МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ТУЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт *прикладной математики и компьютерных наук*

Кафедра «*Информационная безопасность»*

КОНСПЕКТ ЛЕКЦИЙ

по дисциплине

«ДИАГНОСТИКА И НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Уровень профессионального образования: *высшее образование – бакалавриат*

Направление: *09.03.03 Прикладная информатика*

Профиль: *Прикладная информатика в промышленности*

Квалификация выпускника: *бакалавр*

Форма обучения: *заочная (дистанционная)*

Тула, 2020

СОДЕРЖАНИЕ

ТЕМА 1. Основные понятия и определения теории надежности. Показатели надежности невосстанавливаемого объекта

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ТЕОРИИ НАДЕЖНОСТИ

Предмет, подлежащий изучению, называется **объектом**. Каждый объект предназначен для выполнения определенных функций. Способность объекта выполнять требуемые функции характеризуется набором параметров. Для каждого параметра в нормативно-технической документации установлены допустимые предельные значения.

Надежность - свойство объекта сохранять во времени значения всех параметров в допустимых диапазонах. ГОСТ дает следующие определение термина **надежность**:

" *Свойство объекта выполнять заданные функции, сохраняя во времени значения установленных эксплуатационных показателей в заданных пределах, соответствующих заданным режимам и условиям использования, технического обслуживания, ремонта, хранения и транспортирования* ".

Работоспособным называется такое состояние объекта, при котором значения всех параметров находятся в заданных пределах.

Неработоспособным называется состояние объекта, при котором значение хотя бы одного параметра выходит за установленные пределы.

Событие, заключающееся в переходе объекта из работоспособного состояния в неработоспособное, называется **отказом**. Обратное событие - переход из неработоспособного состояния в работоспособное, называется **восстановлением**.

Понятие "восстановление" следует понимать не только как ремонтные операции, но и как замену отказавшего объекта.

В теории надежности принято различать два типа отказов: **внезапные** и **постепенные**.

Под внезапным отказом объекта подразумевается мгновенный выход из строя, означающий невозможность его применения. Внезапный отказ возникает в какой-то случайный момент времени. Примеры: перегорание электрической лампочки, обрыв проводника и т.п.

Под постепенным подразумевается отказ объекта, связанный с постепенным ухудшением его характеристик. Для устранения таких отказов требуется регулировка.

Постепенные отказы можно условно рассматривать как внезапные: как только значение хотя бы одного из параметров выходит за заданные пределы, объект считается отказавшим. В нашем курсе будем рассматривать только внезапные отказы.

Объект относится к **невосстанавливаемым**, если его восстановление после отказа нецелесообразно или невозможно.

Если после отказа проводится восстановление, то объект относится к **восстанавливаемым**.

Один и тот же объект в различных условиях применения может быть отнесен к невосстанавливаемым (например, если он расположен в помещении, куда невозможен доступ) и к восстанавливаемым.

В теории надежности вводятся понятия элемента и системы.

Системой называется совокупность **элементов**, взаимодействующих между собой в процессе выполнения заданных функций.

Элементом называют составную часть **системы**, которая рассматривается без дальнейшего разделения как единое целое.

Различие между элементом и системой чисто условное и состоит в том, что при определении надежности системы элемент считают неделимым, его надежность считается заданной или определяется экспериментально. Систему же представляют в виде совокупности отдельных элементов, надежность каждого из которых определяют отдельно. Надежность системы будет зависеть от количества образующих систему элементов, от способа их объединения в систему и от характеристик надежности каждого отдельного элемента.

Система может представлять собой не только совокупность технических устройств, но и включать в себя в качестве элементов и нетехнические средства, например, программные обеспечение, обслуживающий персонал и т.п.

Деление объектов на "системы" и образующие их "элементы" носит условный характер и зависит от постановки задачи и цели исследования. Один и тот же объект может рассматривать и как система, состоящая из элементов, и как элемент более сложной системы.

ТЕМА 2. Показатели надежности невосстанавливаемого объекта

НАРАБОТКА ДО ОТКАЗА

Промежуток времени от начала функционирования объекта до момента его отказа называется **временем безотказной работы.**

Время безотказной работы не является объективным показателем надежности, так как объект не постоянно занят работой. Суммарное время работы между моментом начала работы объекта и моментом отказа объекта называется **наработкой до отказа**. Если объект работает без перерывов, наработка до отказа совпадает с временем безотказной работы.

Заранее указать наработку до отказа невозможно, будем рассматривать ее как непрерывную случайную величину T, имеющую функцию распределения $F(t)=P\{T<t\}$ и плотность f(t), которую в теории надежности называют **частотой отказов**. Так как наработка до отказа T - положительная величина, то $F(t)=f(t)=0$ при $t \le 0$.

3. ФУНКЦИЯ НАДЕЖНОСТИ И ФУНКЦИЯ ОТКАЗА

Функция надежности или **вероятность безотказной работы** объекта p(t) определяется как $p(t) = P\{T \ge t\} = 1 - F(t) = \int_t^{\infty} f(x)dx$ - вероятность того, что объект будет работать безотказно в течение времени t. Функция надежности определена при $t \ge 0$.

Чтобы отличать функцию надежности от вероятности договоримся, что запись p(...) будет обозначать функцию надежности, а запись P{...} - вероятность.

Свойства функции надежности:

1. p(t) - убывающая функция.
2. $p(0)=1, \quad \lim_{t \to \infty} p(t) = 0.$
3. $\frac{d}{dt}(p(t)) = -f(t).$

Функция отказа объекта q(t) в теории надежности определяется как $q(t) = P\{T < t\} = F(t) = \int_0^t f(x)dx$ - вероятность того, что за время t произойдет отказ объекта.

Функцию отказа легко выразить через функцию надежности g(t)=1-p(t).

Свойства функции отказа:

1. q(t) - возрастающая функция.
2. $q(0)=1, \quad \lim_{t \to \infty} q(t) = 1.$

3. $\frac{d}{dt}(q(t)) = f(t)$.

Типичный график функции надежности изображен на рисунке 2.1. Типичный график функции отказа - на рисунке 2.2.

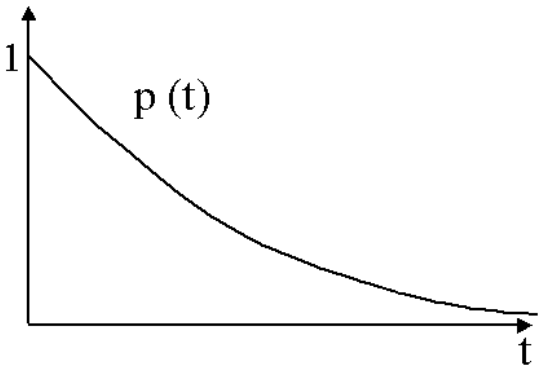

Рис. 2.1. Функция надежности.

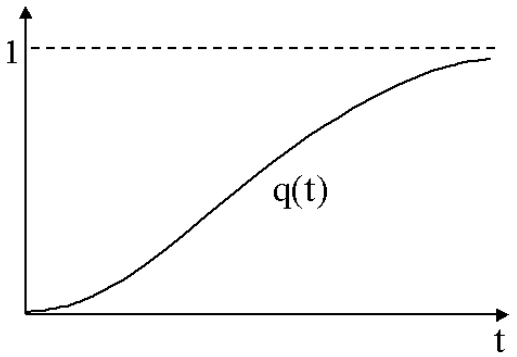

Рис. 2.2. Функция отказа.

Функция надежности p(t) как количественная характеристика надежности обладает следующими достоинствами:

1) характеризует изменение надежности во времени;

2) дает возможность достаточно наглядно судить о надежности;

3) может быть использование для расчета надежности систем при их проектировании.

Но функция надежности имеет также и существенные недостатки:

1) характеризует надежность только до первого отказа;

2) не всегда удобна для оценки надежности простых объектов;

3) по известной функции надежности довольно трудно вычислить другие количественные характеристики надежности.

Из-за этих недостатков для полной характеристики надежности нужны и другие количественные характеристики.

4. СРЕДНЯЯ НАРАБОТКА ДО ОТКАЗА

Средней наработкой до отказа называется математическое ожидание наработки до отказа:

$$\tau = M(T) = \int_0^\infty t \cdot f(t)dt .$$

Проведем интегрирование по частям, используя соотношение $\int udv = uv - \int vdu$.

Если $u = p(t), v = t, mo\ du = p'(t)dt = -f(t)dt$.

Тогда $\int_0^\infty p(t)dt = t \cdot p(t)\Big|_0^\infty + \int_0^\infty t \cdot f(t)dt$.

Можно доказать, что $\lim_{t\to\infty} t \cdot p(t) = 0$, тогда $\int_0^\infty p(t)dt = \int_0^\infty t \cdot f(t)dt$.

Следовательно, можно записать другое выражение для средней наработки:

$$\tau = \int_0^\infty p(t)dt \quad . \qquad (1)$$

Формула (1) связывает среднюю наработку до отказа и функцию надежности: средняя наработка до отказа равна площади под кривой функции надежности.

Средняя наработка до отказа является одной из наиболее наглядных количественных характеристик надежности. Однако эта характеристика имеет и существенные недостатки. Она не может полностью характеризовать время работы объекта. Кроме того, величина τ характеризует надежность объекта до первого отказа, т.е. характеризует надежность объектов разового использования.

5. ИНТЕНСИВНОСТЬ ОТКАЗОВ

Интенсивностью отказов называется величина

$$\lambda(t) = \frac{f(t)}{p(t)} \quad .$$

Так как $f(t) = -p'(t)$, то $\lambda(t) = -\frac{p'(t)}{p(t)} = -\frac{d}{dt}(\ln p(t))$.

Выясним смысл интенсивности отказов.

Пусть объект проработал время t. Найдем условную вероятность того, что отказ произойдет до момента $t+\Delta t$ при условии, что до момента t отказа не было.

Введем события:

$A=\{T \geq t\}$ - до момента t объект оставался работоспособным,

$B=\{T \leq t+\Delta t\}$ - отказ произошел до момента $t+\Delta t$.

Тогда $P\{B|A\} = P\{AB\}/P\{A\}$.

Но $P\{A\}=P\{T \geq t\}=p(t)$;

$P\{AB\}=P\{t \leq T \leq t+\Delta t\}= \int_t^{t+\Delta t} f(x)dx$.

Тогда

$$\lim_{\Delta t\to 0}\frac{1}{\Delta t}P\{T\le t+\Delta t\}|T\ge t\}=\lim_{\Delta t\to 0}\frac{\int_{t}^{t+\Delta t}f(x)dx}{\Delta t}\cdot\frac{1}{p(t)}=\frac{f(t)}{p(t)}=\lambda(t).$$

Итак, смысл интенсивности отказов: при малых Δt $P\{T\le t+\Delta t|T\ge t\}\approx\lambda(t)\Delta t$.

Зная интенсивность отказов, можно определить функцию надежности. Для этого возьмем первообразные от обеих частей равенства

$$\lambda(t)=-\frac{d}{dt}(\ln p(t)).$$

Получаем $\int_{o}^{t}\lambda(x)dx=-\ln p(t)+C,$ где C - некоторая константа.

Так как при t=0 $\int_{0}^{0}\lambda(x)dx=0$ и ln (p(0)) = ln 1=0, то и C=0.

Итак, $\ln p(t)=-\int_{0}^{t}\lambda(x)dx$.

Отсюда $p(t)=exp(-\int_{0}^{t}\lambda(x)dx)$.

Теперь несложно выразить через интенсивность и среднюю наработку

$$\tau=\int_{0}^{\infty}\exp(-\int_{0}^{t}\lambda(x)dx)dt.$$

Частота отказов и интенсивность отказов связаны между собой зависимостью

$$f(t)=\lambda(t)p(t)=\lambda(t)\exp(-\int_{0}^{t}\lambda(x)dx).$$

Определим размерность λ(t):

p(t)=P{T≥t} - как вероятность, является безразмерной величиной;

$$f(t)=-p'(t)=-\lim_{\Delta t\to 0}\frac{p(t+\Delta t)-p(t)}{\Delta t}$$

имеет размерность, обратную размерности Δt.

Такую же размерность, обратную единицам времени, имеет и интенсивность отказов λ(t). Обычная единица измерения интенсивности отказов - (час$^{-1}$).

Типичная зависимость интенсивности от времени показано на рисунке 2.3.

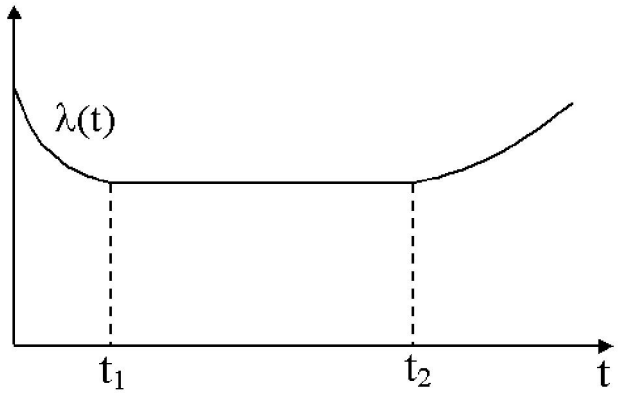

Рис. 2.3. Интенсивность отказов.

На графике можно выделить три характерных участка.

На первом участке от 0 до t_1 интенсивность отказов падает. Это так называемый **период приработки**. При статистических испытаниях в этом периоде характерны ранние отказы вследствие дефектов материала или производственных дефектов. В демографии этот отрезок кривой называется периодом "детской смертности".

На втором участке от t_1 до t_2 интенсивность отказов примерно постоянна. Этот участок называется **периодом нормальной эксплуатации**. Отказы, появляющиеся в этом периоде называются **внезапными**. Они вызываются тяжелыми условиями работы, неожиданным изменениям условий эксплуатации и т.п. Можно провести аналогию между отказами этого периода и несчастными случаями, происходящими с людьми ежедневно.

На третьем участке после момента t_2 интенсивность начинает возрастать. Этот участок называется **периодом старения**. Отказы этого периода называются **износовыми**.

Интенсивность отказов как количественная характеристика надежности имеет ряд достоинств. Она является функцией времени и позволяет установить характерные участки работы объекта. Если известны моменты t_1 и t_2 , то можно разумно установить период опытной эксплуатации объекта до момента t_1 и окончание эксплуатации к моменту t_2. Недостаток тот же, что и у остальных показателей: интенсивность характеризует надежность объектов лишь до первого отказа.

Однако в силу своих положительных свойств интенсивность является наиболее удобной характеристикой надежности.

6. МОДЕЛИ НАДЕЖНОСТИ

1. Модель с показательным распределением.

Наработка до отказа имеет показательное распределение с плотностью

$$f(t)=\begin{cases}0, & t<0,\\ \lambda\, e^{-\lambda t}, & t\geq 0\end{cases}$$

и функцией распределения

$$F(t)=\begin{cases}0, & t\leq 0\\ 1-e^{-\lambda t}, & t>0,\end{cases}$$

где λ>0 - параметр распределения.

Для такого распределения функция надежности $p(t)=1-F(t)=e^{-\lambda t}$.

функция отказа равна $q(t)=1-e^{-\lambda t}$.

При малых значениях t часто пользуются приближенными соотношениями $q(t)\approx\lambda t,\quad p(t)\approx 1-\lambda t$.

Средняя наработка равна

$$\tau=\int_0^\infty p(t)dt=\int_0^\infty e^{-\lambda t}dt==\frac{1}{\lambda}.$$

Интенсивность равна $\lambda(t)=\dfrac{f(t)}{p(t)}=\dfrac{\lambda e^{-\lambda t}}{e^{-\lambda t}}=\lambda=const$.

Таким образом, модель показательного распределения хорошо описывает период нормальной эксплуатации. В силу этого показательное распределение наиболее часто используется в теории надежности.

Данная модель обладает свойством, которое назовем **замечательным свойством модели показательного распределения.**

Пусть объект проработал без отказа время t_1. Определим условную вероятность того, что он проработает без отказа еще время t_2, т.е. до момента t_1+t_2:

$$P\{T\geq t_1+t_2\,|\,T\geq t_1\}=\frac{P\{T\geq t_1, T\geq t_1+t_2\}}{P\{T\geq t_1\}}=\frac{P\{T\geq t_1+t_2\}}{P\{T\geq t_1\}}=\frac{p(t_1+t_2)}{p(t_1)}=$$

$$=\frac{e^{-\lambda(t_1+t_2)}}{e^{-\lambda t_1}}=e^{-\lambda t_2}=p(t_2).$$

Получаем, что распределение оставшегося времени наработки не зависит от того, сколько времени объект проработал до этого.

2. Модель с распределением Вейбулла.

Наработка до отказа имеет распределение Вейбулла:

$$f(t)=\begin{cases}0, & t\le 0,\\ \lambda\alpha\, t^{\alpha-1}e^{-\lambda\, t^{\alpha}}, & t>0,\end{cases}$$

$$F(t)=\begin{cases}0, & t\le 0,\\ 1-e^{-\lambda\, t^{\alpha}}, & t>0,\end{cases}$$

где $\lambda>0, \alpha>0$ - параметры распределения.

При $\alpha=1$ распределение Вейбулла совпадает с показательным распределением.

Для этой модели $p(t)=1-F(t)=e^{-\lambda\, t^{\alpha}}$,

$\tau=\dfrac{\Gamma(1+1/\alpha)}{\lambda^{1/\alpha}}$, где $\Gamma(x)=\int_0^{\infty} t^{x-1}e^{-t}dt$ (гамма-функция),

$\lambda(t)=\dfrac{f(t)}{p(t)}=\lambda\,\alpha\, t^{\alpha-1}$.

График интенсивности отказов при распределении Вейбулла изображен на рисунке 2.4.

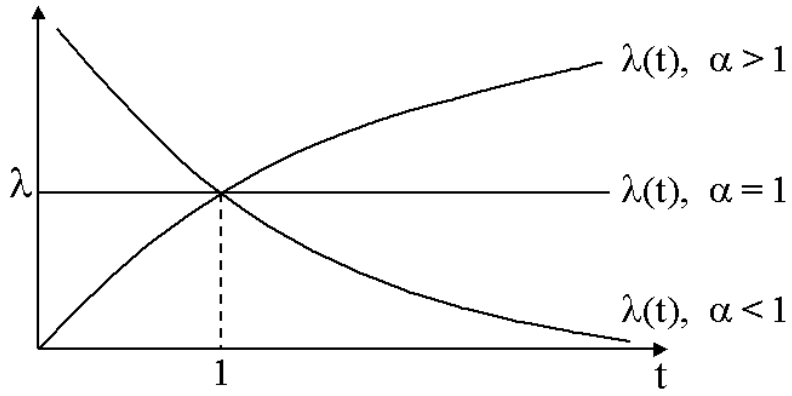

Рис. 2.4. Интенсивность отказов при распределении Вейбулла.

При $\alpha>1$ интенсивность отказов монотонно возрастает, при $\alpha<1$ - монотонно убывает.

После показательного распределения наиболее часто в теории надежности используются распределения Вейбулла.

3. Модель с нормальным распределением.

Наработка до отказа имеет нормальное распределение с плотностью

$$f(t) = \frac{1}{\sqrt{2\pi}\sigma} \cdot e^{-\frac{(t-m)^2}{2\sigma^2}}, \quad -\infty < t < \infty,$$

где m и σ>0 - параметры распределения.

Нормальное распределение не совсем подходит для задач теории надежности, так как случайная величина с нормальным распределением может принимать любые значения от $-\infty$ до ∞, а наработка до отказа - положительная величина.

Поэтому вместо нормального в теории надежности часто используют **усеченное нормальное распределение**, имеющее плотность

$$\tilde{f}(t) = \begin{cases} \frac{c}{\sqrt{2\pi}\sigma} \cdot e^{-\frac{(t-m)^2}{2\sigma^2}}, & t \geq 0, \\ 0, & t < 0, \end{cases}$$

где m>0, а c>1 - нормирующий множитель, выбираемый из условия $\int_0^\infty \tilde{f}(t)dt = 1$.

Усеченное нормальное распределение обычно применяют, если m<3σ. В противном случае $c \leq 1{,}0015$ и использование неусеченного нормального распределения дает достаточную точность.

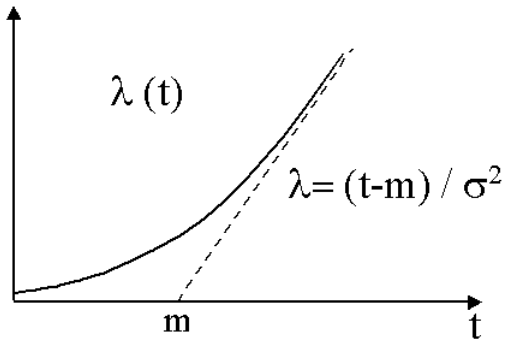

Рис. 2.5. Интенсивность отказов при усеченном нормальном распределении.

Можно доказать, что в данной модели интенсивность монотонно возрастает и при больших t начинает приближаться к асимптоте $\lambda = \frac{t-m}{\sigma^2}$ (см. рис. 2.5.).

7. СТАТИСТИЧЕСКОЕ ОЦЕНИВАНИЕ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ.

Показатели надежности оцениваются по результатам испытаний совокупности объектов.

Планом испытаний называют правила, устанавливающие количество исследуемых объектов, порядок проведения испытаний и критерии их прекращения.

Наименование плана принято обозначать тремя параметрами. Первый параметр указывает число испытываемых объектов (N), второй - наличие (В) или отсутствие (Б) восстановлений на время испытаний в случае отказа объекта, третий - условия прекращения испытаний.

Чаще всего применяются следующие планы испытаний:

[N,Б,T] - в течении времени T без восстановления испытываются N объектов;

[N,Б,r] - испытания N объектов проводятся без восстановления до того момента, пока не случится r отказов. При r=N получаем план [N,Б,N] - испытания проводятся, пока не откажут все объекты;

[N,Б,(r,T)] - испытания прекращаются либо после r отказов, либо после времени T (в зависимости от того, что наступит раньше);

[N,B,T], [N,B,r], [N,B,(r,T)] - планы испытаний, в которых производится восстановление отказавших объектов.

Рассмотрим наиболее распространенный план испытаний [N,Б,N]. Введем функцию n(t) - число объектов, отказавших за время t. Тогда оценка функции отказа

$$\hat{q}(t) = \frac{n(t)}{N}.$$

Оценка функции надежности

$$\hat{p}(t) = \frac{N - n(t)}{N}.$$

Для оценки интенсивности введем малое значение Δt. Тогда оценка частоты отказов

$$\hat{f}(t) = \frac{n(t + \frac{\Delta t}{2}) - n(t - \frac{\Delta t}{2})}{N\,\Delta t}.$$

Оценка интенсивности отказов

$$\hat{\lambda}(t) = \frac{\hat{f}(t)}{\hat{p}(t)} = \frac{n(t + \frac{\Delta t}{2}) - n(t - \frac{\Delta t}{2})}{(N - n(t))\Delta t}.$$

Рассмотрим моменты t_i, i=1,2,...,N отказов каждого объекта. Тогда оценка средней наработки

$$\hat{\tau} = \frac{1}{N}\sum_{i=1}^{N} t_i .$$

Пусть известно, что наработка до отказа имеет показательное распределение. Тогда постоянную интенсивность λ оцениваем по формуле

$$\hat{\lambda} = \frac{1}{\hat{\tau}} = \frac{N}{\sum_{i=1}^{N} t_i}.$$

ТЕМА 3. Надежность невосстанавливаемых систем

1. НАДЕЖНОСТЬ НЕВОССТАНАВЛИВАЕМЫХ СИСТЕМ. СТРУКТУРНАЯ СХЕМА

Пусть изучаемая система состоит из n элементов. Предположим, нам известны показатели надежности каждого из элементов. Пусть элемент с номером i имеет функцию надежности $p_i(t)$, функцию отказа $q_i(t)$, интенсивность отказов $\lambda_i(t)$. Нам неизвестны показатели надежности всей системы, которые обозначим $p_s(t)$, $q_s(t)$, $\lambda_s(t)$.

Сделаем следующие предположения:

1. Каждый элемент может находиться в одном из двух состояний: работоспособное состояние или отказ.

2. Элементы выходят из строя независимо друг от друга. Отказ элемента не влияет на надежность остальных элементов системы.

3. Известна структура системы, которая позволяет определить влияние отказа на рабочие характеристики системы.

Структура системы обычно изображается в виде графа, ребрами которые являются элементы системы. В графе есть две специальные вершины, обозначаемые обычно A и B. Вершина A называется входом, вершина B - выходом. На графе должен быть путь от A к B.

При отказе какого-либо множества элементов системы $\{i_1,\ldots,i_k\}$ из графа удаляются все ребра, соответствующие отказавшим элементам. Если при отказе элементов $\{i_1,\ldots,i_k\}$ система остается работоспособной, то в полученном подграфе вершины A и B должны оставаться связными. Если система выходит из строя, то в полученном подграфе вершины A и B становятся несвязными, т.е. пути , соединяющего A и B, больше нет.

Такой граф называется **структурной схемой** системы.

2. СИСТЕМА С ПОСЛЕДОВАТЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Соединение элементов называется **последовательным** (в смысле надежности), если отказ любого элемента вызывает отказ системы.

Структурная схема системы с последовательным соединением элементов изображена на рисунке 3.1.

Таким образом, при последовательном соединении система работоспособна тогда и только тогда, когда работоспособен каждый ее элемент. Если $T_1,\ldots,T_n$ - наработки до отказа каждого из элементов, то наработка до отказа всей системы $T_s = \min(T_1,\ldots,T_n)$.

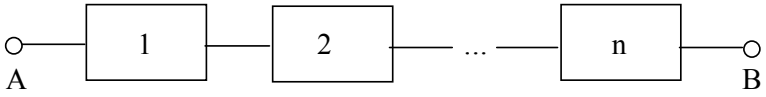

Рис. 3.1. Структурная схема системы с последовательным соединением элементов.

Найдем характеристики надежности системы

$p_s(t) = P\{T_s \geq t\} = P\{T_1 \geq t, T_2 \geq t, \ldots, T_n \geq t\} = P\{T_1 \geq t\} \cdot P\{T_2 \geq t\} \ldots \cdot P\{T_n \geq t\} =$

$= p_1(t) \cdot p_2(t) \cdot \ldots p_n(t)$

Итак, для системы с последовательным соединением элементов

$$p_s(t) = \prod_{i=1}^{n} p_i(t).$$

Для функции отказа системы получаем

$$q_s(t) = 1 - p_s(t) = 1 - \prod_{i=1}^{n} (1 - q_i(t)).$$

Если все элементы системы обладают высокой надежностью, т.е. все $q_i(t) << 1$, то $\prod_{i=1}^{n} (1 - q_i(t)) \approx 1 - q_1(t) - q_2(t) - \ldots - q_n(t)$.

Поэтому при последовательном соединении высоконадежных элементов

$$q_s(t) \approx \sum_{i=1}^{n} q_i(t), \quad p_s(t) \approx 1 - \sum_{i=1}^{n} q_i(t).$$

Определим интенсивность отказов системы

$$\lambda_s(t) = -\frac{d}{dt}(\ln p_s(t)) = -\frac{d}{dt}(\ln \prod_{i=1}^{n} p_i(t)) = -\frac{d}{dt}(\ln p_1(t)) - \ldots - \frac{d}{dt}(\ln p_n(t)) =$$

$$= \lambda_1(t) + \ldots + \lambda_n(t).$$

Итак,

$$\lambda_s(t) = \sum_{i=1}^{n} \lambda_i(t),$$

т.е. интенсивность отказов системы с последовательным соединением элементов равна сумме интенсивностей отказов каждого элемента.

3. ПОСЛЕДОВАТЕЛЬНОЕ СОЕДИНЕНИЕ ЭЛЕМЕНТОВ С ПОСТОЯННОЙ ИНТЕНСИВНОСТЬЮ ОТКАЗОВ

Если наработка до отказа каждого элемента имеет показательное распределение, то интенсивности отказов - константы: $\lambda_s(t) = \lambda_i = const$.

Следовательно, $\lambda_s(t) = \sum_{i=1}^{n} \lambda_i = const$.

Вывод: при последовательном соединении элементов с постоянной интенсивностью отказов интенсивность отказов всей системы также будет постоянной.

