щим причинам на отдельные классы, характеризующиеся различными видами источников общих причин, и адаптация существующих параметрических моделей применительно к специфике каждого класса.

Детализация моделей должна касаться определения показателей, характеризующих событие отказа по общей причине: возможность и периодичность контроля таких событий, возможность и времена их устранения. Методика их определения должна учитывать возможность различных стратегий контроля отказов и их устранения, условия безопасной эксплуатации АС. Число элементов, отказавших в одном событии по одной общей причине, может быть избыточно по сравнению с числом элементов, достаточным для отказа системы. Поэтому модель восстановления элементов, отказавших в таком событии, должна учитывать необходимость устранения отказов нескольких элементов для восстановления работоспособности системы. Очередность восстановления элементов может зависеть от стратегий контроля отказов и ремонта элементов.

Способ введения событий отказов по общей причине в логическую модель должен обеспечивать ее компактность при моделировании различных задач. Это достигается при осуществлении этой процедуры на уровне минимальных сечений. Алгоритм процедуры должен исключать возможность недоучета или многократного учета одних и тех же минимальных сечений с отказами по общей причине, предусматривать способы просеивания минимальных сечений и оценку значений необходимых параметров, характеризующих событие отказа по общей причине. Алгоритм должен быть реализован в расчетной программе для персональной ЭВМ, совместимой с остальными программами для проведения вероятностных анализов безопасности АС.

2.4.Разработка методики анализа функциональных зависимостей.

Анализ и моделирование функциональных зависимостей проводится на различных этапах выполнения ВАБ. Особенностью методики проведения ВАБ, разработанной в институте "Атомэнергопроект", являются три уровня моделирования путей развития аварии /25/. На верхнем уровне моделирование проводится с помощью функционально-системных деревьев событий (см.рис.2.3), представляющих логическую модель развития аварии от исходного события до множества конечных состояний. Пути развития аварии отображаются на них в виде отдельных траекторий, которые характеризуются функциональными минимальными сечениями (т.е. минимальным набором функций безопасности, невыполнение которых приводит к реализации рассматриваемого пути развития аварии).

На втором уровне рассматривается перечень систем безопасности, выполняющих свои функции при рассматриваемом исходном событии (эти системы отражены на функциональных деревьях), и разрабатываются логические диаграммы (см.рис.2.4), описывающие условия выполнения или невыполнения) функции каждой такой технологической системой безопасности. Элементами диаграммы являются модули, представляющие отдельные каналы технологических и обеспечивающих систем или их части, а также наиболее важные действия персонала.

На основании построенных диаграмм производится преобразование при помощи ЭВМ каждого пути развития аварии (функционального минимального сечения) в набор модуляризованных минимальных сечений, т.е. сечений, элементами которых являются отказы модулей.

На третьем уровне производится разработка детальных вероятностных моделей, характеризующих рассматриваемые пути развития аварий. Эти модели представляют собой элементные деревья отказов для отдельных модулей (см.рис.2.5). Такое представление путей развития

Исходное событие	Системы/функции безопасности					Характеристика аварийной последовательности			
	АЗ	САОЗ ВД	САР	ГА	САОЗ НД	N	Тип КС	Время до СМ	Булева функция
	a	f	p	g_1	g_2				
*	N	N	N			1	S		
O						2	S		
						3	СМ		fg_2
						4	СМ		fg_1
						5	СМ	5 часов	fp
	N	N	N			6	ATWS		a
→ mp									

mp - малая вероятность аварийной последовательности

N - выполнение функции не требуется

z - зависимый отказ

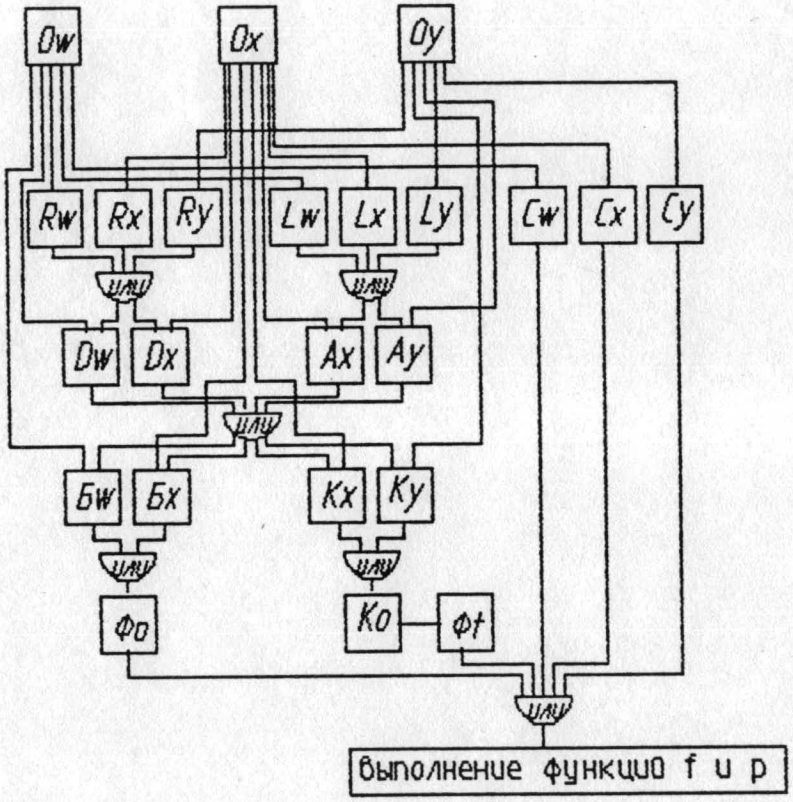
O - функция выполняется с участием персонала

