Новосибирский государственный технический университет

Факультет: Мехатроники и автоматизации
Кафедра: Электротехнических комплексов

Малозёмов Б.В.

Конспект лекций
по дисциплине

Диагностика и надежность автоматизированных систем

Новосибирск-2014

СОДЕРЖАНИЕ

Предисловие

Проблема надёжности информационных систем (ИС) является комплексной, системотехнической. Производственный опыт и теоретические исследования свидетельствуют, что нельзя добиться значительного увеличения надёжности отдельными разрозненными мероприятиями. Совместное проведение многих мероприятий объединенных в систему не только увеличивает эффективность каждого из них, но и даёт возможность получить качественно новые результаты.

Надёжность ИС определяется надёжностью её элементов и аппаратуры, надёжностью программного обеспечения, управляющего выполнением вычислительного процесса, а также использованием средств контроля и восстановления системы. Пользователя компьютерной техники интересует только получение правильных результатов вычислений за заданное время. Для достижения этой цели необходимо, чтобы всё названные составляющие обладали необходимой надёжностью. Для разработки эффективной системы мероприятий по обеспечению надёжности ИС нужно ясное понимание студентами идей, лежащих в основе многих различных методов оценки и повышения надёжности, позволяющее им трезво оценить возможности и особенности применения этих методов.

Цель курса лекций «Надёжность информационных систем» – освещение вопросов, связанных с обеспечением высокой надёжности информационных систем. В лекциях изложены вопросы оценки и расчёта надёжности аппаратурных и программных средств ИС на основе статистических, структурных и эксплуатационных моделей, вопросы надёжности ПО, надежность ОУС, задачи оптимального резервирования ИС.

Данный курс базируется на знаниях общих и профилирующих дисциплин. Учебным планом для этой дисциплины отводится: общее количество лекционных часов – 36, практических часов – 18, лабораторных – 18 часов.

Надеюсь, что курс лекций по надёжности ИС будет полезен магистрам, аспирантам и широкому кругу специалистов, связанных с проектированием и разработкой высоконадёжных информационных и технических систем.

Лекция 1

Тема: Основные понятия надёжности информационных систем и пути её обеспечения

План

1. Основные определения и понятия надёжности технических систем (ИС).
2. Задачи теории надёжности, основные причины определяющие внимание к проблеме надёжности ИС.
3. Классификация отказов ИС, стандартизированные определения показателей надёжности.
4. Средства повышения и обеспечения надёжности. Перспективные методы обеспечения надёжности ИС.

Ключевые слова

Надёжность, информационные системы, классификация отказов, внезапный отказ, постепенный отказ, сбой, безотказность, сохраняемость, ремонтопригодность, восстанавливаемые системы, обслуживаемые, необслуживаемые, высоконадёжный элемент, резервирование, аппаратная избыточность, программное обеспечение, контроль, диагностика, встроенные средства, типовые элементы замены, самопроверяемые устройства, самовосстановление, отказоустойчивость, работоспособность.

Информационная система – это сложная человеко-машинная система, включающая в свой состав эргатические звенья, технические средства и программное обеспечение.

Использование современных компьютеров и компьютерных систем (КС) может иметь место при условии их достаточно надежной работы. Основными причинами, определяющими повышенное внимание к проблемам надежности являются:

- рост сложности аппаратуры и появление сложных высокопроизводительных компьютерных систем КС;
- медленный рост уровня надежности комплектующих элементов;
- увеличение важности выполняемой аппаратурой функций;
- усложнение условий эксплуатации и др.

Надежность компьютеров и КС определяется, с одной стороны, отсутствием отказов, сбоев и ошибок в работе устройств, с другой возможностью восстановления аппаратуры и вычислительного процесса.

Основными *задачами теории надежности* являются:

- методы анализа надежности элементов и систем;
- установление видов количественных показателей надежности;
- выработка методов аналитической оценки надежности;

- разработка методов оценки надежности по результатам испытаний;
- оптимизация надежности на стадиях разработки и эксплуатации.

При определении основных терминов и понятий в области надежности (например, отказ, восстановление, само понятие надежности и др.) будем следовать нормативно-техническим документам системе государственных стандартов «Надежность в технике», описываемая ГОСТ.24.701-86.

Основным понятием в теории надежности является понятие системы. Под *системой* понимают совокупность элементов, взаимодействующих между собой в процессе выполнения заданных функций. Например, в качестве систем могут рассматриваться КС, вычислительный комплекс, автоматическая система управления движением космического корабля, судна, микропроцессорная система и др.

Объекты, образующие системы представляют собой элементы системы. *Элементом* системы называют часть системы, которая имеет самостоятельную характеристику надежности, используемую при расчетах и выполняющую определенную функцию в интересах системы. Примерами элементов для систем, перечисленных выше, могут служить соответственно ЗУ-КС, мини-микро ЭВМ вычислительного комплекса, исполнительный механизм рулевого привода и т.д. Каждый из этих элементов можно рассматривать в качестве системы, состоящей из более мелких элементов.

Элементы и системы могут находится в двух состояниях: работоспособном и неработоспособном.

Работоспособным называется такое состояние системы (элемента), при котором они способны выполнить заданные функции, сохраняя значения заданных параметров в пределах установленных нормативно-технической документацией (НТД).

Неработоспособным называется состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не находится в переделах, установленных, нормативно-технической документацией.

Событие, заключающееся в нарушении работоспособности системы, т.е. в переходе её из работоспособного в неработоспособное состояние, называется *отказом*.

Отказы объектов могут классифицироваться по многим признакам, например по характеру возникновения, внешним проявлениям, способам обнаружения. Приведем классификацию отказов по основным признакам (табл. 1).

Таблица 1

Классификационный признак		Значение классификационного признака	Вид отказа
1	Характер изменения параметров объекта до возникновения отказов	Скачкообразное изменение одного или нескольких параметров	Внезапный отказ
		Постепенное изменение одного или нескольких параметров	Постепенный отказ

2	Взаимосвязь отказов	Отказ элемента объекта не обусловлен отказами других элементов объекта	Независимый отказ элемента
		Отказ элемента объекта обусловлен отказами других элементов объекта	Зависимый отказ элемента
3	Происхождение отказов	Нарушение норм и методов конструирования	Конструкционный отказ
		Нарушение процесса изготовления, ремонта, технологии	Производственный отказ
		Нарушение условия эксплуатации объекта	Эксплуатационный отказ
4	Устойчивость неработоспособного состояния (характер воздействия отказа)	Неработоспособность сохраняется устойчиво	Устойчивый отказ
		Неработоспособность сохраняется кратковременно, затем восстанавливается	Самоустраняющийся отказ (сбой)
		Неработоспособность одного и того же характера возникает и самоустраняется многократно	Перемежающийся отказ

При анализе надежности конкретного объекта классификация его отказов позволяет выявить причины отказов и найти пути повышения надежности. Отметим, что в общей массе отказов в вычислительных машинах и микропроцессорных системах преобладают *сбои*, т.е. *самоустраняющиеся отказы*.

Под *сбоем* логического элемента КС понимается непредусмотренное изменение состояния этого элемента, после которого работоспособность самовосстанавливается (без проведения ремонта). Сбои приводят к кратковременному нарушению работоспособности, они опасны для компьютеров, КС, любых ИС так как приводят к искажению информации и к неправильному функционированию системы.

На основании использования понятий работоспособности и отказа сформулируем понятие надежность [1, 2, 3].

Основные стандартизованные определения показателей надежности

Надежность – свойство объекта (ИС) сохранять во времени в установленных пределах способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортирования.

Надежность является комплексным свойством включающим в себя безотказность, ремонтопригодность и сохраняемость.

Безотказность – свойство системы или элемента непрерывно сохранять работоспособное состояние в течение некоторого времени или некоторой наработки.

Под наработкой понимают объем работы объекта (системы).

Сохраняемость – свойство системы непрерывно сохранять исправное, работоспособное состояние в течение всего времени хранения.

Ремонтопригодность – свойство системы или элемента, заключающееся в приспособлении к предупреждению, обнаружению и устранению причин возникновения отказов путем проведения ремонтов и технического обслуживания.

Объекты делятся на *восстанавливаемые* и *невосстанавливаемые*, в зависимости от того какое решение должно быть принято в случае отказа объекта.

Таким образом можно видеть, что понятие надежности является фундаментальным понятием, которое охватывает все стороны технической эксплуатации элементов и систем. В свою очередь надежность является составной частью более широкого понятия – эффективности.

Под эффективностью понимается свойство системы (элемента) выполнять заданные функции с требуемым качеством.

Средства повышения надежности ИС

В настоящее время, можно выделить несколько основных направлений работ по повышению надежности ИС и микропроцессорных систем [1,35,52].

1. В первую очередь надежность ИС достигается за счет использования в ней высоконадежных элементов. Это достигается применением в устройствах ИС интегральных схем с высокой степенью интеграции (интенсивность отказов в ИС $10^{-6} \div 10^{-8}$ 1/ч), использованием оптических элементов, а также внедрением новых типов печатных плат, контактных соединений, новых технологий ИС и т.д.
2. Вторым направлением повышения надежности являются обеспечение *оптимальных режимов* работы элементов. Большое значение при этом имеет выбор коэффициента нагрузки по тепловому, механическому и радиационному режиму. Режимы зависят от конструкции устройств, от принятых технических решений, которые необходимо учитывать в процессе проектирования.
3. Эффективным средством повышения надежности технических систем является введение избыточности или резервирования. *Резервирование* – применение дополнительных средств и возможностей с целью сохранения работоспособного состояния объекта при отказе одного или нескольких его элементов. В компьютерах, КС используются различные виды резервирования: структурное, временное, функциональное, информационное и программное.
4. Эффективным методом повышения надежности является *восстановление* отказавших устройств. Здесь необходимо решить задачи, связанные с обнаружением отказа и с поиском отказавших элементов. Эффективность диагностирования повышается при использовании автоматизированных систем контроля.

Одним из средств повышения надежности является уменьшение времени восстановления. Время восстановления сокращается за счет обеспечения доступности всех узлов устройства для осмотра, т.е. определяется ремонтопригодностью разрабатываемых конструкций. В настоящее время широко используется модульно-блочный принцип построения устройств, при которых замена отказавших элементов осуществляется путем замены целых блоков. Снятые блоки уже вне изделия подлежат восстановлению на специальных стендах с использованием контрольно-измерительных приборов.

5. Для повышения надежности компьютеров, КС, ИС необходимо обеспечить надежность программного обеспечения. Надежность программного обеспечения может быть увеличена за счет программного резервирования и использования средств автоматического контроля за правильностью выполнения вычислительного процесса. Наличие системы автоматического контроля способствует увеличению готовности и обслуживаемости ИС.

6. Одним из перспективных путей достижения высоких показателей надежности ИС является их построение на базе использования *самопроверяемых средств функционального диагностирования*, создание самопроверяемых устройств и отказоустойчивых систем.

Из всех перечисленных особо можно отметить проблему контроля и диагностирования.

Анализ надежности элементов ИС показывает, что примерно 40-45% всех отказов возникает из-за ошибок на этапе проектирования, 20% от ошибок, допущенных при производстве, 30% от неправильной эксплуатации и 5-10% от естественного износа и старения.

Рассмотрим основные методы обеспечения надежности на этапах жизненного цикла ИС, которые могут быть включены в программы по обеспечению надежности.

Этап составления технического задания. На этом этапе необходимо собрать все имеющиеся данные об аналогичных или близких реализованных системах, а также данные об условиях применения технических систем и требованиях предъявляемых к ним (функциям, выполняемым рассматриваемой системой).

Этап эскизного проектирования. На этапе эскизного проектирования выбирается элементная база, структура и организация разрабатываемой системы. Проводится предварительный расчет надежности, принимается решение о резервировании наименее надежных подсистем, а также решения о способах и организации технического обслуживания (профилактических и ремонтных работ). Исследуется вопрос о целесообразности и способах реализации методов автоматического восстановления и отказоустойчивости в системе.

Этапы технического и рабочего проектирования. На этих этапах проверяются и уточняются ранее принятые технические решения. Основой для этого служат данные о надежности, полученные на основании расчетов и

результаты экспериментов над моделями, макетами, опытными и промышленными образцами.

Разрабатывается программное обеспечение системы и проводится её проверка по тестам (путем имитационного моделирования на модели разрабатываемой ТС).

Этап производства. Здесь основным является технический контроль, охватывающий все стадии производственного процесса (входной контроль качества комплектующих изделий, соответствия тех. документациям печатных плат, блоков, устройств, схемных соединений и т.д.) и устранение недостатков в разработке системы.

Этап эксплуатации. На этом этапе важными являются контроль и обеспечение условий окружающей среды, квалификация и состав обслуживающего персонала, организация и проведение технического обслуживания и ремонтов в предусмотренном порядке.

В период эксплуатации продолжается сбор сведений об отказах аппаратуры и программного обеспечения. Эти сведения передаются разработчикам с целью устранения причин отказов и уточнения исходных данных для расчета надежности.

Контрольные вопросы и задания

1. Дайте определение понятию «надежность».
2. Перечислите основные задачи теории надежности.
3. В каких состояниях могут находится элементы и системы ИС?
4. Что такое отказ? Какой вид отказа преобладает в компьютерах и КС?
5. Какие свойства включает в себя надежность?
6. На какие виды делятся объекты ИС?
7. Определите существующие пути повышения надежности элементов и устройств ИС.
8. Назовите наиболее перспективный метод обеспечения надежности современных компьютеров?
9. В каких состояниях могут находится элементы и устройства ИС?
10. Какие свойства включает в себя надежность?

Литература: 1,2,3,6, 10.

Лекция 2

Тема: Показатели надёжности невосстанавливаемых информационных систем

План

1. Вероятностное описание элементов технических систем (ИС).
2. Понятие восстанавливаемых и невосстанавливаемых систем, области применения.
3. Количественные показатели надёжности невосстанавливаемых устройств ИС.
4. Расчетные формулы для статистической, вероятностной оценки параметров ИС.

Ключевые слова

Восстанавливаемые системы, невосстанавливаемые устройства, статистическая оценка, вероятностная оценка, вероятность безотказной работы, отказ, сбой, интенсивность отказа, частота отказа, наработка на отказ, наработка до отказа, вероятность отказа, приближенный расчет, точная оценка.

Показателями надежности называются количественные характеристики одного или нескольких свойств, составляющих надежность системы.

Отказы и сбои элементов и систем являются случайными событиями, поэтому теория вероятностей и математическая статистика – это основной аппарат, используемый при исследовании надежности, следовательно показатели надежности являются вероятностными показателями.

К числу наиболее широко применяемым количественным характеристикам надежности относятся [2, 9]:

- вероятность безотказной работы (ВБР) в течение определенного времени – $P(t)$;
- средняя наработка до первого отказа – $T_{ср.}$;
- вероятность отказа – $Q(t)$;
- наработка на отказ – $t_{ср.}$;
- частота отказов – $a(t)$;
- интенсивность отказов – $\lambda(t)$;
- интенсивность восстановления – μ;
- параметр потока отказов – $w(t)$;
- функция готовности – $K_г(t)$;
- коэффициент готовности – $K_г$;
- коэффициент оперативной готовности – $K_{о.г}$.

Выбор количественных характеристик надежности зависит от вида объекта, – восстанавливаемого или невосстанавливаемого.

Восстанавливаемыми называют такие объекты (ТС, их подсистемы, элементы), которые в процессе выполнения своих функций допускают ремонт. Если произойдет отказ такого объекта, то он вызовет прекращение функционирования объекта только на период устранения отказа. К таким изделиям относятся: компьютер, телевизор, блок питания, автомобиль и т.д.

Обслуживаемая система – система для которой предусматривается проведение регулярного технического обслуживания. *Необслуживаемая система* – система для которой не предусматривается проведение регулярного технического обслуживания.

Невосстанавливаемые объекты в процессе выполнения своих функций не допускают ремонта. Если происходит отказ такого объекта, то выполняемая операция будет сорвана и её необходимо начинать вновь, если возможно устранение отказа. К таким объектам относятся как объекты однократного действия (ракеты, управляемые снаряды, искусственные спутники Земли, системы подводной связи и т.п.), так и объекты многократного действия (некоторые системы навигационного комплекса судового оборудования, системы ПВО, системы управления воздушным движением, ответственными производственными процессами и т.д.)

Показатели надежности невосстанавливаемых элементов. Вероятность безотказной работы $P(t)$ выражает вероятность того, что невосстанавливаемый объект не откажет к моменту времени наработки t (наработка может быть выражена как календарное время, как время работы, как число циклов работы или в виде другой меры проделанной объектом работы). Показатель обладает следующими свойствами:

1. $P(0) = 1$ (предполагается, что до начала работы объект является безусловно работоспособным);
2. $\lim\limits_{t\to\infty} P(t) = 0$ (предполагается, что объект не может сохранять свою работоспособность неограниченно долго);
3. $dP(t)/dt \le 0$ [предполагается, что объект не может после отказа спонтанно восстанавливаться (для объектов, восстанавливаемых обслуживающим персоналом, этот показатель не используется)].

t – время, в течение которого определяется вероятность безотказной работы.

ВБР по статистическим данным об отказах оценивается выражением:

$$\hat{P}(t) = (No - n(t))/No, \qquad (1)$$

где No – число объектов в начале испытания;

$n(t)$ – число отказавших объектов за время t;

$\hat{P}(t)$ – статистическая оценка ВБР.

На практике более удобной характеристикой является вероятность отказа $Q(t)$.

Дополнение ВБР до единицы:

$$Q(t) = 1 - P(t) \qquad (2)$$

называется вероятностью отказа.

Вероятность отказа $Q(t)$ – вероятность того, что случайное время до отказа меньше заданного времени t. Отказ и безотказная работа являются событиями несовместимыми и противоположными, поэтому

$Q(t) = 1 - P(t)$, а статистическая оценка вероятности отказа равна:

$$\hat{Q}(t) = n(t) / No \qquad (3)$$

Функция $Q(t)$ совпадает с функцией распределения времени $F(t)$:

$$Q(t) = F(t) = \int_0^t f_t(x)\, dx, \qquad (4)$$

где $f_t(x)$ – функция плотности распределения времени до отказа;

x – переменная интегрирования.

Тогда показатель надежности [1]:

$$Q(t) = 1 - P(t) = 1 - \int_0^t f_t(x)\, dx = \int_t^\infty f_t(x)\, dx \qquad (5)$$

В качестве показателя надежности неудобно использовать функциональную зависимость, например, $P(t)$. Поэтому в технических условиях (ТУ) обычно задают отдельные ординаты (одну или две) функции $P(t)$ при значениях t, выбираемых из нормированного ряда t = 100; 500; 1000; 2000; 5000; 10000 ч.

Частота отказов представляет собой плотность распределения времени безотказной работы или производную от вероятности безотказной работы, поэтому

$$a(t) = Q'(t) = -P'(t). \qquad (6)$$

Для определения величины $a(t)$ используется следующая статистическая оценка:

$$\hat{a}(t) = n(\Delta t) / No \cdot \Delta t, \qquad (7)$$

где $n(\Delta t)$ – число отказавших объектов в интервале времени от (t-Δt/2) до (t+Δt/2), *No* – число объектов в начале испытания.

Между частотой отказов, вероятностью безотказной работы и вероятностью появления отказа имеются следующие зависимости:

$$Q(t) = \int_0^t a(t) \cdot dt, \qquad (8)$$

$$P(t) = 1 - \int_0^t a(t) \cdot dt. \qquad (9)$$

Интенсивность отказов $\lambda(t)$ выражает интенсивность процессов возникновения отказов. Вероятностная оценка этой характеристики находится из выражения

$$\lambda(t) = a(t) / P(t). \qquad (10)$$

Для определения величины $\lambda(t)$ используется следующая статистическая оценка

$$\hat{\lambda}(\mathrm{t}) = \frac{n(\Delta \mathrm{t})}{\mathrm{N}_{\mathrm{ср.}} \cdot \Delta \mathrm{t}}, \qquad (11)$$

где $N_{ср.}=(N_i+N_{i+1})/2$ – среднее число исправно работающих объектов в интервале времени Δt.

Интенсивность отказов и вероятность безотказной работы связаны между собой зависимостью:

$$P(\mathrm{t}) = e^{-\int_0^t \lambda(\mathrm{t}) \cdot dt} \qquad (12)$$

Если $\lambda(t)= \lambda=$const, то тогда

$P(t) = e^{-\lambda \cdot t}$ и $a(t) = \lambda \cdot e^{-\lambda \cdot t}$ соотношение характеризует экспоненциальное распределение безотказной работы.

Для высоконадежных систем, если

$P(t) \geq 0{,}99$, то $a(t) \approx \lambda(t)$.

Опыт эксплуатации ИС показывает, что интенсивность отказов $\lambda(t)$ в течение времени t изменяется как показано на рис. 1 как видно, функцию можно разделить на три участка. На первом участке $0 - t_1$ интенсивность отказов высока и уменьшается с течением времени. На этом участке

выявляются грубые дефекты производства и сам участок I носит название *участка приработки*.

Для блоков ИС длительность этого участка составляет десятки, иногда сотни часов.

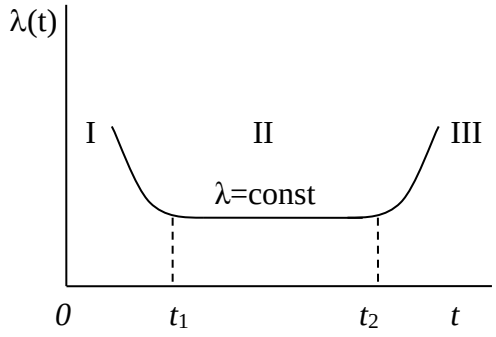


Рис. 1. Изменение интенсивности отказов $\lambda(t)$ во времени

Второй (II) участок t_1–t_2, участок нормальной эксплуатации, характерен тем, что интенсивность отказов имеет постоянное значение, длительность участка составляет тысяча и десятки тысяч часов.

На третьем участке (III) t_2–∞ из-за усиления процессов старения элементов интенсивность отказов начинает возрастать. Время t_2 может служить временем, при достижении которого аппаратура должна сниматься с эксплуатации

$$T_{ср} = M \cdot t = \int_0^{\infty} t \cdot f(x)dx = -t \cdot P(t)\Big|_0^{\infty} + \int_0^{\infty} P(x)dx \qquad (13)$$

Первый член в (1.13) стремится нулю, когда t=0, а также когда $t \to \infty$, так как получающаяся неопределенность $\lim_{t\to\infty} t \cdot P(t)$ при встречающихся на практике функциях $P(t)$ стремится к нулю. Следовательно,

$$T_{ср} = M[T] = \int_0^{\infty} t \cdot f(t) \cdot dt = -\int_0^{\infty} t \cdot dP(t) = -tP(t)\Big|_0^{\infty} + \int_0^{\infty} P(t)dt = \int_0^{\infty} P(t)dt$$

Средняя наработка до отказа (среднее время безотказной работы) представляет собой математическое ожидание наработки объекта до первого отказа, следовательно,

$$T_{ср.} = \int_0^{\infty} P(t) \cdot dt$$

Для экспоненциального закона распределения времени безотказной работы имеем

$$T_{ср.} = \int_0^{\infty} e^{-\lambda t} \cdot dt = \frac{1}{\lambda} \qquad (14)$$

Для определения средней наработки до отказа используется следующая статистическая оценка:

$$\hat{T}_{ср.} = \sum_{t=1}^{No} t_i / No, \qquad (15)$$

где t_i – время безотказной работы i-го объекта;

No – число испытуемых объектов.

Таким образом, рассмотренные характеристики позволяют достаточно полно оценить надежность невосстанавливаемых объектов. Они также позволяют оценить надежность восстанавливаемых изделий до первого отказа. Наличие нескольких критериев вовсе не означает, что нужно оценивать надежность объекта по всем критериям.

Интенсивность отказов – наиболее удобная характеристика надежности простейших элементов, так как она позволяет более просто вычислить количественные характеристики надежности сложной системы.

Наиболее целесообразным параметром надежности является вероятность безотказной работы, это объясняется следующими особенностями вероятности безотказной работы:

- она входит в качестве сомножителя в другие, более общие характеристики системы, например, в эффективность и стоимость;
- характеризует изменение надежности во времени;
- может быть получена расчетным путем в процессе проектирования системы и оценена в процессе её испытания.

Контрольные вопросы и задания

1. Назовите количественные характеристики надежности ИС. Какие из них относятся к показателям безотказности? ремонтопригодности?
2. Что характеризует коэффициент готовности системы?
3. В каких случаях целесообразно выбрать в качестве показателя надежности вероятность безотказной работы; наработку до отказа; наработку на отказ?
4. Как называется параметр надежности устройства ИС, который статистически оценивается по формуле

$$\hat{\lambda}(t) = n(\Delta t) / (N_{ср.} \cdot \Delta t)\,?$$

5. Оцените интенсивность отказов устройства состоящего из 10 интегральных схем, пяти конденсаторов, пяти резисторов, ста паек и одного разъема.
6. Определите параметр надежности, который при экспоненциальном распределении остается постоянной величиной.
7. Почему параметр $P(t)$ наиболее широко используется при оценке надежности ИС? Как ведет себя $P(t)$ с течением времени?
8. Какие объекты являются предметом надежностного анализа?
9. Дайте определение понятию «безотказность».
10. Что такое наработка на отказ?
11. Напишите формулу по которой частота отказов оценивается статистически.

Литература: 1,2,3,6

Лекция 3

Тема: Показатели надёжности восстанавливаемых устройств технических объектов ИС. Зависимость надёжности от времени.

План

1. Основные определения показателей надёжности восстанавливаемых устройств технических систем (ИС).
2. Количественные характеристики, расчётные статистические и вероятностные формулы для оценки восстанавливаемых объектов.
3. Специальные методы и рекомендации по выбору показателей надежности ИС.
4. Законы распределения в надёжности: экспоненциальный, нормальный, закон Рэлея и другие.
5. Графические зависимости ВБР от времени, интенсивностей и частоты отказов и другие от времени.

Ключевые слова

Восстанавливаемые устройства, количественные характеристики, вероятность отказа, время восстановления, интенсивность восстановления, поток отказа, коэффициент готовности, наработка на отказ, оперативная готовность, простой, ремонт, экспоненциальный закон, Рэлея, нормальный закон, параметры надежности, статистическая оценка, вероятностная оценка.

Показатели надежности восстанавливаемых объектов

К показателям надежности восстанавливаемых объектов могут быть отнесены: например параметр потока отказов, наработка на отказ, коэффициент готовности, коэффициент вынужденного простоя, интенсивность восстановления [1, 2, 3].

Параметром потока отказов называется отношение числа отказавших объектов в единицу времени к числу испытываемых объектов при условии, что все вышедшие из строя изделия заменяются исправными (новыми или отремонтированными).

Статистически этот показатель оценивается по следующей формуле:

$$\hat{\omega}(t) = n(\Delta t)/(N \cdot \Delta t), \qquad (1)$$

где $n(\Delta t)$ – число отказавших образцов в интервале времени от t-$\Delta t/2$ до t+$\Delta t/2$; N – число испытываемых образцов; Δt – интервал времени.

