Ю.Ю. ГРОМОВ, О.Г. ИВАНОВА,
Н.Г. МОСЯГИНА, К.А. НАБАТОВ

НАДЁЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

ТАМБОВ
• ИЗДАТЕЛЬСТВО ГОУ ВПО ТГТУ •
2010
УДК 004.052(075)
ББК 32.973.202я73
Г874

Р е ц е н з е н т ы:

Доктор технических наук, профессор ГОУ ВПО ТГТУ
В.А. Погонин

Доктор физико-математических наук, профессор
Института проблем экоинформатики Академии естественных наук РФ
Ф.А. Мкртчян

Г874 Надёжность информационных систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, Н.Г. Мосягина, К.А. Набатов. – Тамбов : Изд-во ГОУ ВПО ТГТУ, 2010. – 160 с. – 100 экз. – ISBN 978-5-8265-0911-1.

Рассмотрены основные понятия теории надёжности, показатели надёжности и аналитические зависимости между ними, вопросы надёжности программного и аппаратного обеспечения, понятия теории восстановления, надёжность восстанавливаемых и невосстанавливаемых технических устройств, структурные схемы надёжности, вопросы оценки надёжности аппаратно-программных комплексов с учётом характеристик программного и информационного обеспечения, практические методы статистической оценки надёжности.

Предназначено для студентов 4 курса очной формы обучения и 5 курса заочной формы обучения специальности 230201 "Информационные системы и технологии".

УДК 004.052(075)
ББК 32.973.202я73

ISBN 978-5-8265-0911-1

Министерство образования и науки Российской Федерации

Государственное образовательное учреждение высшего профессионального образования "Тамбовский государственный технический университет"

Ю.Ю. ГРОМОВ, О.Г. ИВАНОВА, Н.Г. МОСЯГИНА, К.А. НАБАТОВ

НАДЁЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Допущено УМО вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230200 "Информационные системы", специальности 230201 "Информационные системы и технологии"

Тамбов
Издательство ГОУ ВПО ТГТУ
2010

Учебное издание

ГРОМОВ Юрий Юрьевич,
ИВАНОВА Ольга Геннадьевна,
МОСЯГИНА Надежда Геннадьевна,
НАБАТОВ Константин Александрович

НАДЁЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебное пособие

Редактор Т.М. Г л и н к и н а
Инженер по компьютерному макетированию М.Н. Р ы ж к о в а

Подписано в печать 18.04.2010.
Формат 60 × 84 / 16. 9,3 усл. печ. л. Тираж 100 экз. Заказ № 210

Издательско-полиграфический центр ГОУ ВПО ТГТУ
392000, Тамбов, Советская, 106, к. 14

ВВЕДЕНИЕ

Наука о надёжности является сравнительно молодой, её формирование относится к середине XX века. Развитие и усложнение техники потребовали разработки научных основ нового направления – теории надёжности. Предмет её исследований составляют изучение причин, вызывающих отказы объектов; определение закономерностей, которым подчиняются отказы; разработка способов количественного измерения надёжности, методов расчёта и испытаний, разработка путей и средств повышения надёжности.

Первые шаги в области исследований надёжности были связаны со сбором статистических данных о надёжности радиоэлементов, а все усилия специалистов были направлены на определение причин ненадёжности. Следующими шагами стали развитие физической надёжности (физики отказов) и развитие математических основ теории надёжности, явившихся обязательным атрибутом разработки и проектирования сложных и ответственных технических систем.

В соответствующих областях техники разрабатывались и продолжают разрабатываться прикладные вопросы надёжности, вопросы обеспечения надёжности данной конкретной техники (радиоэлектронные приборы, средства вычислительной техники, транспортные машины, продуктопроводы, химические реакторы и т.д.). При этом решается вопрос о наиболее рациональном использовании общей теории надёжности в конкретной области и ведётся разработка таких новых положений, методов и приёмов, которые отражают специфику данного вида техники. Так возникла прикладная теория надёжности.

Комплексная автоматизация производственных процессов поставила перед управляющими устройствами новые, исключительно ответственные задачи, которые должны выполняться безупречно на протяжении всего периода работы автоматической линии, автоматизированного цеха или предприятия.

Современное общество нередко называют информационным. Под информационным обществом понимают такую ступень в развитии цивилизации, которая характеризуется возрастанием роли информации во всех областях общественной жизни; созданием и развитием рынка информационных услуг, новых форм социальной и экономической деятельности; созданием глобального информационного пространства, обеспечивающего доступ к мировым информационным ресурсам; превращением информационных ресурсов общества в реальные ресурсы социально-экономического развития.

Поэтому в настоящее время проблема надёжности является ключевой по отношению к современным информационным системам, по существу, от неё во многом зависят темпы их развития. Отказ в работе (в том числе и неправильное функционирование) информационных систем может привести даже к катастрофическим последствиям глобального масштаба.

Наука о надёжности развивается в тесном взаимодействии с другими науками [1].

Математическая логика позволяет представить сложные логические зависимости между состояниями системы и её комплектующих частей.

Теория вероятностей, математическая статистика и теория вероятностных процессов дают возможность учитывать случайный характер возникающих в системе событий и процессов, формировать математические основы теории надёжности.

Теория графов, исследования операций, теория информации, техническая диагностика, теория моделирования, основы проектирования систем и технологических процессов позволяют обоснованно решать задачи надёжности.

Можно выделить следующие основные направления развития теории надёжности.

1. Развитие математических основ теории надёжности. Обобщение статистических материалов об отказах и разработка рекомендаций по повышению надёжности объектов вызвали необходимость определять математические закономерности, которым подчиняются отказы, а также разрабатывать методы количественного измерения надёжности и инженерные расчёты её показателей.
2. Развитие методов сбора и обработки статистических данных о надёжности. Обработка статистических материалов в области надёжности потребовала развития существующих методов и привела к накоплению большой статистической информации о надёжности. Возникли статистические характеристики надёжности и закономерности отказов.
3. Развитие физической теории надёжности. Наука о надёжности не могла и не может развиваться без исследования физико-химических процессов. Поэтому большое внимание уделяется изучению физических причин отказов, влиянию старения и прочности материалов на надёжность, разнообразных внешних и внутренних воздействий на работоспособность объектов.

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ТЕОРИИ НАДЁЖНОСТИ

1.1. ПОНЯТИЕ НАДЁЖНОСТИ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Функциональные качества технических устройств (ТУ), в том числе и информационных систем (ИС), в значительной степени зависит от их надёжности.

ИС – это сложная программно-аппаратная система, включающая в свой состав эргатические (человеко-машинные) звенья, технические или аппаратные средства и программное обеспечение.

Говоря о надёжности ИС, необходимо учитывать две её составляющие: надёжность аппаратных средств и надёжность программного обеспечения. Если методы исследования и обеспечения надёжности технической (аппаратной) составляющей ИС аналогичны соответствующим мероприятиям других ТУ, то программное обеспечение отличается от подобной методологии. Так, при исследовании этих структур имеется в виду достоверность информации, её корректность, правильность интерпретации. В дальнейшем, говоря о ТУ, будем иметь в виду, в том числе, и аппаратные составляющие ИС (компьютеры, периферийное оборудование, коммутационное оборудование, кабельное оборудование и др.). Названные категории не исключают, а взаимно дополнят друг друга, поскольку в такой сложной системе, как ИС, обеспечить необходимый уровень надёжности можно, только учитывая, особенности её составляющих.

Теория надёжности опирается на совокупность различных понятий, определений, терминов и показателей, которые строго регламентируются в государственных стандартах (ГОСТ). В основу перечня положен ГОСТ 27.002–89 "Надёжность в технике. Основные понятия. Термины и определения" [2], формулирующий применяемые в науке и технике термины и определения в области надёжности, и материалы сайта [3].

Объект – техническое изделие определённого целевого назначения, рассматриваемое в периоды проектирования, производства, испытаний и эксплуатации.

Объектами могут быть различные системы и их элементы, в частности: сооружения, установки, технические изделия, устройства, машины, аппараты, приборы и их части, агрегаты и отдельные детали.

Система – объект, представляющий собой совокупность элементов, связанных между собой определёнными отношениями и взаимодействующих таким образом, чтобы обеспечить выполнение системой некоторой достаточно сложной функции.

Признаком системности является структурированность системы, взаимосвязанность составляющих её частей, подчинённость организации всей системы определённой цели. Системы функционируют в пространстве и времени.

Элемент системы – объект, представляющий отдельную часть системы. Само понятие элемента условно и относительно, так как любой элемент, в свою очередь, всегда можно рассматривать как совокупность других элементов. Понятия "система" и "элемент" выражены друг через друга, поскольку одно из них следовало бы принять в качестве исходного, постулировать. Понятия эти относительны: объект, считавшийся системой в одном исследовании, может рассматриваться как элемент, если изучается объект большего масштаба. Кроме того, само деление системы на элементы зависит от характера рассмотрения (функциональные, конструктивные, схемные или оперативные элементы), от требуемой точности проводимого исследования, от уровня наших представлений, от объекта в целом. Человек-оператор также представляет собой одно из звеньев системы человек–машина.

Различают следующие состояния объекта.

Исправность – состояние объекта, при котором он соответствует всем требованиям, установленным нормативно-технической документацией (НТД).

Неисправность – состояние объекта, при котором он не соответствует хотя бы одному из требований, установленных НТД.

Работоспособность – состояние объекта, при котором он способен выполнять заданные функции, сохраняя значения основных параметров в пределах, установленных НТД.

Неработоспособность – состояние объекта, при котором значение хотя бы одного заданного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям, установленным НТД.

Переход объекта в различные состояния:

Повреждение – событие, заключающееся в нарушении исправности объекта при сохранении его работоспособности.

Отказ – событие, заключающееся в нарушении работоспособности объекта.

Критерий отказа – отличительный признак или совокупность признаков, согласно которым устанавливается факт отказа. Признаки (критерии) отказов устанавливаются НТД на данный объект.

Восстановление – процесс обнаружения и устранения отказа (повреждения) с целью восстановления его работоспособности (исправности).

Восстанавливаемый объект – объект, работоспособность которого в случае возникновения отказа подлежит восстановлению в рассматриваемых условиях.

Невосстанавливаемый объект – объект, работоспособность которого в случае возникновения отказа не подлежит восстановлению в рассматриваемых условиях.

Временные характеристики объекта:

Наработка – продолжительность или объём работы объекта. Объект может работать непрерывно или с перерывами. Во втором случае учитывается суммарная наработка. Наработка может измеряться в единицах времени, циклах, единицах выработки и других единицах.

В процессе эксплуатации различают суточную, месячную наработку, наработку до первого отказа, наработку между отказами, заданную наработку и т.д. Если объект эксплуатируется в различных режимах нагрузки, то, например, наработка в облегчённом режиме может быть выделена и учитываться отдельно от наработки при номинальной нагрузке.

Технический ресурс – наработка объекта от начала его эксплуатации до достижения предельного состояния. Обычно указывается, какой именно технический ресурс имеется в виду: до среднего, капитального, от капитального до ближайшего среднего и т.п. Если конкретного указания не содержится, то имеется в виду ресурс от начала эксплуатации до достижения предельного состояния после всех (средних и капитальных) ремонтов, т.е. до списания по техническому состоянию.

Срок службы – календарная продолжительность эксплуатации объекта от её начала или возобновления после капитального или среднего ремонта до наступления предельного состояния.

Эксплуатация объекта – это стадия его существования в распоряжении потребителя при условии применения объекта по назначению, что может чередоваться с хранением, транспортированием, техническим обслуживанием и ремонтом, если это осуществляется потребителем.

Срок сохраняемости – календарная продолжительность хранения и (или) транспортирования объекта в заданных условиях, в течение и после которой сохраняются значения установленных показателей (в том числе и показателей надёжности) в заданных пределах.

Определение надёжности. Работа любой технической системы может характеризоваться её эффективностью (рис. 1.1), под которой понимается совокупность свойств, определяющих способность системы выполнять при её создании определённые задачи.

В соответствии с ГОСТ 27.002–89 под *надёжностью* понимают свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортировки.

При описании характеристик составляющих и показателей надёжности, основных понятий и определений теории надёжности были использованы материалы источников [4 – 21].

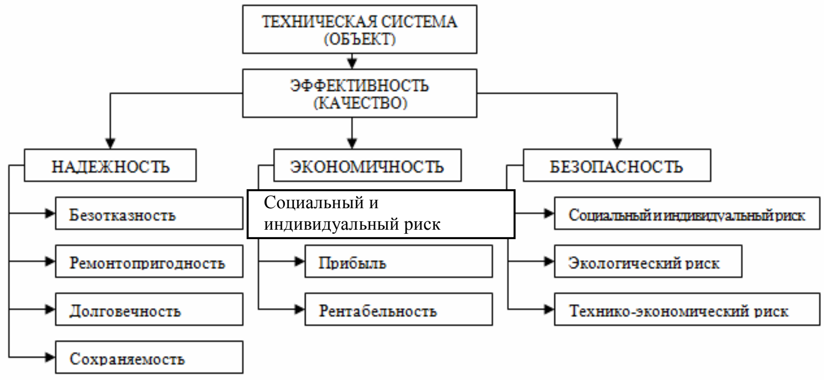


Рис. 1.1. Основные свойства технических систем

Самые совершенные начальные технические характеристики ТУ являются необходимыми, но не достаточными условиями высоких эксплуатационных качеств этих устройств. Начальные характеристики ТУ показывают его потенциальные технические возможности. Важной является способность ТУ сохранять эти характеристики в течение всего жизненного цикла или в процессе эксплуатации. Эта способность зависит как от свойств, которые были заложены в ТУ в процессе проектирования и изготовления, так и от интенсивности эксплуатации, правильности и своевременности технического обслуживания. Поэтому физический смысл надёжности состоит в способности сохранять эти свойства, сопротивляться агрессивным эксплуатационным факторам. Надёжность может выступать как в качестве самостоятельной эксплуатационной характеристики, так и служить составляющей других эксплуатационных характеристик. При этом надёжность является частью более широкого понятия – эффективности.

Эффективность ТС – это свойство системы выполнять заданные функции с требуемым качеством. Причём на эффективность функционирования ТС наряду с надёжностью влияют и другие характеристики, такие как точность, быстродействие, помехоустойчивость и т.д.

Говоря о некотором ТУ, нужно иметь в виду, что его надёжность $P_{\text{ТУ}}$ в общем случае оказывает влияние на эффективность работы Э более сложной системы, частью которой он является. Это влияние осуществляется через технико-экономическую эффективность ТЭ, представляющую собой характеристику уровня выполнения системой своих функций с учётом финансовых, трудовых и материальных затрат. Формально это можно записать следующим образом:

$$\text{Э} = f(\text{ТЭ}, \Phi_1, ..., \Phi_n);$$

$$\text{ТЭ} = f(P_{\text{ТУ}}, \Phi_1, ..., \Phi_n);$$

$$P_{\text{ТУ}} = (K_{\text{н}}, \text{У}_{\text{и}}),$$

где $K_{\text{н}}$ – начальный уровень надёжности ТУ; $\text{У}_{\text{и}}$ – фактор, учитывающий условия эксплуатации и технического обслуживания этой системы; $\Phi_1, ..., \Phi_n$ – прочие факторы.

В качестве критерия оценки технико-экономической эффективности ТЭ технического устройства может быть использовано соотношение:

$$\text{ТЭ} = \frac{Q}{\sum E},$$

где Q – полезный эффект; $\sum E$ – суммарные затраты.

Зависимость между характеристиками надёжности и технико-экономической эффективностью может быть представлена в виде:

$$\text{ТЭ} = a_0(t) + \sum_i^m a_i(t) P_i.$$

В этом выражении P_i – количественные показатели надёжности, такие как безотказность, долговечность, сохраняемость и ремонтопригодность; $a_i(t)$ – коэффициенты, показывающие степень влияния соответствующих показателей надёжности; $a_0(t)$ – коэффициент, учитывающий влияние прочих эксплуатационных факторов.

В заданных условиях эксплуатации необходимо стремиться к тому, чтобы поддерживать такое значение $P_{ТУ}$, которое позволит эксплуатировать ТУ без ограничений при минимальных трудовых, материальных и финансовых затратах.

Таким образом, основной задачей при проектировании ТС различного назначения можно назвать повышение эффективности и качества, а, следовательно, улучшение таких характеристик ТС, как надёжность, прочность, быстродействие и т.д. Одним из методов повышения надёжности, широко используемым при проектировании ТС, является *резервирование* – метод повышения надёжности за счёт введения избыточности. Под *избыточностью* понимают дополнительные средства и возможности сверх минимально необходимых для выполнения ТС заданных функций.

1.2. Состояние объекта, понятие события и отказа

Как и всякое свойство, в общем случае надёжность в процессе эксплуатации изменяется. Уменьшение надёжности ТУ происходит в результате его износа и старения. Тогда можно сказать, что в момент начала эксплуатации ТУ надёжность была максимальной и с течением времени это свойство, несмотря на профилактические мероприятия, уменьшилось настолько, что дальнейшая эксплуатация ТУ стала нецелесообразной.

В связи с этим вводятся понятия работоспособности и отказа, которые определяются как состояние ТУ.

В соответствии с определением надёжности по ГОСТ 27.002–83 *работоспособность* можно определить как состояние, при котором ТУ способно выполнять заданные функции, сохраняя значения заданных параметров в пределах, установленных нормативно-технической документацией (НТД).

Понятие работоспособности нельзя путать с понятием исправности.

Исправность – это такое состояние ТУ, при котором оно соответствует всем требованиям, установленным нормативно-технической документацией. Поэтому понятие "исправность" более широкое, чем работоспособность. Действительно, ТУ может быть в неисправном состоянии, но функционировать нормально.

Если хотя бы один из заданных параметров ТУ, характеризующих его способность выполнять заданные функции, не соответствует требованиям, то это ТУ находится в неработоспособном состоянии. Такое неработоспособное состояние называется *отказом* и является противоположным по отношению к работоспособному состоянию.

Переход ТУ из одного состояния в другое называется *событием.*

Отказ является событием нарушения работоспособности и происходит в результате воздействия на ТУ различных агрессивных факторов, по большей части носящих случайный характер. Таким образом, отказ является случайным событием со всеми особенностями, присущими случайному событию.

При переходе объекта в различные состояния могут возникнуть также *повреждения* – события, заключающиеся, в отличие от отказа, в нарушении исправности объекта при сохранении его работоспособности.

Выделяется понятие *критерий отказа* – отличительный признак или совокупность признаков, согласно которым устанавливается факт отказа. Признаки (критерии) отказов устанавливаются НТД на данный объект.

1.3. Классификация отказов технических УСТРОЙСТВ

Возникающие в ТУ отказы разнообразны как по характеру развития и проявления, так и по причинным связям (табл. 1.1).

1.1. Классификация отказов ТС

Признаки отказа	Вид отказа	Характеристика отказа
Характер изменения параметра до момента возникновения отказа	Внезапный	Скачкообразное изменение значений одного или нескольких параметров ТС
	Постепенный	Постепенное изменение одного или нескольких параметров за счёт медленного, постепенного ухудшения качества ТС
Связь с отказами других элементов (узлов, устройств)	Независимый (первичный)	Отказ не обусловлен повреждениями или отклонениями других элементов (узлов)
	Зависимый (вторичный)	Отказ обусловлен повреждениями или отказами других элементов (узлов, устройств)
Возможность использования элемента после отказа	Полный	Полная потеря работоспособности, исключающая использование ТС по назначению

	Частичный	Дальнейшее использование системы возможно, но с меньшей эффективностью
Характер проявления отказа	Сбой	Самоустраняющийся отказ, приводящий к кратковременному нарушению работоспособности
	Перемежающийся	Многократно возникающий сбой одного и того же характера (то возникающий, то исчезающий), связанный с обратными случайными изменениями режимов работы и параметров устройства
	Устойчивый (окончательный)	Отказ, устраняемый только в результате проведения восстановительных работ, является следствием необратимых процессов в деталях и материалах
Признаки отказа	Вид отказа	Характеристика отказа
Причина возникновения отказа	Конструкционный	Возникает вследствие нарушения установленных правил и норм конструирования
	Производственный	Возникает из-за нарушения или несовершенства технологического процесса изготовления или ремонта ТС
	Эксплуатационный	Возникает вследствие нарушения установленных правил и условий эксплуатации ТС
Время возникновения отказа	Период приработки	Обусловлен скрытыми производственными дефектами, не выявленными в процессе контроля
	Период норм эксплуатации	Обусловлен несовершенством конструкции, скрытыми производственными дефектами и эксплуатационными нагрузками
	Период старения	Обусловлен процессами старения и износа материалов и элементов ТС
Возможности обнаружения отказа	Очевидные (явные)	
	Скрытые (неявные)	

1.4. ФАКТОРЫ, ВЛИЯЮЩИЕ НА СНИЖЕНИЕ НАДЁЖНОСТИ ТЕХНИЧЕСКИХ УСТРОЙСТВ

Все отказы ТУ происходят вследствие воздействия различных факторов, к которым относятся физические, физико-химические и химические, биологические и эксплуатационные факторы.

Физические причины возникновения отказов. Физические причины или факторы возникновения отказов представляют собой физические явления, процессы и свойства среды, воздействующие на ТУ и наносящие им вред, тем самым ухудшая их состояния.

Физические факторы делятся на внешние и внутренние. Внешние физические факторы являются совокупностью свойств внешней окружающей среды, оказывающих влияние на работоспособность ТУ.

К ним относятся чрезмерно высокая или низкая окружающая температура, осадки, высокая влажность воздуха, низкое давление, наличие в воздухе взвешенной пыли, аномальные электромагнитные проявления окружающей среды.

Внутренние физические факторы представляют собой те явления и процессы, которые, развиваясь в ТУ во время их функционирования, одновременно влияют на состояние и рабочие режимы этих же ТУ и их составных элементов, а также ТУ, взаимосвязанных с ними. Сюда можно отнести вибрацию, внутренний перегрев и другие факторы. Под влиянием длительного воздействия на ТУ физических факторов происходит износ элементов (деталей сложных ТУ) и старение материалов, из которых они выполнены. Износ характеризуется постепенным изменением формы и размера отдельных элементов системы, что приводит к ухудшению их работы. Старение характеризуется постепенным структурным изменением материалов, из которых изготовлены ТУ. Это, в свою очередь, ведёт к ухудшению их рабочих характеристик.

Физико-химические и химические причины возникновения отказов. К физико-химическим факторам, снижающим надёжность работы ТУ, относятся такие процессы внешней среды и процессы, происходящие в самих ТУ, в результате физического действия которых происходят химические реакции или изменение физических свойств ТУ.

К таким явлениям можно отнести вредные химические примеси в атмосфере, действие лучистой энергии, электроэрозию, чрезмерное выделение тепла, например в результате короткого замыкания.

К химическим причинам относятся химические реакции, приводящие к изменению молекулярного состава материалов. К наиболее распространённой реакции такого типа относится окисление железа. Появляющиеся в результате этого процесса окислы имеют отличные от первоначальных материалов физико-химические свойства. Другой распространённой медленнотекущей химической реакцией является полимеризация изоляционных материалов в электрических проводах. Полимеризация ведёт к отвердеванию изоляции, к потере упругости и изолирующих свойств и дальнейшему разрушению. Вследствие этого происходят короткие замыкания, приводящие к большим разрушениям и даже человеческим жертвам.

Биологические факторы, влияющие на ухудшение эксплуатационных свойств технических объектов. К биологическим факторам относятся воздействия животных и растительных организмов, наносящих вред ТУ. Наиболее часто биологические факторы проявляются при хранении ТУ. В этот период, если не соблюдены необходимые при хранении профилактические меры, хранящееся устройство может подвергнуться воздействию термитов, уничтожающих изоляционные материалы, каучуки, полимеры. Аналогичным образом воздействуют на ТУ и мелкие грызуны. Большой вред для электрических и электронных систем могут принести тараканы. Они становятся причиной короткого замыкания в электрических и электронных схемах. Многие ТУ в холодное время является источником тепла. Поэтому мелкие животные через различные отверстия могут проникнуть внутрь и стать причиной замыканий, несрабатывания, поломок и разрушений отдельных деталей.

Эксплуатационные факторы возникновения отказов. К эксплуатационным факторам относятся технические возможности самих ТУ, технологического оборудования для профилактических работ, а также объективные и субъективные возможности специалистов, задействованных в процессе эксплуатации ТУ. К причинам, по которым могут возникать отказы в процессе эксплуатации и проведения профилактических работ, чаще всего относят:

- несоблюдение требований эксплуатации, чрезмерно высокая интенсивность эксплуатации;
- невыполнение требуемого объёма ремонта;
- отсутствие технологического оборудования и приспособлений;
- слабое крепление деталей;
- постановка нестандартных деталей;
- отклонение от установленных размеров;
- отступление от технологических требований;
- неудовлетворительный осмотр;
- личные качества исполнителей.

Первый из перечисленных факторов определяется неудовлетворительной работой специалистов или созданием сложных условий эксплуатации, как климатических, так и режимных. Невыполнение требуемого объёма ремонта большого перечня типов ТУ является причиной более четверти отказов от их общего количества, т.е. возникают такие отказы достаточно часто. На выявление скрытых дефектов тратится много времени, отведённого для выполнения ремонтных операций, поэтому трудно переоценить значение средств технической диагностики. Отсутствие необходимого оборудования приводят к низкой распознаваемости скрытых дефектов. Дефекты, возникающие из-за слабого крепления деталей и узлов, характерны для многих типов ТУ. Отказы, возникающие по этой причине, происходят, во-первых – из-за отсутствия или неприменения необходимых средств контроля и во-вторых – из-за несоблюдения правил сборки.

Нестандартными деталями называются такие, которые производятся не предприятиями-изготовителями ТУ, а эксплуатирующими организациями. В основном это детали механических узлов и агрегатов. Их изготовление характеризуется большим разнообразием технологических операций и непостоянством исполнителей. Вследствие этого на ТУ могут быть установлены детали низкого качества. Они могут отказывать сами и быть причиной отказа других деталей.

Дефекты по отклонению от установленных размеров возникают в местах соединения проводов, деталей и узлов между собой, в их расположении по отношению друг к другу и корпусу ТУ. Основными причинами возникновения отказов из-за этих дефектов при исполнении монтажных работ являются несоблюдения исполнителями конструктивных размеров, определяющих взаимное расположение деталей, а также изменение этих размеров в процессе эксплуатации из-за ослабления вследствие агрессивных воздействий внешней среды.

Отступление от технологических требований проявляются, прежде всего, в том, что на ремонтируемое ТУ, вопреки требованиям нормативно-технической и ремонтной документации, устанавливается некондиционное оборудование.

При неудовлетворительном осмотре в период профилактических работ не выявляются скрытые дефекты, что приводит к отказам оборудования в период эксплуатации ТУ.

Вопросы воспитания специалистов, соблюдения правил трудовой дисциплины, технической учёбы и повышения квалификации, вопросы самоконтроля и контроля выполняемых работ являются очень важными в деле профилактики дефектов и возникающих по их причинам отказов по вине человеческого фактора.

Уменьшение влияния названных и ряда других факторов является одной из основ работа по поддержанию надёжности работы ТУ.

1.5. Факторы, определяющие надёжность информационных систем

Для построения надёжных ИС можно использовать различные виды обеспечения: экономическое, временное, организационное, структурное, технологическое, эксплуатационное, социальное, эргатическое, алгоритмическое, синтаксическое, семантическое.

Обеспечение можно характеризовать как совокупность факторов, способствующих достижению поставленной цели.

Организационное, экономическое и *временное обеспечения*, обуславливаемые необходимостью материальных и временных затрат, используются для поддержания достоверности результатов работы ИС. Они включают в себя:

- правовые и методические аспекты функционирования ИС;
- нормативы достоверности информации по функциональным подсистемам и этапам преобразования информации;
- методики выбора и обоснования оптимальных структур, процессов и процедур преобразования информации.

Структурное обеспечение ИС должно обеспечивать надёжность функционирования технических комплексов и эргатических звеньев, а также ИС в целом. Здесь обосновывается рациональное построение структуры ИС, зависящее от выбора структуры технологического процесса преобразования информации, обоснования взаимосвязи между отдельными звеньями системы, резервирования функциональных звеньев системы и использования устройств, осуществляющих процедуры контроля.

Надёжность технологического обеспечения связана с выбором схемных и конструктивных решений отдельных ТУ и технологических комплексов, входящих в состав системы, технологий и протоколов реализации информационных процессов.

Эксплуатационное обеспечение связано с выбором режимов работы устройств, технологий обслуживания, профилактик и ремонтов.

К *социальному обеспечению* относятся такие факторы, как создание здоровой психологической обстановки в коллективе, повышение ответственности за выполненную работу, повышение квалификации специалистов, моральной и материальной заинтересованности в правильности выполнения работы.

Эргатическое обеспечение включает комплекс факторов, связанных с рациональной организацией работы человека в системе. Это правильное расположение функций между людьми и техническими средствами, обязательность норм и стандартов работы, оптимальность интенсивности и ритмичности, построение рабочих мест в соответствии с требованиями эргономики.

Надёжность алгоритмического обеспечения связана с обеспечением высокого качества и безошибочности алгоритмов и программ преобразования информации, реализации контроля достоверности информации.

Информационное синтаксическое и *семантическое обеспечение* должно обеспечить специальную информационную избыточность, избыточность данных и смысловую избыточность, обуславливающие возможность проведения контроля достоверности информации.

Личные качества исполнителей также играют немаловажную роль. Ошибки обслуживающего персонала, выход ИС из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала – операторов (превышение расчётного числа запросов, чрезмерный объём обрабатываемой информации и другие неоправданные действия), невозможность или нежелание обслуживающего персонала выполнять свои функции приводят к чрезвычайно серьёзным последствиям. Это могут быть длительный простой в работе ИС, искажение обрабатываемой информации и получение неверных результатов, потеря информации, сбои в работе программ и оборудования, отказы оборудования.

Таким образом, поддержание высокой надёжности работы ИС в целом является важной и сложной инженерно-технической и социально-организационной задачей.

Вопросы для самоконтроля

1. Указать основные направления развития теории надёжности.
2. Понятие системы и элемента системы.
3. Понятие надёжности ТУ.
4. Составляющие надёжности.
5. Понятие эффективности ТУ.
6. Какое состояние ТУ называется работоспособным?
7. Что такое "отказ"?
8. Дать характеристику отказов ТУ.
9. Причины возникновения отказов.
10. Факторы, влияющие на надёжность информационных систем.

2. ОСНОВНЫЕ ПОКАЗАТЕЛИ НАДЁЖНОСТИ НЕВОССТАНАВЛИВАЕМЫХ ТЕХНИЧЕСКИХ УСТРОЙСТВ

2.1. СОСТАВЛЯЮЩИЕ НАДЁЖНОСТИ

В соответствии с определением надёжность является сложным свойством. Именно благодаря надёжности ТУ выполняет определённые функции, делая это в течение некоторого срока, с заданным качеством. Это происходит вследствие наличия таких составляющих надёжности, как безотказность, ремонтопригодность, долговечность и сохраняемость.

Безотказность – это способность ТУ работать без отказа в течение некоторого времени.

Долговечность – свойство ТУ сохранять работоспособность с необходимыми перерывами для технического обслуживания и ремонта до предельного состояния, оговоренного в технической документации.

Сохраняемость – это свойство ТУ сохранять работоспособность при хранении до начала эксплуатации, в перерывах между периодами эксплуатации и после транспортировки.

Ремонтопригодность – свойство конструктивной приспособленности ТУ к выявлению, устранению и предупреждению в них неисправностей.

Эта составляющая разделяет все ТУ на *восстанавливаемые* (ремонтируемые) и *невосстанавливаемые* (неремонтируемые). К последним относятся такие ТУ, ремонт которых в случае отказа не предусмотрен и не производится. Они составляют достаточно большую часть технических устройств, так как в большинстве случаев являются элементами сложных технических систем.

Названные свойства относятся к так называемым единичным показателям надёжности, объединённым в комплексное понятие собственно надёжности. Рассмотрим эти и другие показатели, характеризующие надёжную работу ТУ, относящихся к неремонтируемым, так как эти показатели носят ключевой характер в теории надёжности.

2.2. Простейший поток отказов

В теории надёжности различают понятия "система" и "элемент". Элемент – составная часть сложного ТУ, которая при расчёте и исследовании надёжности не подлежит расчленению. Система – совокупность совместно действующих элементов, предназначенная для выполнения определённых заданных функций. Тогда отказ системы может наступить при отказе одного элемента этой системы. В теории надёжности, наряду с другими, рассматривают простейший поток отказов, который соответствует простейшему потоку случайных событий.

Простейший поток обладает следующими свойствами:

- стационарность,
- ординарность,
- отсутствие последовательности.

Стационарность определяется тем, что вероятность появления того или иного числа отказов на некотором временном интервале эксплуатации t зависит только от длины этого интервала, но не зависит от положения этого интервала на оси времени. Иными словами, предполагается, что отказы распределены на оси времени в процессе эксплуатации с одинаковой средней плотностью λ.

Ординарность определяется тем, что вероятность возникновения двух или более отказов системы в некоторый момент времени t пренебрежимо мала по сравнению с вероятностью одного отказа. Это означает практически, что одновременно в системе отказа более двух элементов быть не может.

Отсутствие последствия определяется тем, что наступление отказа в момент t не зависит от того, сколько отказов и в какие моменты времени они возникали до момента t. Поскольку простейший поток отказов соответствует простейшему потоку событий, то он подчиняется закону Пуассона.

Если случайная величина ξ *в простейшем потоке событий за время* τ *– некоторое целое положительное значение* K*, то эта величина распределена по закону Пуассона*:

$$p(\xi = K) = \frac{a^K}{K!} e^{-a}.$$

Статистический смысл параметра а заключается в том, что a – это среднее число событий, наступающих в простейшем потоке за время τ:

$$a = \lambda\tau.$$

С точки зрения надёжности случайная величинам ξ представляет собой число отказов ТУ, а число $p(\xi = K)$ представляет собой вероятность появления ровно K отказов ТУ за время τ. Представляет интерес вероятность отсутствия отказов или вероятность работы ТУ без отказов в течение времени τ:

$$p(\xi = 0) = \frac{a^0}{0!} e^{-a} = e^{-a} = e^{-\lambda\tau}.$$

Тогда вероятность противоположного события, заключающегося в том, что за время τ произойдет хотя бы один отказ, будет равна

$$p(\xi \ge 1) = 1 - p(\xi = 0) = 1 - e^{-\lambda\tau}.$$

Особенность закона Пуассона заключается в том, что математическое ожидание и дисперсия равны между собой и равны величине a:

$$M\xi = D\xi = a.$$

2.3. Вероятность безотказной работы и вероятность отказов

Надёжность как качественная характеристика всегда принималась во внимание при решении различных вопросов эксплуатации и технического обслуживания. Количественное определение надёжности появилось с возникновением теории надёжности. Математической платформой теории надёжности являются теория вероятностей и математическая статистика. Действительно, отказы в ТУ происходят случайным образом в неожиданные моменты времени. Это характерно даже для множества однотипных устройств, изготовленных на одном предприятии и поставленных на эксплуатацию в одно и то же время. Несмотря на единый проект, одинаковость технологии производства – каждый из них имеет индивидуальную способность сохранять свои первоначальные качества. Первоначально кажется, что никакой закономерности в появлении отказов нет. Тем не менее, такая закономерность существует. Проявляется она тогда, когда ведётся наблюдение не за одним, а за многими ТУ, находящимися в эксплуатации.

В качестве основной количественной меры надёжности ТУ, характеризующей закономерность появления отказов во времени, принята вероятность безотказной работы.

Вероятность безотказной работы (ВБР) – это вероятность того, что за определённое время работы ТУ и в заданных условиях эксплуатации отказа не происходит. Поскольку возникновение отказа является случайным событием, время его возникновения t_0 – также событие случайное. Поэтому ВБР:

$$p(t) = p(t_0 \geq t),$$

где t – заданное время работы.