S - безопасное состояние

СМ - плавление активной зоны

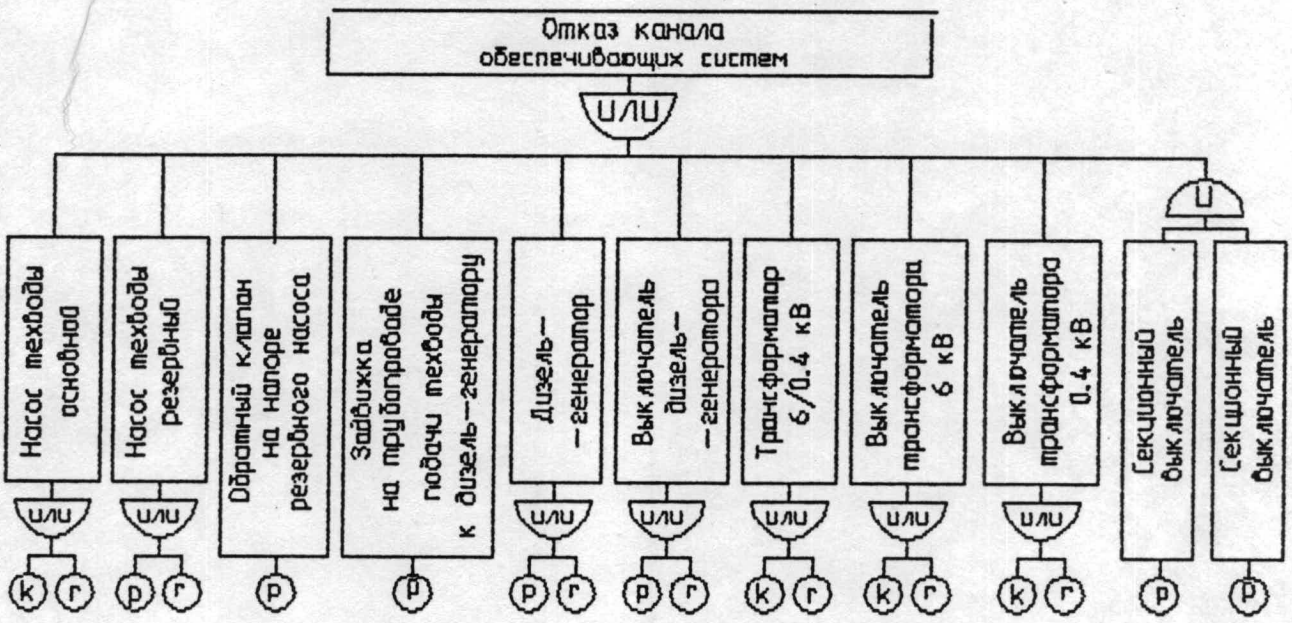
ATWS - класс аварий с отказом аварийной защиты

Рис. 2.3. Системно-функциональное дерево событий для малой течи и обесточивания для АЭС с реактором ВВЭР-440.



O —обеспечивающие системы
D —дополнительная система АПЭН
A —система АПЭН
Б —БРУ—А
K —система расхолаживания через технологические конденсаторы
C —САОЗ высокого давления
R —питательные узлы дополнительной системы АПЭН
L —питательные узлы системы АПЭН
X,Y,Z —индексы каналов систем
Фo —функция персонала по управлению БРУ—А
Фt —функция персонала по подготовке к работе системы расхолаживания через технологические конденсаторы

Рис.2.4. Структурно—функциональная схема совместного выполнения функций f u p.



к — явный отказ непрерывно контролируемого элемента в режиме ожидания
р — скрытый отказ периодически проверяемого элемента
г — отказ при работе во время аварии

Рис.2.5. Дерево отказов канала обеспечивающих систем (модули Ox, Oy, Oz на рис.2.4).

аварии в виде наборов модуляризованных минимальных сечений и элементных деревьев отказов для отдельных модулей позволяет:

-автоматически генерировать элементные деревья отказов, вершинными событиями которых являются модуляризованные минимальные сечения;

-получать полные наборы элементных минимальных сечений, необходимых для проведения количественного анализа.