Следовательно, распределение наработки до отказа всей системы имеет показательное распределение и функция надежности равна

$$p_s(t) = \exp(-\sum_{i=1}^{n} \lambda_i t).$$

Среднюю наработку вычислим по формуле

$$\tau_s = \int_0^{\infty} \exp(-\sum_{i=1}^{n} \lambda_i t) dt = \frac{1}{\lambda_1 + \lambda_2 + ... + \lambda_n}.$$

Если все элементы системы имеют одинаковую интенсивность $\lambda_1 = \lambda_2 = ... = \lambda_n = \lambda$, то $\tau_s = \frac{1}{n\lambda} = \frac{\tau}{n}$, где $\tau = \frac{1}{\lambda}$ - средняя наработка каждого элемента.

Итак, при последовательном соединении n элементов с одинаковой постоянной интенсивностью отказов средняя наработка системы в n раз меньше средней наработки каждого элемента.

4. СИСТЕМА С ПАРАЛЛЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Соединение элементов называется **параллельным** (в смысле надежности), если система работоспособна до тех пор, пока работает хотя бы один из ее элементов.

Структурная схема системы с параллельным соединением элементов изображена на рисунке 3.2.

Таким образом, при параллельном соединении система отказывает тогда и только тогда, когда отказали все ее элементы. Если $T_1, \ldots, T_n$ - наработки до отказа каждого из элементов, то наработка до отказа всей системы $T_s = \max(T_1, ..., T_n)$.

Найдем функцию отказов системы

$$q_s(t) = P\{T_s < t\} = P\{T_1 < t, T_2 < t, ..., T_n < t\} = P\{T_1 < t\} \cdot P\{T_2 < t\} ... \cdot P\{T_n < t\} =$$
$$= q_1(t) \cdot q_2(t) \cdot ... q_n(t).$$

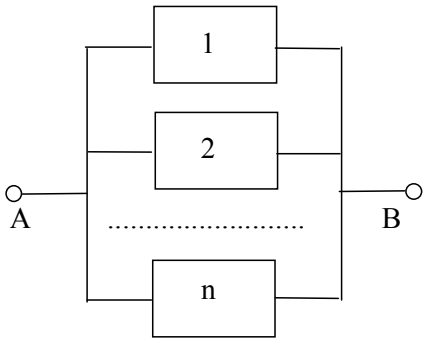

Рис. 3.2. Структурная схема системы с параллельным соединением элементов.

Итак, для системы с параллельным соединением элементов

$$q_S(t) = \prod_{i=1}^{n} q_i(t).$$

Для функции надежности системы получаем

$$p_S(t) = 1 - q_S(t) = 1 - \prod_{i=1}^{n} (1 - p_i(t)).$$

5. ПАРАЛЛЕЛЬНОЕ СОЕДИНЕНИЕ ЭЛЕМЕНТОВ С ПОСТОЯННОЙ ИНТЕНСИВНОСТЬЮ ОТКАЗОВ

Пусть все элементы системы с параллельным соединением имеют одинаковую показательную надежность $p_i(t) = e^{-\lambda t}$. Тогда

$q_s(t) = (1 - e^{-\lambda t})^n$, $p_s(t) = 1 - (1 - e^{-\lambda t})^n$.

Частота и интенсивность отказов системы будут равны

$$f_S(t) = q_S{}'(t) = n\lambda e^{-\lambda t}(1 - e^{-\lambda t})^{n-1};$$

$$\lambda_S(t) = \frac{f_S(t)}{p_S(t)} = \frac{n\lambda e^{-\lambda t}(1 - e^{-\lambda t})^{n-1}}{1 - (1 - e^{-\lambda t})^n} \neq const.$$

Таким образом, при параллельном соединении элементов с постоянной интенсивностью отказов интенсивность отказа системы уже не будет постоянной, т.е. распределение наработки до отказа системы не будет показательным.

Запишем интенсивность отказов системы в следующем виде

$$\lambda_s(t) = \lambda \cdot \frac{n(1-q(t)) \cdot q^{n-1}(t)}{1-q^n(t)} = \lambda \cdot \frac{n \cdot q^{n-1}(t)}{1+q(t)+q^2(t)+q^{n-1}(t)} =$$

$$= \lambda \cdot \frac{n}{(\frac{1}{q(t)})^{n-1} + (\frac{1}{q(t)})^{n-2} + \ldots + 1}.$$

Так как q(t) - возрастающая функция, q(0)=0, $q(\infty) = 1$, то:

а) $\lambda_s(t)$ - возрастающая функция;

б) $\lambda_s(0) = 0,\ \lambda_s(\infty) = \lambda$.

График интенсивности отказов $\lambda_s(t)$ показан на рисунке 3.3.

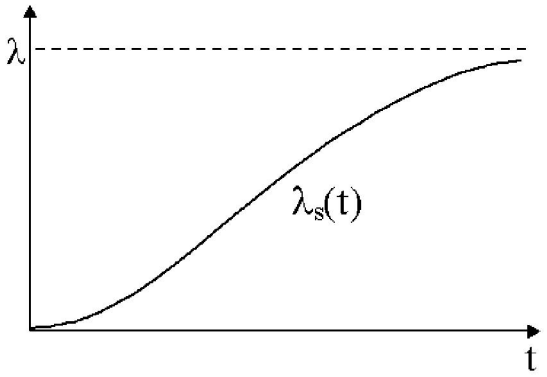

Рис 3.3. Интенсивность отказов системы с параллельным соединением.

Найдем среднюю наработку до отказа системы с параллельным соединением.

$$\tau_s = \int_0^\infty p_s(t)dt = \int_0^\infty (1-(1-e^{-\lambda t})^n)dt.$$

Не будем считать интеграл, а для определения средней наработки используем другой метод - **метод графа состояний системы.**

Процесс функционирования системы представим в виде графа на рисунке 3.4.

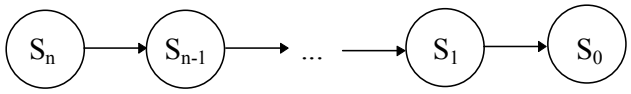

Рис. 3.4. Граф состояний системы с параллельным соединением.

Когда работают все элементы, система находится в состоянии S_n. В этом состоянии она будет находится от момента начала работы некоторое случайное время V_n. После отказа одного из элементов система переходит в состояние S_{n-1} (

работает n-1 элемент). В состоянии S_{n-1} система находит случайное время V_{n-1}, а потом переходит в состояние S_{n-2} (работают n-2 элемента) и т.д.

Наконец, попав в состояние S_1 (работает только один элемент), система через случайное время V_1 переходит в состояние S_0 - состояние отказа системы.

Наработка до отказа системы $T_s = V_n + V_{n-1} + \ldots + V_1$.

Следовательно, $\tau_s = M(T_s) = M(V_n) + M(V_{n-1}) + \ldots + M(V_1)$.

Найдем распределение случайной величины V_n .

$P\{V_n > t\} = P\{T_1 > t, T_2 > t, \ldots, T_n > t\}$ - вероятность того, что ни один из элементов не откажет за время t.

Следовательно, $P\{V_n > t\} = \prod_{i=1}^{n} P\{T_i > t\} = e^{-n\lambda t}$.

Получаем, что V_n имеет такое же распределение, как и наработка до отказа системы с последовательным соединением n элементов.

Следовательно, $M(V_n) = \frac{1}{n\lambda}$.

Рассмотрим состояние S_{n-1}, в котором работает n-1 элемент. Каждый из этих элементов к моменту перехода системы в состояние S_{n-1} уже проработал время V_n. Однако в силу замечательного свойства объектов с показательным распределением наработки распределение оставшегося времени наработки каждого элемента не зависит от величины V_n. Можно считать, что каждый из этих n-1 элементов только что включился в работу.

Поэтому случайная величина V_{n-1} имеет такое же распределение, как и наработка до отказа системы с последовательным соединением (n-1) элементов.

Следовательно, $M(V_{n-1}) = \frac{1}{(n-1)\lambda}$.

Аналогично, $M(V_{n-2}) = \frac{1}{(n-2)\lambda}$, ... , $M(V) = \frac{1}{\lambda}$.

Средняя наработка системы с параллельным соединением элементов

$$\tau_s = \frac{1}{\lambda}\sum_{i=1}^{n}\frac{1}{i} = \tau\sum_{i=1}^{n}\frac{1}{i},$$

где $\tau = \frac{1}{\lambda}$ - средняя наработка каждого элемента.

Итак, при параллельном соединении n элементов с одинаковой постоянной интенсивностью отказов средняя наработка системы в $\sum_{i=1}^{n}\frac{1}{i}$ раз больше средней наработки каждого элемента.

Если n велико, $\sum_{i=1}^{n}\frac{1}{i} \approx \ln n$, т.е. $\tau_s \approx \tau \ln n$.

Пусть теперь все элементы системы имеют различные значения интенсивности $\lambda_1, \lambda_2, \ldots, \lambda_n$.

Тогда $p_s(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t})$,

и для средней наработки можно получить следующее выражение

$$\tau_s = \left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \ldots + \frac{1}{\lambda_n} \right) - \left(\frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \ldots + \frac{1}{\lambda_{n-1} + \lambda_n} \right) +$$

$$+ \left(\frac{1}{\lambda_1 + \lambda_2 + \lambda_3} + \ldots \right) - \ldots + (-1)^{n+1} \frac{1}{\lambda_1 + \lambda_2 + \ldots + \lambda_n}.$$

6. ПОСЛЕДОВАТЕЛЬНО - ПАРАЛЛЕЛЬНОЕ СОЕДИНЕНИЕ

Во многих системах применяются как последовательные, так и параллельные соединения элементов. При оценке характеристик надежности такой системы нужно расчленить ее на ряд подсистем , не имеющих общих элементов. Элементы в каждой подсистеме должны быть соединены либо последовательно, либо параллельно. Находятся характеристики надежности каждой подсистемы. После этого рассматривая подсистемы как условные элементы, находим характеристику надежности всей системы.

Пример 1. Рассмотрим систему со структурной схемой, изображенной на рисунке 3.5. Функции надежности элементов обозначим соответственно $p_1(t), \ldots, p_7(t)$.

Выделим подсистемы S_1, S_2, S_3, имеющие функции надежности

$p_{s_1}(t) = p_1(t) \cdot p_2(t)$;

$p_{s_2}(t) = 1 - (1 - p_3(t)) \cdot (1 - p_4(t))$;

$p_{s_3}(t) = 1 - (1 - p_6(t)) \cdot (1 - p_7(t))$.

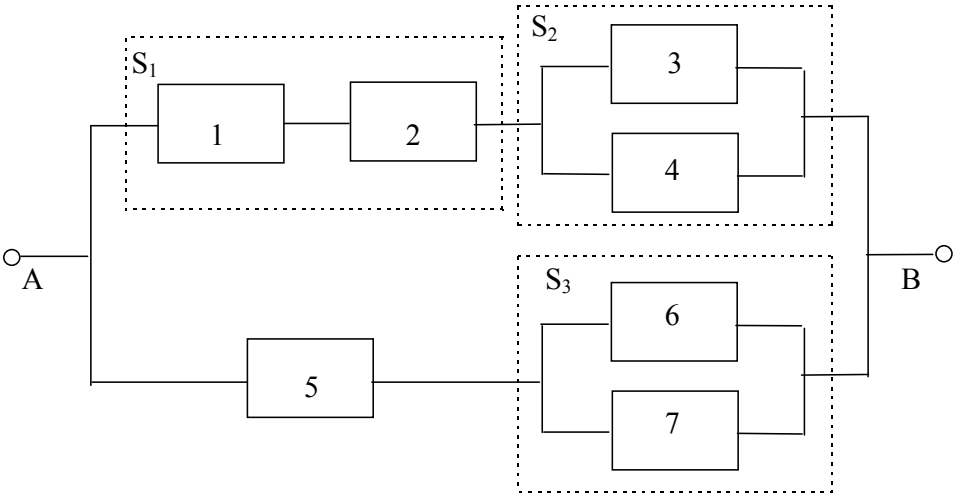

Рис. 3.5. Выделение подсистем в системе с последовательно-параллельным соединением.

Рассматривая подсистемы S_1, S_2, S_3 как условные элементы , получаем новую структурную схему (рис.3.6.).

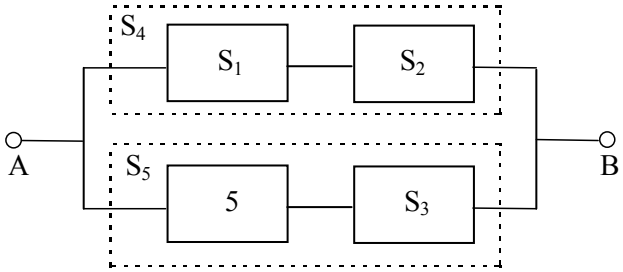

Рис. 3.6. Укрупненная структурная схема.

Выделим в новой структурной схеме подсистемы S_4 и S_5, функции надежности которых

$p_{s_4}(t) = p_{S_1}(t) \cdot p_{S_2}(t)$;

$p_{s_5}(t) = p_5(t) \cdot p_{S_3}(t)$.

Так как подсистемы S_4 и S_5 соединены параллельно, то функция надежности всей системы

$p_s(t) = 1 - (1 - p_{S_4}(t)) \cdot (1 - p_{S_5}(t))$.

ТЕМА 4. Расчет надежности сложных систем

1. РАСЧЕТ НАДЕЖНОСТИ СЛОЖНЫХ СИСТЕМ. СЛОЖНЫЕ СИСТЕМЫ

Не все системы сводятся к последовательно-параллельному соединению элементов. Примером системы, которую нельзя разбить на подсистемы с последовательным или параллельным соединением, является так называемая **мостиковая схема**.

Структурная схема этой системы изображена на рисунке 4.1.

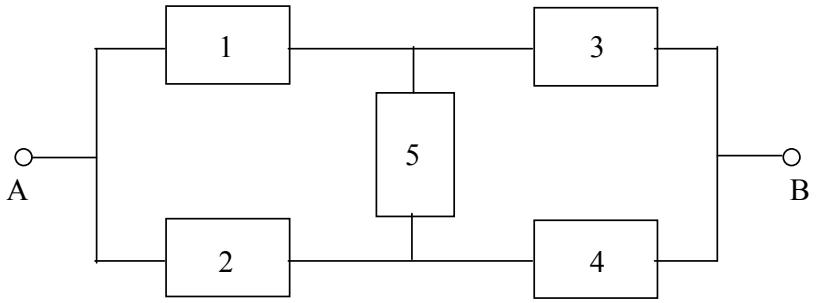

Рис. 4.1. Мостиковая схема.

Системы, не сводящиеся к последовательно - параллельному соединению, будем называть **сложными системами.**

Будем считать, что работоспособность сложной системы можно однозначно определить, зная состояния всех элементов системы.

Опишем несколько методов расчета надежности сложных систем и продемонстрируем их на мостиковой схеме. Для простоты расчетов будем считать, что все элементы имеют одинаковую функцию надежности p (для упрощения формул опустим параметр t) и вероятность отказа q.

2. МЕТОД ПЕРЕБОРА СОСТОЯНИЙ

Состоянием системы будем называть множество работающих элементов системы.

По методу перебора состояний последовательно рассматриваются все возможные состояния системы. Выбираются те состояния, в которых система работоспособна. Для расчета надежности системы суммируются вероятности всех работоспособных состояний.

Для мостиковой схемы получаем следующие работоспособные состояния (каждое состояние определяется указанием работоспособных систем):

Число отказавших элементов	Работоспособные состояния	Вероятность состояния
0	1,2,3,4,5	p^5
1	1,2,3,4 1,2,3,5 1,2,4,5 1,3,4,5 2,3,4,5	p^4q -//-
2	1,2,3 1,2,4 1,3,4 1,3,5 1,4,5 2,3,4 2,3,5 2,4,5	p^3q^2 -//-
3	1,3 2,4	p^2q^3 -//-

Общая надежность системы

$p_s = p^5 + 5p^4q + 8p^3q^2 + 2p^2q^3$.

Например, если $p = q = 0.5$, то $p_s = \frac{1+5+8+2}{2^5} = \frac{16}{32} = 0.5$.

Достоинством метода перебора состояний является его простота. Он относительно легко программируется. Недостатком является громоздкость. Для сложных систем с большим числом элементов метод может оказаться неприменимым из-за больших вычислительных трудностей.

3. МЕТОД РАЗЛОЖЕНИЯ ОТНОСИТЕЛЬНО ОСОБОГО ЭЛЕМЕНТА

В системе выбирается элемент с наибольшим числом связей с другими элементами. Этот элемент называется **особым**. Обозначим надежность этого элемента p_0, вероятность отказа через $q_0 = 1 - p_o$.

1. Предположим, что особый элемент работоспособен (вероятность этого p_0). Тогда получим новую структурную схему надежности.

Предположим, что новая схема является последовательно-параллельным соединением и мы можем рассчитать ее надежность p_{s1}.

Говорим, что новая схема получена из исходной "**замыканием**" особого элемента.

2. Предположим, что особый элемент отказал (вероятность этого q_0). Тогда получим еще одну структурную схему. Если она будет последовательно-параллельным соединением, то рассчитаем ее надежность p_{s2}.

Говорим, что эта схема получена из исходной "**обрывом**" особого элемента.

Введем события:

A - особый элемент работоспособен,

$\overline{A}$ - особый элемент отказал,

B - система работоспособна.

Тогда по формуле полной вероятности

$$P\{B\} = P\{A\} \cdot P\{B|A\} + P\{\overline{A}\} \cdot P\{B|\overline{A}\}.$$

Но так как

$P\{B\} = p_s$ - надежность системы,

$P\{A\} = p_0$, $P\{\overline{A}\} = q_0$,

$P\{B|A\} = p_{s1}$ - функция надежности при замыкании,

$p\{B|\overline{A}\} = p_{s2}$ - функция надежности при обрыве,

то получаем формулу для надежности системы $p_s = p_0 \cdot p_{s1} + q_0 \cdot p_{s2}$.

Для мостиковой схемы особым элементом, имеющим наибольшее число связей, является элемент 5.

При замыкании получаем структурную схему на рисунке 4.2.

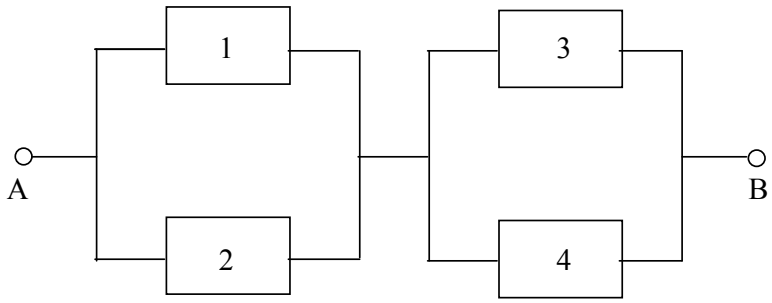

Рис. 4.2. Мостиковая схема после замыкания.

Надежность новой схемы

$$p_{s1} = (1 - q^2)^2.$$

При обрыве получаем схему на рисунке 4.3.

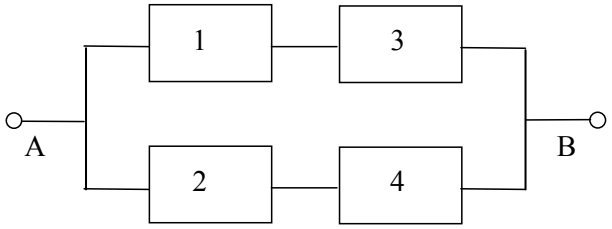

Рис. 4.3. Мостиковая схема после обрыва.

Надежность этой схемы

$p_{s2} = 1 - (1 - p^2)^2$.

Следовательно, для всей системы

$p_s = p \cdot p_{s1} + q \cdot p_{s2} = p(1 - q^2)^2 + q(1 - (1 - p^2)^2)$.

Например, если $p = q = \frac{1}{2}$, то $p_s = \frac{1}{2}(1 - \frac{1}{4})^2 + \frac{1}{2}(1 - (\frac{3}{4})^2) = \frac{1}{2}(\frac{9}{16} + \frac{7}{16}) = \frac{1}{2}$.

Если после замыкания или обрыва структурная схема не сводится к последовательно-параллельному соединению, то выделяем в новой структурной схеме еще один особый элемент и т.д.

4. МЕТОД ПРЕОБРАЗОВАНИЯ "ТРЕУГОЛЬНИК - ЗВЕЗДА"

Допустим, что в структурной схеме можно выделить следующий участок (соединение "треугольником"), состоящий из трех элементов с надежностью p_1, p_2, p_3 (рис.4.4.).

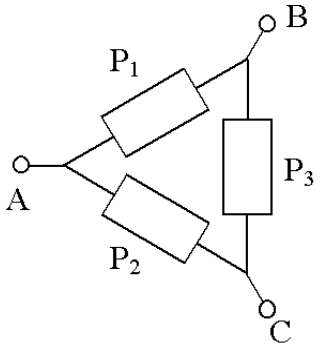

Рис. 4.4. Соединение “треугольником”.

Идея метода в том, что мы заменяем этот участок в схеме другим, состоящим из трех других элементов, имеющих некоторые надежности $\tilde{p}_1, \tilde{p}_2, \tilde{p}_3$, соединенных "звездой" (рис.4.5.).

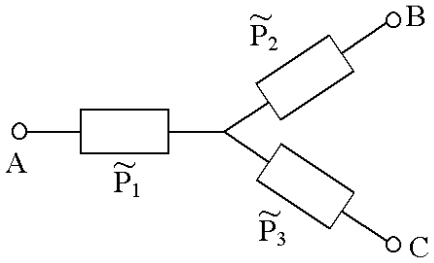

Рис.4.5. Соединение “звездой”.

Надежность системы при этой замене не должна измениться. Это означает, что вероятность связности A и B должна быть одинаковой как для "треугольника ", так и для "звезды". То же самое должно выполняться для вероятностей связности A и C, B и C.

Для соединения "треугольником" вероятность связности A и B можно рассчитать как надежность схемы на рисунке 4.6.

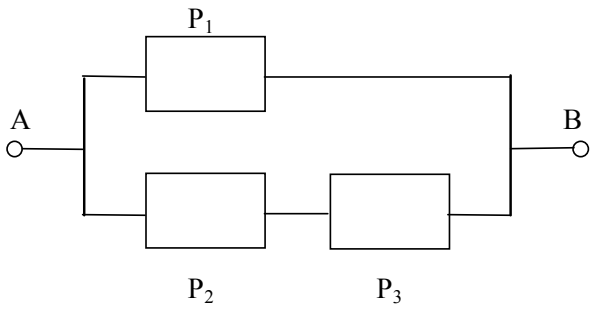

Рис. 4.6. Структурная схема связности A и B при соединении “треугольником”.

Таким образом, первая вероятность равна

$P_I = 1 - (1 - p_1)(1 - p_2 p_3)$.

Для соединения "звездой" вероятность связности A и B можно рассчитать как надежность схемы на рисунке 4.7.

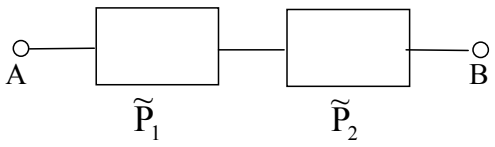

Рис. 4.7. Структурная схема связности A и B при соединении “звездой”.

Таким образом, вторая вероятность равна $P_{II} = \tilde{p}_1\tilde{p}_2$.

Итак, из условия $P_I = P_{II}$ получаем уравнение

$\tilde{p}_1\tilde{p}_2 = 1-(1-p_1)(1-p_2p_3)$.

Аналогично, для вероятностей связности A и C получим уравнение

$\tilde{p}_1\tilde{p}_3 = 1-(1-p_2)(1-p_1p_3)$,

для вероятностей связности B и C уравнение

$\tilde{p}_2\tilde{p}_3 = 1-(1-p_3)(1-p_1p_2)$.

Итак, получаем систему уравнений

$$\tilde{p}_1\tilde{p}_2 = 1-(1-p_1)(1-p_2p_3)$$
$$\tilde{p}_1\tilde{p}_3 = 1-(1-p_2)(1-p_1p_3)$$
$$\tilde{p}_2\tilde{p}_3 = 1-(1-p_3)(1-p_1p_2)$$

В этой системе p_1, p_2, p_3 известны, а $\tilde{p}_1, \tilde{p}_2, \tilde{p}_3$ нужно определить. Решим уравнения:

$$\tilde{p}_1^{\,2} = \frac{\tilde{p}_1\tilde{p}_2 \cdot \tilde{p}_1\tilde{p}_3}{\tilde{p}_2\tilde{p}_3} = \frac{(1-(1-p_1)(1-p_2p_3))(1-(1-p_2)(1-p_1p_3))}{1-(1-p_3)(1-p_1p_2)}.$$

Подобным образом найдем и остальные корни:

$$\tilde{p}_1 = \sqrt{\frac{(1-(1-p_1)(1-p_2p_3))(1-(1-p_2)(1-p_1p_3))}{1-(1-p_3)(1-p_1p_2)}};$$

$$\tilde{p}_2 = \sqrt{\frac{(1-(1-p_1)(1-p_2p_3))(1-(1-p_3)(1-p_1p_2))}{1-(1-p_2)(1-p_1p_3)}}; \qquad (1)$$

$$\tilde{p}_3 = \sqrt{\frac{(1-(1-p_2)(1-p_1p_3))(1-(1-p_3)(1-p_1p_2))}{1-(1-p_1)(1-p_2p_3)}}.$$

В частности, если $p_1 = p_2 = p_3 = p$, то и $\tilde{p}_1 = \tilde{p}_2 = \tilde{p}_3 = \tilde{p}$, причем

$$\tilde{p} = \sqrt{1-(1-p)(1-p^2)} = \sqrt{p+p^2-p^3}. \qquad (2)$$

После замены соединения "треугольником" на соединение "звездой" схема обычно упрощается. При необходимости несколько раз проводят замену

"треугольника" на "звезду", пока не приходят к системе с последовательно-параллельным соединением.

Рассмотрим пример мостиковой схемы. Выделим элементы 1,2 и 5, расположенные "треугольникам" (рис.4.8.), и заменим их на соединение "звездой". Получим систему с последовательно-параллельным соединением (рис.4.9.)

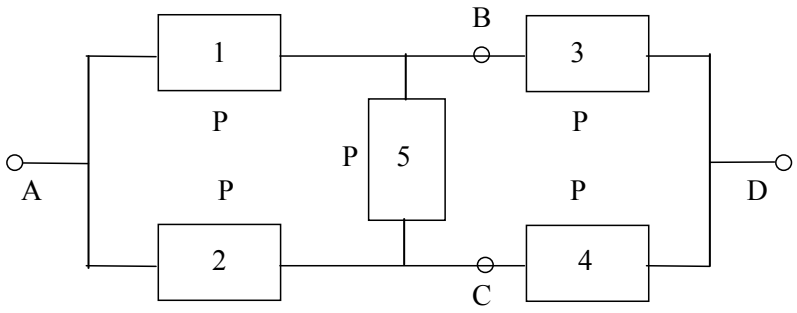

Рис. 4.8. Мостиковая схема.

Надежность новой системы легко рассчитать: $p_s = \tilde{p}(1-(1-\tilde{p}p)^2)$,
где $\tilde{p}$ определяется по формуле (2).

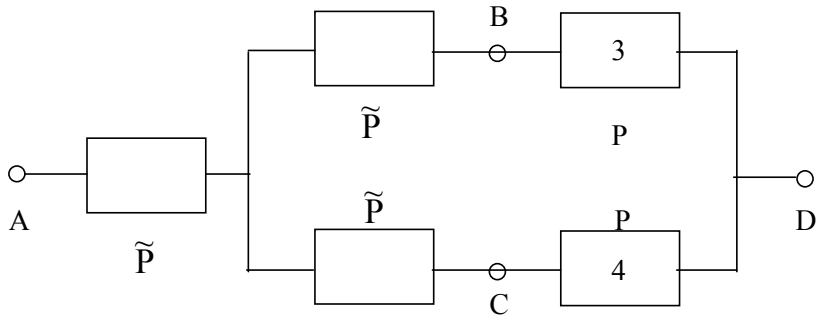

Рис. 4.9. Мостиковая схема после преобразования “треугольник-звезда”.

Пусть $p = \frac{1}{2}$, тогда $\tilde{p} = \sqrt{\frac{1}{2}+\frac{1}{4}-\frac{1}{8}} = \sqrt{\frac{5}{8}} \approx 0{,}7906$,

$$p_s = \sqrt{\frac{5}{8}}(1-(1-\sqrt{\frac{5}{8}}\cdot\frac{1}{2})^2) = \frac{80-\sqrt{250}}{128} \approx 0{,}5015.$$

В двух предыдущих методах мы определим точное значение надежности мостиковой схемы при $p = 0{,}5$: $p_s = 0{,}5$.

По методу преобразования "треугольник - звезда" получаем маленькое отличие в результате. Дело в том, что метод замены "треугольник - звезда" является приближенным: надежность преобразованной схемы не совпадает с надежностью исходной.

