событий, касающихся отказов или работоспособности ВМ, нет указаний на первую отказавшую ВМ в трехмашинной конфигурации, так как любой первый отказ одной из трех ВМ всегда выявляется, ВМ блокируется и исключается из рабочей конфигурации. Некоторые статические вершины И (AND) заменены на динамические вершины приоритетного И (priority AND – PAND), учитывающие очередность возникновения входных событий (слева – направо). Базовые события деревьев (рис 4.3 – 4.7) являются промежуточными событиями, каждое из которых описывают соответствующей комбинацией отказов и работоспособности элементов. Деревья для этих промежуточных событий изображены на рис. 4.8 – 4.12. Причем, на дереве (рис. 4.12) указаны не конкретные номера элементов в соответствии со схемой (рис.4.1), а условные номера УС обмена одной из ВМ (это могут быть или элементы 1, 2, 3 или 4, 5, 6 или 7, 8, 9). Бинарное представление дерева отказов ОУВС в виде диаграммы двоичных решений и сформированное по ней выражение для вероятности отказа системы дано на рис. 4.13. Пояснения по расчетным методам, используемым при анализе деревьев отказов ОУВС, даны в разделе 4.3.

Набор событий и логических операторов, используемых при построении деревьев отказов анализируемой ОУВС, сведен в таблицу 4.1.

Таблица 4.1. Обозначение вершин и событий деревьев отказов ОУВС

вершина	название	описание
	AND	логическое И
	OR	логическое ИЛИ
	VOTING (k/n)	m/n голосование (мажоритарный выбор)
	PRIORITY AND (PAND)	приоритетное И (динамический оператор)
событие	название	описание
	BASIC	базовое событие
	BASIC Repeated Event	повторяющееся базовое событие
	UNDEVELOPED	сложное (составное) базовое событие
	UNDEVELOPED Repeated Event	повторяющееся сложное базовое событие

Вычислительные машины выделены в отдельный блок, по всем возможным состояниям которого осуществлено разложение надежностной модели (деревьев) системы. С одной стороны это сделано для упрощения преобразований и вычислений по деревьям отказов, а с другой – в связи с необходимостью учета в надежностной модели ВМ разных видов отказов и неполноты контроля. Последнее обстоятельство обуславливает использование марковской модели блока ВМ и форму представления в виде графа переходов, изображенного

на рис. 4.14. На графе обозначено:  $\lambda_{\sigma}$ ,  $\lambda_{\text{н}}$  – интенсивности благоприятных и неблагоприятных отказов одной ВМ;  $\eta$  – полнота контроля (условная вероятность выявления отказа при условии, что отказ произошел);  $\lambda_{\text{ВМ}} = \lambda = \lambda_{\sigma} + \lambda_{\text{н}}$ . Решая систему дифференциальных уравнений (4.1), составленных по этой модели, с начальными условиями  $P_1(0) = 1$  получим:

$$\begin{aligned}
 P_1'(t) &= -P_1(t)3\lambda \\
 P_2'(t) &= P_1(t)3\lambda - P_2(t)2(\lambda_{\text{н}} + \lambda_{\sigma}) \\
 P_3'(t) &= P_2(t)2\lambda_{\sigma} - P_3(t)2(\lambda_{\text{н}} + \lambda) \\
 P_4'(t) &= P_2(t)2\lambda_{\text{н}} + P_3(t)2(\eta\lambda_{\text{н}} + \lambda) \\
 P_5'(t) &= P_3(t)((1 - \eta)\lambda_{\text{н}})
 \end{aligned}
 \tag{4.1}$$

Здесь вероятность безотказной работы блока ВМ равна:  $P_1(t) + P_2(t) + P_3(t)$ , а  $P_4(t)$  и  $P_5(t)$  – вероятности безопасного останова и опасного отказа

$$\begin{aligned}
 P_1(t) &= e^{-3\lambda t}; \\
 P_2(t) &= 3(1 - e^{-\lambda t})e^{-2\lambda t}; \\
 P_3(t) &= \frac{6\lambda_{\sigma}}{\lambda + \lambda_{\sigma}}e^{-3\lambda t} - 6e^{-2\lambda t} + \frac{\lambda}{\lambda + \lambda_{\sigma}}e^{-(\lambda + \lambda_{\text{н}})t}; \\
 P_4(t) &= \frac{2[(\lambda_{\sigma}^2 - \lambda_{\text{н}}^2) + \lambda_{\sigma}\lambda_{\text{н}}(1 - \eta)]}{(\lambda + \lambda_{\sigma})\lambda}(1 - e^{-3\lambda t}) - \\
 &\quad \frac{3[(\lambda_{\sigma} + \eta\lambda_{\text{н}}) + \lambda_{\sigma}\lambda_{\text{н}}(1 - \eta)]}{\lambda}(1 - e^{-2\lambda t}) + \\
 &\quad \frac{6\lambda(\lambda + \eta\lambda_{\text{н}})}{(\lambda + \lambda_{\sigma})(\lambda + \lambda_{\text{н}})}(1 - e^{-(\lambda + \lambda_{\text{н}})t});
 \end{aligned}$$

$$P_5(t) = \frac{2\lambda_{\sigma}\lambda_H(1-\eta)}{(\lambda + \lambda_{\sigma})\lambda}(1 - e^{-3\lambda t}) - \frac{3\lambda_H(1-\eta)}{\lambda}(1 - e^{-2\lambda t}) + \frac{6(1-\eta)\lambda\lambda_H}{(\lambda + \lambda_{\sigma})(\lambda + \lambda_H)}(1 - e^{-(\lambda + \lambda_H)t}); \quad (4.2)$$

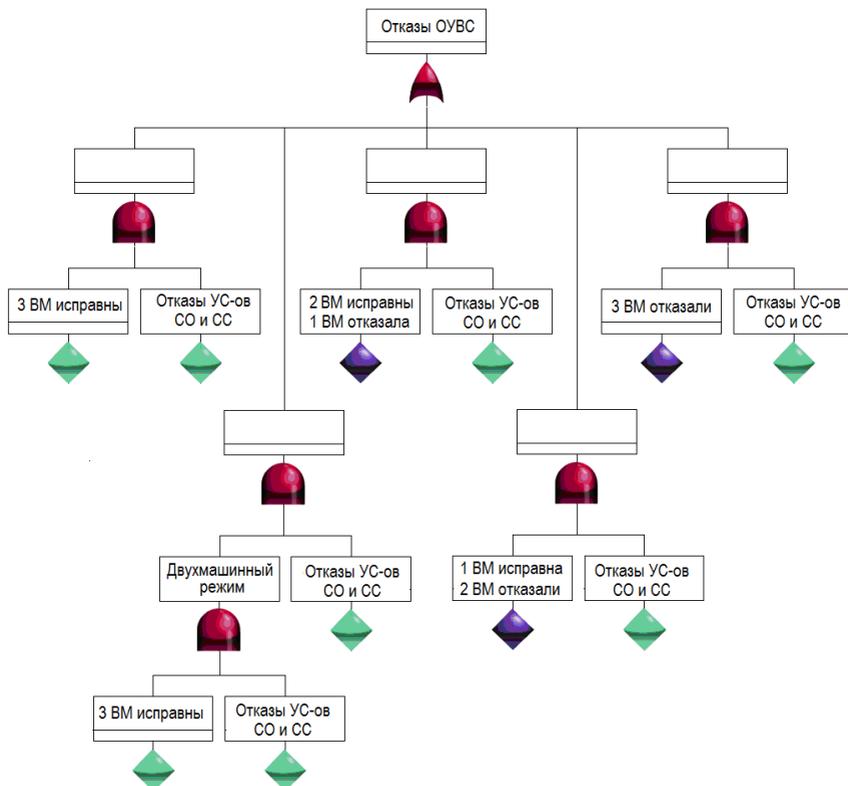


Рис. 4.2. Обобщенное дерево отказов ОУВС

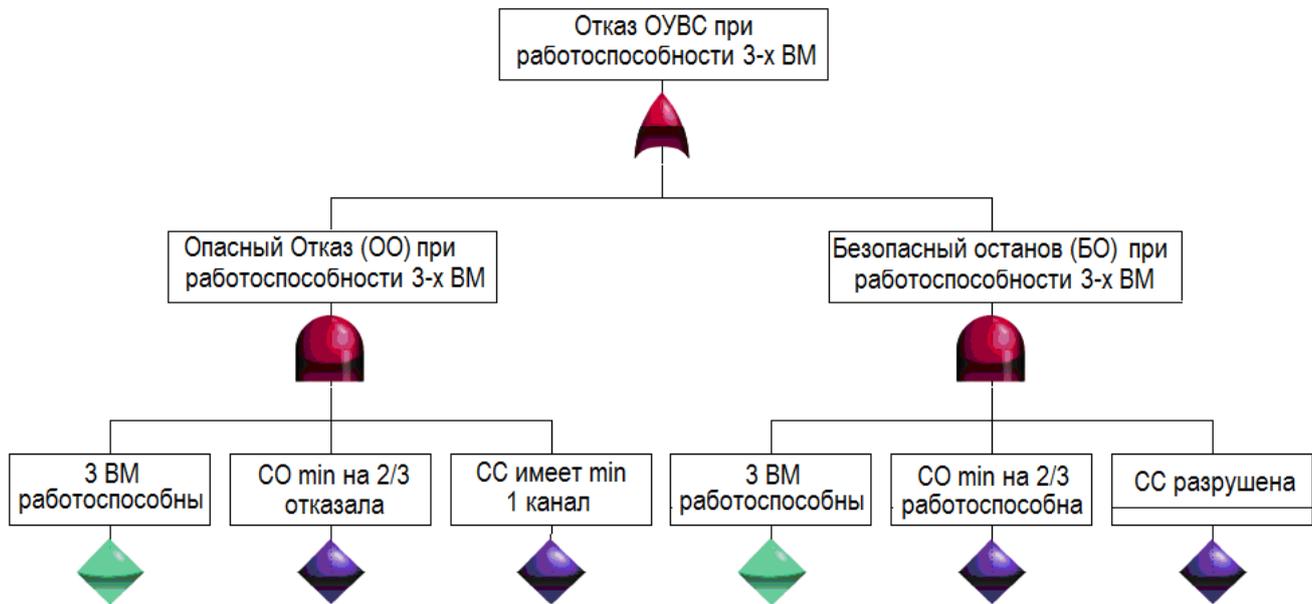


Рис. 4.3. Дерево переходов в состояния отказа ОУВС при работоспособности трех ВМ

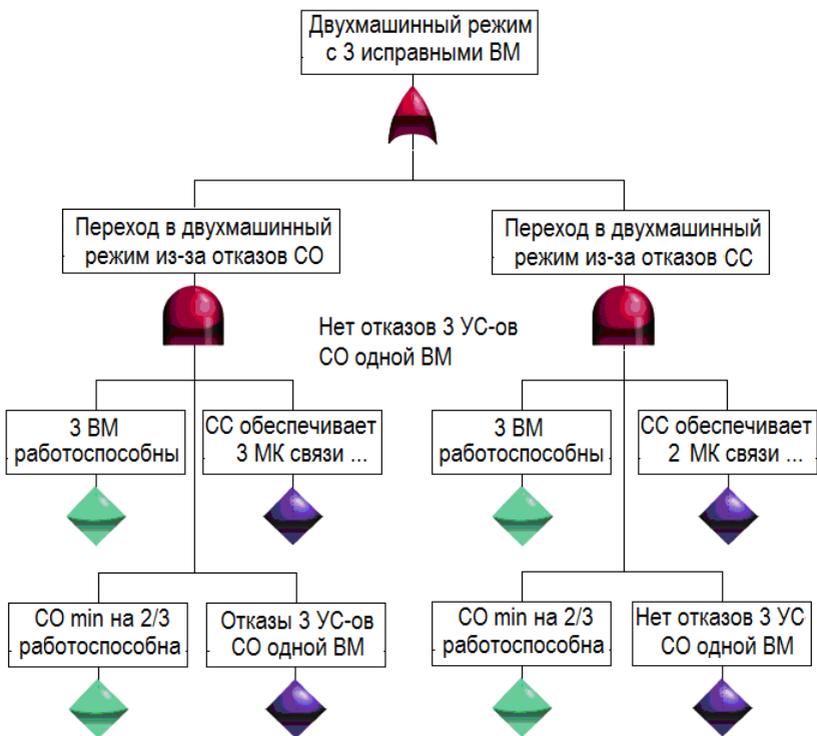


Рис. 4.4. Дерево переходов в двухмашинный режим ОВС из-за отказов УС-ов сети обмена и согласования