Для любого момента времени независимо от закона распределения времени безотказной работы параметр потока отказов больше чем частота отказов, т.е. $\omega(t)>a(t)$. Интенсивность восстановления оценивается

$$\mu = \frac{1}{t_в},$$

где $t_в$ – время восстановления.

Наработкой на отказ называется среднее значение времени между соседними отказами.

Эта характеристика определяется по статистическим данным об отказе по формуле

$$\hat{t}_{ср.} = (\sum_{i=1}^{n} t_i) / n, \qquad (2)$$

где t_i – время исправной работы изделия между (i-1)-м и i-м отказами;

n – число отказов за некоторое время t.

Наработка на отказ является характеристикой надежности, которая получила широкое распространение на практике.

Параметр потока отказов и наработка на отказ характеризуют надежность ремонтируемого изделия и не учитывает времени, необходимого на его восстановление. Поэтому они не характеризуют готовность изделия к выполнению своих функций в нужное время. Для этой цели вводятся такие критерии (признак, мерило по которому оценивается надежность объекта), как коэффициент готовности и коэффициент вынужденного простоя.

Коэффициент готовности $K_г$ используется в качестве показателя надежности, если кроме факта отказа необходимо учитывать время восстановления.

Коэффициент готовности определяется как вероятность того, что в произвольный заданный момент времени t объект находится в состоянии работоспособности (кроме планируемых периодов, в течение которых применение объекты по назначению не предусматривается)

$$K_г = t_{ср.}/(t_{ср.} + t_в), \qquad (3)$$

где $t_{ср.}$ – наработка на отказ, $t_в$ – среднее время восстановления.

Статистически оценка коэффициента готовности

$$\hat{K}_г(t) = N_в(t)/N_0$$

где $N_в(t)$ – число объектов, находящихся в рабочем состоянии в момент времени t.

Разность $N_в - N_0$ – выражает количество объектов, находящихся в момент времени t в состоянии восстановления (ремонта).

Для пользователей сложных информационных систем понятие их надежности ощущается по коэффициенту готовности системы $К_г$, то есть по отношению времени работоспособного состояния системы к времени её

незапланированного простоя. Для типичного современного сервера $К_г$=0,99, что означает примерно 3,5 суток простоя в год. За рубежом часто используется классификация систем по уровню надежности, показанная в табл.

Классификация систем по уровню надежности.

Таблица

Коэффициент готовности, $К_г$	Максимальное время простоя в год	Тип системы
0,99	3,5 сут	Обычная (Conventional)
0,999	8,5 ч	Высокой надежности (High availability)
0,9999	1 ч	Отказоустойчивая (Fault resilient)
0,99999	5 мин	Безотказная (Fault tolerant)

Коэффициент технического использования – отношение математического ожидания интервалов времени пребывания системы в работоспособном состоянии за некоторый период эксплуатации к сумме математических ожиданий интервалов времени пребывания системы в работоспособном состоянии, простоев, обусловленных техническим обслуживанием, и ремонтов за тот же период эксплуатации.

$$K_{\text{ти}} = \frac{T_{\text{ср.}}}{T_{\text{ср.}} + T_{\text{в}} + T_{\text{п}}}$$

где $T_{\text{п}}$ – время простоя системы, обусловленное выполнением планового технического обслуживания и ремонта, пересчитанное на один отказ.

Коэффициентом вынужденного простоя называется отношение времени восстановления к сумме времен наработки на отказ и времени восстановления взятых за один и тот же календарный срок.

$$K_п = t_в/(t_{ср.} + t_в), \qquad (4)$$

Коэффициент готовности и коэффициент вынужденного простоя связанны между собой зависимостью.

$$K_п = 1-K_г. \qquad (5)$$

Коэффициент оперативной готовности $К_{\text{о.г.}}$ – вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается, и, начиная с этого момента, будет работать безотказно в течение заданного интервала времени.

$$K_{о.г.} = \frac{T_{ср.}}{T_{ср.} + t_в} \cdot P(t_x, t), \qquad (6)$$

где $P(t_x,t)$ – условная вероятность безотказной работы системы на интервале $(t_x, t_x+ t)$ при условии, что в момент t_x система была работоспособна.

Выбор показателей надежности.

Показатели надежности в каждом конкретном случае необходимо выбирать так, чтобы они наилучшим образом характеризовали надежность объекта по его целевому назначению. Существуют специальные методики по выбору показателей надежности, приведем некоторые краткие рекомендации [1, 10, 37]:

1. Если невосстанавливаемый объект работает однократно в течение небольшого заданного отрезка времени $t_{зад.} << T_{ср.}$, то в качестве показателя надежности целесообразно выбрать вероятность безотказной работы $P(t_{зад.})$ за заданное время.

Этот же показатель используется в случае периодически обслуживаемых КС и их подсистем, например на борту самолета, когда во время полета ремонт невозможен. В этом случае показатель характеризует отсутствие отказов во время полета.

2. Если отказ невосстанавливаемого объекта не влечет за собой опасных последствий и объект эксплуатируется до наступления отказа, тогда целесообразно характеризовать его надежность через среднюю наработку до отказа $T_{ср.}$ (электромеханических устройств).

3. Если невосстанавливаемый объект характеризуется постоянством интенсивности отказов, тогда в качестве надежности целесообразно использовать её значение λ. Этот показатель используется для характеристики невосстанавливаемых электронных узлов (ИС и БИС).

4. Если время восстановления восстанавливаемого объекта мало по сравнению с временем безотказной работы целесообразно использовать показатели надежности $\omega(t)$ и $t_{ср.}$, когда $\omega(t)=const$.

Для ответственных управляющих технических систем, отказ которых влечет за собой тяжелые последствия, несмотря на скорость восстановления, целесообразно использовать в качестве показателя надежности параметр потока отказов $\omega(t)$ или наработку на отказ $t_{ср.}$ (если $\omega(t)=const$).

5. Если существенное значение имеет полезное время работы восстанавливаемого объекта, в качестве показателя надежности целесообразно использовать коэффициент готовности $K_г$.

Этот показатель применяется для универсальных КС, где существенное значение имеют потери машинного времени.

6. Если важное значение имеет безотказная работа в периоды выполнения операции, то как показатель надежности применяется коэффициент оперативной готовности.

Зависимость надежности от времени

Из рассмотренных выше выражений для оценки количественных характеристик надежности видно, что все характеристики, кроме средней наработки до первого отказа являются функциями времени. Время между соседними отказами для элементов аппаратуры является непрерывной случайной величиной, которая характеризуется некоторым законом распределения. Зависимость надежности от времени описывается с помощью математической модели надежности (ММН) – математического выражения (формулы, алгоритма, уравнения, системы уравнений), позволяющего определить показатели надежности. Простейшие ММН в виде формул носят название *статистических моделей распределения*. При исследовании надежности применяются следующие модели распределения: экспоненциальный, нормальный, Рэлея, Пуассона, Вейбулла и др. [1, 2, 3, 8].

Наиболее распространенной статистической моделью надежности является *экспоненциальная модель распределения времени до отказа*, по которой вероятность безотказной работы объекта выражается зависимостью

$$P_э(t) = e^{-\lambda \cdot t}, \qquad (7)$$

где λ – параметр модели.

Частота отказа при экспоненциальной модели

$$a_э(t) = -dP(t)/dt = \lambda \cdot e^{-\lambda \cdot t}. \qquad (8)$$

Функция интенсивности отказов при экспоненциальной модели

$$\lambda_э(t) = a_э(t)/P_э(t) = \lambda = const. \qquad (9)$$

Графики этих функций приведены на рис. 1.

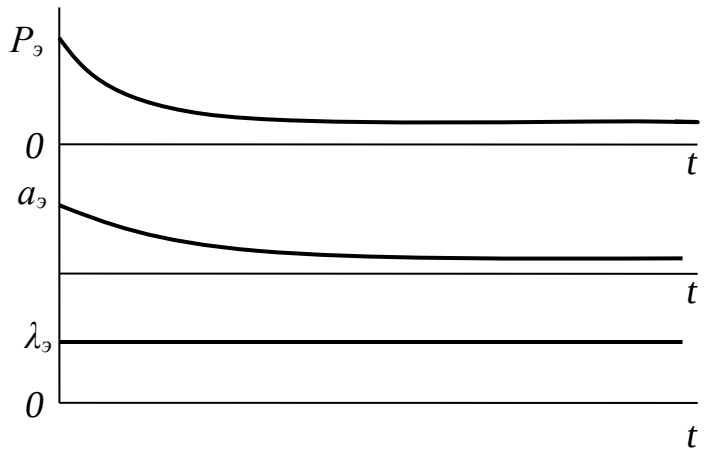


Рис. 1. График зависимости показателей надежности от времени для экспоненциальной модели распределения.

Наработка до отказа при экспоненциальной модели

$$T_{ср.} = \int_0^\infty e^{-\lambda \cdot t} \cdot dt = 1/\lambda \qquad (10)$$

Экспоненциальная модель может быть использована в случае, когда интенсивность отказов постоянная величина (λ=const), а также как характеристика достаточна сложных восстанавливаемых объектов в период эксплуатации II, если исключить период приработки I и период интенсивного старения III (рис. 1).

С экспоненциальной моделью тесно связана модель Пуассона. Она основана на представлении о потоке случайных событий, называемого пуассоновским, если выполнены условия стационарности, ординарности и отсутствия последействия.

Стационарность – свойство потока, выражающееся в том, что параметры потока не зависят от времени.

Ординарность – свойство потока, выражающееся в том, что в один и тот же момент времени может произойти только одно событие.

Отсутствие последействия – свойство потока, выражающееся в том, что вероятность наступления данного события не зависит от того, когда произошли предыдущие события и сколько их было.

Таким образом модель Пуассона позволяет выразить вероятность $P(t, n)$ того, что на заданном интервале времени произошло равно n событий (отказов), если время между отдельными событиями (отказами) распределено экспоненциально с параметром λ. По модели Пуассона

$$P(t, n) = \frac{(\lambda \cdot t)^n}{n!} \cdot e^{-\lambda \cdot t} \qquad (11)$$

Модель Вейбулла находит практическое применение благодаря своей простоте и гибкости, так как в зависимости от значений параметров характер модели видоизменяется в широких пределах. Модель надежности Вейбулла, называемая также *моделью Вейбулла-Гнеденко*, была предложена шведским ученым В. Вейбуллом в качестве модели прочности материалов, а затем обоснована математически российским ученым Б.В. Гнеденко. Вероятность безотказной работы по модели надежности Вейбулла выражается формулой [1, 8].

$$P_B = e^{-\alpha \cdot t^{\beta}}, \qquad (12)$$

где α и β – параметры модели.

Ориентировочно значение β=0,2÷0,4 для электронных устройств с убывающей функцией интенсивности отказов и β=1,2÷1,4 для механических устройств и возрастающей функцией интенсивности отказов.

Пример прогнозирования вероятности безотказной работы КС.

Пусть вероятность безотказной работы КС за t=1000 ч. равна P=0,99, составим прогноз вероятности безотказной работы этой же КС через 10^5 ч. работы без обслуживания.

В случае экспоненциальной модели интенсивность отказов КС

$$\lambda = \frac{dP/dt}{P} \approx 10^{-5} 1/ч\,.$$

В случае модели Вейбулла при β=0,5

$$\alpha = -\frac{\ln P_B(t)}{t^{\beta}} \approx 0{,}000316.$$

Следовательно, через 10^5 ч работы вероятность безотказной работы КС, прогнозированной по экспоненциальной модели, равна

$$P_э = e^{-10^{-5} \cdot 10^5} \approx 0{,}37\,.$$

Прогноз по модели Вейбулла

$$P_B = e^{-0{,}000316 10^{2{,}5}} \approx 0{,}905.$$

Следовательно, выбор правильной модели надежности не безразличен для практики.

Нормальное распределение и модель Рэлея используют для описания таких систем и устройств, которые подвержены действию износа, здесь величина интенсивности $\lambda(t)$ монотонно возрастает.

Выбор модели надежности – сложная научно-техническая проблема. Она может быть удовлетворительно решена стандартными методами математической статистики, если имеется большой статистический материал об отказах исследуемых объектов. Из-за высокой надежности КС и их компонентов, как правило, статистических данных об отказах немного. В последнем случае при выборе модели руководствуются результатами ускоренных испытаний, проводимыми в утяжеленных условиях работы объекта, физическими соображениями, предыдущим опытом.

В случае приближенных оценок часто выбирается экспоненциальная модель как наиболее удобная с точки зрения аналитических преобразований. Экспоненциальную модель рекомендуется применить при выполнении расчетов надежности в случае отсутствия других исходных данных для расчета, кроме интенсивности отказов. В случае наличия более полных исходных данных целесообразно пользоваться другой, более точной моделью, например моделью Вейбулла.

Контрольные вопросы и задания

1. Что характеризует коэффициент готовности системы?
2. В каких случаях целесообразно выбрать в качестве показателя надежности вероятность безотказной работы; наработку до отказа; наработку на отказ?
3. Каким соотношением связаны коэффициент готовности компьютерного устройства – $К_г$ и коэффициент простоя – $К_п$?
4. Какой показатель ремонтопригодности характеризующий надежность объекта, рекомендуется использовать, если важное значение имеет безотказная работа?
5. Какую формулу необходимо использовать при расчете коэффициента простоя?
6. Дайте определение коэффициента готовности системы.
7. Что такое поток отказов?
8. Назовите известные методы расчета восстанавливаемых систем?
9. Как оценить время восстановления системы?
10. Какие законы распределения используются в надежности.

Литература: 1,2,3,6, 11.

Лекция 4

Тема: Методика оценки безотказности нерезервированных систем

План

1. Определение цели расчета надёжности ИС и их подсистем на этапе проектирования.
2. Методика и алгоритм оценки параметров безотказности для нерезервированных систем с последовательным соединением элементов.
3. Расчетные формулы оценки характеристик безотказности нерезервированных объектов.
4. Значение интенсивностей отказов для компонент ИС.

Ключевые слова

Надёжность, методика, алгоритм, оценка параметров, характеристики надёжности, безотказность, последовательное соединение, нерезервированная система, интенсивность отказов, компоненты ИС, внезапный отказ.

Целью расчета надежности КС и их подсистем на этапе проектирования является [1, 2, 3, 6]:

- сравнение вариантов при выборе технического решения;
- получение приближенных оценок показателей надежности разрабатываемой ИС или подсистем (ЭВМ или блоков ЭВМ).

Расчеты для оценки уровней надежности объектов выполняются приближенным методами, т.к. исходные данные о надежности весьма приближенные. В то же время сравнительные расчеты надежности целесообразно выполнить по точным методам, так как приближенные оценки не могут улавливать разницу в надежности тех или других технических решений.

Методика оценки безотказности устройств ИС включает в себя следующие моменты:

- определение типа элемента и его характеристик;
- выбор метода расчета с последующим подбором определенных номограмм, таблиц, графиков или поправочных коэффициентов (вибрации, ударные нагрузки, температура, высота и т.д.);
- определение электрических нагрузок и влияния внешней среды на каждой элемент;
- определение по таблице или графику интенсивности отказа каждого элемента;

- суммирование всех интенсивностей отказов для определения интенсивности отказов изделия.

Расчет и оценка надежности устройств ИС и машин проводится в следующем порядке.

1. Формируется понятие отказа для рассматриваемого устройства и его отдельных составных частей.

Прежде чем поступить к расчету надежности, необходимо четко сформулировать, что следует понимать под отказом устройства, а затем уже выбирать число элементов, которое должно быть учтено при расчете вероятности исправной работы или при расчете других количественных характеристик надежности (учитывать только те элементы, выход из строя которых приводит к отказу системы).

2. На основании анализа структуры устройства определяется основные и вспомогательные блоки устройства.
3. *Составляется схема расчета надежности*.

Схему расчета необходимо составить таким образом, чтобы элементами расчета были конструктивно оформленные блоки. В устройствах в которых отсутствует элементная избыточность (т.е. нерезервированные системы), структурная схема расчета имеет вид последовательного соединения (рис. 1).

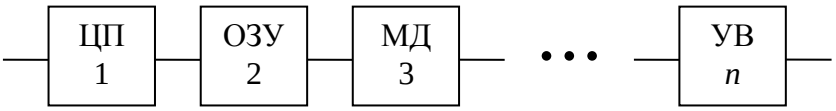


Рис. 1. Структурная схема расчета надежности

Пусть ИС состоит из n – элементов. Все элементы системы имеют свое функциональное назначение, следовательно здесь отказ любого элемента влечет за собой отказ системы. Схема расчета надежности будет представлять собой *основное соединение*.

4. *Выбирается метод расчета надежности и производится оценка безотказности устройства* по внезапным отказам.

В соответствии с видом расчета выбираются расчетные формулы и для определения интенсивности отказов изделия по таблицам определяются величины интенсивности отказов элементов.

Расчет надежности конструктивных единиц нерезервированных систем производится суммированием интенсивностей отказов.

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

а среднее время безотказной работы

$$T_{ср.} = \frac{1}{\sum_{i=1}^{n} \lambda_i(t)} .$$

Если система содержит N_i – элементов i-типа, а n_1 означает количество разновидностей элементов системы, то

$$\lambda_c(t) = \sum_{i=1}^{n_1} N_i \cdot \lambda_i \cdot (t),$$

где n_1 – число типов элементов, N_i – число элементов i-типа.

Для определения интенсивности отказов типового элемента замены (ТЭЗ-ов) суммируются интенсивности отказов входящих в него ИС, паек, разъемов.

Для определения надежности стойки суммируются интенсивности отказов входящих в нее панелей и других компонентов.

Интенсивность отказов компьютера определяется суммированием интенсивностей отказов входящих в её состав подсистем, стоек и других составляющих конструкций.

Если оценивается надежность не только аппаратуры, но всей ИС с учетом надежности программного обеспечения (ПО), необходимо к интенсивности отказов аппаратуры прибавлять также и интенсивность отказов ПО.

Вероятность безотказной работы группы элементов при условии, что отказы элементов независимы, равна произведению вероятностей безотказной работы её элементов.

$$P_c(t) = \prod_{i=1}^{n} P_i(t),$$

где $P_i(t)$ – вероятность безотказной работы i-го элемента; n – число элементов, имеющих основное соединение.

Для экспоненциального закона надежности ВБР определяется по формуле

$$P_c(t) = \prod_{i=1}^{n} e^{-\lambda_i \cdot t} = \exp(-t \cdot \sum_{i=1}^{n} \lambda_i) .$$

Определение интенсивности отказов элементов осуществляется путем обработки статистических данных по результатам испытаний и эксплуатации.

Приведем некоторые данные об интенсивностях отказов компонентов ИС (табл. 1). Приведенные цифры необходимо умножить на 10^{-6}, чтобы получить значения интенсивностей отказов на час.

Таблица 1

Компонент	**Интенсивность отказов $\lambda \times 10^{-6}$ 1/ч**	**Компонент**	**Интенсивность отказов $\lambda \times 10^{-6}$ 1/ч**
ИС	0,1	разъем	2,0-3,5
диод	0,2-0,5	сердечник	0,00001
транзистор	0,05-0,3	выключатель	0,2-0,5
конденсатор	0,002-0,04	память емкости 4 Кслов	100
резистор	0,01-0,1	память емкостью 48 Кслов	300
трансформатор	0,1-0,2	контроллер пишущий машинки	10
пайка	0,0001	устройство ввода с перфиленты	250
пишущая машинка	1000	контроллер устройства ввода	10
память на дисках	250	печатающее устройство	420
память на МЛ	350	контроллер печатающего устройства	15
контроллер памяти на дисках	15		

5. *Рассчитываются количественные характеристики надежности*.

Данные расчеты заносятся в итоговые таблицы или приводятся в виде графиков. Расчеты оформляются в виде технического отчета.

Отчет должен содержать:

а) структурную схему надежности системы с кратким объяснительным текстом;

б) формулировку понятия отказа системы;

в) расчетные формулы для количественных характеристик надежности;

г) расчет количественных характеристик надежности;

д) оценку точности расчета;

е) выводы и рекомендации.

Контрольные вопросы и задания

1. В чем суть методики оценки безотказности нерезервированных систем?
2. Определите параметр надежности, который при экспоненциальном распределении остается постоянной величиной.
3. Составьте структурную схему надежности компьютера, состоящего из пяти устройств.
4. Перечислите основные моменты методики оценки надежности ИС.
5. Как определить интенсивность отказов ТЭЗ устройств ИС?

6. Что происходит в устройстве, структурная схема надежности которого имеет основное соединение, если один из элементов отказал?
7. Какова интенсивность отказов современного процессора?

Литература: 1,2,3,6, 8.

Лекция 5

Тема: Надёжность невосстанавливаемых и нерезервированных информационных систем

План

1. Расчетные формулы характеристик надёжности при основном соединение элементов ИС.
2. Прикидочный и ориентировочный методы расчета количественных характеристик устройств ИС.
3. Окончательный метод расчета надёжности ИС. Основные допущения и учёт режимов работы при окончательной расчете.
4. Применение перечисленных видов расчета на различных этапах проектирование ИС.

Ключевые слова

Характеристика надёжности, основное соединение, прикидочный расчет, ориентированный расчет, окончательный расчет, количественные параметры, режим работы, нерезервированная система, этап проектирования, внешние воздействия.

Рассмотрим расчет характеристик надежности невосстанавливаемых изделий при основном соединении элементов.

Если отказ технического устройства наступает при отказе одного из его элементов такое устройство имеет основное соединение элементов. При расчете надежности таких устройств предполагают, что отказ элемента является событием случайным и независимым.

Тогда вероятность безотказной работы равна произведению вероятностей безотказной работы её элементов в течение времени *t*. Так как ВБР элементов в течение времени *t* можно выразить через интенсивность отказов, то расчетные формулы для ВБР устройства при основном соединении элементов можно записать следующим образом:

$$P_C(t) = P_1(t) \cdot P_2(t) \ldots P_N(t) = \prod_{i=1}^{N} P_i(t), \qquad (1)$$

$$P_C(t) = \exp(-\int_0^t \lambda_1(t)dt) \exp(-\int_0^t \lambda_2(t)dt) \ldots \exp(-\int_0^t \lambda_N(t)dt) = \\ = \exp(-\sum_{i=1}^{N} \int_0^t \lambda_i(t)dt), \qquad (2)$$

где N – число элементов.

Выражения (2) наиболее общие. Они позволяют определить ВБР изделий до первого отказа при любом законе изменения интенсивности отказов во времени.

На практике часто интенсивность отказов изделий является величиной постоянной. При этом время возникновения отказов обычно подчинено экспоненциальному закону распределения, т.е. для нормального периода работы аппаратуры справедливо условие λ=const.

В этом случае выражения для количественных характеристик примут вид:

$$P_c(t) = e^{-\lambda_c \cdot t} = e^{-t/T_{cp.c.}}, \qquad \lambda_c = \sum_{i=1}^{N} \lambda_i ,$$

$$a_c(t) = \lambda_c e^{-\lambda_c \cdot t}, \qquad T_{cp.c.} = 1/\lambda_c .$$

Если все элементы данного типа равнонадежны, интенсивность отказов системы будет

$$\lambda_c = \sum_{i=1}^{r} N_i \lambda_i ,$$

где N_i – число элементов i-го типа;

r – число типов элементов.

На практике очень часто приходится вычислять вероятность безотказной работы высоконадежных систем. При этом произведение $\lambda_c \cdot t << 1$ значительно меньше единицы, а ВБР близка к единице. В этом случае, разложив $e^{-\lambda_c \cdot t}$ в ряд и ограничившись первыми двумя членами, с высокой степенью точности можно вычислить $P(t)$.

Тогда основные количественные характеристики надежности можно с достаточной для практики точностью вычислить по следующим приближенным формулам:

$$P_c(t) = 1 - t \cdot \sum_{i=1}^{r} N_i \lambda_i = 1 - \lambda_c \cdot t , \qquad (3)$$

$$\lambda_c = \sum_{i=1}^{r} N_i \lambda_i ,$$

$$T_c = 1/\sum_{i=1}^{r} N_i \lambda_i = 1/\lambda_c , \quad a(t) \approx \lambda_c (1 - \lambda_c t) \quad . \qquad (4)$$

Вычисление количественных характеристик надежности по приближенным формулам не дает больших ошибок для систем, ВБР которых превышает 0,9, т.е. для $\lambda \cdot t \le 0{,}1$.

При расчете надежности систем часто приходится перемножать ВБР отдельных элементов расчета, возводить их в степень и извлекать корни.

При вычислениях $P(t)$, близких к единице, эти вычисления можно с достаточной для практики точностью выполнять по следующим приближенным формулам:

$$P_1(t)P_2(t)...P_N(t) \approx 1 - \sum_{i=1}^{N} q_i(t), \quad (5)$$

$$P_i^N(t) = 1 - Nq_i(t), \quad (6)$$

$$\sqrt[N]{P_i(t)} = 1 - q_i(t)/N, \quad (7)$$

где $q_i(t)$ – вероятность отказа i-го блока.

В зависимости от полноты учета факторов, влияющих на работу изделия, различают прикидочный, ориентировочный и окончательный расчет надежности.

Прикидочный расчет надежности.

Прикидочный расчет основывается на следующих допущениях:

- все элементы изделия равнонадежны;
- опасности отказов всех элементов изделия не зависят от времени, т.е. $\lambda_i = const$;
- отказ любого элемента приводит к отказу всего изделия.

Прикидочный расчет надежности применяется в следующих случаях:

1) при проверке требований по надежности, выдвинутых заказчиком в техническом задании (ТЗ) на проектирование изделия;
2) при расчете нормативных данных по надежности отдельных блоков, устройств и приборов системы (расчет норм надежности отдельных частей системы);
3) для определения минимально допустимого уровня надежности элементов проектируемого изделия;
4) при сравнительной оценке надежности отдельных вариантов изделия на этапах эскизного проектирования.

Прикидочный расчет надежности позволяет судить о *принципиальной возможности* обеспечения требуемой надежности изделия.

Характеристики надежности рассчитываются по вышеприведенным формулам, при этом $\lambda_c = N \cdot \lambda_{экв.}$, где $\lambda_{экв.}$ – эквивалентное значение интенсивности отказов элементов, входящих в изделие.

Ориентировочный расчет надежности.

Ориентировочный расчет надежности учитывает влияние на надежность только количества и типов примененных элементов и основывается на следующих допущениях:

- все элементы данного типа равнонадежны, т.е. величины интенсивности отказов (λ_i) для этих элементов одинаковы;
- все элементы работают в номинальном (нормальном) режиме, предусмотренном техническими условиями;

- интенсивности отказов всех элементов не зависят от времени, т.е. в течение срока службы у элементов, входящих в изделие, отсутствует старение и износ, следовательно, $\lambda_i(t)=const$;
- отказы элементов изделия являются событиями случайными и независимыми;
- все элементы изделия работают одновременно.

Для определения надежности изделия необходимо знать:

1) вид соединения элементов расчета надежности;
2) типы элементов, входящих в изделие, и число элементов каждого типа;
3) величины интенсивности отказов элементов λ_i, входящие в изделие. Выбор λ_i для каждого типа элементов производится по соответствующим таблицам.

Таким образом, при ориентировочном расчете надежности достаточно знать *структуру* системы, номенклатуру примененных элементов и их количество.

Ориентировочный метод расчета надежности используется на этапе эскизного проектирования после разработки принципиальных электрических схем изделий.