Чтобы убедиться в этом, сравним соединения на рисунке 4.10.

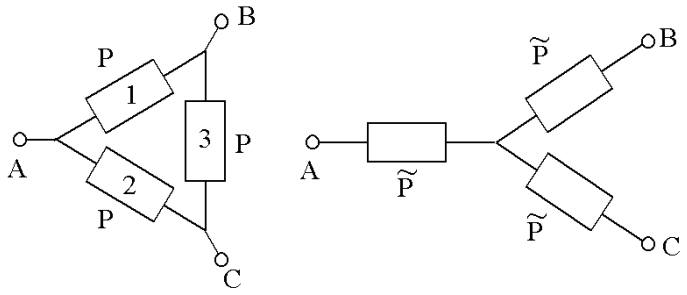

Рис. 4.10. Соединение “треугольником” и соединение “звездой” однотипных элементов.

Вероятности, что связаны A и B, A и C, B и C одинаковы, как для "треугольника", так и для "звезды". Сравним вероятности, что связаны все три вершины A,B и C.

Для "треугольника" все три вершины будут связаны, если работают либо все три элемента (вероятность этого p^3), либо если работают два элемента из трех (1 и 2, 1 и 3 или 2 и 3 - вероятность каждого случая $p^2(1-p)$). Таким образом, общая вероятность будет равна $P_\alpha = p^3 + 3p^2(1-p) = 3p^2 - 2p^3$.

Для "звезды" все вершины будут связаны только, если будут работать все три элемента. Таким образом, $P_в = (\tilde{p})^3 = \sqrt{(p + p^2 - p^3)^3}$.

Вероятности P_a и $P_в$ не совпадают. Например, при $p = 0.5$

$P_a = 0.5$, $P_в = \sqrt{\frac{125}{512}} \approx 0{,}494$.

Итак, метод замены "треугольник - звезда" является приближенным методом.

5. ИНТЕРВАЛЫ НАДЕЖНОСТИ

Иногда структура системы может быть настолько сложной, что задача точного определения надежности оказывается практически не разрешимой. В таких случаях иногда можно ограничиться определением интервалов надежности, т.е. построить оценки надежности сверху и снизу.

Пусть известны надежности $p_i, i = 1,\ldots,n$ каждого элемента. Оценки сверху и снизу можно получить из следующих соображений. Пусть событие A заключается в том, что система работает, событие A_1 - все элементы системы работают, событие A_2 - работает хотя бы один из элементов системы.

Тогда $A_1 \subseteq A \subseteq A_2$, и следовательно, $P\{A_1\} \le P\{A\} \le P\{A_2\}$.

Но $P\{A\} = p_s$;

$P\{A_1\} = \prod_{i=1}^{n} p_i$ - надежность системы с последовательным соединением;

$P\{A_2\} = 1 - \prod_{i=1}^{n} q_i$ - надежность системы с параллельным соединением.

Итак, получаем следующие оценки для интервала надежности

$$\prod_{i=1}^{n} p_i \le p_s \le 1 - \prod_{i=1}^{n} q_i .$$

Полученные оценки называют **грубыми** или **тривиальными** .

Например, для мостиковой схемы получаем тривиальные оценки $p^5 \le p_s \le 1 - q^5$. При p=0,5 это дает диапазон значений $0.031 \le p_s \le 0.969$.

Правило получения тривиальных оценок можно сформулировать следующим образом: если все элементы системы соединить последовательно, то надежность системы понизится; если все элементы соединить параллельно, то надежность системы повысится.

6. МЕТОД МИНИМАЛЬНЫХ ПУТЕЙ И МИНИМАЛЬНЫХ СЕЧЕНИЙ

Данный метод дает более точные оценки интервалов надежности.

Минимальным путем (или **мини - путем**) называется множество элементов системы, для которого выполняются два свойства:

1) если все элементы, принадлежащие мини-пути, работают, то система работает;

2) если отказали все элементы, не принадлежащие мини-пути и хоть один из элементов мини-пути, то система откажет.

Пример 1.

A. Для последовательного соединения единственным мини-путем является все множество элементов системы.

B. Для параллельного соединения каждый элемент системы является отдельным мини-путем. Других мини-путей нет.

C. Для мостиковой схеме определим все мини-пути:

{1,3}, {2,4}, {1,5,4}, {2,5,3}.

Пусть для имеющейся системы найдены все мини-пути. При этом некоторые элементы системы могут принадлежать и нескольким мини-путям.

Мини-путь назовем **работающим**, если работают все входящие в него элементы.

Вероятность работы мини-пути равна произведению вероятностей работы всех входящих в этот мини-путь элементов. Поэтому каждому мини-пути сопоставим систему из последовательно соединенных элементов этого мини-пути.

Если хоть один из мини-путей системы работает, то работает вся система. И наоборот, если все мини - пути не работают, то и система откажет. Таким образом, отказ системы заключается в отказе всех мини-путей.

Пусть событие А - отказ системы, $A_1, A_2, \ldots, A_k$ - отказ одного из мини-путей системы. Тогда $A = A_1 \cdot A_2 \cdot \ldots \cdot A_k$.

По теореме умножения вероятностей

$P\{A_1 A_2 \ldots A_k\} = P\{A_1\} \cdot P\{A_2 | A_1\} P\{A_3 | A_1 A_2\} \cdot \ldots \cdot P\{A_k | A_1, \ldots, A_{k-1}\}$.

Но если первый и второй мини-пути не содержат общих элементов, то отказы их независимы и $P\{A_2 | A_1\} = P\{A_2\}$.

Если же мини-пути содержат общие элементы, то отказ одного из них, очевидно, увеличивает вероятность отказа другого. Следовательно, $P\{A_2 | A_1\} \geq P\{A_2\}$.

Аналогично, $P\{A_3 | A_1 A_2\} \geq P\{A_3\}$ и т.д. Получаем, что $P\{A\} = P\{A_1 A_2 \ldots A_k\} \geq P\{A_1\} \cdot P\{A_2\} \cdot \ldots \cdot P\{A_K\}$, т.е. вероятность отказа системы больше или равна произведения вероятностей отказа мини-путей.

Следовательно, если мы все мини - пути соединим параллельно, то получим новую систему с надежностью, не меньшей, чем надежность исходной системы.

Итак, методика получения оценки надежности сверху:

1)находим все мини - пути системы;

2)элементы каждого мини-пути соединяем последовательно;

3) все полученные на предыдущем шаге системы с последовательным соединением соединяем параллельно.

Полученная система с последовательно- параллельным соединением имеет не меньшую надежность, чем исходная система.

Пример 2.

А. Для последовательного соединения мини-путь один, и он совпадает с исходной системой.

В. Для параллельного соединения существует n мини-путей, состоящих из одного элемента, и их параллельное соединение совпадает с исходной системой.

С. Для мостиковой схемы параллельное соединение мини-путей дает систему на рисунке 4.11.

Надежность этой системы $p_1 = 1 - (1 - p^2)^2 (1 - p^3)^2$.

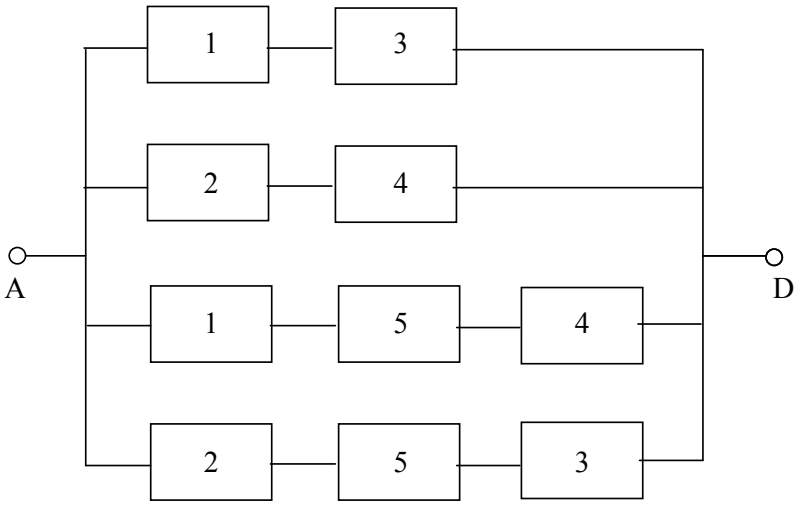

Рис. 4.11. Параллельное соединение мини-путей мостиковой схемы.

Следовательно, для мостиковой схемы получаем оценку сверху $p_S \le p_1 = 1-(1-p^2)^2(1-p^3)^2$.

Например, при p=0,5 получаем $p_1 \approx 0{,}57$.

Введем теперь понятие минимального сечения системы.

Минимальным сечением (или **мини-сечением**) называется множество элементов системы, для которого выполняются два свойства:

1)если работают все элементы, не принадлежащие мини-сечению и хоть один из элементов мини-сечения, то и система работает;

2)если все элементы, принадлежащие мини-сечению, отказали, то и вся система отказала.

Пример 3.

A. Для системы с последовательным соединением элементов каждый элемент является мини-сечением системы. Других мини-сечений нет.

B. Для системы с параллельным соединением элементов единственным мини-сечением является все множество элементов системы.

C. Для мостиковой схемы мини-сечениями являются:

{1,2}, {3,4}, {1,5,4}, {2,5,3}.

Пусть для имеющейся системы найдены все мини-сечения. Мини-сечение назовем **работающим**, если в нем работает хоть один из элементов. Каждому

мини-сечению сопоставим систему из параллельно соединенных элементов этого мини-сечения.

Система будет работать тогда и только тогда, когда будет работать все ее минимальные сечения.

Пусть событие B - работа системы, события $B_1,\ldots,B_l$ - работа соответствующего мини-сечения. Тогда $B = B_1 \cdot \ldots \cdot B_l$. Аналогично случаю с мини-путями получаем $P\{B\} \geq P\{B_1\} \cdot P\{B_2\} \cdot \ldots \cdot P\{B_l\}$, т.е. вероятность работы системы больше или равна произведению вероятностей работы мини-сечений.

Следовательно, если мы все мини-сечения соединим последовательно, то получим новую систему с надежностью не большей, чем надежность исходной системы.

Итак, методика получения оценки надежности снизу:

1)находим все мини-сечения системы;

2)элементы каждого мини-сечения соединяются параллельно;

3)все полученные на предыдущем шаге системы с параллельным соединением соединяем последовательно.

Надежность полученной системы с последовательно- параллельным соединением не превышает надежности исходной системы.

***Пример 4*.**

A. Для системы с последовательным соединением построенная таким образом система совпадает с исходной.

B. Для системы с параллельным соединением получаем аналогичный результат.

C. Для мостиковой схемы последовательное соединение мини-сечений приводит к системе на рисунке 4.12.

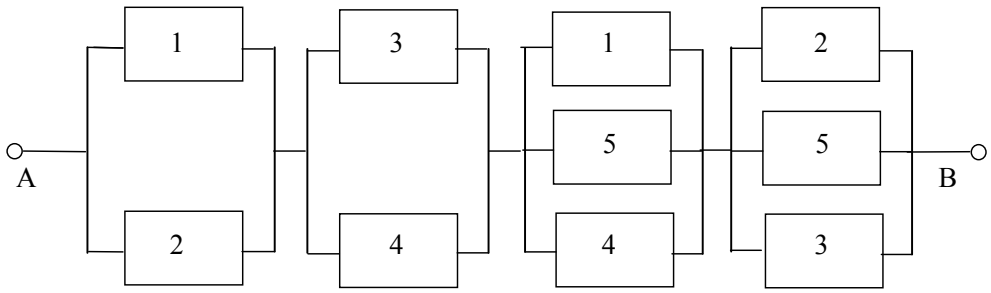

Рис. 4.12. Последовательное соединение мини-сечений мостиковой схемы.

Надежность этой системы $p_2 = 1-(1-q^2)^2(1-q^3)^2$.

Следовательно, для мостиковой схемы получаем оценку надежности снизу $p_S \leq p_2 = 1-(1-q^2)^2(1-q^3)^2$.

Например, при p=q=0,5 получаем $p_2 \approx 0{,}43$.

7. СТРУКТУРЫ ТИПА “K ИЗ N”

Не для всех систем удается построить структурную схему надежности. Примерами систем, для которых нет структурной схемы, являются так называемые **структуры типа “k из n”** - системы из n элементов, имеющих одинаковые функции надежности. Структура типа “k из n” работает тогда и только тогда, когда работают по крайней мере k ее элементов. При k=1 такая структура превращается в параллельное соединение, при k=n - в последовательное соединение.

Пусть функция надежности каждого элемента структуры p(t). Тогда вероятность того, что в момент t в структуре работает ровно i элементов, определяется по формуле Бернулли $C_n^i(p(t))^i(1-p(t))^{n-i}$. Следовательно, надежность структуры типа “k из n” равна

$$p_S(t)=\sum_{i=k}^{n} C_n^i(p(t))^i(1-p(t))^{n-i}=1-\sum_{i=0}^{k-1} C_n^i(p(t))^i(1-p(t))^{n-i}.$$

Предположим, что все элементы структуры имеют показательное распределение наработки до отказа с интенсивностью λ. Определим среднюю наработку до отказа всей системы.

Воспользуемся методом графа состояний. Для структуры типа “k из n” граф состояний изображен на рисунке 4.13.

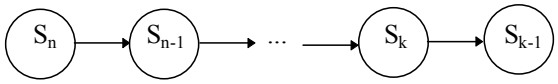

Рис. 4.13. Граф состояний структуры типа “k из n”.

десь S_n - состояние, когда работают все n элементов,..., S_k - работает к элементов, S_{k-1} - отказ системы.

Среднее время пребывания системы в состоянии S_i $(i=n,n-1,\ldots,k)$ будет равно $\frac{1}{\lambda i}$. Следовательно, средняя наработка структуры типа к из n равна

$$\tau_S=\frac{1}{\lambda n}+\frac{1}{\lambda(n-1)}+\ldots+\frac{1}{\lambda k}=\frac{1}{\lambda}\sum_{i=k}^{n}\frac{1}{i}.$$

8. СТРУКТУРНАЯ ФУНКЦИЯ НАДЕЖНОСТИ

Часто вместо структурной схемы надежности системы используют структурную функцию надежности.

Рассмотрим систему, состоящую из n элементов с индикаторами состояния $x_1, x_2, \ldots, x_n$:

$$x_i = \begin{cases} 1, & \textit{если } i-\textit{й элемент работает} \\ 0, & \textit{если } i-\textit{й элемент отказал.} \end{cases}$$

Структурная или индикаторная, функция $\varphi(x) = \varphi(x_1, \ldots, x_n)$ системы определяется следующим образом

$$\varphi = \begin{cases} 1, & \textit{если система работает,} \\ 0, & \textit{если система отказала.} \end{cases}$$

Структурная функция системы является булевой функцией, поэтому ее часто определяют с помощью логических операций.

Система из последовательно соединенных элементов имеет структурную функцию

$$\varphi(x) = \prod_{i=1}^{n} x_i = \min(x_1, \ldots, x_n) = x_1 \& \ldots \& x_n .$$

Для системы из параллельно соединенных элементов структурная функция имеет вид

$$\varphi(x) = \max(x_1, \ldots, x_n) = 1 - \prod_{i=1}^{n} (1 - x_i) = x_1 \vee x_2 \vee \ldots \vee x_n .$$

Для структуры типа к из n структурная функция выглядит следующим образом

$$\varphi(x) = \begin{cases} 1, & \textit{если } \sum_{i=1}^{n} x_i \geq k \\ 0, & \textit{если } \sum_{i=1}^{n} x_i < k. \end{cases}$$

Для задания структурной функции сложной системы можно использовать мини-пути и мини-сечения.

Так как система работает тогда и только тогда, когда работает хоть один из ее мини путей, то структурную функцию можно задать как дизъюнктивную нормальную форму, в которой каждая элементарная конъюнкция является конъюнкцией элементов соответствующего мини-пути.

Например, для мостиковой схемы структурную функцию можно задать как:

$$\varphi(x_1, x_2, x_3, x_4, x_5) = x_1 x_3 \vee x_2 x_4 \vee x_1 x_5 x_4 \vee x_2 x_5 x_3 .$$

С другой стороны, система работает тогда и только тогда, когда работают все ее мини-сечения. Поэтому структурную функцию можно задать в конъюктивной нормальной форме, в которой каждая элементарная дизъюнкция является дизъюнкцией элементов соответствующего мини-сечения.

Например, для той же мостиковой схемы структурную функцию можно записать в виде

$$\varphi = (x_1 \vee x_2)(x_3 \vee x_4)(x_1 \vee x_5 \vee x_4)(x_2 \vee x_5 \vee x_3) .$$

С помощью метода перебора состояний структурную функцию можно задать в виде СДНФ. Например, для мостиковой схемы

$$\varphi = x_1x_2x_3x_4x_5 \vee x_1x_2x_3x_4\overline{x}_5 \vee x_1x_2x_3\overline{x}_4x_5 \vee x_1x_2\overline{x}_3x_4x_5 \vee$$
$$\vee x_1\overline{x}_2x_3x_4x_5 \vee \overline{x}_1x_2x_3x_4x_5 \vee x_1x_2x_3\overline{x}_4\overline{x}_5 \vee x_1x_2\overline{x}_3x_4\overline{x}_5 \vee$$
$$\vee x_1\overline{x}_2x_3x_4\overline{x}_5 \vee x_1\overline{x}_2x_3\overline{x}_4x_5 \vee x_1\overline{x}_2\overline{x}_3x_4x_5 \vee \overline{x}_1x_2x_3x_4\overline{x}_5 \vee$$
$$\vee \overline{x}_1x_2x_3\overline{x}_4x_5 \vee \overline{x}_1x_2\overline{x}_3x_4x_5 \vee x_1\overline{x}_2x_3\overline{x}_4\overline{x}_5 \vee \overline{x}_1x_2\overline{x}_3x_4\overline{x}_5.$$

ТЕМА 5. Резервирование

1. РЕЗЕРВИРОВАНИЕ ВИДЫ РЕЗЕРВИРОВАНИЯ

Резервированием называется способ повышения надежности системы с помощью применения дополнительных средств. Существуют следующие виды резервирования: **структурное, функциональное, временное, информационное**.

Структурное резервирование предусматривает в системе замену отказавших элементов резервными при условии, что резервные элементы входят конструктивно и функционально в состав системы. Включение резерва может быть произведено вручную или автоматически. Возможна такая функциональная связь резервного элемента с основным, при которой не требуется специального включения.

Программное обеспечение тоже может быть резервировано. В этом случае под резервом понимается наличие запасных вариантов (версий) всей программы или ее отдельных модулей, которые будут задействованы при помощи команд условного перехода при отказе основной программы.

При **функциональном резервировании** используется способность элементов выполнять дополнительные функции, а также возможность выполнять заданную функцию дополнительными средствами. Такое резервирование часто применяют для многофункциональных систем.

При **временном резервировании** выделяется резервное время для выполнения заданной функции.

Пусть для выполнения некоторой операции требуется время t. При планировании работы на эту операцию отводится время $t + t_r$, где t_r - резервное время. Оно может быть использовано либо для повторения операции, либо для устранения неполадок.

Другой вид временного резервирования заключается в том, что допускается перерыв функционирования элемента в системе. Временное резервирование обеспечивает непрерывность технологического процесса за счет введения складов сырья и полуфабрикатов.

При **информационном резервировании** в качестве резерва используется избыточная информация, с помощью которой оценивается достоверность передаваемой информации. Типичный пример информационного резервирования – использование дополнительных разрядов при кодировании информации. Это позволяет обнаружить и даже устранять ошибки в передаче информации.

2. СТРУКТУРНОЕ РЕЗЕРВИРОВАНИЕ

Структурное резервирование является самым распространенным и наиболее эффективным средством повышения надежности.

Есть два принципиально отличных метода повышения надежности системы путем структурного резервирования: **общее резервирование**, при котором

резервируется система в целом, и **раздельное (поэлементное) резервирование**, при котором резервируются отдельные элементы системы.

В производственных системах наибольшее применение находит раздельное резервирование, так как при раздельном резервировании выигрыш в надежности достигается значительно меньшими затратами, чем при общем резервировании, особенно в системах с большим количеством элементов.

Различают резервирование с целой и дробной кратностью.

Резервированием с целой кратностью называют такое резервирование, при котором для нормальной работы основного элемента за ним закреплены один или несколько резервных элементов**. Резервированием с дробной кратностью** называют такое резервирование, при котором резервный элемент может заменить любой из некоторого множества основных элементов.

Частным случаем резервирования с дробной кратностью является **резервирование со скользящим (плавающим) резервом**, при котором любой из резервных элементов может замещать любой элемент основной системы. При этом после замещения этот резервный элемент становится основным, и при отказе сам может быть замещен любым из оставшихся резервных элементов. Последний вид резервирования применяется в специальных производственных системах с большим количеством однотипных элементов.

Резервные элементы или системы различаются по способу содержания в условиях эксплуатации: одни могут включаться на все время работы системы, другие – только при отказе основных элементов. Поэтому различают два вида включения резерва: **постоянный**, или **пассивный** (первый случай), и **активный,** или **замещением** (второй случай). При резерве замещением возможны в свою очередь три вида условий работы резервных элементов до момента их включения в работу.

Первый вид характеризуется тем, что внешние условия резерва совпадают с условиями работы основных элементов, поэтому этот вид резерва называют **горячим** или **нагруженным.** Ресурс резервных элементов в этом случае начинает расходоваться с момента включения в работу всей системы, и вероятность безотказной работы резервных элементов в этом случае не зависит от того, в какой момент времени элемент включается в работу.

Второй вид резерва характеризуется тем, что внешние условия, воздействующие на резервные элементы до момента их включения в работу, облегченные. Поэтому этот вид резерва называют **теплым** или **облегченным** резервом. В этом случае ресурс резервных элементов начинает также расходоваться с момента включения всей системы в работу, однако интенсивность расхода ресурса резервных элементов до момента включения их вместо отказавших значительно ниже, чем в рабочих условиях. Вероятность безотказной работы резервных элементов в случае этого вида резерва будет зависеть как от момента включения их в работу, так и от того, насколько отличаются законы распределения их наработки до отказа в рабочем и резервном условиях.

Последний, третий, вид резерва замещением – **холодный** или **ненагруженный** резерв. В этом случае резервные элементы начинают расходовать

свой ресурс только с момента включения их в работу вместо отказавших основных. Следовательно, у холодного резерва в резервном состоянии надежность всегда равна единице.

Оба вида резерва имеет свои преимущества и недостатки. Достоинством постоянного резерва является простота, так как в этом случае не требуется никаких переключающих устройств, а самое главное, отсутствует перерыв в работе. Недостатком этого способа резервирования является нарушение режима работы резервных элементов при отказе основных.

Включение резерва замещением обладает следующими преимуществами: не нарушает режима работы резервных элементов, сохраняет в большей степени надежность резервных элементов, позволяет использовать резервный элемент на несколько основных элементов. Существенный недостаток этого способа резервирования заключается в необходимости применения переключающих устройств, которые могут значительно понизить надежность всей системы. Поэтому резервирование замещением выгодно, как правило, только при высокой надежности переключающих устройств.

Расчеты надежности резервированных систем в существенной степени зависят от способа резервирования.

3. НАДЕЖНОСТЬ СИСТЕМ ПРИ ПОСТОЯННОМ РЕЗЕРВИРОВАНИИ

Выведем зависимости надежности резервированной системы при известных значениях надежности ее элементов. Будем считать, что основные элементы в системе соединены последовательно, и что основные и резервные элементы одного и того же назначения имеют одинаковые значения надежности.

Функция надежности системы без резервных элементов определяется как

$$p_s(t) = \prod_{i=1}^{n} p_i(t),$$

где $p_i(t)$ – функции надежности элементов системы.

Пусть для повышения надежности в системе применено резервирование с целой кратностью k, т.е. для каждого основного элемента в систему включено к резервных, имеющих такую же функцию надежности.

Рассмотрим два варианта резервирования.

1. Общее резервирование.

При общем резервировании (рис. 5.1.) систему можно рассматривать как параллельное соединение (k+1)-й подсистемы, где каждая подсистема состоит из n последовательно соединенных элементов.

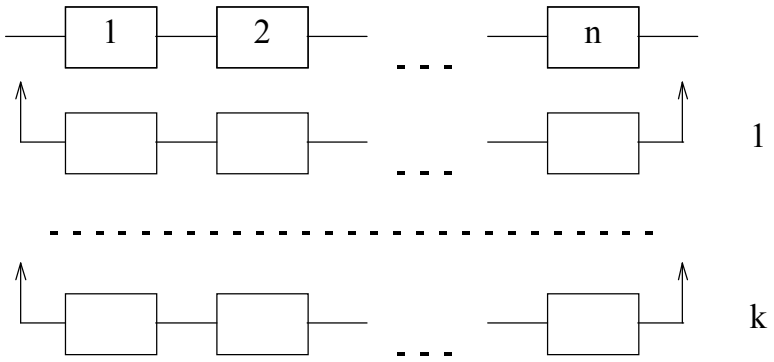

Рис. 5.1. Схема общего резервирования.

Таким образом, функция отказа резервированной системы

$$q_s^{(r)}(t) = (q_s(t))^{k+1} = (1 - \prod_{i=1}^{n} p_i(t))^{k+1},$$

а функция надежности равна

$$p_s^{(r)}(t) = 1 - (1 - \prod_{i=1}^{n} p_i(t))^{k+1}.$$

Если все элементы системы имеют одинаковую надежность p(t), то

$$p_s^{(r)}(t) = 1 - (1 - p^n(t))^{k+1}.$$

Если все элементы системы имеют постоянные интенсивности отказов λ_i, i=1,2,...,n, то нерезервированная система имеет постоянную интенсивность отказов $\lambda_s=\lambda_1+\lambda_2+...+\lambda_n$, и средняя наработка системы при общем резервировании с целой кратностью k равна

$$\tau_s^{(r)} = \frac{1}{\lambda_1 + \lambda_2 + \ldots + \lambda_n}(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{k+1}).$$

2. Раздельное резервирование.

При раздельном резервировании (рис. 5.2.) систему можно рассматривать как последовательное соединение n подсистем, где каждая система состоит из (k+1) параллельно соединенных элементов.

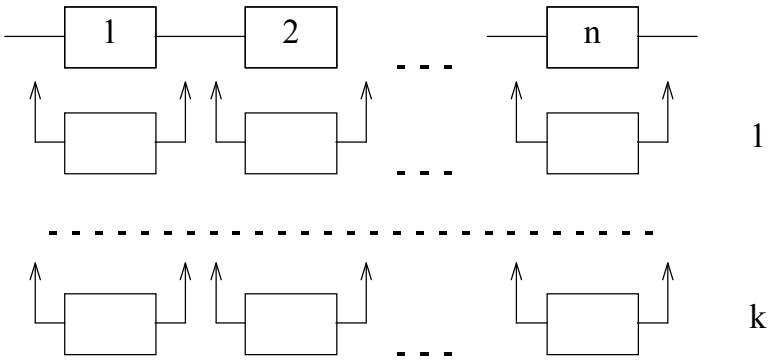

Рис. 5.2. Схема раздельного резервирования.

Таким образом, функция надежности системы с раздельным резервированием

$$p_s^{(r)}(t) = \prod_{i=1}^{n} (1 - (1 - p_i(t))^{k+1}).$$

Если все элементы системы имеют одинаковую надежность p(t), то

$$p_s^{(r)}(t) = (1 - (1 - p(t))^{k+1})^n.$$

Пример 1. Система состоит из 10 последовательно соединенных элементов, надежность работы каждого элемента 0,9. Сколько необходимо резервных элементов при обоих способах резервирования, для того чтобы надежность резервированной системы была не меньше 0,95?

Решение:

В нашем случае n = 10, p = 0,9, $p_s^{(r)} = 0,95$.

Кратность резерва при общем резервировании определим из неравенства

$$p_s^{(r)} \le 1 - (1 - p^n)^{k+1},$$

откуда

$$k \ge \frac{\ln(1 - p_s^{(r)})}{\ln(1 - p^n)} - 1.$$

Подставляя исходные данные, получим

$$k \ge \frac{\ln(1 - 0,95)}{\ln(1 - 0,9^{10})} - 1 = \frac{\ln 0,05}{\ln 0,65} - 1 \approx 5,99.$$

Следовательно, для обеспечения требуемой надежности необходимо 6 резервных систем по 10 элементов в каждой, т.е. всего 60 элементов.