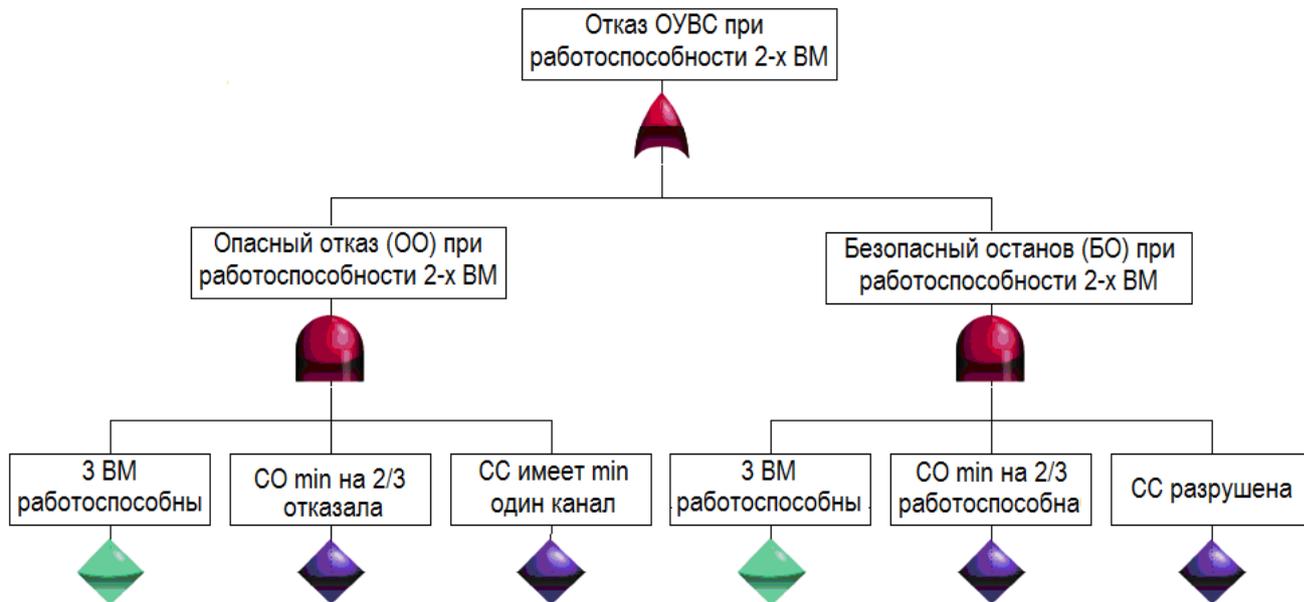


Рис. 4.5. Дерево переходов в состояния отказа ОВС при работоспособности двух ВМ

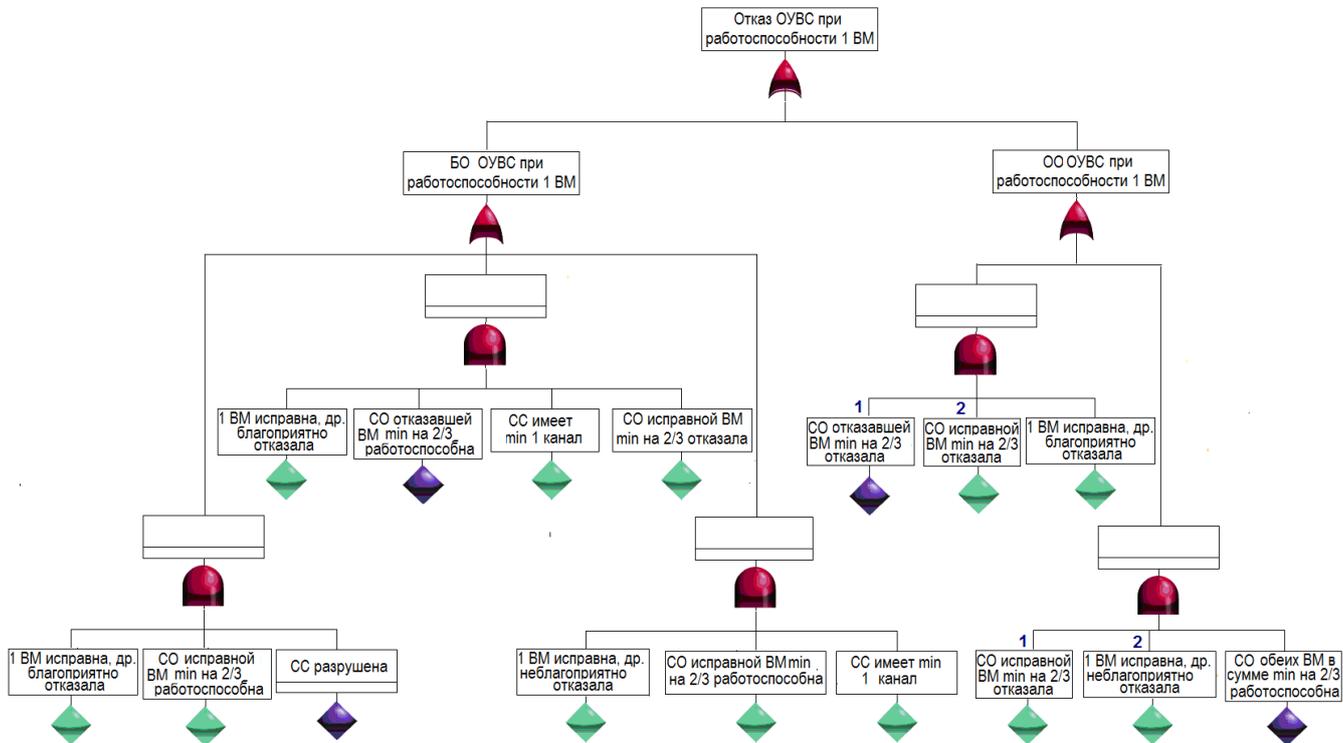
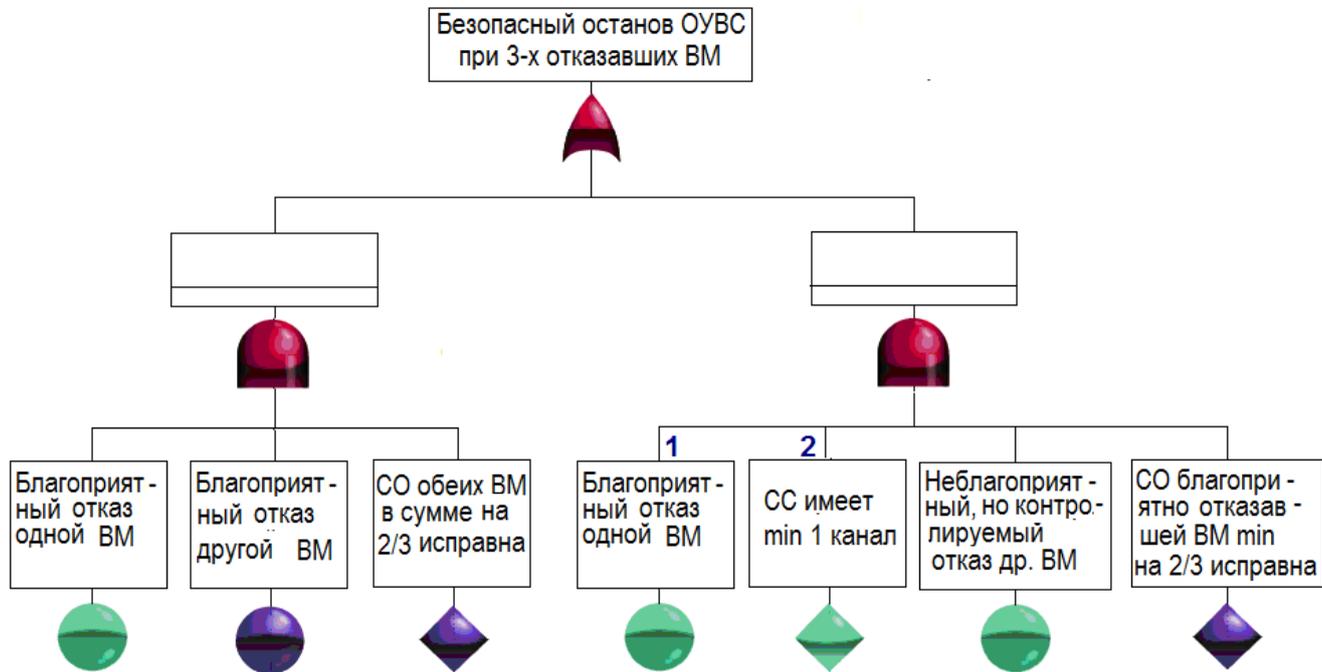
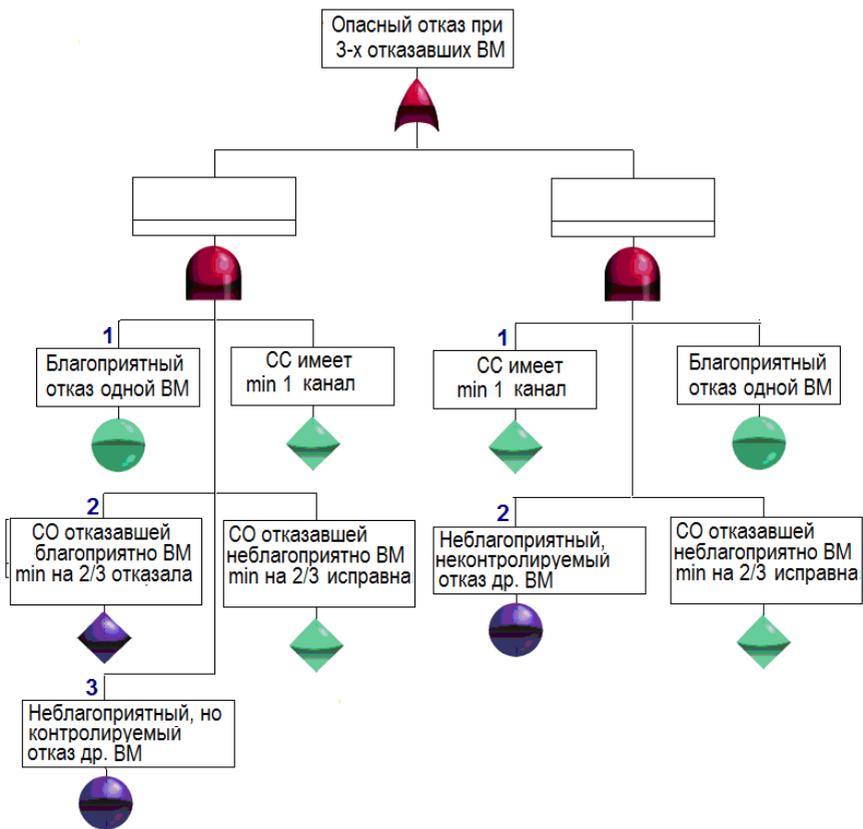


Рис. 4.6. Дерево переходов в состояния отказа ОУВС при одной работоспособной ВМ



а) переход в безопасный останов



б) Переход в опасный отказ.