Этот расчет позволяет определить рациональный состав элементов изделий и наметить пути повышения надежности изделия на стадии эскизного проектирования и проводится по формулам приведенным выше.

Расчет надежности с учетом режимов работы элементов (*окончательный*).

Окончательный расчет надежности изделия выполняется тогда, когда известны реальные режимы работы элементов после испытания в лабораторных условиях макетов и основных узлов изделия.

Элементы изделия находятся обычно в различных режимах работы, сильно отличающихся от номинальной величины. Это влияет на надежность как изделия в целом, так и отдельных его составляющих частей. Выполнение окончательного расчета надежности возможно только при наличии данных о коэффициентах нагрузки отдельных элементов и при наличии графиков зависимости интенсивности отказов элементов от их *электрической нагрузки, температуры* окружающей среды и других факторов, т.е. для окончательного расчета необходимо знать зависимости

$$\lambda_c = f(K_н, T^0, \ldots)$$

Эти зависимости приводятся в виде графиков либо их можно рассчитывать с помощью так называемых поправочных коэффициентов интенсивности отказов $\Delta\lambda_{K_н}\Delta\lambda_T$, позволяющих учесть влияние различных факторов на надежность изделия.

Для определения надежности изделия необходимо знать:

1) число элементов с разбивкой их по типам и режимам работы;

2) зависимости интенсивности отказов элементов λ_i от электрического режима работы и заданных внешних условий;
3) структуру системы.

В общем случае λ_i зависит от следующих воздействующих факторов: *электрического режима* работы данного элемента; окружающей *температуры*; *вибрационных* воздействий; механических *ударов*; линейных *ускорений*; *влажности*; воздействия *биологических факторов* (грибок, плесень, насекомые); давления; облучения и ряда других возможных факторов.

При разработке и изготовлении элементов обычно предусматриваются определенные «нормальные» условия работы: температура $+25\pm10^0$C, номинальный электрический режим, относительная влажность 60±20%, отсутствие механических перегрузок и т.д. Интенсивность отказов элементов в номинальном режиме эксплуатации называется номинальной интенсивностью отказов λ_{0i}.

Интенсивность отказов элементов при эксплуатации в реальных условиях λ_i равна номинальной интенсивности отказов λ_{0i}, умноженной на поправочные коэффициенты α_i и k_i. Поправочный коэффициент интенсивности отказов $\alpha_i = f(t^0, K_н)$ учитывает влияние окружающей температуры и электрической нагрузки, поправочный коэффициент интенсивности отказов $k_i = f(j, \varphi)$ – тип воздействия, главным образом механические перегрузки и относительную влажность окружающего воздуха.

Графики $\alpha_i = f(t^0, K_н)$ и $k_i = f(j, \varphi)$ приведены в справочниках по расчету надежности (Ушаков И.А., Половко А.М.).

Окончательный расчет надежности применяется на этапе технического проектирования изделия. Поправочные коэффициенты в зависимости от воздействий механических факторов, влажности, температуры и высоты приведены в табл. 1.

Таблица 1

Условия эксплуатации аппаратуры	Вибрация k_1	Ударная нагрузка k_2	Сумма воз. $k_1 \cdot k_2$
1. Лабораторные	1,0	1,0	1,0
2. Стационарные (полевые)	1,04	1,03	1,07
3. Железнодорож	1,4	1,1	1,54
4. Самолетные и т.д.	1,46	1,13	1,65

Влажность	Температура	Поправочный коээфициент k_i
60-70	20-40	1,0
90-98	20-25	2,0
90-120	30-40	2,5

Высота км	Поправочные коэффициенты k_i
0-1	1,0
1-2	1,05
2-3	1,1
3-5	1,14
5-6	1,16
⋮	⋮
30-40	1,45

При расчете изделие расчленяется на отдельные конструктивно самостоятельные части. Расчет производится последовательно от простого сложному.

Контрольные вопросы и задания

1. Напишите выражение по которой рассчитывается вероятность безотказной работы при последовательном соединение элементов ИС.
2. Какие приближенные формулы используются при расчете наработки на отказ и частоты отказов?
3. На каких допущениях основывается прикидочный расчет надежности?
4. В каких случаях используется ориентировочный расчет?
5. При каком методе расчета надежности учитываются режимы работы элементов ИС?
6. Что такое коэффициент нагрузки?
7. На каком этапе проектирования устройств ИС используется окончательный расчет надежности?
8. Приведите графическую зависимость $\lambda(t)$ от времени и объясните какой участок имеет $\lambda(t)=const$.

Литература: 1,2,3,5,10.

Лекция 6
Тема: Структурное резервирование и его виды

План

1. Классификация структурного резервирования, основные определения.
2. Основные схемы расчета надёжности по способу включения резервных элементов: постоянное, раздельное, замещением, скользящее.
3. Виды резервных элементов и режимы работы при нагруженном, облегченном и ненагруженном резервах.
4. Расчетно-логическая схема структурного резервирования сложной системы.
5. Организация резерва на уровне элементов, устройств и систем ИС.

Ключевые слова

Резервирование, избыточность, схема расчета, цифровое устройство, постоянное резервирование, раздельное резервирование, резервирование замещением, нагруженный резерв, ненагруженый резерв, режимы работы, скользящий резерв, переключающая схема, надёжность, безотказность.

Резервированием называют метод повышения надежности объекта путем введения избыточности. Задача введения избыточности – обеспечить нормальное функционирование системы после возникновения отказов в ее элементах.

Резервирование может быть структурным, информационным, временным, программным. Информационное резервирование предусматривает использование избыточной информации. Временное резервирование – использование избыточного времени. Программное резервирование – избыточных программ.

Структурное резервирование заключается в том, что в минимально необходимый вариант системы, элементы которой называются основными, вводятся дополнительные элементы и устройства, либо вместо одной системы предусматривается использование нескольких идентичных систем. При этом избыточные резервные структурные элементы берут на себя выполнение рабочих функций при отказе основных элементов [1, 2, 3, 5].

Перечисленные виды резервирования могут быть применены либо к системе в целом, либо к отдельным ее элементам или их группам.

На практике большое распространение получило структурное резервирование (рис. 1).

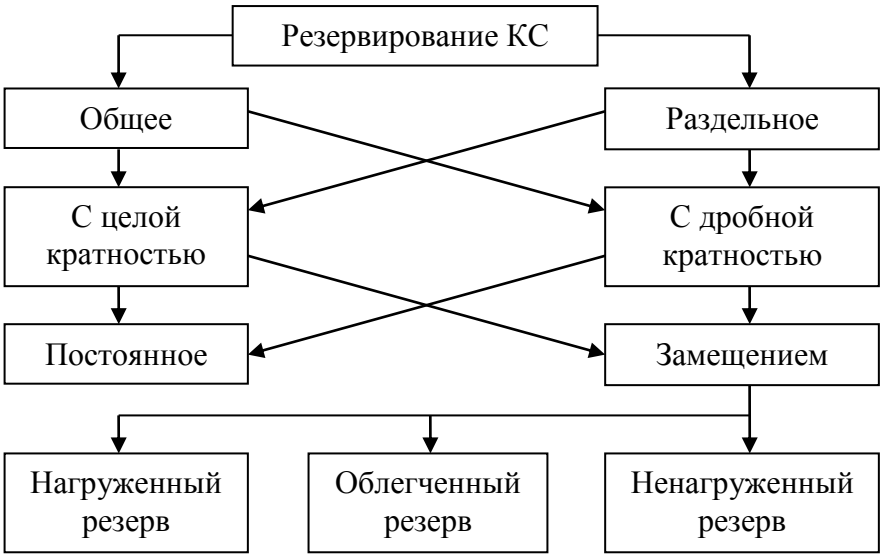


Рис. 1. Способы резервирования КС

По схеме включения резервных элементов различают постоянное, раздельное резервирование, резервирование с замещением и скользящее резервирование.

Постоянное резервирование – это такое резервирование, при котором резервные элементы участвуют в функционировании объекта наравне с основными (рис. 2).

Для постоянного резервирования в случае отказа основного элемента не требуется специальных устройств, вводящих в действие резервный элемент, так как он вводится в действие одновременно с основными.

Основным параметром резервирования является его *кратность* (степень избыточности). Под кратностью резервирования m понимается отношение числа резервных объектов к числу резервируемых (основных).

Раздельным резервированием называется метод повышения надежности, при котором резервируются отдельные части объекта (рис. 2.3).

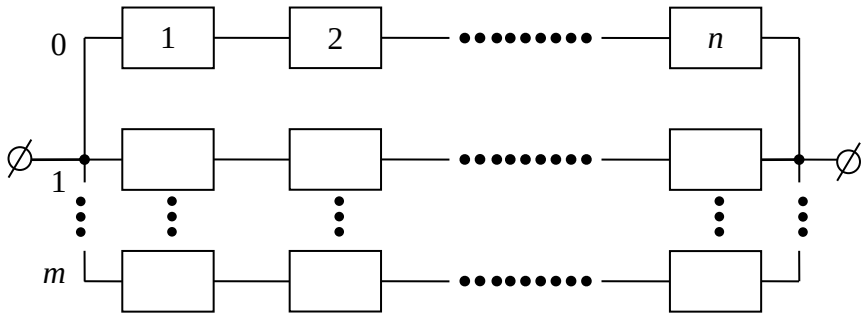


Рис. 2. Общее резервирование и постоянное включение резерва с постоянно включенным резервом.

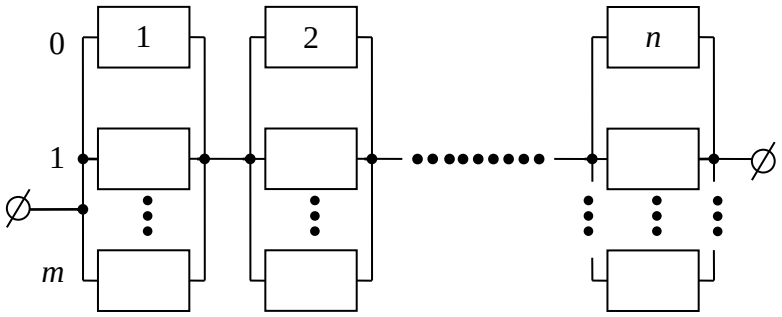


Рис. 3. Раздельное резервирование с постоянно включенным резервом

Резервирование замещением – это резервирование, при котором функции основного элемента передаются резервному только после отказа основного (рис. 4 а, б). При использовании резервирования замещением необходимы контролирующие и переключающие устройства для обнаружения факта отказа основного элемента и переключения его с основного на резервный.

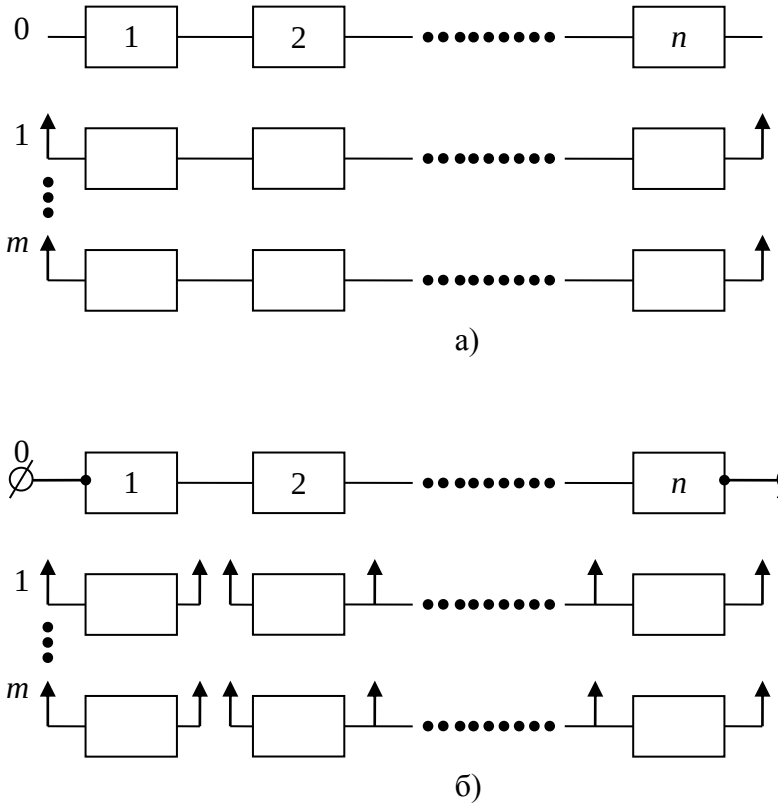


Рис. 4. а) Общее резервирование с включением резерва замещением.
б) Раздельное резервирование с включением резерва замещением.

Скользящее резервирование – это резервирование замещением, при котором группа основных элементов объекта резервируется одним или несколькими резервными, каждый из которых может заменить любой отказавший элемент в данной группе.

Скользящее резервирование всегда является активным, всегда имеется переключающее устройство, определяющее наличие отказа и включающее резервный элемент (рис. 5).

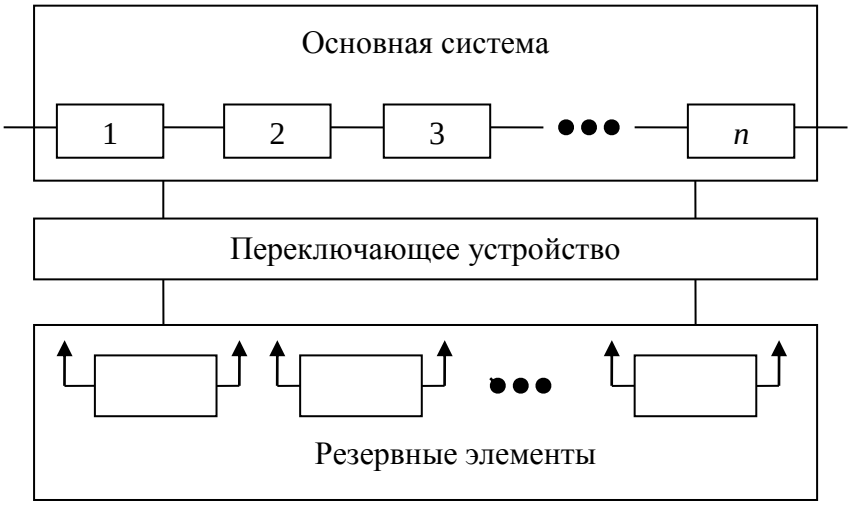


Рис. 5. Схема скользящего резервирования

Виды резервных элементов в зависимости от режима работы

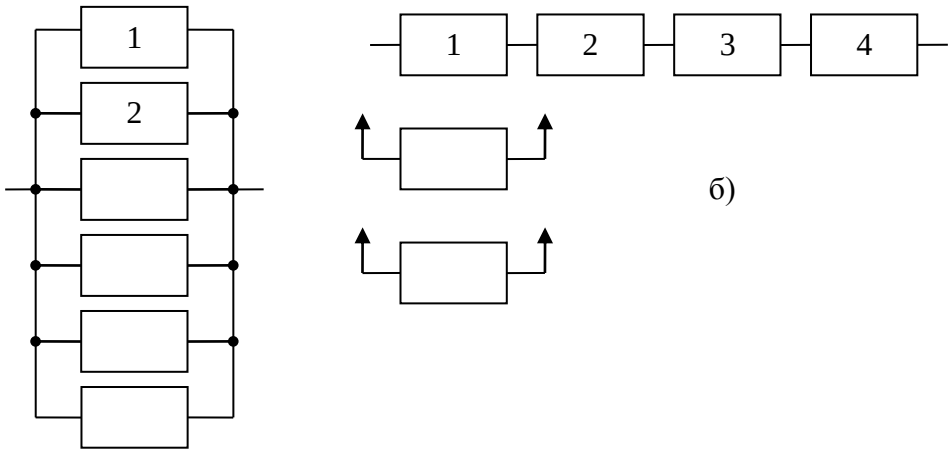
В зависимости от режима работы различают:

Нагруженный резерв – резервный элемент находится в том режиме работы, что и основной. При этом принимается, что характеристики надежности резервных элементов в период их пребывания в качестве резервных и в период использования вместо основных после отказа последних, остаются неизменными.

Облегченный резерв – резервный элемент находится в менее нагруженном режиме, чем основной. Принимается, что характеристики надежности резервных элементов в период их пребывания в качестве резервных выше, чем в период их использования вместо основных после отказа последних.

Ненагруженный резерв – резервный элемент практически не несет нагрузки. Такой резервный элемент, находясь в резерве, отказывать не должен, т.е. обладает в этот период идеальной надежностью. В период же использования этого элемента вместо основного после отказа последнего надежность становится равной надежности основного.

Различают резервирование с целой и дробной кратностью. Для их различия на схеме указывают кратность резервирования m (рис. 6, а, б).



а)

Рис. 6. Резервирование: а) постоянное резервирование с дробной кратностью (*m*=4/2);
б) раздельное резервирование с дробной кратностью (*m*=2/4)

При резервировании с целой кратностью величина m есть целое число, при резервировании с дробной кратностью *m* есть дробное несокращаемое число. Например, *m*=4/2 означает наличие резервирования с дробной кратностью, при котором число резервных элементов равно 4, число основных 2, а общее число элементов равно 6. Сокращать дробь нельзя, так как если *m*=4/2=2, то это означает, что имеет место резервирование с целой кратностью, при котором число резервных элементов равно 2, а общее число 3.

Для резервирования объектов, состоящих из одинаковых элементов, можно использовать небольшое число резервных элементов взамен любых отказавших основных элементов (скользящее резервирование).

Мажоритарное и комбинированное резервирование

Частным случаем резервирования с дробной кратностью является мажоритарное резервирование, часто используемое в устройствах дискретного действия (рис. 7). При мажоритарном резервировании вместо одного элемента (канала) включается три идентичных элемента, выходы, которых подаются на мажоритарный орган *M* (элемент голосования). Если все элементы этой резервной группы исправны, то на вход *M* поступают три одинаковых сигнала и такой же сигнал поступает во внешнюю цепь с выхода *M*.

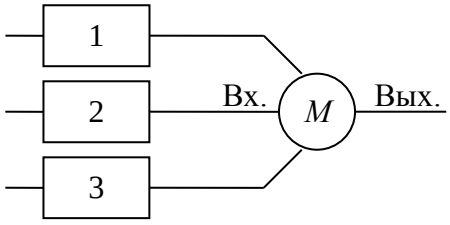


Рис. 7. Мажоритарное резервирование (выбор по большинству)

Если один из трех резервных элементов отказал, то на вход *M* поступают два одинаковых сигнала (истинных) и один сигнал ложный. На выходе *M* будет сигнал, совпадающий с большинством сигналов на его входе, т.е. мажоритарный орган, осуществляет операцию голосования или выбора по большинству. Таким образом, условием безотказной работы группы при мажоритарном резервирование является безотказная работа любых двух элементов из трех и мажоритарного органа в течение заданного времени.

Комбинированный резерв – на рис. 8 представлена резервированная группа, сочетающая преимущества нагруженного резерва (непрерывность работы) и ненагруженного резерва (обеспечение большого выигрыша в надежности). В данном случае два элемента образуют дублирующую группу (нагруженный резерв), а третий находится ненагруженном резерве. Такой резерв называют комбинированным.

В устройствах ИС ответственного назначения могут быть использованы все виды структурного резервирования (рис. 9).

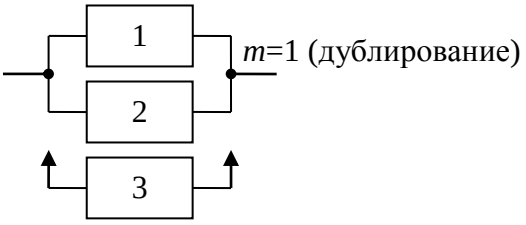


Рис. 8. Комбинированный резерв

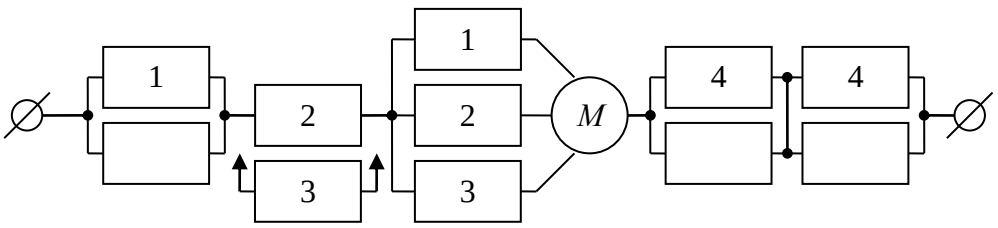


Рис. 9. Расчетно-логическая схема структурного резервирования подсистемы сложной ТС

Теоретически введением избыточности в структуру системы и выбором оптимальных режимов можно создать сколь угодно надежную КС. Но не всегда это практически выполнимо. Анализируя все виды резервирования, следует сделать практический вывод: обеспечить высокую надежность КС путем общего нагруженного резерва не представляется возможным по экономическим соображениям. Наибольший эффект дает поэлементное резервирование [1, 2, 3, 6].

Сравнивая между собой виды резервирования с нагруженным и ненагруженным резервом, можно заметить, что при прочих равных условиях система с ненагруженным резервом надежнее системы с нагруженным резервом.

Организация резерва на уровне компьютера и КС

Резервирование на уровне компьютера. В аппаратуре универсальных компьютеров резервирование встречается на различных уровнях. На уровне компьютера резервирование заключается в наличии большого числа однотипных машин, что необходимо для решения постановленных задач. В этом случае надежность системы оценивается как для систем со скользящим резервированием. В случае универсальных компьютеров целесообразно использовать производительность всех имеющихся процессоров. Тогда свойство системы удобнее характеризовать через эффективную производительность системы.

$$\Pi_{эф.}=\sum_{i=1}^{n}\Pi_i \cdot K_i$$

где Π_i – производительность (число задач выполняемых машиной в единицу времени) i-ой машины;

n – число машин в системе;

K_i – коэффициент готовности i-ой машины.

Если отдельные системы компьютера, объединенные через адаптеры между каналами для периферийных устройств, через общее поле памяти или другим способом, образуют многомашинную (многопроцессорную) КС, то эффективная производительность такой системы

$$\Pi_{эф.с}=\sum_{j=1}^{m}\Pi_j \cdot P_j \ ,$$

где m – количество состояний системы;

P_j – вероятность того, что система находится j-м состоянии;

Π_j – производительность системы в j-м состоянии.

Вероятность P_j определяют методом Марковских цепей. Поскольку конфигурация таких систем может быть самой различной, для оценки

вероятности сохранения связности системы следует применять методы расчета надежности систем со сложной структурой, например метод минимальных путей и сечений.

Резервирование на уровне устройств. На более низких уровнях иерархии структуры в универсальных компьютерах резервирование встречается на уровне периферийных устройств (ПУ). Для решения задач требуется некоторое минимальное число ПУ.

Резервирование на уровне кодов – в компьютерах для повышения надежности ОЗУ и ПЗУ применяются коды с обнаружением и исправлением ошибок. Применение этих кодов дает возможность исправлять определенное число ошибок в каналах передачи или восстанавливать информацию в случае отказа некоторых ячеек в ОЗУ и ПЗУ или дорожек (то есть усилителей записи-считывания) в накопителях на магнитных дисках. Надежность таких устройств оценивается как надежность резервированных систем со скользящим резервом.

Резервирование в специализированных и управляющих компьютерах. В специализированных, а особенно в управляющих машинах резервирование применяется значительно шире в связи с высокими требованиями к надежности таких систем.

На уровне компьютера, а иногда на уровне программного обеспечения применяется троирование. Встречаются также системы, где используется несколько резервных машин. В целях повышения надежности часть из них может работать в режиме нагруженного резерва, часть в режиме ненагруженного. Однако резервирование на уровне компьютера не самое экономичное. Для повышения надежности при ограничении массы, стоимости и габаритных размеров КС используется резервирование отдельных устройств машин троированием или применением нескольких нагруженных или ненагруженных резервов. Для повышения надежности самых ответственных узлов применяется троирование или логика с переплетениями (представляется в виде избыточной логической схемы, где ошибки в одном слое корректируются в этом же или следующем слое логических элементов).

Все рассмотренные методы резервирования в КС относятся к пассивному резервированию, так как не предусматривают реконфигурацию системы. Способы резервирования, предусматривающие автоматическую реконфигурацию системы используются в отказоустойчивых компьютерных системах (ОКС). В ОКС используются средства обнаружения, локализации отказа и средства реконфигурации.

Отказы в ОКС обнаруживается при помощи средств контроля, а локализуются при помощи средств диагностики и устраняются автоматической реконфигурацией системы. Реконфигурация заключается в перестройке структуры вычислительных средств таким образом, чтобы ее отказавшие части были устранены от участия в работе.

Контрольные вопросы и задания

1. Что такое резервирование?
2. Какие виды структурного резервирования широко распространены на практике?
3. Что такое постоянное (общее) резервирование?
4. Каково значение кратности резервирования при дублировании?
5. Приведите пример комбинированного резерва элементов КТ?
6. Составьте структурную схему надежности устройства состоящего из четырех основных элементов, включенных по схеме раздельного резервирования с нагруженным резервом (m = 1).
7. Как оценивается ВБР при мажоритарном резервировании?
8. Где чаще всего применяется динамическое резервирование?
9. Составьте структурную надежности устройства КС состоящего из 4-х основных элементов, включенных по схеме общего резервирования с нагруженным резервом при m = 2.
10. При каком способе резервирования устройств ИС всегда присутствуют переключающие устройства (коммутатор)?

Литература: 1,2,3,5,6, 7.

Лекция 7

Тема: Расчет характеристик надёжности невосстанавливаемых резервированных систем

План

1. Расчетные формулы для общего и раздельного резервирования с постоянно включенным резервом и целой кратностью.
2. Расчетные формулы для общего, раздельного резервирования с замещением с целой и дробной кратностью.
3. Расчетные формулы для скользящего и мажоритарного резервирование устройств ИС.
4. Структурная схема надёжности конкретного устройства ИС. Пример расчета показателей надёжности для экспоненциального закона распределения.

Ключевые слова

Надёжность, общее резервирование, раздельное резервирование, кратность резервирования, постоянный резерв, резервирование замещением, дробная кратность, структурная схема надёжности, мажоритарное резервирование, скользящий резерв, показатели надёжности, вероятность безотказной работы, экспоненциальный закон.

Приведем основные расчетные формулы для указанных выше видов резервирования [1, 2, 3, 4, 5, 6].

Общее резервирование с постоянно включенным резервом и целой кратностью. В этом случае ВБР системы равна:

$$P_c(t) = 1 - [1 - \prod_{i=1}^{n} P_i(t)]^{m+1}, \qquad (1)$$

где $p_i(t)$ – вероятность безотказной работы i-го элемента в течение времени t;

n – число элементов основной или любой резервной цепи;

m – число резервных цепей (кратность резервирования).

Для последовательного включения элементов отказы являются независимыми случайными событиями, тогда по аксиоме умножения вероятностей ВБР системы:

$$P_{посл.} = \prod_{i=1}^{n} p_i ,$$

где p_i – ВБР подсистемы.

Для параллельного включения элементов ВБР равна:

$$P_{пар.} = 1 - \prod_{i=1}^{n} (1 - p_j),$$

где p_j – ВБР подсистемы.