Определим теперь необходимое число резервных элементов при раздельном резервировании, для чего воспользуемся неравенством

$$p_s^{(r)} \le (1 - (1 - p)^{k+1})^n,$$

откуда

$$k \ge \frac{\ln(1 - \sqrt[n]{p_s^{(r)}})}{\ln(1 - p)} - 1.$$

Подставив исходные данные, получим

$$k \ge \frac{\ln(1 - \sqrt[10]{0{,}95})}{\ln(1 - 0{,}9)} - 1 \approx 1{,}29.$$

Следовательно, для обеспечения требуемой надежности требуется резервирование кратности k=2, а всего резервных элементов будет 20.

Таким образом, применяя в данном случае раздельное резервирование, можно при той же надежности выиграть в стоимости системы (в данном случае в $\frac{10+60}{10+20} = 2\frac{1}{3}$ раза).

4. НАДЕЖНОСТЬ СИСТЕМ ПРИ РЕЗЕРВИРОВАНИИ ЗАМЕЩЕНИЕМ

Рассмотрим показатели надежности для следующих вариантов резервирования:

а) резервирование с целой кратностью, когда резервированная система содержит один основной элемент и k резервных. Такое резервирование называется **резервированием кратности k.**

б) резервирование со скользящим резервом, при котором система содержит n последовательно соединенных основных элементов и k резервных. При этом любой из резервных элементов может заменить любой из основных. Такое резервирование называется **резервированием кратности k/n.**

Основные и резервные элементы предполагаем физически однотипными, т.е. имеющими одинаковые функции надежности при условии одинаковой эксплуатации.

Рассмотрим случаи различных видов резерва.

А. Горячий резерв.

А1. Резервирование кратности k.

Система работает до тех пор , пока не откажут все элементы, и ее можно рассматривать как параллельное соединение (k+1)-го элемента. Следовательно, функция надежности

$$p_s^{(r)}(t) = 1 - (1 - p(t))^{k+1}.$$

Если все элементы имеют постоянную интенсивность отказов λ, то средняя наработка резервированной системы равна

$$\tau_s^{(r)} = \frac{1}{\lambda} \sum_{i=1}^{k+1} \frac{1}{i}.$$

A2. Резервирование кратности k/n.

Система будет работать до тех пор, пока из всех элементов, как основных, так и резервных, будут работать хотя бы n. Поэтому в случае горячего резерва систему можно рассматривать как структуру типа «n из n+k».

Следовательно,

$$p_s^{(r)}(t) = \sum_{i=n}^{n+k} C^i_{n+k}\, p^i(t)\, q^{n+k-i}(t).$$

Если все элементы имеют постоянную интенсивность отказов λ, то средняя наработка резервированной системы равна

$$\tau_s^{(r)} = \frac{1}{\lambda} \sum_{i=1}^{n+k} \frac{1}{i}.$$

B. Холодный резерв.

B1. Резервирование кратности k.

Система функционирует следующим образом: основной элемент работает в течение некоторой случайной наработки T_0, затем один из резервных переходит в рабочее состояние и работает в течение времени T_1, затем включается второй резервный элемент и т.д. Наработка до отказа всей системы

$$T_s = T_0 + T_1 + \ldots + T_k.$$

Так как в случае холодного резерва случайные величины T_0, T_1, ..., T_k независимы и имеют одинаковые распределения, то средняя наработка резервированной системы равна

$$\tau_s^{(r)} = M(T_s) = M(T_0) + M(T_1) + \ldots + M(T_k) = (k + 1)\,\tau,$$

где τ - средняя наработка одного элемента.

Зная распределение наработки элемента, можно определить и распределение наработки системы как суммы (k+1) независимых случайных величин с одинаковым распределением.

Если все элементы имеют постоянную интенсивность отказов λ, то можно вывести, что функция надежности резервированной системы равна

$$p_s^{(r)}(t) = e^{-\lambda t} \sum_{i=0}^{k} \frac{\lambda^i t^i}{i!}.$$

B2. Резервирование кратности k/n.

Ограничимся рассмотрением случая, когда все элементы имеют одинаковую постоянную интенсивность отказов λ.

Функционирование системы можно представить в виде графа состояний на рисунке 5.3. Здесь $S_{n,\,i}$ – состояние, в котором n элементов работают (среди которых могут быть и резервные, переведенные в рабочее состояние), а i элементов находятся в резерве, S_0 – состояние отказа системы.

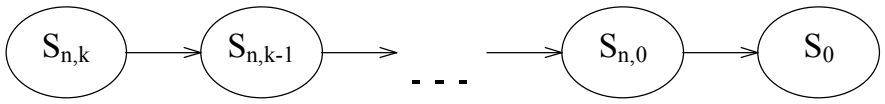

Рис 5.3. Граф состояний холодного резерва кратности k/n

Каждое из состояний $S_{n,\,i}$ имеет случайную длительность, распределенную так же, как и наработка системы из n последовательно соединенных элементов с интенсивностью λ, т.е. наработка объекта с интенсивностью nλ. Поэтому у исследуемой системы надежность такая же, как у системы с холодным резервом кратности k и интенсивностью каждого элемента nλ. Подставив в формулы из предыдущего раздела вместо λ значение nλ, получим, что для системы с холодным резервом кратности k/n функция надежности равна

$$p_s^{(r)}(t) = e^{-n\lambda t}\sum_{i=0}^{k}\frac{(n\lambda t)^i}{i!},$$

а средняя наработка до отказа

$$\tau_s^{(r)} = \frac{k+1}{n\lambda} = \frac{k+1}{n}\tau.$$

С. Теплый резерв.

Ограничимся рассмотрением случая, когда все элементы имеют постоянную интенсивность отказов. Пусть у основного элемента интенсивность λ, у резервного элемента в резервном состоянии постоянная интенсивность $\lambda_r < \lambda$; как только резервный элемент переходит в рабочее состояние, значение интенсивности сразу становится равным λ.

С1. Резервирование кратности k

Функционирование системы можно представить в виде графа состояний на рисунке 5.4.

Рис 5.4. Граф состояний теплого резерва кратности *к.*

Здесь S_{k+1} – состояние, в котором исправны и основной, и все резервные элементы. Оно продолжается случайное время V_{k+1}. Какой бы элемент не отказал в этом состоянии первым: основной или резервный, система в любом случае переходит в состояние S_k: один элемент основной (или резервный, но в рабочем состоянии) и k-1 резервных элементов в резервном состоянии. Случайное время пребывания системы в состоянии S_k обозначим V_k. После этого система переходит в состояние S_{k-1} (один какой-то элемент работает, k-2 в резерве). Попав в состояние S_1, в котором работает один элемент, и резерва больше нет, система через случайное время V_1 переходит в состояние отказа S_0.
Случайная величина V_{k+1} имеет такое же распределение, как и наработка до отказа системы из k+1 последовательно соединенных элементов, в которой у одного из элементов интенсивность λ, а у всех остальных – λ_r. Поэтому среднее время пребывания системы в состоянии S_{k+1} равно

$$M(V_{k+1}) = \frac{1}{\lambda + k\lambda_\tau}.$$

Аналогично,

$$M(V_k) = \frac{1}{\lambda + (k-1)\lambda_\tau}, \ldots, M(V_1) = \frac{1}{\lambda}.$$

Таким образом, для системы с теплым резервом кратности k средняя наработка в случае постоянной интенсивности отказов равна

$$\tau_s^{(r)} = M(V_{k+1}) + M(V_k) + \ldots + M(V_1) = \sum_{i=0}^{k} \frac{1}{\lambda + i\lambda_r}.$$

С2. Резервирование кратности k/n

Построим граф состояний системы (рис.5.5.). Здесь $S_{n,\,i}$ – состояние, в котором n элементов находятся в рабочем состоянии, i элементов - в резервном состоянии, S_0 - состояние отказа системы.

Рис 5.5 Граф состояний теплого резерва кратности k/n.

Пусть в состоянии $S_{n,\,i}$ система находится некоторое случайное время $V_{n,\,i}$, тогда наработка до отказа системы

$$T_s = V_{n,\,k} + V_{n,\,k-1} + \ldots + V_{n,\,0}\ .$$

Каждая из случайных величин $V_{n,\,i}$ распределена так же, как и наработка системы из n+i последовательно соединенных элементов, n из которых имеют интенсивность отказов λ, а i элементов - интенсивность отказов λ_r.

Следовательно,

$$M(V_{n,i}) = \frac{1}{n\lambda + i\lambda_r}.$$

Таким образом, получаем, что для системы с теплым резервом кратности k/n средняя наработка в случае постоянной интенсивности отказов равна

$$\tau_s^{(r)} = \sum_{i=0}^{k} \frac{1}{n\lambda + i\lambda_r}.$$

5. ЗАДАЧА ОПТИМАЛЬНОГО РЕЗЕРВИРОВАНИЯ

Пусть система представляет собой последовательное соединение элементов, среди которых есть однотипные классы. Разобъем множество элементов системы на классы однотипных элементов. В системе окажется m классов элементов. Считаем, что класс с номером i содержит n_i элементов с постоянной интенсивностью отказов λ_i.

Предположим, что для элементов класса i применяется холодное резервирование кратности k_i/n_i. Тогда, рассматривая класс i как подсистему из n_i последовательно соединенных элементов, получаем, что функция надежности такой подсистемы с учетом резервирования равна

$$p_{si}^{(r)}(t) = \exp(-n_i\lambda_i t)\sum_{j=0}^{k_i} \frac{(n_i\lambda_i t)^j}{j!}.$$

Вся система является последовательным соединением таких подсистем, поэтому ее функция надежности равна

$$p_s^{(r)}(t) = \prod_{i=1}^{m} e^{-n_i\lambda_i t} \sum_{j=0}^{k_i} \frac{(n_i\lambda_i t)^j}{j!}. \qquad (1)$$

Очевидно, чем больше k_i, тем выше надежность. Однако есть экономические ограничения. Пусть стоимость одного элемента i-й группы c_i, а общие затраты на резерв не должны превышать C. Получаем ограничение

$$\sum_{i=1}^{m} c_i k_i \le C.. \qquad (2)$$

Пусть в качестве показателя надежности системы выбрана вероятность безотказной работы системы в течение определенного срока t. Тогда задача оптимального резервирования ставится следующим образом: среди всех вариантов резервирования системы (k_1, ... ,k_m), которые удовлетворяют ограничению (2), выбрать вариант, при котором функция надежности (1) достигает максимума.

Задачу можно несколько упростить, если учесть, что

$$p_S^{(r)}(t) = p_S(t) \cdot \prod_{i=1}^{m} \sum_{j=0}^{k_i} \frac{(n_i \lambda_i t)^j}{j!},$$

где $p_S(t) = \prod_{i=1}^{m} e^{-n_i \lambda_i t}$ - надежность нерезервированной системы.

Значения $p_S(t)$ и $n_i \lambda_i t$, i=1,2, ... ,m не зависят от варианта резервирования. Поэтому вместо максимума функции надежности можно искать максимум более простой функции

$$\prod_{i=1}^{m} \sum_{j=0}^{k_i} \frac{(\mu_i)^j}{j!},$$

где $\mu_i = n_i \lambda_i t$ - фиксированные величины в нашей задаче.

Таким образом, задача оптимального резервирования сводится к задаче математического программирования: найти набор неотрицательных целочисленных значений $k_1, k_2, ..., k_m$, удовлетворяющих ограничению

$$\sum_{i=1}^{m} c_i k_i \le C$$

и максимизирующих целевую функцию

$$\prod_{i=1}^{m} \sum_{j=0}^{k_i} \frac{(\mu_i)^j}{j!}.$$

Так как для любого допустимого варианта резервирования $0 \le k_i \le C/c_i$, то допустимых вариантов – конечное число, и оптимальное резервирование можно определить простым перебором. Если вариантов слишком много, то применяют специальные методы оптимизации.

6. УЧЕТ НАДЕЖНОСТИ ПЕРЕКЛЮЧАЮЩИХ УСТРОЙСТВ

До сих пор, говоря о "переключении" на резервный элемент, мы предполагали, что либо для этого не требуется специального переключающего устройства, либо надежность переключающего устройства равна единице. Это допущение справедливо, если можно считать, что вероятность отказа переключателя значительно меньше вероятности отказа рабочего элемента, и

тогда отказом переключателя можно пренебречь. В противном случае необходимо учитывать также и возможный отказ переключателя.

Рассмотрим случай горячего резерва кратности 1. В системе есть основной элемент 1, резервный элемент 2 и переключающее устройство П. Надежности основного и резервного элементов равны p, надежность переключателя равна p_o.

Для расчета надежности объединим переключатель П и элемент 2 в одну подсистему с последовательным соединением.

Будем рассматривать эту подсистему как параллельно включенный условный элемент (рис.5.6.)

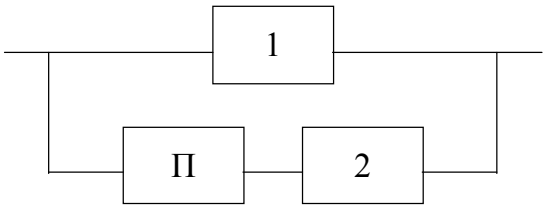

Рис 5.6. Резервированная система с переключателем.

Надежность резервированной системы равна

$$p_s^{(r)} = 1-(1-p)(1-p_o p).$$

Таким образом, неполная надежность переключателя может быть учтена простым умножением надежности резервного элемента на надежность переключателя.

Если у нас 1 основной элемент и k резервных с надежностью p, и каждый из резервных элементов снабжен своим переключателем с надежностью p_o, (рис.5.7.) то надежность каждого резервного элемента умножается на надежность соответствующего переключателя

$$p_s^{(r)} = 1-(1-p)(1-p_o p)^k.$$

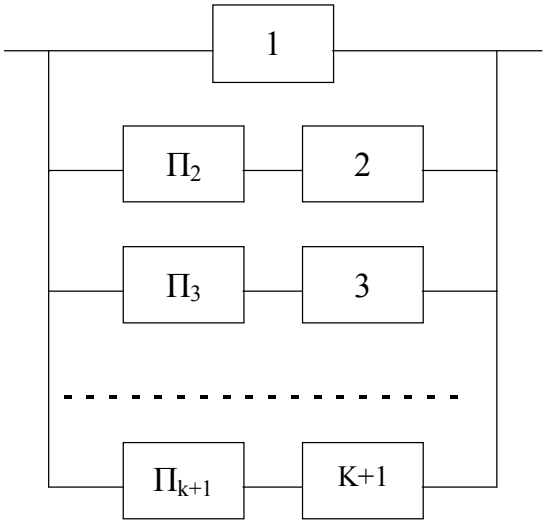

Рис 5.7. Резервированная система с индивидуальными переключателями.

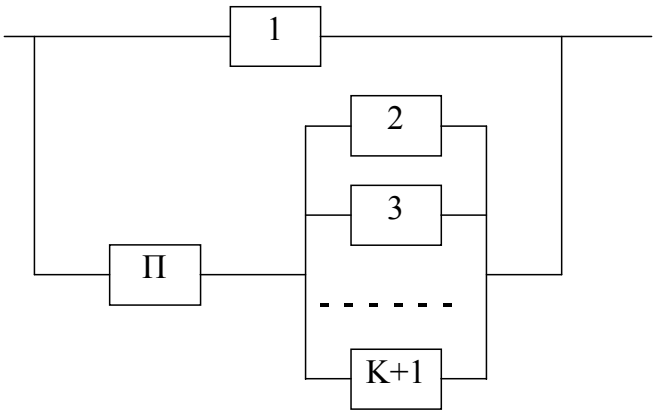

Рис 5.8. Резервированная система с общим переключателем.

Может оказаться, что переключение на любой резервный элемент осуществляется одним и тем же переключателем П (рис.5.8.).
Тогда переключатель П вместе со всем блоком резервных элементов можно рассматривать как один условный резервный элемент с надежностью

$$p_2 = p_o(1-(1-p)^k),$$

а надежность всей системы вычисляется по формуле

$p_s^{(r)} = 1-(1-p)(1-p_2) = 1- q(1-p_o(1-q^k))$, где $q = 1-p$.

Пример 1. Определить надежность системы, состоящей из основного элемента 1 и трех резервных элементов 2, 3, и 4, имеющих одинаковую надежность p=0,9. Переключение на резервные элементы осуществляется с помощью одного и того же переключателя, имеющего надежность p_o = 0,95 (рис.5.9.).

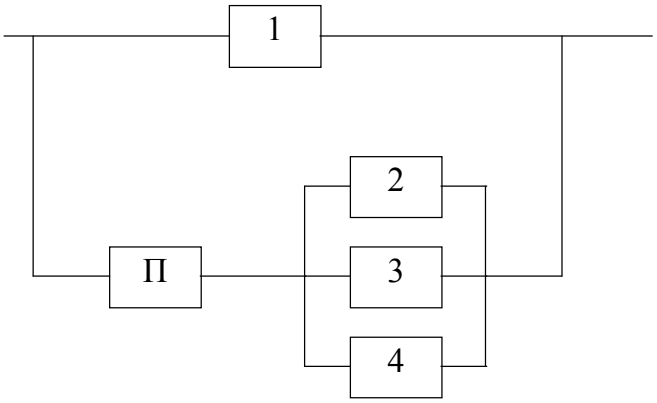

Рис 5.9.

Решение. Объединим переключатель с резервными элементами 2, 3, и 4 в условный элемент с надежностью

$p_2 = p_o(1-(1-p))^3 = 0,95 \bullet (1 - 0,1^3) \approx 0,949.$

Надежность всей системы $p_s^{(r)} = 1 - (1 - 0,9) \bullet (1 - 0,949) = 0,995.$

В данном примере сравнительно низкая надежность переключателя практически обесценивает большое количество резервных элементов.

Большую надежность системы мы получили бы, если бы каждый резервный элемент был снабжен своим переключателем (рис.5.10.)

Пусть у всех переключателей одинаковая надежность p_o = 0,95. Объединяем все резервные элементы и переключатели в один условный элемент с надежностью

$$p_2 = 1 -(1-p_o p)^3 = 1-(1-0,95 \bullet 0,9)^3 \approx 0,997.$$

Надежность всей системы

$$p_s^{(r)} = 1 -(1-p)(1-p_2) = 1 - 0,1 \bullet 0,003 \approx 0,9997.$$

Расчет надежности системы с учетом надежности переключателя становится гораздо более сложным в случае холодного или теплого резерва.

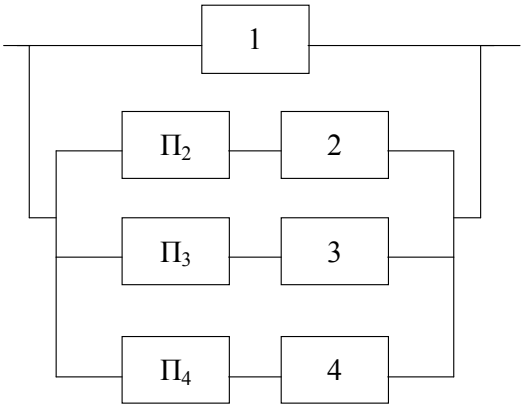

Рис 5.10.

Рассмотрим частный случай холодного резерва кратности 1. Пусть основной элемент и резервный в рабочем состоянии имеют одинаковую постоянную интенсивность отказов λ. Будем считать, что переключатель представляет собой сложный комплекс аппаратуры с постоянной интенсивностью отказов λ_o. Можно показать, что в этом случае надежность резервированной системы составит

$$p_S^{(r)}(t) = e^{-\lambda t}(1 + \frac{\lambda}{\lambda_o}(1 - e^{-\lambda_o t})).$$

Для случая холодного резерва кратности 2 и одного переключателя функция надежности будет равна

$$p_S^{(r)}(t) = e^{-\lambda t} \cdot (1 + \frac{\lambda}{\lambda_o}(1 - e^{-\lambda_o t}) + (\frac{\lambda}{\lambda_o})^2 (1 - (1 + \lambda_o t)e^{-\lambda_o t})).$$

7. МАЖОРИТАРНОЕ РЕЗЕРВИРОВАНИЕ

Пусть функции объекта заключается в том, что он принимает и передает сигнал. Сигнал может быть двух типов: "0" или "1" (отсутствие сигнала или наличие сигнала). Объект должен принять сигнал и передать его дальше. Отказ объекта заключается в том, что он начинает передавать сигнал неправильно. В частности, возможны отказы типа "обрыв", когда на выходе объекта вообще ничего не передается, и отказы типа "короткое замыкание", когда на выходе передается постоянный сигнал.

Мажоритарное резервирование заключается в том, что вместо одного объекта работают n объектов, называемых **передающими элементами**, которые должны передавать один и тот же сигнал. В случае отказа части элементов в сигналах на выходах наступит рассогласование. Тогда в качестве общего выходного сигнала

выбирается сигнал, присутствующий на выходе большинства передающих элементов. Для выбора этого сигнала необходим специальный решающий элемент, называемый **мажоритарным элементом**.

Итак, в системе с мажоритарным резервированием есть n передающих элементов и один мажоритарный элемент. Чтобы мажоритарный элемент мог всегда осуществить выбор сигнала, присутствующего на выходе большинства передающих элементов, число n должно быть нечетным, т.е. n=2k+1.

Систему с мажоритарным резервированием можно рассматривать как последовательное соединение структуры типа к+1 из 2к+1 и мажоритарного элемента. Пусть p - надежность передающего элемента, p_m - надежность мажоритарного элемента, тогда надежность всей резервированной системы определяется по формуле

$$p_s = p_m \sum_{i=k+1}^{2k+1} C^i_{2k+1} p^i (1-p)^{2k+1-i}.$$

В частности, для простейшего случая мажоритарного резервирования, когда n=3, получаем

$$p_s = p_m (C_3^2 p^2 (1-p) + C_3^3 p^3) = p_m (3p^2-2p^3).$$

ТЕМА 6. Надежность восстанавливаемых систем

1. НАДЕЖНОСТЬ ВОССТАНАВЛИВАЕМЫХ СИСТЕМ. ПРОЦЕССЫ ВОССТАНОВЛЕНИЯ

До сих пор, рассматривая задачи надежности, мы исходим из того, что отказавший объект выходит из строя окончательно и никакого восстановления его функций не производится. Предположим теперь, что отказавшие объекты восстанавливаются - заменяются новыми или ремонтируются.

Предположим в этом разделе, что время, требуемого на замену или ремонт отказавшего объекта очень мало по сравнению с промежутками между отказами. Тогда можно считать, что объект восстанавливается **мгновенно.**

Рассмотрим случайные моменты времени, в которые происходят восстановления объекта t_1, t_2, t_3,... Случайные наработки после каждого восстановления $T_1 = t_1$, $T_2 = t_2 - t_1$,..., $T_i = t_{i+1} - t_i$,... являются независимыми и одинаково распределенными случайными величинами.

Последовательность случайных моментов времени t_1, t_2, ... называется **процессом восстановления**. Для задачи надежности представляют интерес следующие характеристики процесса восстановления.

1) За промежуток от 0 до t происходит случайное число восстановлений N_t. Важно знать закон распределения N_t, т.е. вероятности $P\{N_t = k\}$, где к = 0,1,2,... Важно также математическое ожидание $M(N_t)$.

2) Пусть событие $A(t,\Delta t)$ заключается в том, что на промежутке $(t, t+\Delta t)$ происходит восстановление. Величина $u(t) = \lim\limits_{\Delta t \to 0} \dfrac{P\{A(t,\Delta t)\}}{\Delta t}$ называется **плотностью восстановления.**

Можно показать, что плотность восстановления u(t) и частота отказов f(t) (плотность распределения времени между двумя последовательными восстановлениями) связаны интегральным уравнением $u(t) = f(t) + \int\limits_0^t f(x)u(t-x)dx$.

Доказано, что $\lim\limits_{t\to\infty} u(t) = \dfrac{1}{\tau}$, где τ — среднее время между восстановлениями (средняя наработка до отказа).

Рассмотрим важный случай, когда промежутки между восстановлениями имеют показательное распределение с параметром λ. В этом случае процесс восстановления называется **простейшим потоком**. Для простейшего потока распределение числа восстановлений на промежутке (0,t) :

$$P\{N_t = k\} = \frac{\lambda^k t^k}{k!} e^{-\lambda t} \text{ , k = 0, 1, 2, ...}$$

Среднее число восстановлений на промежутке (0, t) равно $M(N_t) = \lambda t$.

Плотность восстановления простейшего потока является константой: $u(t) = \lambda$.

2. ПОКАЗАТЕЛИ НАДЕЖНОСТИ ВОССТАНАВЛИВАЕМОГО ОБЪЕКТА

Будем теперь учитывать время восстановления. Считаем, что время восстановления также является случайной величиной, со своим распределением. Функционирование объекта можно представить как последовательность моментов времени

t_{01}, t_{b1}, t_{02}, t_{b2}, t_{03}, t_{b3} ,...

где t_{01} - момент первого отказа;

t_{b1} - момент первого восстановления;

t_{02} - момент второго отказа;

t_{b2} - момент второго восстановления;

...

При этом случайные величины t_{01}, $t_{02} - t_{b1}$, $t_{03} - t_{b2}$, $t_{04} - t_{b3}$, ... независимы и имеют одно и тоже распределение - распределение наработки до отказа, а случайные величины $t_{b1} - t_{01}$, $t_{b2} - t_{02}$, $t_{b3} - t_{03}$, ... также независимы и имеют одно и то же распределение - распределение времени восстановления.

Показателями надежности восстанавливаемых систем являются:

1) **функция готовности** $К_г(t)$ - вероятность того, что объект работает в момент t;

2) **функция простоя** $К_п(t) = 1 - К_г(t)$ - вероятность того, что объект не работает в момент t;

3) **функция оперативной готовности** $К_{ог}(t_1, t_2)$ - вероятность того, что объект окажется работающим в момент t_1 и проработает без отказа до момента $t_1 + t_2$.

Доказано, что

$$\lim_{t\to\infty} K_Г(t) = K_Г = \frac{\tau}{\tau + \tau_в} \; ; \quad \lim_{t\to\infty} K_П(t) = K_П = \frac{\tau_в}{\tau + \tau_в} \; ,$$

где τ - средняя наработка до отказа (для восстанавливаемых объектов обычно говорят "средняя наработка между отказами");

$\tau_в$ - среднее время восстановления.

Величины $К_г$ и $К_п$ называются соответственно **коэффициентом готовности** и **коэффициентом простоя**.

Обычно $\tau_в$ мало по сравнению с τ , и $K_П \approx \frac{\tau_в}{\tau}$, $K_Г \approx 1 - \frac{\tau_в}{\tau}$.

Значение коэффициента готовности может определить и другим путем. Обозначим через r(t) суммарную наработку объекта за время t. Тогда отношение r(t)/t представляет собой долю рабочего времени объекта в течение промежутка времени t. Предельное значение доли рабочего времени и будет равна коэффициенту готовности $K_Г = \lim_{t\to\infty} \frac{r(t)}{t}$.

Можно показать, что два приведенных выше определения $К_г$ эквивалентны.

3. УРАВНЕНИЯ СОСТОЯНИЙ ВОССТАНАВЛИВАЕМОГО ОБЪЕКТА

Рассмотрим теперь случай, когда наработка между отказами имеет показательное распределение с параметром λ (λ называется интенсивностью отказов), а время восстановления имеет показательное распределение с параметром μ (μ называется интенсивностью восстановления).

В этом случае средняя наработка между отказами и среднее время восстановления равны $\tau = \frac{1}{\lambda}$, $\tau_в = \frac{1}{\mu}$. Коэффициенты готовности и простоя соответственно равны $K_Г = \frac{\mu}{\lambda + \mu}$, $K_П = \frac{\lambda}{\lambda + \mu}$.

Обычно λ мало по сравнению с μ, тогда $K_П \approx \frac{\lambda}{\mu}$, $K_Г \approx 1 - \frac{\lambda}{\mu}$.

Можно определить и предельное значение функции оперативной готовности. Введем события:

$A(t_1)$ - объект работает в момент t_1 ,

$B(t_1 , t_2)$ - на промежутке $(t_1, t_1 + t_2)$ не будет отказов.

Тогда $K_{ОГ}(t_1, t_2) = P\{A(t_1)\} P\{B(t_1, t_2) | A(t_1)\}$.

Но $P\{A(t_1)\} = K_Г(t_1)$; $P\{B(t_1, t_2) | A(t_1)\} = e^{-\lambda t_2}$.

Таким образом, $K_{ОГ}(t_1, t_2) = K_Г(t_1) e^{-\lambda t_2}$.