Рис. 4.7. Дерево переходов в состояния отказа ОУВС при трех отказавших VM

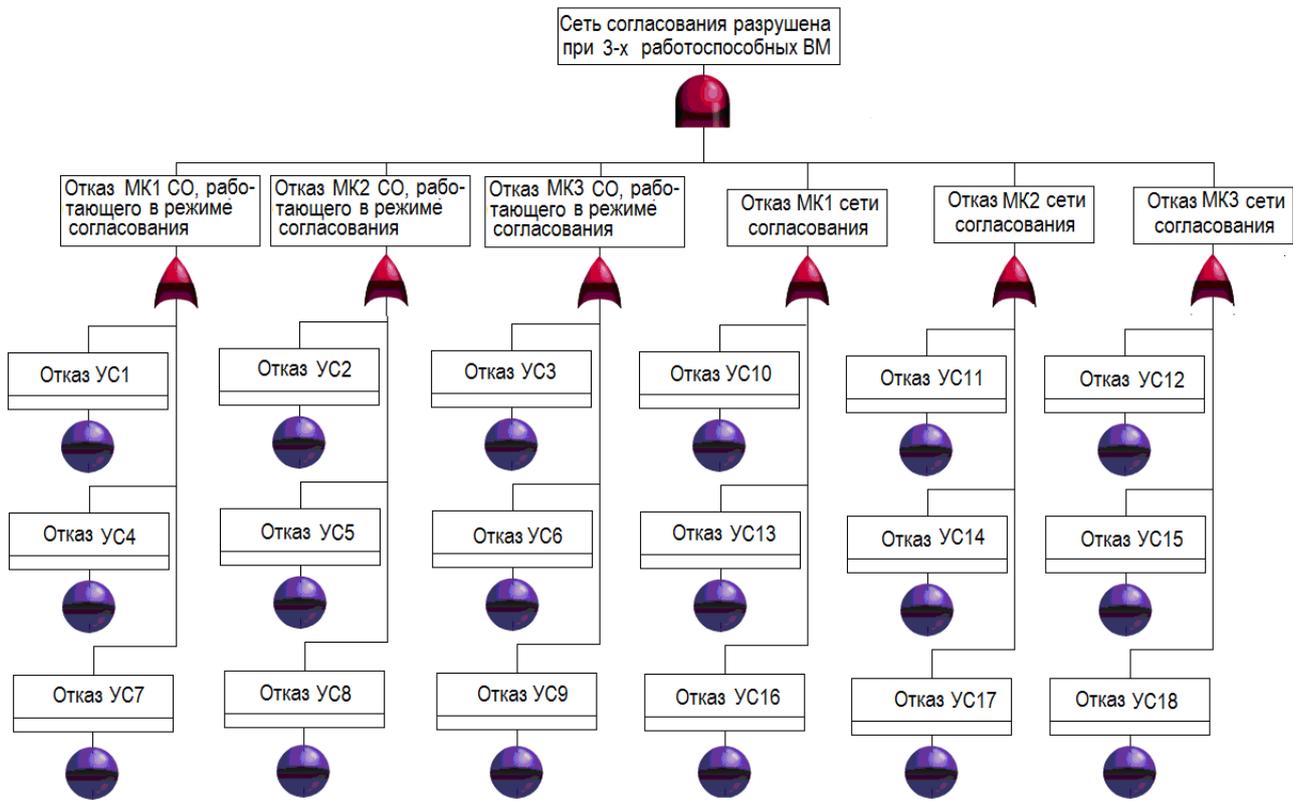


Рис. 4.8. Дерево отказов сети согласования ОУВС при трех работоспособных VM

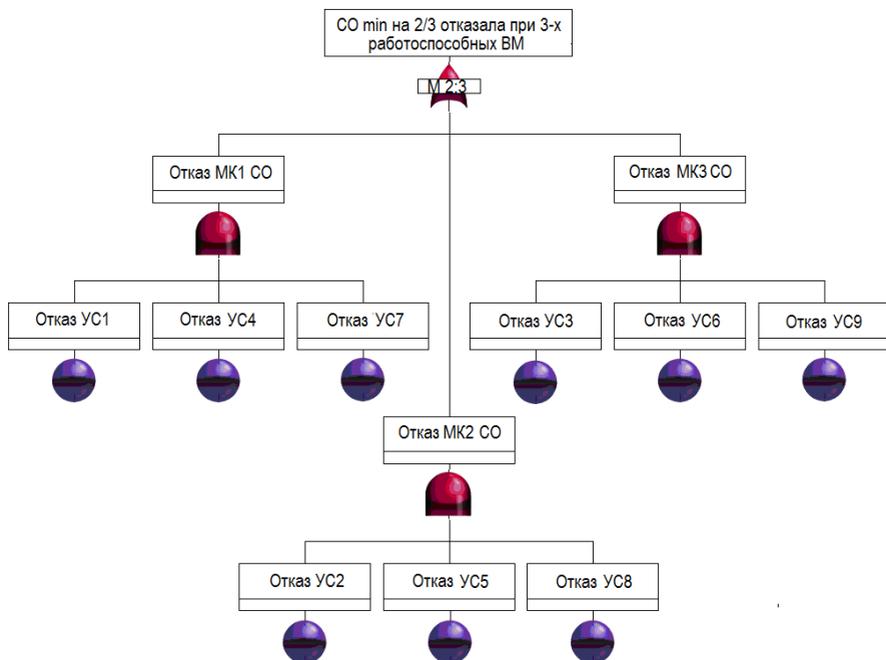


Рис. 4.9. Дерево переходов в событие “СО min на 2/3 отказала при 3-х работоспособных ВМ”

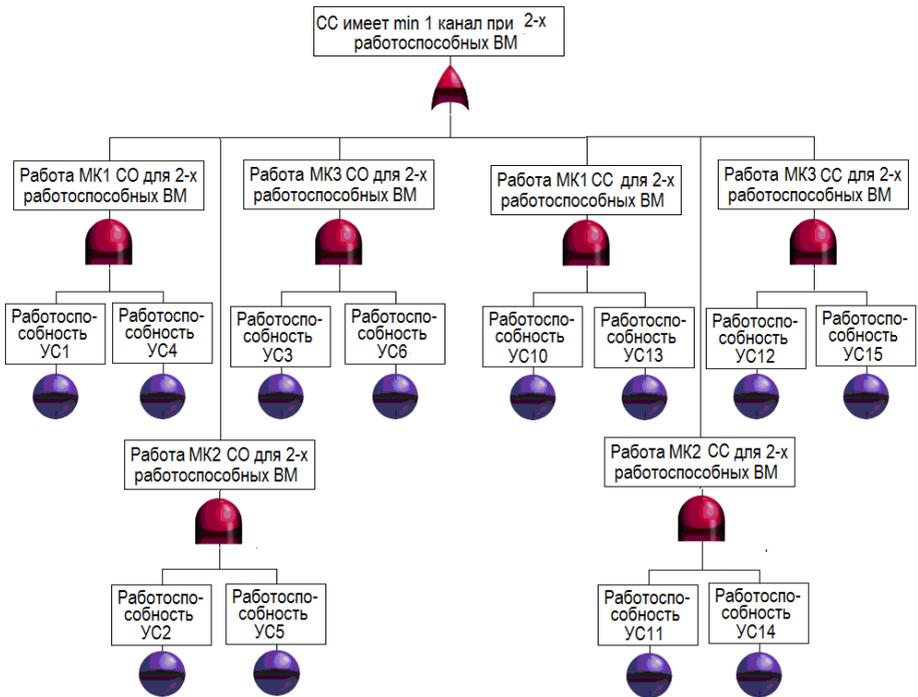


Рис. 4.10. Дерево работоспособности min одного канала согласования при 2-х работоспособных ВМ

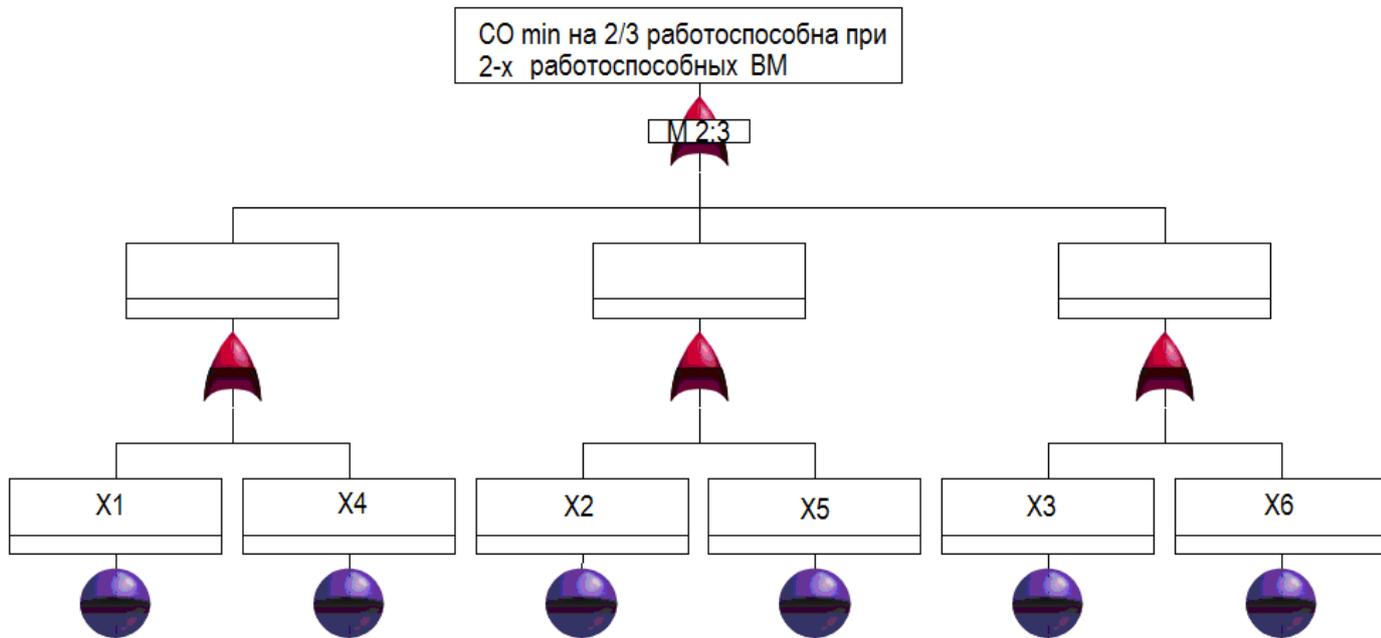


Рис. 4.11. Дерево работоспособности сети обмена при 2-х исправных ВМ.

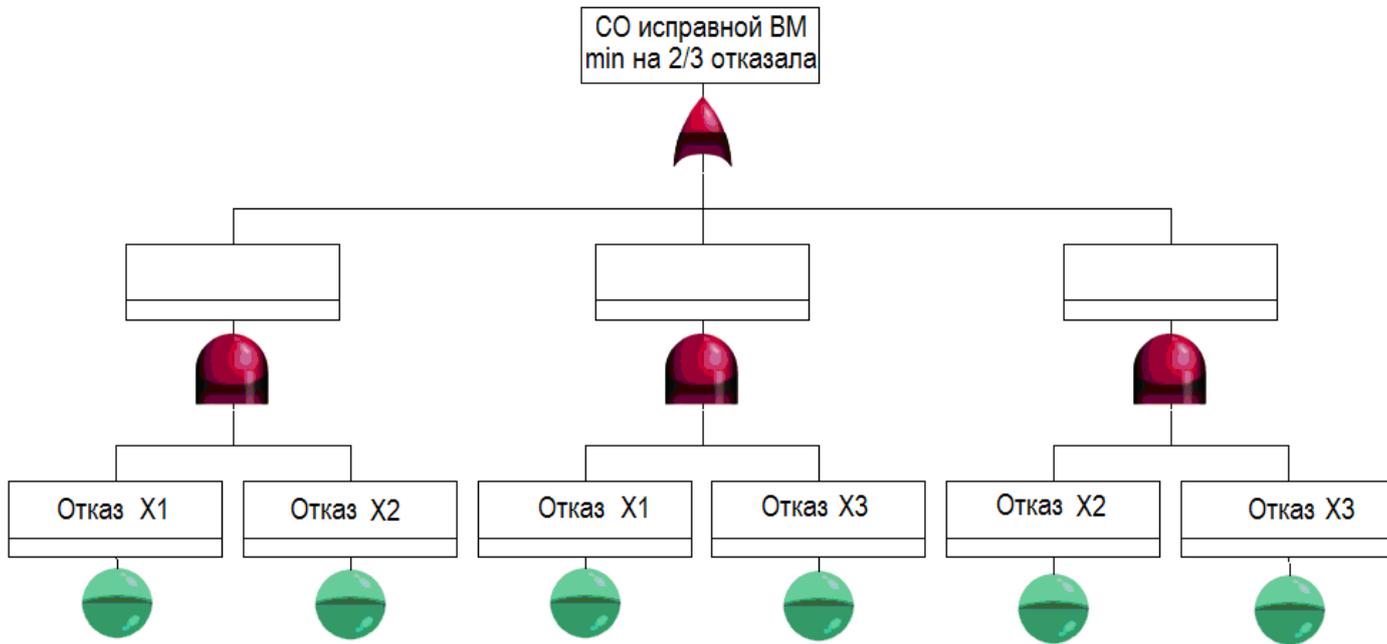


Рис. 4.12. Дерево отказов СО исправной ВМ.