Вероятность появления отказа – это вероятность противоположного события:

$$q(t) = p(t_0 < t).$$

Но событие отказа и событие безотказности – суть противоположные события. Поэтому в соответствии со свойством вероятностей противоположных событий можно записать:

$$p(t) + q(t) = 1.$$

На практике определяют оценки этих вероятностей. Пусть N – это общее количество однотипных ТУ, эксплуатируемых в течение времени t. За это время $N(t)$ ТУ работало безотказно, а $n(t)$ отказало. Таким образом:

$$N = N(t) + n(t),$$

т.е. через время t общее количество как исправных, так и отказавших ТУ, равно первоначальному. Статистическая вероятность безотказной работы определяется выражением:

$$p^*(t) = \frac{N(t)}{N},$$

а частота отказов:

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

Найдём сумму этих частот:

$$p^*(t) + q^*(t) = \frac{N(t)}{N} + \frac{n(t)}{N} = \frac{N(t) + n(t)}{N} = \frac{N}{N} = 1.$$

Для перехода от $p^*(t)$ и $q^*(t)$ к $p(t)$ и $q(t)$ нужно взять предел отношений частот:

$$p(t) = \lim_{N \to \infty} \frac{N(t)}{N},$$

$$q(t) = \lim_{N \to \infty} \frac{n(t)}{N}.$$

Так как $N \to \infty$ достичь невозможно, то под этой декларацией на практике можно подразумевать весь парк поставленных на эксплуатацию однотипных ТУ. С течением времени общее количество отказов ТУ увеличивается. Следовательно, увеличиваются и $q(t)$, а значит, уменьшается $p(t)$. Кривые, определяющие характер изменения этих изменений, представлены на рис. 2.1.

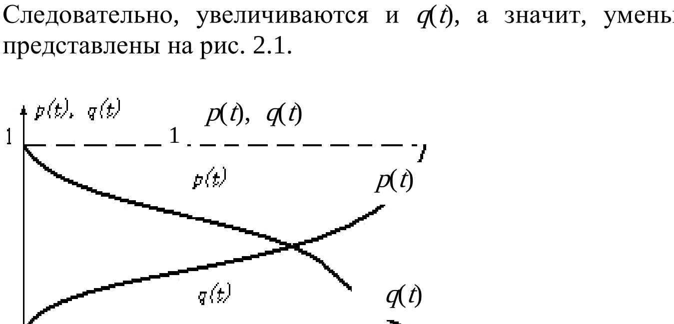


Рис. 2.1. Характер изменения кривых *p*(*t*) и *q*(*t*)

На практике часто необходимо определить надёжность ТУ в течение некоторого интервала времени от t_a до t_b (например, в течение периода работы этого устройства) при условии, что оно уже находилось в эксплуатации некоторое время t_b. ВБР ТУ за время $t_b - t_a$ при условии, что оно безотказно проработало в течение t_a часов, определяется условной вероятностью

$$p\left(\frac{t_b - t_a}{t_a}\right) = p\left(t_0 \geq t_b\right).$$

Эта условная вероятность численно равна вероятности $p\left(\frac{t_b}{t_a}\right)$.

$$p\left(\frac{t_b - t_a}{t_a}\right) = p\left(\frac{t_b}{t_a}\right) = \frac{p\left(t_b t_a\right)}{p\left(t_a\right)}.$$

Но $p\left(t_b,\, t_a\right)$ численно равна вероятности того, что ТУ безотказно проработает t_b часов:

$$p\left(t_b,\, t_a\right) = p\left(t_b\right).$$

Тогда

$$p\left(\frac{t_b}{t_a}\right) = \frac{p\left(t_b\right)}{p\left(t_a\right)}.$$

В частном представлении эта формула примет вид:

$$p^*\left(\frac{t_b}{t_a}\right) = \frac{N\left(t_b\right)}{N\left(t_a\right)},$$

так как

$$p^*\left(t_a\right) = \frac{N\left(t_a\right)}{N}; \quad p^*\left(t_b\right) = \frac{N\left(t_b\right)}{N}.$$

Используя величину вероятности безотказной работы p(t), можно оценить среднее количество элементов или устройств ИС (например, сети, ЭВМ или её периферии) $n(t)$, которые могут отказать за интервал времени Δt при известной наработке t:

$$n(t) = Np(t) - Np(t + \Delta t),$$

где N – число исправных элементов ИС в начале её эксплуатации.

2.4. Интенсивность отказов

С течением времени ТУ становятся менее надёжными и в процессе эксплуатации отказывают. Если весь период эксплуатации разделить на равные промежутки времени Δt_i ($i = \overline{1,\, k}$), то в любой из этих промежутков отказывают Δn_i однотипных объектов. Числовой характеристикой, которая путём учёта отказавших однотипных объектов позволила бы определить уровень надежности этих объектов в любой момент времени, является *интенсивность отказов*. Она определяется количеством отказов Δn_i в интервале Δt_i, отнесённых к исправно действующим однотипным ТУ в данном интервале:

$$\lambda_i^* = \frac{\Delta n_i}{N_i \Delta t_i},$$

где N_i – среднее число исправно действующих ТУ в интервале Δt_i. Индекс i представляет собой указатель интервала, для которого рассчитывается интенсивность отказа.

Обычно из условия задачи известны количество m отказавших ТУ, Δn_i и величина интервала времени Δt_i. Величина N_i по своей сути представляет собой математическое ожидание числа безотказно проработавших ТУ в течение i-го интервала времени. Наиболее очевидной статистической оценкой этой величины могло бы стать среднее арифметическое

$$N_i = \frac{\sum_{i=1}^{m}\left(N - \Delta n_i\right)}{i}.$$

Однако существует оценка, которая с большей точностью соответствует значению математического ожидания:

$$N_i = N - \sum_{k=1}^{i-1} \Delta n_k - \frac{\Delta n_i}{2}.$$

Переходя от дискретного времени Δt к непрерывному $\left(\Delta t \to 0\right)$, получим:

$$\lambda(t) = \frac{1}{N(t)} \frac{dn(t)}{dt}.$$

Введём понятие плотности вероятности отказа в однотипных ТУ. Если в знаменателе выражения для Δ_i^* величину N_i заменить на N, получим:

$$f_i^* = \frac{\Delta n_i}{N \Delta t_i},$$

или при $\Delta t \to 0$:

$$f(t) = \frac{1}{N}\frac{dn(t)}{dt}.$$

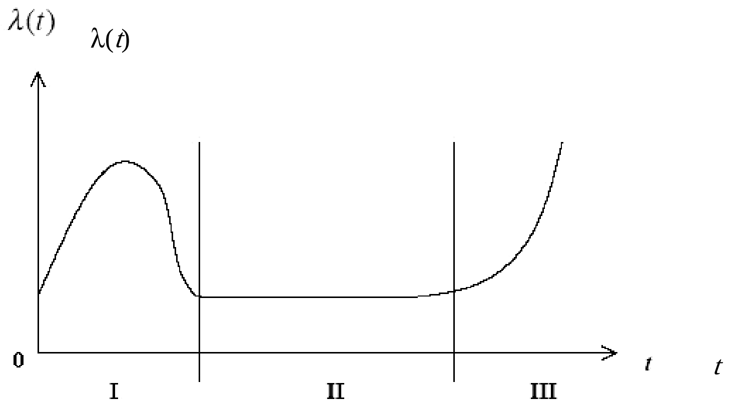


Рис. 2.2. Кривая интенсивности отказов

Отсюда следует, что

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

или

$$f(t) = \lambda(t)\, p(t)\,.$$

Интенсивность отказов имеет характерные изменения в процессе эксплуатации (рис. 2.2). Характерными являются 3 участка, получившие название периодов приработки (I), нормальной эксплуатации (II) и период износа и старения (III). В первом периоде проявляются конструктивно производственные недостатки, во II периоде отказы происходят в основном из-за нарушений или изменений условий эксплуатации.

В III периоде отказы определяются причинами, скрытыми в самом названии этого периода.

2.5. СРЕДНЕЕ ВРЕМЯ БЕЗОТКАЗНОЙ РАБОТЫ

Часто в качестве характеристики надёжности используют среднее время безотказной работы. Обозначим эту величину буквой T. Тогда некоторое количество из множества однотипных ТУ, находящихся в эксплуатации, проработает безотказно какое-то время $t \geq T$, причём каждый из ТУ – своё, остальные же откажут раньше, чем наступит время T. Отсюда время T можно рассматривать как математическое ожидание отрезков времени безотказной работы этих однотипных ТУ.

В соответствии с определением получается:

$$T = \int_0^\infty t f(t)\, dt.$$

Здесь $f(t)$ – плотность вероятности времени отказов однотипных ТУ. Статистическим аналогом среднего времени безотказной работы является среднее статистическое время безотказной работы:

$$T^* = \frac{\sum_{j=1}^{n} t_j}{n},$$

где t_j – время появления отказа j-го ТУ; n – количество отказов в различные j-е моменты времени.

2.6. Аналитические зависимости между основными показателями надёжности

Вероятность отказов $q(t)$ определяется выражением

$$q(t) = p(t_0 < t)\,.$$

С другой стороны, выражение $p(t_0 < t)$ по определению функции распределения есть не что иное как функция распределения времени до отказа:
$q(t) = F(t)$.

Тогда
$$f(t) = \frac{dF(t)}{dt} = \frac{dq(t)}{dt}.$$

Учитывая, что $p(t) = 1 - q(t)$, получим

$$f(t) = \frac{dp(t)}{dt}.$$

Отсюда следует, что

$$f(t) = q'(t) = -p'(t).$$

Подставим значение плотности вероятности отказов в выражение интенсивности отказов:

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

В результате получится дифференциальное уравнение относительно вероятности безотказной работы:

$$\lambda(t) = -\frac{p'(t)}{p(t)}.$$

Эта важная зависимость широко используется в теории надёжности. Она является обобщённым законом надёжности невосстанавливаемых ТУ в дифференциальной форме. Результатом интегрирования этого уравнения будет
$$-\int_0^t \lambda(t)\,dt = \ln p(t),$$
откуда
$$p(t) = e^{-\int_0^t \lambda(t)\,dt}.$$

Полученное выражение представляет собой обобщенный закон надёжности в интегральной форме. Подставляя этот результат в выражение $f(t) = \lambda(t)\,p(t)$, получим

$$f(t) = \lambda(t)\,e^{-\int_0^t \lambda(t)\,dt}.$$

Проведём аналогичные преобразования для среднего времени безотказной работы:

$$T = \int_0^\infty tf(t)\,dt = -\int_0^\infty \frac{dp(t)}{dt}\,dt = -\int_0^\infty tdp(t).$$

Интегрируем полученное выражение по частям:

$$-\int_0^\infty tdp(t) = -tp(t)\Big|_0^\infty + \int_0^\infty p(t)\,dt - tp(t)\Big|_0^\infty = 0, \text{ так как } p(\infty) = 0.$$

Поэтому
$$T = \int_0^\infty p(t)\,dt$$
или
$$T = \int_0^\infty e^{-\int_0^\infty \lambda(t)\,dt}.$$

Это выражение связывает среднюю наработку до отказа с вероятностью безотказной работы. Отсюда следует, что средняя наработка до отказа равна площади под кривой вероятности безопасной работы. Необходимо учитывать, что приведённые показатели надёжности относятся к работоспособным объектам, включённым в работу в нулевой момент времени.

Рассмотрим более подробно период нормальной эксплуатации.

В этот период в основном имеют место внезапные отказы. Они, имея случайный характер происхождения, подчиняются закону распределения, вытекающему из условий постоянства интенсивности отказов. Поэтому для этого периода можно считать, что интенсивность отказов является практически постоянной величиной, т.е. $\lambda(t) = \text{const} = \lambda$.

В связи с этим основные зависимости примут вид:

$$p(t) = e^{-\lambda t},$$

$$q(t) = 1 - p(t) = 1 - e^{-\lambda t},$$

$$f(t) = \lambda e^{-\lambda t},$$

$$T = \int_0^{\infty} e^{-\lambda t} dt = -\frac{1}{\lambda}\int_{\lambda}^{\infty} e^{-\lambda t} d(\lambda t) = \frac{1}{\lambda}.$$

Полученное выражение для $p(t)$ называют *экспоненциальным законом надёжности.* В период нормальной эксплуатации поток отказов является простейшим. Принимая во внимание последнее выражение, получим

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

При $t = T$ вероятность безотказной работы будет равна

$$p(t) = e^{-1} = \frac{1}{e} \approx 0,37.$$

Это говорит о том, что для обеспечения высокого уровня надёжности невосстанавливаемых ТУ следует выбирать срок их службы намного меньший, чем среднее время безотказной работы. Так, например, если $t / T = 0,1$, то $p(t) = 0,9$, или сокращение срока службы в 10 раз ведёт к увеличению вероятности безотказной работы приблизительно в 2,4 раза.

Если срок службы ТУ во много раз меньше среднего времени безотказной работы, то характеристики надёжности удобно рассчитывать по упрощённым формулам. Разлагая выражение

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

в ряд и принимая во внимание только первый член этого ряда, получим:

$$p(t) \approx 1 - \frac{t}{T} = 1 - \lambda t,$$

$$q(t) \approx \frac{t}{T} = \lambda t.$$

Эти формулы дают хорошее приближение при $\lambda t < 0,1$. При экспоненциальном законе распределения вероятность $p = \left(\frac{t_b}{t_a}\right)$ может быть переписана в следующем виде:

$$p\left(\frac{t_b}{t_a}\right) = \frac{e^{-\lambda\ t_a}}{e^{-\lambda\ t_b}} = e^{-\lambda(t_b - t_a)},$$

где $e^{-\lambda(t_b - t_a)}$ есть безусловная вероятность безотказной работы ТУ в интервале времени $(t_b - t_a)$. Таким образом, в период нормальной эксплуатации вероятность безотказной работы в течение некоторого времени совершенно не зависит от величины наработки данного ТУ, предшествующего отрезку этого времени.

2.7. Долговечность

Время нормального функционирования всякого ТУ ограничено неизбежными изменениями свойств материалов и деталей, из которых они изготовлены. Именно поэтому долговечность определяется сроком службы и ресурсом. Срок службы определяется календарной продолжительностью эксплуатации ТУ от ее начала или возобновления после ремонта до предельного состояния (рис. 2.3).

Различаются:

– средний срок службы или математическое ожидание срока службы:

$$T_{\text{ср.сл}} = \int_0^{\infty} t_{\text{сл}\ i}\, f(t_{\text{сл}})\, dt,$$

где $t_{сл\ i}$ – срок службы i-го ТУ; $t_{сл}$ – плотность распределения срока службы;

– средний срок службы до списания $t_{ср.\ сл.\ сп}$ – это средний срок службы от начала эксплуатации ТУ до его списания;

– гамма-процентный срок службы – это срок службы, в течение которого объект не достигает предельного состояния с заданной вероятностью:

$$T_{ср.\gamma} = -\frac{1}{\lambda}\ln\frac{\gamma}{100}.$$

Кроме срока службы, долговечность ТУ характеризуется его ресурсом. Ресурсом называется наработка ТУ от начала эксплуатации или же её возобновления после ремонта до наступления предельного состояния. В отличие от определения понятия "срок службы", понятие "ресурс" оперирует не календарной продолжительностью, а общей

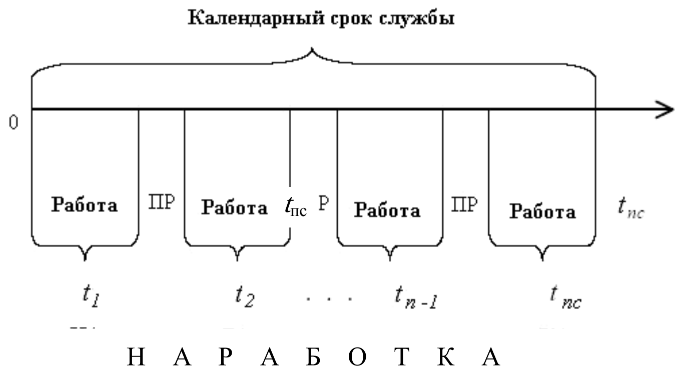


Рис. 2.3. Календарный срок службы и наработка ТУ:
ПР – профилактика; $t_{пс}$ – время наступления предельного состояния

боткой ТУ. Эта наработка в общем случае является величиной случайной. Поэтому, наряду с понятиями назначенного ресурса, долговечность оценивают средним ресурсом, гамма-процентным ресурсом и другими видами ресурсов.

Назначенный ресурс $R_н$ – это суммарная наработка ТУ, при достижении которой эксплуатация должна быть прекращена независимо

от его состояния. Средний ресурс $R_{ср}$ – математическое ожидание ресурса.

$$R_{ср} = \int_0^\infty rf(r)\,dt,$$

где r – ресурс некоторого ТУ; $f(r)$ – плотность вероятности величины r.

Гамма-процентный ресурс R_γ – наработка, в течение которой ТУ не достигает предельного состояния с заданной вероятностью γ процентов.

Гарантийный ресурс $R_г$ является понятием юридическим. Этот ресурс определяет, когда предприятие-изготовитель принимает претензии по качеству выпущенных изделий. Гарантийный ресурс совпадает с периодом приработки.

Вопросы для самоконтроля

1. Какие показатели относятся к составляющим надёжности?
2. Какой поток случайных событий называется простейшим?
3. Свойства простейшего потока и их характеристики.
4. Вероятность безотказной работы.
5. Определение вероятности безотказной работы на некотором интервале времени.
6. Что такое вероятность отказов?
7. Что такое интенсивность отказов?
8. Плотность вероятности отказов.
9. Характерные участки кривой интенсивности отказов невосстанавливаемых технических устройств.
10. Как определяется среднее время безотказной работы?
11. Основные расчётные соотношения между показателями надёжности для случая, когда $t << T$.

3. НАДЁЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Решение любой задачи, выполнение любой функции, возложенной на ЭВМ, работающей в сети или локально, возможно при взаимодействии аппаратных и программных средств. Поэтому при анализе надёжности выполнения ЭВМ заданных функций следует рассматривать единый комплекс аппаратных и программных средств [4].

По аналогии с терминами, принятыми для обозначения показателей надёжности ТУ, *под надёжностью программного обеспечения* (ПО) понимается свойство этого обеспечения выполнять заданные функции, сохраняя свои характеристики в установленных пределах при определённых условиях эксплуатации.

Надёжность ПО определяется его *безотказностью* и *восстанавливаемостью.*

Безотказность ПО – это свойство сохранять работоспособность при использовании его для обработки информации в ИС. Безотказностью программного обеспечения оценивается вероятность его работы без отказов при определённых условиях внешней среды в течение заданного периода наблюдения.

В приведённом определении под *отказом ПО* понимается недопустимое отклонение характеристик функционирования этого обеспечения от предъявляемых требований. Определённые условия внешней среды – это совокупность входных данных и состояние самой ИС. Заданный период наблюдения соответствует времени, необходимому для выполнения на ЭВМ решаемой задачи.

Безотказность ПО может характеризоваться средним временем возникновения отказов при функционировании программы. При этом предполагается, что аппаратные средства ЭВМ находятся в исправном состоянии. С точки зрения надёжности, принципиальное отличие ПО от аппаратных средств состоит в том, что программы не изнашиваются и их выход из строя из-за поломки невозможен. Следовательно, характеристики функционирования ПО зависят только от его качества, предопределяемого процессом разработки. Это означает, что безотказность ПО определяется его корректностью и зависит от наличия в нём ошибок, внесённых на этапе его создания. Кроме того, проявление ошибок ПО связано ещё и с тем, что в некоторые моменты времени на обработку могут поступать ранее не встречавшиеся совокупности данных, которые программа не в состоянии корректно обработать. Поэтому входные данные в определённой мере влияют на функционирование ПО.

В ряде случаев говорят об устойчивости функционирования ПО. Под этим термином понимается способность ПО ограничивать последствия собственных ошибок и неблагоприятных воздействий внешней среды или противостоять им. Устойчивость ПО обычно обеспечивается с помощью введения различных форм избыточности, позволяющих иметь дублирующие модули программ, альтернативные программы для одних и тех же задач, осуществлять контроль за процессом исполнения программ.

3.1. СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ ПРОГРАММНЫХ И АППАРАТНЫХ ОТКАЗОВ

Программные отказы изделия и аппаратные отказы имеют много общего, но во многом существенно различаются. Общее между ними:

а) невыполнение объектом заданных функций;

б) времена до отказов и времена устранения отказов носят случайный характер;

в) методы обработки статистических данных об отказах одинаковы, а потому статистические оценки показателей надёжности аппаратной и программной, полученные по результатам испытаний и эксплуатации, могут быть одинаковыми по своему названию: средняя наработка объекта на программный отказ, интенсивность программных отказов объекта и т.д. Возможны и объединённые (комплексные) оценки: *средняя наработка объекта на программный и аппаратный отказ* и т.п.

Вместе с тем отказы программные существенно отличаются от отказов аппаратурных:

а) отказ аппаратный зависит либо от времени, либо от объёма выполненной работы, а отказ программный – от той функции, которую выполняет изделие под управлением программы (точнее, от того, с какой вероятностью программа выйдет на такой участок, который содержит ошибку);

б) обнаружение и устранение аппаратного отказа (заменой отказавшего элемента исправным) не означает, что такой же отказ не повторится при дальнейшей работе изделия, а обнаружение и устранение отказа программного (исправление программы) означает, что такой отказ в дальнейшем не повторится;

в) программный отказ, обнаруживаемый при автономной проверке программы, может переходить в разряд недействующих, если состояние аппаратуры делает её нечувствительной к данному виду программного отказа. Например, если в программе ошибочно не предусмотрена программная защита от аппаратного сбоя, то это программный отказ, но если при этом в аппаратуре не возникает сбоя, то отказ программный становится недействующим;

г) прогнозировать возникновение аппаратных отказов сравнительно легко, а прогнозировать возникновение отдельных программных отказов трудно, а часто и невозможно. Для отдельных программных отказов трудно предвидеть время, когда они становятся действующими, а когда – недействующими;

д) аппаратные отказы целесообразно подразделять на внезапные и постепенные, т.е. отказы, различные по своей физической природе, законам распределения времени до отказа, методам борьбы за снижение их вероятности. Программные отказы нет смысла делить на внезапные и постепенные. Они возникают, как только программа переходит на такой участок, который содержит "ошибку". В то же время они по природе своей не совпадают с внезапными аппаратными отказами. Вероятность их возникновения не связана с продолжительностью работы изделия, а связана с условной вероятностью того, что программа содержит ошибку в данной части программы, и вероятностью того, что изделие будет работать под управлением этой части программы.

3.2. ОСНОВНЫЕ ПРИЧИНЫ ОТКАЗОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Основными причинами, вызывающими нарушения нормального функционирования ПО, являются:

ошибки, скрытые в самой программе;

искажение входной информации;

неверные действия пользователя;

неисправность аппаратных средств ИС, на которой реализуется вычислительный процесс.

Ошибки, скрытые в программе. При разработке сложного ПО возможно возникновение ошибок, которые не всегда удаётся обнаружить и ликвидировать в процессе отладки. В силу этого в программах остается некоторое количество скрытых ошибок. Они являются причиной неверного функционирования этих программ. Среди ошибок подобного рода можно выделить следующие характерные группы.

Ошибки вычислений. Ошибки этой группы связаны с некорректной записью или программированием математических выражений, а также неверным преобразованием типов переменных. Вследствие этого получаются неправильные результаты.

Логические ошибки. Эта группа ошибок является причиной искажения алгоритма решения задачи. К ошибкам подобного рода можно отнести неверную передачу управления, неверное задание диапазона изменения параметра цикла, неверное условие и другие ошибки.

Ошибки ввода-вывода. Эти ошибки связаны с неправильным управлением ввода-вывода, формированием выходных записей, определением размера записей и другими неправильно свершёнными действиями.

Ошибки манипулирования данными. К числу таких ошибок относятся: неверное определение числа элементов данных; неверные начальные значения, присвоенные данным; неверное указание длины операнда или имени переменной и другие ошибки.

Ошибки совместимости связаны с отсутствием совместимости разрабатываемого или применяемого ПО с операционной системой или другими прикладными программами.

Ошибки сопряжений. Группа этих ошибок вызывает неверное взаимодействие ПО с другими программами или подпрограммами, с системными программами, устройствами ЭВМ или входными данными.

Искажение входной информации. Указанная причина вызывает нарушение функционирования ПО, когда входные данные не попадают в допустимую область значения переменных. В этом случае возникает несоответствие между исходной информацией и возможностями программы.

Неверные действия пользователя связаны с неправильной интерпретацией сообщений, с неправильными действиями пользователя при работе в диалоговом режиме. Часто эти ошибки являются следствием некачественной программной документации.

Неисправность аппаратных средств ИС. Эти неисправности оказывают определённое влияние на характеристики надёжности ПО. Появление отказов или сбои в работе аппаратуры приводят к нарушению хода обработки информации и, как следствие, могут искажать как исходные данные, так и саму программу.

Следствием появления ошибок в программе является её отказ. Последствия отказов ПО можно разделить на:

– полное прекращение выполнения функций программы;
– кратковременное нарушение хода обработки информации в ИС.

Степень серьёзности последствий отказов ПО оценивается соотношением между временем восстановления программы после отказа и динамическими характеристиками объектов, использующих результаты работы этой программы.

Аварийное завершение работы прикладного ПО легко идентифицируется, так как операционная система выдаёт сообщения, содержащие аварийный код. Характерными причинами появления аварийного завершения являются ошибки при выполнении макрокоманды, неверное использование методов доступа, нарушение защиты памяти, нехватка ресурсов памяти, неверное использование макрокоманды, возникновение программных прерываний, для которых не указан обработчик, и другие причины.

3.3. ОСНОВНЫЕ ПОКАЗАТЕЛИ НАДЁЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Если рассматривать отказавшее ПО без учёта его восстановления, а также случайный характер отказов в программах, то основные показатели надёжности в этом случае не отличаются от тех, которые были рассмотрены в главе 2. При этом характер изменения этих показателей во времени будет зависеть от модели надёжности ПО.

Таким образом, основными показателями надёжности ПО являются:

– вероятность безотказной работы программы $p(t)$, представляющая собой вероятность того, что ошибки программы не проявятся в интервале времени $(0, t)$;

– вероятность отказа программы $q(t)$ или вероятность события отказа ПО до момента времени t;

– интенсивность отказов программы $\lambda(t)$;

– средняя наработка программы на отказ T, являющаяся математическим ожиданием временного интервала между последовательными отказами.

3.4. МОДЕЛИ НАДЁЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

При определении характеристик надёжности ПО учитывается тот факт, что возникающие при работе программ ошибки устраняются, количество ошибок уменьшается и, следовательно, их интенсивность понижается, а наработка на отказ программы увеличивается. В связи с такими предположениями рассматриваются несколько моделей надёжности ПО: модель с дискретно-понижающей частотой появления ошибок, модель с дискретным увеличением наработки на отказ или ошибку ПО, экспоненциальная модель надёжности ПО.

Модель с дискретно-понижающей частотой появления ошибок ПО. В этой модели предполагается, что интенсивность отказов программы $\lambda(t)$ является постоянной величиной до обнаружения возникшей ошибки и, как следствие – отказа программы и её устранения. После этого значение $\lambda(t)$ уменьшается и интенсивность отказов снова становится константой. В этой модели предполагается, что между $\lambda(t)$ и числом оставшихся в программе ошибок существует зависимость:

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

где M – неизвестное первоначальное число ошибок; i – число обнаруженных ошибок, зависящее от времени t; K – некоторая константа.

Характер изменения интенсивности отказов для этой модели представлен на рис. 3.1.

Плотность распределения времени обнаружения i-й ошибки t_i определяется соотношением

$$f\left(t_i\right) = \lambda_i e^{-\lambda_i t_i}.$$

Значения неизвестных параметров K и M могут быть оценены на основании последовательности наблюдения интервалов между моментами обнаружения ошибок.

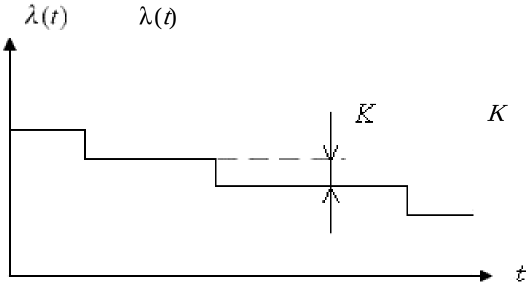


Рис. 3.1. Характер изменения интенсивности отказов программы от времени наработки при модели с дискретно-понижающей частотой появления ошибок

На практике условия рассмотренной модели нередко не соблюдаются, а именно:

– не всегда при устранении ошибки интенсивность отказов уменьшается на одну и ту же величину K, так как разные ошибки имеют различное влияние на ход исполнения программы;

– довольно часто возникают ситуации, при которых устранение одних ошибок приводит к появлению новых;

– не всегда удаётся устранить причину ошибки и программу продолжают использовать, так как при других исходных данных ошибка может себя и не проявить.

Модель с дискретным увеличением времени наработки на отказ. Основным допущением в этой модели является предположение о том, что отказы и ошибки программы в начале эксплуатации возникают часто. По мере отладки программы таких ошибок становится меньше, а время наработки на отказ после ликвидации очередного отказа увеличивается (рис. 3.2).

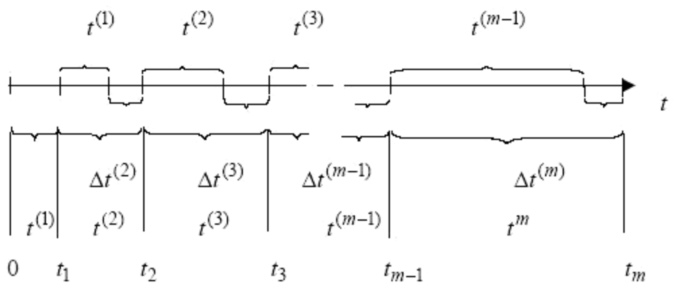


Рис. 3.2. Диаграмма интервалов времени наработки на отказ компьютерной программы

На диаграмме величины $t_1, t_2, t_3, ..., t_{m-1}, t_m$ – случайные моменты времени возникновения первого, второго, третьего и так далее – m-го отказов. Величины $t^{(1)}, t^{(2)}, t^{(3)}, ..., t^{(m-1)}, t^{(m)}$ – случайные интервалы времени между соседними отказами программы (обозначены под первым рядом нижних скобок диаграммы).

Интервалы $\Delta t^{(1)}, \Delta t^{(2)}, \Delta t^{(3)}, ..., \Delta t^{(m-1)}, \Delta t^{(m)}$ также являются случайными временными интервалами.

Пусть первая ошибка, проявившаяся в результате отказа программы, произошла в случайный момент времени t_1 и была устранена. Наработка до первого отказа и возникшей ошибки равна интервалу времени $t^{(1)}$. Вторая ошибка возникла в момент времени t_2. Наработка до второй ошибки определяется интервалом $t^{(2)}$. В соответствии с предположением, этот интервал больше, чем $t^{(1)}$, так как после перезапуска программа проработала время до первой ликвидированной ошибки, продолжила работу до новой, второй ошибки. Следовательно, интервал $t^{(2)}$ можно представить в виде

$$t^{(2)} = t^{(1)} + \Delta t^{(2)},$$

где $\Delta t^{(2)}$ – дополнение интервала $t^{(1)}$ до величины интервала $t^{(2)}$.

Обобщая эти рассуждения до любого i-го интервала $(i = \overline{1,\ m})$, можно записать:

$$t^{(i)} = t^{(i-1)} + \Delta t^{(i)}.$$

Случайные величины $\Delta t^{(i)}$ являются независимыми, имеют математическое ожидание $M[\Delta t]$ и дисперсию $\sigma^2_{\Delta t}$.

Случайное время возникновения $(i-1)$ ошибки t_i отсчитывается от начального момента времени $t_0 = 0$. Время, необходимое на ликвидацию ошибки, в расчёт не берется. В этом случае для всех случайных моментов времени возникновения ошибки и временных интервалов между соседними ошибками можно записать:

$$t_1 = t^{(1)};$$
$$t_2 = t_1 + t^{(2)} = t^{(1)} + t^{(1)} + \Delta t^{(2)};$$
$$t_3 = t_2 + t^{(3)} = t^{(1)} + t^{(2)} + t^{(3)} = t^{(1)} + t^{(1)} + \Delta t^{(2)} + t^{(1)} + \Delta t^{(2)} + \Delta t^{(3)};$$
$$\ldots$$
$$t_m = mt^{(1)} + (m-1)\Delta t^{(2)} + (m-2)\Delta t^{(3)} + \ldots + 2\Delta t^{(m-1)} + \Delta t^{(m)}.$$

Учитывая, что от момента времени $t_0 = 0$ до начала момента t_1 не выявлено ни одной ошибки программы и в силу того, что интервал $t^{(1)}$ сравнительно невелик, так как ошибки программы в начале её эксплуатации происходят довольно часто, можно представить интервал $t^{(1)}$ как $\Delta t^{(i)}$. Тогда, с учётом этой замены, выражение примет вид

$$t_m = m\Delta t^{(1)} + (m-1)\Delta t^{(2)} + (m-2)\Delta t^{(3)} + \ldots + 2\Delta t^{(m-1)} + \Delta t^{(m)}$$

или

$$t_m = \sum_{i=1}^{m} \sum_{j=1}^{i} \Delta t^{(j)} .$$

Рассмотрим выражение для $t^{(i)}$ при $i = 1$. Согласно ранее принятой замене $t^{(1)}$ на $\Delta t^{(i)}$, получим

$$t^{(1)} = t^{(0)} + \Delta t^{(1)} = \Delta t^{(1)} .$$

Действительно, интервал $t^{(0)}$ равен нулю, так как до начала эксплуатации программы никаких её отказов произойти не могло. Поэтому для любого $i = m$ при $i > 1$ можно записать:

$$t^{(m)} = \sum_{i=1}^{m} \Delta t^{(i)} .$$

Но $t^{(m)}$ – это наработка между $(m-1)$ и m-отказами. Тогда для любых m средняя наработка между $(m-1)$ и m-отказами равна математическому ожиданию интервала $t^{(m)}$:

$$t_{\text{ср}}^{(m)} = M[t^{(m)}] = M\left[\sum_{i=1}^{m} \Delta t^{(i)}\right].$$

Но для любого i

$$M[\Delta t^{(i)}] = M[\Delta t].$$

Поэтому

$$t_{\text{ср}}^{(m)} = M\left[\sum_{i=1}^{m} \Delta t^{(i)}\right] = \sum_{i=1}^{m} M[\Delta t] = mM[\Delta t] .$$

Отсюда видно, что с увеличением m увеличивается и средняя наработка между двумя отказами. Рассмотрим среднюю наработку до возникновения m-го отказа. Она равна математическому ожиданию от t_m:

$$t_{m\text{ср}} = M[t_m] = M\left[\sum_{i=1}^{m} \sum_{j=1}^{i} \Delta t^{(j)}\right] = \sum_{i=1}^{m} \sum_{j=1}^{i} M[\Delta t] = \frac{m(m+1)}{2} M[\Delta t] .$$

Как и предыдущем случае, из полученного выражения видно, что средняя наработка до отказа возрастает с увеличением числа отказов. Оценки $M[\Delta t]$ и $\sigma_{\Delta t}^2$ получаются по данным об отказах программы в течение периода наблюдения $t_{\text{н}}$:

$$\bar{M}[\Delta t] = \frac{1}{m_{\text{н}}} \sum_{i=1}^{m_{\text{н}}} \Delta t^{(i)};$$

$$\bar{\sigma}_{\Delta t}^2 = \frac{1}{(m_{\text{н}} - 1)} \sum_{i=1}^{m_{\text{н}}} \left(\Delta t^{(i)} - \bar{M}[\Delta t]\right)^2 ,$$

где $m_{\text{н}}$ – число отказов за интервал времени $(0,\ t_{\text{н}})$.

Экспоненциальная модель надёжности ПО. Основным предположением этой модели является экспоненциальный характер изменения числа ошибок в программе во времени. Прогноз надёжности программы производится на основании данных, получаемых во время её тестирования.

Основными параметрами модели являются:

τ – суммарное время функционирования от начала тестирования (с устранением обнаруженных ошибок) до момента оценки надёжности;

M – число ошибок, имеющихся в программе перед началом тестирования;

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

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

Предполагается, что число ошибок в программе в каждый момент времени имеет пуассоновское распределение, а временной интервал между двумя ошибками распределён по экспоненциальному закону. Параметр этого распределения изменяется после распределения очередной ошибки. Интенсивность отказов считается непрерывной функцией, пропорциональной числу оставшихся ошибок. С учётом введенных параметров и предположений

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

а интенсивность ошибок

$$\lambda(\tau) = Cm_0(\tau),$$

где C – коэффициент пропорциональности, учитывающий быстродействие ЭВМ и число команд в программе.