Моделирование функциональных зависимостей между системами безопасности (их частями) производится на втором уровне с помощью логических диаграмм в виде структурно-функциональных схем.Структурно-функциональная схема представляет собой блок-диаграмму (модель путей успеха), на которой модули отображаются в виде отдельных блоков, а их зависимости - в виде линий со стрелками. Направление стрелок показывает ,что выполнение функции модулем, из которого исходит линия, необходимо для функционирования модуля, в который она входит. Для отображения более сложных зависимостей используются логические операторы "и", "или", "m из n". Входами структурно-функциональной схемы является выполнение заданных функций отдельными модулями, а выходом - выполнение хотя бы одной функции безопасности из образующих рассматриваемый путь развития аварии.

Критерием выделения части системы в отдельный модуль является полное совпадение функциональных зависимостей всех его элементов (или структурных частей) с остальными рассматриваемыми модулями, что устанавливается на основе таблиц качественного анализа (FMEA) (видов и последствий отказов элементов). Модуль может представлять собой отдельный канал системы безопасности, его часть, группу одноименных каналов ряда систем. Последнее типично для АС со сквозной канальностью систем безопасности и полным функциональным разделением отдельных каналов. На диаграмме, представленной на рис.2.4, так объединены каналы системы аварийного охлаждения активной зоны

высокого давления с влияющими только на их работоспособность обеспечивающими системами безопасности при рассматриваемом пути развития аварии (модули C_x, C_y, C_w). Также объединены в совместные модули каналы остальных обеспечивающих систем, оказывающих влияние на все рассматриваемые системы безопасности (модули O_x, O_y, O_w). В то же время системы безопасности, осуществляющие отвод тепла через второй контур, разбиты на более мелкие модули, так как эти системы имеют сложные перекрестные связи.

Критерием необходимости отображения действий персонала в виде отдельных модулей является их детерминированное влияние на работоспособность двух или более представленных на диаграмме модулей систем. Это могут быть действия, связанные с подготовкой систем к работе (модуль Φ_t) или управления системами при аварии (модуль Φ_o).

Для построения структурно-функциональной схемы осуществляется качественный анализ в следующей последовательности /I9,28/:

I.Для каждой функции безопасности, входящей в рассматриваемый путь развития аварии, определяются технологические системы, непосредственно выполняющие данную функцию;

2.Для каждой технологической системы безопасности определяются критерии ее успешного функционирования и структура системы. Возможно влияние исходного события аварии на работоспособность и эффективность отдельных систем, каналов и элементов и, следовательно, возникновение различных структур систем при рассматриваемом исходном событии. В этом случае определяется условная вероятность возникновения каждой структуры, для каждой из них проводится самостоятельный анализ, и строится отдельная структурно-функциональная схема;

3.Для каждого модуля технологических систем безопасности определяется достаточный для выполнения им своих функций (при условии нормальной работы остальных модулей системы) набор обеспечивающих

систем безопасности или их каналов и составных частей;

4.Определяется возможность резервирования каждого отказавшего модуля обеспечивающей системы безопасности ее работоспособными модулями. При этом не должна нарушаться работоспособность каких-либо технологических систем безопасности и оборудования нормальной эксплуатации смежного энергоблока (если обеспечивающая система общая для двух блоков);

5.Определяется степень снижения эффективности модулей технологических систем безопасности и возникающая их структура в случае отказа каких-либо модулей обеспечивающих систем безопасности;

6.Аналогичный анализ проводится для определения взаимного влияния обеспечивающих систем друг на друга, а также взаимного влияния технологических систем, если таковое имеет место;

7.Выявляются общие части в смежных технологических системах безопасности, приводящие в случае их отказа к невыполнению несколькими системами своих функций. Такие общие части моделируются отдельными модулями;

8.Выявляются действия персонала, общие для двух или более модулей систем, выполняющих рассматриваемые функции безопасности. Такие действия моделируются отдельными модулями;

9.Модули, оказывающие одинаковое влияние на выполнение системами своих функций, объединяются в группы, которые в дальнейшем моделируются как один укрупненный модуль.

Результаты качественного анализа используются для определения набора модулей и их зависимостей, отображаемых на структурно-функциональной схеме.

Структурно-функциональная схема используется для получения набора модульных минимальных сечений, характеризующих рассматриваемый путь развития аварии, что дает возможность проводить их качественное просеивание. Цель просеивания (отбрасывания незначимых) сечений

заключается в уменьшении размеров логической модели и, следовательно, затрат машинного времени и памяти.

Для проведения просеивания модульных минимальных сечений разработаны следующие принципы:

I.Просеивание осуществляется на основании результатов грубого оценивания вероятностей реализации модульных минимальных сечений;

2.Для проведения оценивания элементам модульных минимальных сечений присваиваются следующие вероятности:

$I*IO^{-1}$ -модулям,представляющим собой ошибочные действия персонала;

$I*IO^{-3}$ -части модульного минимального сечения (нескольким модулям), имеющей в своем составе хотя бы одну группу элементов, подверженных воздействию общей для всей группы причины;

$I*IO^{-2}$ -остальным модулям, элементы которых не подвержены воздействию общих причин совместно с элементами модулей, образующих оцениваемое сечение.