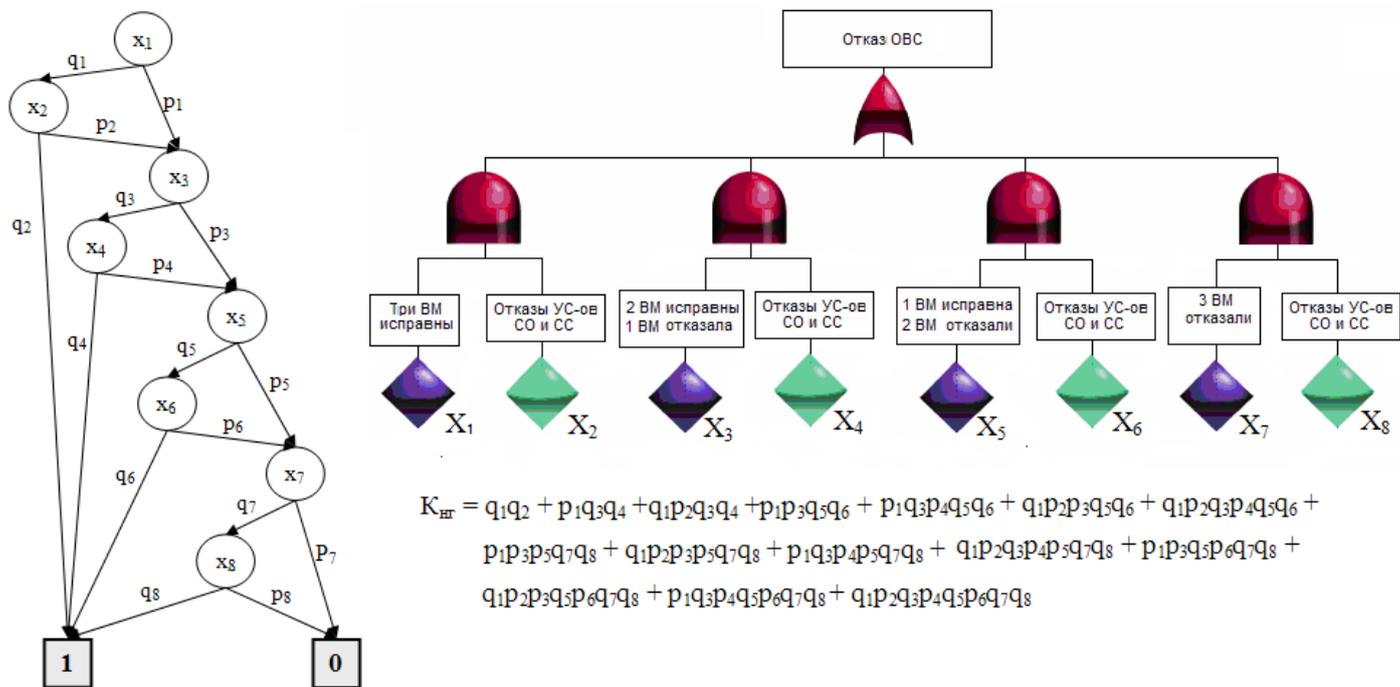


Рис. 4.13. Диаграмм двоичных решений дерева отказов ОУВС

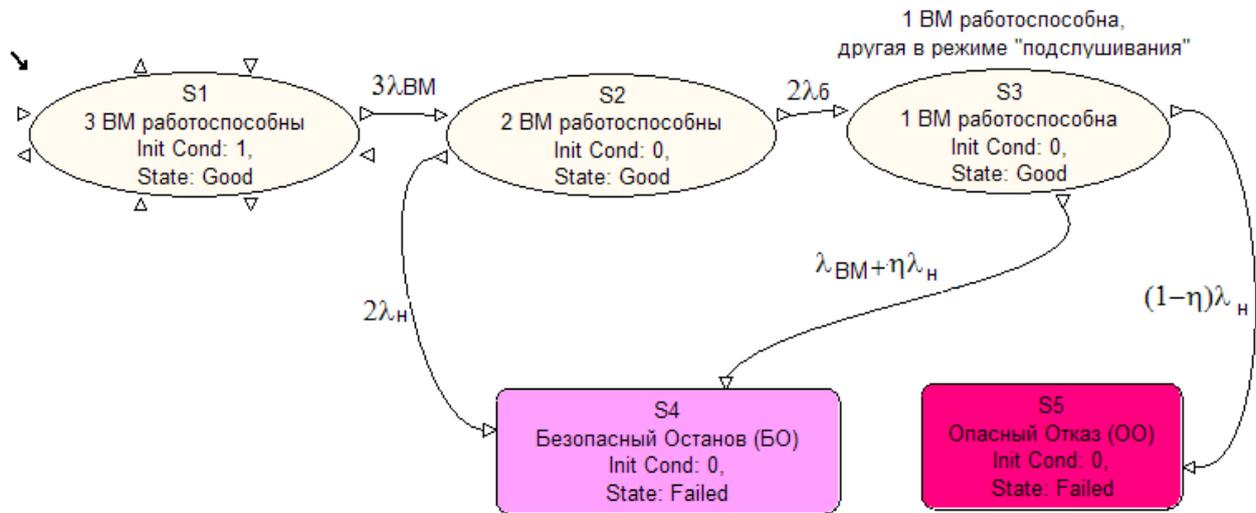


Рис. 4.14. Марковская модель надежности блока BM.

### 4.3. Методы расчета показателей надежности на деревьях отказов ОУВС

При анализе надежности ОУВС мы использовали свойство аппарата деревьев отказов, чрезвычайно существенное с точки зрения решения проблем размерности, а именно, возможность представления в деревьях отказов интересующего вершинного события через промежуточные. Мы сформулировали критерии отказа системы (возникновение вершинных событий) в терминах промежуточных событий. А промежуточные события соответствовали состоянию выделенных при структурной декомпозиции блоков (совокупностей элементов) системы. Рассматривая промежуточное событие в качестве конечного (для конкретного блока), можно, последовательно применяя правила построения деревьев отказов, в конечном счете добраться до первичных (базовых) событий, каковыми являются, например, отказы элементов системы. Таким образом, было произведено иерархическое описание и построение модели возникновения отказов ОУВС, наиболее выгодное в смысле трудоемкости (уход от полных переборов, присущих, например, марковским моделям) и снижения размерности задачи.

Результатом проведения количественного анализа ДО являются численные значения следующих показателей надежности:

- коэффициент готовности/неготовности (вероятность реализации вершинного события в заданный момент времени)  $(K(t))$
- вероятность отказа/безотказной работы (вероятность реализации вершинного события на заданном интервале времени)  $(P(t))$
- параметр потока отказов  $(w(t))$
- средняя наработка между отказами
- среднее время восстановления
- среднее число отказов за заданный интервал времени

Количественный анализ деревьев отказов, моделирующих сложное надежностное поведение ОУВС, невозможно проводить без поддержки специализированного программного обеспечения (ПО). В современном ПО анализа ДО, как правило, реализованы методы расчета показателей, основанные на теореме о вероятности суммы совместных событий (в данном случае под событием понимается реализация минимального сечения).

Минимальным сечением ( $C_i$ ) в системе произвольной структуры называется минимальное множество элементов, отказ которых приводит к отказу системы. А именно: а) если откажут все элементы сечения  $C_i$ , то система откажет независимо от состояния других элементов; б) никакое подмножество  $C_i$  не удовлетворяет первому условию.

Методы, основанные на вычислении вероятности суммы совместных событий реализации сечений (в англоязычной литературе метод называется Cross Product) используют формулу:

$$\begin{aligned}
 Q(t) = & \sum_{i=1}^n P_r\{C_{i_1}\} - \sum_{i_1=i_2>i_1}^{n-1} \sum_{j=1}^n P_r\{\bigcap_{j=1}^2 C_{i_j}\} + \\
 & (-1)^2 \sum_{i_1=i_2>i_1}^{n-2} \sum_{i_3>i_2}^{n-1} \sum_{j=1}^n P_r\{\bigcap_{j=1}^3 C_{i_j}\} + \dots + (-1)^{n-2} \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} P_r\{\bigcap_{j=1}^{n-1} C_{i_j}\} + (-1)^{n-1} P_r\{\bigcap_{i=1}^n C_i\}
 \end{aligned} \quad , \quad (4.3),$$

где  $Q(t)$  – вероятность наступления вершинного события (или любого промежуточного события, если для него определены наборы соответствующих минимальных сечений),  $C_i$  –  $i$ -ое минимальное сечение,  $n$  – число минимальных сечений. Для дерева отказов вероятность  $Q(t)$  является коэффициентом неготовности. Вероятности  $q_i$  ( $p_i$ ), являющиеся сомножителями в выражении для вычисления вероятности реализации сечения  $P_r\{C_i\}$ , определяются как коэффициенты неготовности базовых событий. Максимально возможное число пересекаемых сечений  $r$  равно  $n$ . При  $r = n$  получаем точное значение вероятности реализации рассматриваемого события, но при больших  $n$  наблюдается нелинейный рост времени расчета. Если  $r$  – нечетное, имеем верхнюю оценку коэффициента неготовности, при  $r$  четном – нижнюю оценку. При  $r = 1$  (в англоязычной литературе метод называется Cut Summation), получаем верхнюю оценку коэффициента неготовности, пригодную только для расчетов высоконадежных систем.

Для получения точного значения коэффициента неготовности  $Q(t)$  необходимо провести все пересечения сечений. Тогда число слагаемых в правой части (4.3) будет  $2^n - 1$ , что является серьезным препятствием для применения этого метода. Например, тестовый пример корабельной электроэнергетической системы, известный под названием «задача №35 И.А.Рябинина» [25, 40], имеет 15 элементов, 31 минимальное сечение и 92 минимальных пути ( $2^{31} > 2 \cdot 10^9$ ). В программных продуктах, реализующих этот метод вычисления показателей надежности (например, Risk Spectrum), вынуждены отказываться от получения точных значений показателей и ограничиваться приближенными, которые при невысоких надежности элементов дают слишком грубую оценку. Сложной задачей является также алгоритмизация нахождения пересечений символьных подмножеств путей, сечений.

Параметр потока отказов системы  $w(t)$  есть ожидаемое число появления отказов системы в момент времени  $t$  (т.е. на  $(t, t+\Delta t)$  при  $\Delta t \rightarrow 0$ ), что означает возникновение, по крайней мере, одного сечения в момент времени  $t+\Delta t$ . Пусть  $e_i$  – событие появления  $i$ -го сечения в  $(t, t+\Delta t)$ , где  $e_i(t+\Delta t)$  – конъюнкция  $n_i$  переменных (элементов), образующих сечение  $C_i$ . Появление  $e_i$  на  $\Delta t$  означает (при ординарном потоке отказов), что в момент  $t$  неработоспособными были  $(n_i - 1)$  элементов сечения  $C_i$  (это событие обозначим через  $e_i'$ ) и произошел отказ на  $\Delta t$  одного (работоспособного в момент  $t$ ) элемента. Тогда вероятность появления на  $\Delta t$  сечения  $e_i$  (т.е. параметр потока отказов  $w(t)$ ) определится по формуле полной вероятности так:

$$w_i(t) = \sum_{j_i=1}^{n_i} [\omega_{j_i}(t) \prod_{g_i \neq j_i}^{n_i} Q_{g_i}(t)], \quad (4.4)$$

где  $\omega_{j_i}(t)$ ,  $Q_{g_i}(t)$  - параметр потока отказов и коэффициент неготовности элементов  $j_i$ ,  $g_i$  сечения  $C_i$  в момент времени  $t$ , а  $n_i$  – число элементов сечения  $C_i$ .

Формула (4.4) дает верхнюю оценку  $w(t)$ , т.к. не учитывает всех возможных состояний системы, а учитывает лишь состояния, предшествующие реализации сечения.

Известный метод вычисления параметра потока отказов  $\omega_S$  также основывается на формуле (4.3):

$$\omega_S \Delta t = P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^n e_i)\} =$$

$$P\{\bigcup_{i=1}^n e_i\} - P\{(S(x, t) = 0) \wedge (\bigcup_{i=1}^n e_i)\} = (\omega_{S1} - \omega_{S2}) \Delta t \quad ; \quad (4.5)$$

$$\omega_{S1} \Delta t = \sum_{i_1=1}^n P\{e_{i_1}\} - \sum_{i_1=1}^{n-1} \sum_{i_2 > i_1}^n P\{e_{i_1} \cap e_{i_2}\} +$$

$$\sum_{i_1=1}^{n-2} \sum_{i_2 > i_1}^{n-1} \sum_{i_3 > i_2}^n P\{e_{i_1} \cap e_{i_2} \cap e_{i_3}\} - \dots +$$

$$(-1)^{n-1} P\{e_1 \cap e_2 \cap \dots \cap e_n\} \quad ; \quad (4.6)$$

$$\begin{aligned}
\omega_{S2}\Delta t = & \sum_{i=1}^n \left[ \sum_{j \neq i}^n P\{C_j \wedge e_i\} - \sum_{\substack{j_1=1 \\ j_1 \neq i}}^{n-1} \sum_{j_2=j_1+1}^n P\{C_{j_1} \wedge C_{j_2} \wedge e_i\} + \dots + \right. \\
& (-1)^{n-2} P\{C_1 \wedge \dots \wedge C_{i-1} \wedge C_{i+1} \wedge \dots \wedge C_n \wedge e_i\} \left. \right] - \\
& \left[ \sum_{j \neq i_1, i_2}^n P\{C_j \wedge (e_{i_1} \cap e_{i_2})\} - \right. \\
& - \sum_{i_1=i_2=i_1+1}^{n-1} \sum_{\substack{j_1=1 \\ j_1, j_2 \neq i_1, i_2}}^{n-1} \sum_{j_2=j_1+1}^n P\{C_{j_1} \wedge C_{j_2} \wedge (e_{i_1} \cap e_{i_2})\} + \dots + \quad . \quad (4.7) \\
& (-1)^{n-3} P\{C_1 \wedge C_2 \wedge \dots \wedge C_{i_1-1} \wedge C_{i_1+1} \wedge \dots \\
& \wedge C_{i_2-1} \wedge C_{i_2+1} \wedge \dots \wedge C_n \wedge (e_{i_1} \cap e_{i_2})\} \left. \right] + \\
& \dots + \sum_{j=1}^n (-1)^{n-1} P\{C_j \wedge (e_1 \cap \dots \cap e_{j-1} \cap e_{j+1} \cap \dots \cap e_n)\}
\end{aligned}$$

Событие  $\{C_{j_1} \wedge C_{j_2} \wedge (e_{i_1} \cap e_{i_2})\}$  означает, что в момент  $t$  система находилась в отказе по причине реализации двух сечений  $C_{j_1}$ ,  $C_{j_2}$  и за  $\Delta t$  произошел отказ общего для сечений  $C_{i_1}$ ,  $C_{i_2}$  элемента (т.е. на  $(t, t+\Delta t)$  появились сечения  $i_1$  и  $i_2$ ). Если такого элемента нет, то вероятность события появления сразу двух (и более) сечений на  $\Delta t$  равна нулю. Общий член равен

$$\begin{aligned}
& P\{C_{j_1} \wedge C_{j_2} \wedge \dots \wedge \dots \wedge C_{j_U} \wedge (e_{i_1} \cap e_{i_2} \cap \dots \cap e_{i_G})\} = \\
& = \omega_{GU}(t)\Delta t \prod_{\substack{1 \dots G \\ 1 \dots U}} Q(t) \quad , \quad (4.8)
\end{aligned}$$

где  $\omega_{GU}(t)$  – параметр потока группы общих элементов, входящих в  $G$  сечений и не входящих в  $U$  из остальных  $(l - G)$ ;  $\prod_{1..U}^{1..G} Q(t)$  – произведение коэффициентов простоя всех элементов входящих в  $G$  сечений и  $U$  сечений из остальных  $(l - G)$  за исключением тех элементов, которые используются при вычислении  $\omega_{GU}(t)$ . При этом в произведении каждый элемент учитывается только один раз. Вычисления параметра потока отказов по (4.4) – (4.8) – ещё более трудоёмкая задача (более чем в 3 раза), чем вычисление коэффициента неготовности по (4.3).