Пусть в процессе исправления ошибок новые ошибки не появляются. Следовательно, интенсивность исправления ошибок будет равна интенсивности их обнаружения:

$$\frac{dm(\tau)}{d\tau} = \lambda(\tau).$$

Совместное решение полученных выражений даёт:

$$\frac{dm(\tau)}{d\tau} + Cm(\tau) = CM.$$

Решением этого уравнения является выражение

$$m(\tau) = M\left[1 - \exp(-C\tau)\right].$$

Будем характеризовать надёжность программы после тестирования в течение времени τ средним временем наработки на отказ:

$$T_0 = \frac{1}{\lambda(\tau)}.$$

Следовательно,

$$T_0 = \frac{1}{CM}\exp(C\tau).$$

Введем величину T_{0m} – исходное значение среднего времени наработки на отказ перед тестированием, которое равно

$$T_{0m} = \frac{1}{CM}.$$

Подставляя это значение в выражение T_0, получим:

$$T_0 = T_{0m}\exp\left(\frac{\tau}{MT_{0m}}\right).$$

Из этого выражения видно, что среднее время наработки на отказ увеличивается по мере выявления и исправления ошибок.

Таким образом, аналитические модели надёжности дают возможность исследовать закономерности проявления ошибок в программе и прогнозировать надёжность при её разработке и эксплуатации.

Вопросы для самоконтроля

1. Что понимается под термином "надёжность программного обеспечения"?
2. Что понимается под терминами "безотказность ПО" и "отказ ПО"?
3. Чем отличаются программные и аппаратурные отказы?
4. Основные причины отказов ПО.
5. Модель с дискретно-понижающей частотой появления ошибок ПО.
6. Модель с дискретным увеличением времени наработки на отказ.
7. Экспоненциальная модель надёжности ПО.

4. НАДЁЖНОСТЬ НЕВОССТАНАВЛИВАЕМЫХ ТЕХНИЧЕСКИХ УСТРОЙСТВ В ПРОЦЕССЕ ИХ ЭКСПЛУАТАЦИИ

4.1. ХАРАКТЕРИСТИКИ НАДЁЖНОСТИ НА РАЗЛИЧНЫХ ЭТАПАХ ЭКСПЛУАТАЦИИ

В предыдущих рассуждениях было принято допущение о том, что поток отказов невосстанавливаемых ТУ подчиняется закону Пуассона, т.е. закон распределения времени до отказа является экспоненциальным. Практика показала, что эти допущения правомерны более чем для 60% таких ТУ. Рассмотрим интенсивность отказов по периодам эксплуатации (рис. 4.1).

Из рисунка видно, что в любой момент времени $t < t_{\text{пр}}$ суммарная интенсивность отказов периода приработки $\lambda_{\Sigma\text{пр}}(t)$ будет равна

$\lambda_{\Sigma\text{пр}}(t) = \lambda + \lambda_{\text{пр}}(t)$.

Отсюда вероятность безотказной работы в этот период будет равна

$$P_{\text{пр}}(t) = e^{-\int_0^t (\lambda + \lambda_{\text{пр}}(t))dt} = e^{-\int_0^t \lambda_{\text{пр}}(t)dt} e^{-\lambda t}.$$

Аналогичным образом можно получить выражение для вероятности безотказной работы в период износа и старения. В этом случае для $t > t_{\text{н}}$ суммарная интенсивность постепенных отказов периода износа и старения $\lambda_{\Sigma\text{ис}}(t)$ определяется выражением

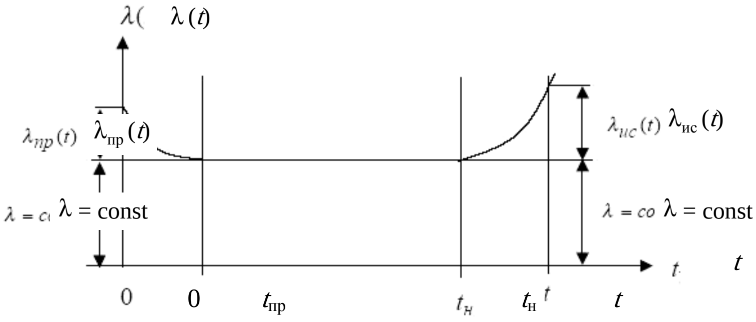


Рис. 4.1. Кривая интенсивностей отказов по периодам эксплуатации:
$t_{\text{пр}}$ – время окончания периода приработки; $t_{\text{н}}$ – время окончания периода нормальной эксплуатации;
t – некоторый текущий момент времени;
$\lambda_{\text{пр}}(t)$ – интенсивность отказов в период приработки;
λ – интенсивность отказов при нормальной эксплуатации;
$\lambda_{\text{ис}}(t)$ – интенсивность постепенных отказов в период износа и старения

$\lambda_{\Sigma\text{ис}}(t) = \lambda + \lambda_{\text{ис}}(t)$,

откуда можно определить вероятность безотказной работы при постепенных отказах:

$$P_{\text{ис}}(t) = e^{-\int_0^t \lambda_{\Sigma\text{ис}}(t)dt} = e^{-\int_0^t (\lambda + \lambda_{\text{ис}}(t))dt} = e^{-\int_0^t \lambda_{\text{ис}}(t)dt} e^{-\lambda t}.$$

Интенсивность отказов в зависимости от типа, назначения, качества, нагрузочных режимов и режимов эксплуатации может иметь разнообразный характер, её кривая – различные формы. Представим эту зависимость в общем виде:

$$\lambda(t) = \lambda + \lambda_1 t^n,$$

где λ – интенсивность отказов в период нормальной эксплуатации; λ_1 – параметр масштаба интенсивности отказов; n – параметр формы интенсивности отказов.

Подставим полученное выражение интенсивности в левую часть обобщённого закона надёжности в дифференциальной форме:

$$(\lambda + \lambda_1(t)) = -\frac{p'(t)}{p(t)},$$

и проинтегрируем уравнение от 0 до t. В результате вероятность безотказной работы будет определяться общим выражением:

$$p(t) = e^{-\lambda t} e^{-\frac{\lambda_1}{n+1} t^{n+1}}.$$

Второй сомножитель в левой части выражения определяет вероятность с переменной во времени интенсивностью и представляет собой распределение Вейбулла. Вид распределения Вейбулла зависит от показателя n (рис. 4.2).

В таблице представлены величины интенсивно

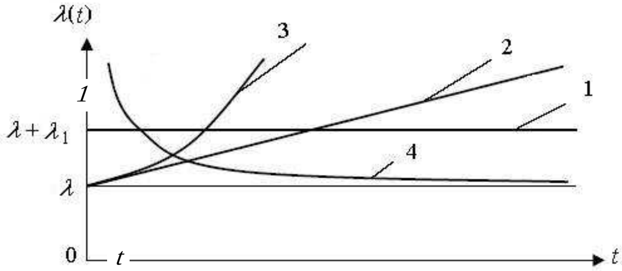


Рис. 4.2. График изменения интенсивности отказов в зависимости от показателя *n*

Значение *n*	Зависимость	Кривая на рис. 4.2
0	$\lambda(t) = \lambda + \lambda_1$	1
1	$\lambda(t) = \lambda + \lambda_1 t$	2
Больше 1	$\lambda(t) = \lambda + \lambda_1 t^n$	3
Меньше 1	$\lambda(t) = \lambda + \lambda_1 \dfrac{1}{t^n}$	4

стей отказов. Для конкретных задач определения надёжности при внезапных и постепенных отказах выбираются необходимые зависимости $\lambda(t)$. При этом выбор значения показателя n производится, исходя из следующих возможностей: результатов специальных испытаний ТУ на надёжность, накопленных данных об отказах этих ТУ при различных режимах работы в процессе эксплуатации и справочных материалов об интенсивностях отказов.

Надёжность в период износа и старения. В период износа и старения развиваются постепенные отказы. Для этих отказов характерно то, что для них нельзя указать определённые границы времени начала и конца их появления. Времена наступления постепенных отказов имеют тенденцию группироваться вокруг среднего времени безотказной работы T', определяемого из условия появления только износовых отказов.

Распределение времени безотказной работы до появления износового отказа во многих случаях хорошо описывается нормальным законом распределения.

Тогда

$$f(t) = \begin{cases} 0 & , \quad t \le 0; \\ ce^{-(t-T')^2/2\sigma^2} & , \quad t > 0, \end{cases}$$

где $c = \dfrac{1}{\sigma\sqrt{2\pi}}$ – нормирующий множитель; t – текущее время работы ТУ с момента ввода его в эксплуатацию; σ – среднее квадратическое отклонение времени безотказной работы T'.

Для определения безусловной вероятности отказа ТУ в интервале времени (t_1, t_2) воспользуемся формулой

$$q(t_1, t_2) = \int_{t_1}^{t_2} f(t)\,dt = \frac{1}{\sigma\sqrt{2\pi}} \int_{t_1}^{t_2} e^{-(t-T')^2/2\sigma^2}\, dt.$$

Применим замену переменной:

$$\frac{(t-T')}{\sigma} = z; \quad dz = \frac{dt}{\sigma}.$$

Величина z центрирована относительно T', т.е. $z = 0$ при $t = T'$. Тогда, делая соответствующую подстановку, получим

$$q(t_1, t_2) = \frac{1}{\sqrt{2\pi}} \int_0^{\frac{t_2-T'}{\sigma}} e^{-\frac{z^2}{2}} dz - \int_0^{\frac{t_1-T'}{\sigma}} e^{-\frac{z^2}{2}} dz.$$

Полученные интегралы в правой части можно вычислить с помощью специальной функции, представляющей собой определённый интеграл от выражения $e^{-z/2}$. Эта функция называется функцией Лапласа, обозначается символами $\Phi(x)$ и для неё составлены таблицы. Функция Лапласа равна

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{z^2}{2}} dz.$$

В силу замены $\dfrac{(t-T')}{\sigma}$ получим

$$q(t_1,\, t_2) = \Phi\left(\frac{t_2 - T'}{\sigma}\right) - \Phi\left(\frac{t_1 - T'}{\sigma}\right).$$

Графики функций $q(t)$ и $\Phi\left(\dfrac{t-T'}{\sigma}\right)$ показаны на рис. 4.3. Так как $\Phi\left(\dfrac{t-T'}{\sigma}\right)$ является законом распределения времени до отказа, а $q(t) = p\,(t < T')$ по определению является также законом распределения времени до отказа, то эти законы совпадают и приведены на рисунке одним графиком.

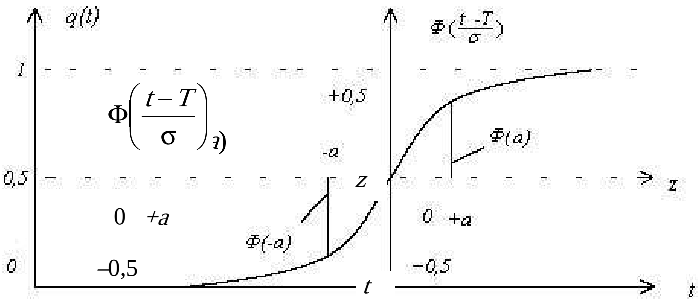


Рис. 4.3. График функции распределения времени до отказа

Если через ординату $\Phi\left(\dfrac{t-T'}{\sigma}\right) = 0,5$ провести прямую, параллельную оси абсцисс z, а затем принять её за новую ось абсцисс z, то видно, что в новой системе координат значения функции $\Phi\left(\dfrac{t-T'}{\sigma}\right)$ в точках, равностоящих от новой оси ординат, равны по абсолютной величине:

$$\left|\Phi(a)\right| = \left|\Phi(-a)\right|.$$

Это вдвое сокращает объём табличного материала для функции $\Phi\left(\dfrac{t-T'}{\sigma}\right)$. Следует иметь в виду, что при работе с отрицательными аргументами справедливо следующее соотношение:

$$\Phi(-a) = -\Phi(a).$$

Если предположить, что $t_1 = 0$, где t_1 – время начала износа старения, и при условии, что $T' >> \sigma$, с известной долей приближения можно записать

$$\Phi\left(\frac{t_1 - T'}{\sigma}\right) = \Phi\left(-\frac{T'}{\sigma}\right) \cong -0,5.$$

Тогда

$$q(t) = \Phi\left(\frac{t-T'}{\sigma}\right) - (-0,5) = 0,5 + \Phi\left(\frac{t-T'}{\sigma}\right).$$

В силу того, что вероятность безотказной работы $p(t_1,\, t_2)$ может быть вычислена по формуле

$$p(t) = 1 - q(t)$$

с учётом полученного выражения для вероятности отказов, можно записать:

$$p(t) = 0,5 - \Phi\left(\frac{t-T'}{\sigma}\right).$$

Тогда общая вероятность безотказной работы ТУ с учётом внезапных и постепенных отказов в период износа и старения будет определяться следующим выражением:

$$p_{\text{ис}}(t) = p(t)\cdot p(t_n) = e^{-\lambda t_e}\left(0,5 - \Phi\left(\frac{t_n - T'}{\sigma}\right)\right),$$

где $p_n(t)$ – вероятность безотказной работы ТУ в период износа и старения.

Вероятность отказа ТУ в период износа и старения увеличивается со временем. Если функция интенсивности отказов $\lambda(t)$ для этого периода известна, то при определении условной вероятности безотказной работы за промежуток времени $\Delta t = t_2 - t_1$ можно воспользоваться формулой

$$p\left(\frac{t_1,\ t_2}{t_1}\right) = p(t_1,\ t_2) = e^{-\int_{t_1}^{t_2} \lambda(t)\, dt}.$$

Поскольку в период износа и старения интенсивность отказов непрерывно увеличивается, величина $p\left(\frac{t_1,\ t_2}{t_1}\right)$ для одинаковых по продолжительности отрезков времени будет различной в зависимости от того, к какому моменту времени общего срока эксплуатации примыкает рассматриваемый отрезок времени. Отсюда следует, что в этот период надёжность ТУ как свойство выполнять заданные функции в пределах требуемого промежутка времени Δt зависит от возраста ТУ или его наработки к началу рассматриваемого отрезка времени.

Существует ряд мероприятий по профилактике износа ТУ. Основным из них является соблюдение правил эксплуатации. Это позволяет избежать преждевременного износа и сокращения периода нормальной эксплуатации. Важную роль играет и система технического обслуживания ТУ, включающая настройку, регулировку и другие мероприятия. Не менее важным способом предотвращения отказов по причине износа является замена устройств до наступления периода износа и старения. Наиболее широко этот способ применяется для обеспечения необходимого уровня надёжности и безотказности ТУ, выполняющих ответственные функции, особенно если они связаны с риском для жизни людей.

Надёжность технических устройств в период хранения.

В главе 2 было дано определение понятия сохраняемости. Эта составляющая надёжности характеризует свойство ТУ противостоять вредным воздействиям среды при их хранении и транспортировке.

В понятии сохраняемости следует различать две стороны. Одна из них связана с надёжностью ТУ в процессе их хранения на складах. Здесь используются такие показатели, как интенсивность отказов при хранении, среднее время безотказного хранения (средний срок сохраняемости) и другие характеристики. Другая сторона понятия сохраняемости характеризует способность ТУ противостоять отрицательному влиянию условий хранения и транспортировки на его безотказность при последующей эксплуатации в рабочих режимах. В этом случае сохраняемость характеризуется некоторым сроком хранения в определенных условиях с соответствующим техническим обслуживанием.

В течение этого срока уменьшение средней наработки до отказа, обусловленное хранением, должно находиться в допустимых пределах, оговоренных нормативно-технической документацией. В качестве основных количественных показателей сохраняемости используются:

– срок сохраняемости – календарная продолжительность хранения или транспортировки ТУ, в течение которого сохраняются в заданных пределах значения параметров, характеризующих способность ТУ выполнять заданные функции;

– средний срок сохраняемости $T_{\text{сохр. ср}}$. Эта величина является математическим ожиданием срока сохраняемости:

$$T_{\text{сохр. ср}} = \int_0^{\infty} t_{\text{сохр}\ i}\, f\left(t_{\text{сохр}}\right) dt,$$

где $t_{\text{сохр}\ i}$ – сохраняемость i-го ТУ; $f(t_{\text{сохр}})$ – плотность распределения величины $t_{\text{сохр}}$;

– гамма-процентный срок сохраняемости $T_{\text{сохр}\,\gamma}$ – срок сохраняемости, который будет достигнут ТУ с заданной вероятностью γ процентов.

Срок сохраняемости в теории надёжности рассматривается как случайная величина.

4.2. ХАРАКТЕРИСТИКИ НАДЁЖНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРИ ХРАНЕНИИ ИНФОРМАЦИИ

Хранение информации в ИС производится как на программном, так и на аппаратном уровне. Если говорить о программном уровне, то в качестве информационных хранилищ могут рассматриваться базы и банки данных и знаний. Поскольку и те и другие являются программными продуктами, то они обладают теми же свойствами и характеристиками, что и программное обеспечение вообще. Если говорить об аппаратном уровне, то основным аппаратным средством, предназначенным для хранения информации, является память компьютера. Она имеет иерархическую организацию и состоит из верхней памяти, внешней памяти и съемных хранилищ. Верхняя память состоит из регистров процессора, составляющих внутреннюю память процессора, кэш-памяти, разделяемой в современных ЭВМ на два уровня, и оперативной памяти, реализованной в настоящее время чаще всего на базе микросхем динамической памяти с произвольным доступом. К внешней памяти относится жёсткий фиксированный магнитный диск (винчестер). Съёмные хранилища представляют собой внешние накопители на магнитной ленте, магнитооптические диски и другие виды носителей.

Верхняя память предназначена для кратковременного хранения информации в процессе выполнения компьютером программы. Оперативная память в современных компьютерах является полупроводниковым устройством. Модули оперативной памяти изготавливаются на основе интегральной технологии.

В процессе работы этих устройств возникают ошибки, которые разделяются на *неустранимые* и *корректируемые*.

Причинами неустранимых ошибок являются дефекты физического характера. Они заключаются в том, что некоторые элементы микросхем перестают изменять состояние при записи, вследствие чего считываемый с них код не соответствует переданному при записи. Неустранимые ошибки являются следствием дефектов производственного характера, старения или условий эксплуатации.

Корректируемые ошибки носят случайный характер и не являются результатом неисправности модуля. Они вызываются причинами, начиная от воздействия помех в цепях питания, внешней радиации и кончая температурной нестабильностью в работе микросхем.

Оба этих типа ошибок представляют серьёзную опасность, как во время работы программы, так и при хранении информации. Поэтому в компьютерах предусмотрены схемы выявления и коррекции ошибок. Модули оперативной памяти относятся к невосстанавливаемым элементам ИС и потому показатели надёжности для них аналогичны тем, которые описаны в главе 2. При этом следует иметь в виду, что надёжность современных модулей памяти весьма высока – среднее время наработки на отказ (среднее время безотказной работы) составляет сотни тысяч часов.

Регистровая кэш-память представляет собой буфер между оперативной памятью и центральным процессором компьютера. Она обладает высокой скоростью передачи данных и сравнительно небольшим объёмом. В кэш-памяти кратковременно хранятся копии блоков данных тех областей оперативной памяти, к которым выполнялись последние обращения, и весьма вероятны обращения в ближайшие такты работы. Создается кэш-память на основе тех же технологий, что и оперативная память. Поэтому особенности её работы и характеристики надёжности соответствуют тем, которыми обладает оперативная память.

В современных ЭВМ внешняя память представлена накопителями на жестких магнитных дисках (винчестерах). Магнитный диск представляет собой пластину круглой формы из немагнитного металла или пластика, покрытую слоем магнитного материала. Данные записываются на носитель и считываются с него с помощью магнитной головки, являющейся миниатюрным электромагнитом. Винчестеры предназначены для долговременного хранения информации как во время работы компьютера, так и в периоды его отключения. Отдельные элементы винчестера (диск, магнитная головка) можно считать функционально независимыми с точки зрения хранения информации, так как состояние магнитной головки не может оказать влияние на качество уже записанной на диск информации. Поэтому речь будет идти именно о дисковой части винчестера как невосстанавливаемом элементе ИС, отказы которых представляют собой наибольшую опасность для хранимой на них информации.

Практика их эксплуатации показывает, что среднее время наработки на отказ для винчестеров растёт и для ряда моделей в настоящий момент достигает значения 1 200 000 ч. Оценим этот показатель. Для этого введём некоторые допущения. Пусть оцениваемые нами винчестеры находятся в периоде нормальной эксплуатации. Все винчестеры принадлежат к одной серии и введены в эксплуатацию одновременно. Установим режим работы – 24 часа в сутки в течение всего года. Кроме того, будем предполагать, что винчестеры поставлены на эксплуатацию после прохождения периода приработки. Это означает, что отказы, связанные с дефектами проектирования, монтажа, изготовления, не учитываются. Допущение о круглосуточной работе даёт основание предполагать, что остановки накопителей информации будут связаны с отключением электроэнергии, бросками тока и напряжения. С одной стороны, эти остановки приводят к ускоренному износу оборудования, а с другой – постоянная работа винчестера будет причиной достаточно быстрого износа механических элементов диска. Будем также считать, что любой отказ винчестера связан с полной или частичной потерей или искажением записанной информации.

В силу принятых допущений будем считать, что средняя наработка винчестера на отказ будет $T = 60\,000$ ч, что вполне соответствует показателям для дисков, установленных на современных компьютерах. Тогда для периода нормальной эксплуатации интенсивность отказов будет равна:

$$\lambda = \frac{1}{T} = 0{,}000016(6)\frac{1}{\text{ч}} \approx 0{,}000017\frac{1}{\text{ч}}.$$

Определим величину вероятности безотказной работы поставленных на эксплуатацию винчестеров через год, два, три, четыре и пять. Пусть на восстановление информации по отказам жёстких дисков тратится 10% годового бюджета времени. Тогда количество рабочих дней $t_{\text{р. д}}$ будет равно: $t_{\text{р. д}} = 365 - 36{,}5 = 328{,}5$ (рабочих дней), или в часах: $t_{\text{ч}}(1) = 328{,}5 \cdot 24 = 7884$ (ч), где $t_{\text{ч}}(1)$ – количество часов работы винчестера в год. Тогда вероятности безотказной работы этих устройств $P(i)$, где $i = 1, 2, 3, 4, 5$ – количество лет работы, будут равны:

$$p(1) = e^{-\lambda t_{\text{ч}}(1)} = e^{-0{,}000017 \times 7884} = 0{,}875;$$

$$p(2) = e^{-\lambda t_{\text{ч}}(2)} = 0{,}764;$$

$$p(3) = e^{-\lambda t_{\text{ч}}(3)} = 0{,}669;$$

$$p(4) = e^{-\lambda t_{\text{ч}}(4)} = 0{,}571;$$

$$p(5) = e^{-\lambda t_{\text{ч}}(5)} = 0{,}504.$$

Полученные результаты говорят о том, что в среднем следует ожидать через год отказа около 13% винчестеров, через 2 года – около 24%, через 3 года – более 33%, через 4 – около 43% и через 5 лет откажет почти половина поставленных на эксплуатацию жёстких дисков.

Можно предполагать, что чем дольше диск работает, тем более ценная информация на нём хранится. Поэтому ущерб, наносимый при выходе винчестера из строя через 5 лет, будет более ощутим, чем при его отказе через год. Следовательно, при эксплуатации компьютеров чрезвычайно важными являются мероприятия, связанные с обеспечением сохранности информации. Прежде всего, к ним необходимо отнести работы по созданию и поддержанию стабильного электропитания и необходимого микроклимата. Затем необходимо создать системы антивирусной защиты и профилактики. И, наконец, необходимо обеспечить сохранность информации путём применения систем резервного копирования.

Вопросы для самоконтроля

1. Охарактеризовать интенсивности отказов ТУ в различные периоды эксплуатации.
2. Основные количественные показатели сохраняемости.
3. Каким законом может быть описано распределение времени безотказной работы в период износа и старения?

4. Как определяется общая вероятность безотказной работы ТУ с учётом внезапных и постепенных отказов?
5. Устройства информационных систем, являющиеся основными хранилищами информации?
6. Основные показатели надёжности при хранении информации.
7. Основные мероприятия по обеспечению надёжности аппаратных средств.

5. НАДЁЖНОСТЬ ВОССТАНАВЛИВАЕМЫХ ТЕХНИЧЕСКИХ УСТРОЙСТВ

5.1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ТЕОРИИ ВОССТАНОВЛЕНИЯ

К *восстанавливаемым* ТУ относятся такие ТУ, ремонт которых в случае отказов или выработки ими предусмотренного срока эксплуатации производится в соответствии с заданной технологией и в необходимом объёме. После эксплуатация ТУ возобновляется до его предельного состояния или следующего ремонта.

Восстанавливаемые ТУ в общем случае представляют собой сложные системы, состоящие из высоконадёжных элементов, отказы которых являются независимыми. Для таких систем появление отказов на одном интервале наработки практически не влияет на вероятность появления какого-либо количества отказов на другом интервале, не пересекающемся с первым. В этом случае отказы можно считать независимыми, а время наработки между отказами распределённым по экспоненциальному закону.

Восстановление устройства после отказа производят путём замены неисправного элемента или путём его ремонта. При этом в теории надёжности не учитывают время, необходимое на восстановление. Предполагается, что возникающие отказы ТУ устраняются мгновенно. Это – так называемая модель мгновенного восстановления работоспособности ТУ. При рассмотрении характеристик надёжности восстанавливаемых ТУ считается, что восстановление полностью возвращает устройству те же свойства, которыми оно обладало до отказа так, что его невозможно отличить от нового. При таком допущении продолжительность работы ТУ с момента его восстановления до очередного отказа не зависит от того, сколько раз оно отказывало в прошлом.

Одной из основных характеристик восстанавливаемых ТУ является *ремонтопригодность* или *восстанавливаемость*. Численной мерой восстанавливаемости является вероятность восстановления, под которой понимается вероятность того, что за определённый интервал времени и в заданных условиях ремонта неисправное ТУ будет восстановлено:

$$p\left(t_{\text{рем}}\right) = p\left(t_{\text{ф}} < t_{\text{рем}}\right),$$

где $t_{\text{ф}}$ – фактическое время восстановления; $t_{\text{рем}}$ – заданное время процесса восстановления. В процессе эксплуатации сложные восстанавливаемые ТУ в любой момент времени, принятый за начало отсчёта времени эксплуатации, могут находиться в одном из двух состояний: исправном или неисправном. Исправное состояние восстанавливаемого ТУ в течение некоторого периода рабочего времени $(t-\tau)$ определяется следующими двумя необходимыми условиями:

– наличием исправного состояния в любой данный момент времени t, принятый за начало отсчёта;
– непоявлением отказа в полуинтервале времени $(t-\tau)$, исключая момент t.

В силу сказанного, количественная мера надёжности определяется как эксплуатационная надёжность, представляющая собой функцию эксплуатационной надёжности или вероятность исправного состояния ТУ в течение интервала $(t-\tau)$:

$$p_{\text{э}}(\tau) = p_0(t)\, p(\tau).$$

Это выражение определяется произведением вероятности исправного состояния $P_0(t)$ в любой момент времени $t < \tau$ и вероятности непоявления отказа ТУ $p(\tau)$ в течение интервала от момента t до τ, исключая сам момент t.

Первый сомножитель равен

$$p_0(t) = \frac{N(t)}{N},$$

где N – некоторое постоянное количество восстанавливаемых ТУ, находящихся под наблюдением; $N(t)$ – количество восстанавливаемых ТУ, находящихся к моменту времени t в исправном состоянии.

Аналогично определяется и вероятность отказа в любой момент времени $t < \tau$:

$$q_0(t) = \frac{N - N(t)}{N} = \frac{n(t)}{N}.$$

Очевидно, что

$$p_0(t) + q_0(t) = 1.$$

Если предположить, что t меняется от 0 до τ (а это корректное предположение, так как по принятому условию момент времени t принят за начало отсчёта), то второй сомножитель эксплуатационной надёжности

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

Последовательности событий, состоящие в возникновении отказов в случайные моменты времени t_1, t_2, t_3, ..., t_n, образуют поток событий или поток отказов. Тогда в качестве характеристик надёжности восстанавливаемых ТУ можно принять характеристики потока отказов. Основными характеристиками потока отказов являются средняя статистическая плотность вероятности отказов или параметр потока отказов и суммарная статистическая плотность вероятности отказов.

Средняя статистическая плотность вероятности отказов или параметр потока отказов определяется как отношение количества отказавших ТУ Δn_i в интервале времени Δt_i к числу ТУ $N_э$, находящихся в эксплуатации, при условии, что все отказавшие ТУ мгновенно восстанавливаются или заменяются исправными:

$$\omega_i = \frac{\Delta n_i}{N_э \Delta t_i}.$$

Суммарная статистическая плотность вероятности отказов выражается отношением полного числа отказов $n(t)$ ко времени эксплуатации t:

$$\Omega = \frac{n(t)}{t}.$$

Одним из важных показателей в теории восстановления является среднее время наработки между двумя отказами $T_{м.\,о}$. Оно определяется как отношение времени наработки t ТУ к полному числу отказов ТУ, возникших в нём за это время:

$$T_{м.о} = \frac{t}{n(t)} \text{ или } T_{м.о} = \frac{1}{\Omega}.$$

Известно, что для любого закона распределения времени безотказной работы ТУ значение средней плотности вероятности отказов $\omega(t)$ для восстанавливаемых устройств в установившемся режиме их работы при $t \to \infty$ имеет предел:

$$\lim_{t\to\infty} \omega(t) = \frac{1}{T} = \text{const} = \lambda,$$

где λ – интенсивность отказов; T – среднее время безотказной работы.

5.2. КОЭФФИЦИЕНТЫ ОТКАЗОВ

Иногда в качестве вспомогательного критерия надёжности элементов восстанавливаемых ТУ применяются различные коэффициенты, в частности – коэффициент отказов. Коэффициент отказов представляет собой отношение числа отказов однотипных элементов $n_э$ к общему числу отказов в системе $n_с$:

$$k_о = \frac{n_э}{n_с}.$$

Величина этого коэффициента позволяет оценить степень влияния определённого типа элемента на надёжность системы в целом. Однако он не даёт возможности определить, какой тип элементов системы менее надёжен, а какой более надёжен. Для этой цели может быть использован относительный коэффициент отказов:

$$k_{о.о} = \frac{n_э N_с}{n_с N_э},$$

где $N_э$ – количество элементов определённого типа в системе; $N_с$ – полное количество элементов всех типов в системе.

Эти коэффициенты могут быть выражены через другие показатели надёжности. Так, количество отказов в системе вследствие неисправных элементов определённого типа в течение промежутка времени Δt можно определить с помощью выражения

$$n_э = N_э \omega_э \Delta t,$$

где $\omega_э$ – средняя плотность вероятности отказов элементов определённого типа. За это же время в системе произойдёт всего отказов:

$$n_с = \Omega_с \Delta t,$$

где $\Omega_с$ – суммарная плотность вероятности отказов в системе.

Подставим полученные значения в выражение коэффициента отказов

$$k_о = \frac{N_э \omega_э \Delta t}{\Omega_с \Delta t} = N_э \frac{\omega_э}{\Omega_с}.$$

При $\Delta \to \infty$ предельное значение средней плотности вероятности элементов определённого типа будет равно $\omega_э = \lambda_э$. Следовательно,

$$k_{\text{о}} = N_{\text{э}} \frac{\lambda_{\text{э}}}{\Omega_{\text{с}}}.$$

Аналогично можно найти зависимость относительного коэффициента отказов от средней и суммарной плотности вероятности отказов:

$$k_{\text{о.о}} = \frac{n_{\text{э}} N_{\text{с}}}{n_{\text{с}} N_{\text{э}}} = \frac{\omega_{\text{э}} N_{\text{э}} N_{\text{с}} \Delta t}{\Omega_{\text{с}} N_{\text{э}} \Delta t} = N_{\text{с}} \frac{\omega_{\text{э}}}{\Omega_{\text{с}}}.$$

В предельном случае $\omega_{\text{э}} = \lambda_{\text{э}}$ будет получено значение $k_{\text{о.о}} = N_{\text{с}} \frac{\lambda_{\text{э}}}{\Omega_{\text{с}}}$. Таким образом, коэффициенты отказов могут быть выражены через интенсивность отказов и суммарную плотность вероятности отказов.

5.3. КОМПЛЕКСНЫЕ ПОКАЗАТЕЛИ НАДЁЖНОСТИ

Процесс эксплуатации сложных восстанавливаемых ТУ не следует рассматривать как непрерывный процесс. Обычно функциональное использование их чередуется с *простоем* вследствие двух основных причин:

– бездействие исправных ТУ ввиду отсутствия необходимости их применения или наличия причин и условий, препятствующих их эксплуатации, в результате образуется так называемый конъюнктурный простой;

– проведение мероприятий, связанных с профилактикой и текущим ремонтом, в результате чего образуется вынужденный простой.

Поэтому текущее время эксплуатации ТУ складывается из следующих компонентов:

$$t_{\text{э}} = t_{\Sigma} + t_{\text{в.п}} + t_{\text{к.п}},$$

где t_{Σ} – суммарное время наработки ТУ в течение определённого календарного времени эксплуатации $t_{\text{э}}$; $t_{\text{в. п}}$ – суммарное время вынужденного простоя (по отказам и плановым профилактикам и восстановлению после них) за этот же период эксплуатации; $t_{\text{к. п}}$ – суммарное время конъюнктурного простоя за этот же период. Здесь под конъюнктурным простоем понимается бездействие исправного ТУ ввиду отсутствия необходимости применения.

Время вынужденного простоя $t_{\text{в. п}}$ представляет собой сумму $t_{\text{в. п}} = t_{\text{пл}} + t_{\text{нпл}}$, где $t_{\text{пл}}$ – плановое время вынужденного простоя, которое образуется вследствие проведения плановых профилактик. Эта величина вполне определена и практически пропорциональна времени эксплуатации; $t_{\text{нпл}}$ – неплановое время вынужденного простоя из-за восстановления по отказам. Это величина случайная и определяется временем $t_{\Sigma p}$, необходимым для восстановления по всем отказам за определённый календарный период.

Одним из важнейших критериев надёжности является *готовность ТУ быть эксплуатируемым* (или готовность к применению), которая выражается коэффициентом эксплуатационной готовности:

$$K_{\text{э.г}} = \frac{t_{\Sigma}}{t_{\Sigma} + t_{\text{в.п}}}.$$

Величина этого коэффициента зависит не только от надёжности, но и от эксплуатационного совершенства, характеризующего степень приспособленности ТУ к проведению профилактических работ. Ввиду того, что плановое время вынужденного простоя не является случайной величиной и значение его отношения к наработке не зависит от количества возникающих отказов, то можно определить величину, выражающую собой вероятность того, что ТУ в любой момент времени может находиться в исправном состоянии. Эта величина носит название *коэффициента готовности* и выражается как

$$K_{\text{г}} = \frac{t_{\Sigma}}{t_{\Sigma} + t_{\Sigma p}}.$$

На практике важен такой показатель, как степень использования ТУ в эксплуатации за календарное время $t_{\text{э}}$. Определяется эта величина как коэффициент использования:

$$K_{\text{ис}} = \frac{t_{\Sigma}}{t_{\text{э}}}.$$

Коэффициент использования численно равен вероятности того, что в любой момент времени $t_{\text{э}}$ ТУ выполняет свои предписанные функции. В рассмотренном ранее коэффициенте готовности

$$K_{\text{г}} = \frac{t_{\Sigma}}{t_{\Sigma} + t_{\Sigma p}}$$

величины t_Σ и $t_{\Sigma p}$ могут быть получены из выражений:

$$t_{\Sigma p} = n(t_\Sigma)\,T_p,$$
$$t_\Sigma = n(t_\Sigma)\,T_{\text{м.о}},$$

где T_p – среднее время восстановления ТУ; $T_{\text{м. о}}$ – среднее время наработки между двумя отказами.

Тогда, после подстановки этих значений в исходную формулу коэффициента готовности, получим

$$K_{\text{г}} = \frac{T_{\text{м.о}}}{T_{\text{м.о}} + T_p}.$$

При $t \to \infty$ предельное значение среднего времени наработки между двумя отказами будет равно

$$\lim_{t\to\infty} T_{\text{м.о}} = T.$$

Подставляя это значение в выражение коэффициента готовности, получим

$$K_{\text{г}} = \frac{T}{T + T_p}.$$

С учётом того, что

$$T_{\text{м.о}} = \frac{1}{\Omega},$$

последнее выражение можно записать в виде

$$K_{\text{г}} = \frac{1}{1 + \Omega T_p}.$$

Для сложных информационных систем понятие надёжности в большей степени определяется по коэффициенту готовности $K_{\text{г}}$, т.е. по вероятности того, что ИС в любой момент времени находится в исправном состоянии. Для типичного современного сервера $K_{\text{г}}$ = 0,99. Это означает примерно 3,5 суток простоя в год. За рубежом популярной является классификация ИС по уровню надёжности.