При экспоненциальном законе надежности, когда ВБР $p_i(t) = e^{-\lambda_i \cdot t}$,

$$P_c(t) = 1 - [1 - e^{-\lambda_0 \cdot t}]^{m+1}, \qquad (2)$$

средняя наработка до первого отказа

$$T_{ср.с.} = 1/\lambda_0 \cdot \sum_{i=1}^{m} 1/i + 1 = T_{ср.о.} \cdot \sum_{i=1}^{m} 1/i + 1, \qquad (3)$$

где $\lambda_0 = \sum_{i=1}^{n} \lambda_i$ – интенсивность отказов нерезервированной системы или любой из резервных систем;

$T_{ср.о.}$ – среднее время безотказной работы нерезервированной системы или любой из резервных систем.

Раздельное резервирование с постоянно включенным резервом и целой кратностью

$$P_c(t) = \prod_{i=1}^{n} \{1 - [1 - p_i(t)]^{m+1}\}, \qquad (4)$$

где $p_i(t)$ – вероятность безотказной работы i-го элемента;

m_i – кратность резервирования i-го элемента;

n – число элементов основной системы.

При экспоненциальном законе, когда $p_i(t) = e^{-\lambda_i \cdot t}$, ВБР системы:

$$P_c(t) = \prod_{i=1}^{n} \{1 - [1 - e^{-\lambda_i \cdot t}]^{m_i+1}\}, \qquad (5)$$

где m_i – кратность резервирования i-го элемента.

Средняя наработка до первого отказа:

$$T_{ср.с.} = \int_0^{\infty} P_c(t) dt$$

Общее резервирование с замещением и целой кратностью

$$P_{m+1}(t) = P_m(t) + \int_0^t P(t - \tau) \cdot a_m(\tau) d\tau, \qquad (6)$$

где $P_{m+1}(t)$, $P_m(t)$ – ВБР резервированной системы кратностью m и $m+1$ соответственно;

$P(t-\tau)$ – ВБР основной системы в течение времени $(t-\tau)$;

$a_m(\tau)$ – частота отказов резервированной системы кратности m в момент времени τ.

Эта формула позволяет получить расчетные соотношения для устройств любой кратности резервирования. Для получения таких формул необходимо выполнить интегрирование в правой части, подставляя вместо $P(t-\tau)$ и $a_m(\tau)$ их значения в соответствии с выбранным законом распределения и состоянием резерва.

При экспоненциальном законе надежности и ненагруженном состоянии резерва:

$$P_c(t) = e^{-\lambda_0 \cdot t} \cdot \sum_{i=0}^{m} [\lambda_0 \cdot t]^i / i! \qquad (7)$$

$$T_{ср.с.} = T_{ср.0} \cdot (m+1), \qquad (8)$$

где $\lambda_0 = \sum_{i=1}^{n} \lambda_i$, $T_{ср.0}$ – интенсивность отказа и средняя наработка до первого отказа основного (нерезервированного) устройства;

m – число резервных цепей (кратность резерва);

Раздельное резервирование замещением с целой кратностью

Вероятность безотказной работы в этом случае:

$$P_c(t) = \prod_{i=1}^{n} P_i(t), \qquad (9)$$

где $P_i(t)$ – ВБР системы i-го типа, резервированных по способу замещения;

$P_i(t)$ – вычисляют по формулам общего резервирования замещением;

n – число элементов основной группы.

Скользящее резервирование. $P_c(t)$ определяется:

$$P_c(t) = e^{-\lambda_0 \cdot t} \cdot \sum_{i=0}^{m_0} [\lambda_0 \cdot t]^i / i!, \qquad (10)$$

$$T_{ср.с.} = T_{ср.0} \cdot (m_0 + 1), \qquad (11)$$

где $\lambda_0 = \lambda \cdot n$ – интенсивность отказов нерезервированной системы;

λ – интенсивность отказов элемента;

n – число элементов основной системы;

$T_{ср.0}$ – среднее время безотказной работы нерезервированной системы;

m_0 – число резервных элементов

В этом случае кратность резервирования $m=m_0/n$.

Мажоритарное резервирование

Вероятность безотказной работы системы:

$$P_c(t) = P_m(t) \cdot [3P^2(t) - 2P^3(t)], \qquad (12)$$

где $P_m(t)$ – ВБР в течение времени t мажоритарного органа;

$P(t)$ – ВБР в течение времени t одного элемента (для случая когда m=2 и n=1).

Обеспечение надежности баз данных ИС

Несколько специфичны вопросы обеспечения целостности базы данных в ИС. К надежности баз данных (БД) предъявляется особо жесткие требования, поскольку информация, хранимая в них, используется обычно многократно.

Под **целостностью базы данных** понимается такое ее состояние, когда имеет место полное и точное сохранение всех введенных в БД данных и отношений между ними, иными словами, если не произошло случайного разрушения или искажения этих данных или их структуры. Для сведения к минимуму потерь от случайных искажений данных необходимо иметь возможность своевременно обнаруживать и устранять ошибки на этапах хранения, обновления и реорганизации базы данных. Это требует большого набора вспомогательных программ обслуживания баз данных.

К ним относятся программы:

– ведения системного журнала, подробно фиксирующего каждую операцию (транзакцию) над базой данных;

– эффективного контроля достоверности;

– репликация для получения копии базы данных (или ее частей) с целью последующего их восстановления при искажении;

– восстановления для возврата базы данных в первоначальное состояние при обнаружении искажения данных (используя копии базы данных и массивы изменений, формируемых в журнале).

Для надежной работы базы данных ИС осуществляются:

– непрерывное администрирование базы данных ИС;

– регистрация каждого имевшего место доступа к базе данных и выполненных изменений в журнале БД. В журнал заносятся:

– текст запроса на изменение БД, содержащий описание транзакции, терминала и пользователя, время, текст исходного сообщения, тип и адрес изменения данных;

– копии файлов БД до внесения в нее изменений;

– использование средств СУБД для санкционированного доступа и защиты данных (формирование подсхем базы данных как подмножества структуры базы данных).

– создание резервных копий БД, «зеркалирование» дисков;

– введение четко регламентированной системы документооборота и форм документов, разрешенных к использованию;

– криптографирование базы данных;

– формирование групп пользователей работы и привилегий доступа к ресурсам БД.

Для обеспечения целостности БД могут устанавливаться специальные режимы использования файлов базы данных:

– **монопольный** – запрещающий обращения к БД от всех программ кроме одной, вносящей изменения и считывающей информацию из полей базы данных;

– **защищенный** – вносить изменения в БД вправе лишь одна программа, а остальные программы могут только считывать информацию.

Резервирование и восстановление баз данных при аварийных завершениях программы (отказ системы, повреждение носителя) выполняется по нескольким стратегиям. В частности, резервирование файлов базы данных может выполняться:

– в одном поколении (создание точных копий – дублей файлов БД);

– в разных поколениях (хранятся дубли нескольких временных поколений файлов: «дед», «отец», «сын», и т.д., а также ведется системный журнал изменений);

– смешанное резервирование, использующее совместно две первые стратегии.

Контрольные точки (точки рестарта, точки отката) – место повторного запуска программы при аварийном ее завершении. В контрольных точках обычно выполняются: внесение изменений в БД, разблокирование всех файлов, на обращение к которым был заложен запрет, запись информации о контрольной точке в системный журнал.

Использование **массивов RAID** (Redundant Array of Inexpensive Disks – избыточный массив недорогих дисков) существенно уменьшает риск простоя системы из-за отказов накопителей на магнитных дисках, которые являются одним из наименее надежных компонентов современных компьютеров.

В качестве наиболее эффективных мер комплексного обеспечения надежности ИС можно назвать кластеризацию компьютеров и использование отказоустойчивых компьютеров.

Контрольные вопросы и задания

1. Приведите аналитическое выражение для оценки ВБР при общем (постоянном) резервировании?
2. Составьте структурную схему надежности устройства состоящего из четырех основных элементов, включенных по схеме раздельного резервирования с нагруженным резервом (m = 1).
3. Как оценивается ВБР при мажоритарном резервировании?
4. Как определить наработку на отказ при скользящем резервировании?
5. Где чаще всего применяется динамическое резервирование?
6. Как оценить частоту отказа в случае раздельного резервирования системы?
7. При каком способе резервирования резервный элемент работает одновременно с основным?
8. Определите структурную схему надежности невосстанавливаемого резервированного устройства, где безотказность следует рассчитывать по формуле:

$$P(t) = \prod_{i=1}^{n} \{1 - [1 - P_i(t)]^{m_i+1}\}$$

9. Определить наработку на отказ при экспоненциальном законе надежности и ненагруженном состоянии резерва.
10. Какие осуществляются меры для надежной работы базы данных?
11. Что напоминается под целостностью базы данных?
12. В каких случаях может, выполнятся резервирование файлов данных?
13. Дайте определение понятиям: монопольный, защищенный и разделенный режимы использования файлов БД.
14. Для чего в КС используют RAID – массивы?

Литература: 1,2,3,6,10.

Лекция 8

Тема: Надёжность резервированных устройств с последовательно-параллельной структурой (метод свертки)

План

1. Метод свертки, оценка надёжности для последовательно-параллельных систем с нагруженным резервом.
2. Расчетные формулы для оценки количественных характеристик методом свертки.
3. Основные достоинства и недостатки метода свертки.

Ключевые слова

Показатели надёжности, метод свёртки, нагруженный резерв, последовательно-параллельная структура, схема основного соединения, преобразование формул, вероятность безотказной работы, интенсивность отказов, этапы преобразования, структурная схема надёжности.

Для последовательно-параллельных невосстанавливаемых структур технических систем (ИС) эффективным методом оценки надежности является метод свертки.

Данный метод является точным методом и основан на последовательном преобразовании структуры устройств ИС и сведения её к основному соединению элементов. Покажем применение данного метода на примере структуры, показанной на рис. 1.

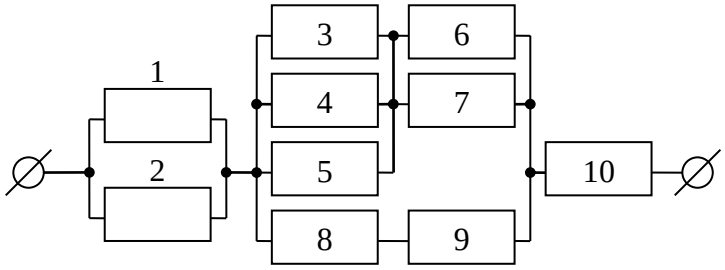


Рис. 1. Структурная схема надежности последовательно-параллельной структуры ТС

Пусть каждый элемент рассматриваемой структуры характеризуется вероятностью безотказной работы P_i. Необходимо определить вероятность безотказной работы, системы.

Метод свертки состоит из нескольких этапов.

На первом этапе рассматриваются все параллельные соединения, которые заменяются эквивалентными элементами с соответствующим показателем надежности. В рассматриваемом примере такими параллельными элементами являются: 1 и 2; 3, 4 и 5; 6 и 7.

После первого этапа преобразований схема примет вид (рис. 2).

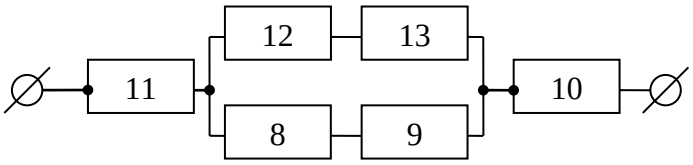


Рис. 2. Схема после первого этапа преобразований

Характеристики надежности элементов схемы равны (согласно формуле: $P_{пар.} = 1 - \prod_{j=1}^{m}(1 - P_j)$, где P_j – вероятность безотказной работы подсистем).

$$P_{11} = 1 - (1 - P_1) \cdot (1 - P_2);$$
$$P_{12} = 1 - (1 - P_3) \cdot (1 - P_4) \cdot (1 - P_5);$$
$$P_{13} = 1 - (1 - P_6) \cdot (1 - P_7).$$

На втором этапе рассматриваются все последовательные соединения, которые заменяются эквивалентными элементами.

Здесь последовательными элементами являются 8 и 9; 12 и 13. после второго этапа преобразований схема примет вид, показанный на рис. 3.

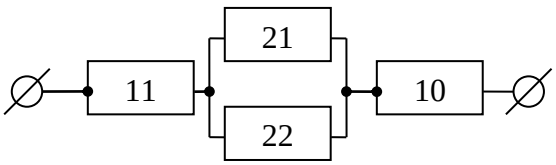


Рис. 3. Схема после второго этапа преобразований

Характеристики надежности элементов определяются с помощью следующих выражений ($P_{посл.} = \prod_{i=1}^{n} P_i$):

$$P_{21} = P_{12} \cdot P_{13} = [1-(1-P_3)(1-P_4)(1-P_5)] \cdot [1-(1-P_6)(1-P_7)];$$

$$P_{22}=P_8 \cdot P_9$$

На третьем этапе вновь, рассматриваются все параллельные соединения, которые заменяются эквивалентными элементами.

В рассматриваемом примере такими параллельными элементами являются 21 и 22.

После третьего этапа преобразований схема примет вид, показанной на рис. 4.

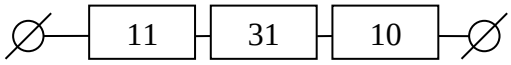


Рис. 4. Схема после третьего этапа преобразований

Характеристики надежности элементов определяются с помощью следующих выражений.

$$P_{31} = 1-(1-P_{21})(1-P_{22}) = 1-\{1-[1-(1-P_3)(1-P_4)(1-P_5)] \cdot [1-(1-P_6)(1-P_7)]\} \cdot (1-P_8P_9);$$

На четвертом этапе для последовательной структуры устройств ИС определяется ВБР системы.

$$P_c = P_{11} \cdot P_{31} P_{10} = [1-(1-P_1)(1-P_2)] \cdot \{1-\{1-[1-(1-P_3)(1-P_4)(1-P_5)] \cdot [1-(1-P_6)(1-P_7)]\} \cdot (1-P_8P_9)\} \cdot P_{10};$$

Пример. Определим показатели надежности системы при условии, что вероятности безотказной работы элементов соответственно равны:

P_1=0,8; P_2=0,9; P_3=0,7; P_4=0,8;
P_6=0,9; P_7=0,95; P_8=0,95; P_9=0,9;
P_5=0,9;
P_{10}=0,98.

Результаты расчета вероятности безотказной работы сведем в таблицу 1.

Таблица 1.

Исходные данные расчета	1-й этап расчета	2-й этап расчета	3-й этап расчета	4-й этап расчета
P_1=0,8	P_{11}=0,98	P_{11}=0,98	P_{11}=0,98	P_c=0,959
P_2=0,9	P_{12}=0,994	P_{21}=0,991	P_{31}=0,999	
P_3=0,7	P_{13}=0,995	P_{22}=0,855	P_{10}=0,98	
P_4=0,8	P_8=0,95	P_{10}=0,98		
P_6=0,9	P_9=0,9			
P_7=0,95	P_{10}=0,98			
P_8=0,95				
P_9=0,9				
P_5=0,9				
P_{10}=0,98				

Как видно из приведенного примера, метод свертки является весьма эффективным методом определения показателей надежности невосстанавливаемых параллельно-последовательных структур.

Число элементов мало влияет на сложность проведения расчетов, в основном происходит увеличение числа этапов расчета.

Недостатком метода свертки является его ограниченность параллельно-последовательными схемами. Например, показатели надежности мостиковой структуры ИС с помощью указанного метода определить невозможно.

Контрольные вопросы и задания

1. К какому способу оценки надежности относится метод свертки?
2. Составьте структурную надежности устройства ИС состоящего из 4-х основных элементов, включенных по схеме общего резервирования с нагруженным резервом при $m = 2$.
3. В каком случае резервный элемент, обладает идеальной надежностью?
4. Какой из характеристик надежности устройств КТ относится к показателям безотказности?
5. Какую формулу необходимо использовать при расчете вероятности отказа ИС.
6. Определите значение интенсивности отказов высоконадежных устройств ИС.
7. Дайте классификацию видов резервирования.
8. Укажите основные достоинства и недостатки метода свертки для расчета надежности последовательно-параллельных структур.
9. На чем основан метод свертки?
10. Как влияет число элементов в устройстве на сложность проведения расчетов методом свертки?

Литература: 1,2,3,5,6, 7.

Лекция 9

Тема: Оценка надежности методом путей и сечений. Логико-вероятностные методы анализа сложных систем

План

1. Метод минимальных путей и сечений для расчета показателей надежности систем с разветвленной структурой.
2. Основные определения и понятия логико-вероятностных методов анализа и оценка надежности ИС.
3. Сущность метода кратчайшего пути успешного функционирования и минимального сечения отказов.
4. Расчет функции работоспособности и функции отказа для мостиковой структуры.
5. Области применения этих методов. Статистическое моделирование для оценки надежности ИС.

Ключевые слова

Показатели надежности, разветвленная структура ИС, минимальных путь, сечение, логико-вероятностный метод, мостиковая схема, функция работоспособности, кратчайший путь успешного функционирования, минимальное сечение отказов, вероятность безотказной работы, функция алгебры логики, структурная схема расчета надежности.

Встречаются структуры и способы организации ИС, когда резервирование имеет место, но его нельзя представить по схеме последовательного и параллельного включения элементов или подсистем. Для анализа надежности таких структур используют метод минимальных путей и сечений, который относится к приближенным методам и позволяет определить граничные оценки надежности сверху и снизу [1, 2, 3, 5, 6].

Путем в сложной структуре называется последовательность элементов, обеспечивающих функционирование (работоспособность) системы.

Сечением называется совокупность элементов, отказы которых приводят к отказу системы.

Вероятность безотказной работы последовательно включенных параллельных цепей дает верхнюю оценку для ВБР системы данной структуры. Вероятность безотказной работы параллельно включенных последовательных цепей из элементов путей дает нижнюю оценку для ВБР системы данной структуры. Фактическое значение показателя надежности находится между верхней и нижней границами.

Рассмотрим мостиковую схему соединения элементов системы, состоящей из пяти элементов (рис. 1).

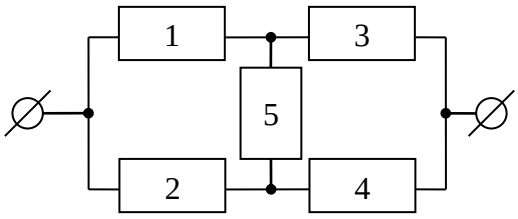


Рис. 1. Мостиковая схема соединения элементов (подсист.)

Здесь набор элементов образует минимальный путь, если исключение любого элемента из набора приводит к отказу пути. Из этого вытекает, что в переделах одного пути элементы находятся в основном соединении, а сами пути включаются параллельно. Набор минимальных путей для мостиковой схемы представлен на рис. 2. Пути образуют элемента 1, 3; 2, 4; 1, 5, 4; 2, 5, 3.

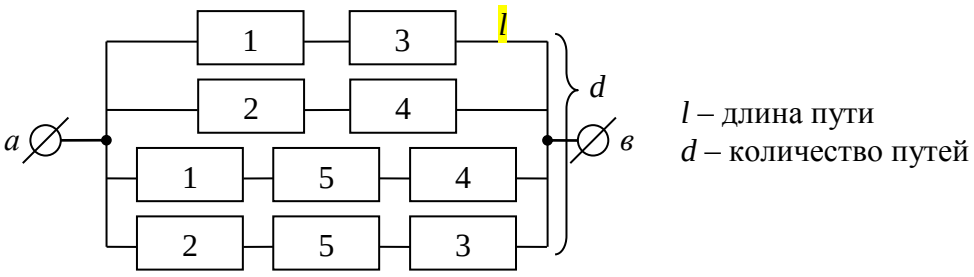


Рис. 2. Набор минимальных путей.

Для всех элементов схемы известны ВБР P_1, P_2, P_3, P_4, P_5 и соответствующие им вероятности отказа типа «обрыв» $Q_1 \div Q_5$, необходимо определить вероятность наличие цепи между точками *а* и *в*. Поскольку один и тот же элемент включается в два параллельных пути, то в результате расчета получается оценка безотказности сверху.

$$P_в = 1\text{-}Q_{13}\cdot Q_{24}\cdot Q_{154}\cdot Q_{253} = 1\text{-}\ (1\text{-}P_1P_3)(1\text{-}P_2P_4)(1\text{-}P_1P_5P_4)(1\text{-}P_2P_5P_3)$$

При определении минимальных сечений осуществляется подбор минимального числа элементов, перевод которых из работоспособного состояния в неработоспособное вызывает отказ системы.

При правильном подборе элементов сечения возвращение любого из элементов в работоспособное состояние восстанавливает работоспособное состояние системы.

Поскольку отказ каждого из сечений вызывает отказ системы, то первые соединяются последовательно. В переделах каждого сечения элементы соединяются параллельно, так как для работы системы достаточно наличия работоспособного состояния любого из элементов сечения.

Схема минимальных сечений для мостиковой схемы приведена на рис. 3. Так как один и тот же элемент включается в два сечения, то полученная оценка является оценкой снизу.

$$P_н = P_{12}\cdot P_{34}\cdot P_{154}\cdot P_{253} = (1-q_1q_2)\cdot(1-q_3q_4)\cdot(1-q_1q_5q_4)\cdot(1-q_2q_5q_3)$$

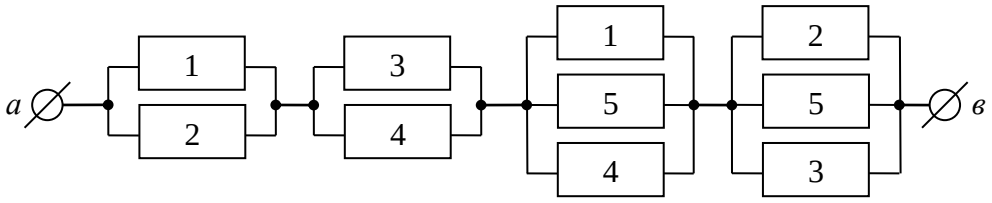


Рис. 3. Набор минимальных сечений

Вероятность безотказной работы системы P_c оценивается тогда по двойному неравенству

$$P_н \le P_c \le P_в$$

Таким образом, данный метод позволяет представить систему с произвольной структурой в виде параллельных и последовательных цепей. (При составлении минимальных путей и сечений любая система преобразуется в структуру с параллельно-последовательным или последовательно-параллельным соединением элементов). Метод прост, но требует точного определения всех путей и сечений. Он получил широкое применение при расчете надежности подсистем АСУТП, особенно применительно к системам защиты и логического управления. Его используют в системах регулирования мощности реактора, предусматривающая возможность перехода от одной неисправной цепи регулирования к другой, находящийся в резервном состоянии.

Логико-вероятностные методы анализа надежности систем

Сущность логико-вероятностных методов заключается в использовании функций алгебры логики (ФАЛ) для аналитической записи условий работоспособности системы и переходе от ФАЛ к вероятностным функциям (ВФ), объективно выражающим безотказность системы. Т.е. с помощью логико-вероятностного метода можно описать схемы ИС для расчета надежности с помощью аппарата математической логики с последующим использованием теории вероятностей при определении показателей надежности [2, 3, 8].

Система может находится только в двух состояниях: в состоянии полной работоспособности ($y = 1$) и в состоянии полного отказа ($y = 0$). При этом предполагается, что действие системы детерминировано зависит от действия ее элементов, т.е. y является функцией $x_1, x_2, \ldots, x_i, \ldots, x_n$. Элементы могут находиться также только в двух несовместных состояниях: полной работоспособности ($x_i = 1$) и полного отказа ($x_i = 0$).

Функцию алгебры логики, связывающую состояние элементов с состоянием системы y (x_1, x_2, …, x_n) называют *функцией работоспособности* системы $F(y) = 1$.

Для оценки работоспособных состояний системы используют два понятия:

1) кратчайшего пути успешного функционирования (КПУФ), который представляет собой такую конъюнкцию её элементов, ни одну из компонент которой нельзя изъять, не нарушив функционирования системы. Такая конъюнкция записывается в виде следующей ФАЛ:

$$\rho_l = \bigwedge_{i \in K_{\rho_l}} x_i \ ,$$

где i – принадлежит множеству номеров K_{P_l}, соответствующих данному l-му пути.

Другими словами, КПУФ системы описывает одно из её возможных работоспособных состояний, которое определяется минимальным набором работоспособных элементов, абсолютно необходимых для выполнения заданных для системы функций.

2) минимального сечения отказов системы (МСО) представляющего собой такую конъюнкцию из отрицаний её элементов, ни одну из компонент которой нельзя изъять, не нарушив условия неработоспособности системы. Такую конъюнкцию можно записать в виде следующей ФАЛ:

$$S_j = \bigwedge_{i \in K_{S_j}} x_i' \ ,$$

где K_{S_j} означает множество номеров, соответствующих данному сечению.

Другими словами, МСО системы описывает один из возможных способов нарушения работоспособности системы с помощью минимального набора отказавших элементов.

Каждая избыточная система имеет конечное число кратчайших путей (l = 1, 2,…, m) и минимальных сечений (j =1, 2, …, m).

Используя эти понятия можно записать условия работоспособности системы.

1) в виде дизъюнкции всех имеющихся кратчайших путей успешного функционирования.

$$y(x_1,...,x_n) = \bigvee_{l=1}^{d} \rho_l = \bigvee_{l=1}^{d} \left[\bigwedge_{i \in K_{\rho_l}} x_i \right];$$

2) в виде конъюнкции отрицаний всех МСО

$$y(x_1,...,x_n) = \bigwedge_{j=1}^{m} S'_j = \bigwedge_{j=1}^{m} \left[\bigvee_{i \in K_{\rho_l}} x_i \right];$$

Таким образом, условия работоспособности реальной системы можно представить в виде условий работоспособности некоторой эквивалентной (в смысле надежности) системы, структура которой представляет параллельное соединение кратчайших путей успешного функционирования, или другой эквивалентной системы структура которой представляет соединение отрицаний минимальных сечений.

Например, для мостиковой структуры ИС функция работоспособности системы с помощью КПУФ запишется следующим образом:

$$y = (x_1, x_2, x_3, x_4, x_5) = \begin{vmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \\ \rho_4 \end{vmatrix} = \begin{vmatrix} x_1 x_3 \\ x_2 x_4 \\ x_1 x_5 x_4 \\ x_2 x_5 x_3 \end{vmatrix};$$

функцию работоспособности этой же системы через МСО можно записать в следующем виде:

$$y = (x_1, x_2, x_3, x_4, x_5) = |x_1 x_2| x_3 x_4 | x_1 x_5 x_4 | x_2 x_5 x_3| = |S'_1, S'_2, S'_3, S'_4, S'_5|$$

При небольшом числе элементов (не более 20) может быть использован табличный метод расчета надежности, который основан на использовании теоремы сложения вероятностей совместных событий.

Вероятность безотказной работы системы можно вычислить по формуле (через вероятностную функцию вида):

$$P_c = [y(x_1, x_2,..., x_n) = 1] = P_c\{\bigvee_{l=1}^{d} \rho_l\}$$

Логико-вероятностные методы (методы: разрезания, табличный, ортогонализации) широко применяют в *диагностических процедурах* при построении деревьев отказов и определении базисных (исходных) событий, вызывающих отказ системы.