При $t_1 \to \infty$ функция оперативной готовности переходит в **стационарную функцию оперативной готовности** :

$$K_{ОГ}(t_2) = \lim_{t_1 \to \infty} K_{ОГ}(t_1, t_2) = K_Г e^{-\lambda t_2} = \frac{\mu}{\lambda + \mu} e^{-\lambda t_2} .$$

Восстанавливаемый объект может находиться в двух состояниях: S_0, в котором объект работает, и S_1, в котором объект восстанавливается. Функционирование объекта заключается в последовательности переходов от одного состояния к другому. Интенсивность перехода от S_0 к S_1 равна λ (интенсивности отказов), интенсивность перехода от S_1 к S_0 равна μ (интенсивности восстановления).

Функционирование объекта можно описать графом, изображенном на рис.6.1.

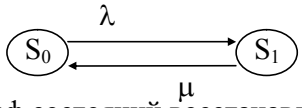

Рис.6.1. Граф состояний восстанавливаемого объекта.

Обозначим через $П_0(t)$ вероятность того, что в момент t объект находится в состоянии S_0 (т.е. работает), через $П_1(t)$ - вероятность того, что в момент t объект находится в состоянии S_1 (т.е. восстанавливается). Таким образом, $П_0(t) = K_г (t)$, $П_1(t) = K_п(t)$. Изменение состояний представляет собой дискретный марковский процесс, а вероятности $П_0(t)$ и $П_1(t)$ описываются системой уравнений :

$$\Pi_0'(t) = -\lambda\Pi_0(t) + \mu\Pi_1(t);$$

$$\Pi_1'(t) = \lambda\Pi_0(t) - \mu\Pi_1(t); \quad (6.1)$$

$$\Pi_0(t) + \Pi_1(t) = 1; \quad (6.2)$$

$$\Pi_0(0) = 1, \Pi_1(0) = 0. \quad (6.3)$$

Дифференциальные уравнения (6.1) называются **уравнениями переходного режима**. Уравнение (6.2) - **уравнением нормировки**, условия (6.3) - **начальными условиями**. Отметим, что уравнение нормировки (6.2) делает лишним одно из дифференциальных уравнений (6.1) (одно из уравнений будет следовать из другого) и одно из начальных условий (6.3). Получаем в результате систему уравнений :

$$\Pi_0'(t) = -\lambda\Pi_0(t) + \mu\Pi_1(t);$$

$$\Pi_0(t) + \Pi_1(t) = 1;$$

$$\Pi_0(0) = 1.$$

Решив эти уравнения, получаем

$$\Pi_0(t) = \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu};$$

$$\Pi_1(t) = \frac{\lambda}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right).$$

Таким образом, получили выражения для функции готовности $K_Г(t) = \Pi_0(t)$ и функции простоя $K_п(t) = \Pi_1(t)$

Теперь можем записать в аналитическом виде и функцию оперативной готовности

$$K_{ОГ}(t_1, t_2) = K_Г(t_1)e^{-\lambda t_2} = \frac{\lambda}{\lambda+\mu} e^{-\lambda(t_1+t_2)-\mu t_1} + \frac{\mu}{\lambda+\mu} e^{-\lambda t_2}.$$

Отметим, что при $t \to \infty$

$$\lim_{t\to\infty} \Pi_0(t) = \Pi_0 = \frac{\mu}{\lambda+\mu}; \quad \lim_{t\to\infty} \Pi_1(t) = \Pi_1 = \frac{\lambda}{\lambda+\mu}$$

Значения Π_0 и Π_1 совпадают с полученными в начале этого раздела значениями $K_Г$ и $K_П$.

Задав некоторую допустимую погрешность, можем считать, что начиная с некоторого момента времени t* вероятности $\Pi_0(t)$, $\Pi_1(t)$ становятся практически равными Π_0, Π_1. Промежуток времени $0 < t < t^*$ называется **переходным режимом** функционирования объекта, при $t > t^*$ говорят о **стационарном режиме** функционирования. Обычно время переходного режима значительно меньше промежутка времени, в течение должен эксплуатироваться объект. Поэтому в основном нас будет интересовать стационарный режим.

Для получения вероятностей Π_0, Π_1 (**стационарного решения**) необязательно решать уравнения (1) - (3). В стационарном режиме $\Pi_0(t) = \Pi_0$, $\Pi_1(t) = \Pi_1$, следовательно, $\Pi_0'(t) = 0$, $\Pi_1'(t) = 0$. Начальные условия (3) для стационарного режима не нужны, а уравнения (1) - (2) переходят в систему линейных уравнений

$0 = -\lambda\Pi_0 + \mu\Pi_1;$

$0 = \lambda\Pi_0 - \mu\Pi_1;$

$\Pi_0 + \Pi_1 = 1.$

Отсюда опять получается то же самое решение $\Pi_0 = \frac{\mu}{\lambda + \mu}$, $\Pi_1 = \frac{\lambda}{\lambda + \mu}$.

4. ГРАФ СОСТОЯНИЙ ВОССТАНАВЛИВАЕМОЙ СИСТЕМЫ

Функционирование восстанавливаемой системы можно представить в виде последовательной смены состояний системы. Обозначим состояния системы через S_0 ,S_1,...S_n . Каждое состояние определяется множеством работоспособных элементов и множеством восстанавливающихся элементов (возможно, что некоторые отказавшие элементы могут в данном состоянии не восстанавливаться).

Пусть S_0,..., S_m - состояния, в которых система работоспособна, при этом S_0 - состояние, в котором все элементы системы работают; S_{m+1}, ... , S_n - состояния отказа системы. Вероятности, что система в момент t находится в одном из этих состояний, обозначим соответственно $\Pi_0(t)$, $\Pi_1(t)$,..., $\Pi_n(t)$.

В качестве показателей надежности системы используются функция готовности $K_Г(t)$ - вероятность того, что система в момент t находится в состоянии готовности:

$$K_Г(t) = \sum_{i=0}^{m} \Pi_i(t),$$

а также функция простоя $K_п$ (t) - вероятность того, что система в момент t находится в состоянии простоя:

$$K_П(t) = 1 - K_Г(t) = \sum_{i=m+1}^{n} \Pi_i(t).$$

При исследовании надежности восстанавливаемых систем будем предполагать, что каждый элемент системы имеет постоянную интенсивность отказов, и время его восстановления распределено по показательному закону. Таким образом, элемент k в системе описывается интенсивностью отказов λ_k и интенсивностью восстановления μ_k .

Если переход из состояния S_i в состояние S_j происходит за счет отказа или восстановления одного из элементов, то введем **интенсивность перехода** из S_i в S_j, равную интенсивности соответствующего отказа или восстановления. Обозначим интенсивность перехода из S_i в S_j, через Λ_{ij} . Если перейти из S_i в S_j в результате отказа или восстановления одного элемента невозможно, то $\Lambda_{ij} = 0$. Возможно, однако, что переход из S_i в S_j может произойти несколькими различными путями (например, при отказе одного из нескольких однотипных элементов). В этом случае Λ_{ij} равна сумме соответствующих интенсивностей отказа или восстановления.

Построим граф состояний системы: вершины графа будут соответствовать состояниям системы; если $\Lambda_{ij} > 0$, то вершины S_i и S_j соединяются дугой, направленной от S_i в S_j. Дуга помечается интенсивностью перехода Λ_{ij}.

Пример 1. Рассмотрим систему из двух последовательно соединенных элементов. У первого элемента интенсивность отказа - λ_1, интенсивность восстановления - μ_1, у второго соответственно λ_2 и μ_2. Во время восстановления одного из элементов система прекращает работу, и второй элемент в это время отказать не может. Состояния системы:

S_0 - оба элемента работают;

S_1 - отказал и восстанавливается первый элемент;

S_2 - отказал и восстанавливается второй элемент.

Граф состояний системы изображен на рисунке 6.2.

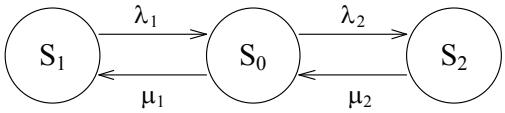

Рис. 6.2.

Здесь S_0 - рабочее состояние, S_1 и S_2 - состояния отказа.

$K_Г(t) = П_0(t)$, $K_П(t) = П_1(t) + П_2(t)$.

***Пример* 2.** Пусть в предыдущем примере элементы соединены параллельно. Тогда при отказе одного из элементов система продолжает работать, и другой элемент может отказать раньше, чем первой восстановится. Считаем, что отказе двух элементов оба будут восстанавливаться одновременно (неограниченное восстановление), и после восстановления хотя бы одного элемента система сразу включается в работу. Добавим к состояниям S_0, S_1 и S_2 состояние S_3 - отказали и восстанавливается оба элемента.

Граф состояний системы изображен на рисунке 6.3. Здесь S_0, S_1, S_2 - рабочие состояния, S_3 - состояние отказа.

$K_Г(t) = П_0(t) + П_1(t) + П_2(t)$, $K_П(t) = П_3(t)$.

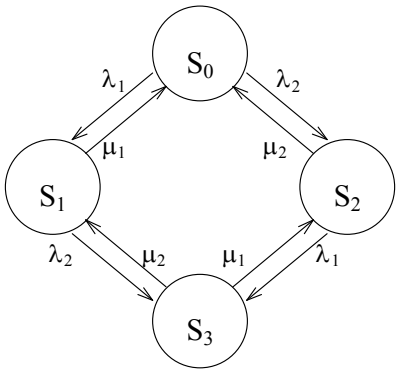

Рис. 6.3.

***Пример* 3.** Рассмотрим систему с параллельным соединением из предыдущего примера. Предположим, что восстанавливающее устройство (или мастер - ремонтник) только одно. Тогда в случае отказа обоих элементов восстанавливаться может только один (который отказал первым), а другой элемент ожидает окончания восстановления первого элемента, и только после этого начинает восстанавливаться (ограниченное восстановление).

Состояния системы:

S_0 - оба элемента работают;

S_1 - первый восстанавливается, второй работает;

S_2 - второй восстанавливается, первый работает;

S_3 - первый восстанавливается, второй ожидает;

S_4 - второй восстанавливается, первый ожидает;

Граф состояний системы изображен на рисунке 6.4.

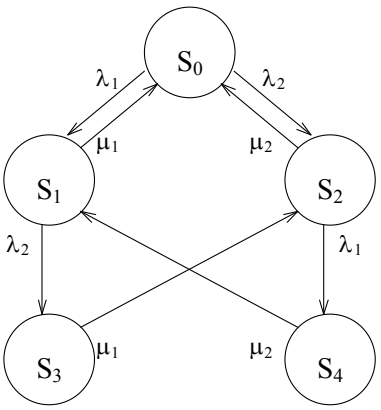

Рис. 6.4.

Здесь S_0, S_1 , S_2 - рабочие состояния, S_3 , S_4 - состояния отказа.

$К_Г(t) = П_0(t) + П_1(t) + П_2(t)$, $К_П(t) = П_3(t) + П_4(t)$.

***Пример* 4**. Предположим, что у обоих элементов системы одинаковые интенсивности отказов и интенсивности восстановлений: $\lambda_1 = \lambda_1 = \lambda$, $\mu_1 = \mu_2 = \mu$. Тогда можно упростить графы состояний.

Для системы с последовательным соединением (пример 1) можно построить граф, изображенный на рисунке 6.5.

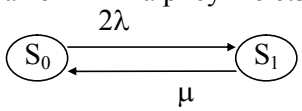

Рис.6.5.

Здесь S_0 - оба элемента работают;

S_1 - один из элементов отказал и восстанавливается.

Тогда $К_Г(t) = П_0(t)$, $К_П(t) = П_1(t)$.

Для системы с параллельным соединением и неограниченным восстановлением (пример 2) можно построить граф, изображенный на рисунке 6.6.

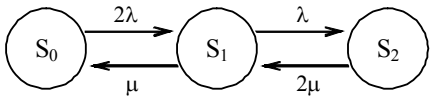

Рис. 6.6.

Здесь S_2 - оба элемента восстанавливаются.

Тогда $К_Г(t) = П_0(t) + П_1(t)$, $К_П(t) = П_2(t)$.

Для системы с параллельным соединением и ограниченным восстановлением (пример 3) граф состояний изображен на рисунке 6.7.

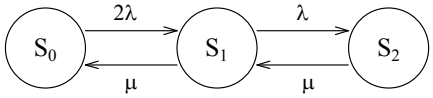

Рис. 6.7.

Здесь S_0 - оба элемента работают;

S_1 - один элемент работает, другой восстанавливается;

S_2 - один элемент восстанавливается, другой ожидает очереди на восстановление.

В этом случае также $К_Г (t) = П_0(t) + П_1(t)$, $К_П(t) = П_2(t)$.

5. УРАВНЕНИЯ СОСТОЯНИЙ ВОССТАНАВЛИВАЕМОЙ СИСТЕМЫ

Пусть для восстанавливаемой системы построен граф состояний с интенсивностями перехода Λ_{ij}. По графу состояний можно построить систему дифференциальных уравнений, для вероятностей состояний $\Pi_i(t)$:

$$\Pi_i'(t) = -\Pi_i(t) \sum_{j \neq i} \Lambda_{ij} + \sum_{j \neq i} \Lambda_{ji} \Pi_j(t), \; i = 0,1,...,n. \qquad (6.4)$$

Уравнения (6.4) называется **уравнениями переходного режима**. Правые части уравнений составляются по следующему правилу: производная $\Pi_i'(t)$ равна взвешенной сумме вероятности $\Pi_i(t)$ и вероятностей $\Pi_j(t)$ всех тех состояний S_j, из которых на графе выходит дуга, входящая в S_i ($\Lambda_{ji} > 0$). При этом весовой множитель для $\Pi_j(t)$, $j \neq i$ равен интенсивности Λ_{ji} перехода из S_j в S_i. Весовой множитель при $\Pi_i(t)$ берется со знаком "-", а по абсолютной величине он равен сумме всех интенсивностей на дугах, выходящих из S_i.

***Пример* 1**. Рассмотрим систему с ограниченным восстановлением, для которой в предыдущем разделе был получен граф состояний (рис. 6.4.).

Запишем для этой системы уравнения переходного режима:

$$\Pi_0'(t) = -(\lambda_1 + \lambda_2)\Pi_0(t) + \mu_1 \Pi_1(t) + \mu_2 \Pi_2(t);$$

$$\Pi_1'(t) = -(\lambda_2 + \mu_1)\Pi_1(t) + \lambda_1 \Pi_0(t) + \mu_2 \Pi_4(t);$$

$$\Pi_2'(t) = -(\lambda_1 + \mu_2)\Pi_2(t) + \lambda_2 \Pi_0(t) + \mu_1 \Pi_3(t);$$

$$\Pi_3'(t) = -\mu_1 \Pi_3(t) + \lambda_2 \Pi_1(t);$$

$$\Pi_4'(t) = -\mu_2 \Pi_4(t) + \lambda_1 \Pi_2(t).$$

Для того, чтобы найти $\Pi_0(t)$, $\Pi_1(t)$,..., $\Pi_n(t)$ к уравнениям (6.4) надо добавить **уравнение нормировки**

$$\Pi_0(t) + \Pi_1(t) + ... + \Pi_n(t) = 1 \qquad (6.5)$$

и **начальное условие**

$$\Pi_0(0) = 1. \qquad (6.6)$$

По уравнениям (6.4), (6.5) и (6.6) можно однозначно определить все функции $\Pi_i(t)$.

Как и у восстанавливаемого объекта, у восстанавливаемой системы тоже есть стационарный режим, при котором вероятности $\Pi_i(t)$ переходят в стационарные значения Π_i. При этом уравнения переходного режима превращаются в **уравнения стационарного режима :**

$$0 = -\Pi_i \sum_{j \neq i} \Lambda_{ij} + \sum_{j \neq i} \Lambda_{ji} \Pi_j, \; i = 0,1,...,n, \qquad (6.7)$$

а уравнение нормировки выглядит так :

$$\Pi_0 + \Pi_1 + ... + \Pi_n = 1 \qquad (6.8)$$

Уравнения (6.7) - (6.8) представляют собой систему линейных уравнений, решая которую, получаем стационарное решение Π_0, Π_1, ..., Π_n .

Отметим, что если просуммировать все уравнения (6.7), то получится тождество 0 = 0. Поэтому при решении уравнений (6.7) - (6.8) одно из уравнений стационарного режима можно исключить (обычно исключают самое громоздкое уравнение).

Функции готовности и простоя для стационарного режима переходят в **коэффициенты готовности** и **простоя**: $K_Г = \sum_{i=0}^{m} \Pi_i$, $K_П = 1 - K_Г = \sum_{i=m+1}^{n} \Pi_i$.

Обычно при расчете надежности восстанавливаемых систем ограничивается анализом стационарного режима. Значения $К_Г$ и $К_П$ выбираются в качестве показателей надежности системы.

Пример 2. Для системы с ограниченным восстановлением из предыдущего примера запишем уравнения стационарного режима:

$$0 = -(\lambda_1 + \lambda_2)\Pi_0 + \mu_1 \Pi_1 + \mu_2 \Pi_2;$$

$$0 = -(\lambda_2 + \mu_1)\Pi_1 + \lambda_1 \Pi_0 + \mu_2 + \Pi_4;$$

$$0 = -(\lambda_1 + \mu_2)\Pi_2 + \lambda_2 \Pi_0 + \mu_1 \Pi_3;$$

$$0 = -\mu_1 \Pi_3 + \lambda_2 \Pi_1;$$

$$0 = -\mu_2 \Pi_4 + \lambda_1 \Pi_2.$$

Уравнение нормировки $\Pi_0 + \Pi_1 + \Pi_2 + \Pi_3 + \Pi_4 = 1$.

Первое уравнение может исключить. Для упрощения расчетов возьмем конкретные значения интенсивностей : $\lambda_1=1$, $\lambda_2=3$; $\mu_1=2$, $\mu_2=5$.

Получаем уравнения:

$$0 = -5\Pi_1 + \Pi_0 + 5\Pi_4;$$

$$0 = -6\Pi_2 + 3\Pi_0 + 2\Pi_3;$$

$$0 = -2\Pi_3 + 3\Pi_1;$$

$$0 = -5\Pi_4 + \Pi_2;$$

$$\Pi_0 + \Pi_1 + \Pi_2 + \Pi_3 + \Pi_4 = 1.$$

Решая эту систему, получим

$\Pi_0 = 0{,}38$; $\Pi_1 = 0{,}13$; $\Pi_2 = 0{,}25$; $\Pi_3 = 0{,}19$; $\Pi_4 = 0{,}05$.

Следовательно, показатели надежности

$К_Г = \Pi_0 + \Pi_1 + \Pi_2 = 0{,}76$; $К_П = \Pi_3 + \Pi_4 = 0{,}24$.

6. ВОССТАНАВЛИВАЕМАЯ СИСТЕМА С ПОСЛЕДОВАТЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Рассмотрим систему из n последовательно соединенных элементов. Пусть элемент с номером i отказывает с интенсивностью λ_i и восстанавливается с интенсивностью μ_i . При восстановлении элемента система останавливается, и отказов других элементов в это время не происходит.

Введем состояния системы :

S_0 - все элементы работают;

S_1 - отказал элемент 1;

. . . . . .

. S_n - отказал элемент n.

Граф состояний системы изображен на рисунке 6.8.

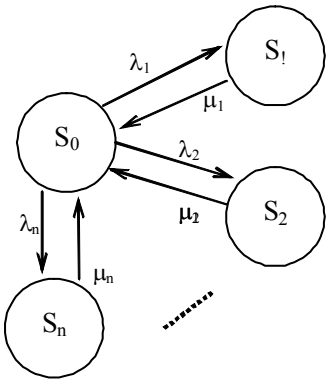

Рис 6.8. Граф состояний восстанавливаемой системы с последовательным соединением элементов.

Выпишем уравнения стационарного режима вместе с условием нормировки:

$$0 = -\Pi_0\left(\lambda_1 + \lambda_2 + \ldots + \lambda_n\right) + \mu_1 \Pi_1 + \mu_2 \Pi_2 + \ldots + \mu_n \Pi_n \ ;$$

$$0 = -\mu_1 \Pi_1 + \lambda_1 \Pi_0 \ ;$$

$$0 = -\mu_2 \Pi_2 + \lambda_2 \Pi_0 \ ;$$

. . . . . .

$$0 = -\mu_n \Pi_n + \lambda_n \Pi_0 \ ;$$

$$\Pi_0 + \Pi_1 + \Pi_2 + \ldots + \Pi_n = 1.$$

Первое уравнение, как самое громоздкое, отбрасываем. Из остальных уравнений получаем

$$\Pi_1 = \frac{\lambda_1}{\mu_1}\Pi_0 \ ;$$

$$\Pi_2 = \frac{\lambda_2}{\mu_2}\Pi_0 \ ;$$

. . . . . .

$$\Pi_n = \frac{\lambda_n}{\mu_n}\Pi_0 ;$$

$$\Pi_0\left(1 + \frac{\lambda_1}{\mu_1} + \ldots + \frac{\lambda_n}{\mu_n}\right) = 1.$$

Откуда

$$\Pi_0 = \frac{1}{1 + \sum\limits_{i=1}^{n} \lambda_i / \mu_i},$$

$$\Pi_k = \frac{\lambda_k / \mu_k}{1 + \sum\limits_{i=1}^{n} \lambda_i / \mu_i}, \; k = 1,2,\ldots,n.$$

Так как система работоспособна только в состоянии S_0, то

$K_Г = \Pi_0$,

$$K_П = 1 - \Pi_0 = \frac{\sum\limits_{i=1}^{n} \lambda_i / \mu_i}{1 + \sum\limits_{i+1}^{n} \lambda_i / \mu_i}.$$

Обычно восстановление происходит гораздо быстрее, чем отказ, т.е. λ_i намного меньше μ_i . Тогда для расчета коэффициентов готовности и простоя можно воспользоваться приближенными формулами

$$K_П \approx \sum_{i=1}^{n} \lambda_i / \mu_i \; ; \; K_Г = 1 - K_П \approx 1 - \sum_{i=1}^{n} \lambda_i / \mu_i .$$

7. ВОССТАНАВЛИВАЕМАЯ СИСТЕМА С ПАРАЛЛЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Пусть имеется система из n параллельно соединенных элементов. Будем считать, что все элементы имеют одинаковую надежность с постоянной интенсивностью λ, а время восстановления каждого элемента имеет показательное распределение с интенсивностью μ .

Предположим сперва, что при нескольких отказавших элементах восстановление производится по очереди (т.е. в любой момент времени восстанавливается не более одного элемента). Такое восстановление называется **полностью ограниченным**.

Определим состояния системы:

S_0 - отказавших элементов нет;

S_1 - отказал один элемент;

S_2 - отказали два элемента;

.....

S_n - отказали все элементы.

Граф состояний системы изображен на рисунке 6.9.

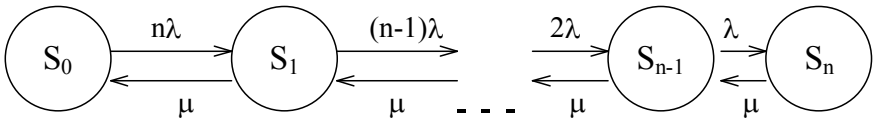

Рис.6.9. Граф состояний системы с параллельным соединением и полностью ограниченным восстановлением.

Предположим теперь, что среди n элементов системы k параллельно соединенных элементов являются основными, а остальные l = n-k - резервными. При этом любой резервный элемент может замещать любой из отказавших основных, и после восстановления любой из элементов становится либо на место основного, если к этому моменту в системе работают менее k элементов, либо становится в резерв.

Если резерв горячий, граф состояний не меняется.

При холодном резерве получаем граф, показанный на рис. 6.10.

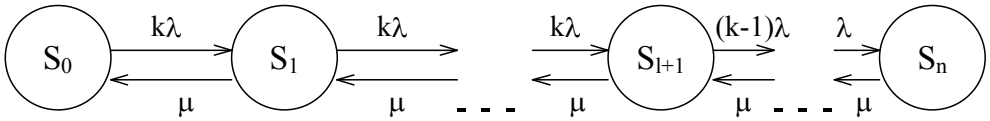

Рис. 6.10. Граф состояний системы с параллельным соединением, холодным резервом и полностью ограниченным восстановлением.

В случае теплого резерва получаем граф, изображенный на рисунке 6.11.

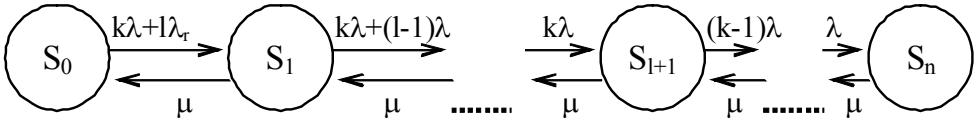

Рис 6.11. Граф состояний системы с параллельным соединением, теплым резервом и полностью ограниченным восстановлением.

Все эти графы состояний можно записать в общем виде (рис.6.12.)

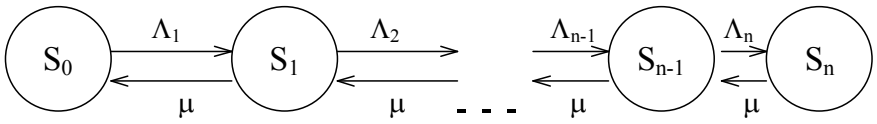

Рис. 6.12. Общий вид графа состояний системы с параллельным соединением и полностью ограниченным восстановлением.

Все рассмотренные выше системы относились к случаю полностью ограниченного восстановления. Рассмотрим теперь случай, когда все отказавшие элементы сразу начинают восстанавливаться. Такое восстановление называется **неограниченным.** Для неограниченного восстановления получаем граф состояний, изображенный на рисунке 6.13.

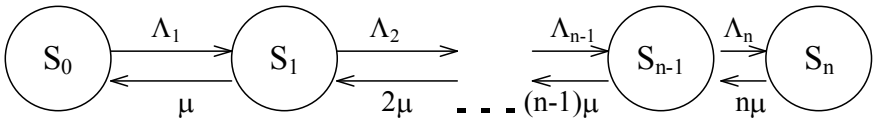

Рис. 6.13. Граф состояний системы с параллельным соединением и неограниченным восстановлением.

Возможен также случай, когда одновременно могут восстанавливаться не более r элементов (например, если есть всего r ремонтных мест). Такое восстановление называется **частично ограниченным**.

Для случая частично ограниченного восстановления получаем граф состояний, изображенный на рисунке 6.14.

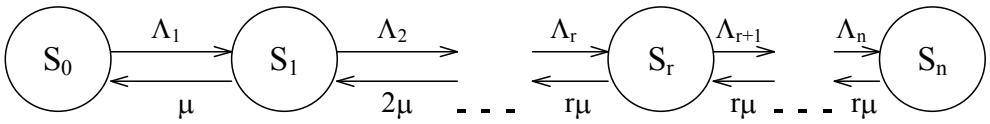

Рис. 6.14. Граф состояний системы с параллельным соединением и частично ограниченным восстановлением.

Таким образом, для любого вида резервирования и любого вида восстановления граф состояний системы с параллельным соединением имеет вид, как на рисунке 6.15.

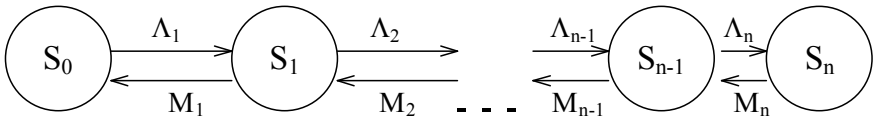

Рис. 6.15. Общий вид графа состояний восстанавливаемой системы с параллельным соединением.

Рассчитаем стационарные вероятности системы. Получаем систему уравнений

$$0 = -\Lambda_1 \Pi_0 + M_1 \Pi_1;$$
$$0 = -(\Lambda_2 + M_1)\Pi_1 + \Lambda_1 \Pi_0 + M_2 \Pi_2;$$
. . . . . .
$$0 = -M_n \Pi_n + \Lambda_n \Pi_{n-1};$$
$$\Pi_0 + \Pi_1 + \ldots + \Pi_n = 1.$$

Из первого уравнения получаем $\Pi_1 = \frac{\Lambda_1}{M_1}\Pi_0.$

Подставив это значение во второе уравнение, получим $\Pi_2 = \frac{\Lambda_1 \Lambda_2}{M_1 M_2}\Pi_0.$

И далее, вычисляя последовательно Π_3, Π_4 ,....., получаем

$$\Pi_k = \frac{\Lambda_1 \cdot \Lambda_2 \cdot \ldots \cdot \Lambda_k}{M_1 \cdot M_2 \cdot \ldots M_k}\Pi_0 \quad , \; k = 3,4,\ldots,n.$$

Введем для простоты обозначений константы

$$\gamma_0 = 1 \; ; \; \gamma_k = \gamma_{k-1}\frac{\Lambda_k}{M_k} = \prod_{i=1}^{k}\frac{\Lambda_i}{M_i} \; , \; k = 1,2,\ldots,n.$$

Тогда $\Pi_k = \gamma_k \Pi_0, \quad k = 1,2,\ldots,n.$

В силу уравнения нормировки

$$\Pi_0 = \frac{1}{1+\gamma_1+\ldots+\gamma_n}, \Pi_i = \frac{\gamma_i}{1+\gamma_1+\ldots+\gamma_n}, \quad i = 1,2,\ldots,n.$$

Так как работоспособными являются все состояния системы, кроме S_n , то $K_Г = \frac{1+\gamma_1+\ldots+\gamma_{n-1}}{1+\gamma_1+\ldots+\gamma_n}$; $K_П = \frac{\gamma_n}{1+\gamma_1+\ldots+\gamma_n}$.