Коэффициент готовности $K_{\text{г}}$	Максимальное время простоя в год	Тип ИС
0,99	3,5 сут	Обычная
0,999	8,5 ч	Высокая надёжность
0,9999	1 ч	Отказоустойчивая
0,99999	5 мин	Безотказная

Необходимо отметить и другие качества надёжности функционирования ИС. Так, одним из важнейших комплексных показателей качества функционирования ИС является функциональная полнота F, представляющая собой отношение области автоматизированной обработки информации $Q_{\text{а}}$ той системы, для которой была спроектирована ИС, к области обработки информации $Q_{\text{и}}$ для функционирования всей обслуживаемой системы:

$$F = \frac{Q_{\text{а}}}{Q_{\text{и}}}.$$

Качественной характеристикой ИС являются показатели их надёжности. Различают функциональную и адаптивную надёжность. Функциональная надёжность представляет собой свойство ИС реализовать в определённой степени функции программно-технологического, технического и эргономического обеспечения. Адаптивная надёжность ИС состоит в возможности реализовывать свои функции в пределах установленных границ:

$$K_{\text{ад}} = \frac{T_{\text{ИС}}}{T_{\text{ИС}} + T_{\text{в.ИС}}},$$

где $T_{\text{ИС}}$ – средняя наработка на отказ ИС; $T_{\text{в. ИС}}$ – среднее время восстановления ИС.

Как видно из последнего выражения, $K_{\text{ад}}$ есть не что иное, как коэффициент готовности для ИС.

5.4. АНАЛИТИЧЕСКИЕ ЗАВИСИМОСТИ МЕЖДУ ПОКАЗАТЕЛЯМИ НАДЁЖНОСТИ ВОССТАНАВЛИВАЕМЫХ ТЕХНИЧЕСКИХ УСТРОЙСТВ

В п. 5.1 был определён показатель надёжности – средняя статистическая плотность вероятности. Пусть $\Delta t_i \to 0$. Тогда при переходе от дискретного времени к непрерывному определим плотность вероятности отказов восстанавливаемых ТУ:

$$\lim_{\Delta t_i \to 0} \omega_i = \omega(t) = \frac{1}{N} \frac{dn_0(t)}{dt},$$

где $dn_0(t) = d_n(t) - d_m(t)$; $d_n(t)$ – число отказов, возникших в ТУ за интервал времени dt, а $d_m(t)$ – количество восстановленных ТУ из числа неисправных за этот же интервал времени dt.

Отсюда

$$\omega(t) = \frac{1}{N}\frac{dn(t)}{dt} - \frac{1}{N}\frac{dm(t)}{dt} = \frac{1}{N(t)} \cdot \frac{dn(t)}{dt} \cdot \frac{N(t)}{N} - \frac{1}{n(t)} \cdot \frac{dm(t)}{dt} \cdot \frac{n(t)}{N}.$$

С учётом того, что

$$\frac{1}{N(t)} \cdot \frac{dn(t)}{dt} = \lambda(t),$$

а величина

$$\frac{1}{n(t)} \cdot \frac{dm(t)}{dt}$$

называется интенсивностью восстановления отказавших ТУ и обозначается символом $\mu(t)$:

$$\mu(t) = \frac{1}{n(t)} \cdot \frac{dm(t)}{dt},$$

$\omega(t)$ примет вид

$$\omega(t) = \lambda(t)\, p_0(t) - \mu(t)\, q_0(t).$$

Известно, что для невосстанавливаемых ТУ плотность вероятности отказов аналитически выражается через вероятность безотказной работы как

$$f(t) = -\frac{dp(t)}{dt}.$$

Та же зависимость характерна и для восстанавливаемых ТУ, а именно:

$$\omega(t) = -\frac{dp_0(t)}{dt}.$$

Тогда можно записать:

$$\frac{dp_0(t)}{dt} = -\lambda(t)\, p_0(t) + \mu(t)\, q_0(t).$$

При выражении $q_0(t)$ через $p_0(t)$ получается:

$$\frac{dp_0(t)}{dt} + \left[\lambda(t) + \mu(t)\right] p_0(t) = \mu(t).$$

Решение этого дифференциального уравнения имеет вид:

$$p_0(t) = e^{-\int\left[\lambda(t)+\mu(t)\right]dt} \left[\int \mu(t)\, e^{\int\left[\lambda(t)+\mu(t)\right]dt} dt + C\right].$$

Относительно постоянной интегрирования C можно выдвинуть две версии:

– в момент начала эксплуатации ТУ исправно: $p_0(0) = 1$;
– в момент начала эксплуатации ТУ неисправно: $p_0(0) = 0$.

Тогда для случая λ = const и μ = const при $p_0(0) = 1$ имеем:

$$p_0'(t) = \frac{\mu}{\lambda+\mu}\left[1+\frac{\lambda}{\mu}e^{-(\lambda+\mu)t}\right],$$

а при $p_0(0) = 0$

$$p_0''(t) = \frac{\mu}{\lambda+\mu}\left[1-\frac{\lambda}{\mu}e^{-(\lambda+\mu)t}\right].$$

График изменения $p_0'(t)$ и $p_0''(t)$ представлены на рис. 5.1.

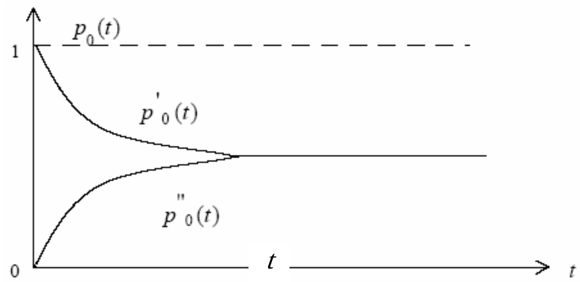


Рис. 5.1. Графики изменения $p_0(t)$ при различных начальных условиях

При допущениях λ = const и μ = const, и, следовательно, $\lambda = \frac{1}{T}$; $\mu = \frac{1}{T_p}$ получим

$$\frac{\mu}{\lambda+\mu} = \frac{\frac{1}{T_p}}{\frac{1}{T}+\frac{1}{T_p}} = \frac{T}{T+T_p} = K_{\text{г}}.$$

Тогда

$$P_0'(t) = K_{\text{г}}\left[1+\frac{\lambda}{\mu}e^{-(\lambda+\mu)t}\right],$$

$$P_0''(t) = K_{\text{г}}\left[1-\frac{\lambda}{\mu}e^{-(\lambda+\mu)t}\right].$$

Практически, для установившегося процесса эксплуатации считают, что $p_0 = K_{\text{г}}$. Таким образом:

$$P_{\text{э}}(t) = K_{\text{г}}\,p(\tau).$$

Отсюда

$$p_{\text{э}}(t) = K_{\text{г}}e^{-\lambda t} = \frac{\mu}{\lambda+\mu}e^{-\lambda t}.$$

Для оценки вероятности того, что в любой момент времени восстанавливаемое ТУ будет находиться в ремонте, используется *функция простоя* $K_{\text{п}}$:

$$K_{\text{п}} = \frac{\lambda}{\lambda+\mu} = \frac{T_p}{T+T_p}.$$

В том случае, когда λ и μ являются величинами одного порядка, наиболее точные результаты эксплуатационной надёжности можно получить, применяя закон полной вероятности сложного события. *Полная вероятность выполнения ТУ заданных функций* равна сумме произведений вероятности частных событий на вероятность существующих гипотез:

$$P_{\text{ф}}(t,\, t_p) = K_{\text{г}}\,p(t) + (1-K_{\text{г}})\,U(t_p)\times p(t-t_p).$$

Здесь предполагается, что существуют только два состояния: исправное рабочее и восстанавливаемое. Тогда $K_{\text{г}} = \frac{T}{T+T_p}$ представляет собой вероятность исправного состояния ТУ; $p(t) = e^{-\frac{1}{T}}$ – вероятность безотказной работы в течение времени t;

$1-K_{\text{г}} = \dfrac{T_p}{T+T_p}$ – вероятность неисправного состояния ТУ; $U(t_p) = 1-\left(1+2\dfrac{t_p}{T_p}\right)e^{-\frac{2t_p}{T_p}}$ – вероятность восстановления неисправного состояния ТУ за время t_p; $p(t-t_p) = e^{\frac{t-t_p}{T}}$ – вероятность безотказной работы ТУ за оставшееся после ремонта время
$t-t_p$, достаточное для выполнения заданной функции.

Подставляя эти значения в исходное выражение, получим:

$$P_{\text{ф}}(t,\ t_p) = \frac{T}{T+T_p}e^{-\frac{t}{T}} + \frac{T_p}{T+T_p}\times\left[1-\left(1+\frac{2t_p}{T_p}\right)e^{-\frac{t-t_p}{T}}\right]e^{-\frac{t-t_p}{T}}.$$

При $t >> t_p$ и $T >> T_p$ разница между $P_{\text{э}}$ и $P_{\text{ф}}$ небольшая, поэтому с достаточной степенью точности можно ограничиться формулой $P_{\text{э}} = K_{\text{г}}e^{-\frac{1}{T}}$.

Применять расчёт $P_{\text{ф}}(t, p)$ целесообразно, когда T и T_p, а также t и t_p имеют один порядок.

Вопросы для самоконтроля

1. Какие ТУ называются восстанавливаемыми?
2. Основные характеристики надёжности восстанавливаемых ТУ.
3. Что такое коэффициент отказов?
4. Какие показатели надёжности относятся к комплексным?
5. Что такое коэффициент готовности?
6. Аналитические выражения коэффициента готовности.
7. Что такое интенсивность восстановления?
8. Основные аналитические зависимости между показателями надёжности восстанавливаемых ТУ.

6. СТРУКТУРНЫЕ СХЕМЫ НАДЁЖНОСТИ

Ранее (в главе 1) говорилось о том, что ТУ подразделяются на элементы и системы, причём система состоит из элементов. Элементы, составляющие систему, могут быть соединены между собой различным образом. С точки зрения надёжности, такие соединения представляют собой структуры, каждая из которых имеет свой способ расчёта. Такой расчёт представляет собой *расчёт надёжности*. Сами структуры носят название *структурных схем надёжности* [6].

Структурные схемы надёжности нельзя путать с принципиальными, функциональными, структурными и другими схемами систем, хотя в частных случаях они могут совпадать. Соединение элементов в структурных схемах надёжности можно свести к четырём видам:

– последовательному,
– параллельному,
– смешанному,
– произвольному.

В качестве основных показателей надёжности здесь используются вероятность безотказной работы и вероятность отказа.

6.1. СТРУКТУРНЫЕ СХЕМЫ НАДЁЖНОСТИ С ПОСЛЕДОВАТЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Последовательное соединение в структурной схеме надёжности – это такое соединение, при котором отказ хотя бы одного элемента приводит к отказу всей системы в целом (рис. 6.1). Этот тип соединения в теории надёжности ещё называет основным соединением.

Если считать отказы элементов независимыми, то на основании теоремы умножения вероятностей вероятность безотказной работы ТУ выражается следующим образом:

$$P_{\text{с}}(t) = p_1(t)\cdot p_2(t)\cdot\ldots\cdot p_n(t) = \prod_{i=1}^{n} p_i(t).$$

где $p_i(t)$ – вероятность безотказной работы i-го элемента; $P_{\text{с}}(t)$ – вероятность безотказной работы системы.

Если $p_i(t) = p_2(2) = \ldots = p_n(t) = p(t)$, то $P_{\text{с}}(t) = p^n(t)$.

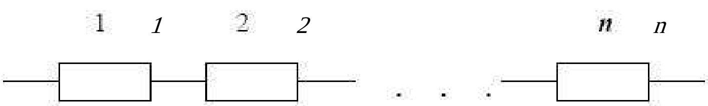


Рис. 6.1. Структурная схема надёжности с последовательным соединением элементов

С учётом выражения вероятности безотказной работы через интенсивность отказов можно записать

$$P_c(t)=\prod_{i=1}^{n} e^{-\int_0^t \lambda_i(t)\,dt} = e^{-\sum_{i=1}^{n}\int_0^t \lambda_i(t)\,dt} = e^{-\int_0^t \sum_{i=1}^{n}\lambda_i(t)\,dt}.$$

Отсюда можно сделать заключение, что суммарная интенсивность отказов n последовательно соединённых элементов находится как сумма интенсивностей отдельных элементов:

$$\lambda_\Sigma(t)=\sum_{i=1}^{n}\lambda_i(t)$$

или, для случая равнонадёжных элементов:

$$\lambda_\Sigma(t)=n\lambda(t).$$

Для случая λ = const имеем

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

Откуда

$$\lambda_\Sigma=\sum_{i=1}^{n}\lambda_i .$$

Из последнего выражения видно, что для обеспечения требуемой техническими условиями вероятности безотказной работы ТУ при увеличении числа последовательно соединённых элементов необходимо снижать величину интенсивности отказов каждого элемента или, что тоже самое, принимать меры к увеличению их средней наработки на отказ.

Нередки случаи, когда система последовательно соединённых элементов состоит из k подсистем, а каждая j-я ($j=\overline{1,\ k}$) подсистема состоит из n_j равнонадёжных элементов. В этом случае вероятность безотказной работы системы будет определяться выражением

$$P_c(t)=\prod_{j=1}^{k} p^{n_j(t)},$$

где n_j – количество равнонадёжных элементов j-го типа; $p(t)$ – вероятность безотказной работы элемента j-й подсистемы.

Суммарная интенсивность отказов равна

$$\lambda_\Sigma(t)=\sum_{j=1}^{k} n_j\lambda(t).$$

Анализ полученных выражений показывает:

– вероятность безотказной работы будет тем ниже, чем больше элементов в него входит;

– вероятность безотказной работы последовательного соединения будет ниже, чем эта же вероятность у самого надёжного элемента системы.

6.2. СТРУКТУРНЫЕ СХЕМЫ НАДЁЖНОСТИ С ПАРАЛЛЕЛЬНЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Параллельным соединением элементов в структурной схеме надёжности называется такое соединение, при котором система отказывает только при отказе всех n элементов, образующих эту схему (рис. 6.2).

Согласно определению,

$$Q_c(t)=q_1(t)\cdot q_2(t)\cdot\ldots\cdot q_n(t)=\prod_{i=1}^{n} q_i(t)=\prod_{i=1}^{n}(1-p_i(t)).$$

Отсюда

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

С учётом интенсивности отказов выражение примет вид

$$P_c(t)=1-\prod_{i=1}^{n}\left(1-e^{\int_0^t \lambda_i(t)\,dt}\right).$$

Для случая равнонадёжных элементов имеем

$$P_c(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda(t)dt}),$$

а при λ = const последнее выражение примет вид

$$P_c(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda t}).$$

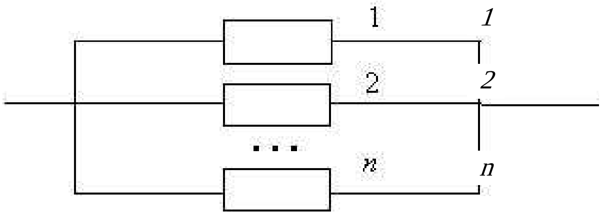


Рис. 6.2. Структурная схема надёжности с параллельным соединением элементов

Основные правила расчёта надёжности при последовательном и параллельном соединениях элементов в структурной схеме надёжности можно формулировать следующим образом:

- определить количество элементов, составляющих структурную схему надёжности;
- из справочных таблиц или статистики определить интенсивность отказов λ_i каждого элемента;
- на основании λ_i по формулам видов соединений в структурных схемах надёжности определяется ВБР.

6.3. СТРУКТУРНЫЕ СХЕМЫ НАДЁЖНОСТИ СО СМЕШАННЫМ СОЕДИНЕНИЕМ ЭЛЕМЕНТОВ

Иногда в сложных устройствах структурные схемы надёжности содержат как последовательные, так и параллельные надёжностные структуры. Речь идёт о том, что в схеме надёжности присутствуют и те и другие виды соединений (рис. 6.3).

В этом случае для расчёта надёжности структурную схему разбивают на последовательные или параллельные участки таким образом, чтобы каждый участок имел либо только последовательную, либо только параллельную структурную схему. На каждом участке определяется вероятность безотказной работы в соответствии с теми формулами, которые соответствуют структурным схемам рассматриваемого участка. Таким образом, исходная структурная схема надёжности превращается в структуру с последовательным или параллельным соединением элементов (рис. 6.4).

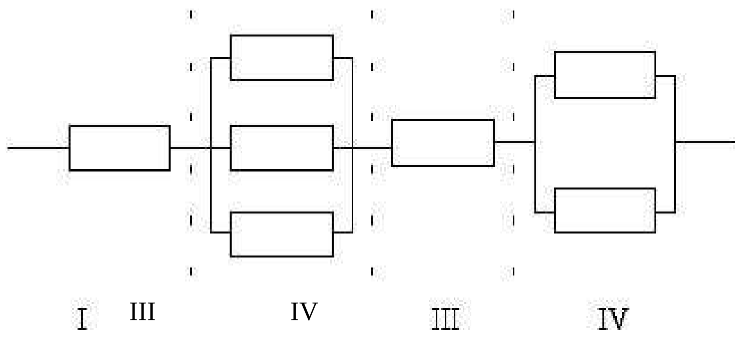


Рис. 6.3. Пример структурной схемы надёжности со смешанным соединением элементов

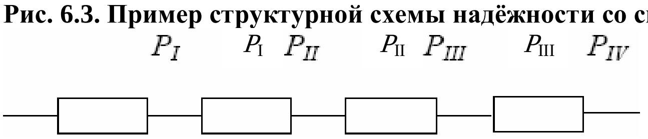


Рис. 6.4. Преобразованная структура со смешанным соединением элементов:
P_{I}, P_{II}, P_{III}, P_{IV} – вероятности безотказной работы соответственно первого, второго, третьего и четвёртого последовательных участков

Тогда вероятность безотказной работы системы в представленном примере будет равна $P_c(t) = P_{\mathrm{I}} \cdot P_{\mathrm{II}} \cdot P_{\mathrm{III}} \cdot P_{\mathrm{IV}}$. В общем случае для системы с k последовательными участками, полученными в результате предварительных преобразований, выражение для вероятности безотказной работы будет иметь вид:

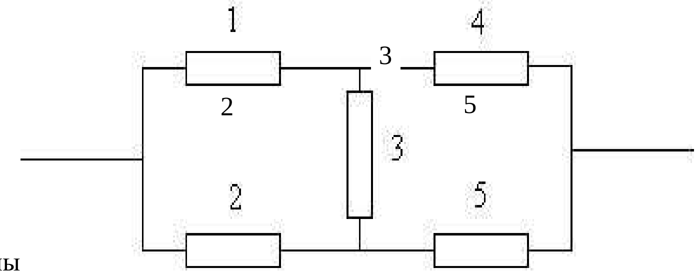
$$P_c(t) = \prod_{j=1}^{k} P_j(t),$$

где $P_j(t)$ – вероятность безотказной работы j-го участка.

6.4. СЛОЖНАЯ ПРОИЗВОЛЬНАЯ СТРУКТУРА

Когда невозможно при составлении структурных схем надёжности применить последовательную, параллельную или смешанную схемы, то приходится иметь дело с так называемой сложной произвольной структурой. Для такой структуры не существует общих методов расчёта надёжности. Одной из наиболее часто встречающихся схем такой структуры является мостиковая схема (рис. 6.5).

Расчёт вероятност 1 ззотказной работ 4 ой схемы можно осуществить методом прямого перебора всех состояний. В частности, мостиковая схема считается работоспособной при пяти вариантах отказов по одному элементу (отказавшие элементы: 1, или 2, или 3, или 4, или 5), при восьми вариантах отказов по два элемента (отказавшие



группы

Рис. 6.5. Произвольная структурная "мостиковая" схема надёжности

элементов: 1 и 4, или 2 и 5, или 1 и 3, или 2 и 3, или 3 и 4, или 3 и 5, или 1 и 5, или 2 и 4), при двух вариантах отказа по трём элементам (отказавшие группы элементов: 1 и 3 и 4, или 2 и 3 и 5) или когда все 5 элементов работоспособны. Тогда для случая равнонадёжных элементов вероятность безотказной работы системы, структурная схема надёжности которой представляет собой мостиковую схему, будет равна

$$p_c(t) = p^5 + 5p^4q + 8p^3q^2 + 2p^2q^3 = p^5 + 5p^4(1-p) + 8p^3(1-p)^2 + 2p^2(1-p)^3,$$

где $p = p(t)$ – вероятность безотказной работы одного элемента; $q = q(t)$ – вероятность отказа одного элемента.

В начале главы говорилось о том, что в большинстве случаев структурные схемы надёжности не совпадают с принципиальными, функциональными и структурными схемами ТУ. Наиболее ярко это утверждение можно продемонстрировать на примере электрических систем, показав, что принципиальная электрическая схема может не совпадать со структурной схемой надёжности.

Известно, что основными отказами электрических систем являются отказы типа "обрыв" и "короткое замыкание". Пусть система состоит из двух диодов $Д_1$ и $Д_2$, включённых параллельно (рис. 6.6, *а*).

Для отказа типа "короткое замыкание" система выйдет из строя, когда откажет любой из двух диодов. Поэтому структурная схема надёжности для этого случая изображается в виде последовательного соединения элементов. В другом случае при отказе типа "обрыв" параллельная цепочка диодов откажет только в случае отказа двух диодов.

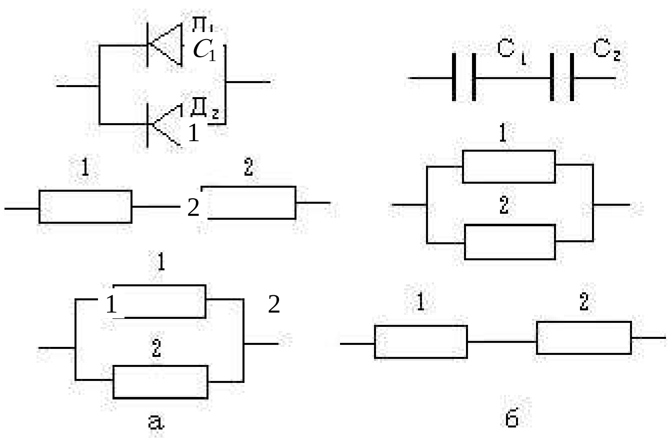


Рис. 6.6. Принципиальные электрические схемы и соответствующие им структурные схемы надёжности:
а – для диодов; *б* – для конденсаторов

Следовательно, структурная схема надёжности будет представлять собой параллельное соединение элементов. Последовательная цепочка конденсаторов C_1 и C_2 изображена на рис. 6.6, *б*. При "коротком замыкании" эта схема выйдет из строя, если только "пробьёт" и C_1 и C_2

В силу этого структурная схема надёжности представляется в виде параллельного соединения элементов. И, наконец, при "обрыве" конденсаторная цепочка откажет, если откажет любой из двух конденсаторов. Это значит, что структурная схема надёжности будет иметь последовательное соединение.

6.5. РАСЧЁТ НАДЁЖНОСТИ ПО ВНЕЗАПНЫМ ОТКАЗАМ

В связи с наличием двух типов отказов элементов (постепенные и внезапные отказы) различаются и два способа расчёта надёжности, соответствующих двум типам отказов. При внезапных отказах применяют *покаскадный метод расчёта надёжности* и (или) *поэлементный метод*.

Покаскадный метод расчёта надёжности кроме расчёта надёжности по внезапным отказам даёт приемлемую оценку безотказности на самых ранних этапах проектирования ТУ. В качестве исходных данных используется число каскадов и принадлежность их к той или иной группе. Считается, что все элементы каскада образуют основное соединение элементов в смысле надёжности. Поэтому для расчёта берутся формулы:

$$p_{\text{в}}(t) = e^{-\int_0^t \lambda(t)\,dt},$$

где $\lambda(t)$ представляет собой суммарную интенсивность отказов по всем элементам системы;

$$\lambda(t) = \sum_{i=1}^{k} n_i \lambda_i(t),$$

где n_i – количество однотипных элементов в i-м ($i = \overline{1,\ n}$) каскаде; k – количество каскадов.

Для оценки суммарной интенсивности используют выражение

$$\lambda^* = \frac{k}{k_a} 10^{-4} \ \text{(1/ч)},$$

где k_a – коэффициент, учитывающий условия эксплуатации. Для надёжных элементов значения этого коэффициента лежат в диапазоне от величины 1,2 до 1,4.

Поэлементный метод расчёта надёжности. Этот метод позволяет получить более точную оценку безотказности. Его также можно применять при проектировании ТУ, но на более поздних этапах. В качестве исходных данных берётся общее число элементов, их тип и данные по эксплуатации аналогичного типа оборудования. Расчёт производится по вышеприведённым формулам, но при определении величины интенсивности отказов используются данные, полученные на предыдущем этапе эксплуатации ТУ аналогичного типа.

При этом

$$\lambda = \frac{\lambda_{\text{э.а}}}{n_{\text{э.а}}} = \frac{\lambda_{\text{п.а}}}{n_{\text{п.а}}},$$

где $\lambda_{\text{э.а}}, \lambda_{\text{п.а}}$ – суммарные интенсивности отказов эксплуатируемого аналога и проектируемой аппаратуры; $n_{\text{э. а}}$, $n_{\text{л. а}}$ – количество элементов эксплуатируемой и проектируемой аппаратуры.

Отсюда:

$$\lambda_{\text{п.а}} = \frac{n_{\text{п.а}}}{n_{\text{э.а}}} \lambda_{\text{э.а}}.$$

Покаскадный и поэлементный методы расчёта по интенсивностям отказов позволяют достаточно полно оценить безотказность проектируемой аппаратуры. В качестве исходных данных используются принципиальная схема, сведения о количестве групп и типов комплектующих элементов, сведения об интенсивностях отказов комплектующих элементов и узлов.

Порядок расчёта следующий.

1. Согласно принципиальной схеме и спецификации, производят разбивку всех элементов на группы, имеющие приблизительно одинаковую интенсивность отказов. Подсчитывают число элементов в каждой группе n_i.
2. По справочным данным находят минимальную и максимальную интенсивности отказов $\lambda_{i\ \max}, \lambda_{i\ \min}$.
3. Определяют максимальную и минимальную интенсивности отказов по группам: $n_i, \lambda_{i\ \max,\min}$.
4. Вычисляют общую интенсивность отказов $\lambda(t) = \sum_{i=1}^{k} n_i \lambda_i$.
5. Используя это выражение, определяют вероятность безотказной работы и $T_{\text{ср}}$ (расчёт ведётся по значениям $\lambda_{i\min}, \lambda_{i\max}$, а также по средним значениям интенсивностей отказов).

6.6. РАСЧЁТ НАДЁЖНОСТИ ПО ПОСТЕПЕННЫМ ОТКАЗАМ

Основой для расчёта являются данные о закономерностях изменения определяющих параметров исследуемого ТУ во времени, а также установленные допуски на эти параметры. Исследования поведения параметров многочисленных типов транспортных ТУ показывают, что распределение времени безотказной работы при постепенных отказах соответствует нормальному закону. Это значит, что для каждого параметра могут быть найдены значения T_i и σ_i, вероятность безотказной работы по i-му параметру системы или элемента определяется выражением

$$P_{\text{п}\,i}(t)=\frac{\Phi\left(\dfrac{T_i-t}{\sigma_i}\right)}{\Phi\left(\dfrac{T_i}{\sigma_i}\right)}.$$

В этом случае вероятность безотказной работы по постепенным отказам всего ТУ, если считать отказы элементов независимыми, находится из выражения

$$P_{\text{п}}(t)=\prod_{i=1}^{h}P_{\text{п}\,i}(i),$$

где h – число определяющих параметров.

Вероятность безотказной работы сложного ТУ по внезапным и постепенным отказам может быть найдена из выражения

$$P_{\Sigma}(t)=p_{\text{в}}p_{\text{п}}(t)=e^{-t\sum_{i=1}^{k}n_i\lambda_i}\prod_{i=1}^{h}P_{\text{п}\,i}(i).$$

Вопросы для самоконтроля

1. Структурная схема надёжности, её отличие от принципиальной схемы ТУ.
2. Структурная схема надёжности с последовательным соединением элементов.
3. Структурная схема надёжности с параллельным соединением элементов.
4. Расчёт надёжности при последовательном соединением элементов.
5. Расчёт надёжности при параллельном соединением элементов.
6. Произвольная структурная схема надёжности.
7. Надёжность при произвольной структурной схеме.
8. Основы расчёта надёжности при постепенных отказах.
9. Основы расчёта надёжности при внезапных отказах.

7. ОЦЕНКА НАДЁЖНОСТИ АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ С УЧЁТОМ ХАРАКТЕРИСТИК ПРОГРАММНОГО И ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ

7.1. ПОСТАНОВКА ЗАДАЧИ

При оценке надёжности аппаратно-программных комплексов (АПК) исходят из того, что надёжность "мягкого оборудования" (математического, программного и информационного обеспечения) не является самостоятельным свойством, так как может проявиться только в процессе его функционирования в составе АПК. Поэтому правильным является подход, при котором надёжность "мягкого оборудования" оценивается по степени влияния на комплексные показатели надёжности системы, имеющей в своем составе техническое (ТО), математическое (МО), программное (ПО) и информационное (ИО) обеспечения. Это важно ещё и потому, что отказы технического (ТК) и программного (ПК) комплексов являются взаимозависимыми событиями. Взаимозависимость может возникать по многим причинам, в том числе из-за влияния режимов применения, влияния отказов друг на друга. Вместе с тем с целью декомпозиции задачи возможно получение отдельных оценок показателей надёжности для ТК и ПК с последующим их объединением по схеме независимых событий. Игнорирование взаимозависимости отказов приводит к оценке снизу для показателей надёжности АПК. И это надо иметь в виду, чтобы контролировать уровень возникающей при этом методической погрешности. Для описания методов оценки АПК были использованы материалы источника [17].

Как объект анализа и как часть АПК программное обеспечение, как было показано в главе 3, имеет следующие особенности:

ПО не подвержено износу, и в нём практически отсутствуют ошибки производства;

если обнаруженные в процессе отладки и опытной эксплуатации дефекты устраняются, а новые не вносятся, то интенсивность отказов ПК уменьшается, т.е. он является "молодеющей" системой;

надёжность программ в значительной степени зависит от используемой входной информации, так как от значения входного набора зависит траектория исполнения программы; если при этом ИО само содержит дефекты, то программа выдаст неправильный результат даже при отсутствии программных ошибок;

если при возникновении ошибок дефекты не диагностировать и не устранять, то ошибки ПО будут носить систематический характер;

надёжность ПО зависит от области применения; при расширении или изменении области применения показатели надёжности могут существенно изменяться без изменения самого ПО.

Исходная информация о надёжности технических устройств – структурных элементов системы – может быть получена путём обработки статистических данных о результатах эксплуатации некоторого количества однотипных образцов таких устройств. Возможности использования такого пути для программного изделия ограничены, так как копии программного изделия идентичны и вместе с тиражированием изделия тиражируются и дефекты – проектные ошибки. Вместе с тем есть другая возможность использования предыдущего опыта. Характеристики числа допущенных проектных ошибок являются довольно устойчивым показателем качества работы сложившегося коллектива программистов и используемых ими средств САПР ПО. Если регистрировать сведения о проектных ошибках во всех ранее разработанных проектах, то после соответствующей обработки можно получить заслуживающие доверия исходные данные для оценки надёжности ПО в новом проекте. Если же такие данные отсутствуют, то используют более общие сведения о процессе проектирования ПО или данные о результатах отладки ПО разрабатываемого проекта. Чтобы по этим данным оценить показатели надёжности, разрабатывают соответствующие модели надёжности в зависимости от этапа жизненного цикла программы.

На ранних стадиях проектирования используют описание алгоритмов по входам и выходам (описание "черного ящика") или структуру алгоритма как совокупность структурных элементов и описание каждого структурного элемента по входам и выходам (описание "белого ящика"). Когда разработаны тексты программ, можно использовать параметры программ: словарь языка программирования, количество операций, операндов, используемых подпрограмм, локальных меток и пр.

В процессе отладки и эксплуатации, когда появляются статистические данные об обнаруженных дефектах, исходное число дефектов как одну из важных характеристик качества программирования можно оценить с помощью методов математической статистики.

Далее в данной главе модели надёжности и методы оценки показателей надёжности ПК разделены на две группы:

модели и методы проектной оценки надёжности, основанные на исходных данных, которые можно получить до начала отладки и эксплуатации программ;

модели и методы статистической оценки надёжности, основанные на результатах отладки и опытной или нормальной эксплуатации ПК.

7.2. ОБЩАЯ СХЕМА ПРОЕКТНОЙ ОЦЕНКИ НАДЁЖНОСТИ ПРОГРАММНОГО КОМПЛЕКСА

В качестве исходных данных используются структурная схема функционального программного обеспечения (ФПО) по каждой функционально самостоятельной операции (ФСО), а также описание входов

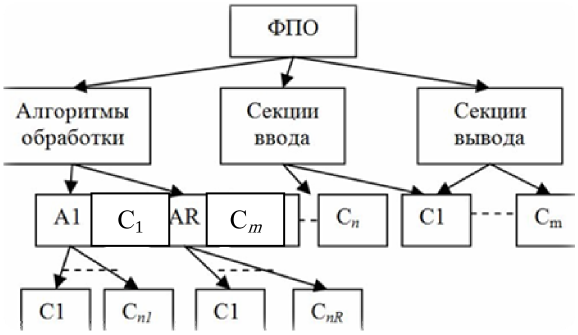


Рис. 7.1. Типовая структура ФПО нижнего уровня

и выходов каждого структурного элемента, межмодульных и внешних связей комплекса алгоритмов и программ.

Типовая структура ФПО имеет в своем составе ФПО верхнего (ФПО ВУ) и нижнего (ФПО НУ) уровней. В свою очередь типовая структура ФПО НУ включает в себя совокупность алгоритмов обработки данных, совокупность секций ввода и вывода, соединяющих АПК с объектом управления (рис. 7.1).

Каждый алгоритм может быть разбит на секции (модули) определённого размера в соответствии с рекомендациями технологии программирования. На ранних этапах проектирования в условиях значительной неопределённости к структурным характеристикам добавляют ещё уровень используемых языков программирования. На более поздних этапах проектирования, когда разработаны тексты программ, могут быть использованы параметры программных модулей.

Методика проектной оценки и прогнозирования надёжности с учётом планируемых результатов отладки содержит несколько этапов.

Расчёт исходного числа дефектов. При расчёте исходного числа дефектов (ИЧД) сначала рассчитывают ожидаемое ИЧД в секциях алгоритмов и секциях ввода и вывода по одной из следующих формул:

$$N_{ci}^{(1)} = N_{ci}^{(1)}(n_{i\text{вх}},\, n_{i\text{вых}},\, l_i); \qquad (7.1)$$

$$N_{ci}^{(2)} = N_{ci}^{(2)}(n_{1i},\, n_{2i},\, N_{1i},\, N_{2i}), \qquad (7.2)$$

где $n_{i\text{вх}}$, $n_{i\text{вых}}$ – число входов и выходов в i-й секции; l_i – уровень языка программирования; n_{1i}, n_{2i} – число различных операций и операндов; N_{1i}, N_{2i} – всего операций и операндов в i-й секции.

Формула (7.1) используется на ранних стадиях проектирования, когда ещё нет текстов программ, формула (7.2) – после программирования секций на принятом языке программирования. Суммарное количество дефектов в отдельных алгоритмах и совокупности алгоритмов и секций ввода и вывода находят по следующим формулам:

$$N_{\text{а}i} = \sum_{j=1}^{m_i} N_{cj} + N_{\text{св}\,i}(n_{\text{св}\,i}); \qquad (7.3)$$

$$N_{\text{а}} = \sum_{i=1}^{R} N_{\text{а}i} + N_{c,\text{а}}(M_{\text{а}}); \qquad (7.4)$$

$$N_{\text{вв}} = \sum_{i \in E_{\text{вв}}} N_{ci} + N_{c,\text{вв}}(M_{\text{вв}}); \quad N_{\text{выв}} = \sum_{i \in E_{\text{выв}}} N_{ci} + N_{c,\text{выв}}(M_{\text{выв}}), \qquad (7.5)$$

где m_i – количество секций в i-м алгоритме ФПО; R – количество алгоритмов; $E_{\text{вв}}$, $E_{\text{выв}}$ – множество секций ввода и вывода; $n_{\text{св}\,i}$ – количество межсекционных связей в i-м алгоритме; $M_{\text{а}}$, $M_{\text{вв}}$, $M_{\text{выв}}$ – количество связей между алгоритмами, межсекционных связей ввода и вывода.