В качестве примера рассмотрим модульное минимальное сечение $O_xO_yC_w\Phi_o$,где:

Φ_o - модуль, представляющий ошибочные действия персонала (оценивается вероятностью 0,I);

C_w - отказ канала технологической системы безопасности(оценивается вероятностью 0,0I);

O_xO_y - отказы каналов обеспечивающих систем безопасности, которые имеют в своем составе элементы, подверженные воздействию одной общей причины (дизель-генераторы, выключатели и т.п.). Поэтому группа модулей O_xO_y оценивается вероятностью $I*IO^{-3}$.

Таким образом, грубая оценка вероятности реализации модульного минимального сечения составляет $I*IO^{-6}$;

3.Критерием исключения модульных минимальных сечений из дальнейшего рассмотрения является $I*IO^{-3}*P_{max}$, где P_{max} - наибольшая

вероятность реализации среди оцененных сечений. Исключаются сечения, имеющие меньшую, чем критериальное значение, вероятность. Например,если вероятность P_{max} составляет $I*IO^{-3}$ или менее, то рассмотренное выше сечение оставляется для дальнейшего анализа.

Проверка правомерности таких принципов просеивания была проведена в работе /26/. При моделировании пути развития аварии с помощью диаграммы, представленной на рис.2.4, было получено 60 модульных минимальных сечений. После просеивания было оставлено 7 из них для дальнейшего моделирования. Для проверки был рассчитан вклад отброшенных сечений в вероятность реализации пути развития аварии, который не превысил 0,5%.

Использование промежуточной логической модели (структурно-функциональной схемы) для моделирования функциональных зависимостей на уровне систем имеет следующие достоинства:

I) уменьшение объема вводимой в программу исходной логической информации;

2) наглядность отображения функциональных зависимостей в логической модели;

3) возможность проведения просеивания минимальных сечений на основании качественных или количественных критериев, позволяющая значительно сократить объем вычислений;

4) возможность получения списка доминантных модульных минимальных сечений системного уровня и их вероятностей. Это облегчает инженерный анализ получаемых количественных результатов.

Каскадные отказы рассматриваются на третьем уровне моделирования при проведении анализа надежности систем безопасности /28/. Такие отказы возникают детерминированно вследствие ограниченного числа определенных функциональных зависимостей между элементами системы, что позволяет моделировать их явно на элементном дереве отказов. Для этого необходимо, чтобы модель каскадных отказов поз-

воляла адекватно определять вероятности возникновения и устранения этих событий при использовании методологии минимальных сечений.

Как правило, проектом предусматриваются технические средства защиты против каскадных отказов. В таком случае интенсивность их возникновения определяется по формуле

$$\lambda_{ко} = \lambda_{П} * q_{зс} \qquad (2.4.I)$$

где $\lambda_{ко}$ -интенсивность каскадного отказа;

$\lambda_{П}$ -интенсивность отказа-первопричины;

$q_{зс}$ -условная вероятность отказа защитных средств при возникновении отказа-первопричины.

Например, при неоткрытии арматуры на напоре запускающегося центробежного насоса (отказ-первопричина),отказ технических средств будет заключаться в непрохождении сигнала от концевого выключателя арматуры на останов насоса.

Основной особенностью каскадных отказов, определяющей вид их логической модели, является необходимость восстановления нескольких элементов, отказавших одновременно. Это элемент, отказ которого явился первопричиной события, и один или несколько элементов, отказы которых явились следствием. Следует отметить, что последние получают способность выполнять заданные функции только после совместного восстановления и их самих, и элемента, отказ которого явился первопричиной события. В вышеуказанном примере насос может выполнить свои функции только после его восстановления совместно с восстановлением и открытием арматуры на напоре.

Необходимость восстановления нескольких элементов учитывается при определении времени устранения каскадного отказа. Следовательно, если отказ элемента А явился причиной отказа элементов $B_1,..B_n$, то среднее время устранения каскадного отказа B/A для экспоненциального закона времени восстановления элементов А и B_1, B_n опреде-

ляется по формулам:

а)при параллельном восстановлении элементов А и $B_1,...,B_n$:

$$t_b^{B/A} = \max\ (t_b^A;\ t_b^{B_i}) \qquad i=1,...,n \qquad (2.4.2)$$

б)при последовательном восстановлении элементов А и $B_1,...,B_n$:

$$t_b^{B/A} = t_b^A + \sum_{i=1}^{n} t_b^{B_i} \qquad (2.4.3)$$

где $t_b^{B/A}$ -время устранения каскадного отказа,

t_b^A -время восстановления элемента А,

t_b^B -время восстановления элемента В.

Примеры отображения события каскадного отказа на дереве отказов приведены на рис.2.6 и 2.7.