В [41] рассматриваются более эффективные методы вычисления неготовности (готовности), позволяющие проводить точные расчеты показателей коэффициента готовности (неготовности) и параметра потока отказов. Эти методы используют рекурсивное наращивание переменных. Остановимся кратко на этих методах.

Пусть элементы системы  $x_i, i=1, \bar{N}$  и система  $S(\mathbf{x}), \mathbf{x}=\{x_i\}$  могут находиться в двух состояниях – работоспособном и неработоспособном

$$x_i = \begin{cases} 1, & \text{когда элемент } i \text{ работоспособен} \\ 0, & \text{когда элемент } i \text{ отказал} \end{cases} \quad (4.9)$$

$$S(\mathbf{x}) = \begin{cases} 1, & \text{когда система работоспособна} \\ 0, & \text{когда система отказала} \end{cases} \quad (4.10)$$

Пусть состояние системы полностью определяется состоянием в момент  $t$  ее элементов. Обозначим:  $\mathbf{A}=\{A_j\}$  – множество всех минимальных путей работоспособности системы,  $\mathbf{C}=\{C_j\}$  – множество всех минимальных сечений неработоспособности системы.

Тогда работоспособность системы в момент  $t$  записывается как

$$S(\mathbf{x}, t) = \left\{ \bigvee_{j=1}^d A_j \right\} = 1, \quad (4.11)$$

а неработоспособность

$$\bar{S}(x,t) = \left\{ \bigvee_{j=1}^n C_j \right\} = 1. \quad (4.12)$$

Каждый минимальный путь (сечение) представляет собой конъюнкцию некоторого набора из работоспособных (отказавших) элементов  $\mathbf{x} = \{x_i\}$ .

Коэффициент готовности (простоя) системы определяется по следующим выражениям:

$$\begin{aligned} P\{S(x,t) = 1\} &= P\{\bar{S}(x,t) = 0\} = P\left\{ \bigvee_{j=1}^d A_j = 1 \right\} = \\ &= 1 - P\left\{ \bigvee_{j=1}^n C_j = 1 \right\} \end{aligned} \quad (4.13)$$

$$\begin{aligned} P\{S(x,t) = 0\} &= P\{\bar{S}(x,t) = 1\} = P\left\{ \bigvee_{j=1}^n C_j = 1 \right\} = \\ &= 1 - P\left\{ \bigvee_{j=1}^d A_j = 1 \right\} \end{aligned} \quad (4.14)$$

где  $P\{\cdot\}$  – вероятность наступления в момент  $t$  заключенного в скобки события.

Пусть

$$\begin{aligned} p^{(k)} &= P\{S(x_1, \dots, x_k; t) = 1 / x_{k+1} = 1, x_{k+2} = 1, \dots, x_N = 1\} \\ r^{(k)} &= P\{S(x_1, \dots, x_k; t) = 1 / x_{k+1} = 0, x_{k+2} = 1, \dots, x_N = 1\} \end{aligned} \quad (4.15)$$

Вычисления проводятся по формуле

$$p^{(k+1)} = R_{k+1}(t)p^{(k)} + Q_{k+1}(t)r^{(k)}, \quad (4.16)$$

где  $R_{k+1}(t) = 1 - Q_{k+1}(t) = P\{x_{k+1}(t) = 1\}$ ,  $p^{(0)} = 1$ . Последовательно вычисляя  $p^{(1)}, \dots, p^{(N)}$ , на последнем  $N$ -ом шаге рекурсии получим коэффициент готовности системы.

Аналогичный подход применим и для вычисления параметра потока отказов.

Пусть

$$\omega^{(k)}(t)\Delta t = P\left\{S(x, t) = 1 \wedge \left(\bigcup_{i=1}^n e_i\right) / x_{k+1} = x_{k+2} = \dots = x_N = 1\right\} \quad (4.17)$$

$$v^{(k)}(t)\Delta t = P\left\{S(x, t) = 1 \wedge \left(\bigcup_{i=1}^n e_i\right) / x_{k+1} = 0, x_{k+2} = \dots = x_N = 1\right\}$$

Тогда параметр потока отказов системы рекурсивно вычисляется следующим образом

$$\begin{aligned} \omega^{(k+1)}(t) &= R_{k+1}(t)\omega^{(k)}(t) + Q_{k+1}(t)v^{(k)}(t) + \\ &+ P_{\text{предотк}}^{x_{k+1}}(t)\omega_{k+1}(t), \quad \omega^{(0)}(t) = 0, \quad \omega_{\text{сист}}(t) = \omega^{(N)}(t), \end{aligned} \quad (4.18)$$

где  $P_{\text{предотк}}^{x_{k+1}}(t) = (p^{(k)} - r^{(k)})$ ,  $k = (0, 1, \dots, N-1)$

Там же в [41] проводятся ручные расчеты готовности и параметра потока отказов мостиковой структуры (число элементов равно 5, число сечений – 4). Показано, что для расчета коэффициента готовности по выражению 4.3 проведено 15 шагов, а по (4.15 – 4.16) – 5 шагов. Для расчета параметра потока отказов по (4.4 – 4.7) – 65 шагов, а по (4.17 – 4.18) – 10 (5 из которых касаются вычисления готовности/неготовности).

Необходимо также отметить, что логико-вероятностные методы, являющиеся математическим аппаратом вычислений для моделей надежности на деревьях отказов, позволяют вычислять только показатели в момент времени  $t$ . Таковыми являются только коэффициент готовности/неготовности и параметр потока отказов. Поэтому для систем с восстановлением такой основной показатель надежности как вероятность безотказной работы (отказа) на интервале  $(0, t)$  с использованием деревьев отказа вычислен быть не может. Например, при вычислении показателя вероятность безотказной работы (ВБР) в специализированном ПО анализа надежности Windchill Quality Solutions (бывший Relex) и Isograph система искусственно делается невозстанавливаемой (тогда ВБР просто совпадает с коэффициентом

готовности). В настоящее время авторами завершаются исследования по оценке ВБР (для автоматизированных расчетов на деревьях) выражения

$$P(t) = e^{-\int_0^t \frac{w(\tau)}{K(\tau)} d\tau} \quad (4.19)$$

Численное решение по (4.19) хорошо автоматизируется и выдает результаты предписанной точности при использовании адаптивных квадратурных алгоритмов. Именно так реализована процедура чис-

ленного расчета  $P(t)$ , средней наработки до отказа  $(\int_0^{\infty} P(\tau) d\tau)$  и сред-

него числа отказов на интервале времени  $(0, t)$   $(\int_0^t w(\tau) d\tau)$  в разрабо-

танной авторами программе логико-вероятностного моделирования надежности – RAY.

Отметим, что программная реализация количественного анализа деревьев отказов, описанная выше, является сложной программистской задачей, так как требует разработки быстрых алгоритмов генерации наборов минимальных сечений и сложных процедур кодирования выражений (4.3 – 4.18). Новейшей тенденцией в автоматизации ДО является привлечение современных эффективных методов дискретной математики для представления и манипуляции булевыми функциями, соответствующими деревьям отказов. В качестве искомого представления логики дерева предлагается применять диаграммы двоичных решений (Binary Decision Diagram – ДДР) [42 – 45]. В терминах ДДР логические функции представляются в виде направленного ациклического графа (бинарного дерева), у которого внутренние вершины представляют аргументы функции. Кроме того, выделены два типа терминальных вершин, обозначенные как 0 и 1. Каждая нетерминальная вершина графа имеет двух потомков. Ветви графа упорядочены – проход по левой означает, что аргументу присвоено значение 1, а по правой – значение 0. Присвоение 1 отобра-

жается сплошной линией ветви, присвоение 0 – пунктирной. Значение логической функции определяется спуском по дереву от корня к терминалам.

При автоматизации анализа надежности важными преимуществом диаграмм двоичных решений являются

- представление логических функций в формах перехода к замещению, допускающих замещение логических переменных вероятностями, а логических операций арифметическими. Это достигается за счет того, что сам принцип построения ДДР, подобно алгоритму разрезания [46], обеспечивает разложение логической функции на ортогональные слагаемые
- при машинной реализации ДДР воплощается нелинейной динамической структурой данных – двоичным деревом, для которого разработаны эффективные алгоритмы обхода узлов, сложность которых зависит от количества уровней дерева, т.е. приблизительно от  $\log_2 n$  ( $n$  – количество узлов).

На рис. 4.13. приведено представление дерева отказов ОУВС диаграммой двоичных решений, по которой непосредственно получено расчетное выражение для показателя коэффициент неготовности системы.

Недостатком является то, что размерность порождаемых диаграмм сильно зависит от предварительного этапа упорядочения аргументов логической функции, который в настоящее время недостаточно формализован.

Для того, чтобы сохранить в качестве входного описания дерева отказов, а вычисления реализовывать на ДДР, необходимо разработать соответствующие алгоритмы преобразования ( $ДО \rightarrow ДДР$ ). Одна из возможных реализаций такого алгоритма приведена в [28].

На деревьях рис.4.6. и 4.7 некоторые базовые события отмечены цифрами, соответствующими номеру события в последовательности их возникновения. Это означает, что только указанная последовательность возникновения базовых событий приводит к “срабатыванию” вершинного события. Классические (статические) деревья отказов, имеющие только три вида вершин И, ИЛИ, НЕ и являющиеся визуальной интерпретацией логико-вероятностных методов, не позволяют в полной мере учесть особенности “надежностного поведе-

ния” сложных систем, в частности последовательность возникновения отказов во времени. Для учета этой особенности предлагается использовать следующий прием.

Пусть имеется два элемента, А и В. Нас интересует конечное событие, которое происходит, если первым откажет элемент А, а затем – элемент В. Дерево в этом случае имеет вид, показанный на рис. 4.15. Необходимо найти вероятность наступления на интервале  $(0, T)$  вершинного события  $(Y=1)$ , если известны функции распределения  $F_i(t)$  и плотности распределения  $f_i(t)$  наработки до отказа для каждого элемента. Тогда искомая вероятность (с учетом последовательности отказов) может быть записана, например, любым из двух способов:

$$P\{Y(T) = 1\} = \int_0^T f_A(t)(1 - F_B(t))F_B(T - t)dt. \quad (4.20)$$

$$P\{Y(T) = 1\} = \int_0^T f_B(t)\left(\int_0^t f_A(\tau)d\tau\right)dt. \quad (4.21)$$

Пусть  $f_A(t) = \lambda_A e^{-\lambda_A t}$ ;  $f_B(t) = \lambda_B e^{-\lambda_B t}$ . Тогда

$$\begin{aligned} P\{Y(T) = 1\} &= \int_0^T \lambda_B e^{-\lambda_B t} \cdot \left(\int_0^t \lambda_A e^{-\lambda_A \tau} d\tau\right) dt = \\ &= \frac{\lambda_A}{\lambda_A + \lambda_B} + \frac{\lambda_A}{\lambda_A + \lambda_B} e^{-(\lambda_A + \lambda_B)T} - e^{-\lambda_B T}. \end{aligned} \quad (4.22)$$

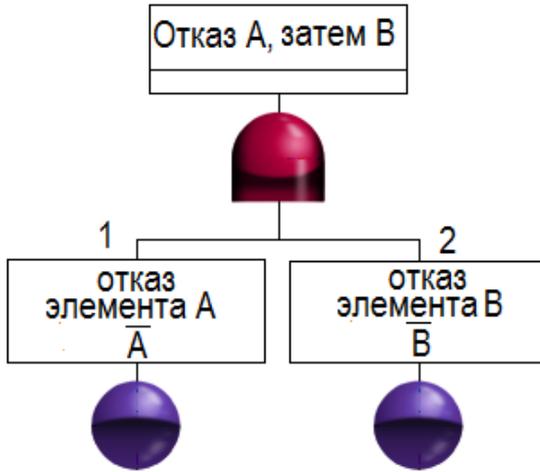


Рис.4.15. Динамическое дерево для учета последовательности возникновения отказов

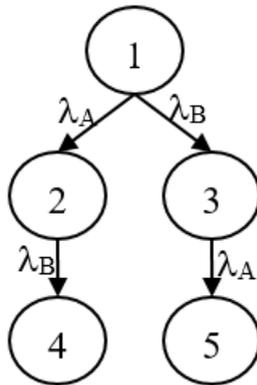


Рис.4.16. Марковская модель двухвходовой вершины AND, учитывающей последовательность отказов (PAND).