В АСОИУ часто применяют группы однотипных датчиков и исполнительных механизмов, для управления которыми используют копии программных секций ввода и вывода. Тогда в (7.5) включают только один экземпляр секции, но все межсекционные связи. Если при выполнении ФСО используют одну или несколько баз данных (БД), содержащих постоянные и условно-постоянные данные, вносимые на этапе проектирования, то рассчитывают суммарное количество дефектов по всем БД:

$$N_{\text{БД}} = \sum_{i=1}^{R_1} (N_{1i}(V_i,\, V_{0i},\, S_i,\, l_i) + N_{2i}(V_i,\, \lambda_{\text{c}i},\, \tau_i) + N_{3i}), \qquad (7.6)$$

где N_{1i}, N_{2i}, N_{3i} – количество дефектов подготовки данных, дефектов данных вследствие сбоев аппаратуры, дефектов после неумышленных ошибок вследствие несанкционированного доступа к данным; V_{0i}, V_i – общий объём и объём, используемый при выполнении данной ФСО в i-й БД; l_i – уровень языка; $\lambda_{\text{c}i}$ – интенсивность сбоев; τ_i – время функционирования БД при выполнении ФСО; S_i – характеристики структуры данных.

Наконец рассчитывают исходное число дефектов по всему ФПО и ИО при выполнении данной ФСО в виде суммы:

$$N_{\text{ФСО}} = N_{\text{а}} + N_{\text{вв}} + N_{\text{выв}} + N_{\text{БД}}\,. \qquad (7.7)$$

Расчёт остаточного числа дефектов после автономной отладки. После разработки алгоритмов и программных модулей (секций) проводят автономную отладку (АО). Остаточное число дефектов (ОЧД) оценивают с помощью модели АО, позволяющей установить зависимость

$$N_{ci}^{(\text{АО})} = N_{ci}^{(\text{АО})}(N_{ci},\, n_i,\, \tau_{\text{а}i},\, Э_{\text{а}i}), \qquad (7.8)$$

где N_{ci} – исходное число дефектов в i-й секции; n_i – размерность входного вектора; $\tau_{\text{а}i}$ – длительность отладки; $Э_{\text{а}i}$ – коэффициент эффективности отладки.

Расчёт по формуле (7.8) может дать дробное число и трактуется как математическое ожидание случайного числа дефектов. Разработка секций является в основном результатом индивидуального творчества программиста, но проводится в некоторой среде САПР ПО с помощью инструментальных средств. Поэтому эффективность АО зависит также и от возможностей и характеристик САПР ПО. Эта зависимость учитывается при оценке коэффициента $Э_{\text{а}i}$. После коррекции числа дефектов в секциях по результатам АО проводят перерасчёт числа дефектов в укрупнённых составных частях с помощью формул (7.3) – (7.7).

Расчёт остаточного числа дефектов после комплексной отладки. *Комплексная отладка* (КО) предусматривает статическую отладку отдельных алгоритмов, совокупности алгоритмов и секций ввода/вывода, всех средств ФПО и ИО, используемых при выполнении конкретной ФСО, а затем динамическую отладку. В этой процедуре можно выделить три этапа:

1. Отладка путём имитации реальных алгоритмов в инструментальной среде САПР ПО при имитации окружающей среды, в том числе объекта управления. Этот этап является, по существу, отладкой математического обеспечения.
2. Отладка реальных алгоритмов при имитации окружающей среды. Этап позволяет провести статическую отладку и в ограниченной степени – динамическую отладку.
3. Отладка реальных алгоритмов, сопряжённых с реальным объектом управления. Этап позволяет провести в полном объёме динамическую отладку.

Модели КО разрабатывают применительно к этапам 1 и 2, они призваны оценить ещё на стадии разработки программ эффективность отладки, остаточное число дефектов (ОЧД) после КО в укрупнённых составных частях ФПО и ИО с помощью зависимостей типа:

$$N_{\text{а}}^{(\text{КО})} = N_{\text{а}}^{(\text{КО})}(N_{\text{а}}^{(\text{АО})},\, n_k,\, \tau_k,\, Э_k);$$

$$N_{\text{вв/выв}}^{(\text{КО})} = N_{\text{вв/выв}}^{(\text{КО})}(N_{\text{вв}}^{(\text{АО})},\, N_{\text{выв}}^{(\text{АО})},\, n_{1k},\, \tau_{1k},\, Э_{1k});$$

$$N_{\text{БД}}^{(\text{КО})} = N_{\text{БД}}^{(\text{КО})}(N_{\text{БД}}^{(\text{АО})},\, \tau_{2k},\, Э_{2k}),$$

где n_k, n_{1k} – размерности входного вектора; $\tau_k, \tau_{1k}, \tau_{2k}$ – длительности отладки; $Э_k, Э_{1k}, Э_{2k}$ – коэффициенты эффективности отладки.

Перерасчёт остаточного числа дефектов для ФПО и ИО проводится по формуле (7.7).

Оценка вероятности проявления дефекта при однократном выполнении ФСО. Дефекты, не обнаруженные при автономной и комплексной отладках, не являются случайными событиями, так как, в отличие от дефектов производства аппаратуры, они не развиваются во времени, а программное изделие не подвержено процессу физического старения.

Дефекты программ могут проявляться только при работе АПК и только на вполне определённых значениях наборов входных переменных или их последовательностей и при вполне определённых состояниях системы, отражённых в условно-постоянной информации. Сочетаний входных наборов и состояний очень много, а появление определённых сочетаний трудно предсказуемо. Поэтому появление именно таких из них, при которых дефект проявляется и превращается в ошибку, становится уже случайным событием, а момент появления – случайной величиной. К их анализу можно применять вероятностные методы. Если известно распределение дефектов по полю программ и данных, то можно найти вероятность проявления дефектов при однократном выполнении ФСО в режиме МКЦП:

$$Q_1 = Q_{11}(N_{\text{а}},\ m,\ B,\ F_{\text{п}},\ F_1) + Q_{12}(N_{\text{БД}},\ V,\ V_0,\ v,\ F_{\text{д}},\ F_2), \qquad (7.9)$$

где $N_{\text{а}}$, $N_{\text{БД}}$ – остаточное число дефектов в алгоритмах и базах данных; $F_{\text{п}}$, $F_{\text{д}}$ – распределения входных наборов и запросов по полю данных при однократном выполнении ФСО; B – вектор параметров ПО; m – количество входных наборов, поступающих в систему при однократном выполнении ФСО; v – объём фрагмента данных, используемых при однократном выполнении ФСО.

В режиме НПДП в качестве цикла однократного выполнения ФСО может быть принят фрагмент определённой длительности, в котором начинается и завершается обработка информации.

Оценка вероятности проявления дефектов при многократном выполнении ФСО. Вероятность проявления остаточных дефектов при M прогонах программ Q_M зависит от вероятности Q_1 и степени независимости различных прогонов. Если прогоны осуществляются на одних и тех же входных наборах, то зависимость максимальна и тогда $Q_M = Q_1$. Если же прогоны независимы, то

$$Q_M = 1-(1-Q_1)^M \approx MQ_1 . \qquad (7.10)$$

Все остальные случаи находятся между этими двумя крайними. Очевидно, что в сложном ПК даже при большом числе дефектов вероятность их проявления может быть очень мала, поскольку велико множество возможных сочетаний значений входных векторов и внутренних состояний программ. Верно и обратное: длительное безошибочное функционирование ПК вовсе не гарантирует того, что в нём нет дефектов, которые могут проявиться в самый неблагоприятный момент, несмотря на самую тщательную отладку. Об этом свидетельствует и практика эксплуатации больших ПК, например в информационно-вычислительных системах космических аппаратов.

Оценка характеристик потоков инициирующих событий. Инициирующим является любой сигнал, требующий выполнения в полном объёме или частично одной из ФСО. Основным источником инициирующих событий (ИС) является объект управления, в котором изменение состояния может сопровождаться формированием индикатора ИС. К другим источникам ИС относятся оперативный персонал, отказы технических средств, смежные системы.

Суммарный поток ИС характеризуется интенсивностью $\nu(t)$, зависящей в общем случае от времени функционирования.

Оценка показателей надёжности с учётом случайного потока инициирующих событий. В режиме МКЦП в качестве показателей надёжности могут использоваться вероятность безотказной работы, коэффициент готовности, коэффициент оперативной готовности. Для безотказной работы системы требуется успешное выполнение всех циклов, инициированных в течение установленного календарного времени. Поскольку число ИС является случайной величиной, модель надёжности учитывает интенсивность потока ИС и вероятность проявления дефектов при однократном выполнении ФСО:

$$P_{\text{с}}(t) = P_{\text{с}}(t,\ Q_1,\ \nu(t)). \qquad (7.11)$$

Коэффициент готовности $K_{\text{г.с}}$ определяется средним значением интервала между соседними проявлениями дефектов и средним временем устранения обнаруженного дефекта. Коэффициент оперативной готовности $K_{\text{о.г.с}} = K_{\text{г.с}}(1-Q_1)$.

7.3. ФАКТОРНЫЕ МОДЕЛИ

При проектной оценке надёжности факторные модели являются вспомогательными, предназначенными для вычисления параметров, необходимых при формировании модели надёжности, и определения вида зависимостей (7.9) – (7.11).

К факторным относят модели распределения исходного числа дефектов по полю программ и данных, модели эффективности автономной и комплексной отладки, модели режимов применения, характеризующие потоки входных наборов данных, модели потоков инициирующих событий.

Модели распределения числа дефектов в алгоритмах и базах данных. На ранних стадиях проектирования в качестве исходных данных при оценке числа дефектов используют количество входов и выходов в структурной единице ПО и уровень языка программирования. По этим данным рассчитывают потенциальный объём программы:

$$V_{\text{п}} = (n_2^*+2)\log_2(n_2^*+2) = 1,443(n_2^*+2)\ln(n_2^*+2),$$

$$n_2^* = n_{\text{вх}} + n_{\text{вых}}, \qquad (7.12)$$

где n_2 – суммарное количество независимых входов и выходов. Зависимость (7.1) имеет вид

$$N_{\text{и}} = V_{\text{п}}^2/(lV_{\text{у}}),\quad V_{\text{у}} = 24^3/l^2. \qquad (7.13)$$

Здесь $V_у$ – удельный объём программы, равный среднему объёму программы, приходящемуся на один дефект; l – уровень языка. Для естественного языка и близких к нему объектно-ориентированных языков программирования l = 2,16, для языка типа ассемблер l = 0,88.

По разработанным текстам программ можно найти параметры программ, и тогда исходное число дефектов находят по формуле:

$$N_и = V / V_у; \quad V = A \log_2 n, \quad n = n_1 + n_2,$$

$$A = n_1 \log_2 n_1 + n_2 \log_2 n_2,$$

$$n_1 = n_{с.к} + n_{пп}, \quad n_2 = n_{м.п} + n_{мет} + n_k, \qquad (7.14)$$

где V – наблюдаемый объём программы; A – теоретическая длина программы; n – словарь языка; n_1 – число операций; n_2 – число операндов; $n_{с.к}$ – количество используемых словарных конструкций; $n_{пп}$ – количество подпрограмм; $n_{м.п}$ – количество массивов переменных; $n_{мет}$ – количество локальных меток; n_k – количество констант; $V_у = 3000$. Формулу (7.14) используют и для расчёта ИЧД в базах данных. В этом случае V – объём в байтах, $V_у$ = 17 850.

Модели распределения дефектов в базах данных. При отсутствии специальных знаний о возможном распределении дефектов в базах данных естественной является модель равномерного распределения числа дефектов n по полю данных объёмом V_0. Если для выполнения конкретной ФСО используется только часть этого объёма, а именно данные объёма $V < V_0$, то в объёме V оказывается случайное число дефектов, задаваемое некоторым распределением. При построении распределения можно использовать дискретную или непрерывную модели. Если база данных структурирована и в ней выделены структурные единицы (кластеры, теги и др.) примерно одинакового объёма v, причём V_0 / v много больше, чем n, то с высокой вероятностью в каждой структурной единице будет не более одного дефекта. Тогда число дефектов в объёме V имеет гипергеометрическое распределение

$$P_m(V, V_0, n) = C_M^m C_{N-M}^{n-m} / C_N^n, \quad M = \frac{V}{v}, \quad N = \frac{V_0}{v}; \qquad (7.15)$$

$$\max(0, n + M - N) \le m \le \min(n, M).$$

Если база данных не структурирована, то используется биномиальная модель

$$P_m(V, V_0, n) = C_n^m q^m p^{n-m}, \quad p = 1 - q, \quad q = V / V_0. \qquad (7.16)$$

Эта модель допускает наличие в одном фрагменте данных объёма v более одного дефекта. При больших V_0 и малых v распределения (7.15) и (7.16) близки друг к другу.

Модели эффективности отладки. Для прогнозирования момента обнаружения (проявления) дефекта можно использовать экспоненциальную, вейбулловскую или степенную модели. Тогда зависимости можно трактовать как функции распределения времени обнаружения дефекта. Однако они не учитывают такой важный параметр, как исходное число дефектов. Используя главную идею моделей о нелинейной зависимости числа обнаруженных дефектов от времени отладки, можно рассчитывать ОЧД с помощью формул:

$$N_0(\tau) = N \exp(-a\tau / \tau_n), \ a > 0; \qquad (7.17)$$

$$N_0(\tau) = N(1 - (\tau / \tau_n)^{1/m}), \ m > 1; \qquad (7.18)$$

$$N_0(\tau) = N \exp(-(a\tau / \tau_n)^m), \ 0{,}8 \le m \le 1{,}2, \qquad (7.19)$$

где τ_n, m, a – параметры моделей.

Значения параметров определяют на основании опыта отладки других программных изделий и уточняют по результатам отладки после обнаружения первого и второго дефектов в данном программном изделии.

Рассмотрим ещё одну модель отладки ПО, основанную на понятии конгруэнтного множества (КМ). Пусть имеется комбинационная логическая структура со входным вектором $X = (x_1, x_2, ..., x_n)$ и выходным вектором $Y = (y_1, y_2, ..., y_r)$. В комбинационной схеме каждому набору X соответствует определённый набор Y, не зависящий от внутреннего состояния системы при правильной её работе. Обнаружение дефекта происходит по несовпадению фактического значения вектора Y с правильным значением. Назовём *конгруэнтным множеством* подмножество E_i множества E значений вектора X, обладающее следующим свойством: предъявление любого значения из E_i способно обнаружить дефект определённого типа. Логическим индикатором КМ является минимальная дизъюнктивная нормальная форма, содержащая все элементарные конъюнкции логических переменных без отрицания. Число r называют рангом КМ. Например, логический индикатор КМ первого ранга имеет вид $F(X) = x_1 \vee x_2 \vee ... \vee x_n$. Размером КМ называют количество конституант единицы в совершенной дизъюнктивной нормальной форме (СДНФ) логической функции, соответствующей одной тестовой комбинации.

Так, для $F(X) = x_1$ количество конституант единицы равно 2^{n-1}. Элементарной конъюнкции $x_1 x_2$ соответствует СДНФ, содержащая 2^{n-2} конституант единицы. В общем случае КМ r-го ранга имеет размер 2^{n-r}, а относительный размер равен 2^{-r}. Количество КМ такого размера равно C_n^r.

Для полного тестирования КМ r-го ранга надо предъявить 2^r входных наборов. Предъявляя входные наборы сериями по C_n^m входных наборов (m = 0, ..., n), так что в каждой серии набор содержит ровно m единиц, проводим тестирование одновременно нескольких КМ. После серии с номером m полностью проверенными оказываются КМ ранга $r \le m$ и частично проверенными – КМ ранга $r > m$. Если в КМ r-го ранга есть хотя бы один дефект, то после завершения m-й серии условная вероятность его обнаружения равна

$$Q_r(m) = \sum_{i=0}^{m} C_r^i 2^{-r}, \;\; r > m; \;\; Q_r(m) = 1, \;\; r \le m. \qquad (7.20)$$

Если известно распределение вероятностей дефекта $\{\beta_r, r = 1, ..., n\}$ по конгруэнтным множествам, то после завершения m-й серии шагов отладки безусловная вероятность обнаружения дефекта

$$Q_1(m, \beta) = \sum_{r=1}^{n} \beta_r Q_r(m) = \sum_{r=1}^{m} \beta_r + \sum_{r=m+1}^{n} \beta_r \sum_{i=0}^{m} C_r^i 2^{-r}. \qquad (7.21)$$

Общая длина тестовой последовательности

$$L_m = \sum_{i=0}^{m} C_n^i. \qquad (7.22)$$

Вероятность необнаружения дефекта после завершения m-й серии

$$P_1(m, \beta) = 1 - Q_1(m, \beta) = \sum_{r=m+1}^{n} \beta_{1r},$$

$$\beta_{1r} = \beta_r P_r(m), \quad P_r(m) = \sum_{i=m+1}^{n} C_r^i 2^{-r}. \qquad (7.23)$$

Здесь β_{1r} имеет смысл вероятности того, что после m-й серии отладочных наборов дефект в КМ r-го ранга не проявится. Вероятность проявления дефекта после m-й серии равна $\alpha_r = \beta_r - \beta_{1r} = \beta_r Q_r(m)$. Согласно другой трактовке, β_{1r} есть безусловная вероятность того, что в КМ после отладки останется дефект, а α_r – вероятность отсутствия дефекта после отладки.

Пусть теперь m-я тестовая серия длиной C_n^m выполнена не полностью, а проверен результат только по l наборам $(l < C_n^m)$. Представим (7.20) в виде

$$Q_r(m) = \sum_{i=0}^{m} \Delta Q_r(i), \;\; \Delta Q_r(i) = C_r^i 2^{-r}. \qquad (7.24)$$

Тогда вероятность проявления дефекта в КМ r-го ранга при неполной m-й серии

$$\Delta Q_r(m, l) = l \Delta Q_r(m) / C_n^m = \frac{l}{2^r}(C_r^m / C_n^m).$$

После $(m - 1)$ полных и m-й неполной серии условная вероятность проявления дефекта в КМ r-го ранга

$$Q_r(m-1, l) = \sum_{i=0}^{m-1} \Delta Q_r(i) + \Delta Q_r(m, l).$$

Безусловная вероятность проявления дефекта

$$Q_1(m-1, l, \beta) = \sum_{r=1}^{m-1} \beta_r + \sum_{r=m}^{n} \beta_r \left(\sum_{i=0}^{m-1} C_r^i 2^{-r} + \Delta Q_r(m, l) \right).$$

Вероятность того, что дефект не будет обнаружен после неполной m-й серии:

$$P_1(m-1,\ l,\ \beta) = \sum_{r=m+1}^{n} \beta_{1r} + \sum_{r=m}^{n} \beta_r \Delta Q_r(m)\ (1 - l / C_n^m) =$$

$$= P_1(m,\ \beta) + \Delta P_1(m,\ \beta)\ (1 - l / C_n^m),$$

$$\Delta P_1(m,\ \beta) = P_1(m,\ \beta) - P_1(m-1,\ \beta).$$

Вероятность $Q_1(m,\ P)$ можно трактовать как математическое ожидание количества обнаруженных дефектов при наличии в программе не более одного дефекта. Если в ней есть N дефектов, то математическое ожидание числа обнаруженных дефектов после m-й серии

$$\overline{N}_1 = MN_1 = M(X_1 + ... + X_N) = NQ_1(m,\ p).$$

Среднее остаточное количество дефектов

$$\overline{N}_0 = N - \overline{N}_1 = NP_1(m,\ p) = NP_1(m,\ \beta) = \sum_{r=m}^{n} \beta_{1r}. \qquad (7.25)$$

При неполной m-й серии

$$\overline{N}_0 = NP_1(m-1,\ l,\ P). \qquad (7.26)$$

Вероятность того, что после m-й серии в программе не останется ни одного дефекта

$$P_0 = Q_1^N(m,\ P). \qquad (7.27)$$

Вероятность P_0 является гарантированной нижней оценкой вероятности безотказной работы. Правило завершения отладки может быть составлено либо путём нормирования длительности отладки, либо путём нормирования коэффициента эффективности отладки. В первом случае отладка завершается по достижении длиной тестовой последовательности нормативного значения L^0. Исходя из этого рассчитывают коэффициент эффективности отладки по одной из следующих формул:

$$Э_0^{(1)} = \overline{N}_1 \neq Q_1(m-1,\ l,\ p);\ \ Э_0^{(2)} = P_0(L^0) = Q_1^N(m-1,\ l,\ p);\ \ \ L^0 = L_{m-1} + l.$$

Во втором случае отладка завершается по выполнении одного из следующих неравенств:

$$Э_0^{(1)}(L) = Q_1(m-1,\ l,\ \beta) \geq Э_{00}^{(1)};$$

$$Э_0^{(2)}(L) = Q_1^N(m-1,\ l,\ \beta) \geq Э_{00}^{(2)};\ \ L = L_{m-1} + l. \qquad (7.28)$$

Если в (7.28) принято первое правило, то нормируется остаточное число дефектов. Из уравнения находят сначала m и l, а затем L. Если принято второе правило, то нормируется вероятность полного отсутствия дефектов. Второе требование более жёсткое и требует знания исходного числа дефектов N. Оба правила дают одинаковые длительности отладки, если $Э_{00}^{(1)} = \left(Э_{00}^{(2)}\right)^{1/N}$.

Пример. Пусть на вход программы комбинационного типа подаётся набор данных из пяти бинарных переменных. Известно, что после программирования ожидаемое число дефектов равно 2 и они распределены по КМ равномерно. Необходимо оценить эффективность отладки после m-й серии отладочных наборов (m = 1 ... 5) и найти гарантированную нижнюю оценку вероятности безотказной работы программы для L = 6, 16, 26 и 31.

Решение. Результаты расчётов приведены в табл. 7.1.

Из данных, приведённых в табл. 7.1, видно, что труднее всего обнаруживаются дефекты в КМ более высокого ранга. При длительности теста, составляющей 50% от длительности полного теста (m = 2, L = 16), в первых двух КМ дефекты обнаруживаются гарантированно, а в КМ 5-го ранга – лишь с вероятностью 0,5. Расчёт безусловной вероятности обнаружения дефекта, которая является показателем эффективности отладки, проводится по формуле (7.21). Результаты расчётов приведены в первой строке табл. 7.2.

Эффективность отладки достигает значения 0,95 при длительности отладки, достигающей значения 81,25% от длительности полного теста.

7.1. Условная вероятность обнаружения дефекта в КМ r-го ранга

r	$Q_r(m)$ $m = 0$	$m = 1$	$m = 2$	$m = 3$	$m = 4$	$m = 5$
1	0,5	1	1	1	1	1
2	0,25	0,75	1	1	1	1
3	0,125	0,50	0,875	1	1	1
4	0,0625	0,3125	0,6875	0,9325	1	1
5	0,03125	0,1875	0,5000	0,8175	0,96875	1

7.2. Безусловная вероятность обнаружения дефекта

Модель	$Q_1(m,(\beta))$ $m = 0$	$m = 1$	$m = 2$	$m = 3$	$m = 4$	$m = 5$
КМ	0,194	0,55	0,813	0,950	0,994	1
Экспонента	0,125	0,55	0,881	0,969	0,984	0,986
Степенная	0,290	0,55	0,781	0,929	0,989	1
Средняя	0,207	0,55	0,831	0,949	0,986	0,993

Зависимость вероятности Q_1 от L, как и в моделях (7.17) – (7.19), нелинейная. Для сравнения в табл. 7.2 приведены результаты расчётов для экспоненциальной и степенной моделей. Для определения параметров a и m используется точка L = 6:

$$1-\exp(-6a/32)=0,55;\ \ (6/32)^{1/m}=0,55\,.$$

Отсюда a = 4,26, m = 2,8. Из таблицы 7.2 видно, что почти всюду экспоненциальная и степенная модели дают двустороннюю оценку значения, полученного по модели КМ. Поэтому среднее арифметическое этих значений довольно близко к значениям модели КМ. Максимальное относительное отклонение (при m = 2) не превышает 10%. Среднее остаточное число дефектов, рассчитанное по формуле (7.25), уменьшается более чем вдвое уже при коэффициенте полноты тестирования $K_п = L/L_п = 6/32 = 0,19$ и в 20 раз при $K_п = 0,8$ (табл. 7.3).

Нижняя гарантированная оценка вероятности безотказной работы, рассчитанная по формуле (7.27), составляет 0,66 при m = 2 и 0,9 при m = 3. Для баз данных можно рассмотреть две стратегии отладки:

1. Отладка всего объёма V_0 проводится автономно и независимо от ФСО. Если на каждом шаге тестирования проверяется объём v, а исходное число дефектов $N_и$ известно, то количество дефектов в объёме v имеет биномиальное распределение с параметрами $N_и$ и $q = v/V_0$. При отладке происходит "просеивание" дефектов с вероятностью, равной коэффициенту эффективности отладки a. Значение a оценивается по статистическим данным предыдущих опытов отладки. Остаточное число дефектов определяют по формулам $N_0 = \beta N_и$, $\beta = 1-a$. Если отладка разделена на автономную и комплексную, то остаточное число дефектов после автономной и комплексной отладки

$$N_0^{АО}=\beta_{АО}N_и,\ \ N_0^{КО}=\beta_{КО}N_0^{АО}=\beta N_и,\ \ p=1-\alpha=\beta_{АО}\beta_{КО}\,. \qquad (7.29)$$

2. Отладка проводится только в той части V общего объёма V_0, которая используется при выполнении конкретной ФСО. Дефекты обнаруживаются в процессе многократного выполнения ФСО на тестовых задачах или в процессе эксплуатации.

7.3. Среднее остаточное число дефектов

Модель	$N_0(m)$ $m = 1$	$m = 2$	$m = 3$	$m = 4$
КМ	0,9	0,375	0,100	0,0075
Средняя	0,9	0,278	0,102	0,027

Модели потоков инициирующих событий. Запуск ФСО в режиме МКЦП происходит либо по расписанию, либо при появлении случайных событий определённого типа. Первый способ возникает при опросе пассивных дискретных датчиков (ДД), при появлении регулярных сигналов от смежных систем или команд от оперативного персонала. Случайные инициирующие события (ИнС) возникают по сигналам инициативных ДД, логических схем сравнения показаний аналоговых датчиков (АД) с уставками. Инициирующим событием является любое изменение состояния ДД, достижение аналоговым параметром уровня уставки, изменение состояния любого исполнительного механизма (самопроизвольное или по командам дистанционного управления). В реальных условиях потоки инициирующих событий определяются динамикой изменения физико-химических и технологических процессов в объекте управления, надёжностью средств автоматики, контроля и управления, стратегией дистанционного автоматизированного управления.

Потоки ИнС первого типа, получаемые на регулярной основе, близки по своим характеристикам к стационарным рекуррентным потокам с постоянной интенсивностью. Потоки ИнС второго типа близки к стационарным пуассоновским потокам. Потоки обоих типов являются суммами некоторого количества независимых слагаемых потоков. Поэтому интенсивность суммарного потока находят как сумму интенсивностей слагаемых потоков:

$$\Lambda_{\text{с}} = \Lambda_1 + \Lambda_2 + \Lambda_3 + \Lambda_4 ,$$

где Λ_1 – интенсивность потока ИнС, обусловленного изменениями технологических процессов в объекте управления; Λ_2 – интенсивность суммарного потока отказов технических средств управления; Λ_3 – интенсивность потока заявок от подсистемы дистанционного управления; Λ_4 – интенсивность потока регулярных ИнС.

7.4. ПРОЕКТНАЯ ОЦЕНКА НАДЁЖНОСТИ ПРОГРАММНОГО КОМПЛЕКСА ПРИ ВЫПОЛНЕНИИ ФСО

Если программы не используются, то они и не отказывают. Если же они востребованы и в них есть дефекты, то проявление дефекта зависит от случая, состоящего в том, что на вход поступит как раз тот набор значений переменных, при котором дефект проявляется и превращается в ошибку. В этом смысле ошибки носят случайный характер, и можно говорить о вероятности проявления дефекта.

Вероятность проявления дефекта при однократном выполнении ФСО. При построении модели вероятности проявления дефекта при однократном выполнении ФСО принимают следующие допущения:

1. Во входном векторе можно выделить подвектор переменных, которые можно считать независимыми. В этом смысле не все бинарные сигналы или значения аналоговых переменных, поступающие в систему управления от дискретных или аналоговых датчиков, можно считать независимыми. Например, сигналы от мажорированных датчиков функционально зависимы, и при безотказной работе техники они должны быть одинаковыми.
2. Среди значений входного набора переменных не все комбинации фактически могут появляться на входе программы. Поэтому в множестве значений выделяют область допустимых значений.
3. В режиме МКЦП за один цикл выполняется один прогон программы и в течение одного прогона обнаруживается не более одного дефекта. Вероятность проявления дефекта оценивают в такой последовательности. По формуле (7.25) или (7.26) находят остаточное количество дефектов после автономной отладки для всех структурных единиц ФПО, а затем суммарное количество дефектов. К нему добавляют исходное число дефектов межсекционных и внешних связей (МВС), рассчитанное по формулам (7.12) и (7.13), поскольку МВС не участвуют в автономной отладке:

$$N_0^{\text{АО}} = \sum_{(i)} N_{ci}^{\text{АО}} + N_{\text{МВС}}.$$

Если размерность входного вектора ФСО равна n, а длина тестовой последовательности, согласно (7.22), равна L_m то по формуле (7.24) находят распределение вероятностей β_{1r}, $r = m+1, ..., n$, а по формуле (7.25) при $N = N_0^{\text{АО}}$ – остаточное число дефектов ФПО после комплексной отладки $N_0^{\text{КО}}$. Заметим, что β_{1r} есть безусловная вероятность того, что дефект окажется в КМ r-го ранга, а в КМ осталось N_{1r} непроверенных комбинаций. Это число рассчитывают по формуле

$$N_{1r} = \sum_{i=m+1}^{r} C_r^i.$$

При равномерном распределении вероятность того, что дефект проявится при предъявлении конкретной комбинации из N_{1r}, равна $\alpha_{1r} = \beta_{1r} / N_{1r}$. Вероятность проявления одного дефекта при предъявлении одного входного набора

$$Q_1(1, 1) = \sum_{r=m+1}^{n} \gamma_r \alpha_{1r} = \sum_{r=m+1}^{n} \gamma_r \beta_{1r} / N_{1r} , \qquad (7.30)$$

где γ_r – вероятность того, что предъявленный входной набор принадлежит подмножеству непроверенных комбинаций КМ r-го ранга. При равномерном распределении предъявляемых наборов

$$\gamma_r = \frac{C_n^r}{2^n} \frac{N_{1r}}{2^r}, \; r = m+1, ..., n . \qquad (7.31)$$

Подставляя (7.31) в (7.30), получим:

$$Q_1(1, 1) = \sum_{r=m+1}^{n} Q_{1r}(1, 1) = \sum_{r=m+1}^{n} C_n^r \beta_{1r} 2^{-n-r} . \qquad (7.32)$$

Если остаточное число дефектов равно N_0, а при однократном выполнении ФСО предъявляется k входных наборов, то вероятность проявления хотя бы одного дефекта

$$Q_1(N_0, k) = 1-(1-Q_1(1, 1))^{N_0 k} \approx N_0 k Q_1(1, 1) . \qquad (7.33)$$

Рассмотрим теперь модель проявления дефектов в базах данных. Пусть до проведения отладки ожидаемое число дефектов $N_{и} = n$ в базе данных объёмом V_0 рассчитывается по формуле (7.13), а при выполнении ФСО используется часть БД объёмом V. Тогда при равномерном распределении вероятностей каждого дефекта по полю V_0 число дефектов в объёме V имеет биномиальное распределение с параметрами n и $q = 1 - p = V / V_0$. Вероятность того, что в объёме V будет хотя бы один дефект, равна $1 - p_n$. Если во время однократного выполнения ФСО запрашивается фрагмент объёмом v и находящийся в нём дефект гарантированно обнаруживается, то вероятность проявления дефекта при однократном выполнении ФСО до отладки

$$Q_{1БД}(v,\ V,\ V_0,\ N_{и}) = \frac{1-(1-qq_1)^n}{1-p^n} = \frac{1-(1-v/V_0)^n}{1-(1-V/V_0)^n},\ q_1 = \frac{v}{V} .$$

При отладке только в объёме V дефекты подвергаются "просеиванию" только в этом объёме. Их количество N_v имеет биномиальное распределение с параметрами $N_{и}$ и $q = V / V_0$. Если $N_v = n_1$, то отладка уменьшает среднее число дефектов до $n_2 = n_1\beta$, где $(1 - \beta)$ – эффективность отладки. Вероятность проявления дефекта после отладки есть вероятность наличия в объёме v хотя бы одного дефекта при условии, что в объёме V есть дефекты:

$$Q_1(n_2) = \frac{1-p_1^{n_2}}{1-p^{N_{и}}},\ p = 1 - V/V_0,\ p_1 = 1 - v/V.$$

Поскольку n_2 – случайная величина, имеющая биномиальное распределение с параметрами $N_{и}$ и $q_0 = \beta_q$, безусловная вероятность

$$Q_1 = \sum_{i=1}^{N_{и}} Q_1(i)\, C_{N_0}^i q_0^i \frac{(1-q_0)^{N_{и}-i}}{(1-p^{N_{и}})} = (1-(1-q_0 q_1)^{N_{и}})/(1-p^{N_{и}}) .$$

Если прогон программы осуществляется после автономной отладки, то $\beta = \beta_{АО}$, если же после комплексной отладки, то $\beta = \beta_{АО}\beta_{КО}$.

Вероятность проявления дефекта при многократном выполнении ФСО. Если при многократном прогоне программы на вход поступают независимые наборы значений переменных, то вероятность проявления дефектов

$$Q_M(N_0,\ k) = 1-(1-Q_1(N_0,\ k))^M = 1-(1-Q_1(1, 1))^{MN_0k} = 1-(P_1(1, 1))^{MN_0k} .$$
(7.34)

Дефект в БД не проявится при M-кратном прогоне, если он не находится в объёме V (с вероятностью $p = 1 - V/V_0$) или находится в объёме V, но не окажется в выбранных фрагментах объёма v (с вероятностью p_1^M). Если всего в объёме V_0 находится n дефектов, то условная вероятность проявления дефектов при M-кратном выполнении ФСО до начала отладки

$$Q_{уБД}(M,\ v,\ V,\ V_0,\ n) = \frac{(1-(1-q(1-p_1^M))^n)}{(1-p^n)},\ n = N_{и} . \qquad (7.35)$$

После отладки с параметром разрежения β условная вероятность проявления дефектов

$$Q_{уБД}(M,\ v,\ V,\ V_0,\ n,\ \beta) = \frac{(1-(1-q_0(1-p_1^M))^n)}{(1-p^n)},\ n = N_{и},\ q_0 = \beta q, \quad (7.36)$$

где $\beta = \beta_{АО}$ или $\beta = \beta_{АО}\beta_{КО}$.

Безусловные вероятности проявления дефектов

$$Q_{БД}(M) = 1-(1-q(1-p_1^M))^n;$$

$$Q_{БД}(M,\ p) = 1-(1-q_0(1-p_1^M))^n,\ q_0 = \beta q . \qquad (7.37)$$

Отсюда следует, что при увеличении M вероятность проявления дефектов асимптотически стремится к величине $1 - p_n$.

Вероятность безотказной работы ПК в режиме МКЦП при случайном потоке инициирующих событий. При простейшем потоке ИнС с параметром Λ вероятность безотказной работы находят как безусловную вероятность того, что все циклы выполнения ФСО в интервале (0, t) будут безошибочными:

$$P_c(t) = \sum_{M=0}^{\infty} \frac{(\rho\,(1 - Q_1(N_0,\, k)))^M}{M!}\; e^{-\rho} P_{\text{БД}}(M),\;\; \rho = \Lambda t.$$

Подставляя сюда выражение для $P_{\text{БД}}(M)$ из (7.37), получим:

$$P_c(t) = \sum_{M=0}^{\infty} \frac{(\rho P_1(N_0,\, k))^M}{M!}\; e^{-\rho}\,(p_0 + q_0 p_1^M)^n. \qquad (7.38)$$

Если q_0 мало, то можно использовать приближённое выражение

$$P_{\text{БД}}(M) \approx 1 - nq_0(1 - p_1^M).$$

Тогда

$$P_c(t) = \exp(-\rho Q_1(N_0,\, k))\;(1 - nq_0 + nq_0 \exp(-\rho q_1 P_1(N_0,\, k))). \quad (7.39)$$

Если использовать схему независимых событий, то можно получить нижнюю оценку вероятности безотказной работы системы как произведение вероятностей безотказной работы ФПО и ИО:

$$P_c(t) \approx \exp(-\rho Q_1(N_0,\, k))\;(1 - nq_0 + nq_0 \exp(-\rho q_1)). \qquad (7.40)$$

Отсюда следует, что интенсивность отказов и средняя наработка на отказ ПК равны

$$\lambda_{\text{ПК}} = \lambda_{\text{ФПО}} + \lambda_{\text{БД}};\;\; \lambda_{\text{ФПО}} = \Lambda Q_1(N_0,\, k);$$

$$\lambda_{\text{БД}} = \Lambda Q_{\text{БД}}(1,\, \beta) = nqq_1\beta\Lambda;$$

$$T_{\text{ПК}} = \frac{1 - nq_0}{\Lambda Q_1(N_0,\, k)} + \frac{nq_0}{\Lambda(Q_1(N_0,\, k) + q_1 P_1(N_0,\, k))} \approx \frac{1}{\lambda_{\text{ПК}}}. \quad (7.41)$$

Приближённую формулу для $T_{\text{ПК}}$ можно использовать только при малых q_0 и Q_1.