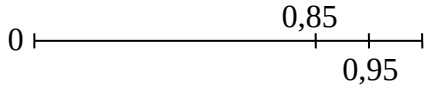
Для надежности компьютерной системы со сложной структурой резервирования может быть использован метод статистического моделирования.

Идея метода заключается в генерировании логических переменных x_i с заданной вероятностью pi возникновения единицы, которые подставляются в

логическую структурную функцию моделируемой системы в произвольной форме и затем вычисляется результат.

Совокупность $x_1, x_2, \ldots, x_n$ независимых случайных событий, образующих полную группу, характеризуется вероятностями появления каждого из событий $p(x_i)$, причем $\sum_{i=1}^{n} p(x_i) = 1$.

Для моделирования этой совокупности случайных событий используется генератор случайных чисел, равномерно распределенных в интервале [0-1]



– схема задания случайных событий

Значение p_i выбирается равным вероятности безотказной работы i-й подсистемы. При этом процесс вычисления повторяется N_0 раз с новыми, независимыми случайными значениями аргументов x_i (при этом подсчитывается количество $N(t)$ единичных значений логический структурной функции). Отношение $N(t)/N_0$ является статистической оценкой $\hat{P}_c(t)$ вероятности безотказной работы

$$\hat{P}_c(t) = \frac{N(t)}{N_0},$$

где $N(t)$ – количество безотказно работающих до момента времени t объектов, при их исходном количестве.

Генерирование случайных логических переменных x_i с заданной вероятностью появления единицы p_i осуществляется на основании равномерно распределенных в интервале [0-1] случайных величин, получаемых с помощью стандартных программ, входящих в математическое обеспечение всех современных компьютеров.

Контрольные вопросы и задания

1. Назовите метод оценки надежности ИС, где вероятность безотказной работы системы определяется как $P_н \le P_c \le P_в$.
2. Для расчета надежности каких систем используется метод путей и сечений?
3. С помощью какого метода можно оценить надежность устройств мостикового типа?
4. Какие методы определения показателей надежности восстанавливаемых систем известны?
5. Структурно представьте мостиковую схему набором минимальных путей и сечений.
6. Дайте определение минимального пути и минимального сечения.

7. Запишите функцию работоспособности для устройства с разветвленной структурой?
8. Что называется функцией работоспособности?
9. Что такое кратчайший путь успешного функционирования (КПУФ). Запишите условия работоспособности в виде КПУФ.
10. Где используется логико-вероятностный метод оценки надежности?

Литература: 1, 2, 3, 5, 6, 8.

Лекция 10

Тема: Расчет надежности восстанавливаемых систем (метод дифференциальных уравнений)

План

1. Общие методы расчета надежности восстанавливаемых систем.
2. Построение графа возможных состояний системы для оценки надежности восстанавливаемых систем.
3. Метод систем дифференциальных уравнений (СДУ), правило Колмогорова для составления СДУ
4. Нормировочные и начальные условия для решения СДУ.

Ключевые слова

Восстанавливаемая система, количественные характеристики надежности, граф состояний, работоспособное состояние, система дифференциальных уравнений, правило Колмогорова, вероятность безотказной работы, интенсивность восстановления, интенсивность отказа нормировочные условия, начальные условия, параметры надежности, нерезервированная система.

Основной задачей расчета надежности проектируемых ИС является построение математических моделей адекватных вероятностным процессам их функционирования. Эти модели позволяют оценить степень удовлетворения требований по надежности к проектируемым или эксплуатируемым системам.

Вид математической модели определяет возможность получения расчетных формул. Для проведения расчета надежности восстанавливаемых резервированных и нерезервированных систем используются: метод интегральных уравнений, метод дифференциальных уравнений, метод переходных интенсивностей, метод оценки надежности по графу возможных состояний и др. [1, 2, 3, 5, 6].

Метод интегральных уравнений. Метод интегральных уравнений является наиболее общим, его можно применять при расчете надежности любых (восстанавливаемых и невосстанавливаемых) систем при любых распределениях ВБР и времени восстановления.

В этом случае для определения показателей надежности системы составляют и решают интегральные и интегро-дифференциальные уравнения, связывающие характеристики распределения ВБР, а для восстанавливаемых систем – и время восстановления элементов.

В ходе составления интегральных уравнений обычно выделяют один или несколько бесконечно малых интервалов времени, для которых рассматривают сложные события, проявляющие при совместном действии нескольких факторов.

В общем случае решения находят численными методами с помощью компьютера. Метод интегральных уравнений не получил широкого распространения из-за трудности решения [1, 3, 8].

Метод дифференциальных уравнений. Метод применяется для оценки надежности восстанавливаемых объектов и основан на допущении о показательных распределениях времени между отказами (наработки) и времени восстановления. При этом параметр потока отказов $w = \lambda = 1/t_{ср.}$ и интенсивность восстановления $\mu = 1/t_в$, где $t_{ср.}$ – среднее время безотказной работы, $t_в$ – среднее время восстановления.

Для применения метода необходимо иметь математическую модель для множества возможных состояний системы $S = \{S_1, S_2, \ldots, S_n\}$, в которых она может находиться при отказах и восстановлениях системы. Время от времени система S скачком переходит из одного состояния в другое под действием отказов и восстановлений ее отдельных элементов.

При анализе поведения системы во времени в процессе износа удобно пользоваться графом состояний. Граф состояний – это направленный граф, где кружками или прямоугольниками изображают возможные состояния системы. Он содержит столько вершин, сколько различных состояний возможно у объекта или системы. Ребра графа отражают возможные переходы из некоторого состояния во все остальные с параметрами интенсивностей отказов и восстановлений (около стрелок показаны интенсивности переходов).

Каждой комбинации отказовых и работоспособных состояний подсистем соответствует одно состояние системы. Число состояний системы $n = 2^k$, где k – количество подсистем (элементов).

Связь между вероятностями нахождения системы во всех его возможных состояниях выражается системой дифференциальных уравнений Колмогорова (уравнений первого порядка).

Структура уравнений Колмогорова построена по следующим правилам: в левой части каждого уравнения записывается производная вероятности нахождения объекта в рассматриваемом состоянии (вершине графа), а правая часть содержит столько членов, сколько ребер графа состояний связано с этой вершиной. Если ребро направлено из данной вершины, соответствующий член имеет знак минус, если в данную вершину – знак плюс. Каждый член равен произведению параметра интенсивности отказа (восстановления), связанного с данным ребром, на вероятность нахождения в той вершине графа, из которой исходит ребро.

Система уравнений Колмогорова включает столько уравнений, сколько вершин в графе состояний объекта.

Система дифференциальных уравнений дополняется нормировочным условием:

$$\sum_{j=0}^{n} P_j(t) = 1,$$

где $P_j(t)$ – вероятность нахождения системы в j-м состоянии;

n – число возможных состояний системы.

Решение системы уравнений при конкретных условиях дает значение искомых вероятностей $P_j(t)$.

Все множество возможных состояний системы разбивается на две части: подмножество состояний n_1, в которых система работоспособна, и подмножество состояний n_2, в которых система неработоспособна.

Функция готовности системы:

$$K_{\text{г}}(t) = \sum_{j=0}^{n_1} P_j(t) = 1,$$

где $P_j(t)$ – вероятность нахождения системы в j работоспособном состоянии;

n_1 – число состояний в которых система работоспособна.

Когда необходимо вычислить коэффициент готовности системы или коэффициент простоя (перерывы в работе системы допустимы), рассматривают установившийся режим эксплуатации при $t \to \infty$. При этом все производные $P_j'(t) = 0$ и система дифференциальных уравнений переходят в систему алгебраических уравнений, которые легко решаются.

Пример графа состояний нерезервированной восстанавливаемой системы с n – элементами приведен на рис. 1.

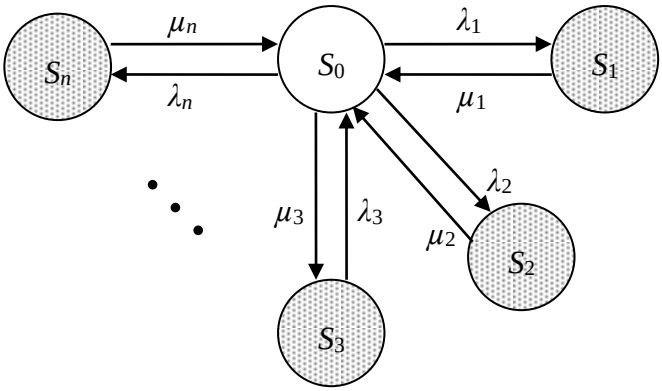


Рис. 1. Граф состояний восстанавливаемой системы (штриховкой отмечены неработоспособные состояния)

Рассмотрим возможные состояния в которых может находиться система. Здесь возможны следующие состояния:

S_0 – все элементы работоспособны;

S_1 – первый элемент неработоспособен остальные работоспособны;

S_2 – второй элемент неработоспособен остальные работоспособны;

.

.

.

S_n – n-й элемент неработоспособен остальные работоспособны.

Вероятность одновременного появления двух неработоспособных элементов пренебрежимо мала. Символами $\lambda_1, \lambda_2, \ldots, \lambda_n$ обозначены интенсивности отказов, $\mu_1, \mu_2, \ldots, \mu_n$ интенсивности восстановления соответствующих элементов;

По графу состояний (рис. 1) составляют систему дифференциальных уравнений (уравнение для состояния S_0 опускаем из-за громоздкости):

С нормировочным условием: $\sum_{j=0}^{n} P_j(t) = 1.$

$$\left.\begin{aligned} dP_1(t)/dt &= \lambda_1 \cdot P_0(t) - \mu_1 \cdot P_1(t) \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ dP_2(t)/dt &= \lambda_2 \cdot P_0(t) - \mu_2 \cdot P_2(t) \\ &\cdot \\ &\cdot \\ &\cdot \\ dP_n(t)/dt &= \lambda_n \cdot P_0(t) - \mu_n \cdot P_n(t) \end{aligned}\right\}$$

Начальные условия:

$$\overset{0}{P_0}(t) = 1$$
$$P_1(\underset{t}{0}) = P_2(0) = \ldots = P_n(0) = 0$$

При установившемся режиме эксплуатации (при $t \to \infty$) имеем:

$$\left.\begin{aligned} \lambda_1 \cdot P_0(t) - \mu_1 \cdot P_1(t) &= 0 \\ \lambda_2 \cdot P_0(t) - \mu_2 \cdot P_2(t) &= 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \lambda_n \cdot P_0(t) - \mu_n \cdot P_n(t) &= 0 \end{aligned}\right\}$$

Решив полученную систему алгебраических уравнений с учетом нормировочного условия, находим показатели надежности.

При решении системы уравнений можно использовать преобразование Лапласа для вероятностей состояний или численные методы.

Контрольные вопросы и задания

1. Какие методы определения показателей надежности восстанавливаемых систем известны?
2. Как определяются состояния элементов и устройств ИС?
3. Как определить области работоспособных состояний системы?

4. Почему метод дифференциальных уравнений получил широкое распространение при оценке надежности восстанавливаемых систем?
5. Что является необходимым условием при решении систем дифференциальных уравнений?
6. Как составляется дифференциальные уравнения для определения параметров надежности ИС?
7. Каким условием должно быть дополнено система дифференциальных уравнений (СДУ) для более эффективного решения.
8. Запишите условия работоспособности системы, состоящий из трех элементов.
9. Чему равно число состояний устройства состоящего из четырех элементов?
10. Какое правило используется при составлении СДУ?

Литература: 1, 2, 3, 5, 6, 8.

Лекция 11

Тема: Марковские модели для оценки надежности резервированных восстанавливаемых информационных систем

План

1. Понятие Марковского свойства, определение состояния системы.
2. Методика и алгоритм построения Марковской модели.
3. Расчетные формулы для расчета показатели надежности ТС
4. Матрица интенсивностей переходов для оценки показателей надежности резервированных восстанавливаемых ИС.

Ключевые слова

Марковская модель, состояние системы, работоспособность, матрица интенсивностей переходов, граф состояний, восстанавливаемая система, резервирование, последовательная схема, постоянный резерв, система дифференциальных уравнений, правило Колмогорова, схема расчета надежности, приближенный метод, алгоритмы построения СДУ, нормировочные условия, начальные условия, вероятность безотказной работы, интенсивность отказа.

Функционирование ИС и их составных частей можно представить как совокупность процессов перехода из одного состояния в другое под воздействием каких либо причин.

С точки зрения надежности восстанавливаемых ИС их состояние в каждый момент времени характеризуется тем, какие из элементов работоспособны, а какие восстанавливаются.

Если каждому возможному множеству работоспособных (неработоспособных) элементов поставить в соответствие множество состояний объекта, то отказы и восстановления элементов будут отображаться переходом объекта из одного состояния в другое:

Пусть, к примеру, объект состоит из двух элементов. Тогда он может находиться в одном из четырех состояний: $n = 2^k = 2^2 = 4$.

S_1 – оба элемента работоспособны;

S_2 – неработоспособен только первый элемент;

S_3 – неработоспособен только второй элемент;

S_4 – неработоспособны оба элемента.

Множество возможных состояний объекта: $S = \{S_1, S_2, S_3, S_4\}$.

Полное множество состояний исследуемой системы может быть дискретным, либо непрерывным (непрерывно заполнять один или несколько интервалов числовой оси).

В дальнейшем будем рассматривать системы с дискретным пространством состояний. Последовательность состояний такой системы и сам процесс переходов из одного состояния в другое называется цепью.

В зависимости от времени пребывания системы в каждом состоянии различают процессы с непрерывным временем и процессы с дискретным временем. В процессах с непрерывным временем переход системы из одного состояния в другое осуществляется в любой момент времени. Во втором случае время пребывания системы в каждом состоянии – фиксировано так, что моменты переходов размещаются на временной оси через равные промежутки.

В настоящее время наиболее изучены цепи, обладающие марковским свойством. Вероятности переходов обозначаются символами $P_{ij}(t)$, а процесс P_{ij} переходов называется Марковской цепью или цепью Маркова.

Марковское свойство связанно с отсутствием последействия. Это означает, что поведение системы в будущем зависит только от ее состояния в данный момент времени, и не зависит от того каким образом она пришла в это состояние.

Марковские процессы позволяют описать последовательности отказов-восстановлений в системах, описываемых при помощи графа состояний.

Наиболее часто для расчета надежности применяется метод марковских цепей с непрерывным временем, основанный на системе дифференциальных уравнений, которая в матричной форме может быть записана как:

$$\frac{dP(t)}{dt} = P(t) \cdot \Lambda,$$

где $P(t) = P_0$ – начальные условия;

$$\frac{dP(t)}{d(t)} = \left[\frac{dP_1(t)}{dt} \frac{dP_2(t)}{dt} \ldots\ldots\ldots \frac{dP_n(t)}{dt} \right],$$

а Λ – матрица интенсивности переходов (матрица коэффициента при вероятностях состояний):

$$\Lambda = \begin{vmatrix} -\sum_{i=2}^{n} \lambda_{1i} & \lambda_{12} & \lambda_{13} & . & \lambda_{1n} \\ \lambda_{21} & -\sum_{i=1}^{n} \lambda_{2i} & \lambda_{23} & . & \lambda_{2n} \\ \lambda_{31} & \lambda_{32} & -\sum_{i=1}^{n} \lambda_{3i} & . & \lambda_{3n} \\ . & . & . & . & . \\ \lambda_{n1} & \lambda_{n2} & \lambda_{n3} & . & -\sum_{i=1}^{n} \lambda_{ni} \end{vmatrix}$$

$$\lambda_i = -\sum_{\substack{j=1 \\ i=1}}^{n} \lambda_{ij},$$

где λ_{ij} – интенсивности перехода системы из i-го состояния в j-е;

P_j – вероятность того, что система находится в j-м состоянии.

При оценке надежности сложных резервированных и восстанавливаемых систем метод марковских цепей приводит к сложным решениям из-за большого числа состояний. В случае однотипных подсистем работающих в одинаковых условиях, для уменьшения числа состояний используют метод укрупнения. Состояния с одинаковым количеством подсистем объединяются. Тогда размерность уравнений уменьшается [1, 2, 3, 5, 8].

Последовательность методики оценки надежности резервированных восстанавливаемых систем с использованием метода марковских цепей следующая:

1. Анализируется состав устройства и составляется структурная схема надежности. По схеме строится граф, в котором учитывается все возможные состояния;
2. Все вершины графа в результате анализа структурной схемы разделяются на два подмножества: вершины соответствующие работоспособному состоянию системы и вершины соответствующие неработоспособному состоянию системы.
3. С помощью графа состояний составляется система дифференциальных уравнений (используется правило Колмогорова);
4. Выбираются начальные условия решения задачи;
5. Определяются вероятности нахождения системы в работоспособном состоянии в произвольный момент времени;
6. Определяется вероятность безотказной работы системы;
7. В случае необходимости определяются и другие показатели.

Контрольные вопросы и задания

1. Что подразумевается под цепью Маркова?
2. Приведите алгоритм оценки надежности ИС с использованием Марковских моделей.
3. Как составляется дифференциальные уравнения для определения параметров надежности ИС?
4. Значение каких показателей надежности можно получить используя Марковский метод?
5. Перечислите основные этапы построения Марковской модели надежности сложной системы.
6. Что является необходимым условием при решении систем дифференциальных уравнений?

7. Как определяются состояния элементов и устройств КС?
8. Дайте определение понятию восстанавливаемых систем.
9. Что такое Марковская цепь?
10. Для оценки каких систем используют Марковские модели надежности?

Литература: 1, 2, 3, 10, 11.

Лекция 12

Тема: Приближенные методы расчета надежности технических средств ИС

План

1. Основные допущение и ограничения при оценки надежности последовательно-параллельных структур.
2. Приближенные методы расчета надежности восстанавливаемых ИС, при последовательном и параллельном включении подсистем ИС.
3. Структурные схемы расчета надежности ИС.

Ключевые слова

Надежность, последовательно-параллельная структура, приближенные методы расчета надежности, структурное схема расчета надежности, интенсивность отказа, интенсивность восстановления, коэффициент готовности, время восстановления, компьютерная система.

Приближенный метод расчета надежности восстанавливаемых КС

Рассмотрим простой приближенный метод расчета установившихся значений показателей надежности восстанавливаемых КС. Метод основан на следующих допущениях:

1. Время восстановления намного меньше времени безотказной работы;
2. Интенсивности отказов и восстановлений системы – постоянные величины;
3. Отказы и восстановления отдельных подсистем – независимые случайные события;

Для последовательного включения подсистем имеются следующие приближенные зависимости:

$$\left.\begin{aligned} \lambda_i &= \sum_{i=1}^{n} \lambda_i \\ K_г &= 1 - n + \sum_{i=1}^{n} K_{гi} \\ \mu &= \lambda/(1-K_г) \end{aligned}\right\} \qquad (1)$$

Для параллельного включения подсистем:

$$\left.\begin{aligned} \mu_i &= \sum_{i=1}^{m} \mu_i \\ K_г &= 1 - n + \prod_{i=1}^{m} (1 - K_{гi}) \\ \lambda &= \mu \cdot (1 - K_г) \end{aligned}\right\} \qquad (2)$$

В этих формулах приняты следующие обозначения:

λ – интенсивность отказов $n(m)$ последовательной ($n(m)$ параллельной) системы из $n(m)$ подсистем.

$K_г$ – коэффициент готовности последовательной (параллельной) подсистемы группы из $n(m)$.

Те же переменные с индексом i обозначают соответствующие показатели отдельных подсистем.

Если в системе применяется скользящее резервирование, то для определения коэффициента готовности применяется формула:

$$K_г = \sum_{i=r}^{m} C_m^i K_{гп}^i (1 - K_{гп})^{m-i}, \qquad (3)$$

где r – минимально необходимое по требованиям производительности число работоспособных подсистем;

$K_{гп}$ – коэффициент готовности подсистем (при скользящем резервировании все подсистемы однотипны).

Интенсивность восстановления в случае скользящего резервирования определяется по формуле:

$$\mu = (m\text{-}r+1)\cdot\mu_n , \qquad (4)$$

μ_n – интенсивность восстановления подсистем.

В случае указанных выше допущений интенсивность отказов λ численно равна параметру потока отказов w.

Рассмотрим КС, состоящую из шести подсистем: ЦП, ОЗУ, МД, МЛ, ПУ и УВ. Данные для подсистем приведены в таблице 1:

Используя приближенные формулы, рассчитать показатели надежности.

Таблица 1.

Наименование	Значения $m(r)$	Интенсивность		Коэффициент готовности $K_{гi}$
		Отказов λ_i,1/ч	Восстановлений μ_n, 1/ч	
Центральный процессор (ЦП)	1	$152\cdot10^{-6}$	1	$1\text{-}1{,}52\cdot10^{-4}$
Модуль ОЗУ	4(3)	$300\cdot10^{-6}$	0,01	$1\text{-}3\cdot10^{-2}$
Устройство памяти на дисках (МД)	3(2)	$250\cdot10^{-6}$	0,025	$1\text{-}10^{-2}$

Устройство памяти на магнитных лентах (МЛ)	8(2)	$350 \cdot 10^{-6}$	0,0035	$1\text{-}10^{-1}$
Печатающее устройство (ПУ)	2(1)	$420 \cdot 10^{-6}$	0,021	$1\text{-}2 \cdot 10^{-2}$
Устройство ввода с перфоленты (УВ)	2(1)	$250 \cdot 10^{-6}$	0,025	$1\text{-}10^{-2}$

Схема расчета надежности КС имеет вид:

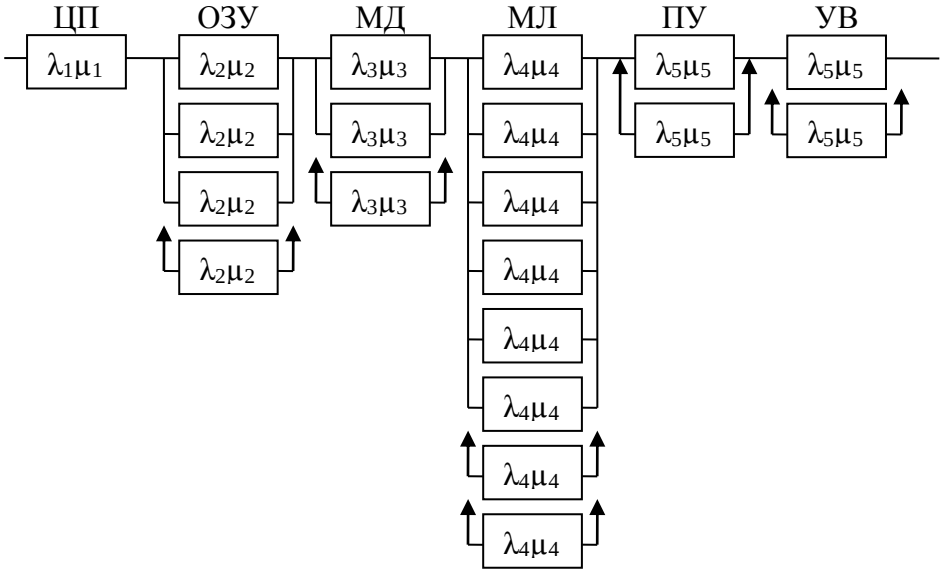


Рис. 1. Схема расчета надежности.

Контрольные вопросы и задания

1. Определите понятие надежности ИС.
2. Какие виды отказов учитываются при расчете надежности последовательно-параллельных структур?
3. Как определяется интенсивность восстановления при последовательном соединении подсистем КС?
4. Определите значение коэффициента готовности при параллельном соединении подсистем КС.
5. Как определяется интенсивность восстановления при скользящем резервировании подсистем КС?
6. Приведите структурную схему надежности особо ответственных КС для расчета показателей безотказности систем.
7. Какова значения интенсивности отказов современного процессора?
8. Какой вид резервирования использован для повышения надежности оперативного запоминающего устройства (рис. 1)?

Литературы: 1, 2, 3, 5, 8.

Лекция 13

Тема: Надежность программного обеспечения информационных систем

План

1. Основные понятия и определения надежности программного обеспечения.
2. Показатели надежности программного обеспечения.
3. Причины отказов программного обеспечения, признаки появления ошибок.
4. Способы обеспечения и повышения надежности программ.

Ключевые слова

Надежность программного обеспечения, ПО, отказ, скрытые ошибки, спецификация, корректность программы, контроль ПО, логические ошибки, ошибки ввода-вывода, сбой, резервирование программ, ошибки манипулирования.

Основные понятия надежности ПО

Надежность работы вычислительной аппаратуры следует рассматривать совместно с программным обеспечением как надежность вычислительного процесса.

Под *надежностью программного обеспечения* (ПО) будем понимать свойство программы выполнять заданные функции, сохранять свои характеристики в установленных переделах при определенных условиях эксплуатации.

Надежность ПО определяется его безотказностью и восстанавливаемостью.

Безотказность программы или программного обеспечения есть его (ее) свойство сохранять работоспособность при использовании в процессе обработки информации на компьютере.

Безотказность ПО можно оценивать вероятностью его работы без отказов при определенных условиях внешней среды в течении заданного времени наблюдения.

Безотказность программного средства можно также характеризовать средним временем между возникновениями отказов в функционировании программы. При этом предполагается, что аппаратура компьютера находится полностью в работоспособном состоянии.

С точки зрения надежности принципиальное отличие ПО от аппаратуры состоит в том, что программы не изнашиваются и, следовательно, не выходят из строя из-за поломки.

Безотказность ПО определяется его корректностью (правильностью) и, следовательно, целиком зависит от наличия в нем ошибок, внесенных на этапах его создания. В то время как безотказность аппаратуры определяется в основном случайными отказами, зависящими от изменений параметров аппаратуры во время эксплуатации.

Механизм возникновения отказа аппаратуры и отказа ПО существенно отличаются друг от друга. Отказ аппаратуры обусловлен разрушением каких-либо элементов аппаратуры. Отказ ПО обусловлен несоответствием ПО поставленным задачам.

Несоответствие может возникать по двум причинам: либо разработчиком программы допущено нарушение спецификации – технических требований к программе, либо спецификация неточная или неполная.

Корректность программы – ее соответствие спецификации.

Важной характеристикой надежности ПО является его *восстанавливаемость*, которая определяется затратами времени и труда не устранение отказа из-за проявившейся ошибки в программе и его последствий.

Восстановление после отказа в программе может заключаться в корректировке и восстановлении текста программы, исправлении данных, внесении изменений в организацию вычислительного процесса.

Восстанавливаемость ПО может быть оценена средней продолжительностью устранение ошибки в программе и восстановления ее работоспособности. Восстанавливаемость ПО зависит от многих факторов: от сложности структуры комплекса программ, алгоритмического языка, на котором разрабатывалась программа, стиля программирования, качества документации на программу и т.д.

Причины отказов программного обеспечения

Основными причинами непосредственно вызывающими нарушение нормального функционирования программы, являются [1, 2, 3, 10, 11]:

1. ошибки, скрытые в самой программе;
2. искажения входной информации, подлежащей обработке;
3. неверные действия пользователя;
4. неисправность аппаратуры установки, на которой реализуется вычислительный процесс.