8. СРЕДНЯЯ НАРАБОТКА ДО ПЕРВОГО ОТКАЗА ВОССТАНАВЛИВАЕМОЙ СИСТЕМЫ

Во многих задачах надежности важным показателем является средняя наработка до первого отказа системы. Этот показатель особенно важен для систем, у которых восстановление отдельных элементов возможно только при условии одновременной работы системы (например, для системы обеспечения жизнедеятельности). Такие системы уже не восстановимы после отказа.

Обозначим среднюю наработку до первого отказа через τ_1 .

Пример 1. Рассмотрим восстанавливаемый объект с графом состояний, изображенным на рисунке 6.1. Средняя наработка до первого отказа равна среднему времени до первого наступления состояния S_1. Очевидно, $\tau_1 = 1/\lambda$.

Пример 2. Рассмотрим восстанавливаемую систему с последовательным соединением. Граф состояний такой системы изображен на рисунке 6.8. Среднее время до первого отказа - это среднее время до выхода системы из состояния S_0 . Очевидно, $\tau_1 = \frac{1}{\lambda_1 + \lambda_2 + \ldots + \lambda_n}$.

Пример 3. Рассмотрим систему из двух параллельно соединенных элементов с одинаковой интенсивностью отказов и интенсивностью восстановлений. Пусть восстановление в системе является неограниченным. Граф состояний системы изображен на рисунке 6.16.

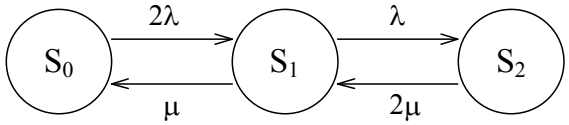

Рис. 6.16.

Система отказывает в состоянии S_2, следовательно, τ_1 равна среднему времени до первого попадания системы в состояние S_2 .
Преобразуем эту систему. Пусть после отказа система уже не восстанавливается, т.е. попав в состояние S_2, система уже из этого состояния не выходит. В этом случае состояния S_2 называется **поглощающим**. Тогда получаем новую систему с графом состояний, изображенным на рисунке 6.17. Здесь S_0 ,S_1 - работоспособные состояния, S_2 - состояние отказа.

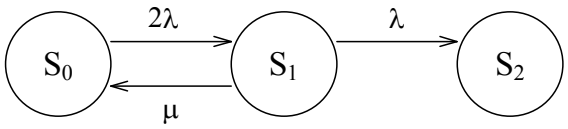

Рис. 6.17.

Тогда средняя наработка до первого отказа τ_1 в исходной системе будут равна средней наработке до отказа новой системы.

Рассмотрим теперь метод расчета средней наработки до первого отказа для произвольной восстанавливаемой системы. Обозначим состояния системы через S_0 ,S_1 ,...S_n . Пусть в состояниях S_0,S_1,...S_m система работает (при этом через S_0 обозначим состояние, в котором работают все элементы системы), S_{m+1},...,S_n - состояния отказа системы.

Построим граф состояний системы с интенсивностями переходов Λ_{ij} и запишем уравнения переходного режима. Для упрощения записи формул введем величины $\Lambda_{ii} = 0$, i = 0,1,..., n:

$$\Pi_i'(t) = -\sum_{j=0}^{n} \Lambda_{ij}\,\Pi_i(t) + \sum_{j=0}^{n} \Lambda_{ji}\,\Pi_j(t), \quad i = 0,1,\ldots,n.$$

Сделаем все состояния отказа системы S_{m+1} ,...,S_n поглощающими, т.е. положим все $\Lambda_{ij} = 0$, если i>m, а в графе сотрем все стрелки, выходящие из вершин S_{m+1} ,...,S_n . Для новой системы уравнения переходного режима будут следующими:

$$\Pi_i'(t) = -\sum_{j=0}^{n} \Lambda_{ij} \Pi_i(t) + \sum_{j=0}^{m} \Lambda_{ji} \Pi_j(t) \text{ , } i = 0,1,...,m;$$

$$\Pi_i'(t) = -\sum_{j=0}^{m} \Lambda_{ji} \Pi_j(t) \text{ , } i = m+1, \text{ ... , } n.$$

К этим уравнениям добавим уравнение нормировки :

$\Pi_0(t) + \Pi_1(t) + ... + \Pi_n(t) = 1$,

и начальные условия:

$\Pi_0(0) = 1$, $\Pi_i(0) = 0$, $i = 1,2,\ldots,n$.

Решая эти уравнения, можно однозначно определить все $\Pi_i(t)$. Отметим, что система обязательно когда-нибудь попадет в одно из поглощающих состояний S_{m+1} ,...,S_n . Это означает что для всех i = 0, 1, ... , m

$$\Pi_i(\infty) = \lim_{t \to \infty} \Pi_i(t) = 0.$$

Средняя наработка до первого отказа исходной системы τ_1 совпадает со средней наработкой до отказа новой системы с поглощающими состояниями, значит,

$$\tau_1 = \int_0^{\infty} \rho_S(t) dt \text{ ,}$$

где $\rho_S(t)$ - функция надежности новой системы, т.е. вероятность того, что в момент t новая система находится в одном из своих работоспособных состояний. Таким образом,

$\rho_S(t) = \Pi_0(t) + \Pi_1(t) + ... + \Pi_m(t)$.

Итак, получаем

$$\tau_1 = \sum_{i=0}^{m} \int_0^{\infty} \Pi_i(t) dt \text{ .}$$

Для того, чтобы найти τ_1 , нет необходимости решать систему дифференциальных уравнений и находить все функции $\Pi_i(t)$. Вместо этого возьмем уравнения переходного режима для работоспособных состояний:

$$\Pi_i'(t) = -\sum_{j=0}^{n} \Lambda_{ij} \Pi_i(t) + \sum_{j=0}^{m} \Lambda_{ji} \Pi_j(t) \text{ , } i = 0,1,\ldots, m.$$

Проинтегрируем эти уравнения по t от 0 до ∞:

$$\int_0^{\infty} \Pi_i'(t) dt = -\sum_{j=0}^{n} \Lambda_{ij} \int_0^{\infty} \Pi_i(t) dt + \sum_{j=0}^{m} \Lambda_{ji} \int_0^{\infty} \Pi_j(t) dt \text{ , } i = 0,1,...,m \text{ .}$$

Обозначим $u_i = \int_0^{\infty} \Pi_i(t) dt$, $i = 0,1,\ldots, m$.

Так как $\int_0^{\infty} \Pi_i'(t) dt = \Pi_i(\infty) - \Pi_i(0) = \begin{cases} -1 \text{ , если } i = 0, \\ 0 \text{ , если } i = 1,2,\ldots,m, \end{cases}$

то получаем систему линейных уравнений

$$-1 = -u_0 \sum_{j=0}^{n} \Lambda_{0j} + \sum_{j=0}^{m} \Lambda_{j0} u_j ;$$

$$0 = -u_i \sum_{j=0}^{n} \Lambda_{ij} + \sum_{j=0}^{m} \Lambda_{ji} u_j , \ i = 1,2,\ldots, \ m.$$

Из этой системы находим значения u_i и определяем среднюю наработку исходной системы до первого отказа

$\tau_1 = u_0 + u_1 + \ldots + u_m$.

Пример 4. Рассмотрим снова систему из примера 3. Сделав состояние отказа поглощающим, мы получили граф, изображенный на рисунке 6.17.

Запишем уравнения переходного режима для работоспособных состояний

$$\Pi_0'(t) = -2\lambda \Pi_0(t) + \mu \Pi_1(t);$$

$$\Pi_1'(t) = -(\lambda + \mu) \Pi_1(t) + 2\lambda \Pi_0(t).$$

Отсюда получаем систему линейных уравнений

$-1 = -2\lambda u_0 + \mu u_1;$

$0 = -(\lambda + \mu)u_1 + 2\lambda u_0 .$

Решив эту систему, получаем $u_0 = \dfrac{\lambda + \mu}{2\lambda^2}$, $u_1 = \dfrac{1}{\lambda}$.

Следовательно, $\tau_1 = u_0 + u_1 = \dfrac{3\lambda + \mu}{2\lambda^2}$.

ТЕМА 7. Надежность программного обеспечения (ПО)

1. НАДЕЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ПРОГРАММНЫЕ ОТКАЗЫ

Нет единого определения понятия "программный отказ". Наиболее общим является следующее определение: программный отказ возникает, когда программа работает не так, как предполагает пользователь.

При разработке программного обеспечения (ПО) может возникнуть ряд причин, приводящих к возникновению отказов: неправильное понимание программистом алгоритма, неправильное составление общей структуры ПО и взаимосвязи программ, неправильный выбор методов защиты программ и т.д.

Отладка ПО не может устранить все ошибки, так как число возможных комбинаций входных данных настолько велико, что заранее проверить все возможные ветви исполнения программы практически невозможно. Поэтому моменты появления отказов ПО носят случайный характер: отказы проявляются в случайные моменты времени, когда программа выйдет на участок, содержащий ошибку.

Общая черта между программными и аппаратурными отказами состоит в том, что моменты отказов и время восстановления после отказа носят случайный характер. Однако есть и существенные различия:

1) элементы ПО не имеют периодов приработки или старения. Вероятность программного отказа зависит не от времени или объема выполненной работы, а от выхода программы на участок, содержащий ошибку;

2) устранение аппаратурного отказа не гарантирует, что такой же отказ не повторится в дальнейшем, а устранение программного отказа гарантирует, что этот отказ уже в дальнейшем не произойдет;

3) аппаратурные отказы подразделяют на внезапные и постепенные. Программные отказы могут быть только внезапными.

Существуют два подхода к выбору показателей надежности ПО. С одной стороны, возможно использовать обычные показатели надежности: вероятность отсутствия отказов за время t, среднее время между отказами и т.п. Такие показатели целесообразно использовать для непрерывно применяемого ПО (например, операционных систем). Для ПО, используемого периодически, возможно применение таких показателей, как вероятность успешного выполнения одного прогона программы.

С другой стороны, для описания надежности ПО могут быть использованы специальные показатели, характерные только для ПО, например показатель корректности ПО: предполагаемое число ошибок в ПО. Есть и другие показатели, характеризующие такие свойства ПО как способность функционировать в условиях возмущенной внешней среды, способность к внесению исправлений, защищенность от внесения искажений при постороннем вмешательстве.

2. МОДЕЛИ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Основным средством определения количественных показателей надежности ПО являются модели надежности, под которыми понимают математические модели построенные для оценки зависимости надежности от заранее известных или оцененных в ходе создания ПО параметров.

Рассмотрим классификацию моделей надежности ПО (МНПО) (рис.7.1.)

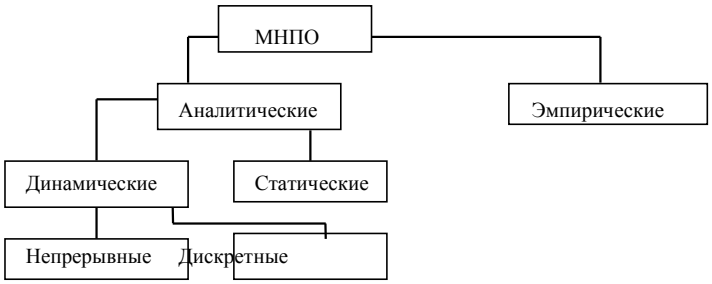

Рис.7.1. Классификация моделей надежности ПО.

МНПО подразделяются на аналитические и эмпирические. Аналитические модели дают возможность рассчитать количественные показатели надежности, основываясь на данных о поведении программы в процессе тестирования. Эмпирические - основаны на анализе структурных особенностей ПО и рассматривают зависимость показателей надежности от числа межмодульных связей, количество циклов в модулях, отношения числа прямолинейных участков программы к числу точек ветвления и т.д. Эти модели можно использовать на этапе проектирования ПО, когда осуществлена разбивка на модули и известна структура ПО.

Аналитические модели делятся на две группы: динамические модели и статические. В динамических моделях появление отказов рассматривается во времени. В статических моделях не анализируют время появления отказов, а рассматривают зависимость количества оставшихся ошибок от числа тестовых прогонов или зависимость вероятности отказов от характеристики входных данных.

Для использования динамических моделей необходимо иметь данные о появлении отказов во времени. Если фиксируются моменты каждого отказа, то получим непрерывную картину появления отказов во времени (группа непрерывных динамических моделей). С другой стороны, может фиксироваться только число отказов за произвольный интервал времени. В этом случае поведение ПО может быть представлено только в дискретных точках (группа дискретных динамических моделей).

3. НЕПРЕРЫВНЫЕ ДИНАМИЧЕСКИЕ МОДЕЛИ

Пусть функционирование ПО описывается графом состояний, изображенным на рисунке 7.2. Здесь S_i — состояние системы, когда произошел i-й по счету отказ, λ_i — интенсивность наступления следующего ((i+1)-го по счету) отказа. После каждого отказа тратится какое-то время на поиск и исправление ошибок, приведших к отказу. Однако это время гораздо меньше промежутка между отказами, и мы в моделях надежности не будем его учитывать.

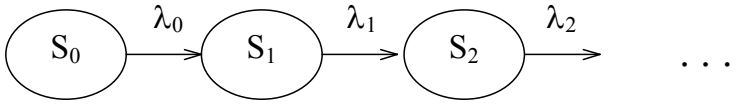

Рис.7.2. Граф состояний функционирования ПО.

Можно задать какую-либо зависимость интенсивности наступления следующего отказа от числа уже наступивших отказов, например, $\lambda_i = \lambda_0 r^i$, где $r < 1$. Значение λ_0 и r можно оценить статистически по данным о моментах отказов.

МОДЕЛЬ ЛИТТЛВУДА-ВЕРРАЛЛА. Чем меньше λ_i, тем надежнее программа. Программист стремится сделать программу более надежной, чем она была до наступления отказа, т.е. добиться соотношения $\lambda_{i+1} < \lambda_i$. Однако нельзя быть уверенным, что после исправления ошибки, вызвавшей отказ, программа действительно стала лучше — возможно, что при исправлении программы вводится новый источник ошибок.

Рассмотрим интенсивность λ_i как случайную величину с функцией распределения $F_i(\lambda)$. Стремление программиста после исправления ошибок повысить надежность программы запишем следующим образом: $F_i(\lambda) < F_{i+1}(\lambda)$ для всех i и λ.

Обычно при изучении этой модели считают, что случайные величины λ_i имеют плотности вероятностей

$$f_i(\lambda) = \begin{cases} \psi^a(i)\lambda^{a-1}e^{-\psi(i)\lambda}, & \text{если } \lambda > 0; \\ 0, & \text{если } \lambda \le 0; \end{cases}$$

где $\lambda > 0$ - параметр распределения;

$\psi(i)$ — некоторая монотонно возрастающая функция от i.

Часто функцию $\psi(i)$ выбирают в виде $\psi_i = \exp(\beta_0 + \beta_1 i)$, где β_0, β_1 — параметры модели.

Модель Литтлвуда-Веррала хорошо объясняет процессы, происходящие при отладке ПО. Но для практических расчетов и прогнозов надежности предложены более простые модели.

МОДЕЛЬ ДЖЕЛИНСКОГО-МОРАНДЫ. Модель основана на допущении, что интенсивность отказов программы пропорциональна количеству оставшихся в программе ошибок, а после каждого отказа одна ошибка исправляется.

Пусть N - первоначальное число ошибок ПО, тогда $\lambda_1 = CN$, $\lambda_2 = C(N-1),\ldots, \lambda_N = C$, $\lambda_{N+1} = \lambda_{N+2} = \ldots = 0$, где C - коэффициент пропорциональности.

Наиболее вероятные значения N и C можно определить на основе данных, полученных при тестировании. Для этого фиксируется время выполнения программы до очередного отказа $t_1, t_2, \ldots, t_k$.

Плотность вероятности времени t_i равна

$$f_i(t_i) = \lambda_i e^{-\lambda_i t_i} = C(N-i+1)e^{-C(N-i+1)t_i}.$$

Составим функцию правдоподобия

$$L = \prod_{i=1}^{k} f_i(t_i) = \prod_{i=1}^{k} C(N-i+1)e^{-C(N-i+1)t_i} \longrightarrow \max.$$

Прологарифмируем

$$\ln L = \sum_{i=1}^{k} (\ln C + \ln(N - i + 1) - C(N - i + 1)t_i) \longrightarrow \max .$$

Максимум функции ln L достигается при значениях, для которых

$$\frac{\partial(\ln L)}{\partial C} = 0; \ \frac{\partial(\ln L)}{\partial N} = 0 .$$

Получаем

$$\begin{cases} \frac{\partial(\ln\ \mathrm{L})}{\partial C} = \sum_{i=1}^{k} (\frac{1}{C} - (N - i + 1)t_i) = 0; \\ \frac{\partial(\ln\ \mathrm{L})}{\partial N} = \sum_{i=1}^{k} (\frac{1}{N - i + 1} - Ct_i) = 0. \end{cases}$$

Выразим C из каждого выражения.

$$\begin{cases} C = \frac{k}{\sum_{i=1}^{k} (N - i + 1)\, t_i}; \\ C = \frac{\sum_{i=1}^{k} \frac{1}{N - i + 1}}{\sum_{i=1}^{k} t_i}. \end{cases}$$

Отсюда получаем уравнение для определения N:

$$\frac{k}{\sum_{i=1}^{k} (N - i + 1)t_i} = \frac{\sum_{i=1}^{k} \frac{1}{N - i + 1}}{\sum_{i=1}^{k} t_i}.$$

Решая численно это уравнение, можно найти значение N, а затем и значение C.

Недостаток этой модели в том, что при неточном определении величины N интенсивность отказов программы может стать отрицательной, что приводит к бессмысленному результату. Кроме того, предполагается, что при исправлении

обнаруженных ошибок не вносятся новые ошибки, что тоже не всегда выполняется.

МОДЕЛЬ ОСОБЫХ СИТУАЦИЙ. В этой модели предполагается, что в ходе работе ПО возникает особые ситуации, в которых может произойти отказ ПО (а может и не произойти). Например, такие ситуации могут возникать в случае поступления входных данных из некоторой специфической области. Время между наступлениями особых ситуаций считается случайным, имеющим показательное распределение с плотностью $f(t) = \lambda e^{-\lambda t}$. При наступлении особой ситуации с некоторой вероятностью может произойти отказ ПО. Однако по мере обнаружения и исправления ошибок вероятность отказа в каждой следующей особой ситуации уменьшается. В простейшем варианте модели принято $p_i = 1 - (1 - p_1)r^{i-1}$, где p_i - вероятность безотказной работы ПО в i-й по счету особой ситуации, $i = 1,2,...$, r - параметр модели, $0 < r < 1$. Неизвестные параметры λ, p_1 , r определяются по данным о моментах отказов.

МОДЕЛЬ ПЕРЕХОДНЫХ ВЕРОЯТНОСТЕЙ. В этой модели учитывается также и время на поиск и исправление ошибки после очередного программного отказа.

Предполагается, что время на поиск и исправление очередной ошибки имеет показательное распределение с параметром μ. Однако интенсивность μ может изменяться в зависимости от предыдущих выявленных ошибок (обычно каждую следующую ошибку искать труднее, поэтому μ уменьшается после каждой исправленной ошибки). Процесс возникновения отказов и исправления ошибок описывается графом состояний, изображенном на рисунке 7.3.

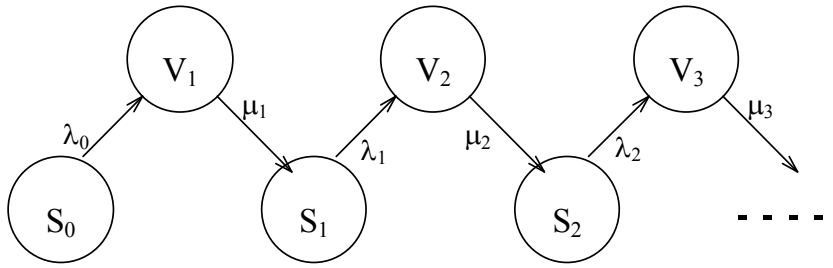

Рис. 7.3. Граф состояний модели переходных вероятностей.

Здесь V_i - состояние, когда произошел i-й по счету отказ ПО и ищется ошибка, вызвавшая этот отказ;

S_i - состояние, когда ошибка, вызвавшая i-й отказ обнаружена исправлена, а следующий отказ еще не наступил.

Обозначим через $\Pi_{Si}(t)$ вероятность того, что ПО в момент t будет находится в состоянии S_i , через $\Pi_{Vi}(t)$ - вероятность того, что ПО будет находится в состоянии V_i.

Тогда эти вероятности описываются бесконечной системой уравнений

$$\Pi'_{S0}(t) = -\lambda_0 \Pi_{S0}(t)\ ;$$

$$\Pi'_{Si}(t) = -\lambda_i \Pi_{Si}(t) + \mu_i \Pi_{Vi}(t)\ ;$$

$$\Pi'_{Vi}(t) = -\mu_i \Pi_{Vi}(t) + \lambda_{i-1} \Pi_{Si-1}(t); \qquad i = 1, 2, \ldots$$

$$\Pi_{S0}(t) + \sum_{i=1}^{\infty} (\Pi_{Si}(t) + \Pi_{Vi}(t)) = 1\ .$$

Начальные условия: $\Pi_{S0}(0) = 1$, $\Pi_{Si}(0) = \Pi_{Vi}(0) = 0$, i = 1,2,...

Значение параметров λ_i и μ_i выбираются на основе предыдущего опыта разработчика ПО.

4. ДИСКРЕТНЫЕ МОДЕЛИ НАДЕЖНОСТИ ПО

В дискретных моделях предполагается, что сначала проводится тестирование ПО (возможно, в несколько этапов). В случае появления отказов ищутся и исправляются все ошибки, из-за которых произошли отказы. После этого начинается период эксплуатации ПО.

МОДЕЛЬ МУСА. В этой модели надежность ПО на этапе эксплуатации оценивается по результатам тестирования.

Пусть T - суммарное время тестирования, M - число отказов, произошедших за время тестирования.

Тогда по модели Муса средняя наработка до отказа после тестирования определяется по формуле

$$\tau = \tau_0 \exp\left(\frac{CT}{M\tau_0}\right),$$

где τ_0 - средняя наработка до отказа до начала тестирования,

C - коэффициент, учитывающий уплотнение тестового времени по сравнению с временем реальной эксплуатации. Например, если один час тестирования соответствует 12 ч работы в реальных условиях, то C=12.

Неизвестный параметр τ_0 можно оценить из следующего соотношения:

$$\tau_0 = \frac{1}{fKN},$$

где N - первоначальное число ошибок в ПО. Его можно оценить с помощью другой модели, позволяющей определить N на основе статистических данных, полученных при тестировании (например, с помощью рассмотренной ниже модели Шумана);

K - коэффициент проявления ошибок. Значение K определяется эмпирическим путем по однотипным программам. Обычно это значение изменяется от $1{,}5*10^{-7}$ до $4*10^{-7}$;

f - средняя скорость исполнения ПО, деленная на число команд (операторов).

Надежность ПО для периода эксплуатации t определяются по формуле

$$p(t) = e^{-\frac{t}{\tau}}.$$

Пусть в договоре с заказчиком определена требуемая величина средней наработки на отказ τ_d, а рассчитанное по результатам тестирования значение τ меньше требуемого τ_d. Тогда необходимо провести еще тестирование в течении некоторого времени ΔT. Дополнительное время тестирования ΔT рассчитывается в предположении, что за дополнительное время новых отказов ПО не возникает. Тогда общее время тестирования $T + \Delta T$ должен удовлетворять соотношению

$$\tau_d = \tau_0 \exp\left(\frac{C(T+\Delta T)}{M\tau_0}\right).$$

Отсюда легко получить $\Delta T = \frac{M\tau_0}{C}\ln\left(\frac{\tau_d}{\tau}\right)$.

МОДЕЛЬ ШУМАНА. В этой модели предполагается, что тестирование проводится в несколько этапов. Каждый этап представляет собой выполнение программы на наборе тестовых данных. Выявленные в течение этапа тестирования ошибки регистрируются, но не исправляются. По завершении этапа исправляются все обнаруженные на этом этапе ошибки, корректируются тестовые наборы и проводится новый этап тестирования.

Предполагается, что при корректировке новые ошибки не вносятся, и что интенсивность обнаружения ошибок пропорциональна числу оставшихся ошибок (как в модели Джелинского-Моранды).

Пусть всего проводятся k этапов тестирования. Обозначим продолжительность каждого этапа через $t_1, ...t_k$, а число ошибок, обнаруженных на каждом этапе, через $m_1, ...m_k$.

Пусть $n = m_1 + ... + m_k$ — общее число обнаруженных и исправленных при тестировании ошибок;

$n_i = m_1 + ... + m_k$. - число ошибок, исправленных к началу (i+1)-го этапа тестирования ($n_0 = 0$).

В модели Шумана ПО на i-м этапе тестирования имеет функцию надежности

$$p_i(t) = \exp(-C(N - n_{i-1})t),$$

где N — первоначальное количество ошибок в ПО;

$N - n_{i-1}$ — количество ошибок, оставшихся к началу i-го этапа;

C - коэффициент пропорциональности.

Неизвестные параметры модели N и C можно приближенно определить из системы уравнений

$$\sum_{i=1}^{k} m_i = C\sum_{i=1}^{k}(N - n_{i-1})t_i;$$

$$C\sum_{i=1}^{k} t_i = \sum_{i=1}^{k}\frac{m_i}{N - n_{i-1}}.$$

Вычислив значения N и C можно определить показатели:

1) число оставшихся ошибок в ПО $N_т = N - n$.

2) функцию надежности ПО по завершении тестирования:

$$p(t) = \exp(-C(N-n)t).$$

МОДЕЛЬ ШИКА-ВОЛВЕРТОНА. Это модификация модели Шумана. Считается, что на каждом этапе тестирования интенсивность отказов ПО пропорциональна не только количеству оставшихся ошибок, но и времени тестирования, т.е. вероятность обнаружения ошибок с течением времени возрастает. Обозначим

$T_0 = 0$; $T_i = t_1 + ... + t_i$, i = 1,2,...,k-1; $T = t_1 + ... + t_k$.

Здесь T_i — суммарная продолжительность первых i этапов тестирования, T - общее время тестирования.

В модели Шика-Волвертона интенсивность отказов ПО на i-м интервале тестирования предлагается равной

$$\lambda_i = C(N - n_{i-1})(T_{i-1} + \frac{t_i}{2}).$$

Параметры N и C определяются из системы уравнений

$$\sum_{i=1}^{k} m_i = C\sum_{i=1}^{k}(N - n_{i-1})(T_{i-1} + \frac{t_i}{2})t_i ;$$

$$C\sum_{i=1}^{k} t_i = \sum_{i=1}^{k}\frac{m_i}{(N - n_{i-1})(T_{i-1} + \frac{t_i}{2})}.$$

5. СТАТИЧЕСКИЕ МОДЕЛИ НАДЕЖНОСТИ ПО

Статические модели отличаются от динамических прежде всего тем, что в них не учитывается время появления ошибок.

МОДЕЛЬ МИЛЛСА. Использование этой модели предполагает необходимость перед началом тестирования искусственно вносить в программу некоторое количество известных ошибок. Ошибки вносятся случайным образом и фиксируются в протоколе искусственных ошибок. Специалист, проводящий тестирование, не знает ни количества, ни характера внесенных ошибок. Предполагается, что все ошибки (как естественные, так и искусственно внесенные) имеют равную вероятность быть найденными в процессе тестирования.

Программа тестируется в течении некоторого времени и собираются статистики об обнаруженных ошибках.