Учёт процедур парирования ошибок. Процедура парирования ошибок обеспечивает разрежение потока отказов, не допуская перехода обнаруженного дефекта в программах или данных в отказ системы. Зная структуру потока ошибок по типам парируемых ошибок

$$\Lambda Q_1(N_0,\, k) = \sum_{i=1}^{n_1} \lambda_{\text{ПО},\,i};\;\; \Lambda q_1 = \sum_{i=1}^{n_2} \lambda_{\text{ИО},\,i},$$

получим интенсивности разреженных потоков ошибок:

$$v_1 = \sum_{i=1}^{n_1} \lambda_{\text{ИО},\,i}\, q_{\text{ИО},\,i};\;\; v_2 = \sum_{i=1}^{n_2} \lambda_{\text{ИО},\,i}\, q_{\text{ИО},\,i}.$$

Подставляя v_1 и v_2 в (7.39) вместо ΛQ_1 и Λq_1, находим:

$$P_c(t) = e^{-v_1 t}(1 - nq_0 + nq_0 e^{-v_2 t P_{1,\,p}(N_0,\, k)});\;\; P_{1,\,p}(N_0,\, k) = \sum_{i=1}^{n_1} q_{1i} Q_{1i},\;\; Q_{1i} = \frac{\lambda_{\text{ПО},\,i}}{\Lambda},$$

где Q_{1i} – вероятность того, что будет обнаружен дефект i-го типа.

7.5. ПРИМЕР ПРОЕКТНОЙ ОЦЕНКИ НАДЁЖНОСТИ ПРОГРАММНОГО КОМПЛЕКСА

Аппаратно-программный комплекс предназначен для выполнения трёх основных функций:

автоматического управления (АУ) без участия ФПО верхнего уровня системы управления;

дистанционного управления (ДУ) исполнительными механизмами (ИМ) и режимами работы подсистем нижнего уровня с помощью ФПО верхнего уровня;

отображения на мониторах верхнего уровня параметров (ОП), измеряемых на объекте управления, и параметров, отражающих состояние средств самой системы управления, а также регистрации и архивирования информации в базах данных.

АПК построен как двухканальная система с нагруженным дублированием ФПО нижнего (НУ) и верхнего (ВУ) уровней и баз данных (рис. 7.2). Информация в АПК поступает из системы сбора данных (ССД) от измерительных каналов, содержащих дискретные (ДД) и аналоговые (АД) датчики. Управляющие воздействия поступают из АПК в систему вывода данных (СВД), содержащую некоторое количество ИМ. ССД и СВД не входят в рассматриваемую систему и являются буфером между АПК и объектом управления. Подсистема АПК верхнего уровня обменивается информацией со смежными системами.

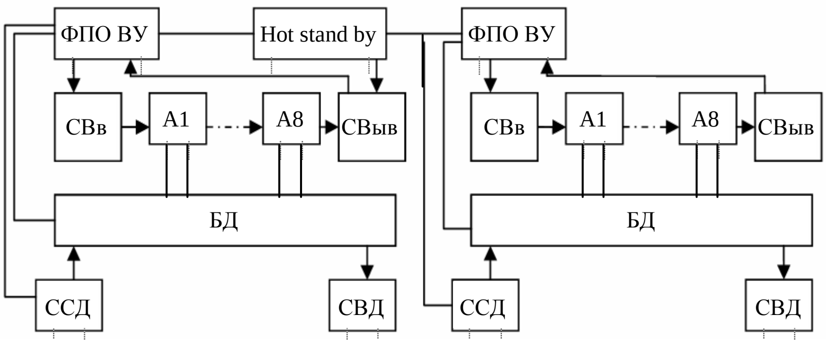


Рис. 7.2. Структурная схема ФПО и ИО АПК

На нижнем уровне структурными единицами ФПО НУ являются алгоритмы А1...А8, секции ввода ($С_{Вв}$) и вывода ($С_{Выв}$) данных. Секции ввода данных могут принимать информацию от ССД или ФПО ВУ. Секции вывода данных выполняют функции контроллеров для управления ИМ и для передачи служебной информации в адрес ФПО ВУ и ФПО НУ. База данных используется не только для выполнения указанных функций, поэтому объём данных БД превышает объём, необходимый для выполнения функций АУ, ДУ и ОП.

Оценка исходного числа дефектов. Надёжность ПК оценивается на стадии проектирования, когда известны структура ФПО и описание каждой структурной единицы по входам и выходам. Поэтому для оценки ИЧД используются формулы (7.12) и (7.13). Чтобы оценить влияние структурирования на ожидаемое число дефектов, каждый алгоритм разбивается на секции, размеры которых определяются требованиями технологии программирования, принятой в САПР ПО, и соображениями повышения эффективности работы отдельного программиста с учётом рекомендаций психологии программирования и соображений удобства дальнейшей отладки. Исходные данные для расчётов и результаты расчётов ИЧД по секциям и алгоритмам приведены в табл. 7.4.

Расчёты проведены для двух вариантов исходных данных. В первом варианте учтены все обрабатываемые входы и все ветвящиеся выходы.

Во втором варианте учтены только независимые входы и выходы. Расчёты показывают, что разбиение алгоритмов на секции приводит к увеличению суммарного количества входов и выходов: в первом варианте на 35%, а по отдельным алгоритмам до 70%; во втором варианте на 29%, а по отдельным алгоритмам до 60%. Однако суммарное количество дефектов при разбиении на секции сократилось: на 40% в варианте 1 и на 30% в варианте 2. Разбиение на секции отдельных алгоритмов не всегда приводит к снижению ИЧД. Так произошло для А1 в варианте 1 и для А4 в варианте 2. Но разбиение всё-таки проводят по другим причинам. Например, разбиение А1 полезно для облегчения автономной отладки. В этом случае при разбиении на две секции для полной отладки надо просмотреть $2^7 + 2^9 = 640$ комбинаций значений бинарных входов, а без разбиения – $2^{11} = 2048$ комбинаций, т.е. в 3,2 раза больше. Варианты 1 и 2 могут рассматриваться как крайние для получения двусторонней оценки ИЧД, так как при функционально зависимых входах и выходах независимыми остаются операции адресации, при программировании которых также могут возникать ошибки. Именно поэтому может быть использовано среднее арифметическое оценок. В качестве секций ввода в состав ФПО НУ входят модули сравнения результатов измерения аналоговых параметров с уставками с последующей индикацией нарушения уставки. В качестве секций вывода используют два типа контроллеров, БУ1 и БУ2, для управления ИМ двух различных типов. Исходные данные о секциях ввода и вывода и результаты расчётов ИЧД приведены в табл. 7.5.

7.4. Название

Наименование	Исходные данные							
	Входы		n_2^*		$V_п$		ИЧД	
	1	2	1	2	1	2	1	2
Алгоритм А1ц	11	9	17	15	80,71	69,49	1,01	0,745
Алгоритм А1с	16	10	28	20	–	–	1,264	0,609
Секция А11	7	4	14	12	64,0	53,3	0,632	0,439
Секция А12	9	6	14	8	64,0	33,2	0,632	0,170
Алгоритм А2ц	–	–	48	36	283,2	199,4	12,29	6,137
Алгоритм А2с	41	32	68	48	–	–	3,71	1,763
Секция А21	14	10	23	16	116,1	75,06	2,08	0,869
Секция А22	10	10	15	14	69,5	64,0	0,745	0,632
Секция А23	6	2	12	4	53,3	15,51	0,439	0,002
Секция А24	6	6	9	8	38,1	33,22	0,223	0,170
Секция А25	5	4	9	6	38,1	24,00	0,223	0,089
Алгоритм А3	17	13	30	21	160,0	104,0	3,95	1,67
Алгоритм А4ц	9	6	15	8	69,5	33,22	0,745	0,170
Алгоритм А4с	12	8	22	12	–	–	0,714	0,178
Секции А41,А42	6	4	11	6	48,1	24,0	0,357	0,089
Алгоритм А5ц	–	–	19	19	92,2	92,2	1,313	1,313
Алгоритм А5с	20	20	32	32	–	–	0,681	0,681
Секции А51…А54	5	5	8	8	33,22	33,22	1,170	0,170
Алгоритм А6ц	–	–	28	20	147,2	98,1	3,344	1,485
Алгоритм А6с	28	20	48	32	–	–	1,754	0,681
Секции А61…А64	7	5	12	8	53,22	33,22	0,439	0,170
Алгоритм А7	20	20	21	21	104,0	104,0	1,67	1,67
Алгоритм А8	12	8	24	20	122,2	98,1	2,305	1,485
А1…А8$_ц$	–	–	202	160	–	–	26,63	14,68
А1…А8$_с$	166	141	273	206	–	–	16,05	10,34

П р и м е ч а н и е. 1 – учитываются все обрабатываемые входы; 2 – учитываются все независимые входы; $A_ц$ – алгоритм без разбиения на секции; $A_с$ – алгоритм с разбиением на секции.

7.5. Исходное число дефектов в секциях ввода и вывода

Наименование	n_2^*	$V_п$	ИЧД
СВв	4	16	0,04
БУ1	42	240	8,90
БУ2	28	147	3,34

Оценка числа дефектов ФПО по подсистемам до автономной отладки. Для выполнения отдельной ФСО привлекают некоторое подмножество структурных единиц ФПО, образующих подсистему. В неё включают также совокупность межсекционных и внешних связей структурных единиц подсистемы. Сведения о составе подсистем приведены в табл. 7.6.

В структуре ФПО (см. табл. 7.2) предусмотрено два канала обработки. Однако в них используют идентичные копии алгоритмов, модулей БУ1 и БУ2, секций ввода. Поэтому количество дефектов от появления копий в параллельных каналах не возрастает, лишь увеличивается вдвое количество связей. В каждом канале используется несколько секций БУ1 и БУ2 в виде идентичных копий, поэтому в расчёте ИЧД представлен только один экземпляр каждой секции. В составе секций ввода в основном только адресные операции. Поскольку они различны для различных копий, в расчётах ИЧД присутствуют все экземпляры СВв. Результаты расчётов для одного и двух каналов представлены в табл. 7.7.

7.6. Состав подсистем ФПО

ФСО	Количество модулей				Количество связей	
	А1…А8	СВв	БУ1	БУ2	МС	ВС
АУ	1	54	20	2	15	3
ДУ	1	0	20	2	15	21
ОП	1	54	0	0	15	9

7.7. Исходное число дефектов в подсистемах до автономной отладки

ПС	$N_и$										
	А1…А8		БУ1	БУ2	СВ	Связи		Всего			
								Вариант 1		Вариант 2	
	В1	В2	n = 17	n = 11		Канал 1	Канал 2	Канал 1	Канал 2	Канал 1	Канал 2
АУ	16,1	10,34	8,9	3,34	2,2	1,21	2,42	31,66	32,9	25,96	27,45
ДУ	16,1	10,34	8,9	3,34	0	6,44	12,87	34,72	41,16	29,01	35,45
ОП	16,1	10,34	0	0	2,2	2,42	4,85	20,63	23,06	14,92	17,35
Все	16,1	10,34	8,9	3,34	2,2	10,07	20,14	40,54	49,61	34,83	43,90

П р и м е ч а н и е. Здесь n – число входов; В1 – вариант 1; В2 – вариант 2.

Из данных, приведенных в табл. 7.7, видно, что наибольшее количество дефектов ожидается в подсистеме дистанционного управления и возникать они будут в основном из-за большего количества внешних связей. Наименьшее количество дефектов – в подсистеме ОП, в которую не входят секции ввода и вывода. Количество дефектов во всём ФПО примерно на 20% превышает ожидаемое число дефектов в наиболее сложной подсистеме.

При оценке ИЧД в базе данных используются следующие исходные данные:

общий объём БД V_0 = 6 Мбайт;

объём данных, используемых при выполнении ФСО: V = = 0,55 Мбайт для всех ФСО, V = 0,5 Мбайт для ОП и ДУ, V = 0,25 Мбайт для подсистемы АУ;

уровень языка программирования I = 0,88.

Согласно (7.13), ожидаемое число дефектов по всей БД $N_и = 352$, в подсистемах ДУ и ОП $N_и = 29$, в подсистеме АУ $N_и = 14{,}5$.

Оценка остаточного числа дефектов после автономной отладки. Автономная отладка проводится по секциям. Функционирование секций проверяется путём предъявления входных наборов сериями, соответствующими конгруэнтным множествам, начиная с m = 1 ранга. Для расчёта ОЧД используется формула (7.25) или (7.26). Как следует из табл. 7.4, при m = 9 полностью проверяются секции АИ, А12, А23, А24, А41, А42, А51...А54, А61...А64. Для А21, А22, А3, А7 и А8 число входов более 9. Поэтому эти секции и алгоритмы проверяются лишь частично. При m = 10 полностью проверяется также секция А22.

При расчёте ОЧД в секциях БУ1 и БУ2 учитываем, что в них число входов n = 17 и n = 11 соответственно. Результаты расчётов приведены в табл. 7.9.

Расчёт ОЧД в МВС проведён для n = 18, 36 и 24 (подсистемы АУ, ДУ и ОП соответственно). При расчёте ОЧД в БД по формуле (7.29) коэффициент полноты проверки принят равным 0,95. Из данных, приведённых в табл. 7.9, видно, что автономная отладка существенно сокращает ожидаемое число дефектов в секциях: по всем подсистемам ФПО (А1...А8 и БУ) от 30,45 до 0,88 при m = 9 и до 0,4 при r = 10.

В БД число дефектов уменьшается от 32 до 1,6. Эффективность АЛ по таким компонентам ФПО и ИО, как отношение числа устранённых дефектов к исходному числу, составляет 0,96 при m = 9 и 0,97 при m = 10. Однако в целом по всем компонентам эффективность существенно меньше: от 0,544 в двухканальной системе при r = 9 до 0,7 в одноканальной системе при m = 10 (табл. 7.8). Снижение эффективности объясняется тем, что при АО не проверяют МВС. Остаточное количество дефектов колеблется от 12,1 до 22,6. Это довольно много, поэтому необходима комплексная отладка

7.8. Среднее остаточное число дефектов в секциях после АО

m	А21	А22	А3	А7	А8	А1…А8	БУ1	БУ2
9	0,0023	0,00007	0,199	0,1965	0,005	0,424	0,4495	0,00208
10	0,0065	0	0,087	0,113	0,00007	0,207	0,196	0,00015

7.9. Результаты автономной отладки (вариант 1)

ПС	m	Среднее остаточное число дефектов								
		Алгоритм	БУ	БД	МВС		Всего			
					Ка-нал 1	Ка-нал 2	Ка-нал 1	Ка-нал 2	Канал 1	Канал 2
АУ	9	0,424	0,452	0,73	1,21	2,42	2,82	4,03	0,911	0,876
АУ	10	0,207	0,196	0,73	1,21	2,42	2,34	3,55	0,926	0,892
ДУ	9	0,424	0,452	1,45	6,44	12,87	8,77	15,23	0,747	0,630
ДУ	10	0,207	0,196	1,45	6,44	12,87	8,29	14,65	0,761	0,644
ОП	9	0,424	0	1,45	2,42	4,85	4,30	6,72	1,792	0,709
ОП	10	0,207	0	1,45	2,42	4,85	4,08	6,51	0,802	0,718
Все	9	0,424	0,452	1,60	10,07	20,14	12,55	22,62	0,690	0,544
Все	10	0,207	0,196	1,60	10,07	20,14	12,08	22,14	0,702	0,553

Здесь МВС – межсекционные и внешние связи.

. Для дальнейших расчётов выбираем вариант с глубиной автономной отладки, соответствующей m = 9, по следующим причинам. С ростом m быстро возрастает трудоёмкость отладки, измеряемая суммарной длиной тестовой последовательности. На все секции, проверенные полностью, при m = 9 затрачивается L = 1568 входных наборов. Значения длины тестовой последовательности для остальных секций, рассчитанные по формуле (7.21), приведены в табл. 7.10. В строке 8 указана сумма значений строк 1...5, в строке 9 к ним добавлено число комбинаций для полностью проверенных секций алгоритмов.

Для алгоритма А7 переход от m = 8 к m = 9 означает увеличение трудоёмкости отладки на 63,6%, а переход от m = 9 к m = 10 – увеличение на 42,8%. Переход от m = 9 к m = 10 приводит к увеличению L: для А3 и БУ на 21,6%, для всех алгоритмов А1...А8 на 37,8%, по секциям БУ на 21,1%, по ФПО в целом на 35,4%.

Степень снижения остаточного числа дефектов и рост эффективности отладки можно проследить по данным, приведённым в табл. 7.11.

7.10. Длина тестовой последовательности после m-й серий

Наименование	n	L		
		m = 8	m = 9	m = 10
Секция А21	14	12 911	14 913	15 914
Секция А22	10	1013	1023	1024
Алгоритм А3	17	65 536	89 846	109 294
Алгоритм А7	20	263 950	431 910	616 666
Алгоритм А8	12	3797	4017	4083
Секция БУ1	17	65 536	89 846	109 294
Секция БУ2	11	1981	2036	2047
Секции А21…А8	–	347 207	541 709	746 981
Алгоритмы А1…А8	–	348 774	543 277	748 549
БУ1, БУ2	–	67 517	91 882	111 341
А1…А8	–	416 291	635 159	859 890

7.11. Зависимость эффективности АО от трудоёмкости

ФСО	m	L	$N_{АО}$	$Э_{АО}$	AL / L
АУ, ДУ	9	635 159	0,876	0,969	–
АУ, ДУ	10	859 890	0,403	0,986	0,354
ОП	9	543 277	0,424	0,974	–
ОП	10	748 277	0,207	0,987	0,377

Для АУ и ДУ увеличение эффективности отладки на 1,7% требует увеличения трудоёмкости на 35,4%. Для ОП рост эффективности на 1,3% требует увеличения трудоёмкости на 37,7%.

Оценка остаточного числа дефектов после комплексной отладки. Комплексная отладка проводится по подсистемам в целом и имеет целью функциональное тестирование и тестирование межсекционных и внешних связей. Остаточное число дефектов и эффективность отладки прогнозируются с помощью модели КМ.

Результаты расчётов вероятности необнаружения дефекта $P_1(m, P)$ и среднего остаточного числа дефектов по формулам (7.23) и (7.25) для двухканальной системы при $m = 8$ и $\beta_k = 1/n$ приведены в табл. 7.12. Данные для расчёта взяты из табл. 7.9.

7.12. Результаты комплексной отладки

ФСО	n	$P_1(m, \beta)$	$N_{АО}$, $m = 9$		$N_{ПО}$, $m = 8$	
			ФПО	ИО	ФПО	ИО
АУ	20	0,1843	3,30	0,73	0,608	0,073
ДУ	17	0,0982	13,78	1,45	1,353	0,145
ОП	20	0,1843	5,27	1,45	0,971	0,145
Все	–	–	21,02	1,60	2,93	0,16

Для оценки остаточного числа дефектов в БД принят коэффициент эффективности тестирования $\alpha_{КО} = 0,9$. Трудоёмкость КО равна сумме длительностей тестовых последовательностей при отладке подсистем: $L = 2\sum_{i=1}^{8} C_{20}^{i} + \sum_{i=1}^{8} C_{17}^{i} = 2 \cdot 263\,950 + 65\,536.$

Полученное значение сравнимо с трудоёмкостью автономной отладки ($L_{АО}$ = 635 159).

После КО не полностью проверенными оказались КМ ранга r от 9 до 17 для подсистемы ДУ и ранга r от 9 до 20 для АУ и ОП. Проанализируем связь эффективности и полноты отладки.

1. Поскольку в пределах КМ наблюдается равномерное распределение вероятности появления дефекта по различным комбинациям, значения полноты отладки как доли числа R_{0r} проверенных комбинаций и эффективности отладки как доли обнаруженных дефектов совпадают. Это значит, что между ними есть линейная зависимость.

2. Коэффициент полноты отладки для КМ n-то ранга и для всей логической структуры в соответствии с (7.20) и (7.22) совпадают. Однако при $m < r < n$ коэффициент полноты отладки δ_r существенно больше, чем при $r = n$ (табл. 7.13), и соответственно больше коэффициента эффективности отладки. Поскольку при увеличении длины тестовой последовательности одновременно тестируются в определённой степени все КМ, это порождает нелинейную зависимость числа обнаруженных дефектов и эффективности отладки от полноты отладки логической структуры.

3. Сравнивая данные, приведённые в табл. 7.12 и 7.13, видим, что для подсистем АУ и ОП (n = 20) при полноте отладки 0,249 коэффициент эффективности отладки достигает значения 0,83 и лежит между значениями коэффициента эффективности для КМ 13-го и 14-го рангов. Для подсистемы ДУ (n = 17) при полноте отладки 0,5 коэффициент эффективности отладки $Э_{КО} = 0,9$ и лежит между значениями для КМ 12-го и 13-го рангов.

7.13. Коэффициент полноты отладки КМ различных рангов

r	$2r$	R_{0r}	δ_r
9	512	511	0,998
10	1024	1013	0,989
11	2048	1981	0,972
12	4096	3797	0,927
13	8192	7099	0,867
14	16 384	12 911	0,788
15	32 768	22 819	0,696
16	65 536	39 203	0,598
17	131 072	65 536	0,500
18	262 144	106 762	0,407
19	524 288	169 826	0,324
20	1 048 576	260 950	0,249

4. Для всей совокупности подсистем полнота отладки

$$\delta = \frac{(L(17) + 2L_{\delta}(20))}{(2^{17} + 2\cdot 2^{20})} = \frac{587\ 436}{2\ 228\ 224} = 0,267\,.$$

При этом коэффициент эффективности отладки равен 0,863, зависимость – существенно нелинейная. При довольно высокой эффективности комплексной отладки и небольшом среднем остаточном числе дефектов доля непроверенных комбинаций велика. Поэтому при нормальной эксплуатации дефекты могут проявляться в течение очень длительного времени.

Оценка вероятности проявления дефекта при однократном и многократном выполнении ФСО после КО. Каждая подсистема ФПО характеризуется следующими показателями: $\bar{N}_0$ – среднее остаточное число дефектов после КО; k – среднее число значений входного вектора, предъявляемых при однократном выполнении ФСО; $\beta_{1r(n)}$ – распределение вероятностей наличия дефекта по КМ различных рангов. Исходные данные для расчёта вероятностей проявления дефектов $Q_1(1, 1)$ и $Q_1(N_0, k)$ по формулам (7.32) и (7.33) приведены в табл. 7.14, а результаты расчётов – в табл. 7.15.

7.14. Распределение вероятностей проявления дефекта по КМ

R	$P_r(m)\times 2^{-m-1}$	$\beta_{1k}(17)$	$\beta_{1k}(20)$	$C_n^r 2^{-n-r}$		$Q_{1r}(1,1)$	
				$n = 17$	$n = 20$	$n = 17$	$n = 20$
9	1	$1,15\cdot 10^{-4}$	$9,77\cdot 10^{-5}$	$3,62\cdot 10^{-4}$	$3,13\cdot 10^{-4}$	$4,17\cdot 10^{-8}$	$3,06\cdot 10^{-8}$
10	5,5	$6,32\cdot 10^{-4}$	$5,37\cdot 10^{-4}$	$1,45\cdot 10^{-4}$	$1,72\cdot 10^{-4}$	$9,16\cdot 10^{-8}$	$9,24\cdot 10^{-8}$
11	16,75	$1,93\cdot 10^{-3}$	$1,64\cdot 10^{-3}$	$4,61\cdot 10^{-4}$	$7,82\cdot 10^{-5}$	$8,90\cdot 10^{-8}$	$1,28\cdot 10^{-7}$
12	37,38	$4,29\cdot 10^{-3}$	$3,65\cdot 10^{-3}$	$1,15\cdot 10^{-5}$	$2,93\cdot 10^{-5}$	$4,95\cdot 10^{-8}$	$1,07\cdot 10^{-7}$
13	68,31	$7,85\cdot 10^{-3}$	$6,67\cdot 10^{-3}$	$2,22\cdot 10^{-6}$	$9,03\cdot 10^{-6}$	$1,74\cdot 10^{-8}$	$6,02\cdot 10^{-8}$
14	108,53	0,0125	$1,06\cdot 10^{-2}$	$3,17\cdot 10^{-7}$	$2,26\cdot 10^{-6}$	$3,9\cdot 10^{-10}$	$2,39\cdot 10^{-8}$
15	155,45	0,01786	0,01518	$3,17\cdot 10^{-8}$	$4,51\cdot 10^{-7}$	$5,7\cdot 10^{-10}$	$6,85\cdot 10^{-9}$
16	205,73	0,02365	0,0201	$1,98\cdot 10^{-9}$	$7,05\cdot 10^{-8}$	$4,7\cdot 10^{-11}$	$1,42\cdot 10^{-9}$
17	256,00	0,02941	0,0250	$5,8\cdot 10^{-10}$	$8,30\cdot 10^{-9}$	$1,7\cdot 10^{-11}$	$2,1\cdot 10^{-11}$
18	303,48	–	9,0296	–	$6,9\cdot 10^{-10}$	–	$2,1\cdot 10^{-11}$
19	346,15	–	0,0338	–	$3,6\cdot 10^{-11}$	–	$1,2\cdot 10^{-12}$
20	384,58	–	0,0376	–	$9,1\cdot 10^{-12}$	–	$3,4\cdot 10^{-13}$
9-17	854,65	0,0982	–	–	–	$2,94\cdot 10^{-7}$	–
9-20	1888,9	–	0,1845	–	–	–	$4,51\cdot 10^{-7}$

7.15. Вероятность проявления дефекта при однократном выполнении ФСО

ФСО	n	k	$N_{КО}$	$Q_1(1, 1)$	$Q_1(N_{k0}, K)$
АУ	20	10	0,608	$4{,}51 \cdot 10^{-7}$	$2{,}74 \cdot 10^{-6}$
ДУ	17	15	1,353	$2{,}94 \cdot 10^{-7}$	$5{,}96 \cdot 10^{-6}$
ОП	20	20	0,971	$4{,}51 \cdot 10^{-7}$	$8{,}76 \cdot 10^{-6}$

7.16. Вероятность проявления дефекта при многократном выполнении ФСО

ФСО	$Q_1(N_{k0}, K)$	M	$QM(N_{k0}, K)$
АУ	$2{,}74 \cdot 10^{-6}$	10 100 1000	$2{,}74 \cdot 10^{-5}$ $2{,}76 \cdot 10^{-4}$ 0,00276
ДУ	$5{,}96 \cdot 10^{-6}$	10 100 1000	$6{,}21 \cdot 10^{-5}$ $6{,}21 \cdot 10^{-4}$ 0,00619
ОП	$8{,}76 \cdot 10^{-6}$	10 100 1000	$8{,}98 \cdot 10^{-5}$ $8{,}98 \cdot 10^{-4}$ 0,00894

Условную и безусловную вероятности проявления дефектов БД при однократном и многократном обращении к ней до проведения отладки находят по формулам (7.35) и (7.37), а при обращении после отладки – по формулам (7.36) и (7.37). Расчёты проводят при следующих исходных данных: V_0 = 6 Мбайт, V = 0,5 Мбайт для подсистем ДУ и ОП, V = 0,25 Мбайт для подсистемы АУ, $\beta_r = 1/n$, $N_и$ = 352, $\beta_{АО} = 0{,}05$, $\beta_{КО} = 0{,}1$. Результаты расчётов приведены в табл. 7.17 – 7.21. До отладки условная и безусловная вероятности практически совпадают, так как $p'' = 5 \cdot 10^{-14}$.

Из данных, приведённых в табл. 7.17, видно, что в начале АО первый дефект уверенно обнаруживается уже после первых 10 – 15 тестов БД. После АО вероятность проявления дефекта снижается, но остаётся довольно высокой (см. табл. 7.19). Вероятность того, что после АО в БД не останется ни одного дефекта, оценивается величиной p'' = 0,48 при выполнении АУ и p'' = 0,23 при выполнении ДУ или ОП.

7.17. Вероятность проявления дефектов БД от отладки

M								
	$v = 2$		$v = 4$		$v = 8$		$v = 16$	
	АУ	ДУ	АУ	ДУ	АУ	ДУ	АУ	ДУ
1	0,1107	0,1107	0,2093	0,2093	0,3748	0,3748	0,6094	0,6094
5	0,4389	0,5585	0,6796	0,6855	0,8901	0,8977	0,9843	0,9881
10	0,6782	0,6848	0,8883	0,8968	0,9834	0,9877	1	1
100	0,9997	0,9999	1	1	1	1	1	1

7.18. Условная вероятность проявления дефектов БД после автономной отладки

M $Q_{БД}(M, v)$								
	$v = 2$		$v = 4$		$v = 8$		$v = 16$	
	АУ	ДУ	АУ	ДУ	АУ	ДУ	АУ	ДУ
1	0,0113	0,0077	0,0225	0,0152	0,0446	0,0301	0,0881	0,0595
5	0,0548	0,0374	0,1063	0,0730	0,2005	0,1396	0,3590	0,2568
10	0,1059	0,0727	0,1990	0,1391	0,3544	0,2551	0,5447	0,4347
100	0,6405	0,4988	0,8545	0,7214	0,9733	0,8982	0,9990	0,9825
1000	0,9998	0,9919	0,9999	0,9999	0,9999	0,9999	0,9999	0,9999

7.19. Безусловная вероятность проявления дефектов БД после автономной отладки

M $Q_{БД}(M, v)$								
	$v = 2$		$v = 4$		$v = 8$		$v = 16$	
	АУ	ДУ	АУ	ДУ	АУ	ДУ	АУ	ДУ
1	0,0059	0,0059	0,0117	0,0117	0,0232	0,0232	0,0458	0,0458
5	0,0285	0,0287	0,0553	0,0562	0,1043	0,1075	0,1867	0,1977
10	0,0551	0,0560	0,1035	0,1071	0,1843	0,1964	0,2989	0,3347
100	0,3331	0,3841	0,4444	0,5555	0,5062	0,6916	0,5196	0,7565
1000	0,5200	0,7638	0,5201	0,7700	0,5201	0,7700	0,5201	0,7700

7.20. Условная вероятность появления дефектов БД после комплексной отладки

M								
	$v = 2$		$v = 1$		$v = 0{,}5$		$v = 0{,}25$	
	АУ	ДУ	АУ	ДУ	АУ	ДУ	АУ	ДУ
1	0,0083	0,0042	0,0041	0,0022	0,0021	0,0232	0,0010	0,0005
5	0,0411	0,0220	0,0206	0,0107	0,0115	0,0059	0,0057	0,0030
10	0,0800	0,0425	0,0411	0,0219	0,0206	0,0107	0,0115	0,0059
100	0,5613	0,5456	0,3379	0,1926	0,1878	0,1020	0,0983	0,0527
1000	0,9996	0,9830	0,9826	0,8695	0,8695	0,6490	0,6419	0,4117

7.21. Безусловная вероятность появления дефектов БД после комплексной отладки

$M(M)$								
	$v = 2$		$v = 1$		$v = 0{,}5$		$v = 0{,}25$	
	АУ	ДУ	АУ	ДУ	АУ	ДУ	АУ	ДУ
1	0,0006	0,0006	$2{,}9\cdot10^{-4}$	$2{,}9\cdot10^{-4}$	$1{,}5\cdot10^{-4}$	$1{,}5\cdot10^{-4}$	$7{,}3\cdot10^{-5}$	$7{,}3\cdot10^{-5}$
10	0,0057	0,0058	$2{,}9\cdot10^{-3}$	0,0030	0,0015	0,0015	0,0008	0,0008
100	0,0397	0,0473	0,0239	0,0263	0,0133	0,0139	0,0070	0,0072
1000	0,0707	0,1342	0,0695	0,1192	0,0615	0,0886	0,0454	0,0562

7.22. Вероятность отказа ФПО и ИО при однократном выполнении ФСО

ФПО		ИО		ФПО + ИО	
		$v = 0{,}25$	$v = 2$	$v = 0{,}25$	$v = 2$
АУ	$2{,}74\cdot10^{-6}$	$7{,}3\cdot10^{-5}$	$5{,}87\cdot10^{-5}$	$7{,}57\cdot10^{-5}$	$5{,}90\cdot10^{-4}$
ДУ	$5{,}96\cdot10^{-6}$	$7{,}3\cdot 10^{-5}$	$5{,}87\cdot10^{-5}$	$7{,}90\cdot10^{-5}$	$5{,}93\cdot10^{-4}$
ОП	$8{,}76\cdot10^{-6}$	$7{,}3\cdot 10^{-5}$	$5{,}87\cdot10^{-4}$	$8{,}18\cdot10^{-5}$	$5{,}96\cdot10^{-4}$

После комплексной отладки, т.е. в начале эксплуатации, вероятность отказа ИО при однократном выполнении ФСО оказывается существенно больше (см. табл. 7.21), чем вероятность отказа ФПО (см. табл. 7.15), – почти на два порядка. При многократном выполнении ФСО в число обращений M включают только независимые обращения. Фактически могут наблюдаться многократные обращения к одному и тому же фрагменту данных, и тогда вероятность проявления дефектов не меняется при увеличении числа обращений. Чтобы учесть этот фактор, введём поправочный коэффициент δ, равный доле независимых обращений. Для данной системы принимается $\delta = 0{,}1$.

Суммарная вероятность отказа ФПО и ИО при однократном выполнении ФСО после комплексной отладки, рассчитанная по схеме независимых событий, приведена в табл. 7.22.

Вероятность отказа существенно зависит от объёма v, используемого при однократном обращении фрагмента БД.

Поток инициирующих событий. В систему поступает несколько потоков инициирующих событий ИС. Поток технологических событий, инициирующих работу ФПО с участием алгоритмов А1...А8, включает в себя только те события, которые требуют взаимосвязанного управления группой технологических параметров. Средний интервал между событиями $T_1 = 8$ ч.

Поток заявок на групповое отображение параметров состоит из заявок, поступающих в среднем один раз в смену, поэтому $T_2 = 8$ ч.

Поток команд с пультов управления и рабочих мест оператора для прямого дистанционного управления исполнительными механизмами и управления режимами работы устройств нижнего уровня имеет средний интервал между событиями $T_3 = 72$ ч.

Поток отказов средств автоматики состоит в основном из отказов 200 дискретных и аналоговых датчиков, имеющих среднюю наработку на отказ 200 тыс. ч, поэтому средний интервал между событиями этого потока $T_4 = 100\,000 / 200 = 500$ ч. Часть этих отказов (их доля 20%) требует вмешательства оперативного персонала с участием подсистемы ДУ. Средний интервал между этими событиями $T_5 = T_4 / 0{,}2 = 2500$ ч.

Интенсивность потоков заявок на выполнение ФСО равна сумме интенсивностей слагаемых потоков

$$\lambda_{\text{АУ}} = \frac{1}{T_1} + \frac{1}{T_5} = \frac{1}{8} + \frac{1}{2500} = 0{,}1254\ \text{ч}^{-1}; \quad T_{\text{АУ}} = \frac{1}{\lambda_{\text{АУ}}} = 7{,}97\ \text{ч}.$$

Для других подсистем

$$\lambda_{\text{ОП}} = \frac{1}{T_1} + \frac{1}{T_2} + \frac{1}{T_3} + \frac{1}{T_4} = 0{,}1266 \text{ ч}^{-1}; \quad T_{\text{ОП}} = \frac{1}{\lambda_{\text{ОП}}} = 3{,}76 \text{ ч}.$$

Вероятность безотказной работы ПК. Система в режиме МКЦП работает со случайными интервалами между циклами. Для безотказной работы системы необходимо безотказное выполнение всех циклов в течение установленного календарного времени. Расчёты проводятся по формуле (7.38) или по приближённым формулам (7.39) или (7.40). Результаты расчётов приведены в табл. 7.23 и 7.24 для времени функционирования $t = 1$ год = 8760 ч и среднего объёма фрагмента данных $v = 0{,}25$ кбайт.