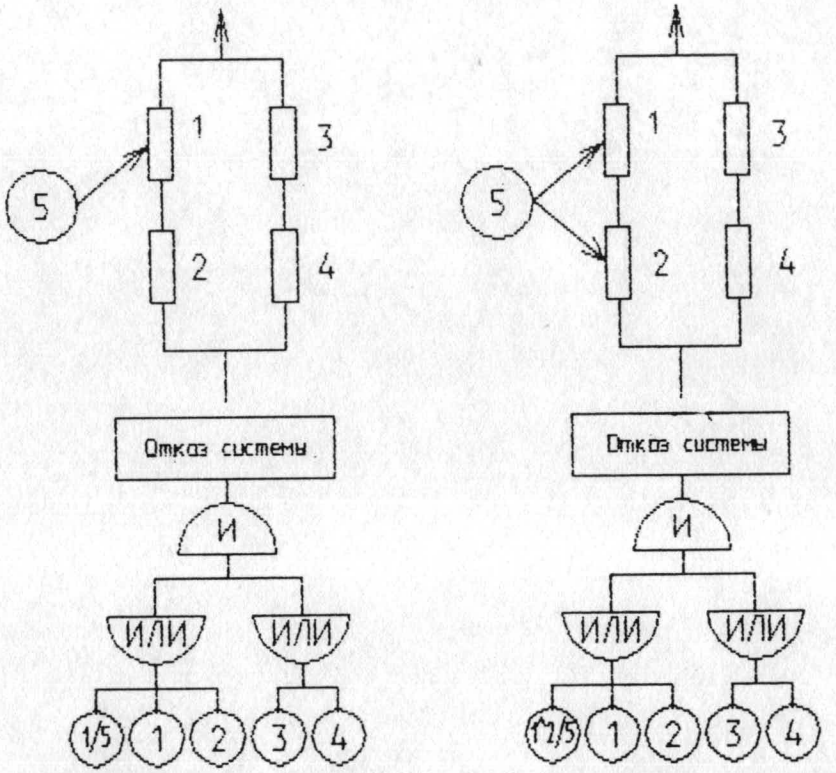
Возможны три отличающихся по структуре вида каскадных отказов:

I)отказ-первопричина вызывает зависимый отказ еще только одного элемента(элемент I на рис. 2.6а);

2)отказ-первопричина вызывает зависимые вторичные отказы нескольких элементов,независимые отказы которых объединены на дереве отказов одним логическим оператором "или"(элементы I и 2 на рисунке 2.6б);

3)отказ-первопричина вызывает вторичные зависимые отказы нескольких элементов,независимые отказы которых не объединены на дереве отказов одним логическим оператором "или"(элементы I и 2 на рисунке 2.7).

В первых двух случаях каскадный отказ отображается на дереве отказов одним первичным событием(событие I/5 на рис.2.6а или I^2/5



а) структурная схема надежности с каскадным отказом 1/5 и соответствующее ему дерево отказов

б) структурная схема надежности с каскадным отказом 1^2/5 и соответствующее ему дерево отказов

Рис.2.6. Примеры отображения каскадных отказов на дереве отказов.

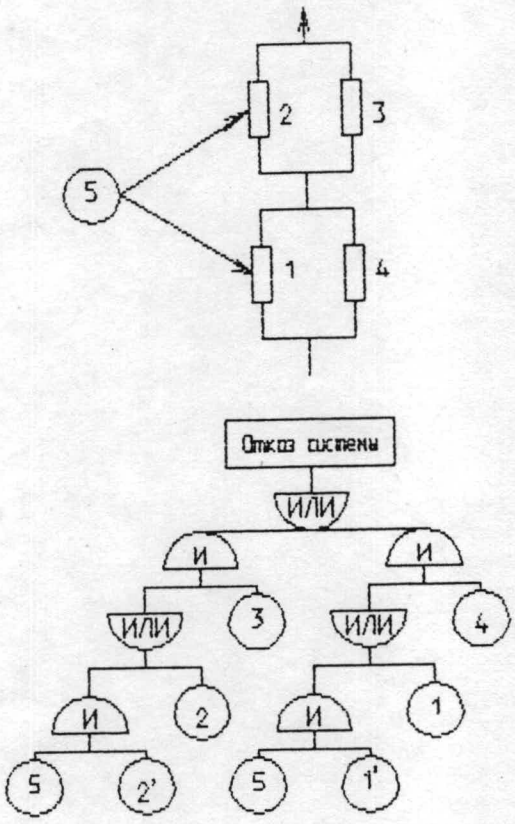


Рис.2.7. Пример отображения каскадного отказа на дереве отказов.

на рис.2.6б), которое присоединяется через логический оператор "или" к независимым отказам элемента(элементов), отказывающего(щих) в событии каскадного отказа вследствие отказа-первопричины.

Интенсивность события каскадного отказа определяется интенсивностью отказа-первопричины и условной вероятностью отказа защитных средств при их наличии(см.формулу 2.4.I). Время устранения каскадного отказа определяется временем восстановления отказа-первопричины и всех вторичных отказов по формулам 2.4.2 и 2.4.3. Наиболее сложным является третий случай,пример которого приведен на рис.2.7, где каскадный отказ I^2/5 входит в два минимальных сечения <2/5,3> и <I/5,4>.Очевидно,что первое сечение прекращает свое существование при устранении отказов 2 и 5,а второе сечение-отказов I и 5.Поэтому при моделировании таких случаев применяется следующий искусственный прием:

К независимому отказу каждого элемента,имеющего также вторичный зависимый отказ в событии каскадного отказа ,присоединяется через логический оператор "или" фрагмент дерева отказов. Фрагмент состоит из двух первичных событий,соединенных логическим оператором "и".Одно событие является отказом невосстанавливаемого элемента с интенсивностью возникновения каскадного отказа(см.формулу 2.4.I), а второе событие является отказом,возникающим с вероятностью единица и устраняемого при совместном восстановлении двух элементов - вызвавшего каскадный отказ и того из отказавших зависимо,к которому присоединен через оператор "или" данный фрагмент дерева отказов. На примере, приведенном на рис.2.7, каскадный отказ I^2/5 отображается двумя фрагментами, присоединенными через оператор "или" к независимым отказам I и 2.При этом:

-элементы 5 на дереве отказов являются невосстанавливаемыми с интенсивностью возникновения каскадного отказа,определяемой по формуле 2.4.I;

-элементы I' и 2' относятся к элементам Р типа (периодически контролируемые в режиме ожидания) с интенсивностью отказов равной нулю и вероятностью отказа на требование (независимая от времени составляющая),равной I.

Время восстановления элемента 2' определяется временем восстановления элементов 2 и 5,а элемента I'- временем восстановления элементов I и 5 по формуле 2.4.2 или 2.4.3.

2.5. Разработка методики анализа отказов по общей причине. Математические модели.

Основная цель разработки методики отказов по общим причинам состояла в создании эффективного инструмента, который бы позволил как количественно прогнозировать результат воздействия таких отказов на вероятностные показатели безопасности с возможно меньшей неопределенностью, так и гибко реагировать на различные проектные решения, направленные на повышение степени защищенности оборудования систем безопасности. Реализация указанного подхода привела к разработке детальных математических моделей отказов по общей причине, учитывающих разнообразную специфику последних /I9,23,28/. Эти модели предназначены для определения вероятности возникновения события отказа по общей причине и вероятности его устранения.

Интенсивность (вероятность) события определяется на основании задаваемых параметрических моделей и зависит только от вида общей причины, степени защиты против нее и числа отказавших элементов.

Методика определения вероятностей возникновения отказов по общей причине базируется на раздельном моделировании событий, имеющих различные по происхождению источники. Методика предусматривает выделение трех классов групп элементов, подверженных возможности отказа по общей причине. Признаками принадлежности групп элементов к тому или иному классу являются следующие:

I класс - общность конструкции резервируемых элементов;

2 класс - общность размещения резервируемых элементов различных каналов;

3 класс - одинаковые для различных элементов процедуры технического обслуживания и/или проверок, которые сопровождаются или могут сопровождаться изменением состояния элемента или его составных

частей.

Элементы различных каналов систем безопасности могут образовывать группы, имеющие признаки принадлежности к нескольким классам.

К первому классу отнесены элементы, у которых отказы по общей причине вызываются наличием дефектов изготовления и монтажа. Это приводит к снижению несущей способности элементов, что не всегда выявляется при пуско-наладочных или периодических испытаниях систем, т.к. нагрузки при испытаниях зачастую не полностью адекватны аварийным. Очевидно, что отказы такого типа являются неконтролируемыми при нормальной эксплуатации и не зависящими от времени безаварийной эксплуатации системы. Для их моделирования удобно использовать модель базового параметра, т.е. непосредственные статистические оценки вероятностей (или интенсивностей) отказов по общей причине определенных комбинаций резервируемых элементов q_i. В этом случае вероятность отказа Q_i ровно i элементов по общей причине определяется по формуле:

$$Q_i = C_n^i * q_i ; \quad i=1,\ldots,n \qquad (2.5.I)$$

где C_n^i - число сочетаний по i из n.

Верхние оценки средних вероятностей отказа на требование Q_2,Q_3 и Q_4 системы из 2-х,3-х и 4-х элементов, соответственно, по любым причинам на интервале времени T(при условии,что отсутствует восстановление отказавших элементов) имеют вид:

$$Q_2 = q_2 + \frac{1}{T} * \int_0^T q(t)dt; \qquad (2.5.2)$$

$$Q_3 = q_3 + 3*q_2*q_2 + 3*q_2*\frac{1}{T}*\int_0^T q(t)dt + \frac{1}{T} * \int_0^T q^3(t)dt;$$

$$Q_4 = q_4 + 3*q_2*q_2 + 6*q_3*q_3 + 12*q_3*q_2 + 12*q_2*q_2*$$

$$*\frac{1}{T}*\int_0^T q(t)dt + 4*q_3*\frac{1}{T}*\int_0^T q(t)dt + 6*q_2*\frac{1}{T}*\int_0^T q^2(t)dt+$$

$$+ \frac{1}{T}*\int_0^T q^4(t)dt;$$

где q_2, q_3, q_4 - вероятность отказа по общей причине определенных 2-х, 3-х и 4-х элементов, соответственно;

$q(t)$ - вероятность независимого отказа элемента.