Для проверки полученного выражения можно составить граф переходов марковской модели (см. рис. 4.16) и найти решение соответствующее этому графу. Нас интересует состояние 4 (сначала отказал элемент А, а затем В). Дифференциальные уравнения имеют вид:

$$\begin{cases} P_1'(t) = -(\lambda_A + \lambda_B)P_1(t) \\ P_2'(t) = \lambda_A P_1(t) - \lambda_B P_2(t) \\ P_4'(t) = \lambda_B P_2(t) \end{cases} \quad (4.23)$$

$$P_1(0) = 1$$

Решая (4.23), получим

$$P_1(T) = e^{-(\lambda_A + \lambda_B)T}$$

$$P_2(T) = e^{-\lambda_B T} - e^{-(\lambda_A + \lambda_B)T}$$

$$P\{Y(T) = 1\} = P_4(T) = \int_0^T \lambda_B (e^{-\lambda_B t} - e^{-(\lambda_A + \lambda_B)t}) dt = \quad (4.24)$$

$$\frac{\lambda_A}{\lambda_A + \lambda_B} + \frac{\lambda_B}{\lambda_A + \lambda_B} e^{-(\lambda_A + \lambda_B)T} - e^{-\lambda_B T}$$

Обозначим  $P\{Y(T)=1\}$  для PAND с  $n$  входами как  $Q_n(T)$ . Тогда рекуррентное соотношение для вычисления вероятности последовательных отказов  $n$  элементов будет:

$$Q_n(T) = \int_0^T f_n(\tau) \cdot Q_{n-1}(\tau) d\tau \quad (4.25)$$

Преимуществом использования рекуррентного интегрального соотношения вместо марковской модели последовательности отказов является снятие ограничения на экспоненциальность распределения случайных наработок элементов, и, как следствие, возможность замены базовых элементов вложенными деревьями и комбинаторными моделями обработки неисправностей.

При наборе деревьев помимо стандартных базовых событий и логических операторов используются повторяющиеся события (repeated events) (см. табл. 4.1). Повторяющиеся базовые события учитывают возможность присутствия одного и того же события в разных ветвях дерева. Например, в дереве (рис. 4.12) отказ элемента

X1 (повторяющееся базовое событие) приведет к тому, что соответствующие входы первой и второй вершины AND одновременно примут значение true (истинна).

#### **4.4. Модели надежности элементов с учетом сбоев**

ОУВС реального времени обладают специфической реакцией на сбой. Специфика реакции определяется, главным образом, временными ограничениями на выдачу управляющих воздействий и высокой степенью резервирования. В этих условиях обычно отказываются от стандартной организации реакции на сбой типа повторов операций и пр. (см. главы 1,2) и применяют оригинальные решения. Так, в рассматриваемой отказоустойчивой вычислительной системе неисправность любого элемента (ВМ, УС) вначале трактуется как сбой и лишь при удовлетворении некоторого критерия идентифицируется как отказ этого элемента. Критерии формулируются в зависимости от вида элемента.

Для устройств связи, участвующих в процессе обмена с внешней средой, критерием отказа является превышение допустимой частоты проявления его неисправности (частотный критерий). Выбор такого критерия является следствием разнородности информации при обменах с внешней средой.

Для УС, реализующих межмашинное согласование, критерием отказа является появление искажения в нескольких последовательных тактах согласования (последовательностный критерий).

Если УС участвует как в процессе обмена, так и в процессе согласования, то для каждого из процессов применяется свой критерий отказа.

Критерием отказа вычислительной машины является неуспех ряда попыток ее восстановления. Считается, что неисправная ВМ, еще не признанная отказавшей, находится в состоянии программного сбоя. Восстановление работоспособности ВМ, находящейся в состоянии программного сбоя, осуществляется с помощью исправных ВМ.

Введение специальных критериев признания неправильно работающих блоков отказавшими является мерой, необходимой для “просеивания” общего потока неисправностей (сбои + отказы). Без такого “просеивания” система бы очень скоро исчерпала свои ресурсы вследствие исключения неисправных блоков и из-за высокой

интенсивности потока сбоев перешла в состояние безопасного остаточного.

При увеличении численного значения критерия (допустимое число сбоев, возникающих на заданном интервале, число неуспешных попыток последовательного согласования, число неуспешных попыток восстановления) уменьшается вероятность ошибочного признания сбойного устройства отказавшим, однако увеличивается вероятность возникновения ситуаций, приводящих к опасным последствиям для системы. Подобные ситуации являются следствием неправильной идентификации отказа устройства как сбоя.

Вероятность  $Q(t)$  признания элемента вычислительной системы на интервале  $(0, T)$  отказавшим определяется как

$$Q(T) = q_{\text{отк}}(T) + (1 - p_{\text{сб}}(T))p_{\text{отк}}(T) = 1 - p_{\text{отк}}(T)p_{\text{сб}}(T), \quad (4.26)$$

где  $p_{\text{отк}}(T)$  – вероятность безотказной работы элемента по постоянным отказам, равная  $e^{-\lambda_{\text{отк}}T}$ ;  $q_{\text{отк}}(T) = 1 - p_{\text{отк}}(T)$  – вероятность отказа элемента;  $p_{\text{сб}}(T)$  – вероятность признания (согласно критериям) того, что неисправность элемента обусловлена сбоем.

Для всех блоков системы организована циклическая работа. Все время функционирования УС разбито на циклы синхронизации ( $\tau_{\text{ц}}$ ), внутри которых выделено время на операции обмена и согласования, по два такта согласования ( $\Delta t_{\text{с}}$ ) и один такт обмена ( $\Delta t_{\text{об}}$ ), чередующиеся в последовательности: согласование – обмен – согласование. Любое количество неисправностей, возникающих на  $\Delta t_{\text{об}}$  ( $\Delta t_{\text{с}}$ ), фиксируется в системе как один сбой соответствующего УС. Временная эпюра работы УС представлена на рис. 4.17. ВМ также имеет циклическую организацию работы с разбиением на интервалы  $\Delta t_{\text{ВМ}}$ . Любое количество неисправностей, возникающих на  $\Delta t_{\text{ВМ}}$ , фиксируется в системе как один сбой ВМ. Анализ надежности проводился для следующих значений временных параметров системы:  $\tau_{\text{ц}} = 25\text{мс}$ ,  $\Delta t_{\text{с}} = 2\text{мс}$ ,  $\Delta t_{\text{об}} = 15\text{мс}$ ,  $\Delta t_{\text{ВМ}} = 1\text{с}$ .

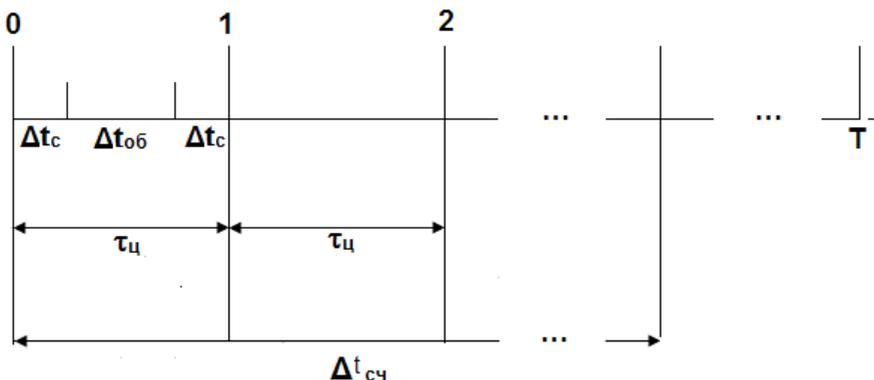


Рис. 4.17. Временная эпюра работы УС ОУВС.

#### 4.4.1. Анализ надежности устройств связи, работающих в режиме обмена

Анализ надежности элементов ОУВС (определение вероятностей возникновения исходных событий в деревьях отказов) проводится в соответствии с установленными в системе критериями определения типов неисправностей устройств. Для УС, работающих в режиме обмена с внешней средой, применяется частотный критерий принятия сбоящего устройства отказавшим. Смысл частотного критерия состоит в том, что происходит подсчет количества сбоев УС-а на заданном интервале времени ( $\Delta t_{сч}$ ) (см. рис. 4.17); в случае превышения этим значением некоторого заданного уровня ( $m_{кр}^{об}$ ) УС признается отказавшим. Процедура принятия сбоящего УС-а отказавшим реализуется с помощью специального счетчика, подсчитывающего количество сбоев на интервале  $(i * \Delta t_{сч} \div (i+1) * \Delta t_{сч})$ ,  $i=0,1,\dots,l_{об}-1$ ,

$$l_{об} = \left\lceil \frac{T}{\Delta t_{сч}} \right\rceil, T - \text{время функционирования системы,}$$

$\lceil a \rceil$  – означает целую часть  $a$ .

Вероятность признания неисправности УС, работающего в режиме обмена, сбоем на интервале  $(0, T)$  определяется как

$$P_{cб}(T) = \left[ \sum_{i=0}^{m_{кр}^{об}-1} C_n^i q_{cб}^i(\Delta t_{об}) p_{cб}^{n-i}(\Delta t_{об}) \right]^{l_{об}}, \text{ где } n = \frac{T}{\tau_{ц}}; \quad (4.27)$$

$P_{cб}(\Delta t_{об}) = e^{-\lambda_{cб}\Delta t_{об}}$  – вероятность бессбойной работы на интервале обмена;  $q_{cб}(\Delta t_{об}) = 1 - e^{-\lambda_{cб}\Delta t_{об}}$  – вероятность возникновения сбоев на интервале обмена.

Подставляя (4.27) в (4.26), получаем выражение для определения функции распределения случайного времени возникновения отказа УС обмена (с учетом как отказов, так и сбоев).

При большом значении  $n$  вычисления по формуле (4.27) становятся громоздкими. Поэтому на практике обычно используют пуассоновское приближение к биномиальному распределению, точность которого увеличивается при увеличении числа  $n$  и уменьшении вероятности  $q_{cб}(\Delta t_{об})$ . Тогда

$$P_{cб}(T) = \left[ \sum_{i=0}^{m_{кр}^{об}-1} \frac{(\lambda_{cб}\Delta t_{сч})^i}{i!} e^{-\lambda_{cб}\Delta t_{сч}} \right]^{l_{об}}. \quad (4.28)$$

Следующий этап упрощения выражения (4.27) связан с записью вероятности признания неисправности УС обмена сбоем на интервале времени работы счетчика через дополнительные события. Учет лишь первого члена из суммы вероятностей признания сбойшего УС отказавшим позволяет записать (4.28) в виде

$$P_{cб}(T) = \left[ 1 - e^{-\lambda_{cб}\Delta t_{сч}} \frac{(\lambda_{cб}\Delta t_{сч})^{m_{кр}^{об}}}{m_{кр}^{об}!} \right]^{l_{об}}. \quad (4.29)$$

Оценка погрешности определения  $P_{cб}(T)$  по (4.29) связана с оценкой остаточного члена ряда Тейлора  $R_n(x_0, x)$  для функции  $e^x$  ( $x = \lambda_{cб}\Delta t_{сч}$ ) с частичной суммой  $S_n = \sum_{i=0}^n \frac{x^i}{i!}$ , где  $n = m_{кр}^{об} - 1$ .

Для заданных параметров системы  $\lambda_{сб} = 4$  1/ч,  $\Delta t_{сч} = 5$ с,  $m_{кр}^{об} = 5$  погрешность вычислений при учете только первого члена  $S_n$  составляет 1%. Дополнительный учет в (4.29) второго члена снижает погрешность до 0,01%. Оценка производилась для остаточного члена, записанного в форме Лагранжа.

#### 4.4.2. Анализ надежности устройств связи, работающих в режиме согласования

Для УС, работающих в режиме межмашинного согласования, применяется последовательный критерий определения типа неисправности. Точное исследование надежного поведения по сбоям для этого режима может быть осуществлено методами комбинаторного анализа. Структура комбинаторной формулы для определения вероятности признания неисправности УС сбоем отражает количество поврежденных интервалов согласования, при котором не встретилось  $m_{кр}^c$  подряд искаженных интервалов. Для заданного в системе значения  $m_{кр}^c$ , равного 2, вероятность безотказной работы УС, работающего в режиме согласования, есть

$$P_{сб}(T) = \sum_{i=0}^{l_c} C_{l_c-1+i}^i q_{сб}^i (\Delta t_c) p_{сб}^{l_c-i} (\Delta t_c), \quad (4.30)$$

где  $l_c = \left\lfloor \frac{2T}{\tau_{ц}} \right\rfloor$ .