7.23. Интенсивность отказов подсистем

ФСО	$\Lambda_{\text{ФПО}}$	$\Lambda_{\text{БД}}$	$Q_{1,\text{ПО}}$	$Q_{1,1\text{ БД}}$	$\lambda_{\text{НК}} \cdot 10^6$ ФПО	ИО	ФПО + + ИО
АУ	0,1254	0,01254	$2{,}74 \cdot 10^{-6}$	$7{,}3 \cdot 10^{-5}$	0,3440	0,9150	1,259
ДУ	0,0142	0,00143	$5{,}96 \cdot 10^{-6}$	$7{,}3 \cdot 10^{-5}$	0,0852	0,1043	0,1895
ОП	0,2660	0,0266	$8{,}76 \cdot 10^{-6}$	$7{,}3 \cdot 10^{-5}$	2,330	1,942	4,272

7.24. Показатели надёжности подсистем

ФСО	$T_{\text{ср}}$, тыс. ч			$P_c(t)$		
	ФПО	ИО	ФПО + ИО	ФПО	ИО	ФПО + ИО
АУ	2900	1090	794	0,997	0,992	0,989
ДУ	11 700	9586	5277	0,9993	0,9991	0,9983
ОП	429	515	234	0,9798	0,9831	0,9632

7.25. Показатели надёжности подсистем с учётом парирования ошибок в ИО

ФСО	$T_{\text{ср}}$, тыс. ч			$P_c(t)$		
	ФПО	ИО	ФИО + ИО	ФПО	ИО	ФПО + ИО
АУ	2900	10 900	2291	0,997	0,992	0,9962
ДУ	11 700	95 860	5277	0,99925	0,99991	0,99916
ОП	429	5150	396	0,9798	0,9983	0,9781

В подсистемах АУ и ДУ определяющим фактором ненадёжности ПК является вклад информационного обеспечения. Не увеличивая длительности отладки базы данных, можно уменьшить влияние ИО путём введения средств парирования ошибок с вероятностью парирования $p_{\text{ИО}} = 1 - q_{\text{ИО}}$. Результаты расчётов по формуле (7.41) при $q_{\text{И}i} = 1$, $q_{\text{ИО}} = 0{,}1$ приведены в табл. 7.25.

Более высокая вероятность безотказной работы подсистемы ДУ достигнута в основном за счёт существенно меньшей интенсивности потока инициирующих событий. Подсистема ОП имеет худшие показатели, уступая по средней наработке подсистеме АУ более чем в 5 раз. Это допустимо, так как функция отображения параметров не связана непосредственно с управлением технологическим объектом, и поэтому "цена отказа" здесь меньше, чем в подсистемах АУ и ДУ.

7.6. ОЦЕНКА НАДЁЖНОСТИ ПРОГРАММНОГО КОМПЛЕКСА ПО РЕЗУЛЬТАТАМ ОТЛАДКИ И НОРМАЛЬНОЙ ЭКСПЛУАТАЦИИ

В процессе отладки и опытной или нормальной эксплуатации программного комплекса появляется возможность использовать статистические данные об обнаруженных и исправленных ошибках и уточнить проектные оценки надёжности. Для этой цели разработаны модели надёжности, содержащие параметры, точечные оценки которых получают путём обработки результатов отладки и эксплуатации ПК. Модели отличаются друг от друга допущениями о характере зависимости интенсивности появления ошибок от длительности отладки и эксплуатации. Некоторые модели содержат определённые требования к внутренней структуре программных модулей.

Экспоненциальная модель Шумана [32, 33]. Модель основана на следующих допущениях:

общее число команд в программе на машинном языке постоянно;

в начале испытаний число ошибок равно некоторой постоянной величине и по мере исправления ошибок становится меньше; в ходе исправлений программы новые ошибки не вносятся;

интенсивность отказов программы пропорциональна числу остаточных ошибок.

О структуре программного модуля сделаны дополнительные допущения:

модуль содержит только один оператор цикла, в котором есть операторы ввода информации, операторы присваивания и операторы условной передачи управления вперёд;

отсутствуют вложенные циклы, но может быть k параллельных путей, если имеется $k - 1$ оператор условной передачи управления.

При выполнении этих допущений вероятность безотказной работы находят по формуле

$P(t, \tau) = \exp(-C\varepsilon_r(\tau)t) = e^{-t/T}$;

$$\varepsilon_r(\tau) = \frac{E_0}{I} - \varepsilon_и(\tau);\ T = 1\Bigg/\left(C\left(\frac{E_0}{I} - \varepsilon_и(\tau)\right)\right), \qquad (7.42)$$

где E_0 – число ошибок в начале отладки; I – число машинных команд в модуле; $\varepsilon_и(\tau)$ и $\varepsilon_r(\tau)$ – число исправленных и оставшихся ошибок в расчёте на одну команду; T – средняя наработка на отказ; τ – время отладки; C – коэффициент пропорциональности.

Для оценки E_0 и C используют результаты отладки. Пусть из общего числа прогонов системных тестовых программ r – число успешных прогонов; $(n - r)$ – число прогонов, прерванных ошибками. Тогда общее время n прогонов, интенсивность ошибок и наработку на ошибку находят по формулам

$$H = \sum_{i=1}^{r} T_i + \sum_{i=1}^{n-r} t_i;\ \lambda = \frac{n-r}{H};\ T = \frac{1}{\lambda} = \frac{H}{n-r}. \qquad (7.43)$$

Полагая $H = \tau_1$ и $H = \tau_2$, найдём:

$$\hat{\lambda}_1 = \frac{n_1 - r_1}{H_1};\ \hat{\lambda}_2 = \frac{n_2 - r_2}{H_2};\ \hat{T}_1 = \frac{1}{\hat{\lambda}_1};\ T_1 = \frac{1}{\hat{\lambda}_2}, \qquad (7.44)$$

где T_1 и T_2 – время тестирования на одну ошибку. Подставляя сюда (7.42) и решая систему уравнений, получим оценки параметров модели:

$$\hat{E}_0 = \frac{I}{\gamma - 1}(\gamma\varepsilon_и(\tau_1) - \varepsilon_и(\tau_2));\ \hat{C} = 1\Bigg/\left(\hat{T}_1\left(\frac{\hat{E}_0}{I} - \varepsilon_и(\tau_1)\right)\right);\ \gamma = \frac{\hat{T}_1}{\hat{T}_2}. \quad (7.45)$$

Для вычисления оценок необходимо по результатам отладки знать $\hat{T}_1, \hat{T}_2, \varepsilon_и(\tau_1)$, $\varepsilon_и(\tau_2)$. Некоторое обобщение результатов (7.43) – (7.45) состоит в следующем. Пусть T_1 и T_2 – время работы системы, соответствующее времени отладки τ_1 и τ_2; n_1 и n_2 – число ошибок, обнаруженных в периодах τ_1 и τ_2. Тогда

$$\frac{T_1}{n_1} = 1\Bigg/\left(C\left(\frac{E_0}{I} - \varepsilon_и(\tau_1)\right)\right);\ \frac{T_2}{n_2} = 1\Bigg/\left(C\left(\frac{E_0}{I} - \varepsilon_и(\tau_2)\right)\right);$$

$$\hat{E}_0 = \frac{I}{\gamma - 1}(\gamma\varepsilon_и(\tau_1) - \varepsilon_и(\tau_2));\ \hat{C} = \frac{n_1}{T_1}\Bigg/\left(\frac{\hat{E}_0}{I} - \varepsilon_и(\tau_1)\right);\ \gamma = \frac{T_1}{n_1}\Bigg/\frac{T_2}{n_2}. \quad (7.46)$$

Если T_1 и T_2 – только суммарное время отладки, то $T_1 = T_1 / n_1$; $T_2 = T_2 / n_2$, и формула (7.46) совпадает с (7.45). Если в ходе отладки прогоняется k тестов в интервалах $(0, \tau_1)$, $(0, \tau_2)$, ..., $(0, \tau_k)$, где $\tau_1 < \tau_2 < ... < \tau_k$, то для определения оценок максимального правдоподобия используют уравнения

$$\hat{C} = \sum_{j=1}^{k} n_j \Bigg/ \left(\frac{\hat{E}_0}{I} - \varepsilon_и(\tau_j)\right) H_j;\ \hat{C} = \left\{\sum_{j=1}^{k} n_j \Bigg/ \left(\frac{\hat{E}_0}{I} - \varepsilon_и(\tau_j)\right)\right\} \sum_{j=1}^{k} H_j, \quad (7.47)$$

где n_j – число прогонов j-го теста, заканчивающихся отказами; H_j – время, затраченное на выполнение успешных и безуспешных прогонов j-го теста. При k = 2 уравнение (7.47) сводится к предыдущему случаю и решение даёт результат в виде (7.46).

Асимптотическое значение дисперсий оценок (для больших значений n_j) определяются выражениями [34]

$$D\hat{C} \cong 1\Bigg/\left\{\sum_{j=1}^{k} n_j / C^2 - \left(\sum_{j=1}^{k} H_j\right)^2 \Bigg/ \sum_{j=1}^{k}\left(n_j \Bigg/ \left(\frac{E_0}{I} - \varepsilon_и(\tau_j)\right)^2\right)\right\};$$

$$DE_0 \cong I^2\Bigg/\left\{\sum_{j=1}^{k}\left(n_j \Bigg/ \left(\frac{E_0}{I} - \varepsilon_и(\tau_j)\right)^2\right) - C^2\left(\sum_{j=1}^{k} H_j\right)^2 \Bigg/ \sum_{j=1}^{k} n_j\right\};$$

$C \cong \hat{C},\ E \cong \hat{E}_0$.

Коэффициент корреляции оценок

$$\rho(\hat{C},\ \hat{E}_0) \cong \left\{\sum_{j=1}^{k} n_j \middle/ \left(\frac{E_0}{I} - \varepsilon_{и}(\tau_j)\right)\right\} \middle/ \left\{\sum_{j=1}^{k} n_j \sum_{j=1}^{k}\left(n_j \middle/ \left(\frac{E_0}{I} - \varepsilon_{и}(\tau_j)\right)^2\right)\right\}^{0,5}.$$

Асимптотические значения дисперсии и коэффициента корреляции используются для определения доверительных интервалов значений E_0 и C на основе нормального распределения.

Наиболее адекватной для модели Шумана является экспоненциальная модель изменения количества ошибок при изменении длительности отладки

$$\varepsilon_{и}(\tau) = \frac{E_0}{I}(1 - e^{-\tau/\tau_0}),$$

где E_0 и τ_0 определяются из эксперимента. Тогда

$$P(t,\ \tau) = \exp(-CE_0\ /\ Ie^{-\tau/\tau_0}\, t).$$

Средняя наработка до отказа возрастает экспоненциально с увеличением длительности отладки:

$$T = I\ /\ CE_0 e^{\tau/\tau_0}.$$

Экспоненциальная модель Джелинского–Моранды [36, 36]. Данная модель является частным случаем модели Шумана. Согласно этой модели, интенсивность появления ошибок пропорциональна числу остаточных ошибок:

$$\lambda(\Delta t_i) = K_{JM}(E_0 - i + 1),$$

где K_{JM} – коэффициент пропорциональности; Δt_i – интервал между i-й и $(i-1)$-й обнаруженными ошибками. Вероятность безотказной работы

$$P(t) = \exp(-\lambda(\Delta t_i)) = K_{JM}((E_0 - i + 1)t),\ \ t_{i-1} < t < t_i. \qquad (7.48)$$

При $K_{JM} = C / I$ и $\varepsilon_{и}(\tau) = (i-1) / I$ формула (7.48) совпадает с (7.42), при последовательном наблюдении k ошибок в моменты $t_1,\ t_2,\ \ldots,\ t_k$ можно получить оценки максимального правдоподобия для параметров E_0 и K_{JM}. Для этого надо решить систему уравнений

$$\sum_{i=1}^{k}\left(\hat{E}_0 - i + 1\right)^{-1} = k \middle/ \left(\hat{E}_0 - \theta k + 1\right);\ \ \hat{K}_{JM} = \frac{k}{A} \middle/ \left(\hat{E}_0 - \theta k + 1\right);$$

$$\theta = \frac{B}{AK};\ \ A = \sum_{i=1}^{k} t_i;\ \ B = \sum_{i=1}^{k} i t_i. \qquad (7.49)$$

Асимптотические оценки дисперсии и коэффициента корреляции (при больших k) определяются с помощью формул:

$$D\hat{E}_0 \cong \frac{k}{kS_2 - A^2C^2};\ \ D\hat{K}_{JM} \cong \frac{S_2 K_{JM}^2}{kS_2 - A^2 K_{JM}^2};$$

$$\rho(\hat{K}_{JM},\ \hat{E}_0) \cong -\frac{AK_{JM}}{(kS_2)^{0,5}};\ \ S_2 = \sum_{i=1}^{k}(E_0 - i + 1)^{-2}.$$

Чтобы получить численные значения этих величин, надо всюду заменить E_0 и K_{JM} их оценками.

Геометрическая модель Моранды. Интенсивность появления ошибок принимает форму геометрической прогрессии:

$$\lambda(t) = DK^{i-1},\ \ t_{i-1} < t < t_i,\ \ K < 1,$$

где D и K – константы; i – число обнаруженных ошибок. Эту модель рекомендуется применять в случае небольшой длительности отладки. Другие показатели надёжности находят по формулам:

$$P(t) = \exp(-DK^n t);\ \ T = 1\ /\ DK^n,$$

где n – число полных временных интервалов между ошибками. Модификация геометрической модели предполагает, что в каждом интервале тестирования обнаруживается несколько ошибок.

Тогда

$$\lambda(t)=DK^{n_{j-1}};\ \ T=1/DK^{n_m};\ \ P(t)=\exp(-DK^{n_m}t),\quad t_{j-1}<t<t_j,$$

где n_{j-1} – накопленное к началу j-го интервала число ошибок; τ – число полных временных интервалов.

Модель Шика–Волвертона [37, 38] является модификацией экспоненциальной модели Джелинского–Моранды. Модель основана на допущении того, что интенсивность обнаружения ошибок пропорциональна числу остаточных ошибок и длительности i-го интервала отладки

$$\lambda(t)=K_{JM}(E_0-i+1)\,t,\quad t_{i-1}<t<t_{i-1} \qquad (7.50)$$

т.е. с течением времени возрастает линейно. Это соответствует рэлеевскому распределению времени между соседними обнаруженными ошибками. Поэтому модель называют также рэлеевской моделью Шумана или рэлеевской моделью Джелинского–Моранды. Параметр рэлеевского распределения

$$\sigma_0=1\Big/\sqrt{K_{JM}(E_0-n)}\,,$$

где n – число полных временных интервалов.

Тогда вероятность безотказной работы и средняя наработка между обнаруженными ошибками

$$P(t)=\exp\left(\frac{-t^2}{2\sigma_0{}^2}\right)=\exp\left(\frac{-K_{JM}(E_0-n)\,t^2}{2}\right),\quad t_n<t<t_{n+1};$$

$$T=\sqrt{\frac{\pi}{2}}\sigma_0=\sqrt{\frac{\pi}{2K_{JM}(E_0-n)}}\,.$$

Сравнительный анализ моделей показывает, что геометрическая модель Моранды и модель Шика–Волвертона дают устойчиво завышенные оценки числа остаточных ошибок, т.е. оценки консервативные или пессимистические. Для крупномасштабных разработок программ или проектов с продолжительным периодом отладки наилучший прогноз числа остаточных ошибок даёт модель Шика–Волвертона.

Модель Липова [39]. Эта модель является смешанной экспоненциально-рэлеевской, т.е. содержит в себе допущения и экспоненциальной модели Джелинского–Моранды, и рэлеевской модели Шика–Волвертона. Интенсивность обнаружения ошибок пропорциональна числу ошибок, остающихся по истечении $(r-1)$-го интервала времени, суммарному времени, уже затраченному на тестирование к началу текущего интервала, и среднему времени поиска ошибок в текущем интервале времени:

$$\lambda(T_{i-1},\,t_i)=K_L(E_0-i+1)\ (T_{i-1}+t_i/2);\ \ T_{i-1}=\sum_{i=1}^{i-1}t_j;\ \ T_0=0, \qquad (7.51)$$

где t_i – интервал времени между i-й и $(i-1)$-й обнаруженными ошибками.

Здесь имеется и ещё одно обобщение: допускается возможность возникновения на рассматриваемом интервале более одной ошибки. Причём исправление ошибок производится лишь по истечении интервала времени, на котором они возникли:

$$n_{i-1}=\sum_{i=1}^{i-1}M_j,\ \ n_0=0\,.$$

где M_j – число ошибок, возникших на j-м интервале. Из (7.51) находим вероятность безотказной работы и среднее время между отказами:

$$P(t)=\exp\left(-K_L(E_0-n_{i-1})\ (T_{i-1}t+t^2/4)\right),\quad 0\le t\le t_i;$$

$$T=\sqrt{\frac{\pi}{(K_L(E_0-n_{i-1}))}}\left(1-2\Phi\left(T_{i-1}\sqrt{2K_L(E_0-n_{i-1})}\right)\right),$$

где $\Phi(x)$ – интеграл Лапласа; K_L и E_0 – параметры модели.

Параметры модифицированных рэлеевской и смешанной моделей оцениваются с помощью метода максимального правдоподобия. Однако в этом случае функция правдоподобия несколько отличается от рассмотренной при выводе уравнений (7.49), так как теперь наблюдаемой величиной является число ошибок, обнаруживаемых в заданном интервале времени, а не время ожидания каждой ошибки. Предполагается, что обнаруженные на определённом интервале времени ошибки устраняются перед результирующим прогоном. Тогда уравнения максимального правдоподобия имеют вид

$$\hat{C}=\frac{K/A}{\hat{E}_0+1-K\theta};\ \ \frac{K}{\hat{E}_0+1-K\theta}=\sum_{i=1}^{M}\frac{M_i}{\hat{E}_0-n_{i-1}};$$

$$K=\sum_{i=1}^{M} M_i;\ \theta=\frac{B}{AK}, \qquad (7.52)$$

где $C = K_{JM}$ для модели (7.50) и $C = K_J$ для модели (7.51); M – общее число временных интервалов.

Коэффициенты A и B находят с помощью формул:

– для рэлеевской модели

$$A=\sum_{i=1}^{M} t_i;\ B_i=\sum_{i=1}^{M}(n_{i-1}+1)\,t_i\,;$$

– для смешанной модели

$$A=\sum_{i=1}^{M} t_i(T_{i-1}+t_i/2);\ B_i=\sum_{i=1}^{M}(n_{i-1}+1)\,t_i(T_{i-1}+t_i/2)\,.$$

Здесь t_i – продолжительность временного интервала, в котором наблюдаются M_i ошибок. Заметим, что при M_i = 1 уравнения (7.52) приобретают вид (7.49), тогда $M = K$, что соответствует k в (7.49).

Модель Муссы–Гамильтона [40] использует так называемую теорию длительности обработки. Надёжность оценивается в процессе эксплуатации, в котором выделяют время реальной работы процессора (наработку) и календарное время с учётом простоя и ремонта. Для числа отказов (обнаруженных ошибок) выводится формула

$$m(\tau)=E_0\left(1-\exp\left(-\frac{C\tau}{E_0T_0}\right)\right), \qquad (7.53)$$

где T_0 – наработка между отказами перед началом отладки или эксплуатации; E_0 – начальное число ошибок; C – коэффициент пропорциональности. Из (7.53) находят:

$$\lambda(\tau)=\frac{dm(\tau)}{d\tau}=\frac{C}{T_0}\exp\left(-\frac{C\tau}{E_0T_0}\right);$$

$$P(t,\tau)=\exp(-\lambda(\tau)t)=\exp\left(-\frac{C}{T_0}\exp\left(-\frac{C\tau}{E_0T_0}\right)t\right).$$

В работе [47] сравниваются экспоненциальная, рэлеевская и смешанная модели. По результатам анализа сделаны следующие выводы:

1. Экспоненциальная и рэлеевская модели дают более точное предсказание числа ошибок, чем смешанная модель.
2. Экспоненциальная и рэлеевская модели более пригодны для небольших программ или для небольших длительностей отладки.
3. Для больших программ или при длительных испытаниях лучшие результаты дают модификации экспоненциальной и рэлеевской моделей.
4. Геометрическая модель даёт удовлетворительные оценки при любой длине программ, но лучше её использовать для коротких программ и небольшой длительности испытаний.
5. Экспоненциальная и рэлеевская модели завышают число оставшихся ошибок, а смешанная модель занижает эту величину по сравнению с действительным значением.
6. Если для большого числа равных интервалов число ошибок на каждом интервале меняется в значительных пределах, то экспоненциальная и рэлеевская модели могут оказаться неудовлетворительными.

Вейбулловская модель (модель Сукерта) [41]. Задаётся совокупностью соотношений

$$\lambda(t)=m\lambda^m t^{m-1};\ P(t)=e^{-(\lambda t)^m};\ T=\frac{1}{\lambda}\Gamma\left(1+\frac{1}{m}\right).$$

Достоинство этой модели в том, что она содержит дополнительный по сравнению с экспоненциальной моделью параметр τ. Подбирая τ и X, можно получить лучшее соответствие опытным данным. Значение m подбирают из диапазона 0 < τ < 1. Оценки параметров получают с помощью метода моментов. Для параметра формы значение находят как решение уравнения:

$$\Gamma\left(1+\frac{2}{m}\right)\Big/\Gamma^2\left(1+\frac{1}{m}\right)=\frac{s^2}{\bar t^{\,2}};\ \bar t=\frac{1}{k}\sum_{i=1}^{k}t_i;\ s^2=\frac{1}{k}\sum_{i=1}^{k}(t_i-\bar t)^2,$$

где $\Gamma(x)$ – гамма-функция. Для параметра масштаба оценка

$$\hat{\lambda} = \Gamma\left(1 + 1/\hat{m}\right) \Big/ \bar{t}.$$

Модель Уолла–Фергюссона (степенная модель) [42]. Число обнаруженных и исправленных ошибок определяется с помощью степенной зависимости

$$\varepsilon_{\text{и}} = \varepsilon_0 \left(\frac{M}{M_0}\right)^{\alpha},$$

где M – степень отлаженности программ; M_0 и ε_0 – эмпирические константы. Отсюда интенсивность отказов

$$\lambda(M) = \frac{d\varepsilon_{\text{и}}(M)}{Md\tau} = R_0 (M / M_0)^{\alpha - 1}, \; R_0 = \alpha\varepsilon_0, \; \alpha < 1; \qquad (7.54)$$

Величина M выражается в человеко-месяцах испытаний, единицах календарного времени и т.д. Адекватность модели проверена на экспериментальных данных, полученных для систем реального времени и программ на алгоритмическом языке FORTRAN. Для грубого предсказания надёжности авторы рекомендуют значение $a = 0{,}5$.

Во всех рассмотренных моделях программа представлена как "черный ящик", без учёта её внутренней структуры. Кроме того, всюду принято допущение, что при исправлении ошибок новые ошибки не вносятся. Следующие две модели рассматривают программы в виде "белого ящика" – с учётом внутренней структуры. Поэтому они называются структурными.

Структурная модель Нельсона [43]. В качестве показателя надёжности принимается вероятность $P(n)$ безотказного выполнения n прогонов программы. Для j-го прогона вероятность отказа представляется в виде

$$Q_j = \sum_{i=1}^{N} p_{ji} y_i,$$

где y_i – индикатор отказа на i-м наборе данных; p_{ij} – вероятность появления i-го набора в j-м прогоне.

Тогда

$$P(n) = \prod_{j=1}^{n} (1 - Q_j) = \exp\left(\sum_{j=1}^{n} \ln(1 - Q_j)\right).$$

Если Δt_j – время выполнения j-го прогона, то интенсивность отказов

$$\lambda(t_j) = \frac{-\ln(1 - Q_j)}{\Delta t_j}; \; P(n) = \exp\left(\sum_{j=1}^{n} \lambda(t_j)\Delta t_j\right); \; \Delta t_j = \sum_{i=1}^{j} \Delta t_i. \quad (7.55)$$

Практическое использование формул (7.54) и (7.55) затруднено из-за множества входов и большого количества трудно оцениваемых параметров модели. На практике надёжность программ оценивается по результатам тестовых испытаний, охватывающих относительно небольшую область пространства исходных данных.

Для упрощённой оценки можно воспользоваться формулой

$$P(N) = \frac{1}{N} \sum_{i=1}^{N} E_i(n_i) W_i; \; \sum_{i=1}^{N} W_i = N,$$

где N – число прогонов; m – число обнаруженных при прогоне i-го теста ошибок; E_i – индикатор отсутствия ошибок при прогоне i-го теста.

Для уменьшения размерности задачи множество значений входных наборов разбивают на пересекающиеся подмножества G_j, каждому из которых соответствует определённый путь L_j, $j = 1 \ldots n$. Если L_j содержит ошибки, то при выполнении теста на поднаборе G_j будет отказ. Тогда вероятность правильного выполнения одного теста

$$P(1) = 1 - \sum_{j=1}^{n} p_j \varepsilon_j, \; p_j = \sum_{i \in G_j} p_{ij}, \; \varepsilon_j < 1.$$

При таком подходе оценка надёжности по структурной модели затруднена, так как ошибка в L_j проявляется не при любом наборе из G_j, а только при некоторых. Кроме того, отсутствует методика оценки по результатам испытаний программ.

Структурная модель роста надёжности (модель Иыуду) [45]. Модель является развитием модели Нельсона. В ней делают следующие допущения:

исходные данные входного набора выбираются случайно в соответствии с распределением p_i, $i = 1 \ldots n$;

все элементы программ образуют s классов, вероятность правильного исполнения элемента l-го класса равна p_l, $l = 1 \ldots s$;

ошибки в элементах программ независимы.

Вероятность правильного исполнения программы по i-му пути

$$P_i = \prod_{l=1}^{s} p_l^{m_{li}}, \qquad (7.56)$$

где m_{li} – количество элементов l-го класса в i-м пути. Безусловная вероятность безотказной работы при однократном исполнении программы в период времени до первой обнаруженной ошибки

$$P_{c0} = \sum_{i=1}^{n} \beta_i P_i; \ \sum_{i=1}^{n} \beta_i = 1, \qquad (7.57)$$

где n – количество путей исполнения программы.

При корректировании программы после обнаружения ошибки учитывается возможность внесения новой ошибки с помощью коэффициента эффективности корректирования q_l. Вместо p_l в (7.56) следует использовать

$$p_{lj} = 1 - (1 - p_{l0}) q_l^{j-1}, \ \ j \ge 1,$$

где j – номер интервала времени между соседними ошибками.

При q_l =1 вероятность P_{lj} не меняется, при $q_l < 1$ вероятность увеличивается, а при $q_l > 1$, напротив, падает. Для j-го интервала вероятность успешного исполнения программы по i-му пути

$$P_{ij} = \prod_{l=1}^{s} (1 - (1 - p_{l0})\, q_l^{\,j-1})^{m_{li}} \cong 1 - \sum_{l=1}^{s} m_{li} (1 - p_{l0})\, q_l^{\,j-1} .$$

При $q_l = q$ выражение (7.57) можно представить в виде

$$P_{ij} \cong 1 - (1 - P_{i0})\, q^{j-1}, \ P_{i0} = \sum_{l=1}^{s} m_{li} (1 - P_{i0}) . \qquad (7.58)$$

Подставляя (7.58) в (7.57), получим:

$$P_{cj} = 1 - (1 - P_{c0})\, q^{j-1}, \ P_{c0} = \sum_{i=1}^{n} \beta_i P_{i0} . \qquad (7.59)$$

Если наиболее вероятные пути проверены, то

$$P_{c0} = \sum_{i:\, \beta_i \ge \varepsilon} \beta_i + \sum_{i:\, \beta_i < \varepsilon} \beta_i \prod_{l=1}^{s} p_{i0}{}^{m_{lj}} .$$

В формуле (7.59) параметры P_{c0} и q можно оценить по экспериментальным данным. Для плана испытаний, в котором определяются значения n_j – числа прогонов между j-м и $(j-1)$-м отказами, $j = 1 \ldots r$, с помощью метода максимального правдоподобия найдём уравнения относительно искомых оценок:

$$\sum_{j=1}^{r} \frac{(n_j - 1)\, q^{j-1}}{1 - Q_{c0} q^{j-1}} - \frac{r}{Q_{c0}} = 0, \ Q_{c0} = 1 - P_{c0}, \ r \ge 2;$$

$$\sum_{j=1}^{r} \frac{(n_j - 1)\, Q_{c0}}{1 - Q_{c0} q^{j-1}} - \frac{r(r-1)}{2q} = 0.$$

В частности, при $r = 2$ имеем:

$$\hat{Q}_{c0} = \frac{1}{n_1}; \ \hat{q} = \frac{n_1}{n_2}.$$

Гиперболическая модель роста надёжности [46]. Пусть P_k – вероятность безотказной работы во время k-го цикла испытаний, P_∞ – установившееся значение вероятности. Тогда кривую роста надёжности можно аппроксимировать с помощью гиперболической зависимости

$$P_k = P_\infty - \frac{\alpha}{k},$$

где α – скорость роста кривой; k – номер цикла.

Оценки параметров P_∞ и α можно получить методом максимального правдоподобия. Для этого организуют испытания по циклам, в каждом из которых выполняют фиксированное число прогонов: n_1, n_2, ..., n_N. Число успешных прогонов X_k из общего количества n_k имеет биномиальное распределение с параметрами n_k и P_k. Тогда функция максимального правдоподобия:

$$L=\sum_{k=1}^{N} s_k \ln P_k+(n_k-s_k)\ln(1-P_k);\ \ P_k=P_\infty-\frac{\alpha}{k},$$

где s_1, s_2, ..., s_n – фактическое количество успешных прогонов в циклах. Приведём уравнения максимального правдоподобия

$$\begin{aligned}\frac{\partial L}{\partial P_\infty}&=\sum_{k=1}^{N}\frac{s_k}{P_\infty-\alpha/k}-\sum_{k=1}^{N}\frac{n_k-s_k}{1-P_\infty+\alpha/k}=0;\\ \frac{\partial L}{\partial \alpha}&=\sum_{k=1}^{N}\frac{s_k/k}{P_\infty-\alpha/k}-\sum_{k=1}^{N}\frac{(n_k-s_k)/k}{1-P_\infty+\alpha/k}=0.\end{aligned} \qquad (7.60)$$

Систему алгебраических уравнений (7.60) решают методом итераций. Однако при $(1 - P_\infty) < \alpha / k$ можно найти приближённое решение:

$$\hat{\alpha}=\frac{1}{\bar{n}}\left(\sum_{k=1}^{N}ks_k-\frac{N+1}{2}\sum_{k=1}^{N}s_k\right)\Bigg/\left(\frac{N+1}{2}C_1-N\right),\quad \bar{n}=\frac{1}{N}\sum_{k=1}^{N}n_k;$$

$$\hat{P}_\infty=\frac{1}{\bar{n}}\left(\frac{C_1}{n}\sum_{k=1}^{N}ks_k-\sum_{k=1}^{N}s_k\right)\Bigg/\left(\frac{N+1}{2}C_1-N\right),\ \ C_1=\sum_{k=1}^{N}\frac{1}{k}\approx\ln(N+0,5)+E,$$

(7.61)

где E = 0,577215 – постоянная Эйлера. Если указанное условие не выполняется, то оценки (7.61) можно использовать как начальное приближение в итерационной процедуре.

Оценки параметров можно получить и с помощью метода наименьших квадратов. Для этого надо найти значения P_∞ и α, которые обеспечат минимум выборочной дисперсии:

$$S^2=Q(P_\infty,\alpha)=\sum_{k=1}^{n}\left(\hat{P}_k-P_k\right)^2=\sum_{k=1}^{n}\left(\frac{s_k}{n_k}-P_\infty+\frac{\alpha}{k}\right)^2=\min.$$

Дифференцируя эту функцию по P_∞ и α, получим систему уравнений:

$$A-NP_\infty+\alpha C_1=0;\ \ B-C_1P_\infty+C_2\alpha=0;$$

$$A=\sum_{k=1}^{n}\frac{s_k}{n_k};\ \ B=\sum_{k=1}^{n}\frac{s_k}{kn_k};\ \ C_1=\sum_{k=1}^{N}\frac{1}{k};\ \ C_2=\sum_{k=1}^{N}\frac{1}{k^2}.$$

Отсюда найдём решение:

$$\hat{P}_\infty=\frac{AC_2-BC_1}{NC_2-C_1^2};\ \ \hat{\alpha}=\frac{AC_1-BN}{NC_2-C_1^2}. \qquad (7.62)$$

Эти оценки являются несмещёнными. Оценки (7.62) можно использовать для нахождения хороших начальных значений оценок максимального правдоподобия.

Вопросы для самоконтроля

1. В чём состоят постановка задачи и этапы проектной оценки надёжности программного обеспечения (ПО)?
2. Перечислите факторные модели в проектной оценке надёжности ПО, их содержание и применение.
3. Каков порядок проектной оценки надёжности ПО?
4. Назовите варианты моделей оценки надёжности программ по результатам их отладки. Сравните эти модели. Приведите перечень необходимых для расчётов исходных данных.
5. Какие существуют структурные модели оценки надёжности программ по результатам испытаний?

8. ПРАКТИЧЕСКИЕ МЕТОДЫ СТАТИСТИЧЕСКОЙ ОЦЕНКИ НАДЁЖНОСТИ

8.1. РОЛЬ ЭКСПЕРИМЕНТА В ОЦЕНКЕ НАДЁЖНОСТИ

Роль эксперимента в оценке надёжности огромна. Достаточно сказать, что эксперимент (в частности, статистический эксперимент) является единственным источником объективной информации о надёжности. Только эксперимент (в реальной или опытной эксплуатации, а также при специальных испытаниях аппаратуры) позволяет получить показатели надёжности элементов, необходимые для теоретического расчёта надёжности систем. Не имея же данных о надёжности элементов, невозможно рассчитать надёжность системы, а в этой ситуации становится бесполезным любой теоретический анализ моделей надёжности.

Однако эксперимента с элементами системы (первичного эксперимента) для оценки надёжности недостаточно. Проводимые на этапе проектирования теоретические расчёты, обладая тем бесспорным достоинством, что они позволяют оценить надёжность систем ещё до их изготовления, являются всё же прогнозом, содержащим даже при абсолютно достоверной информации о надёжности элементов большую или меньшую методическую погрешность. Наличие этой погрешности объясняется двумя причинами:

1) несовершенством математической модели надёжности, так как в ней отражаются не все, а лишь наиболее существенные факторы, влияющие на надёжность;

2) нарушениями в реальной системе (хотя и небольшими в хорошей модели) тех допущений, которые приняты в процессе формирования математической модели надёжности.

Поэтому для подтверждения прогнозируемых теоретическим расчётом показателей надёжности систем необходим вторичный эксперимент над опытными образцами изделия или их макетами. Вторичный эксперимент имеет некоторые особенности по сравнению с первичным экспериментом.

Элементы обычно обладают высокими показателями надёжности (средняя наработка до отказа равна десяткам, сотням тысяч и даже миллионам часов). Однако их производство, как правило, является массовым, и поэтому имеется принципиальная возможность проводить испытания большого числа элементов. В системах количество испытываемых образцов исчисляется десятками, реже сотнями. В высоконадёжных изделиях, где применено глубокое структурное резервирование, для получения хороших оценок надёжности необходимо длительное наблюдение, иначе оценки могут значительно отличаться от реальных показателей надёжности.

Часто не удаётся собрать статистику об отказах малосерийных и уникальных изделий в течение всей их жизни до морального старения. Поэтому иногда ставят под сомнение необходимость теоретических расчётов для таких систем, так как их результаты не удаётся подтвердить экспериментально.

Противоположная точка зрения, согласно которой теоретические расчёты необходимы и для уникальных систем, основана на том, что последние обычно содержат большое число элементов, что позволяет получить хорошие экспериментальные оценки надёжности входящих в систему блоков и устройств. Кроме того, при наличии достоверной информации о надёжности блоков и устройств совершенствование математической модели позволяет снизить методическую погрешность до довольно низкого уровня. При этом по мере усложнения модели необходимо широкое применение методов статистического моделирования.

8.2. КЛАССИФИКАЦИЯ МЕТОДОВ СТАТИСТИЧЕСКИХ ИСПЫТАНИЙ НАДЁЖНОСТИ

Статистические данные об отказах изделий можно получить в результате наблюдений за изделиями в нормальной или опытной (подконтрольной) эксплуатации либо в результате стендовых испытаний.