В уравнениях 2.5.2 учтено, что на один элемент могут воздействовать одновременно не более двух причин, а также опущены члены более малых порядков (произведения минимальных сечений). Ряд слагаемых в правых частях уравнений 2.5.2 учитывает общие причины, влияние которых частично перекрывается. Это слагаемое $3*q_2*q_2$ во втором уравнении и слагаемые $6*q_3*q_3$; $12*q_3*q_2$; $12*q_2*q_2*\frac{1}{T}*\int_0^T q(t)dt$ в третьем уравнении. Например, последнее слагаемое моделирует отказ трех элементов вследствие воздействия двух общих причин (q_2*q_2) и независимый отказ четвертого элемента (выражение под интегралом).

При моделировании элементов 2-го и 3-го классов, отказы которых обусловлены различными общими причинами, возникающими в

период их эксплуатации, определяются вероятностные характеристики этих причин и реакции на них резервируемых элементов. Если существует множество "К" общих причин $\{A_i\}$, воздействующих на группу из "n" резервируемых элементов, которому соответствует множество отказов этих элементов $\{S_j\}$, то вероятность отказа Q_n этой группы элементов по общей причине определяется по формуле:

$$Q_n = \sum_{i=1}^{k} \{ [\prod_{j=1}^{n} P(S_j / A_i)] * P(A_i) \} \qquad (2.5.3)$$

где $P(A_i)$ - вероятность события A_i.

Частным случаем уравнения 2.5.3 является параметрическая биномиальная модель, специфика применения которой для элементов 2-го и 3-го классов рассмотрена ниже.

Элементы второго класса подвержены отказам по общей причине из-за экстремальных внешних воздействий окружающей среды. Эти внешние воздействия делятся на два подкласса по характеру их проявления для рассматриваемых элементов: ударные воздействия, приводящие к идентификации неработоспособного состояния вскоре после своего возникновения (например, пожар), и воздействия, вызывающие скрытые отказы элементов (например, повышенная влажность, температура, вибрация).

Ударные воздействия вызывают явные (быстро выявляемые) отказы, которые не имеют скрытой фазы. Поэтому независимое совпадение моментов возникновения таких воздействий и исходных событий аварий крайне маловероятно. Интерес представляют экстремальные воздействия, которые могут быть следствием исходного события аварии:

-пожары вследствие коротких замыканий при заливе электрооборудования после возникновения исходного события аварии;

-затопления (запаривания) помещений при разрывах трубопроводов или срабатывании паросбросных устройств;

-образование летящих предметов или реактивных струй вследствие

разрушения оборудования.

Для моделирования таких ударных воздействий целесообразно использовать биномиальную модель:

$$q_i = \begin{cases} \nu * p^i * (1-p)^{n-i} & i=1,..,n-1 \\ \nu * (p^n + \omega) & i=n \end{cases} \qquad (2.5.4)$$

где n - число элементов, подверженных ударному воздействию;

ν - условная вероятность возникновения ударного воздействия после начала исходного события аварии;

p - условная вероятность отказа элемента при работе защитных средств (например, системы пожаротушения);

ω - вероятность отказа защитных средств.

Внешние воздействия, приводящие к множественным скрытым отказам оборудования, связаны с нарушением нормальных эксплуатационных условий расположенного в одном помещении резервируемого оборудования. Такое оборудование систем безопасности эксплуатируется в режиме ожидания с периодическими проверками работоспособности , поэтому эти отказы являются периодически контролируемыми. Ряд значительных нарушений нормальной эксплуатации приводит к полному отказу всех элементов (так называемые летальные воздействия), при возникновении остальных нарушений элементы отказывают независимо с условной вероятностью, отличной от единицы (нелетальные воздействия).

Биномиальная модель для таких воздействий имеет вид:

$$\lambda_i = \begin{cases} \nu' * p^i * (1-p)^{n-i} & i=1,...,n-1 \\ \nu' * p^n + \omega' & i=n \end{cases} \qquad (2.5.5)$$

где n - число резервируемых элементов, расположенных в помещении;

λ_i - интенсивность скрытого отказа по общей причине одно-

временно ровно i определенных элементов, I/ч;

ν' - частота нелетальных воздействий, I/ч;

ω' - частота летальных воздействий, I/ч;

p - условная вероятность отказа элемента при нелетальном воздействии.

В этом случае, средняя вероятность отказа Q_n системы из n элементов по любым причинам на интервале времени T (учитывая первый член разложения экспоненциального распределения, если $\lambda*t << 1$ и $\nu'*t*p^{n-i}*(1-p)^i << 1$) определяется по формуле:

$$Q_n = -\frac{1}{T}*\int_0^T [(\lambda*t)^n + (\nu'*p^n + \omega')*t + \sum_{i=1}^{n-1} C_n^i*(\lambda*t)^i*\nu'*t*p^{n-i}*(1-p)^i]dt \qquad (2.5.6)$$

где λ - интенсивность независимых скрытых отказов, I/ч;

C_n^i - число сочетаний из n по i.