Ввиду громозкости точных комбинаторных выражений для  $P_{сб}(T)$  при значениях параметра  $m_{кр}^c > 2$  и здесь целесообразно воспользоваться приближениями.

Приближенная оценка для  $P_{сб}(T)$  осуществляется при использовании аппарата конечных цепей Маркова. При этом процесс функционирования УС по сбоям в режиме согласования представляется цепью, показанной на рис 4.18.

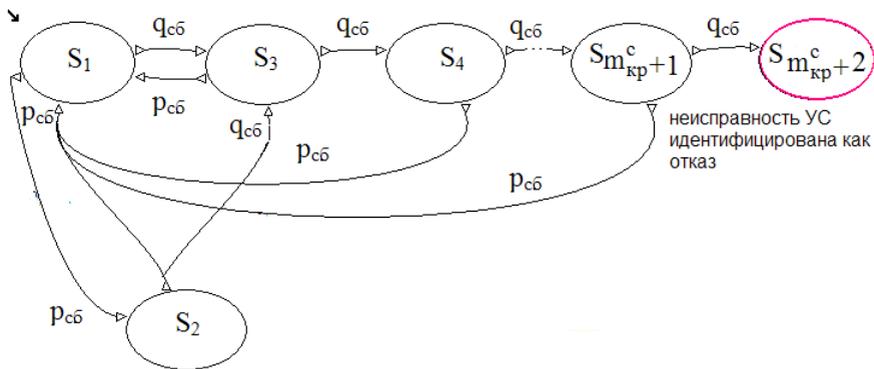


Рис. 4.18. Марковская цепь процесса обработки неисправностей УС для режима согласования.

Для данной цепи определяется среднее время до попадания в поглощающее состояние  $S_{m_{кр}^c+2}$ , соответствующее  $m_{кр}^c$  неудавшимся попыткам согласования:

$$T_{ср} = M_1[f_{m_{кр}+2}] \Delta t_c, \quad (4.31)$$

где  $M_1[f_{m_{кр}+2}] \Delta t_c$  - среднее число шагов, за которое цепь впервые попадает в состояние  $S_{m_{кр}^c+2}$  из начального состояния.

Система алгебраических уравнений для нахождения среднего числа шагов до попадания в заданное состояние имеет вид:

$$M_i[f_j] = \sum_k p_{ik} M_k[f_j] - p_{ij} M_j[f_j] + 1, \quad (4.32)$$

где  $M_i[f_j]$  - матрица средних времен достижения с элементами  $m_{ij}$ , соответствующими среднему числу шагов первого попадания из  $i$ -го состояния в  $j$ -е;  $p_{ij}$  - элементы матрицы  $(P)$  переходных вероятностей цепи, соответствующие вероятностям переходов из  $i$ -го состояния в

$j$ -е за один шаг, равный в данном случае  $\Delta t_c$ . Матрица  $P$ , размерностью  $m_{кр}^c + 2 \times m_{кр}^c + 2$ , для цепи, изображенной на рис. 4.18, представляет собой:

$$P = \begin{vmatrix} 0 & p & q & 0 & \dots & 0 & 0 \\ p & 0 & q & 0 & \dots & 0 & 0 \\ p & 0 & 0 & q & \dots & 0 & 0 \\ p & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \vdots & \dots & \dots \\ p & 0 & 0 & 0 & \dots & 0 & q \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{vmatrix}$$

Решение системы (4.32) позволяет определить среднее время до попадания в состояние, соответствующее признанию сбоившего устройства отказавшим по последовательностному критерию:

$$T_{cp} = \Delta t_c \frac{1 - q^{m_{кр}^c}}{pq^{m_{кр}^c}}. \quad (4.33)$$

Приближенное определение вероятности признания неисправности УС согласования сбоем осуществляется по формуле

$$P_{сб}(T) = e^{\frac{-T}{T_{cp}}}. \quad (4.34)$$

О допустимости применения экспоненциального распределения с параметром  $1/T_{cp}$  для систем с быстрым восстановлением см., например, [47, 48].

Результаты сравнения значений  $P_{сб}(T)$ , вычисленных по точному (4.30) и приближенному (4.34) выражениям при значениях параметров системы  $m_{кр}^c = 2$ ,  $\lambda_{сб} = 4$  1/ч,  $\Delta t_c = 2$ мс,  $T = 10000$ ч показали практическое их совпадение (в пределах машинной точности).

Значение показателей надежности УС, работающих в режиме обмена, сведены в таблицу 4.2, а в режиме согласования в таблицу 4.3.

Определение показателей осуществлялось для следующих параметров системы  $\tau_{ц} = 25\text{мс}$ ,  $\Delta t_0 = 15\text{мс}$ ,  $\Delta t_e = 2\text{мс}$ ,  $\Delta t_{сч} = 5\text{с}$ ,  $\lambda_{откУС} = 0,7 \cdot 10^{-6} \text{ 1/ч}$ ,  $T = 10000\text{ч}$ .

Таблица 4.2. Показатели надежности УС, работающих в режиме обмена

$\lambda_{сб} \text{ [1/ч]}$	$m_{кр}^c$	$T_{ср.сб.} \text{ [ч]}$	$P_{б.п.сб.}(T)$	$Q(T)$
4	1	$\sim 2,5E-1$	$\sim 0$	$\sim 1$
	2	$1,515E+2$	$6,338E-18$	$\sim 1$
	3	$1,37E+5$	$9,573E-1$	$4,942E-2$
	4	$1,675E+8$	$9,9996E-1$	$7,011E-3$
	5	$2,564E+11$	$9,999997E-1$	$6,98E-3$
	6	$4,762E+14$	$9,999999E-1$	$6,97E-3$
20	1	$\sim 5E-2$	$\sim 0$	$\sim 1$
	2	$6,098E+0$	$\sim 0$	$\sim 1$
	3	$1,064E+3$	$3,553E-3$	$9,665E-1$
	4	$2,703E+5$	$9,78E-1$	$2,878E-2$
	5	$8,333E+7$	$9,9993E-1$	$7,047E-3$

Таблица 4.3. Показатели надежности УС, работающих в режиме согласования

$\lambda_{сб}$ [1/ч]	$m_{кр}^c$	$T_{ср.сб.}$ [ч]	$P_{б.р.сб.}(T)$	$Q(T)$
4	1	$\sim 2,5E-1$	$\sim 0$	$\sim 1$
	2	$1,125E+5$	$9,859E-1$	$2,1E-2$
	3	$5,076E+10$	$9,99999968E-1$	$6,976E-3$
	4	$2,278E+16$	$\sim 1$	$6,976E-3$
20	1	$\sim 5E-2$	$\sim 0$	$\sim 1$
	2	$4,505E+3$	$7,01E-1$	$3,04E-1$
	3	$4,05E+8$	$9,99996E-1$	$6,979E-3$
	4	$3,65E+13$	$9,9999999996E-1$	$6,975E-3$

#### 4.4.3. Анализ надежности УС, работающих в двух режимах

Начальная (трехмашинная) конфигурация предполагает работу верхних УС (1-9) попеременно в двух режимах (обмена с внешней средой и межмашинного согласования). В этом случае решение о типе неисправности устройства принимается в зависимости от режима работы, а задача определения вероятности признания неисправного УС отказавшим сводится к задаче определения функции распределения минимума двух случайных величин.

Вычисленные значения для вероятностей признания сбоящих УС отказавшими в случае двухрежимной работы, для ряда сочетаний значений критериев приведены в табл.4.4. (а и б).

Таблица 4.4а. Вероятность признания сбоев УС отказом при двухрежимной работе ( $\lambda_{сб}=4$  1/ч)

$m_{кр}^{об}$ $m_{кр}^c$	1	2	3	4	5
1	1	1	1	1	1
2	1	1	$5,62E-2$	$1,416E-2$	$1,412E-2$
3	1	1	$4,27E-2$	$3,585E-5$	$5,492E-8$
4	1	1	$4,27E-2$	$3,582E-5$	$2,34E-8$

Таблица 4.4б. Вероятность признания сбоев УС отказом при двух-режимной работе ( $\lambda_{сб}=20$  1/ч)

$m_{кр}^{об}$ / $m_{кр}^с$	1	2	3	4	5
1	1	1	1	1	1
2	1	1	9,975E-1	3,144E-1	2,99E-1
3	1	1	9,964E-1	2,196E-2	7,595E-5
4	1	1	9,964E-1	2,195E-2	7,2E-5

#### 4.4.4. Анализ надежности вычислительной машины

Критерием отказа ВМ является неуспех  $m_{кр}^{ВМ}$  попыток восстановления выполняемого вычислительного процесса. При неуспехе  $m_{кр}^{ВМ}$  попыток машина считается отказавшей и исключается из активной конфигурации. Предполагается 100% эффективность процедур восстановления по отношению к сбоям, поэтому неуспех восстановления может быть связан лишь с возникновением повторных сбоев при ее включении в активную конфигурацию после восстановления. Таким образом, процедура определения показателей надежности ВМ аналогична процедуре, применяемой для УС-ов, работающих в режиме согласования. Вычисленные значения показателей надежности ВМ представлены в таблице 4.5. Показатели вычислялись при следующих значениях цикла работы ВМ  $\Delta t_{ВМ} = 1с$  и интенсивности потока отказов  $\lambda_{отк} = 2,34E-6$  1/ч.

Таблица 4.5. Показатели надежности ВМ

$\lambda_{сб}$ [1/ч]	$m_{кр}^{ВМ}$	$T_{ср.сб.}$ [ч]	$P_{б.р.сб.}(T)$	$Q(T)$
<b>10</b>	<b>1</b>	$\sim 1,0E-1$	$\sim 0$	$\sim 1$
	<b>2</b>	$3,615E+1$	$\sim 0$	$\sim 1$
	<b>3</b>	$1,302E+4$	$4,639E-1$	$5,467E-1$
	<b>4</b>	$4,695E+6$	$9,979E-1$	$2,521E-2$
	<b>5</b>	$1,695E+9$	$\sim 1$	$2,313E-2$
<b>50</b>	<b>1</b>	$\sim 2E-2$	$\sim 0$	$\sim 1$
	<b>2</b>	$1,471E+0$	$\sim 0$	$\sim 1$
	<b>3</b>	$1,064E+2$	$1,501E-41$	$\sim 1$
	<b>4</b>	$7,692E+3$	$2,725E-1$	$7,338E-1$
	<b>5</b>	$5,555E+5$	$9,822E-1$	$4,055E-2$
	<b>6</b>	$4,167E+7$	$9,998E-1$	$2,336E-2$

#### 4.5. Результаты анализа ОУВС

В таблице 4.6 представлены результаты расчетов вероятности безотказной работы ( $P(T)$ ) ОУВС для ряда значений  $m_{кр}$ . Анализ зависимости  $P(T)$  от  $m_{кр}$  позволил определить значения  $m_{кр}^{ВМ}$ ,  $m_{кр}^{об}$ ,  $m_{кр}^с$ , граничные с точки зрения влияния безотказности элементов на безотказность системы в целом. Так достижение высокой безотказности системы возможно только при  $m_{кр}^{ВМ} \geq 4$ . Значение показателя  $P(T)$  в указанном в табл.4.6 диапазоне  $m_{кр}^{об}$ ,  $m_{кр}^с$  в основном определяется показателями безотказности блока ВМ и практически не зависит от УС. Это обусловлено, во-первых, принятыми структурными и алгоритмическими решениями обеспечения отказоустойчивости УС (степень резервирования УС выше, чем ВМ) и, во-вторых, меньшей (примерно в три раза) интенсивностью постоянных отказов одного УС по сравнению с одной ВМ. Вероятность безотказной работы ОУВС  $P(T)$  для  $m_{кр}^{об} = 2$  при любых значениях  $m_{кр}^{об}$ ,  $m_{кр}^{ВМ}$  приблизительно равна нулю ( $\leq 10^{-18}$ ), т.е. полностью определяется потоком сбоев и алгоритмом их обработки, принятым для УС обмена.

Таблица 4.6. Результаты расчетов вероятности безотказной работы (P(T)) ОУВС.