1. *Скрытые ошибки* программы являются главным фактором нарушения нормальных условий его функционирования;

Можно выделить следующие основные ошибки в программе:

- *Ошибки* вычислений – ошибки данного класса содержаться в закодированных математических выражениях или получаемых с их помощью результатах. Примерами таких ошибок является неверное преобразование типов переменных, неверный знак операции, ошибка в

выражении индекса, переполнение или потеря значимости при вычислениях.

- *Логические* ошибки – являются причиной искажения алгоритма решения задачи. Такого рода ошибки возникают в связи с неверной передачей управления, неверном задании диапазона изменения параметров цикла, неверных условий и т.д.
- *Ошибки* ввода-вывода – связаны с такими действиями, как управление вводом-выводом, формирование выходных записей и определение размеров записей.
- *Ошибки* манипулирования данными – примерами таких ошибок являются неверно определенное число элементов данных, неверные начальные значения, присвоенные данным, неверно указанная длина операнда, имя переменной и т.д.

Ошибки совместимости связанны с отсутствием совместимости с операционной системой или другими прикладными программами используемыми в данной программе.

Ошибки сопряжений вызывают неверное взаимодействие программы с другими программами (подпрограммами), с системными программами, устройствами компьютера, входными данными и т.д.

В качестве примеров ошибок сопряжения можно привести – несовместимость аргументов и параметров подпрограммы, нарушение синхронизации при синхронном выполнении программы и т.д.

2. *Искажения информации*, подлежащей обработке, вызывает нарушение функционирования ПО, когда входные данные не попадают в область допустимых значений переменных программы. В этом случае между исходной информацией и характеристиками программы возникает несоответствие.

Причинами искажения вводимой информации могут быть, например, следующие:

- искажения данных на первичных носителях информации;
- сбои и отказы в аппаратуре ввода данных с первичных носителей информации;
- шумы и сбои в каналах связи при передачи сообщений по линиям связи и т.д.

3. *Неверные действия* пользователя, приводящие к отказу в процессе функционирования ПО связаны, прежде всего, с неправильной интерпретацией сообщений, неправильными действами пользователя в процессе диалога с компьютером и т.д.

4. *Неисправность аппаратуры* – неисправности, возникающие при работе аппаратуры, используемой для реализации вычислительного процесса, оказывают влияние на характеристику надежности ПО. Появление отказа или сбоя в работе аппаратуры приводит к нарушению нормального хода вычислительного процесса и во многих случаях к искажению данных и текстов программ в основной и внешней памяти.

Признаки появления ошибок

Наиболее типичными симптомами появления ошибок в программе являются:

- преждевременное окончание выполнения программы;
- недопустимое увеличение времени некоторой последовательности команд одной из программ;
- полная потеря или значительное искажение накопленных данных, необходимых для успешного выполнения решаемых задач;
- нарушение последовательности вызова отдельных программ, в результате чего происходит пропуск необходимых программ;
- искажение отдельных элементов данных (входных, выходных, промежуточных) в результате обработки искаженной исходной информации.

Способы обеспечения и повышения надежности программ

Они определены на следующие основные категории:

1. усовершенствование технологии программирования;
2. выбор алгоритмов, не чувствительных к различного рода нарушениям вычислительного процесса (использование алгоритмической избыточности);
3. резервирование программ – дуальное или N-версионное программирование, другие методы введения структурной избыточности;
4. контроль и тестирование программ с последующей коррекцией.

Выбор алгоритмов, не чувствительных к нарушениям вычислительного процесса, основан на исследовании их чувствительности. Мерой чувствительности могут являться погрешности, вызванные этими нарушениями.

Результаты вычислений искажаются погрешностями:

- исходных данных, трансформированными в ходе вычислений:
- округления;
- методическими;
- обусловленными отказами, сбоями и ошибками в программе.

Контрольные вопросы и задания

1. Что понимается под надежностью программного обеспечения (ПО)?
2. Что такое корректность ПО?
3. От чего зависит восстанавливаемость ПО компьютера и КС?
4. Определите основные причины отказов ПО.
5. Какие существуют пути повышения надежности ПО компьютеров и КС?

6. Почему при мультипрограммной обработке информации используют принцип виртуальных машин?
7. Какой из способов обеспечения надежности программ считается более эффективным?
8. Что значит «усовершенствование технологии программирования»?
9. Дайте определение понятию «дуальное и N-версионное» программирование.
10. Как оценить вероятность безотказной работы программ?
11. Что означает термин «алгоритмическая избыточность»?

Литература: 1, 2, 3, 9, 10, 11.

Лекция 14

Тема: Методы введения структурной избыточности в программы

План

1. Понятие о дуальном и N-версионном программировании.
2. Модифицированное дуальное программирование.
3. Виртуальные машины в надежности.
4. Избыточность операционной системы ИС.

Ключевые слова

Дуальное программирование, N-версионное программирование, тестирование программ, алгоритмическая избыточность, виртуальная машина, мультипрограммная обработка, монитор, режим реального времени.

Методы введения структурной избыточности в программы

Надежность программ повышают путем резервирования. Для этого подготавливаются две или несколько версий программ для решения одной и той же задачи. Желательно, чтобы эти версии значительно отличались друг от друга, т.е. основывались, по возможности на различных алгоритмах или были выполнены различными программистами.

Ошибки в программах могут быть обнаружены в ходе отладки версии и программ сравнением результатов. Однако, даже в случае простых программ проверить в ходе отладки все возможные комбинации исходных данных или все возможные последовательности прохождения элементов программы невозможно.

Поэтому была предложена идея параллельного (одновременного) или последовательного во времени выполнения различных версий программ непосредственно в процессе эксплуатации. Версии программ могут быть две или больше. Если версий две – дуальное программирование. *При дуальном программировании*, если обнаруживается расхождение в результатах (результаты сравниваются соответствующими аппаратными средствами), то необходимо определить, по каким-либо дополнительным критериям, какой из результатов правильный и после этого отбрасывать другой результат.

При N-версионном программировании подготавливаются N-версий программ, и правильный результат определяется по мажоритарному признаку при помощи аппаратных или программных средств.

При дуальном или N-версионном программировании требуется в два или N раз больше времени для вычислений, если последние выполняются последовательно во времени. Кроме того, объем труда программистов возрастает во столько же раз.

Дуальное и *N*-версионное программирование целесообразно использовать в случае, если имеет место нагруженное резервирование вычислительной аппаратуры [1, 2, 51].

Создание нескольких версий программ – трудоемкий и дорогостоящий процесс. Поэтому часто используют *модифицированное дуальное программирование*, где наряду с достаточно точной, но сложной программой используется менее точная, но простая резервная программа. Если при одинаковых исходных данных результаты работы программ отличаются на величину большую, чем допустимая погрешность, делается предположение о том, что отказала основная программа, как менее надежная, и в качестве правильного результата принимается результат, полученный при помощи резервной программы. В результате средняя погрешность работы двух программ несколько увеличивается, но вероятность отказа уменьшается.

Обозначим погрешность первой программы через δ_1 и допустимую погрешность второй программы через δ_2. Пусть вероятность отказа (возникновение погрешности значительно больше допустимой) первой программы составляет q_1 и второй программы – q_2.

При независимости этих программ возможны следующие несовместимые события:

1) обе программы работают безотказно, вероятность возникновения этого события $P = 1 - q_1 - q_2 + q_1 \cdot q_2$, погрешность результата – δ_1;
2) откажет основная программа, вероятность возникновения этого события $q_{01} = q_1 \cdot (1 - q_2) = q_1 - q_1 \cdot q_2$, погрешность результата – δ_2;
3) откажет резервная программа, вероятность возникновения этого события $q_{10} = q_2 \cdot (1 - q_1) = q_2 - q_1 \cdot q_2$, погрешность результата – весьма значительная, допустим δ_3 (погрешность отказавшей резервной программы);
4) откажут и основная, и резервная программы, вероятность возникновения этого события $q_{11} = q_1 \cdot q_2$, погрешность δ_3.

Средняя погрешность неотказавшей системы из двух программ равна:

$$\delta_{12} = \frac{P \cdot \delta_1 + q_{01} \cdot \delta_2}{P + q_{01}} = \frac{1 - q_1 + q_2 + q_1 \cdot q_2}{1 - q_2} \cdot \delta_1 + \frac{q_1 - q_1 q_2}{1 - q_2} \cdot \delta_2 = (1 - q_1)\delta_1 + q_1 \delta_2,$$

при вероятности отказа системы:

$$q_c = q_{10} + q_{11} = q_2 - q_1 \cdot q_2 + q_1 \cdot q_2 = q_2.$$

В случае, когда имеется только основная программа, погрешность результата равна δ_1, а вероятность отказа – q_1.

Пример расчета надежности и точности системы с применением модифицированного дуального программирования. Пусть δ_1 = 0,01;

$\delta_2 = 0{,}1$; $q_1 = 0{,}05$; $q_2 = 0{,}001$. Тогда $\delta_{12} = 0{,}95 \cdot 0{,}01 + 0{,}05 \cdot 0{,}1 = 0{,}0145$ и $q_c = q_2 = 0{,}001$.

Следовательно, при использовании системы, состоящей из точной и грубой программы с решающим органом, средняя погрешность работы системы по сравнению с точной программой возрастает в 1,5 раза, а вероятность отказа уменьшается в 50 раз.

Решающим органом при этом является простейшая программа, которая сравнивает результаты работы грубой и точной программы и реализует алгоритм:

$$y = \begin{cases} y_1, \text{если} \mid y_1 - y_2 \mid \leq \delta_1 + \delta_2 \\ y_2, \text{если} \mid y_1 - y_2 \mid > \delta_1 + \delta_2 \end{cases}$$

y_1 – результат первой программы;
y_2 – результат второй программы.

В случае, когда абсолютная разность превышает максимальную суммарную погрешность двух программ, алгоритм осуществляет отбрасывание результата y_1 первой и выдачу результата y_2 второй программы.

Эта описанная система эффективна в случае, когда критерием ее эффективности является усредненная по времени погрешность. Если же эффективность системы определяется максимальным значением погрешности, описанный способ резервирования не эффективен.

Избыточность операционной системы

Методы дуального и *N*-версионного резервирования программ применяются, как относительно программ пользователя, так и относительно операционных систем.

Повышение надежности программ обеспечит применение принципа виртуальной машины в случае мультипрограммной обработки.

Виртуальные машины образуются при помощи *монитора* – специальной программы или программно-аппаратной системы, которая создает для каждого пользователя иллюзию работы на отдельной вычислительной машине.

Виртуальная память (кажущаяся память компьютера), система ЗУ, организованы таким образом, что программист может рассматривать их как одну большую оперативную память, что существенно упрощает процедуру составления программ для мультипрограммных компьютеров.

При этом важна высокая степень изоляции каждой виртуальной машины. Тогда ошибка в программе одной виртуальной машины не влияет на другие.

Высокая степень изоляции может быть достигнута созданием отдельных операционных систем для каждого пользователя. Тогда ошибка в

одной операционной системе не сказывается на работе операционных систем других виртуальных машин.

На рис. 1 изображена структура мультипрограммной обработки на одном компьютере без применения принципа виртуальной машины. Пользователи $П_1$, $П_2$, ... , $П_n$ имеют общую операционную систему ОС. Ошибка в ОС выводит из строя всех пользователей. На рис. 2 изображена структура системы с виртуальными машинами высокой степени изоляции. Только ошибка в сравнительно небольшой программе – мониторе М влечет за собой нарушение работы пользователей $П_1$, $П_2$, ... , $П_n$. Отказы индивидуальных операционных систем $ОС_1$, $ОС_2$, ... , $ОС_n$ вызывают нарушения в работе только «своего» пользователя.

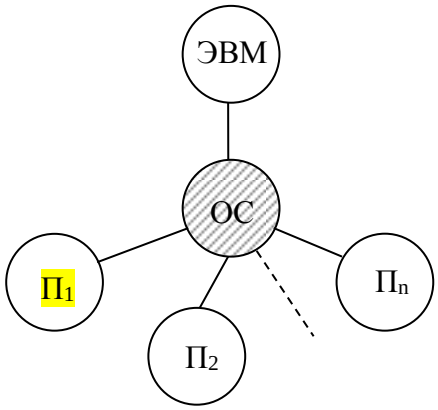


Рис. 1. Структура мультипрограммной обработки

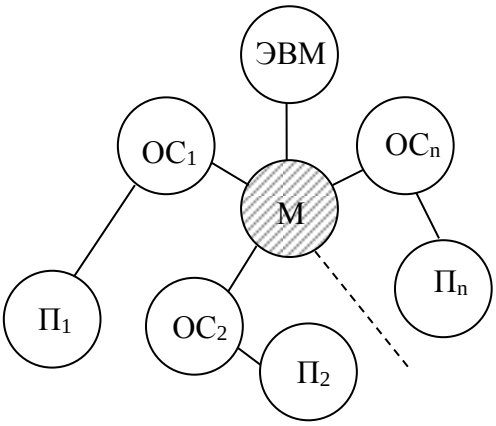


Рис. 2. Структура мультипрограммной обработки с разделением ОС

Метод контрольных функций.

Методы введения избыточности в программы основаны на повторении программ в различных версиях (дуальное, *N*-версионное программирование). Такие методы повышения надежности не экономичны как в смысле расхода ручного труда программиста, так и в смысле использования объема памяти для записи программ, так и экономии машинного времени.

Существует более экономический метод повышения надежности программ – *метод контрольных функций*. При этом методе, наряду с вычисляемой функцией, по иной программе определяется другая функция, находящаяся с основной вычисляемой функцией в соотношениях, называемых *контрольными соотношениями*. Эти соотношения позволяют не только обнаружить отказ одной из программ, но также и восстановить искаженный результат отказавшей программы на основании результата, полученного по безошибочно работающей программе (программам).

Простейшим примером применения метода контрольных соотношений является вычисление функций $\sin x$ и $\cos x$ по отдельным программам. Контрольным соотношениям в данном случае будет соотношение $\sin^2 x + \cos^2 x = 1$.

Пусть имеются две независимые программы, вычисляющие числовые функции f_1 и f_2 (аргументы функции для простоты записи опущены). Необходимо исправлять любую одиночную ошибку в программах. Опишем подход, требующий три дополнительные программы, вычисляющие значения вспомогательных контрольных функций f_3, f_4, f_5 [1]. Эти функции могут, например, удовлетворять уравнениям

$$\begin{aligned} &a_{11} f_1 + a_{12} f_2 + a_{13} f_3 = 0 \\ &a_{21} f_1 + a_{22} f_2 + a_{24} f_4 = 0 \\ &a_{31} f_1 + a_{35} f_5 = 0, \end{aligned} \qquad (1)$$

где $a_{ij} \neq 0$ – произвольные постоянные.

Пусть имеются k-процессоров, вычисляющих числовые функции $f_1,..., f_k$, и ошибки вычислений $f_1,..., f_k$ – независимы. Необходимо исправлять любую одиночную программную ошибку.

(1) была построена на основе контрольной матрицы (код Хэмминга) [ ]. Система

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Для построения контрольных функций $\sum_{j=1}^{k+1} a_{ij} \cdot f_j = 0$ при $i = 1,\ldots, r$, где a_{ij} – постоянные, необходимо выбрать двоичную $r \cdot (k + r)$ матрицу $[h_{ij}]$ с отличающимися друг от друга столбцами, не равными нулю, а затем применить соотношение

$$a_{ij} = a_{ij} \cdot h_{ij}, \qquad (2)$$

где $a_{ij} \neq 0$ произвольные постоянные.

Таким образом, изложенный в подход является обобщением методов кодирования с обнаружением и исправлением ошибок и позволяет исправлять не элемент кода, а вычисляемую функцию, содержащую ошибку. Метод целесообразно использовать тогда, когда имеются независимые программы для вычисления различных функций.

Пример исправления одиночной ошибки с помощью контрольных функций. Пусть вычисляются четыре функции f_1, f_2, f_3, f_4. Необходимо построить систему, позволяющую исправлять ошибку в одной из функции. Для построения системы уравнений используется матрица *H* Хэмминга вида

$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Выбирая коэффициенты d_{ij} равными единице, непосредственно по матрице H с учетом (2) записывается система уравнений:

$$f_2 + f_3 + f_4 + f_5 = 0,$$
$$f_1 + f_3 + f_4 + f_6 = 0,$$
$$f_1 + f_2 + f_4 + f_7 = 0,$$

где дополнительные контрольные функции f_5, f_6 и f_7 определяются по следующим очевидным соотношениям: $f_5 = -(f_2 + f_3 + f_4)$; $f_6 = -(f_1 + f_3 + f_4)$; $f_7 = -(f_1 + f_2 + f_4)$. Если, например, возникает ошибка e_2 при вычислении функции f_2, то $S_1 = S_2 = e_2$, $S_2 = 0$. По виду синдрома ($S_1 \neq 0$, $S_2 = 0$, $S_3 \neq 0$) определяется, что ошибка соответствует второму столбцу матрицы H, т.е. ошибка e_2 относится к функции f_2 и последняя может быть скорректирована вычитанием этой ошибки.

Аналогично исправляются ошибки и в функциях f_1, f_3, f_4.

Контрольные вопросы и задания.

1. Какие существуют методы повышения надежности ПО?
2. Определите разницу между дуальными и N-версионным программированием.
3. Что такое мультимпрограммный режим работы компьютера?
4. Дайте определение понятию монитор.
5. В каких случаях используется модифицированное дуальное программирование?
6. Почему при мультипрограммной обработке информации используют принцип виртуальных машин?
7. Оцените общее число ошибок в тексте программы, если программа проверена тремя специалистами и если первый из них нашел в программе 3 ошибки, второй – 5 ошибок, а третий – 6 ошибок, причем две ошибки из найденных были общими у всех специалистов.

Литературы: 2,3,6, 8,11

Лекция 15
Тема: Модели надёжности программ

План

1. Аналитические модели надёжности программ. Модель надёжности с дискретно-понижающейся интенсивностью проявление ошибок.
2. Экспоненциальная и интуитивная модели, модель надёжности больших программных комплексов и др.
3. Методы оценки и прогнозирование показателей надёжности программного обеспечение.
4. Область использования моделей программного обеспечения ТС

Ключевые слова

Аналитическая модель, показатели надёжности, модели программ, ошибки, программное обеспечение, интуитивная модель, экспоненциальная модель, ранее прогнозирование, вероятность безотказной работы, сохраняемость программ, безотказность, вероятность отказа, модель Джелинского-Моранды, модель Шумана, модель Шика-Волвертона, интенсивность отказов, время восстановления

Аналитические модели надежности дают возможность исследовать закономерности проявления ошибок в программе, а также прогнозировать надежность при разработке и эксплуатации.

Модели надежности программ строятся на предположении о том, что проявление ошибки является случайным событием и поэтому имеет вероятностный характер. Такие модели предназначены для оценки показателей надежности программ и программных комплексов в процессе тестирования. Они дают возможность принять обоснованное решение о времени проектирования отладочных работ.

При построении моделей используются следующие характеристики надежности программ.

Функция надежности $P(t)$, определяется как вероятность того, что ошибки программы не проявляются на интервале времени от 0 до t, т.е временя ее безотказной работы будет больше.

Функция надежности $Q(t)$ – вероятность того, что в течение времени t произойдет отказ программы как результат проявления действия ошибки в программе. Таким образом:

$$Q(t) = 1 - P(t)$$

Интенсивность отказов $\lambda(t)$ – условная плотность вероятности времени от возникновения отказа программы при условии, что до момента t отказа не было.

$$\lambda(t) = -\frac{dP(t)}{dt} \Big/ P(t) = \left|\frac{dQ(t)}{dt}\right| \Big/ P(t)$$

Основными типами применяемых моделей надежности программ являются модели, основанные на предположении о дискретном изменении характеристик надежности программ, и модели с экспоненциальным характером изменения числа ошибок в зависимости от времени тестирования и функционирования программы.

Прогнозирование надежности программ в ходе эксплуатации осуществляется на основе математических моделей надежности, предложенных Литтлвудом, Джелинским-Морандой, Шуманом, Шика-Вольвертоном. Существуют модели надежности программ с дискретно-понижающейся частотой (интенсивностью) появления ошибок и с дискретным увеличением времени наработки на отказ, экспоненциальная модель. Кроме того, созданы модели надежности для прогнозирования надежности программ на ранних этапах их разработки. Рассмотрим некоторые из них [2, 3, 6, 11].

Анализ надежности функционирования крупных зарубежных и российских программных комплексов показывает, что надежность ПО значительно ниже надежности аппаратных средств. Поэтому неучтенная надежность ПО ведет к значительному её завышению при оценке надежности крупных аппаратно-программных комплексов.

Разработанные методы анализа надежности технических средств нельзя автоматически переносить и использовать для оценки надежности ПО, нужны специальные модели анализа надежности ПО.

Модель надежности с дискретно-понижающейся интенсивностью проявления ошибок

В этой модели предполагается, что интенсивность обнаружения ошибок описывается кусочно-постоянной функцией, пропорциональной числу неустранимых ошибок, т.е. предполагается что интенсивность отказов $\lambda(t)$ постоянна до обнаружения и исправления ошибки, после чего она снова становиться константой, но с другим, меньшим значением. При этом предполагается, что между $\lambda(t)$ и числом оставшихся в программе ошибок существует прямая зависимость:

$$\lambda(t) = K(M\text{-}i) = \lambda_i,$$

где M – неизвестное первоначальное число ошибок;

i – число обнаруженных ошибок, зависящих от времени t;

K – некоторая константа.

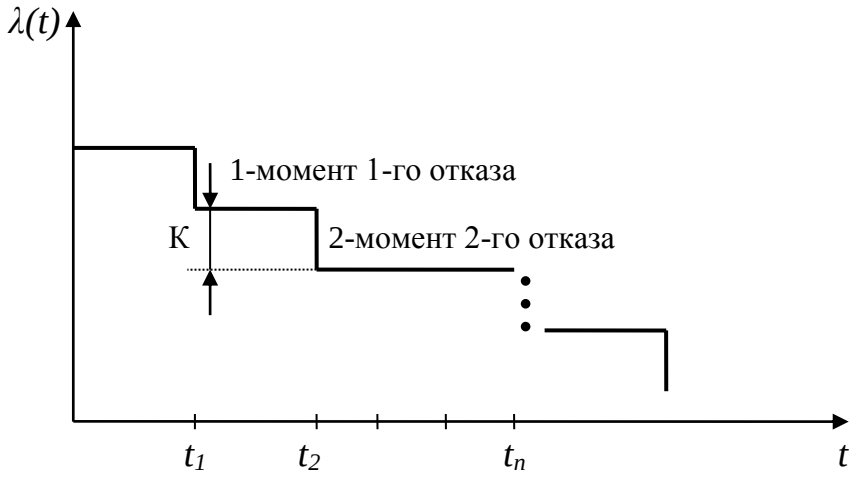


Рис. 1. Зависимость интенсивности отказов программы от времени работы (модель надежности с дискретно-понижающейся интенсивностью проявления ошибок программе)

На рис. 1 приведена зависимость $\lambda(t)$ от времени для некоторого участка эксплуатации программы:

1 – момент первого отказа;

2 – момент второго отказа.

Из графика видно, $\lambda(t_1, t_2, \ldots, t_n)$, при $t = t_1 + t_2 + \ldots + t_n$ убывает монотонно.

Плотность распределения времени обнаружения i-й ошибки задается соотношением:

$$f(t_i) = \lambda_i \cdot e^{-\lambda_i \cdot t_i}$$

Значение неизвестных параметров K и M может быть оценено на основании последовательности наблюдения интервалов между моментами обнаружения ошибок по методу максимального правдоподобия [1, 11].

Модель надежности программ с дискретным увеличением времени наработки на отказ

Она построена на предположении о том, что устранение ошибки в программе приводит к увеличению времени наработки на одну и ту же случайную величину.

Модель Джелинского-Моранды.

Эта модель основана на следующих предположениях:

1. Время до следующего отказа распределено экспоненциально;
2. Интенсивность отказов программы пропорциональна количеству оставшихся в программе ошибок.

Согласно этим допущениям ВБР программ как функция времени t_i равна:

$$P(t_i) = e^{-\lambda_i \cdot t_i}$$
$$\lambda_i = C_D(N-(i-1)), \qquad (1)$$

где i – число обнаруженных ошибок;

C_D – коэффициент пропорциональности, $C_D \approx 0{,}02$ (определяется по методу максимума правдоподобия);

N – первоначальное число ошибок программы. В выражении (1) отчет времени начинается от момента последнего (i–1)-го отказа программы.

Модель Шумана.

Данная модель отличается от модели Джелинского-Моранды только тем, что периоды времени отладки и эксплуатации программ рассматриваются отдельно.

Модель Шика-Вольвертона.

Основой этой модели является предположение о том, что интенсивность ошибок программы пропорциональна не только количеству оставшихся в программе ошибок, но и времени потраченному на отладку.

Экспоненциальная модель надежности программ.

Модель основана на предположении об экспоненциальном характере изменения во времени числа ошибок в программе.

В этой модели прогнозируется надежность программы на основе данных, полученных во время тестирования. В модели вводится суммарное время функционирования τ, которое отсчитывается от момента начала тестирования программы (с устранением обнаруженных ошибок) до конца контрольного момента, когда производится оценка надежности.

Предполагается, что все ошибки в программе независимы и проявляются в случайные моменты времени с постоянной средней интенсивностью в течении всего времени выполнения программы. Основное отличие данной модели от предыдущих состоит в том, что интенсивность отказов предполагается непрерывной функцией. Это упрощает математическое описание модели.

Пусть M – число ошибок, имеющихся в программе перед тестированием (M рассматривается как некоторая константа);

$m(\tau)$ – конечное число исправленных ошибок;

$m_0(\tau)$ – число оставшихся ошибок.

Тогда:

$$m_0(\tau) = M - m(\tau), \qquad (2)$$

Предполагается, что интенсивность отказов пропорциональна числу оставшихся ошибок $m_0(\tau)$, т.е.:

$$\lambda(\tau) = C \cdot m_0(\tau). \qquad (3)$$

C – коэффициент пропорциональности учитывающий реальное быстродействие компьютера и число команд в программе.

Считаем (дополнительное предположение), что в процессе корректировки новые ошибки не порождаются, т.е. что интенсивность исправления ошибок dm/dt будет равна интенсивности их обнаружения, т.е.:

$$dm/dt = \lambda(\tau) \qquad (4)$$

Решая совместно два вышеуказанных уравнения (3) и (4) получаем:

$$dm/dt + C \cdot m = C \cdot M \qquad (5)$$

Перед началом работы компьютера ($t = 0$) ни одна ошибка исправлена не была ($\tau = 0$), поэтому решением управления является:

$$m = M \cdot [1 - \exp(-C \cdot \tau)], \qquad (6)$$

где m – число исправленных ошибок в течении времени τ.

Среднее время наработки на отказ в течении времени τ после тестирования характеризуют надежность программы:

$$t_{cp} = 1/\lambda(\tau)$$

Следовательно:

$$t_{cp} = (1/C \cdot M) \cdot \exp(C \cdot \tau) \qquad (7)$$

Среднее время наработки на отказ увеличивается по мере выявления и исправления ошибок.

Рассмотренная модель может применяться для определения времени испытаний программ с целью достижения заданного уровня надежности, а также для оценки числа оставшихся в программе ошибок.

Модель надежности больших программных комплексов.