Пусть после тестирования обнаружено n собственных ошибок программы и v искусственно внесенных ошибок. Тогда первоначальное число ошибок в программе N можно оценить по формуле Миллса

$$N = n\frac{S}{\nu},$$

где S — количество искусственно внесенных ошибок.

Например, если в программу внесено 50 ошибок и в процессе тестирования обнаружено 25 собственных и 5 внесенных ошибок, то по формуле Миллса делается предположение, что первоначально в программе было 250 ошибок.

Вторая часть модели связана с проверкой гипотезы об N. Допустим мы считаем, что в программе первоначально К ошибок. Вносим искусственно в программу S ошибок и тестируем ее до тех пор, пока все искусственно внесенные ошибки не будут обнаружены. Пусть при этом обнаружено n собственных ошибок программы. Вероятность, что в программе первоначально было К ошибок, можно рассчитать по соотношению

$$p = \begin{cases} 0, & \text{если } n > K; \\ \dfrac{S}{S + K + 1}, & \text{если } n \le K. \end{cases} \qquad (7.1)$$

Например, если утверждается, что в программе нет ошибок (K=0) и при внесении в программу 10 ошибок все они в процессе тестирования обнаружены, но при этом не выявлено ни одной собственной, то $p = {}^{10}\!/_{11} = 0{,}91$. Таким образом, с вероятностью 0,91 можно утверждать, что в программе нет ошибок. Но если в процессе тестирования обнаружена хоть одна собственная ошибка, то P = 0.

Формулу (7.1) можно использовать только в случае, если обнаружены все S искусственно внесенных ошибок. Если же обнаружено только v искусственно внесенных ошибок, то применяют формулу

$$p = \begin{cases} 0, & \text{если } n > K; \\ C_S^{v-1} \Big/ C_{S+K+1}^{K+v}, & \text{если } n \le K. \end{cases}$$

Например, если утверждается, что в программе нет ошибок, а к моменту оценки надежности обнаружено 5 из 10 искусственно внесенных ошибок и не обнаружено ни одной собственной ошибки, то вероятность того, что в программе действительно нет ошибок, будет равна

$$p = \frac{C_{10}^4}{C_{11}^5} = \frac{5}{11} \approx 0{,}45 .$$

Если при тех же исходных условиях оценки надежности производится в момент, когда обнаружены 8 из 10 искусственных ошибок, то

$$p = C_{10}^7 \Big/ C_{11}^8 = \frac{8}{11} \approx 0{,}73 .$$

Достоинством модели Миллса является простота применяемого математического аппарата и наглядность. Применение этой модели для оценки надежности оказывает положительное психологическое воздействие на лиц, выполняющих тестирование, уже только тем, что они знают: в программу внесены ошибки.

Однако есть недостатки:

1) необходимость внесения искусственных ошибок (этот процесс плохо формализуем);

2) достаточно вольное допущение величины K, которое основывается исключительно на интуиции и опыте человека, проводящего оценку, т.е. допускает большое влияние субъективного фактора.

ПРОСТАЯ ИНТУИТИВНАЯ МОДЕЛЬ. Использование этой модели предполагает проведение тестирования двумя группами программистов (или двумя программистами в зависимости от величины программы) независимо друг от друга, использующими независимые тестовые наборы. В процессе тестирования каждая из групп фиксируют все найденные ею ошибки.

Пусть первая группа обнаружила n_1 ошибок, вторая n_2, n_{12} — это число ошибок, обнаруженных как первой, так и второй группой.

Обозначим через N неизвестное количество ошибок, присутствующих в программе до начала тестирования. Тогда можно эффективность тестирования каждой из групп определить как

$$E_1 = \frac{n_1}{N}\ ,\ E_2 = \frac{n_1}{N}\ .$$

Эффективность тестирования можно интерпретировать как вероятность того, что ошибка будет обнаружена. Таким образом, можно считать, что первая группа обнаруживает ошибку в программе с вероятностью $p_1 = \frac{n_1}{N}$, вторая - с вероятностью $p_2 = \frac{n_2}{N}$.

Тогда вероятность p_{12} того, что ошибка будет обнаружена обеими группами, можно принять равной $\frac{n_{12}}{N}$. С другой стороны, так как группы действуют независимо друг от друга, то $p_{12} = p_1 p_2$. Получаем $\frac{n_{12}}{N} = \frac{n_1}{N} \bullet \frac{n_2}{N}$.

Отсюда получаем оценку первоначального числа ошибок программы :

$$N = \frac{n_1 n_2}{n_{12}}\ .$$

МОДЕЛЬ НЕЛЬСОНА. В модели предлагается, что область, которой могут принадлежать входные данные программы, разделена на k непересекающихся областей Z_i, i = 1,2,...,k. Пусть p_i — вероятность того, что для очередного выполнения программы будет выбран набор данных из области Z_i. Значение p_i определяются по статистике входных данных в реальных условиях работы ПО.

Пусть к моменту оценки надежности было выполнено N_i прогонов ПО на наборах данных из области Z_i, и n_i из этих прогонов закончились отказом. Тогда надежность ПО оценивается по формуле $P = 1 - \sum_{i=1}^{K} \frac{n_i}{N_i} p_i$.

6. ЭМПИРИЧЕСКИЕ МОДЕЛИ

Эмпирические модели основана на анализе накопленной информации о функционировании ранее разработанных программ.

Наиболее простая эмпирическая модель связывает число ошибок в ПО с объемом ПО. Опытные данные свидетельствуют, что к началу системного тестирования в ПО на каждые 1000 операторов приходится примерно 10 ошибок. Уровень надежности ПО считается приемлемым для начала эксплуатации, если тому же объему операторов будет соответствовать одна ошибка.

Фирма IBM использует эмпирическую модель, которая оценивает число ошибок в различных редакциях операционной системы:

$N = 23M_{10} + 2M_1$,

где M_{10} — число модулей, потребовавших 10 и более исправлений;

M_1 — число модулей, в которых обнаружено меньше 10 ошибок.

Применяется также эмпирическая формула для оценки средней наработки ПО:

$$\tau = \alpha \frac{V_{on}}{N},,$$

где τ - средняя наработка ПО в часах;

$V_{оп}$ — объем программы в операторах;

N — число ошибок в ПО, оцененное по одной из приведенных выше моделей;

α — коэффициент, лежащий в диапазоне от 100 до 1000.

7. ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОЙ ПРОДОЛЖИТЕЛЬНОСТИ ТЕСТИРОВАНИЯ

На практике модели надежности ПО могут применятся для оценки соответствия ПО системным требованиям, оценки надежности ПО заказчиком и т.д. Наиболее распространенная сфера применения моделей –— определение оптимальной продолжительности тестирования.

Пусть C_1 — полная стоимость тестирования (сюда входят стоимость обнаружения и устранения ошибок и стоимость выполнения тестовых прогонов), C_2 — стоимость устранения ошибок, возникающих на этапе сопровождения. Тогда суммарная стоимость равна $C = C_1 + C_2$.

Пусть каждая ошибка ПО может проявится (привести к программному отказу) с интенсивностью λ. Тогда за время t она проявится с вероятностью $1 - e^{-\lambda t}$. Следовательно, среднее за период t количество отказов равно $n(t) = N(1 - e^{-\lambda t})$, где N - первоначальное число ошибок.

Стоимости C_1 и C_2 можно выразить следующим образом :

$$C_1 = k_1 n(T) + k_3 T,$$
$$C_2 = k_2 n(T_o) - n(T)),$$

где k_1 — стоимость обнаружения и устранения одной ошибки на этапе тестирования ПО,

k_2 — стоимость обнаружения и устранения ошибки на этапе сопровождения ПО,

k_3 — стоимость тестирования ПО в единицу времени,

T_o — длительность жизненного цикла ПО,

T - суммарное время тестирования.

Обычно $k_2 > k_1$. Тогда суммарная стоимость равна

$$C = k_1 n(T) + k_3 T + k_2 (n(T_o) - n(T)) = k_1 N - k_2 e^{-\lambda T_o} + k_3 (T + N \frac{k_2 - k_1}{k_3} e^{-\lambda T}).$$

Выберем время тестирования так, чтобы минимизировать суммарную стоимость C. Для этого нужно найти минимум функции

$$g(T) = T + \frac{N}{S} e^{-\lambda T}, \text{ где } S = \frac{k_3}{k_2 - k_1}.$$

Возьмем производную функции g(T):

$$g'(T) = 1 - \frac{\lambda N}{S} e^{-\lambda T}.$$

Оптимальное значение T^* зависит от соотношения величин λN и S.

Если $\lambda N \le S$, то $g`(T) \ge 0$ для всех T, т.е. g(T) возрастает, и следовательно, $T^* = 0$. В этом случае тестирование проводить нецелесообразно.

Если $\lambda N > S$, то g(T) достигает минимума при $T = T_1 = \frac{1}{\lambda} \ln(\frac{\lambda N}{S})$. Так как время тестирования не может превышать длительность жизненного цикла T_o , то $T^* = \min(T_o , T_1)$.

8. МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Для повышения надежности ПО также применяется резервирование. Для этого подготавливается несколько версий ПО. Желательно чтобы эти версии основывались на различных алгоритмах, или, по крайней мере, были бы созданы различными программистами. Опыт показывает, что совпадение ошибок в различных версиях маловероятно. Версии исполняются одновременно (при наличии нескольких компьютеров) или последовательно во времени.

В случае двух различных версий ПО говорят, что применено **дуальное программирование.** Если при выполнении этих версий обнаруживается расхождение в результатах, то правильный результат выбирается по каким-либо дополнительным критериям (например, проверяется принадлежность результата определенной области).

Если подготавливается и выполняется N версий ПО, то говорят о **N-версионном программировании**. В этом случае в качестве правильного выбирается результат, полученный на выходе большинства версий ПО.

Недостатки дуального и N-версионного программирования: либо в несколько раз возрастает время выполнения (в случае последовательного исполнения версий), либо во столько же раз возрастает количество требуемой вычислительной техники (в случае одновременного исполнения). Кроме того, в несколько раз возрастает труд программистов.

Поэтому все большее распространение получает **модифицированное дуальное программирование**, при котором кроме основной программы, точной, но трудоемкой, подготавливается резервная программа, менее точная, но зато более простая. За счет простоты резервная программа имеет более высокую надежность и выполняется в несколько раз быстрее, чем основная.

Программы выполняются последовательно (общее время выполнения при этом увеличивается незначительно). Задается допустимая погрешность, и если выходные результаты обеих программ различаются больше, чем на допустимую погрешность, то делается вывод, что отказала основная программа, как менее надежная, а в качестве выходных результатов берутся выходные результаты резервной программы.

Пусть y_1 — выходные результаты основной программы, σ_1 — допустимая погрешность основной программы, y_2 и σ_2 — соответственно выходные результаты и допустимая погрешность резервной программы (при этом $\sigma_1 < \sigma_2$). При сравнении выходных результатов y_1 и y_2 задается допустимая погрешность $\sigma_1 + \sigma_2$, а решающим органом служит простейшая программа

$$y = \begin{cases} y_1, \textit{если } |y_1 - y_2| \le \sigma_1 + \sigma_2; \\ y_2, \textit{ если } |y_1 - y_2| > \sigma_1 + \sigma_2. \end{cases}$$

Пусть вероятность отказа у основной программы q_1 , у резервной q_2 (при этом $q_2 < q_1$). Тогда возможны следующие события:

1) отказа не произошло ни в основной, ни в резервной программе. Вероятность этого события $(1-q_1)(1-q_2)$, погрешность выходных результатов $y = y_1$ равна σ_1;

2) отказала основная программа, резервная прошла безотказно. Вероятность этого события $q_1(1- q_2)$, погрешность выходных результатов $y_1 = y_2$ равна σ_2 ;

3) отказала резервная программа. Вероятность этого события q_2 , погрешность выходных результатов $y = y_2$ будет равна некоторому σ_3 , намного большему, чем σ_2.

Следовательно, надежность системы с модифицированным дуальным программированием равна $1-q_2$, т.е. вероятность отказа при введении резервной программы уменьшается в q_1 / q_2 раза. Средняя погрешность при безотказной работе резервной программы будет равна $(1-q_1)\sigma_1 + q_1\sigma_2 = \sigma_1 + (\sigma_2 - \sigma_1)q_1$.

Таким образом, средняя погрешность увеличивается незначительно по сравнительно с погрешностью σ_1 основной программы.

9. НАДЕЖНОСТЬ ЧЕЛОВЕКА КАК ЭЛЕМЕНТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

ПРИНЦИПЫ УЧЕТА ЧЕЛОВЕЧЕСКОГО ФАКТОРА

Роль человека в автоматизированной системе можно охарактеризовать следующими основными положениями:

1. Принцип минимального рабочего усилия. Человек-оператор должен выполнять только ту работу, которая необходима, но не может быть выполнена системой.

2. Принцип максимального взаимопонимания. Система должна обеспечивать полную поддержку человеку: выдаваемая информация не должна требовать интерпретации или перекодировки.

3. Принцип минимального объема оперативной памяти пользователя. От человека требуется, чтобы он запоминал как можно меньше.

4. Принцип максимального контроля со стороны человека. Этот принцип характеризуется следующими требованиями:

- оператор должен иметь возможность изменить очередность обработки, выполняемой системой;
- оператор должен контролировать последовательность работы, особенно там, где нет последовательно определенных операций.

5. Принцип преимущественных возможностей. Состоит в передаче человеку тех функций, которые он выполняет лучше машины, а машине тех, которые она выполняет лучше человека.

6. Принцип оптимальной загрузки. Рекомендует такое распределение функций, при котором оператор по темпу поступления данных не испытывал бы ни сенсорного голода (потеря активности), ни сенсорной перегрузки (пропуск сигналов).

7. Принцип ответственности. Имеет особое значение в системах, где на человека возлагается ряд ответственных функций, даже при наличии технических возможностей их полной автоматизации.

ОШИБКИ ЧЕЛОВЕКА

Надежность работы человека определяется как вероятность успешного выполнения им работы или поставленной задачи на заданном этапе функционирования системы в течение заданного интервала времени.

Ошибка человека определяется как невыполнение поставленной задачи (или выполнение запрещенного действия), которое может явиться причиной нарушения нормального функционирования системы.

Ошибки по вине человека могут возникать в случаях, когда:

1) человек стремится к достижению ошибочной цели;

2) поставленная цель не может быть достигнута из-за неправильных действий человека;

3) человек бездействует в тот момент, когда его участие необходимо.

10. КРИТЕРИИ ОЦЕНКИ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА

Деятельность человека - оператора характеризуется быстродействием и надежностью.

Критерий быстродействия - время решения задачи, т.е. время от момента реагирования оператора на поступивший сигнал до момента окончания управляющих воздействий.

Это время пропорционально количеству перерабатываемой информации:

$$T = a + H/V,$$

где a - скрытое время реакции, т.е. промежуток от момента появления сигнала до реакции на него оператора,

H - количество перерабатываемой информации,

V - средняя скорость переработки информации.

Надежность человека-оператора определяет его способность выполнять в полном объеме возложенные на него функции при определенных условиях работы. Надежность деятельности оператора характеризуют его **безошибочность, готовность, восстанавливаемость, своевременность и точность.**

Вероятность P_i безошибочного выполнения операций i-го вида и интенсивность λ_i допущенных при выполнении этих операций ошибок, определяются на основе статистических данных

$$P_i = \frac{N_i - C_i}{N_i}, \quad \lambda_i = \frac{C_i}{N_i T_i}$$

где N_i - общее число выполняемых операций i-го вида;

C_i - допущенное при этом число ошибок,

T_i - среднее время выполнения операции i-го вида.

Предполагая, что интенсивность λ_i - постоянная величина, можно определить вероятность безошибочного выполнения всей операции в целом:

$$P_0 = \exp\left(-\sum_{i=1}^{r} \lambda_i T_i K_i\right) = \exp\left(-\sum_{i=1}^{r} (1 - P_i) K_i\right),$$

где K_i - число выполняемых операций i-го вида,

r - число различных видов операций.

Коэффициент готовности характеризует вероятность включения человека-оператора в работу в произвольный момент времени

$$K_{ОП} = 1 - \frac{T_0}{T},$$

где T_0 - время, в течении которого человек не может принять поступившую к нему информацию,

T - общее время работы человека-оператора.

Восстанавливаемость оператора оценивается вероятностью исправления допущенной им ошибки:

$$P_в = P_1 \cdot P_2 \cdot P_3,$$

где P_1 - вероятность выдачи сигнала об ошибке контрольной системой,

P_2 - вероятность обнаружения этого сигнала оператором,

P_3 - вероятность исправления ошибочных действий при повторном выполнении всей операции.

Этот показатель позволяет оценить возможность самоконтроля оператором своих действий и исправления допущенных им ошибок.

Своевременность действий оператора оценивается вероятностью выполнения задачи в течении заданного времени:

$$P_{св} = P\left(T \le t^*\right) = \int_0^{t^*} f(t)dt ,$$

где f(t) - плотность вероятности времени решения задачи оператором,

t^* - лимит времени, превышение которого рассматривается как ошибка.

Эта же вероятность может быть определена и по статистическим данным, как

$$P_{св} = \frac{N - N_{не}}{N} ,$$

где N - общее количество выполненных задач,

$N_{не}$ - количество задач с несвоевременным выполнением.

Точность - степень отклонения измеряемого оператором количественного параметра системы от его истинного или заданного значения. Количественно точность оценивается погрешностью, с которой оператор измеряет или регулирует данный параметр:

$$\Delta A = A_И - A_{ОП} ,$$

где $A_И$ - истинное или заданное значение параметра,

$A_{ОП}$ - фактически измеряемое или регулируемое оператором значение этого параметра.

Значение погрешности, превысившее допустимые пределы, является ошибкой, и ее следует учитывать при оценке надежности.

Точность оператора зависит от характеристик сигнала, сложности задачи, условий и темпа работы, состояния нервной системы, квалификации и других факторов.

11. ОЦЕНКА НАДЕЖНОСТИ СИСТЕМЫ "КТС-ПО-ЧЕЛОВЕК"

Сделаем следующие допущения:

1) отказы КТС (комплекса технических средств), ПО и ошибки оператора являются редкими, случайными и независимыми событиями;

2) появление более одного события за время работы системы от t_0 до t_0+t практически невозможно;

3) способности оператора к компенсации ошибок и к безошибочной работе - независимые свойства оператора.

Если компенсация ошибок оператора и отказов КТС или ПО невозможна, то вероятность безотказной работы системы

$$P_1(t_0, t) = P_C(t_0, t) \cdot P_0(t) \ ,$$

где $P_C(t_0, t)$ - вероятность безотказной работы КТС и ПО в течении времени от t_0 до t_0+t,

$P_0(t)$ - вероятность безошибочной работы оператора в течении времени t при условии, что КТС и ПО работали безотказно;

(t_0, t_0+t) - рассматриваемый период работы системы.

При компенсации ошибок оператора с вероятностью p вероятность безотказной работы системы

$$P_2(t_0, t) = P_C(t_0, t)\left(P_0(t) + \left(1 - P_0(t)\right)p\right).$$

В случае компенсации только отказов КТС и ПО вероятность безотказной работы системы

$$P_3(t_0, t) = P_0(t)\left(P_C(t_0, t) + \left(1 - P_C(t_0, t)\right)P_K(t_0, t)\right) ,$$

где $P_K(t_0, t)$ - условная вероятность компенсации последствий отказа и дальнейшей безотказной работы при условии наступления отказа в течение промежутка времени (t_0, t_0+t).

Вероятность безотказной работы системы с компенсацией ошибок оператора и отказов КТС и ПО

$$P_4(t_0, t) = \left(P_0(t) + \left(1 - P_0(t)\right)p\right)\left(P_C(t_0, t) + \left(1 - P_C(t_0, t)\right)P_K(t_0, t)\right).$$

Выигрыш в надежности G_P за счет компенсации ошибок и отказов характеризуется отношением

$$G_P = \frac{P_4(t_0, t)}{P_1(t_0, t)} \ .$$

Выигрыш в надежности увеличивается с ростом p и $P_K(t_0, t)$, т.е. с увеличением уровня натренированности оператора на компенсацию отказов и ошибок.

12. ТЕХНИЧЕСКАЯ ДИАГНОСТИКА

ДИАГНОСТИЧЕСКИЙ ПРОЦЕСС

Опыт эксплуатации показывает, что наиболее продолжительным этапом восстановления работоспособности является поиск отказавшего элемента. Поэтому в сложных системах большое внимание уделяется вопросам технической диагностики (поиска отказавших элементов).

Будем рассматривать системы с последовательным (в смысле надежности) соединением элементов. Считаем, что вероятность возникновения одновременно двух и большего числа отказов пренебрежимо мала по сравнению с вероятностью возникновения одного отказа. Поэтому при отказе системы будем считать, что отказал единственный элемент (неизвестно какой). Целью диагностического процесса является выявление отказавшего элемента.

Поставим задачу оптимизации диагностического процесса по определенному критерию. Таким критерием может быть: продолжительность диагностического процесса; общее число проверок, необходимое для отыскания отказавшего элемента; стоимость реализации диагностического процесса и др. Для многих сложных систем основным критерием оптимизации является продолжительность диагностического процесса.

Весь диагностический процесс состоит из нескольких этапов. Каждый этап включает набор испытаний (в частном случае одно испытание) по заранее заданной программе, каждый новый этап которой определяется на основании информации, полученной в предыдущем этапе.

Условимся в дальнейшем считать процесс поиска неисправного элемента оптимальным, если его продолжительность минимальна. В зависимости от типа системы (характера взаимосвязи между элементами и возможного способа их проверки), а также от квалификации обслуживающего персонала и опыта эксплуатации оптимальная программа поиска может строиться по-разному. Используются следующие методы: метод поэлементных проверок; метод групповых проверок; метод логического анализа симптомов отказа. Первые два метода дают наибольший эффект в ситуации, когда квалификация обслуживающего персонала недостаточно высока. Последний метод весьма эффективен, если специалист в совершенстве знает эксплуатируемую систему.

ТЕМА 8. Энтропия системы

1. ЭНТРОПИЯ СОСТОЯНИЯ ОТКАЗАВШЕЙ СИСТЕМЫ И ИНФОРМАЦИЯ

Диагностический процесс - это процесс, связанный с получением и переработкой информации. Необходимость получения информации возникает всякий раз, когда есть неопределенность исхода испытания. В частности, неопределенность состояния системы после отказа возникает из-за того, что неизвестно, какой именно элемент отказал.

Для каждого элемента i определим **коэффициент отказа β_i** - условную вероятность того, что отказ системы произошел из-за элемента i.

Пусть наработка системы к моменту отказа равна t, функцию отказа i-го элемента обозначим $q_i(t)$. Считаем, что к моменту t все $q_i(t)$ намного меньше 1, тогда вероятностью возникновения одновременно нескольких отказов можно пренебречь. Функция отказа всей системы равна $q_S(t) \approx \sum_{k=1}^{n} q_k(t)$, а коэффициенты отказа будут равны

$$\beta_i = q_i(t) \Big/ \sum_{k=1}^{n} q_k(t), \quad i = 1,2,\ldots,n.$$

В частности, если каждый элемент имеет постоянную интенсивность λ_i, то $q_i(t) \approx \lambda_i t$ и

$$\beta_i = \lambda_i \Big/ \sum_{k=1}^{n} \lambda_k, \quad i = 1,2,\ldots,n.$$

Испытание состоит в том, что проверяется работоспособность одного элемента или группы элементов. Во втором случае после испытания определяется, содержит ли выбранная группа отказавший элемент, или не содержит. После проведения испытания условные вероятности β_i изменяются и становятся равными β_i^*.

Пример 1. Пусть испытание состоит в том, что проверяется элемент 1. Тогда в зависимости от результата испытания возможны два случая.

А. Элемент 1 отказал. Тогда, очевидно, $\beta_1^*=1$, $\beta_i^*=0$, $i>1$, и неопределенность системы исчезает.

В. Элемент 1 исправен. Тогда $\beta_1^* = 0$, $\beta_i^* = \beta_i \Big/ \sum_{k=2}^{n} \beta_k$, $i = 2,3,\ldots,n$.

После испытания неопределенность системы уменьшается. Чтобы количественно измерить изменение неопределенности, введем понятие **энтропии .**

Определение 1. **Энтропией** системы называется величина

$$H = -\sum_{i=1}^{n} \beta_i \log_2 \beta_i .$$

Энтропия служит мерой неопределенности системы. Величина H принимает минимальное значение, когда точно известно, какой элемент отказал (полная определенность). В этом случае $\beta_i = 1$, если отказал элемент с номером i, $\beta_j = 0$ при $j \neq i$. Тогда энтропия системы равна 0.

Максимального значения энтропия достигает при полной неопределенности системы, когда равновероятны отказы каждого элемента: $\beta_i = 1/n$, $i = 1,2,\ldots,n$. В этом случае $H = \log_2 n$.

После проведения испытания коэффициенты отказа становятся равными β_i^*. Соответственно изменяется и энтропия системы, которая становиться равной

$$H^* = -\sum_{i=1}^{n} \beta_i^* \log_2 \beta_i^* .$$

Определение 2. Количество информации, полученное после проведения испытания, будем определять как $I = H - H^*$.

Таким образом, количество информации равно уменьшению энтропии.

Пусть мы собираемся провести испытание. Текущая энтропия H известна, значение H^* зависит от результата испытания. Следовательно, H^* и I можно рассматривать как случайные величины.

Определение 3. **Средним количеством информации**, получаемым при проведении испытания называется математическое ожидание величины I:

$$J = M(I) = H - M(H^*).$$

Пример 2. В системе два элемента с коэффициентами отказа β_1 и $\beta_2 = 1 - \beta_1$. Энтропия равна $H = -\beta_1 \log_2 \beta_2 - \beta_2 \log_2 \beta_2$. Испытание заключается в проверке элемента 1. Возможные результаты сведем в таблицу

РЕЗУЛЬТАТ	ВЕРОЯТНОСТЬ РЕЗУЛЬТАТА	β_1^*	β_2^*	H^*
Элемент исправен	$1-\beta_1$	0	1	0
Элемент отказал	β_1	1	0	0

Таким образом, $M(H^*)=0$ и J=H. Проведенное испытание полностью устраняет неопределенность системы.

Пример 3. В системе четыре элемента с коэффициентами отказа β_1, β_2, β_3, β_4, где $\beta_1 + \beta_2 + \beta_3 + \beta_4 = 1$. Проверяем группу из первого и второго элемента.

Возможные результаты сведем в таблицу.

Результат	Вероятность результата	β_1^*	β_2^*	β_3^*	β_4^*	H^*
Группа содержит отказавший элемент	$\beta_1 + \beta_2$	$\beta_1 / (\beta_1 + \beta_2)$	$\beta_2 / (\beta_1 + \beta_2)$	0	0	$H_1^* = -\beta_1^* \log_2 \beta_1^* - \beta_2^* \log_2 \beta_2^*$
Группа не содержит отказавший элемент	$\beta_3 + \beta_4$	0	0	$\beta_3 / (\beta_3 + \beta_4)$	$\beta_4 / (\beta_3 + \beta_4)$	$H_2^* = -\beta_3^* \log_2 \beta_3^* - \beta_4^* \log_2 \beta_4^*$

Следовательно,

$$M(H^*) = (\beta_1 + \beta_2) H_1^* + (\beta_3 + \beta_4) H_2^* == H + (\beta_1 + \beta_2) \log_2 (\beta_1 + \beta_2) + (\beta_3 + \beta_4) \log_2 (\beta_3 + \beta_4),$$

где $H = -\beta_1 \log_2 \beta_1 - \beta_2 \log_2 \beta_2 - \beta_3 \log_2 \beta_3 - \beta_4 \log_2 \beta_4$ - первоначальная энтропия системы.

Итак, испытание дает среднее количество информации

$$J = -(\beta_1 + \beta_2) \log_2 (\beta_1 + \beta_2) - (\beta_3 + \beta_4) \log_2 (\beta_3 + \beta_4).$$

Результат примера 3 можно обобщить. Пусть испытание заключается в проверке группы элементов системы (в частном случае, одного элемента). При этом сумма всех коэффициентов β_i элементов проверяемой группы равна p . Несложно подсчитать, что испытание дает среднее количество информации

$$J(p) == -p \log_2 p - (1-p) \log_2 (1-p)$$

Функция J(p) достигает максимума при p=0,5 , при этом $J(p) = J(1-p)$. Таким образом, чем ближе значение p к 0,5, тем большим будет среднее количество информации, получаемое при испытании.

Определение 4. **Скоростью получения информации** называется отношение W=J/t,

где W - скорость получения информации,

J - среднее количество информации,

t - средняя продолжительность испытания.