		10000 ч	30000 ч
$m_{кр}^{об} \geq 4$	$m_{кр}^{ВМ} \geq 4$	0,9984	0,9867
$m_{кр}^c \geq 3$	$m_{кр}^{ВМ} = 3$	0,476	0,037
$m_{кр}^{об} = 3$	$m_{кр}^{ВМ} \geq 4$	0,998	0,984
$m_{кр}^c = 2$	$m_{кр}^{ВМ} = 3$	0,474	0,034

Результаты расчетов дали возможность определить значения  $m_{кр}^{ВМ}$ ,  $m_{кр}^{об}$ ,  $m_{кр}^c$ , граничные с точки зрения влияния потока сбоев и потока отказов на показатели безотказности (см. табл.4.3 – 4.6):

- для ВМ при интенсивности потока сбоев  $\lambda_{сбВМ} \cong 10$  1/ч при  $m_{гр1} \geq 4$  показатели безотказности системы не зависят от сбоев, а при  $m_{гр2} \leq 2$  – не зависят от отказов; если интенсивность потока сбоев ВМ  $\lambda_{сбВМ} \cong 50$  1/ч, то эти граничные значения становятся  $m_{гр1} \geq 6$  и  $m_{гр2} \leq 4$ ;
- для УС согласования  $m_{гр1} \geq 3$ ,  $m_{гр2} < 2$  ( $\lambda_{сбУС} \cong 4$  1/ч) и  $m_{гр1} \geq 3$ ,  $m_{гр2} \leq 2$  ( $\lambda_{сбУС} \cong 20$  1/ч);
- для УС обмена  $m_{гр1} \geq 4$ ,  $m_{гр2} \leq 2$  ( $\lambda_{сбУС} \cong 4$  1/ч) и  $m_{гр1} \geq 5$ ,  $m_{гр2} \leq 3$  ( $\lambda_{сбУС} \cong 20$  1/ч).

Кроме того, по результатам расчетов можно сделать выводы о том, что для УС, работающих в двух режимах, целесообразно осуществлять сбалансированный выбор значений  $m_{кр}$ , при которых ни одно из двух значений не выходит на граничный уровень ( $m_{кр}^{об} \leq 2, m_{кр}^c \leq 1$ ).

## 5. ЗАКЛЮЧЕНИЕ

В монографии представлены результаты работ по исследованию ОУВС как объекта надежностного анализа и синтеза. Рассмотрены некоторые модели надежностного поведения ОУВС, основной акцент в которых сделан на учет сбоев и обработку неисправностей. Модели надежности, разработанные для оценки эффективности проектных решений, основываются на декомпозиции надежностного поведения системы. Для исследования эффективности проектных решений по алгоритмической обработке неисправностей проводится разделение на медленные процессы возникновения неисправностей и быстрые процессы их обработки. Для формирования моделей деградации работоспособности резервированных отказоустойчивых вычислительных систем применяются методы структурно-логической декомпозиции, в частности, разложение технической структуры и/или происходящих событий по полной группе ортогональных событий. Процесс возникновения неисправностей и последующей деградации технической структуры системы исследуется с привлечением логико-вероятностных моделей и марковских процессов с прерывным временем.

Анализ решений агрегирования моделей быстрых процессов обработки неисправностей в марковские модели надежности показал, что при моделировании ОУВС обычно проводят укрупнение состояний сбой и отказ в одно состояние и последующую корректировку интенсивностей выхода из укрупненного состояния. Результаты расчетов показателей надежности на моделях с укрупнением показали, что укрупнение существенно различных состояний (сбой, из которого есть возврат в исходное состояние; отказ, из которого принципиально отсутствует возврат в исходное состояние) порождает недопустимую погрешность, что позволило сделать вывод о недопустимости подобного укрупнения. В связи с этим предложена дискретная марковская модель обработки неисправностей с разделением состояний отказ и сбой и учетом возможности возникновения вторичных неисправностей в процессе восстановления нормального хода вычислительного процесса, нарушенного сбоями. Техника интеграции модели обработки неисправностей в общую модель деградации технической структуры ОУВС основывается на вычислении финальных

вероятностей при векторах начальных условий, соответствующих возникновению либо сбоя, либо отказа.

Проведены исследования влияния параметров средств контроля на характеристики надежности ОУВС. Для реализации такого исследования предложен оригинальный подход формирования параметрической матрицы переходов марковского процесса. Исследования показали существенное влияние на надежность ОУВС полноты и надежности контроля. Возможно полноту контроля целесообразно рассматривать в зависимости от состояния анализируемого объекта (системы, вычислительной машины), причем надежность контроля связана с полнотой контроля.

Проведенные исследования расширили перечень подходов к моделированию надежности отказоустойчивых управляющих вычислительных систем.

## ЛИТЕРАТУРА

1. Avizienis A. et al. The STAR (self-testing and repairing) computer: An investigation of the theory and practice of fault-tolerant computer design. // IEEE Trans. Comput., vol. C-20, no. 11, pp. 1312-1321, Nov. 1971.
2. Avizienis A. Architecture of fault-tolerant computing systems. // Dig. 1975 Int. Symp. Fault-Tolerant Computing, Paris, France, June 1975, pp. 3-16.
3. Landwehr C., Randell B., Simoncini L. Dependable Computing and Fault-Tolerant Systems Vol. 1: The Evolution of Fault-Tolerant Computing. Wien: Springer-Verlag, 1993, P.384.
4. Лобанов А.В. Протокол отказоустойчивого обмена // Приборы и системы управления. 1993. № 7. С. 8-11.
5. Лобанов А.В., Нахаев С.А. Обеспечение сбое- и отказоустойчивости в протоколе отказоустойчивого обмена // Приборы и системы управления. 1993. № 7. С. 12-13.
6. Lala J.H, Harper R.E Architectural Principles for Safety-Critical Real-Time Applications, Proc. IEEE, V82 n1, Jan 1994, pp25-40.
7. Siewiorek, D., ed., Fault-Tolerant Computing Highlights from 25 Years, Special Volume of the 25th International Symposium on Fault-Tolerant Computing FTCS-25, Pasadena, CA, June 1995. P.449.
8. Avizienis A. Toward Systematic Design of Fault-Tolerant Systems. - Computer, 30(4), April 1997, pp. 51-58.
9. Лобанов А.В. Распределенное мажорирование информации с обнаружением и идентификацией неисправностей // Автоматика и телемеханика 1997. № 1. С. 145-149.
10. Лобанов А.В. Организация сбое- и отказоустойчивых вычислений в полносвязных многомашинных вычислительных системах // Автоматика и телемеханика. 2000, № 12. С. 138-146.
11. Родзин С.И. Отказоустойчивые вычислительные системы. Таганрог: Изд-во ТРТУ. 2001, 274 с.

12. Белоусов Ю.А. Отказоустойчивые бортовые вычислительные системы. Классификация и оценка технических характеристик // Авиакосмическое приборостроение. 2004, №11. С. 17-24.
13. Шубинский И.Б. Функциональная надежность информационных систем. Методы анализа. Ульяновск: Надежность. 2012. - 295 с.
14. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. Ульяновск: Надежность. 2012. - 215 с.
15. Shooman M.L. Reliability of Computer Systems and Networks \John Wiley & Sons Inc., 2002, p.521..7 No. 3, September, 2012. Pp.66-73.
16. Каравай М.Ф., Подлазов В.С. Расширенный обобщенный гиперкуб как отказоустойчивая системная сеть для многопроцессорных систем // Управление большими системами. 2013. выпуск 45. С. 344-371.
17. Ng Y.-W., Aviiienis A. A model for transient and permanent fault recovery in closed fault tolerant systems. // Proc. 1976 Int. Symp. Fault-Tolerant Computing, Pittsburgh, PA, June 1976, pp.182-188.
18. Castes A., Doucet J.E., Landrault C., Laprie J.S. SURF: A program for dependability evaluation of complex fault-tolerant computing systems. – Proc.1981, Int.Symp. Fault Tolerant Computing Systems, FTCS-11, 1981, pp. 72-78.
19. Muazzani M., Trivedi K. Dependability prediction: comparison of tools and techniques. – SAFECOMP '86: Trends in safe real time computer systems: proceedings of the Fifth IFAC Workshop, Sarlet, France, 14-17 October 1986, pp. 171-178.
20. Bavuso S.J., Dugan J.B., Trivedi K.S., Rothmann E.M., Smith W.E. Analysis of typical fault-tolerant architectures using HARP. – IEEE Transactions on Reliability, vol. R-36, no.2, 1987, Jun, pp.176-185.
21. Geist R.; Trivedi K.S. Reliability estimation of fault-tolerant systems: tools and techniques.-Computer, vol. 23, Issue 7, Jul 1990, pp. 52 – 61.

22. Balakrishnan M., Raghavendra C.S. An Analysis of a Reliability Model for Repairable Fault-Tolerant Systems. - IEEE Transactions on Computers, vol.42, no.3, Mar.,1993, pp. 327-339.
23. Викторова В.С., Кунтшер Х.П., Петрухин Б.П., Степанянец А.С. Relex – программа анализа надежности, безопасности, рисков. // Надежность. 2003. №4 (7). С.42-64.
24. Викторова В.С., Степанянец А.С. Использование модулей Relex при анализе надежности и безопасности систем. // Надежность. 2004. №2 (9). С. 64-71.
25. Викторова В.С., Степанянец А.С. Анализ программного обеспечения моделирования надежности и безопасности систем. // Надежность. 2006. №4 (19). С. 46-57.
26. Викторова В.С., Кунтшер Х.П., Степанянец А.С. Обзор программных разработок по анализу надежности и безопасности систем. // Труды международной конференции “Программные продукты информационного обеспечения безопасности полетов, надежности и технической эксплуатации авиационной техники”. Москва. 14-16 марта 2006. С. 17-26.
27. Викторова В.С., Степанянец А.С. Динамические деревья отказов // Надежность. 2011. № 3. С. 20-32.
28. Викторова В.С., Степанянец А.С. Модели и методы расчета надежности технических систем. Изд. 2, испр. М.: Издательская группа URSS, ООО «ЛЕНАНД», 2016. – 256 с.
29. Molloy M.K., Performance analysis using stochastic Petri nets. IEEE Trans. Comput., C-31, 1982, pp.913-917
30. Петерсон Дж. Теория сетей Петри и моделирование систем. М:Мир, 1984. – 264 с..
31. Chiola G., Marsan M., Balbo G., Conte G. Generalized Stochastic Petri Nets: A Definition at the Net Level and its Implications. - IEEE Transactions on Software Engineering 19(2), 1993, pp. 89-107.
32. Ng Y.W., Avizienis A.A. A unified reliability model for fault tolerant computers. IEEE Transactions on Computers, vol. C-29, no.11, Nov. 1980, pp.1002-1011.
33. Парамонов П.П, Жиринов И.О. Интегрированные бортовые вычислительные системы: обзор современного состояния и анализ перспектив развития в авиационном приборострое-

- нии. // Научно Технический вестник информационных технологий, механики и оптики, Выпуск № 2 (84), 2013. С. 1-17.
34. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза. М.: Печ. двор. 2016. - 544 с.
  35. Geist R.M.; Trivedi K.S. Ultrahigh reliability prediction for fault-tolerant systems. -IEEE Transaction on Computers, vol. C-32, no. 12, Dec 1983, pp. 1118 – 1127.
  36. Balakrishnan M., Raghavendra C.S. On reliability modeling on closed fault-tolerant computer systems. - IEEE Transaction on Computers, vol. C-39, no. 4, Apr 1991, pp. 571 –575.
  37. Спиридонов И.Б., Степанянц А.С., Викторова В.С. Design testability analysis of avionic systems // Reliability: theory & applications. 2012. Vol. 7, № 3 (26). С. 66-73  
[http://www.gnedenko-forum.org/Journal/2012/032012/RTA\\_3\\_2012-08.pdf](http://www.gnedenko-forum.org/Journal/2012/032012/RTA_3_2012-08.pdf).
  38. Лубков Н.В., Спиридонов И.Б., Степанянц А.С. Влияние характеристик контроля на показатели надежности систем // Труды МАИ. 2016. Выпуск № 85. С. <http://www.mai.ru/science/trudy/published.php?ID=67501>.
  39. Можаяев А.С., Громов В.Н. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем. СПб. ВИТУ, 2000. -144 с.
  40. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб.: Изд-во С.-Петербур. ун-та, 2007. - 276 с.
  41. Степанянц А.С. Вычисление параметра потока отказов в логико-вероятностных моделях методом рекурсивного наращивания переменных.- Автоматика и Телемеханика, № 9, 2007, С. 161-175.
  42. Zhou Jinglun, Sun Quan. Reliability analysis based on binary decision diagrams. Journal of Quality in Maintenance Engineering. 1998, vol.4, issue 2, pp. 150-161.
  43. Bartlett, L.M. Neural network selection mechanism for BDD construction. Quality and reliability engineering international, 2004, 20 (3), pp. 217-223

44. Woo Sik Jung, Sang Hoon Han and Jaejoo Ha. A fast BDD algorithm for large coherent fault trees analysis. - Reliability Engineering & System Safety, 2004, Vol. 83, Issue 3, pp. 369-374.
45. Remenyte R.; Andrews, J.D. A simple component connection approach for fault tree conversion to binary decision diagram. - Availability, Reliability and Security, 2006. ARES 2006. /The First International Conference, 20-22 April 2006 , 8 pp.
46. Черкесов Г.Н. Надежность аппаратно-программных комплексов/Учебное пособие. - СПб,: “Питер”, 2005, -.480 стр.
47. Коваленко И. Н. Исследования по анализу надежности сложных систем. — Киев: Наукова Думка, 1975, - 212 стр.
48. Ушаков И.А. Вероятностные модели надежности информационно вычислительных систем. М.: Радио и связь, 1991. – 132 с.