Для прогноза надежности больших программных комплексов может быть использована марковская модель. Надежность всего программного комплекса определяется как функция надежности ее составных частей. Подобная оценка значительно облегчается, если программа строится по модульному принципу. Надежность программного комплекса будет зависеть от последовательности выполняемых модулей и надежности каждого из этих модулей.

Прогнозирование надежности на ранних этапах их разработок.

В настоящее время наиболее отработаны способы прогнозирования ожидаемого числа ошибок в программах [1, 11].

Оценка ожидаемого числа ошибок Y в программе выражается через линейную зависимость:

$$Y = \sum_{j=1}^{r} a_j \cdot Z_j ,$$

где r – число существующих параметров;

a_j – коэффициент, зависящий от типа программ (управляющий, ввода-вывода, вычислительные, служебные);

Z_j – j-параметр программы.

В качестве параметров Z_j выбраны величины:

Z_1 – сложность уловных операторов IF

Z_2 – общее число ветвлений;

Z_3 – общее число связей с прикладными программами;

Z_4 – общее число связей с системными программами;

Z_5 – число операций ввода-вывода;

Z_6 – число вычислительных операторов;

Z_7 – число операторов обработки данных;

Z_8 – число комментариев.

Если число ожидаемых в программе ошибок оценено, то интенсивность отказов программы оценивается по выражению:

$$\lambda_{пр} = \bar{\gamma} \cdot Y / t_{реш} , \qquad (8)$$

где $t_{реш}$ – среднее время однократного прохождения программы;

$\bar{\gamma}$ – усредненное по всем ошибкам значение γ – условной вероятности того, что ошибка в программе проявляется при прохождении программы.

Рекомендуется оценивать γ экспериментально (статистически), определяя интенсивность отказа и количество ошибок для нескольких программ. Тогда:

$$\bar{\gamma} = \frac{1}{n} \cdot \sum_{i=1}^{n} \frac{t_{реш} \cdot \lambda_i}{Y_i}$$

λ_i, Y_i, $t_{реш}$ – соответственно интенсивность отказов, количество ошибок и время решения для i-й программы;

n – количество испытанных программ.

Интуитивная модель.

Эта модель используется при экспериментальной оценке числа ошибок в программе.

Согласно этой модели число ошибок в программе оценивается как:

$$Y = Y_1 \cdot Y_2 / Y_{12} ,$$

где Y_1, Y_2 – число ошибок, обнаруженных первым и вторым программистами, отлаживающих независимо друг от друга первоначальный текст программы, а Y_{12} – число ошибок, обнаруженных как первым, так и вторым программистами.

Очевидно, что первоначальный текст программы должен быть разработан при этом третьим программистом, чтобы поставить отлаживающих текст программистов в равные условия.

Для прогнозирования надежности ПО, в частности для прогнозирования количества не выявленных ошибок на этапе тестирования имеется интуитивная модель.

Пусть одна группа тестирования обнаруживает N_1, а другая N_2 ошибок, N_{12} – количество ошибок, обнаруженных обеими группами. Обозначим через N общее количество ошибок ПО. Если ввести понятие эффективности тестирования групп как отношения количества выявленных ошибок к их общему числу, то эффективности тестирования групп соответственно $E_1 = N_1/N$, $E_2 = N_2/N$;

Предполагается, что эффективность тестирования каждой группы одинакова как на всем множестве пространства ошибок ПО, так и на любом его подмножестве. В этом случае справедливо соотношение:

$$E_1 = N_1/N = N_{12}/N;$$

Подстановка N_2 приводит к выражению вида:

$$N = N_{12}/E_1 \cdot E_2,$$

где $E_1 = N_{12}/N_2$; $E_2 = N_{12}/N_1$;

Пример. Пусть группы тестирования обнаружили соответственно 20 и 25 ошибок, из них 5-ошибки обнаруженные обеими группами. В этом случае $E_1 = 0{,}2$; $E_2 = 0{,}25$.

Общее количество ошибок $N = 100$, а количество ошибок, оставшихся в не выявленными – 60.

Контрольные вопросы и задания

1. Для чего используются модели надежности ПО ИС?
2. Какие параметры надежности можно определить с помощью моделей ПО?
3. Оцените преимущества и недостатки известных моделей ПО.
4. С помощью какой модели можно прогнозировать надежность ПО на этапах разработки ИС?
5. Какие существуют методы повышения надежности ПО?

6. Оцените общее число ошибок в тексте программы, если программа проверена тремя специалистами и если первый из них нашел в программе 3 ошибки, второй – 5 ошибок, а третий – 6 ошибок, причем две ошибки из найденных были общими у всех специалистов.
7. Какие существуют пути повышения надежности ПО компьютеров и КС?
8. Для чего используют модель надежности Шумана?
9. В чем суть интуитивной модели надежности программ?
10. Как оценить ожидаемое число ошибок в программе, если использовать модель надежности программ на ранних этапах разработки.

Литература: 2,3,6, 8,11

Лекция 16

Тема: Надежность отказоустойчивых систем (ОУС). Назначение и свойства ОУС, примеры реализации

План.

1. Актуальность проблемы.
2. Назначение и свойства отказоустойчивых КС.
3. Примеры реализации. Система: TANDEM,
4. Системы: STAR, SIFT.

Ключевые слова

Отказоустойчивость, надежность, конфигурация, восстановление, метод контрольных точек, неисправности, повтор программы, активная отказоустойчивость, пассивная отказоустойчивость, маскирование, рестарт, аппаратное восстановление, программное восстановление, интенсивность отказов, наработка на отказ, безотказная работа, высокая готовность, резервирование, граф состояний.

1. Актуальность проблемы

Для систем управления производственными процессами и приложений по оперативной обработке информации совершенно естественны повышенные требования к организации высоконадежных вычислений. Современные телекоммуникационные системы, системы управлениям воздушным и наземным транспортом, медицинские учреждения, фондовые биржи, банки и промышленные предприятия не могут приостановить свою работу из-за неисправности компьютерной системы. В подобных приложениях простой может привести к задержке выхода продукции, потере прибылей, поломке оборудования и к человеческим жертвам. Поэтому проблема обеспечения надежности и отказоустойчивости современных компьютеров является очень актуальной и перспективной.

В настоящее время одной из основных задач построения компьютерных систем (КС) остается обеспечение их продолжительного надежного функционирования. Эта задача имеет три составляющие: надежность, высокая готовность и удобство обслуживания. Её решение предполагает, в первую очередь, борьбу с неисправностями системы, порождаемыми отказами и сбоями в её работе.

2. Назначение и свойства отказоустойчивых КС

Отказоустойчивость – свойство архитектуры КС, позволяющее пользователю или функциональной программе продолжать работу и тогда, когда в аппаратных или программных средствах возникают отказы.

По способу реализации отказоустойчивость подразделяется на активную и пассивную.

Активная отказоустойчивость базируется на процессах обнаружения отказа, локализации отказа и реконфигурации системы. Отказы обнаруживается при помощи средств контроля, локализируется с помощью средств диагностирования и устраняются автоматической реконфигурацией системы (см. п. 3).

Пассивная отказоустойчивость заключается в свойстве системы не потерять свои функциональные свойства в случае отказа отдельных элементов системы. Пассивная отказоустойчивость связана с увеличением количества аппаратуры в несколько раз. Пассивная отказоустойчивость применяется в случае особо ответственных КС, когда не допустимы даже кратковременные перерывы в обработке КС, а также для обеспечения отказоустойчивости его важнейших блоков или устройств.

Применение активной отказоустойчивости характеризуется более экономными расходом аппаратных средств, чем применение пассивной отказоустойчивости. Однако оно связано с некоторыми потерями времени при восстановлении работы системы после отказа, а также потерями некоторой части данных. Активная отказоустойчивость реализуема только в многопроцессорных системах (с общей памятью, общей шиной, матричной, кольцевой или другой структурой). В то же время применение пассивной отказоустойчивости гарантирует практически безостановочную работу КС и сохранение всей информации. Эти обстоятельства и определяют области применения активной и пассивной отказоустойчивости.

Введение отказоустойчивости является одним из методов повышения надежности КС. Вопрос о построении и применении отказоустойчивых систем возникает тогда, когда другие пути повышения надежности не могут обеспечить требуемого уровня надежности по техническим причинам, или тогда, когда они отказываются экономически не оправданными.

Отдельно от надежности отказоустойчивость системы может быть охарактеризована коэффициентом разряжения первичного потока отказов K_p, показывающим, какая доля из всех отказов системы влечет за собой отказ системы. Коэффициент разряжения равен:

$$K_P = \lambda_C / \Sigma \lambda_Э$$

где λ_C - интенсивность отказов системы, а $\Sigma\lambda_Э$ – суммарная интенсивность отказов всех элементов системы.

В то время как случайные отказы аппаратуры в нормальных условиях работы – редкие события, вероятность разрушения аппаратуры в тяжелых условиях, например в космосе, может быть значительной.

В тяжелых условиях работы аппаратуры механизмы отказа являются часто зависимыми, обусловленными одной и той же внешней причиной. Поэтому наряду с известными вероятностными методами теории надежности для отказоустойчивых систем представляет интерес детерминированный подход. В качестве меры отказоустойчивости при детерминированном

подходе служит d-устойчивость – максимальное число d элементов или других структурных единиц системы, отказ которых ещё не влечет со собой отказ системы.

Примеры реализации отказоустойчивых КС

В настоящее время существуют различные отказоустойчивые компьютерные системы. Типичными примерами таких систем являются: TANDEM, STRATUS, STAR, SIFT, AS220 и другие. Они имеют различное целевое назначение, созданы различными фирмами и обладают принципиальными отличиями в реализации средств обеспечения отказоустойчивости. Рассмотрим некоторые из них.

Система TANDEM

Данная система представляет собой КС, обеспечивающие непрерывное функционирование, в том числе при отказе одного или нескольких элементов аппаратуры. КС предназначена для использования в режиме реального времени, когда требуется высокая надежность.

В состав системы TANDEM может входит от 1 до 16 процессорных модулей, каждый из которых содержит блок управления, 16-разрядный процессор, блок памяти и канал ввода-вывода. Все части этой системы резервированы. Система не имеет выделенного ведущего процессора, функции управления выполняет все процессоры системы. КС допускает ремонт во время работ, т.е. возможность удаления отказавших ТЭЗов и возвращения исправных без прекращения выполнения программ пользователей. Это достигается наличием нескольких процессоров, дублированным доступом к устройствам ввода-вывода, резервированной системой электропитания и операционной системой, основанной на сообщениях.

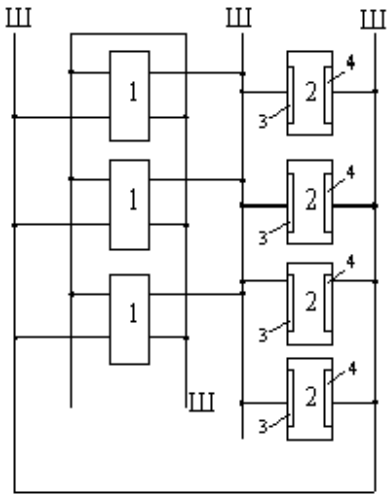


Рис. 4. Структура системы TANDEM

На рис. 4 изображена структура системы TANDEM, состоящей из трех процессоров 1 и четырех контроллеров ввода-вывода 2. Процессоры типа мини-ЭВМ сообщаются через 16-разрядную параллельную дублированную систему шин Ш. Все контроллеры ввода-вывода имеют по два порта 3,4 и доступ по двум каналам, от двух разных процессоров.

Запоминающие устройства на дисках такие имеют по два порта; каждое устройство доступно от двух контроллеров. Данные с диска остаются доступными даже тогда, когда и процессор, и контроллер отказывают.

При отказе привода диска записи могут быть восстановлены, если они были до его остановки записаны на другом диске. Если все записи на дисках дублированы, то система имеет копии всех данных. Когда диск заменяется, записи на нем можно восстанавливать во время работы основной системы.

Электропитание всех процессоров и дисков – независимое.

Каждый процессор системы содержит собственную копию операционной системы, обладающую локальной таблицей, отражающей состояние всех доступных устройств системы.

Контрольные точки. Они являются ключевым механизмом в системе TANDEM. Для каждого текущего вычислительного процесса в системе имеется идентичный полуактивный дублирующий процесс в другом процессоре. Дублирующий процесс должен заменить основной процесс в случае отказа соответствующего процессора. Основной процесс посылает дублирующему процессу «Контрольные соотношения», которые определяют состояние процесса в критических точках вычисления.

Операционная система в каждом процессоре возбуждает дублирующий процесс после обнаружения того, что основной процесс отказал. Дублирующий процесс может тогда продолжать процесс, начиная от состояния, зафиксированного в последней контрольной точке.

Программное обеспечение содержит виртуальную операционную систему и позволяет осуществлять мультипрограммную обработку.

Система сообщений. Изоляция процессов пользователя в TANDEM обеспечивается формированием сообщений. Например, программа пользователя, нуждающаяся в некоторых данных, записанных на диске, формирует некоторое «сообщение», адресованное программе логического управления диском. Просматривая свои таблицы ресурсов, локальная копия операционной системы определяет фактическое местонахождение искомого процесса.

Изоляция задач пользователя существенна для обеспечения ремонта во время работы системы, кроме того, такая изоляция обеспечивает постепенной рост производительности системы.

Система STAR

Компьютерная система STAR (Self-Testing and Repairing) – самопроверяемая и ремонтируемая КС предназначена для беспилотных

космических полетов большой продолжительности (до 10 лет). Здесь выбран следующий принцип организации средств обеспечения отказоустойчивости (СОО). В каждый момент времени функционирует одна вычислительная машина, снабженная эффективными схемами контроля для обнаружения неисправностей и достаточным количеством резервных блоков. При этом используется ненагруженный резерв, т.е. на резервные блоки не подается напряжение питания. В системе STAR большая часть функций средств отказоустойчивости реализуется в виде аппаратного блока (введением структурной избыточности) (рис.6).

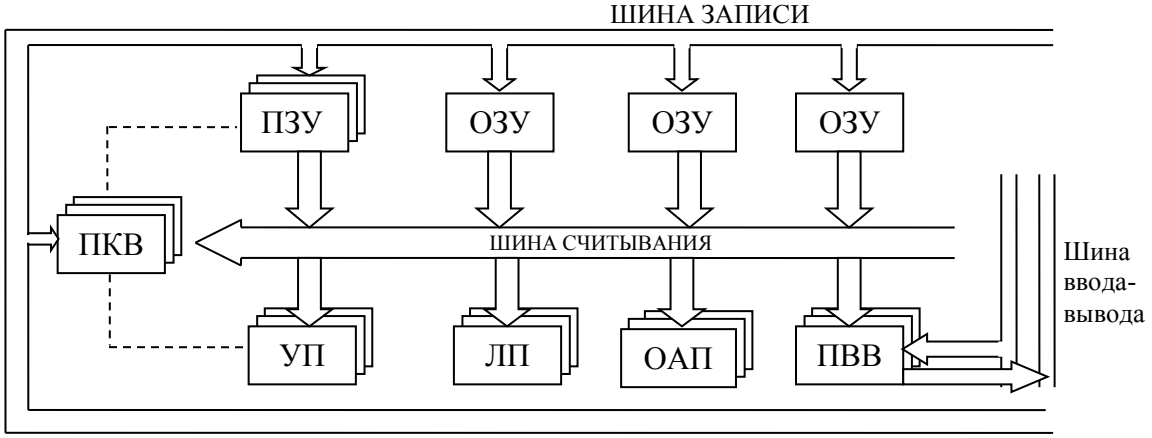


Рис. 6. Структурная схема системы STAR

Поскольку в системе предусмотрен только один рабочий компьютер, потребовалось организовать специальное аппаратное «ядро», которое обеспечило бы диагностику отказов в компьютере, автоматическую замену неисправных блоков на резервные и выработку управляющих сигналов, запускающих программную процедуру восстановления. Это «ядро», получило название – процессор контроля и восстановления (ПКВ).

Схема (рис.6) состоит из семи типов различных модулей, соединенных между собой четырехпроводными шинами и имеющих резервные копии.

УП – управляющий процессор содержит счетчик адресов и индексные регистры, осуществляет модификацию адресов команд перед их выполнением;

ЛП – логический процессор – выполняет логические операции над информационными словами (напряжение питания подается сразу на 2 копии);

ОАП – основной арифметический процессор выполняет арифметические операции над информационными словами;

ПЗУ – постоянное запоминающее устройство;

ПВВ – процессор ввода-вывода содержит буферные регистры ввода-вывода и процессор прерывания, управляет запросами на прерывания;

ПКВ – процессор контроля и восстановления управляет работой компьютера и осуществляет восстановление (питание подается одновременно на три корни, тройной нагруженный резерв).

Информация между модулями передается по шине записи в память и шине считывания из памяти в виде восьми 4-разрядных посылок, т.е. разрядность слова-32. Параллельно-последовательный принцип обработки выбран по причине снижения потребляемой мощности и вероятности отказа в системе [4,6,7].

Модуль ПКВ – самый оригинальный модуль в этой компьютерной системе. Он следит за работой шин посредством проверки справедливости кодов с обнаружением ошибок, а также за сообщениями о состоянии различных функциональных модулей. Если приходит сигнал ошибки с какого-либо модуля или в шину поступает неправильно закодированная информация с выхода модуля, то ПКВ инициирует повторное выполнение сегмента программы. Если ошибка повторяется, производится замена неисправного блока резервным с помощью шины управления.

Функции обнаружения ошибок и восстановления в данной системе подробно описаны в [3,5,7].

Система STAR одна из первых отказоустойчивых КС и идеология её построения оказала большое влияние на последующие разработки КС данного типа.

Система SIFT (Softwave Implemented Fault Tolerance) – представляет собой КС, предназначенную для управления полетом самолета в особо сложных условиях. Основной принцип построения системы, состоит в обеспечении отказоустойчивости в основном программными способами, а не аппаратными. Особенностью СОО является параллельное выполнение каждой программы несколькими блоками обработки данных. Процедуры обнаружения и анализа ошибок и реконфигурация системы возложены на программное обеспечение, отсюда и название системы. Локализация отказов достигается применением специально разработанной избыточной системы шинных соединений блоков обработки данных. Как минимум троекратное резервирование выполнения программ позволяет устранить влияние любого одиночного отказа блока обработки данных или шины, а устойчивость к последовательности отказов создается за счет реконфигурации системы.

Эти примеры приводятся здесь как иллюстрация разных подходов к реализации СОО для конкретных применений и по существу на них хорошо просматривается та совокупность задач, с которыми сталкивается разработчик современных компьютерных систем.

Современный уровень развития отказоустойчивых КС может быть охарактеризован также данными о зарубежных специализированных компьютерах [7,8] для космических кораблей (табл. 1).

Таблица 1.

Параметры	Выпускающая фирма и тип компьютера					
	CDS 496	DELCO M-362	GE.DEC PDP-11	LITTON 4516 E	RCA SCP-234	Rockwell DF-224
Быстродействие,	200	650/840	100	300	70	400

тыс. оп/с						
Длина слова, бит	16(42)	16/32 (120)	16	16/32	16	24
Вероятность безотказной работы, P(t)	0,925 за один год	0,99 за один год	0,99 за два года	0,98 за два года	0,899 за два года	0,92 за три года

Приведенные в таблице 1 значения вероятности безотказной работы определены с учетом резервирования. В случае дублирования эти данные соответствуют интенсивности отказов порядка

$$\lambda = (0{,}5 \div 3) \bullet 10^{-5} \ {}^{1}/_{\tau}$$

для одного компьютера, что достижимо при использовании компонентов наиболее высокого качества и надежности. В типичном случае дублированы устройства ввода-вывода, центральный процессор и устройства управления памятью. Оперативные запоминающие устройства объемом в десяти Кслов секционированы. Переключающие устройства для включения резервов построены с использованием логических схем с переплетениями [7]. В системах применяется аппаратный оперативный контроль вместе с программным тестовым контролем и диагностикой, которые дополняют друг друга и вырабатывают сигналы для автоматического включения резерва.

В компьютерных системах, предназначенных для непилотируемых космических кораблей, наряду с автоматическим контролем и включением резерва предусматриваются наземный телеметрический контроль и реконфигурация системы через каналы телеуправления в случае обнаружения отказов.

Контрольные вопросы и задания

1. Как обеспечить высокую надежность при создании современных компьютерных систем?
2. Какой вид контроля в КС является наиболее перспективным?
3. Дайте определение понятию «реконфигурация».
4. Определите виды ошибок в КС которые можно исправить с помощью маскирования.
5. Какие бывают КС по способу реализации отказоустойчивости?
6. Постройте граф состоянии и переходов процесса восстановления в отказоустойчивых КС.
7. Что характеризует коэффициент разряжения КС?
8. Объясните способы реализации СОО, заложенные в системе TANDEM.
9. Что называется «контрольной точкой»?
10. Для каких целей предназначена система STAR?

11. Какова функция ПКВ в системе STAR?
12. Какой вид контроля используется в системе SIFT?
13. Укажите типичные значения вероятности безотказной работы современных высоконадежных компьютеров.

Литература: 1, 2, 3, 5, 10, 11.

Лекция 17

Тема: Методы и алгоритмы автоматического восстановления ИС

План

1. Реконфигурация в технических устройствах ИС.
2. Способы восстановления в высоконадежных КС.
3. Модель процесса автоматического восстановления отказоустойчивых КС.

Ключевые слова

Отказоустойчивая система, безотказность, реконфигурация, автоматическое восстановление, интенсивность восстановления, состояния, динамическое резервирование, избыточность, активная отказоустойчивость, модель восстановления.

Реконфигурация и способы восстановления КС.

Среди перечисленные выше методов обеспечения и повышения надежности наиболее перспективными являются использование новых способов восстановления, автоматической реконфигурации и создание отказоустойчивых КС. Рассмотрим эти вопросы.

Реконфигурация КС – изменение состава и способа взаимодействия программных и аппаратных средств системы с целью исключения отказавших программных или аппаратных компонентов. Реконфигурация производится после выявления отказа. Различают статическую и динамическую реконфигурацию.

Статическая реконфигурация системы осуществляется путем отключения неисправных компонентов КС. Динамическая реконфигурация по принципу проведения делится на следующие виды: замещение, дублирование, постепенная «деградация».

После реконфигурации для продолжения нормальной работы системы необходимо её восстановить, восстановление системы происходит на двух уровнях (рис. 1).

1. Аппаратный уровень. Здесь производится восстановление отказавших компонентов КС двумя способами:

- автоматическое восстановление, реализуемое путем реконфигурации системы. При этом предполагается, что в системе имеется ряд запасных блоков, благодаря которым она возвращается в работоспособное состояние;
- ремонт (восстановление вручную). В этом случае отказавший блок отключается от системы и она продолжает работу с меньшей производительностью, либо приостанавливается до возвращения отремонтированного блока в активную часть КС.

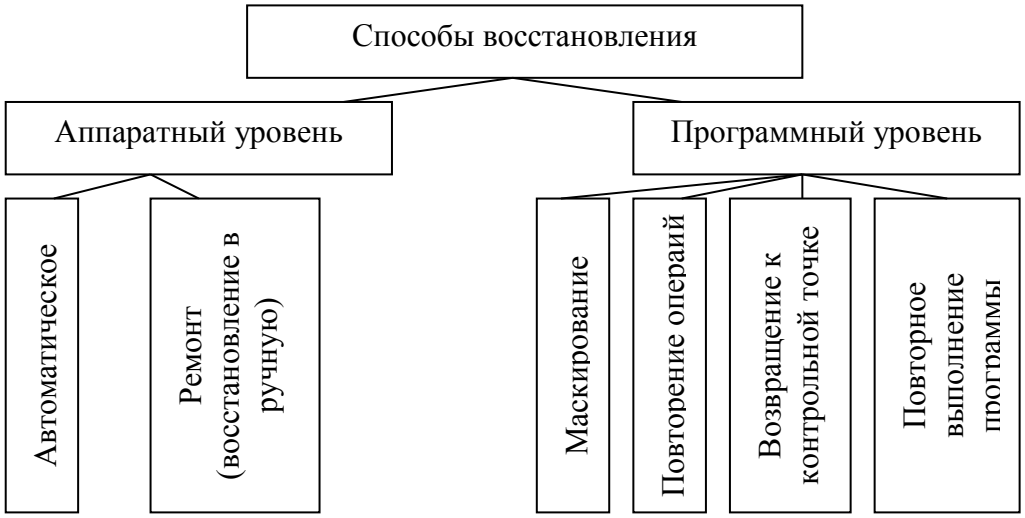


Рис. 1. Классификация способов восстановления КС.

2. Программный уровень, здесь осуществляется восстановление информации о состоянии КС, необходимой для продолжения её работы.

Средства восстановления включаются в работу при обнаружении ошибки системой контроля. Способ восстановления зависит от уровня, на котором обнаружена ошибка. В зависимости от нарушений в работе системы можно выделить следующие способы восстановления: маскирование, повторение операции, возврат к контрольной точке, программный рестарт. На рис. 2 приведен алгоритм автоматического восстановления вычислительного процесса после сбоев, где использованы все виды восстановления.

Маскированием называется исправление ошибки с помощью корректирующих кодов или резервирования. Восстановление путем маскирования или повторения операции выполняется в том случае, когда ошибка обнаружена средствами контроля логического уровня и, следовательно, не успела распространиться.

Восстановление путем повторения операции может быть успешным, если ошибка была случайной или перемежающейся и самоустранилась при повторении, т.е. проявилась как сбой. Поскольку длительность случайной ошибки может быть разной, система должна повторять операции несколько раз. Повторение может быть на уровне микрокоманд, команд и операций ввода-вывода.

В тех случаях, когда ошибка обнаруживается средствами функционального или системного уровня, т.е. успела исказить информацию, используется восстановление путем возврата к контрольной точке.

Контрольной точкой называется некоторая точка в вычислительном процессе (программе), для которой сохранены промежуточные результаты вычислений, и к которой в случае ошибки можно вернуться (передать управление). Этот способ восстановления требует по ходу вычислительного процесса формирования контрольных точек (т.е. периодического запоминания промежуточных результатов вычислительного процесса).

Программным рестартом называется повторный запуск вычислительного задания. Этот способ восстановления используется в том случае, когда ошибка обнаружена средствами контроля пользовательского уровня. Маскирование и повторение операции как способы восстановления более предпочтительны, так как обеспечивают ранее обнаружение ошибки и восстановление. Однако они требуют значительных затрат аппаратуры.

Сохранение работоспособности компьютеров при отказах имеет большое значение при эксплуатации систем, работающих в реальном масштабе времени, систем с разделением времени, систем телеобработки, диалоговых систем и др.

Автоматическое восстановление вычислительного процесса при отказах может быть достигнуто путем введения в КС свойств отказоустойчивости.