Для получения минимальной продолжительности диагностического процесса необходимо стремиться к увеличению скорости уменьшения неопределенности, что равносильно увеличению скорости получения информации.

На первом этапе испытаний добиваются выполнения равенства $W = \max_i \left(J_i / t_i \right)$.

Учитывая результаты первого этапа, определяют второй этап поиска. Из всех возможных вариантов испытаний при создавшейся ситуации выбирается тот, который вновь обеспечивает максимальное значение скорости получения информации. Затем выбирают третий этап поиска, четвертый и т.д., руководствуясь одним и тем же принципом: получением максимальной скорости информации на каждом этапе.

Данный принцип называется **принципом максимальной скорости получения информации (принцип МСПИ) .**

2. МЕТОД ПОЭЛЕМЕНТНЫХ ПРОВЕРОК

Этот метод предусматривает проверку элементов по одному в определенной, заранее заданной последовательности. Каждая проверка имеет два исхода: либо элемент исправен, либо нет. Если проверяемый элемент оказался исправным, то приступают к проверке следующего и так до обнаружения неисправности. Выясним, в какой последовательности необходимо проверять элементы, чтобы удовлетворить принципу МСПИ.

Рассмотрим систему, состоящую из n элементов. Считаем, что коэффициенты отказа элементов β_i и среднее время проверки каждого элемента t_i известны.

Рассмотрим сначала случай, когда $t_1 = t_2 = ... = t_n$. В этом случае принцип МСПИ вырождается в принцип получения максимальной информации за каждую проверку.

Рассмотрим первый этап, на котором проверяется элемент с коэффициентом β_i. При этом испытании среднее количество получаемой информации равно

$$J(\beta_i) = -\beta_i \log_2 \beta_i - (1-\beta_i)\log_2(1-\beta_i).$$

Эта величина достигает максимума при значении β_i , наиболее близком к 0,5. Несложно доказать, что ближе всего к 0,5 будет максимальное из всех значений $\beta_1, \beta_2, ..., \beta_n$. Допустим, это значение β_1 .

Если проверка показала, что выбранный элемент неисправен, то процесс диагностики заканчивается. Если элемент оказался исправным, то для оставшихся элементов коэффициенты отказа становятся равными

$$\beta_2^* = \frac{\beta_2}{1-\beta_1} \ , \ \dots \ , \ \beta_n^* = \frac{\beta_n}{1-\beta_1}.$$

Для второй проверки следует выбрать элемент со значением β_i^* , наиболее близким к 0,5, т.е. с максимальным из всех значений $\beta_2, ..., \beta_n$.

Таким образом, можно сделать вывод: если среднее время проверки любого элемента одно и тоже, то в соответствии с принципом МСПИ элементы следует проверять в последовательности $\beta_1 \geq \beta_2 \geq ... \geq \beta_n$.

Рассмотрим теперь противоположный случай, когда все коэффициенты отказа равны $\beta_1 = \beta_2 = ... = \beta_n = 1/n$, а значения t_1 , t_2 ,...,t_n различны. В этом случае среднее количество получаемой информации J не зависит от выбираемого элемента, и для получения оптимального диагностического процесса в

соответствии с принципом МСПИ, элементы нужно проверять в следующей последовательности: $t_1 \le t_2 \le \ldots \le t_n$.

Если $t_1 = t_2 = \ldots = t_n$, $\beta_1 = \beta_2 = \ldots = \beta_n$, то последовательность проверок безразлична, т.е. проверку можно начинать с любого элемента.

Рассмотрим теперь общий случай, когда различаются и коэффициенты β_i и сроки проверок t_i . В соответствии с принципом МСПИ выбирается для проверки элемент, для которого величина $J(\beta_i)/t_i$ достигает максимума. Если проверка показала, что элемент исправен, то коэффициенты отказа остальных элементов становятся равными β_i^* , и для следующей проверки выбирается элемент, для которого величина достигает максимума.

Пример 1. Рассмотрим систему из четырех элементов со следующими характеристиками :

ЭЛЕМЕНТ	1	2	3	4
β_i	0,1	0,2	0,3	0,4
t_i	1	1,5	1,85	2
$J(\beta_i)$	0,469	0,722	0,881	0,971
$J(\beta_i)/t_i$	0,469	0,481	0,476	0,485

В соответствии с принципом МСПИ первым для проверки выбирается элемент 4. Если проверка показала, что элемент исправен, то получаем систему со следующими характеристиками:

ЭЛЕМЕНТ	1	2	3
β_i^*	0,17	0,33	0,5
t_i	1	1,5	1,85
$J(\beta_i^*)$	0,650	0,918	1
$J(\beta_i^*)/t_i$	0,650	0,612	0,540

По принципу МСПИ для проверки выбирается элемент 1. Если он оказался исправным, то получаем систему

ЭЛЕМЕНТ	2	3
β_i^*	0,4	0,6
t_i	1,5	1,85
$J(\beta_i^*)$	0,971	0,971
$J(\beta_i^*)/t_i$	0,647	0,524

Для очередной проверки выбирается элемент 2. Таким образом, получаем последовательность проверки элементов: 4, 1, 2.

ТЕМА 9. Методы проверки

1. МЕТОД ГРУППОВЫХ ПРОВЕРОК

Метод групповых проверок предусматривает одновременную проверку некоторой группы элементов, в которой может находиться отказавший элемент. Если выясняется, что неисправный элемент находится в проверяемой группе, то последнюю вновь разбивают на две группы, и поиск неисправности ведется среди элементов этих подгрупп. Если проверка показала, что неисправных элементов в проверяемой группе нет, то дальнейшей диагностике подвергается оставшаяся (непроверенная) группа элементов. Такой процесс деления продолжается до обнаружения отказавшего элемента. Пусть проверяемая группа содержит элементы с номерами $i_1, i_2, \dots, i_k$. Обозначим $p(i_1, \dots, i_k) = \beta_{i1} + \dots + \beta_{ik}$ - вероятность того, что отказавший элемент находится в выделенной группе, $t(i_1, \dots, i_k)$ - среднее время, требуемое для проверки выделенной группы.

Если среднее время проверки любой группы элементов одинаково, то принцип МСПИ вырождается в принцип получения максимума информации на каждом этапе диагностического процесса. Тогда на первом этапе диагностики нужно выделить подгруппу таким образом, чтобы $p(i_1, \dots, i_k)$ было бы как можно ближе к 0,5. На следующих этапах очередная подгруппа выделяется аналогично с учетом новых коэффициентов отказа β_i^*.

В общем случае, когда среднее время проверки зависит от состава группы, группа выделяется по условию максимизации величины

$$\frac{J\left(p\left(i_1,\dots,i_k\right)\right)}{t\left(i_1,\dots,i_k\right)}.$$

Трудоемкость вычислительных работ по определению оптимального диагностического процесса методом групповых проверок оправдана значительным сокращением времени, необходимого на поиск отказавшего элемента. Вся вычислительная работа выполняется заранее, еще до наступления отказа системы.

2. МЕТОД ЛОГИЧЕСКОГО АНАЛИЗА СИМПТОМОВ ОТКАЗА

Симптомом отказа системы является информация об отклонениях от норм параметров, характеризующих ее работоспособность или состояние, а также об изменении этих отклонений во времени.

Например, симптомом отказа может быть необычный шум, чрезмерный нагрев, запах горелой изоляции и др.

Симптомы отказа дают специалисту некоторую информацию о возможных состояниях системы. Максимальное количество информации содержится в симптоме, позволяющем однозначно определить отказавший элемент. Однако симптомы отказа не всегда однозначно определяют состояние системы.

Рассмотрим систему из n элементов, при отказе которой может наблюдаться к (или менее) симптомов отказа. Отказы различных элементов могут иметь один и тот же симптом, а отказ одного элемента - несколько симптомов. Таким образом, каждому элементу может соответствовать множество симптомов отказа. Взаимосвязь между элементами и симптомами можно представить в виде матрицы

ЭЛЕМЕНТЫ/СИМПТОМЫ	C_1	C_2	...	C_K
1	0	0	...	1
2	1	0	...	0
...	...	...	...	...
n	1	0	...	1

В клетке i-й строки и j-го столбца ставиться единица, если отказ элемента i сопровождается симптомом C_j, и ноль - в противном случае.

В идеальном для диагностического процесса случае каждому элементу соответствует только один симптом отказа, появление которого однозначно указывает на неисправность элемента. В этом случае при соответствующей нумерации симптомов получаем единичную матрицу, которую удобно использовать.

Благоприятным является случай несовпадения комплекса симптомов ни для каких двух элементов. В этом случае диагностическая задача также решается однозначно. На практике комплексы симптомов могут совпадать, и поэтому приходится использовать информацию, получаемую в результате дополнительных испытаний.

При анализе достаточности симптомов для однозначного выделения отказа любого элемента системы составляют кодовые числа, присущие каждому элементу. Цифры кодового числа составляют из номеров симптомов, наблюдающихся при отказе элемента, и записывают в правую часть таблицы. Для однозначного определения любого отказа необходимо, чтобы не было одинаковых кодовых чисел и кодовых чисел, равных нулю.

Если имеются симптомы, входящие в несколько комплексов, и после их исключения по прежнему выполняется условие различимости отказов, то такие симптомы можно исключить из рассмотрения, т.е. не контролировать некоторые параметры системы. Поиск отказавшего элемента в системе при использовании данного метода осуществляется по кодовому числу.

Пример 1. Пусть связь между элементами и симптомами представлена в таблице

ЭЛЕМЕНТЫ/СИМПТОМЫ	C_1	C_2	C_3	C_4	Кодовые	числа
1	1	1	1	1	1234	134
2	0	1	1	1	234	34

3	0	0	1	0	3	3
4	0	0	0	1	4	4

Анализируя таблицу, приходим к выводу, что условие различимости отказов элементов выполнено. Кроме того, условие различимости отказов не нарушится, если отсутствует симптом C_2. С помощью кодовых чисел можно однозначно определить отказавший элемент при отказе системы.

Достоинством метода поиска отказавших элементов по симптомам отказа является принципиальная возможность его использования в системах любой сложности. Недостатки: 1) метод не дает последовательности проверок для обнаружения любого отказа, 2) невысока разрешающая способность, так как при большом числе элементов в системе отказам некоторых элементов могут сопутствовать мало отличающиеся наборы симптомов.

3. ДИАГНОСТИКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Существуют три основных направления диагностики ПО: доказательство корректности программ, тестирование программ и разработка отказоустойчивых программ. Дадим краткую характеристику этих направлений.

1.Методы доказательства корректности программ (ДКП) .

В начале вычислений каждая ячейка программы содержит числа. Набор этих чисел является вектором состояния вычислений. Каждая операция рассматривается как преобразование существующего вектора состояния в другой вектор состояния. Таким образом, программа может рассматриваться как некоторая функция в пространстве векторов состояний.

Современные методы ДКП используют средства математической логики. С помощью этих методов последовательность векторов состояния превращается в множество утверждений о функциональных связях между переменными программы. Процесс доказательства корректности превращается в доказательство того, что каждое утверждение истинно, как только это утверждение достигается при движении по программе.

2. Тестовое диагностирование программ.

Тестовое диагностирование может применяться на всех этапах жизни ПО: от этапа разработки технического задания до этапа эксплуатации. В зависимости от стратегии разработки ("снизу-вверх", “сверху-вниз”, комбинированной) применяются различные методологии тестирования.

При классической стратегии "снизу-вверх" сначала разрабатываются и тестируются отдельные модули. Затем модули объединяются в подсистемы и проверяются связи между модулями. Подсистемы объединяются в систему, которая подвергается системным и приемочным испытаниям.

Стратегия "сверху-вниз" предполагает иерархическое построение ПО. Сначала разрабатывается и тестируется модуль самого верхнего уровня. Затем к отлаженному модулю верхнего уровня подключаются модули последующего

уровня. Тестовое диагностирование подключенного модуля проводится через модуль верхнего уровня, т.е. модули тестируются одновременно. К недостаткам методологии такого тестового диагностирования следует отнести трудности нахождения таких тестовых воздействий, прикладываемых к модулю верхнего уровня, которые проверяли бы определенные функции модулей нижних уровней.

Поэтому часто применяется комбинированная стратегия разработки, при которой модули тестируются отдельно, но система разрабатывается "сверху-вниз".

Методы тестового диагностирования могут быть разделены на детерминированные и стохастические.

Детерминированные методы разбивают области входных значений на подобласти и определяют тестовые примеры (обычно по одному из каждой подобласти). Выбранные примеры просчитываются программой и результаты сравниваются либо с известными результатами, записанными в техническом задании, либо с результатами, полученными ручным подсчетом, либо с результатами, полученными другой программой. Основной недостаток такого подхода в том, что бывает трудно провести нужное разбиение области входных значений, и при этом могут вкрасться ошибки. Поэтому полученные тесты могут не обнаруживать всех ошибок программы.

Стохастические методы с помощью генератора случайных чисел выбирают некоторое множество тестовых примеров, которые затем просчитываются программой. Недостатки этого подхода в том, что после просчета определенных путей в программе генератор тестов начнет повторяться, генерируя тесты, которые проходят по тем же дугам и путям в программе. Кроме того, количество тестов очень велико и необходимо наличие программы-дубля (ручной просчет неприемлем).

К тестовому диагностированию относятся также методы приемочных испытаний, которые заключаются в выделении и проверке некоторых важных свойств ПО, интересующих пользователя-заказчика.

3. Программы, устойчивые к отказам.

Методы доказательства корректности программ и методы тестового диагностирования могут существенно уменьшить число ошибок, но не полностью ликвидировать эти ошибки. Даже в корректных программах, не содержащих ошибки, могут возникать отказы из-за неисправности аппаратуры.

ПО называется **устойчивым к отказам**, если оно не требует вмешательства извне для того, чтобы сохранить в течении заданного времени правильное выполнение своих функций при наличии определенного множества функциональных ошибок.

Функциональной ошибкой называется изменение значений одной или более логических переменных из-за неисправности аппаратуры.

Правильное выполнение означает, что результаты не содержат ошибок, и время выполнения не превосходит определенных пределов.

При создании программ, устойчивых к отказам, применяют методы информационной и программной избыточности, например, резервирование ПО.

В заключение перечислим основные проблемы диагностирования ПО:

1) разработка методов и средств автоматического доказательства корректности программ для широко используемых языков программирования;

2) создание удобных для тестового диагностирования моделей ошибок ПО, которые хорошо бы отражали накопленный опыт реальных ошибок;

3) разработка методов тестового диагностирования программ;

4) разработка методов не только обнаружения ошибок, но и методов поиска ошибок и их автоматического устранения;

5) создание методов разработки программ, устойчивых к отказам.

ТЕМА 10. Эргономические требования к информационным системам

Современные системы в большинстве своем функционируют при участии человека, поэтому расчет надежности реальных систем должен включать учет показателей надежности работы человека. В этом смысле система «человек—техника—среда» (ЧТС) является тем объектом, надежность которого необходимо рассматривать в комплексе. Основные принципы оценки надежности аппаратуры и программного обеспечения были рассмотрены выше.

Управление практически любыми машинами требует от оператора внимания, чтобы не пропустить появившийся сигнал или не отреагировать на сигнал, которого в действительности не было. Если при этом работа оператора связана с монотонной работой, например наблюдением, при котором в течение длительного времени ничего не происходит, то естественным образом снижается бдительность и готовность к действию. Известно, что при таком состоянии «бездействия» оператор может непроизвольно отвлечься на короткое время, но этого может оказаться достаточным, чтобы пропустить или поздно среагировать на критически важный сигнал. Но даже если за это время ничего не произошло, возврат к нормальному функционированию требует определенного времени.

Кроме того, при исследовании деятельности специалистов различных профессий выяснилось, что существует порог объема информации, воспринимаемой человеком, который превысить практически невозможно. Более того, существуют реальные границы восприятия информации. Например, человек слышит только сигналы частоты определенного диапазона и т. п., а повышение требований к человеческому организму в некоторых случаях не приводит к желаемому результату, а в других случаях приводит к переутомлению и последующему истощению организма. Таким образом, существует реальная проблема оценки надежности человека как звена системы ЧТС.

Надежность работы человека определяется как вероятность успешного выполнения им поставленной задачи на заданном этапе функционирования системы в течение заданного интервала времени при определенных требованиях к продолжительности выполнения работы. Ошибки по вине человека могут возникнуть в тех случаях, когда оператор стремится к достижению ошибочной цели, при наличии правильной цели выполняет неверные действия или поставленная цель не может быть достигнута из-за неправильных действий оператора, который бездействует в тот момент, когда его участие необходимо. Таким образом, ошибка человека может быть определена как несоответствие достигнутого результата конечной цели. Это может произойти по причине действия, совершенного неточно или неправильно, или выполнения запрещенного действия, что приводит в лучшем случае к невыполнению поставленной задачи, а в худшем может явиться причиной достаточно серьезных последствий, связанных с повреждением оборудования и т. п.

Классификация типов ошибок приводится в соответствующей литературе, однако известно, что большинство ошибок сводится к пространственным или

временным ошибкам оператора, связанным с расчетом времени, оценки скорости, неверного считывания контрольной информации, выбора ошибочного переключателя. Однако очень часто за ошибкой оператора стоят конструкторские, административные, организационные ошибки. При этом очевидно, что в любой системе, в которой присутствует человек, совершение ошибок

Человек в системе «человек—техника—среда» практически неизбежно. Также очевидно, что ненадежная работа человека в системе ЧТС значительно снижает надежность самой системы. Поэтому возникает задача минимизации числа человеческих ошибок и уменьшения последствий от их совершения.

В ГОСТ Р ИСО 6385—2007 указано, что в производственной системе на протекание рабочих процессов и обеспечение комфортных условий работы персонала оказывают влияние технологические, экономические, организационные, в том числе и человеческий, факторы. Человек является неотъемлемой частью данной системы, поэтому включение эргономических знаний в практику проектирования производственных систем в значительной мере должно быть направлено на обеспечение требований удобства работы и безопасности производственного персонала. Эргономический анализ имеющихся и проектируемых производственных систем указывает на необходимость повышения внимания к ключевой роли работника в обеспечении качества функционирования этих систем.

Поскольку нарушение в работе системы вызвано либо ошибкой человека, либо несоответствием взаимодействия между человеком и машиной вследствие неправильного проектирования, необходимо рассмотреть возможность уменьшения числа несоответствий путем адекватного проектирования систем автоматизации, создания адекватных условий труда и использования знаний о процессах, происходящих в СЧТС, для создания систем, максимально устойчивых к ошибкам.

Очень часто ошибки вызваны не низкой квалификацией персонала, а несоответствием конструктивных особенностей техники возможностям человека. Таким образом, еще на этапе проектирования сложных систем необходимо ответить на вопрос: есть ли возможность оценить ошибочные действия оператора при проектировании системы? То есть еще на этапе проектирования необходимо оценить вероятность ошибочных действий персонала. Поскольку ошибки будут возникать также и в случае напряженного ритма трудового процесса, большой нагрузки, то при оценке сложности системы необходимо исходить из возможностей человека воспринимать и запоминать информацию, скорости принятия решения, психологических особенностей, коммуникативных навыков.

Задачи, которые должны быть решены при создании новых технически сложных систем или модернизации старых, в первую очередь связаны с решением проблемы недостаточной эффективности СЧТС.

Неэффективность чаще всего связана с тем, что оператор совершает ошибки из-за несовершенства конструкции техники. Однако она также может быть связана и с работой оператора в условиях дефицита времени и информации, негативного воздействия внешних факторов: шум, вибрация, излучения, микроклимат, которые не были учтены при разработке системы.

Совершенно очевидно, что при проектировании, внедрении и эксплуатации систем «человек — техника — среда» должны учитываться реальные возможности человека, которому предстоит работать в системе. Именно на это направлены эргономические исследования трудовой деятельности человека, поскольку эргономичная система повышает безопасность, производительность и эффективность труда, улучшает условия работы и жизни человека и уменьшает вредное воздействие на его здоровье и эффективность деятельности (ГОСТ Р ЕН 614-1-2003).

ТЕМА 11. Качество информационных систем

Качество информационной системы — это совокупность свойств системы, обусловливающих возможность ее использования для удовлетворения определенных в соответствии с ее назначением потребностей. Количественные характеристики этих свойств определяются показателями, которые необходимо контролировать и учитывать. Основными показателями качества информационных систем являются надежность, достоверность, безопасность, эффективность.

Надежность - свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения.

Надежность - важнейшая характеристика качества любой системы, поэтому разработана специальная теория - теория надежности.

Теория надежности может быть определена как научная дисциплина, изучающая закономерности, которых следует придерживаться при разработке и эксплуатации систем для обеспечения оптимального уровня их надежности с минимальными затратами ресурсов.

Надежность - комплексное свойство системы; оно включает в себя более простые свойства, такие как безотказность, ремонтопригодность, долговечность и т д.

Безотказность - свойство системы сохранять работоспособное состояние в течение некоторого времени или наработки (наработка - продолжительность или объем работы системы).

Ремонтопригодность - свойство системы, заключающееся в приспособленности к предупреждению и обнаружению причин возникновения отказов, повреждений и поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов.

Долговечность - свойство системы сохранять при установленной системе технического обслуживания и ремонта работоспособное состояние до наступления предельного состояния, то есть такого момента, когда дальнейшее использование системы по назначению недопустимо или нецелесообразно.

Показатель надежности — это количественная характеристика одного или нескольких свойств, определяющих надежность системы. В основе большинства показателей надежности лежат оценки наработки системы, то есть продолжительности или объема работы, выполненной системой. Показатель надежности, относящийся к одному из свойств надежности, называется единичным. Комплексный показатель надежности характеризует несколько свойств, определяющих надежность системы.

Эффективность - это свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством. Показатели эффективности характеризуют степень приспособленности системы к выполнению поставленных перед нею задач и являются обобщающими

показателями оптимальности функционирования ИС, зависящими от локальных показателей, каковыми являются надежность, достоверность, безопасность.

Кардинальным обобщающим показателем является экономическая эффективность системы, характеризующая целесообразность произведенных на создание и функционирование системы затрат.

На сегодняшний день разработано много конкретных практических способов повышения надежности информационных систем.

Для обеспечения надежности технических средств чаще всего выполняется:

1) резервирование (дублирование) технических средств (компьютеров и их компонентов, сегментов сетей и т. д.);
2) использование стандартных протоколов работы устройств ИС;
3) применение специализированных технических средств защиты информации.

Для обеспечения надежности функционирования программного комплекса ИС выполняется:

1) тщательное тестирование программ, опытное исполнение программы с целью обнаружения в ней ошибок (обязательное условие эффективного тестирования - по крайней мере один раз выполнить все разветвления программы в каждом из возможных направлений);
2) использование стандартных протоколов, интерфейсов, библиотек процедур, лицензионных программных продуктов;
3) использование структурных методов для обеспечения надежной работы программных комплексов (иерархическое построение программ, разбиение программ на сравнительно независимые модули и т. д.);
4) изоляция параллельно работающих процессов, в результате чего ошибки в работе одной программы не влияют на работу операционной системы и других программ.

Надежность информационных систем не самоцель, а средство обеспечения своевременной и достоверной информации на ее выходе. Поэтому показатель достоверности функционирования имеет для информационных систем главенствующее значение.

Достоверность функционирования — свойство системы, обусловливающее безошибочность производимых ею преобразований информации. Достоверность функционирования информационной системы полностью определяется и измеряется достоверностью ее результатной информации.

Достоверность информации — это свойство информации отражать реально существующие объекты с необходимой точностью. Достоверность информации измеряется вероятностью того, что отражаемое информацией значение параметра отличается от истинного значения этого параметра в пределах необходимой точности.

Одним из наиболее действенных средств обеспечения достоверности информации в ИС является ее контроль. Контроль — процесс получения и обработки информации с целью оценки соответствия фактического состояния объекта предъявляемым к нему требованиям и выработки соответствующего управляющего решения.

Методы контроля достоверности информации, применяемые в ИС, весьма разнообразны. Классификация методов контроля может быть выполнена по большему числу признаков, в частности: по назначению, по уровню исследования информации, по способу реализации, по степени выявления и коррекции ошибок.

1. КЛАССИФИКАЦИЯ МЕТОДОВ КОНТРОЛЯ ДОСТОВЕРНОСТИ ПО НАЗНАЧЕНИЮ

Профилактический контроль и одна из наиболее распространенных его форм — тестовый контроль, предназначены для выявления состояния системы в целом и отдельных ее звеньев до включения системы в рабочий режим. Целью профилактического контроля, осуществляемого часто в утяжеленном режиме работы системы, является выявление и прогнозирование неисправностей в ее работе с последующим их устранением.

Рабочий контроль, или контроль в рабочем режиме, выполняется в процессе выполнения системой возложенных на нее функций. Он, в свою очередь, может быть разделен на функциональный контроль и контроль качества продукции. Функциональный контроль может преследовать цель либо только проверки работоспособности (отсутствия неисправностей) системы, либо, кроме того, установления места и причины неисправности (диагностический контроль). Контроль качества продукции является контролем достоверности информации как одного из важнейших показателей качества продукции выпускаемой ИС.

Генезисный контроль проводится для выяснения технического состояния системы в прошлые моменты времени с целью определения причин сбоев и отказов системы, имевших место в прошлом; сбора статистических данных об ошибках, их характере, величине и последствиях (экономических потерях) этих ошибок для ИС.

2. КЛАССИФИКАЦИЯ МЕТОДОВ КОНТРОЛЯ ДОСТОВЕРНОСТИ ПО УРОВНЮ ИССЛЕДОВАНИЯ ИНФОРМАЦИИ

Синтаксический контроль — это, по существу, контроль достоверности данных, не затрагивающий содержательного, смыслового аспекта информации. Предметом синтаксического контроля являются отдельные символы, реквизиты, показатели: допустимость их наличия, допустимость их кодовой структуры, взаимных сочетаний и порядка следования.

Семантический контроль оценивает смысловое содержание информации, ее логичность, непротиворечивость, согласованность, диапазон возможных значений параметров, отражаемых информацией, динамику их изменения.

Прагматический контроль определяет потребительную стоимость (полезность, ценность) информации для управления, своевременность и актуальность информации, ее полноту и доступность.

3. КЛАССИФИКАЦИЯ МЕТОДОВ КОНТРОЛЯ ДОСТОВЕРНОСТИ ПО СПОСОБУ РЕАЛИЗАЦИИ

Организационный контроль достоверности является одним из основных в ИС. Он представляет собой комплекс мероприятий, предназначенных для выявления ошибок на всех этапах участия эргатического звена в работе системы, причем обязательным элементом этих мероприятий является человек или коллектив людей.

Программный контроль основан на использовании специальных программ и логических методов проверки достоверности информации или правильности работы отдельных компонентов системы и всей системы в целом. Программный контроль, в свою очередь, подразделяется на программно-логический, алгоритмический и тестовый.

Программно-логический контроль базируется на использовании синтаксической или семантической избыточности; алгоритмический контроль использует как основу вспомогательный усеченный алгоритм преобразования информации, логически связанный с основным рабочим алгоритмом.

Аппаратный контроль реализуется посредством специально встроенных в систему дополнительных технических схем. Этот вид контроля также подразделяется на непрерывный и оперативный (аппаратно-логический) контроль достоверности, а также непрерывный контроль работоспособности.

4. КЛАССИФИКАЦИЯ МЕТОДОВ КОНТРОЛЯ ДОСТОВЕРНОСТИ ПО СТЕПЕНИ ВЫЯВЛЕНИЯ И КОРРЕКЦИИ ОШИБОК

Обнаруживающий фиксирует только сам факт наличия или отсутствия ошибки.

Локализующий позволяет определить как факт наличия, так и место ошибки (например, символ, реквизит и т. д.).

Исправляющий выполняет функции и обнаружения, и локализации, и исправления ошибки.

Библиографический список

1. Острейковский В. А. Теория надежности / В. А. Острейковский. – М.: Высшая школа, 2008. - 464 с.
2. Ушаков И. А. Курс теории надежности систем / И. А. Ушаков. – М.: Изд-во «Дрофа», 2008. - 240 с.
3. Дианов В. Н. Диагностика и надежность автоматических систем / В. Н. Дианов. – М.: Изд-во МГИУ, 2007. - 160 с.
4. Черкесов Г.Н. Надежность аппаратно-программных комплексов. Учебное пособие. – СПб.: Питер, 2005. – 479 с.

Примечание [M1]: Рекомендовано Министерством образования РФ в качестве учебного пособия по дисциплине «Надежность, эргономика и качество» для студентов вузов, обучающихся по направлению подготовки дипломированных специалистов 654600 «Информатика и вычислительная техника» и направлению подготовки бакалавров и магистров 552800 «Информатика и вычислительная техника»