Множественные отказы элементов 3-го класса связаны с повторяющимися ошибками эксплуатационного персонала при операциях технического обслуживания или проверок работоспособности резервируемого оборудования. Возможны два типа источников отказов по общей причине вследствие ошибок персонала:

-периодические обходы и/или техническое обслуживание резервируемых элементов, проводимое одной группой лиц в течение одной смены, при которых требуются или могут потребоваться активные действия персонала, влияющие на работоспособность оборудования, например, регулировка расхода, корректировка уровня;

-периодические проверки работоспособности или техническое обслуживание резервируемых элементов, проводимые одной группой лиц в течение одной смены, на период которых требуется отключение оборудования.

Отказы по общей причине обоих типов возникают в режиме ожидания оборудования и являются периодически контролируемыми. Их модели-

рование также проводится с помощью биномиальной модели:

$$\lambda_i = \begin{cases} \nu' * p^i * (1-p)^{n-i} & i=1,..,n-1 \\ \nu' * (p^n + \omega) & i=n \end{cases} \qquad (2.5.7)$$

где n - число обслуживаемых (испытываемых) резервируемых элементов;

λ_i - интенсивность отказа вследствие таких ошибок одновременно ровно i определенных элементов, I/ч;

ν' - частота осмотров (операций технического обслуживания) оборудования или испытаний с отключением оборудования, I/ч;

p - условная вероятность неправильного выполнения персоналом исполнительной части функции контроля;

ω - условная вероятность неправильного выполнения персоналом подфункции принятия решения функции контроля.

Средняя вероятность отказа на требование системы из n элементов определяется по формуле (2.5.6), где вместо ω' подставляется $\nu' * \omega$.

Приведенные параметрические модели позволяют оценивать интенсивности (вероятности) отказов по общей причине, что дает возможность их моделирования явным образом на дереве отказов или неявно путем расширения набора соответствующих минимальных сечений.

Остальные характеристики события отказа по общей причине (вид и периодичность контроля, время и возможность устранения) зависят от свойств конкретных отказавших элементов. Методика их определения ориентирована на использование расчетной программы в процессе генерации дополнительных минимальных сечений с отказами по общей причине.

При их определении необходимо учитывать следующие факторы:

а) возможность наличия различных типов контроля отказов элемен-

тов, входящих в рассматриваемое минимальное сечение;

б) возможность наличия различных моментов контроля периодически контролируемых элементов;

в) наличие регламентных ограничений;

г) возможность различных стратегий восстановления отказавших элементов;

д) неполноту данных по интенсивностям (вероятностям) возникновения события.

Последний фактор связан с тем, что параметрические модели, используемые для определения этой характеристики, основываются на статистическом материале. Так как отказы по общей причине большой кратности (размерности) являются крайне редким событием, то, как правило, приходится ограничиваться заданием вероятностей двойных, тройных отказов и отказов всех элементов группы общих причин.Соответственно, и при моделировании рассматриваются только такие кратности отказов.

Определение вида контроля события отказа по общей причине проводится по специальной процедуре. Она заключается в анализе числа непрерывно контролируемых (n_k),периодически контролируемых (n_p) и неконтролируемых (n_n) элементов, отказавших в рассматриваемом событии и в соотнесении указанных чисел с упомянутым ранее уровнем детализации моделирования отказов по общей причине.

Возможны два типа событий. В первом случае событие отказа по общей причине удовлетворяет условию:

$$n_k + n_p + n_n <= LEV + 1 \qquad (2.5.8)$$

где LEV - уровень детализации, т.е. максимальная кратность рассматриваемых отдельно отказов, выше которой возможен только один отказ всей группы элементов. Обнаружение отказа хотя бы одного элемента при таком событии приводит к реализации уже другого отдельно учитываемого в модели (т.е. в других сечениях) события. В этом слу-

чае для определения вида контроля события отказа по общей причине используются следующие правила:

-событие имеет непрерывный контроль, если среди отказавших элементов имеется хотя бы один с непрерывным видом контроля отказов (n_k>=1);

-событие имеет периодический тип контроля, если среди отказавших элементов, отказы которых образуют рассматриваемое событие, нет элемента с непрерывным типом контроля отказов (n_k=0), но имеется хотя бы один элемент с периодическим типом контроля отказов (n_p>=1);

-событие является неконтролируемым в остальных случаях, т.е. когда все отказавшие элементы имеют неконтролируемый тип отказов (n_k=0,n_p=0).

Для событий с большим числом элементов ($n_k + n_p + n_n$> LEV+1), отказавших вследствие воздействия общей причины, указанное правило может быть изменено следующим образом:

-событие имеет непрерывный тип контроля, если $n_p + n_n$ <= LEV;

-событие имеет периодический тип контроля, если n_n < =LEV, а $n_p + n_n$ > LEV;

-событие является неконтролируемым, если n_n > LEV.

Далее, если отказ по общей причине имеет периодический тип контроля, то необходимо определить его периодичность. Рассмотрим случай отказа по общей причине m периодически контролируемых элементов (n_p=m) из группы n элементов, подверженной воздействию общей причины и входящей в N каналов системы безопасности (n>=N). Периодичность контроля события зависит от стратегии проверки каналов.

I стратегия - все каналы проверяются одновременно с одинаковой периодичностью.

При этой стратегии периодичность контроля отказа по общей при-