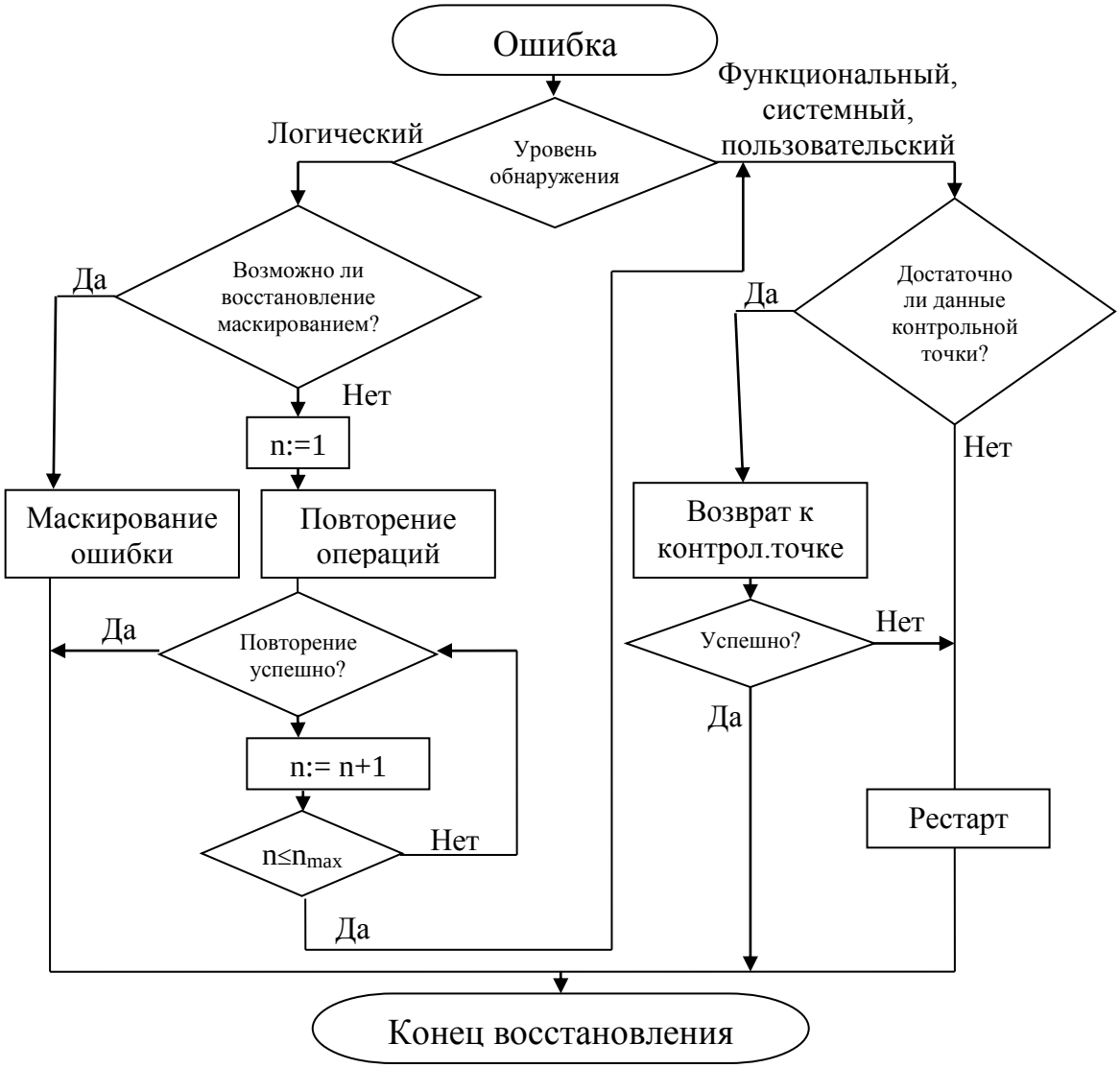


Рис. 2. Функционирование вычислительного процесса.

Модель процесса автоматического восстановления
отказоустойчивых КС

Автоматическое восстановление в компьютерных системах является новым подходам, обеспечивающим высокую степень надежности, готовности и отказоустойчивости КС.

Ниже предлагается модель, описывающая общие свойства различных процессов восстановления, некоторой гипотетической отказоустойчивой КС. Она включает все возможные процессы восстановления, применяемые в реальных КС. Множество возможных событий в системе обозначим через

$$S=\{S_1,S_2,\ldots,S_{16}\}.$$

Процессы восстановления в пассивных и активных отказоустойчивых КС имеют много общего. Рассмотрим граф на рис. 3.[1,7,10]:

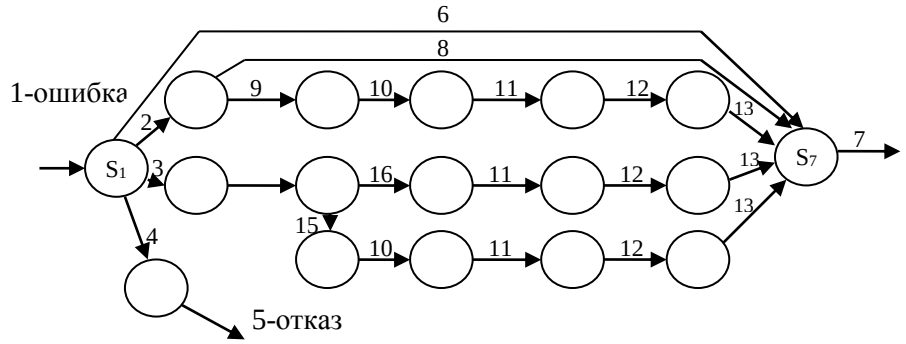


Рис. 3. Граф процесса восстановления

Возникшая в КС ошибка S_1 может обнаруживаться либо аппаратными S_2, либо программными S_3 средствами контроля, либо не обнаруживаться средствами контроля S_4. В последнем случае результатом является отказ системы S_5.

В зависимости от степени применения пассивной отказоустойчивости в КС ошибка может быть маскирована S_6 и вычислительный процесс продолжается без задержки S_7. При обнаружении ошибки аппаратными средствами в большинстве систем проводится повторение выполняемой операции в заданное число раз. Если повторение было успешным, т.е. имел место сбой, последствия которого при повторении операции исчезли, вычислительный процесс продолжается S_8. Для повторении операции необходимо чтобы аппаратные средства сохранили операнды до окончания контроля над выполненной операцией. Если повторении операции было безуспешным S_9, то это говорит об устойчивой ошибке в аппаратуре и поэтому производится автоматическая реконфигурация S_{10}.

Реконфигурация может заключаться либо в замене отказавшей подсистемы (устройства, процессора) за счет резервов, либо в её простом отключении. В последнем случае имеет место постепенная деградация

системы. После реконфигурации производится восстановление информации S_{12}. Для этого по ходу вычислительного процесса предусмотрены контрольные точки, в которых состояние системы и вычислительного процесса подвергаются контролю. В случае положительного результата контроля состояние данной программы и данного процессора (промежуточные результаты, содержание регистров и др.) записывается либо в оперативной памяти другого процессора, либо на магнитных лентах или дисках.

В ходе восстановления информации содержание этих дублирующих записей переписывается в тот процессор, который после реконфигурации берет на себя функции отказавшего. Затем, начиная с контрольной точки, вычислительный процесс возобновляется S_{13}.

Аналогичные процедуры проводятся в случае, когда ошибка обнаружена программными средствами. После обнаружения ошибки программными средствами могут быть задействованы тесты S_{14}. Если тесты подтверждают наличие устойчивого отказа S_{15}, то следует реконфигурация S_{10}, возврат к контрольной точке S_{11}, восстановление данных S_{12} и повторение вычислений S_{13}. Если устойчивого отказа нет S_{16}, то повторяются перечисленные операции без реконфигурации.

Восстановление может оказаться безуспешным также в случае наличия ошибки в программах, разрушения информации в контрольных точках, исчерпания резервов или снижения производительности системы из-за отказов.

Описанный выше процесс может варьироваться в конкретных системах, особенно что касается способов обнаружения отказов. Иногда, например процессоры системы подтверждают свою работоспособность специальными сигналами. По этим сигналам во всех действующих процессорах системы формируется таблицы, показывающие состояние всех других процессоров. На основании этих таблиц обмен с отказавшими процессорами прекращается.

Контрольные вопросы и задания

1. Определите виды ошибок в КС которые можно исправить с помощью маскирования.
2. Дайте определение понятию «реконфигурация».
3. Что такое динамическая и статическая реконфигурация.
4. Постройте граф состоянии и переходов процесса восстановления в отказоустойчивых КС.
5. Что называется контрольной точкой в вычислительном процессе?
6. Определите понятие «программный рестарт».
7. Какой вид отказа является наиболее жестким в теории надежности?
8. Назовите основные метод автоматического восстановления в КС.

Литература: 1, 2, 3, 5, 10.

Лекция 18

Тема: Задачи оптимального резервирования отказоустойчивых ИС

План

1. Прямая и обратная задачи резервирования в отказоустойчивых систем (ОУС).
2. Метод множителей Лагранжа для нахождения оптимального резерва в ОУС.
3. Градиентные метод оптимизации надежности .
4. Расчетные формулы. Графическая зависимость доминирующей последовательности ОУС.

Ключевые слова

Резервирование, отказоустойчивость, высоконадежные системы, задачи оптимизации, метод множителей Лагранжа, оптимальное резервирования, градиентных метод, экстремум функции, доминирующая последовательность, стоимостный показатель.

Задачи оптимального резервирования компьютерных систем

Как уже отмечалось, резервирование является одним из простых и достаточно эффективных методов повышения надежности. Однако при резервировании возникает задача не только обеспечить заданные показатели надежности, но добиться этого как можно более экономично, с наименьшими суммарными затратами на резервные элементы для системы в целом, либо при заданных ресурсных ограничениях достичь максимально возможной надежности.

Задача оптимального резервирования чаще возникает в отказоустойчивых системах позволяющих пользователю или функциональной программе продолжать работу и тогда, когда в аппаратных или программных средствах системы возникают отказы. При проектировании таких систем следует стремиться не только к достижению необходимой их надежности, но и к достижению этой надежности при минимальных средствах, т.е. к нахождению оптимального решения.

В отказоустойчивых компьютерных системах и машинах существует ряд параметров, от которых зависит надежность системы. Сюда относится количество резервных элементов, устройств или подсистем; параметры систем контроля и диагностики; характеристики системы программного обеспечения; величины, характеризующие архитектуру, конфигурацию работы системы и другие:

$$R(t) = F(C, \mathrm{M}, ..., \mathrm{P}, \mathrm{Q}).$$

Надежность представляется в виде функциональной зависимости от перечисленных параметров. В качестве подобных ограничивающих ресурсов можно рассмотреть стоимость, массу, габаритные размеры, потребляемую мощность и т.п. Выбор вида ограничивающего ресурса определяется конкретным типом системы и ее назначением. Часто выделяют одну наиболее важную характеристику – стоимость.

Обычно в задачах оптимального резервирования предполагается, что стоимость резерва для системы в целом:

$$C(m_1,...,m_m) = \sum_{i=1}^{m} C_i(m_i)$$

где m_i – число резервных блоков в *i*-ой подсистеме КС;

и кроме того, сама стоимость резерва *i*-й резервной группы определяется как:

$$C_i(m_i) = c_i \cdot m_i$$

где c_i – стоимость одного блока в *i*-ой подсистеме КС.

При наличии одного ограничивающего фактора (стоимости) возможны постановки двух следующих задач оптимального резервирования [1, 3, 13].

1. *Прямая задача*. Раздельным резервированием системы, состоящей из *m*-резервных групп, добиться того, чтобы показатель надежности был не менее заданного $R_{зад}$ при минимально возможной стоимости резерва в целом, т.е.:

$$\min_{m_i} \{C(m_1,...,m_m) \mid R(m_1,...,m_m) \geq R_{зад}\}.$$

2. *Обратная задача*. Раздельным резервированием системы, состоящей из *m*-резервных групп, добиться того, чтобы при максимально возможном показателе надежности системы *R* стоимость всего резерва не превысила заданного значения $C_{зад}$, т.е.:

$$\max_{m_i} \{R(m_1,...,m_m) \mid C(m_1,...,m_m) \leq C_{зад}\},$$

если в качестве показателя надежности выбрать ВБР P_c, то:

$$\max_{m_i} \{P_c(m_i) \mid C_i(m_i) \leq C_{зад}\},$$

где C_i – стоимость одного блока в *i*-й подсистеме компьютера или КС;

m_i – число резервных блоков в *i*-й подсистеме компьютера или КС;

$C_{зад}$ – заданное значение стоимости резервных блоков машины или КС;

P_c – вероятность безотказной работы КС за время *T*.

Суть оптимизационной задачи, заключающейся в повышении надежности системы путем резервирования при ограничениях на суммарную

стоимость, можно пояснить на двух простых частных случаях. Допустим, что все элементы системы равнонадежны и в каждой резервной группе имеется ровно по одному основному элементу. В этом случае приоритет по резервированию сначала получают те группы, элементы которых характеризуются наименьшей стоимостью. Если же элементы имеют равную стоимость, то сначала следует резервировать наименее надежные резервные группы.

В более сложных случаях, когда резервные группы содержат различное число элементов, а сами элементы в различных группах различаются и по показателям надежности, и по стоимости, для определения оптимального состава резервных элементов в системе требуется использовать специальные алгоритмы решения оптимизационных задач [13, 15, 18].

Экспериментальные задачи (задачи нахождения экстремума функции min или max) с ограничениями могут быть решены аналитически (с использованием метода неопределенных множителей Лагранжа) и с помощью численных методов: метода перебора и градиентного метода.

При решении оптимизационных задач могут быть ограничения на массу, стоимость, габариты и другие характеристики системы.

Рассмотрим, как может быть сформулирована оптимизационная задача резервирования с учетом одного параметра – стоимости.

Задача оптимизации компьютерных систем по показателю надежности заключается в таком резервировании каждой из подсистем, которое доставляет максимальную безотказность всей системы при заданных ограничениях на ее стоимость – $C(m_i) \le C_{зад}$, или можно найти вектор m_i, представляющий собой решение задачи:

$$\max_{m_i}\{P_c(m_i) \mid C_i(m_i) \le C_{зад}\}$$

где m_i – число резервных блоков в i-й подсистеме ВС;

C_i – стоимость одного блока в i-й подсистеме;

$C_{зад}$ – заданное значение стоимости резервных блоков ВС;

P_c – вероятность безотказной работы КС за время Т.

Может быть решена и обратная задача.

Оптимальное распределение резервов в КС на уровне процессоров, устройств или подсистем рассмотрим с использованием аналитического приближенного метода неопределенных множителей Лагранжа.

Пусть имеем систему с нагруженным резервом, подключенным по схеме поэлементного резервирования. Каждая из n-подсистем (процессоры, ОЗУ, ПУ и др.) имеют m_i -1 резервов. Вероятность безотказной работы (ВБР) i-й подсистемы $(i = \overline{l, n})$ обозначается через P_i. Тогда ВБР системы P_c выражается как:

$$P_c = \prod_{i=1}^{n} [1 - (1 - P_i)^{m_i}]. \quad (1)$$

Чтобы упростить формулу, допустим, что $p_i = 1 - q_i \to 1$, где q_i – вероятность отказа *i*-й подсистемы. Тогда вероятность отказа системы *Q*:

$$Q(m) = \sum_{i=1}^{n} q_i^{m_i}, \quad (2)$$

где $m = (m_1, m_2, \ldots, m_n)$.

Масса, габариты или стоимость системы выражается в виде линейной зависимости:

$$C = C(m) = \sum_{i=1}^{n} c_i \cdot m_i, \quad (3)$$

где c_i – стоимость *i*-й подсистемы.

Необходимо определить $\min Q(m)$ при условии, что $C(m) \le C_{зад}$, где $C_{зад}$ – заданное значение стоимости системы. Искомыми являются значения m_i, минимизирующие вероятность отказа *Q*. Поскольку $Q(m)$ и $C(m)$ монотонные зависимости, то условие типа неравенства может быть заменено условием типа равенства, а задача решена методом неопределенных множителей Лагранжа.

Функция Лагранжа $F(m)$ имеет следующий вид:

$$F(m) = Q(m) + \xi \cdot (C_{зад} - C(m)), \quad (4)$$

где ξ – неопределенный множитель Лагранжа.

Совместное решение необходимых условий экстремума (4):

$$\partial F(m) / \partial m_i = 0, \quad (5)$$

и условие типа равенства:

$$C_{зад} = C(m), \quad (6)$$

позволяют определить *n* оптимальных значений m_i и соответствующее им значение неопределенного множителя ξ.

Подставляя $Q(m)$, $C(m)$, из (2), (3) в 4, а $F(m)$ из (4) в (5) получим следующую систему уравнений:

$$q_i^{m_i} \cdot \ln(q) - \xi \cdot c_i = 0, \text{ откуда, } m_i = \ln(\xi) \cdot \alpha_i / \ln(q_i), \quad (7)$$

где $\alpha_i = c_i / \ln(q_i)$.

Для определения ξ поставим m_i, из в (6), тогда:

$$C_{зад} = \sum_{i=1}^{n} c_i \cdot (\ln(\xi) \cdot \alpha_i) / (\ln(q_i)) = \sum_{i=1}^{n} \alpha_i \cdot (\ln(-\xi) + \ln(-\alpha_i)). \qquad (8)$$

В последнем выражении изменены знаки сомножителей ξ и α_i, т.е. вместо ξ и α_i написано $(-\xi)$ и $(-\alpha_i)$ для того, чтобы можно было логарифмировать, так как $\alpha_i \le 0$.

Следовательно, решение существует только в случае, когда ξ – отрицательная величина. Выражая $\ln(-\xi)$ и подставляя, получим окончательное выражение для оптимальных значений m_i:

$$m_i = 1/(\ln(q_i)) \cdot [(Сзза - \sum_{i=1}^{n} \alpha_i \cdot \ln(-\alpha_i)) \Big/ (\sum_{i=1}^{n} \alpha_i) + \ln(-\alpha_i)], \qquad (9)$$

При второй постановке задачи решение осуществляется согласно (min (max) $\varphi(x)$,

$$\prod(x) \in H$$

где H – ограничение, налагаемое на показатель надежности $\Pi(x)$) на основании следующей функции Лагранжа:

$$F_1(m) = C(m) + \eta \cdot (Q_{зад} - Q(m)),$$

где η – неопределенный множитель Лагранжа;

$Q_{зад}$ – заданное значение вероятности отказа.

Решая совместно уравнения $\partial F_1(m) / \partial m_i = 0$ при $i = 1,2,\ldots,n$ и $Q_{зад} = Q(m)$, получим вкражение для оптимальных кратностей резервирования:

$$m_i = 1/(\ln(q_i)) \cdot \ln((\alpha_i \cdot Q_{зад}) \Big/ (\sum_{i=1}^{n} \alpha_i)). \qquad (10)$$

Приведенные выражения являются приближенными из-за необходимости округления результата. Ошибка получается особенно большая при малых m_i. Кроме того, аналитический метод позволяет получить решение в явном виде только при простейших моделях надежности.

Оптимальное распределение резервов численными методами

Задача оптимального резервирования может быть решена не только аналитически (методом неопределенных множителей Лагранжа), но и

численными методами. Численные методы определения оптимального резерва позволяют найти более точное решение, и особенно эффективны при малом числе резервных подсистем.

К численному методу относится метод перебора, когда сравнивают между собой все возможные варианты структуры. Затем выбирают из них тот, который лучше всего отвечает установленным требованиям по надежности. Однако число вариантов получается практически весьма большое, поэтому метод перебора может быть использован только в простейших случаях.

Обозначим количество конкурирующих вариантов N_b. Для структуры сложной КС типа N_b определяется произведением:

$$\mathrm{N_b} = \prod_{\mathrm{i}=1}^{\mathrm{n}} m_{iM} ,$$

где $\prod_{i=1}^{n}$ – общее число подсистем;

m_{iM} – максимально возможное число параллельных подсистем i-го типа.

Например, $n=10$ и $m_{iM}=10$, при $C=\overline{1,n}$, тогда $N_b = 10^{10}$, это практически исключает возможность перебора.

Рассмотрим возможность сокращения числа вариантов при переборе. Введем понятие доминирующий последовательности и рассмотрим график вариантов технический решений в координатах: стоимость C – вероятность отказа Q (рис.1).

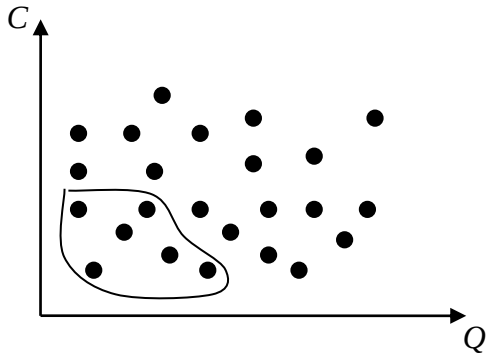


Рис. 1. Графическая иллюстрация доминирующей последовательности

Каждый вариант этом графике представляется точкой. Из всех вариантов заданной стоимости C интерес представляют только варианты, обладающие минимальной вероятностью отказа Q. Из вариантов при заданной (ими меньшей) вероятности отказа Q интересны только варианты, отличающиеся минимальной стоимостью C. Отсюда следуют, что из всего

множества вариантов интерес представляют только те, которые находятся снизу и слева.

Подмножество этих вариантов, перспективных с точки зрения поиска оптимального варианта, называется *доминирующей последовательностью*. На рис. 1 доминирующая последовательность обведена. Мощность (количество элементов) доминирующей последовательности обычно намного меньше мощности множества вариантов. Поэтому легко выбирать оптимальное решение из вариантов, входящих в доминирующую последовательность.

Численные методы позволяют построить доминирующую последовательность поэлементно, – до достижения заданной надежности при минимальной стоимости или до достижения минимальной стоимости при заданной надежности. При структурной оптимизации важно найти эффективный способ ограничения количества рассматриваемых вариантов.

Эффективным методом является *градиентный метод* заключается в пошаговом поиске максимума критерия типа $\Delta\lg(Q)/(\Delta C)$, т.е. отношения приращения логарифма вероятности отказа системы к приращению стоимости [1, 12, 42, 49].

Градиентный метод позволяет определить часть элементов доминирующей последовательности, т.е. некоторые элементы могут отказаться пропущенными. Поэтому получаемые этим методом результаты следует рассматривать как приближенные или проводить дополнительный поиск.

Пример оптимального распределения резервов.

Пусть имеется система, состоящая из четырех подсистем, т.е. $n = 4$. подсистемы характеризуются стоимостями C_i и вероятностями отказа за заданное время q_i:

i	...	1	2	3	4
C_i	...	1,2	2,3	3,4	4,5
q_i	...	0,2	0,3	0,25	0,15

Требуется построить систему, обладающую вероятностью безотказной работы $P \geq 0{,}99$ при минимальной стоимости С. Первоначальное состояние системы, когда нет резервов, описываются вектором состояний $m = (m_1\ m_2\ m_3\ m_4) = (1111)$. Сравнение вариантов (2111), (1211), (1121) и (1112) происходит по критерию $\Delta\lg(Q)/\Delta C$, обеспечивающего максимум критерия. Используя приведенные выше формулы находим приближенное решение задачи. Величина оптимального распределения резерва m = (5543).

Контрольные вопросы и задания

1. Что такое резервирование?
2. Какие виды структурного резервирования широко распространены на практике?
3. Для каких компьютерных систем решаются задачи оптимального резервирования?
4. Какие аналитические и численные методы используются при оптимальном резервировании КС?
5. Определите суть метода Лагранжа для оптимизации надежности.
6. Дайте формулу для расчета нахождения резервного элемента в КС ответственного назначения.
7. Что такое градиентный метод?
8. Укажите метод при оптимизации резервов в КС, где используется понятие «доминирующая последовательность».

Литература: 1, 2, 5, 6, 9, 10.

З А К Л Ю Ч Е Н И Е

Развитие информационных систем в настоящее время осуществляется по следующим основным направлениям: создание высоконадежных аппаратных и программных средств компьютерной техники; суперкомпьютеров большой производительности; систем с высокой степенью интеллекта; обширных компьютерных сетей с огромными банками данных; персональных компьютеров массового применения; микропроцессорных средств управления для различных машин и аппаратов.

Успешная реализация возможностей всех этих направлений предполагает весьма высокую достоверность получаемых с помощью компьютера результатов при ограниченном числе ремонтного персонала. Выполнение этого условия возможно только при систематическом планировании, учете и реализации факторов, обеспечивающих надежность и отказоустойчивость получаемых результатов при высокой степени автоматизации процесса эксплуатации вычислительных средств.

Проблема надежности вычислений и достоверности их результатов в ИС существовала всегда. Однако при небольших объемах и скоростях вычислений и при решении не очень ответственных задач отдельные ошибочные результаты легко обнаруживались и не причиняли особого вреда. Неисправность простых и немногочисленных компьютеров того времени тоже можно было легко устранить.

В настоящее время в связи с непомерно возросшими объемами и скоростями вычислений и с высокими требованиями к достоверности результатов обработки данных поддерживание работоспособности ИС может быть достигнуто путем его полной автоматизации. Учитывая стремительные темпы дальнейшего роста быстродействия и производительности компьютерных средств, можно с уверенностью сказать, что всякие другие пути поддержания работоспособности ИС, кроме его полной автоматизации, наталкивается на непреодолимые трудности, связанные с нехваткой обслуживающего персонала.

Процесс развития ИС не может быть преодолен просто наращиванием компьютерных мощностей. В области обеспечение работоспособности средств компьютерной техники (СКТ) зарождаются новые в принципе технические решения.

С одной стороны, эти решения базируются на новой элементной базе, а с другой – на новых логических, структурных и алгоритмических принципах построения СКТ. Существующие технические решения, основанные на трех- или четырех кратном увеличении аппаратуры и программных средств для достижения увеличения устойчивости ИС к отказам и ошибкам вряд ли соответствуют по уровню отработанности и по изяществу замысла другим техническим решениям, принятым в современной компьютерной технике. В данной области существует широкое поле поиска развития общей теории отказоустойчивых КС, так и в плане изобретательской деятельности для решения частных задач.

Очевидно, решение проблемы отказоустойчивости ИС тесно связано с проблемой распараллеливания вычислений, построения компьютерных сетей, а возможно, с новыми результатами в области применения теории групп и других отраслей современной математики к развитию арифметических и логических основ построения СКТ.

Литература

1. Иыуду К.А Надежность, контроль и диагностика вычислительных машин и систем. М: Высшая школа, 1989-216с
2. Расулова С.С Надежность вычислительных машин и систем. Учебное пособие, ТашГТУ, 1995-60с
3. Расулова С.С Надежность ЭВС. Конспект лекций. ТашГТУ, 2001-90с
4. Расулова С.С. Рашидов А.А. Программа, методические указания, ТашГТУ-2003.
5. Расулова С.С., Рашидов А.А. Построение отказоустойчивых микропроцессорных систем. Ташкент –Mehnat -2004.
6. Расулова С.С. Обеспечение надежности и отказоустойчивости компьютерных систем. Проблемная лекция. ТашГТУ, 2004-27с
7. Дружинин Г.Н. Надежность автоматизированных произвостенных систем. М: Энергаатомиздат
8. Иыуду К.А. Задачи и упражнения по основам эксплуатации электронных приборов. М: МАИ, 1996-120с
9. Самопалов К.Г. и др. Цифровые ЭВМ. Практикум. Киев. Высшая школа. 1990-125с.
10. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации. 2 изд. Учебник. СПб.: «Питер», 2005. глава 20, -703 с.
11. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. Учебное пособие. – СПб.: Питер, 2007. -509 с.