Наблюдения в *нормальной эксплуатации* – самый дешёвый способ получении экспериментальных данных о надёжности. Сведения об отказах (времени, месте, причине отказа, времени устранения, наработке между отказами, условиях эксплуатации и пр.) оформляются на местах эксплуатации оперативно-ремонтным персоналом в документах стандартной формы, собираются в центре сбора и обработки данных и обрабатываются по определённым алгоритмам. Достоинством этого способа является также то, что получаемые данные относятся к реальным системам. Недостатки способа – существенное запаздывание данных, затрудняющее их использование при проведении работ по повышению надёжности, ограниченные возможности активного эксперимента, повышенное влияние субъективного фактора, так как в сборе сведений на местах участвуют не представители служб надёжности, а оперативно-ремонтный персонал.

В *опытной эксплуатации* наблюдения за работоспособностью изделий проводятся с участием представителей служб надёжности, имеющих специальную подготовку, что позволяет проводить эксперименты по единой методике, в том числе и некоторые активные эксперименты в специальных режимах эксплуатации (повышенный уровень помех, введение искусственных отказов и пр.). При этом снижается роль субъективного фактора. Однако, как и в первом случае, возможности активного планирования испытаний ограничены. Кроме того, для сбора сведений необходимо в течение длительного времени задействовать на местах эксплуатации довольно большой штат сотрудников служб надёжности.

Стендовые испытания являются централизованными и проводятся либо на заводах-изготовителях, либо на предприятиях-разработчиках систем. Это весьма дорогостоящий вид испытаний, осуществляемый к тому же не в реальных, а в имитируемых условиях эксплуатации.

Кроме того, в течение всего периода испытаний, как правило, не удаётся использовать системы по назначению. Однако это едва ли не единственная возможность своевременно получить информацию о недостатках схемных решений, конструкции и технологии и применить её для совершенствования технической документации системы и повышения её надёжности. Стендовые испытания позволяют проводить активные эксперименты (в режимах, допускающих выявление слабых мест системы, в "пиковых" режимах, редких или недопустимых при нормальной эксплуатации и пр.) и ускоренные испытания.

Испытания надёжности можно классифицировать не только по виду, но и по ряду других признаков. По типу отказов различают испытания на *внезапные отказы*, на *постепенные отказы* и *комплексные испытания*.

По назначению испытания бывают определительные и контрольные [53].

Определительные испытания предназначены для выявления фактического уровня показателей надёжности. Их результаты не только имеют значение для испытываемой партии изделий, но могут иметь и более широкое применение.

Контрольные испытания предназначены для того, чтобы установить соответствие фактических характеристик надёжности конкретной партии изделий заданным требованиям. При этом фактический уровень надёжности количественно не определяется и результаты контрольных испытаний имеют значение лишь для испытываемой партии изделий.

По объёму выборки различают испытания с полной и усечённой выборкой.

Испытания с полной выборкой проводятся до полного "выжигания" – до отказа всех испытываемых изделий. При *усечённой выборке* часть образцов может проработать безотказно до конца испытаний.

При планировании обычных испытаний необходимо установить:

признаки отказов изделия (все состояния изделия, связанные с отказами отдельных элементов, относят к одному из двух классов – работоспособные и неработоспособные – и таким образом определяют сложное событие "отказ системы");

показатель надёжности, который является главным для данного изделия (в зависимости от назначения изделия и требований к надёжности таким показателем может быть вероятность отказа или вероятность безотказной работы, интенсивность отказов, наработка на отказ, коэффициент готовности и др.);

условия испытаний (электрические режимы, климатические условия, механические нагрузки, последовательность и длительность решения информационных, информационно-расчётных и расчётных задач);

способ контроля работоспособности (либо внутренний контроль, т.е. с помощью средств, предусмотренных для нормальной эксплуатации, либо внешний с помощью средств, предназначенных специально для испытаний, либо комбинированный (внутренний и внешний); по времени работы системы контроля различают контроль непрерывный и периодический с заданным периодом включения;

способ замены отказавших изделий, здесь возможны следующие стратегии: отказавшие изделия не заменяются до конца испытаний (план типа *Б*), заменяются немедленно после отказа (план типа *В*), группою после того, как количество отказавших изделий достигнет заданного уровня (план *Б*, *В*), и т.д.;

количество испытываемых изделий N;

правило окончания испытаний. Здесь возможны следующие варианты планирования: испытания заканчиваются по истечении заданного времени T, после r-го отказа, после отказа всех изделий, в момент времени $T_и = \min(T, T_r)$, где T_r – момент r-го отказа.

Для обозначения планов испытаний будем применять символику с тремя позициями: количество испытываемых изделий, способ замены отказавших изделий, правило окончания испытаний. Возможны такие планы: [N, *Б*, T]; [N, *В*, 7]; [N, *Б*, r]; [N, *В*, r]; [N, *Б*, (T, r)]; [N, *В*, (T, r)] и др.

Чаще всего применяются следующие четыре типа плана:

план [N, *В*, T], испытываются n элементов, каждый отказавший элемент заменяется новым, испытания проводятся в течение фиксированного времени;

план [N, *Б*, T], испытываются n элементов, отказавший элемент выводится из наблюдения, испытания проводятся в течение фиксированного времени τ;

план [N, *В*, r], испытываются n элементов, каждый отказавший элемент заменяется новым, испытания проводятся до получения r-го отказа;

план [N, *Б*, r], испытываются n элементов, отказавший элемент выводится из наблюдения, испытания проводятся до получения r-го отказа.

Для ускорения испытаний выбирается "модель подобия", обеспечивающая определённые пропорции результатов испытаний при реальных и некоторых искусственно созданных условиях и позволяющая установить количественные связи между результатами реальных и ускоренных испытаний с помощью коэффициента ускорения (коэффициента подобия) $K_у$. Чаще всего ускорение обеспечивают ужесточением климатических условий функционирования (температуры, давления, влажности и пр.) и увеличением коэффициента электрической или механической нагрузки $K_н$. Из данных, приведённых в табл. 8.1, следует, что с помощью этих факторов можно добиться ускорения в 10 ... 100 раз и более по сравнению с реальными условиями (30°C, $K_н = 1$).

8.1. Ускорение испытаний с помощью температуры (750°C) и коэффициента нагрузки

Элементы	Коэффициент ускорения			
	$K_н = 1$	$K_н = 1,3$	$K_н = 1,7$	$K_н = 2,0$
Резисторы	2,2	3,8	5,0	7,5
Конденсаторы	3,0	8,2	27	67
Диоды германиевые	27	45	89	134

Для экспоненциального распределения наработки коэффициент подобия трактуется как отношение интенсивностей отказов элементов в условиях ускоренных испытаний и в реальных условиях. Если принять неизменным среднее ожидаемое количество отказов за время испытаний, то при ускоренных испытаниях можно сократить время испытаний обратно пропорционально коэффициенту подобия: $T_у = T / K_у$. Основной областью применения ускоренных испытаний следует считать испытания элементов в реальных условиях и простых модулей.

8.3. ЗАДАЧИ ОПРЕДЕЛИТЕЛЬНЫХ ИСПЫТАНИЙ

Задачи определительных испытаний существенно зависят от выбора оцениваемой характеристики и от наличия априорных сведений о надёжности изделий. Среди характеристик безотказности наибольший интерес представляют вероятность отказа и функция распределения наработки до отказа. При оценке вероятности отказа и других показателей безотказности наиболее удобны планы типа *Б*, так как они позволяют найти эмпирическую функцию распределения. При планах типа *В* по результатам испытаний непосредственно определяются статистические оценки наработки между отказами и параметры потока отказов. Чтобы по этим данным найти оценки показателей безотказности, требуются дополнительные и довольно сложные расчёты. Однако при планах типа *В* можно дать оценку коэффициента готовности. Существует только один случай, когда характеристики безотказности и характеристики потока отказов удобно оценивать по одному и тому же плану (*Б* или *В*). Это случай, когда закон распределения наработки известен заранее и он экспоненциальный. Тогда интенсивность отказов совпадает с параметром потока отказов, так что одновременно получается и характеристика безотказности, и характеристика потока отказов.

Рассмотрим теперь, как выбирается длительность испытаний.

С точки зрения полноты информации наиболее желательным является план [*N*, *Б*, *N*], так как только в этом случае удается полностью построить эмпирическую функцию распределения. Однако длительность этих испытаний, в особенности для высоконадёжных изделий, оказывается неприемлемо большой, во многих случаях она исчисляется многими тысячами часов. Стремление ограничить длительность испытаний приводит к планам типа [*N*, *Б*, *T*], [*N*, *Б*, *r*] и др.

Но при использовании любого из этих планов известна лишь часть эмпирической функции для $t < T$ или T_r. Возможности распространения результатов испытаний для значений $t > T$ или T_r зависят от априорной информации и от свойств получаемых статистических данных. От них же существенно зависит также способ обработки данных с помощью методов математической статистики. По этим признакам можно выделить следующие три задачи определительных испытаний, возникающие на стадии обработки данных и расположенные здесь в порядке их усложнения.

Задача 1. Вид функции распределения $F(t)$ наработки до первого отказа известен. По результатам испытаний необходимо лишь определить параметры этого распределения. Например, пусть в результате теоретических исследований и последующей экспериментальной проверки показано, что для изделий определённого типа закон распределения наработки экспоненциальный, т.е. $F(t) = 1 - \exp(-\lambda t)$,тогда необходимо оценить лишь параметр *X*. При некоторых других распределениях оценивают два параметра: t и σ – при нормальном; m и λ – при распределении Вейбулла; k, λ – при гамма-распределении. Параметры оценивают методами параметрической статистики. При этом допустимо проведение испытаний в течение времени $T < t_з$ – заданного времени эксплуатации изделия в реальных условиях, так как после определения параметров распределения можно прогнозировать вероятность отказа и для любого $t_з > T$ (рис. 8.1).

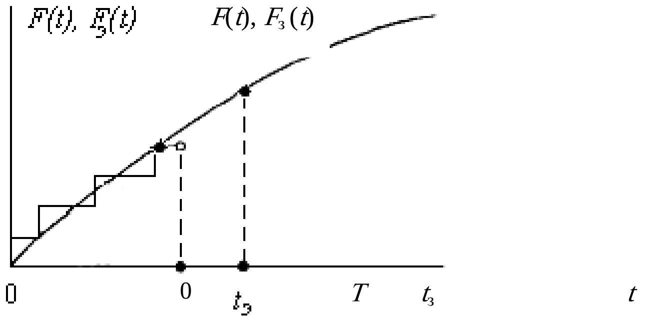


Рис. 8.1. Прогнозирование вероятности отказа по результатам испытаний

Задача 2. Вид функции распределения $F(t)$ заранее неизвестен. Однако результаты испытаний показывают, что эмпирические функции распределения можно плавно аппроксимировать стандартными распределениями или их суперпозициями. Кроме того, из предварительной обработки экспериментальных данных видно, что качественный характер поведения эмпирических функций распределения и гистограмм не меняется от партии к партии. В таких случаях говорят, что статистика однородна. Например, две гистограммы, полученные для различных партий изделий, имеют выраженную асимметрию и одномодальны (рис. 8.2, *а*) либо имеют вид монотонно убывающих ступенчатых функций (рис. 8.2, *б*).

В этом случае необходимо выполнить следующие действия по обработке данных:

выбрать одно из возможных семейств теоретических распределений, качественное поведение которых соответствует экспериментальным данным (например, логарифмически нормальное (рис. 8.2, *а*), и экспоненциальное (рис. 8.2, *б*));

наилучшим образом подобрать параметры распределения, пользуясь, например, методом максимального правдоподобия или его частным случаем – методом наименьших квадратов;

имея точечные оценки параметров, проверить согласие теоретического и экспериментального распределений по критериям согласия математической статистики (критерию χ-квадрат, Колмогорова, Мизеса и др.);

если проверка по критериям согласия дала положительный результат, то можно переходить к решению задачи 1, чтобы найти другие оценки; если же ответ отрицательный, то нужно повторить все действия для другого теоретического распределения, точнее описывающего экспериментальные данные. В случае, когда два распределения дают одинаково хорошие результаты, для дальнейшего применения выбирают то из них, для которого можно предложить теоретическое обоснование.

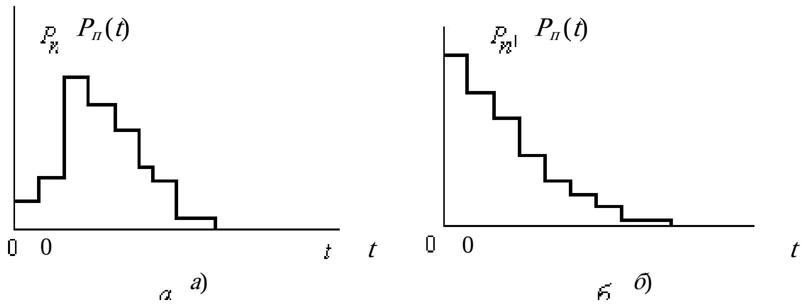


Рис. 8.2. Типовые гистограммы результатов испытаний

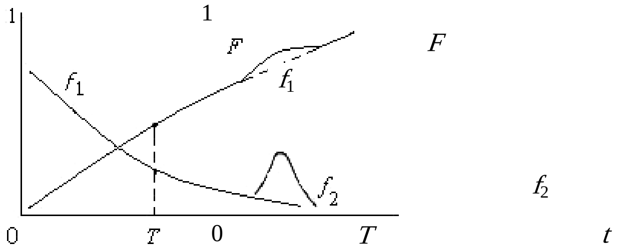


Рис. 8.3. Суперпозиция распределений и планирование испытаний

Использование в условиях задачи 2 результатов эксперимента, проведённого за ограниченное время для получения оценок показателей надёжности при $t_з$, большем длительности испытаний, вообще говоря, неправомерно. Для этого необходимы, по крайней мере, косвенные подтверждения того, что при увеличении длительности испытаний не изменится качественно вид функции распределения, например, к экспоненциальной составляющей функции распределения не добавится нормальная составляющая (рис. 8.3). Таким косвенным подтверждением могут быть результаты длительных испытаний небольших партий изделий или результаты длительной эксплуатации аппаратуры, построенной из тех же элементов. Если не удаётся получить даже косвенного подтверждения, то испытания надо проводить в течение времени, равного времени эксплуатации $t_з$. Тогда вообще может не возникнуть потребность в определении вида функции распределения.

В случае, когда вид функции $F(t)$ неизвестен и статистические данные неоднородны, т.е. качественный вид эмпирической функции распределения и гистограмма меняются от партии к партии, прежде всего необходимо выяснить значимость расхождений, используя методы непараметрической статистики (например, критерий знаков или критерий Вилкоксона).

Если проверка подтвердит значимость расхождений, тогда необходимо выяснить и устранить причины неоднородности, после чего обработка статистических данных проводится, как в задаче 2. Далее для определительных испытаний будут рассмотрены преимущественно задачи первого типа, а из задач второго типа – лишь одна: оценка вероятности отказа при неизвестном законе распределения наработки.

8.4. ОЦЕНКА ВЕРОЯТНОСТИ ОТКАЗА ПО БИНОМИАЛЬНОМУ ПЛАНУ. ТОЧЕЧНАЯ ОЦЕНКА. ДОВЕРИТЕЛЬНЫЕ ИНТЕРВАЛЫ

Пусть для некоторых изделий с неизвестной функцией распределения наработки до первого отказа определяющим показателем надёжности является вероятность отказа изделия $Q(t)$ в течение времени t. Как было показано в предыдущем разделе, в таких условиях прогнозирование вероятности отказа в течение времени, превышающего время испытаний, невозможно. Поэтому выбираем план [N, $Б$, t], где длительность испытаний T равна времени эксплуатации изделия t. Устанавливая на испытания N одинаковых изделий и проверяя их работоспособность через время t, определяем число отказавших изделий $т$. Тогда точечной оценкой вероятности отказа является частота $Q(t) = m(t) / N$.

Согласно закону больших чисел, при увеличении N точечная оценка $Q(t)$ сходится по вероятности к оцениваемой $Q(t)$. Следует, однако, отметить, что при испытаниях надёжности далеко не всегда удаётся установить большое число изделий. Кроме того, для высоконадёжных изделий $Q(t)$ обычно очень мало. В этих условиях дисперсия оценки получается неприемлемо большой и точечная оценка становится неудовлетворительной. Поэтому кроме точечной оценки используют *доверительные интервалы.*

Абсолютно достоверными границами для неизвестной вероятности $Q(t)$ являются 0 и 1. Всякое сужение интервала (0, 1) связано с риском совершить ошибку, состоящую в неверном заключении о том, что $Q(t)$ находится между новыми границами. В зависимости от того, как происходит сужение интервала (0, 1), различают двусторонний и односторонние интервалы.

Двусторонним доверительным интервалом для неизвестной и неслучайной величины вероятности $Q(t)$ называют интервал ($Q_н$, $Q_в$) со случайными границами, зависящими от исхода статистического эксперимента и такими, что вероятность покрытия этим интервалом неизвестного числа $Q(t)$ не меньше заданной вероятности δ, называемой доверительной вероятностью или коэффициентом доверия: $P(Q_н \le Q \le Q_в)$.

Вероятность противоположного события, т.е. того, что $Q(t)$ окажется в интервале (0, $Q_н$) или ($Q_в$, 1), называется уровнем значимости γ и равна $1-\delta$. Уровень значимости можно представить в виде суммы вероятностей:

$$\gamma = \gamma' + \gamma'' = P(0 < Q < Q_н) + P(Q_в < Q < 1).$$

Обычно γ' и γ'' выбирают одинаковыми, так что $\gamma' = \gamma'' = \gamma / 2 = (1 - \delta) / 2$.

Односторонними (*верхним* и *нижним*) *доверительными интервалами* называют соответственно интервалы $(0,\ Q_в)$ и $(Q_н,\ 1)$ – такие, что $P(0 < Q < Q_в) \geq \delta$; $P(Q_н < Q < 1) \geq \delta$.

Здесь уровень значимости $\gamma = 1 - \delta$ выражает вероятность того, что число $Q(t)$ попадёт в интервал$(Q_в,\ 1)$ при верхнем интервале и в интервал $(0,\ Q_н)$ – при нижнем.

Доверительную вероятность нельзя выбирать слишком малой, так как снижается доверие к полученным границам и увеличивается риск сделать неверное заключение. Нельзя выбирать её и слишком близкой к единице, так как чем ближе δ к единице, тем шире границы для неизвестной вероятности. Опыт использования статистических методов показывает, что для практических целей достаточно брать δ из диапазона 0,8 ... 0,95. Иногда коэффициент доверия увеличивают до значения 0,98 или 0,99.

Правила вычисления $Q_н$ и $Q_в$ были предложены в начале 30-х годов XX в. английскими статистиками К. Клогшером и Э. Пирсоном [1]. Поскольку испытания различных образцов одного и того же изделия происходят независимо друг от друга, число *т* отказавших за время *t* изделий распределено по биномиальному закону с параметрами *N* и *Q*, т.е. вероятность отказа ровно *m* изделий из *N* определяется формулой:

$$P\xi = m = C_N^m Q^m (1 - Q)^{N-m}.$$

Вероятность же отказа не более *т* изделий равна:

$$P\xi \leq m = B(m,\ Q,\ N) = \sum_{i=0}^{m} C_N^i Q^i (1 - Q)^{N-i}. \qquad (8.1)$$

Здесь *m* – варианта, а *N* и *Q* – параметры распределения. Функция (8.1) является ступенчатой функцией *m*, изменяющейся от нуля до единицы при увеличении *m* от нуля до *N*. Если построить семейство распределений *у* при одном и том же *N*, но различных *Q*, и для удобства изображения сгладить ступенчатые функции непрерывными кривыми, то получим семейство зависимостей, приведённое на рис. 8.4.

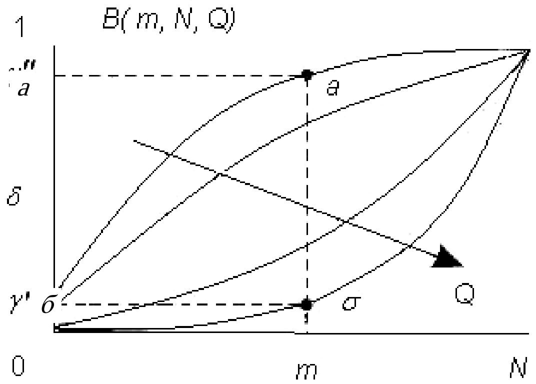


Рис. 8.4. Определение доверительных границ параметра биномиального распределения с помощью принципа Клоппера–Пирсона

В этом семействе параметр *Q* увеличивается в направлении, указанном стрелкой. Если теперь провести перпендикуляр через точку *т*, где *т* – наблюдаемое при испытаниях число отказов, и две горизонтальные прямые на уровне γ' и $1 - \gamma''$, а затем подобрать две кривые семейства, которые проходили бы через точки пересечения *а* и *б*, то параметры этих кривых и дают нижнюю и верхнюю доверительные границы с коэффициентом доверия 5 = 1 – γ' – γ''. Два уравнения, составленные для точек *а* и *б*, называют уравнениями Клоппера–Пирсона, они могут быть использованы для определения доверительных границ:

$$\sum_{i=0}^{m} C_N^i Q_в^i (1 - Q_в)^{N-i} = \gamma'; \qquad (8.2)$$

$$\sum_{i=0}^{m} C_N^i Q_н^i (1 - Q_н)^{N-i} = \gamma''. \qquad (8.3)$$

Учитывая, что $\sum_{i=0}^{m} C_N^i Q^i (1 - Q)^{N-i} = 1$, вместо (8.3) можем записать:

$$\sum_{i=0}^{m-1} C_N^i Q_н^i (1 - Q_н)^{N-i} = 1 - \gamma''. \qquad (8.4)$$

При $\tau = 0$ нижняя граница $Q_н = 0$, а верхняя получается из (8.2):

$$(1 - Q_в)^N = \gamma' = 1 - \delta .$$

Отсюда

$$Q_в = 1 - \sqrt[N]{1 - \delta} . \qquad (8.5)$$

Пример 8.1. При испытаниях 10 комплектов аппаратуры в течение 1000 ч не было обнаружено ни одного отказа. Найти доверительные границы для вероятности безотказной работы аппаратуры в течение 1000 ч при коэффициенте доверия 0,9.

Решение. Поскольку при испытаниях не предусмотрено восстановление работоспособности, а время испытаний совпадает с интервалом времени эксплуатации, заключаем, что план испытаний является планом типа [*N, Б, t*]. Так как во время испытаний не возникло ни одного отказа, используем формулу (8.5) и находим:

$$Q_в = 1 - 10^{-0,1} = 1 - \exp(-0,23) = 0,206.$$

Таким образом, при отсутствии отказов в 10 комплектах с гарантией 90% можно утверждать, что вероятность отказа не более 0,206.

Пример 8.2. Какое количество изделий необходимо поставить на испытания по плану типа [*N, Б, t*], чтобы с гарантией 90% утверждать, что вероятность безотказной работы не ниже 0,9?

Решение. Наименьшее количество изделий потребуется, когда $\tau = 0$. Тогда из (8.5) находим $N = \lg(1 - 5) / \lg P_н$. Подставляя сюда $\delta = 0,9$ и $P_н = 0,9$, находим $N = 22$. Если же $\delta = 0,95$ и $P_н = 0,95$, то $N = = 59$, а при $\delta = 0,95$ и $P_н = 0,99$ необходимое число изделий $N = 299$.

Из примеров 8.1 и 8.2 видно, что подтвердить даже не очень высокие показатели надёжности не так-то просто. Значительно проще иногда удовлетворить требованию заказчика о 100% безотказности при наблюдении за небольшой группой изделий, чем доказать методами математической статистики, что фактическая вероятность безотказной работы не ниже 0,9.

Точное решение задачи о доверительном интервале в некоторых случаях получить затруднительно. Это объясняется сложностью непосредственного решения уравнений Клоппера–Пирсона, а также ограниченностью опубликованных таблиц биномиального распределения.

В таких случаях для расчётов, не требующих высокой точности, можно находить приближённые решения, основанные на использовании распределения Пуассона и нормального распределения. Рассмотрим три такие возможности.

Пуассоновское приближение. Если Q мало, N велико и $m << N$, то справедливо выражение

$$C_N^m Q^m (1 - Q)^{N-m} \approx \frac{a^m}{m!} e^{-a}, \quad a = NQ . \qquad (8.6)$$

С помощью (8.6) уравнения (8.2) и (8.4) преобразуются следующим образом:

$$\sum_{i=0}^{m} \frac{a_в^i}{i!} e^{-a_в} = \gamma' ; \qquad (8.7)$$

$$\sum_{i=0}^{m-1} \frac{a_н^i}{i!} e^{-a_н} = \gamma'' . \qquad (8.8)$$

Для определения $a_н$ и $a_в$ можно использовать таблицы распределения Пуассона. Для входа в таблицу необходимо задать варианту m и вероятность γ'' и найти параметр распределения $a_в$. Аналогично по значениям ($m - 1$, $1 - \gamma''$) определяют $a_н$, а затем делением на N вычисляют границы $Q_н$ и $Q_в$. Вместо таблиц распределения Пуассона можно использовать таблицы квантилей χ^2-распределения, используя тот факт, что квантиль χ^2-распределения и по уровню вероятности p при числе степеней свободы $k = 2m + 2$ связана с параметром a распределения Пуассона, найденным по значениям p и m, соотношением $u(p, 2m + 2) = = 2a(p, m)$. Учитывая (8.7) и (8.8), находим:

$$Q_в = \frac{1}{2N} u(\gamma', 2m + 2) ; \quad Q_н = \frac{1}{2N} u(1 - \gamma'', 2m) . \qquad (8.9)$$

Пример 8.3. При испытании 100 источников стабилизированного питания в течение 2000 ч было зарегистрировано два отказа. Найти доверительные границы для вероятности отказа одного источника за время 2000 ч с коэффициентом доверия 0,9.

Решение. Поскольку здесь число отказов значительно меньше числа испытываемых изделий и точечная оценка $Q = 0,02$ свидетельствует о том, что вероятность отказа мала, для решения задачи используем пуассоновское приближение. По исходным данным определяем $\gamma' = (1 - 0,9) / 2 = 0,05$, $1 - \gamma'' = 0,95$. Из таблицы 7 в [50] при $d = n - 1 = 1$ и $a = 1 - \gamma'' = 0,95$

находим $a_и$ = 0,35536, а при $d = m - 2$ и $a = \gamma$ = 0,05 находим $a_в$ = 6,29579. Отсюда 0,00355 < Q < 0,063. Точность оценок при пуассоновском приближении получается вполне удовлетворительной.

Приближение Большева–Смирнова. Если Q мало, N велико и $mn < (N - 1) / 2$, то при приближённых расчётах доверительных границ вместо биномиального распределения в уравнениях Клоппера–Пирсона (8.2) и (8.4) можно использовать распределение Пуассона (8.7) и (8.8) со значениями параметров

$$a_в = \frac{(2N - m)\,Q_в}{2 - Q_в}; \quad a_н = \frac{(2N - m + 1)\,Q_н}{2 - Q_н}. \qquad (8.10)$$

Отсюда при $m < N$ и $Q < 1$ получаем $a_в \approx NQ_в$, $a_н \approx NQ_н$, т.е. получаем выражения параметров при пуассоновском приближении. Решая (8.10) относительно $Q_н$ и $Q_в$, находим:

$$Q_в = \frac{2a_в(m, \gamma')}{2N - m + a_в(m, \gamma')};$$
$$Q_н = \frac{2a_н(1 - m, 1 - \gamma'')}{2N - m + 1 + a_н(1 - m, 1 - \gamma'')}.$$

Если же используются таблицы χ^2-распределения, то

$$Q_в = \frac{u_в(2m + 2, \gamma')}{2N - m + 0{,}5u_в(2m + 2, \gamma')};$$
$$Q_н = \frac{u_н(2m, \gamma'')}{2N - m + 0{,}5u_н(2m, \gamma'')}. \qquad (8.11)$$

Пример 8.4. В условиях примера 8.3 найти доверительные границы с коэффициентом доверия 0,95, используя приближение Большева–Смирнова.

Решение. Из таблицы 2.2, *а* из [49] находим $u_н$ (4; 0,95) = 0,484; $u_в$ (6; 0,025) = 14,45. Подставляя эти значения в (8.11), получаем 0,00234 < Q < 0,0705.

Нормальное приближение. При достаточно больших NQ при решении уравнений Клоппера–Пирсона можно использовать формулу Муавра–Лапласа:

$$\sum_{i=0}^{m} C_N^i Q^i (1 - Q)^{N-i} \approx \Phi\left(\frac{m + 0{,}5 - NQ}{\sqrt{NQ(1 - Q)}}\right) - \Phi\left(\frac{-0{,}5 - NQ}{\sqrt{NQ(1 - Q)}}\right);$$

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-y^2/2}\, dy, \qquad (8.12)$$

где $\Phi(x)$ – функция Лапласа. Поскольку формула (8.12) применяется при больших значениях NQ (NQ > 9), вторым слагаемым можно пренебречь. Определяя квантиль нормального распределения z_δ по уровню γ'' и используя симметрию этого распределения, получаем уравнение:

$$\frac{m + 0{,}5 - NQ_в}{\sqrt{NQ_в(1 - Q_в)}} = z_{\gamma'} = -z_{\delta_1}, \quad \delta_1 = 1 - \gamma',$$

$$Q_в = \frac{2m + 1 + z_{\delta_1}^2 + z_{\delta_1}\sqrt{z_{\delta_1}^2 + (2m + 1)\left(2 - \frac{(2m + 1)}{N}\right)}}{2(N + z_{\delta_1}^2)}, \qquad (8.13)$$

$$Q_н = \frac{2m - 1 + z_{\delta_1}^2 - z_{\delta_1}\sqrt{z_{\delta_1}^2 + (2m - 1)\left(2 - \frac{(2m - 1)}{N}\right)}}{2(N + z_{\delta_1}^2)}. \qquad (8.14)$$

Достоинством этих формул является то, что они не требуют использования таблиц. Квантили z_p можно заготовить заранее для применяемых на практике уровней значимости: $z_{0,95} = 1{,}645$; $z_{0,9} = 1{,}29$; $z_{0,975} = 1 > 96$.

Пример 8.5. При испытаниях 500 датчиков дискретной информации в системе централизованного контроля и управления в течение 1000 ч были зарегистрированы отказы в 12 из них. Необходимо найти доверительные границы для вероятности отказа с коэффициентом доверия δ = 0,9.

Решение. Согласно исходным данным, $\delta_1 = (1+\delta)/2 = 0,95$, $m = 12$, $N = 500$, $z_\delta = 1,645$. Подставляя эти значения в (8.13), находим:

0,0141 < Q < 0,0392. Точечная оценка Q = 0,024.

8.5. ОЦЕНКА ПАРАМЕТРА ЭКСПОНЕНЦИАЛЬНОГО РАСПРЕДЕЛЕНИЯ. ТОЧЕЧНАЯ ОЦЕНКА. ДОВЕРИТЕЛЬНЫЙ ИНТЕРВАЛ

Пусть известно, что изделия имеют экспоненциальное распределение наработки до первого отказа $F(t)$ =1 – exp (–λt). Необходимо оценить параметр этого распределения λ, имеющий смысл интенсивности отказов. В математической статистике предлагается несколько методов для получения точечной оценки параметра A. Одним из наиболее распространённых и эффективных методов является метод максимального правдоподобия, предложенный английским статистиком Р.А. Фишером в 1912 г. Сущность метода состоит в следующем [67].

Пусть в результате испытаний, проведённых по некоторому плану, зарегистрированы отказы в моменты $t_1, t_2, ..., t_m$. Число $т$ может быть заранее заданным или случайным (в частности, $т$ = 0), однако времена t_i являются случайными величинами. Поэтому вектор $X = (t_1, t_2, ..., t_m)$ можно рассматривать как реализацию многомерной случайной величины. Если известна функция распределения наработки одного изделия $F(t, A)$, зависящая от совокупности параметров $A = (a_1, a_2, ..., a_k)$ (в частности, от одного параметра), постольку для каждого конкретного плана испытаний можно составить элемент вероятности того, что в испытаниях будут получены отказы в моменты t_i.

$$P\{t_1 \le T_1 < t_1 + dt_1, ..., t_m \le T_m < t_m + dt_m\} = p(t_1, t_2, ..., t_m, A)\, dt_1 dt_2 ... dt_m,$$

где $p(t_1, t_2, ..., t_m, A)$ – многомерная плотность распределения случайного вектора $(T_1, T_2, ..., T_m)$. Если зафиксировать t_i такими, какими они оказались на самом деле при испытаниях, и изменять значения параметров A в некотором интервале, то заметим, что плотность $p(t_1, t_2, ..., t_m, A)$ имеет максимум. Согласно методу максимального правдоподобия, точечная оценка $\overline{A} = (\overline{a_1}, \overline{a_2}, ..., \overline{a_k})$ параметров $a_1, a_2, ..., a_k$ должна обладать следующим свойством: обеспечивать максимальное значение плотности вероятности наблюдаемого исхода испытаний, т.е.

$$p(t_1, t_2, ..., t_m, \overline{A}) = \max_{(A)} p(t_1, t_2, ..., t_m, A).$$

На практике удобнее отыскивать не максимум функции $p(A)$, а максимум ln $p(A)$. Такая замена допустима, так как оба максимума достигаются в одной и той же точке. Функция L = ln $p(A)$ называется функцией правдоподобия. С её помощью задача определения точечной оценки ставится так: $\overline{A}$ должно обеспечивать максимальное значение функции L, т.е.

$$L(t_1, t_2, ..., t_m, \overline{A}) = \max_{(A)} L(t_1, t_2, ..., t_m, A).$$

Точка $\overline{A} = (\overline{a}_1, \overline{a}_2, ..., \overline{a}_k)$ в области A, обеспечивающая $\max\limits_{(A)} L$, находится методом градиента, согласно которому A является решением системы уравнений правдоподобия

$$\frac{d}{da_i} L(t_1, t_2, ..., t_m, a_1, a_2, ..., a_k) = 0, \quad i = 1, ..., k.$$

В частности, в случае однопараметрического экспоненциального распределения необходимо решить только одно уравнение,

$$\frac{d}{d\lambda} L(t_1, t_2, ..., t_m, \lambda) = 0.$$

Рассмотрим конкретные планы испытаний и найдём точечные оценки [63].

План [N, B, T]. Поскольку испытания проводятся с немедленной заменой отказавших изделий работоспособными и заканчиваются в момент T, мы учитываем, что интервалы между отказами распределены по экспоненциальному закону с одним и тем же параметром NX, а в интервале (t_m, γ) все изделия проработали безотказно. Составим выражение для элемента вероятности наблюдаемого исхода испытаний:

$$f(t_1, t_2, ..., t_m, \lambda)\, dt_1 dt_2 ... dt_m = (N\lambda e^{-N\lambda t_1} dt_1)(N\lambda e^{-N\lambda t_2} dt_2)...(N\lambda e^{-N\lambda tm} dt_m) \times$$
$$\times e^{-N\lambda(T - t_m)} = (N\lambda)^m e^{-N\lambda T} dt_1 dt_2 ... dt_m.$$

Отсюда $L = m \ln(N\lambda) - N\lambda T$. Уравнение правдоподобия $\dfrac{dL}{d\lambda} = \dfrac{m}{\lambda} - NT = 0$. Отсюда точечная оценка

$$\bar{\lambda} = m/NT. \qquad (8.15)$$

Из (8.15) следует, что достаточной статистикой испытаний является число отказавших изделий *т*. Исследуем следующие свойства полученной оценки: *несмещённость*, *состоятельность*, *эффективность*.

В математической статистике показывается, что при достаточно общих условиях, накладываемых на функцию распределения наработки на отказ одного изделия $F(t, A)$, оценка максимального правдоподобия эффективна независимо от плана испытаний. Поэтому остаётся проверить несмещённость и состоятельность.

Достаточная статистика *т* распределена по закону Пуассона с параметром $N\lambda T$, поэтому её математическое ожидание и дисперсия $Mm = = Dm = N\lambda T$. Тогда из формулы (8.15) находим:

$$M\bar{\lambda} = M\left(\frac{m}{NT}\right) = \frac{Mm}{NT} = \frac{N\lambda T}{NT} = \lambda ,$$

$$D\bar{\lambda} = D\left(\frac{m}{NT}\right) = \frac{Dm}{(NT)^2} = \frac{N\lambda T}{(NT)^2} = \frac{\lambda}{(NT)^2} = \frac{\lambda}{S_B(T)},$$

где $S_B(T)$ – суммарная наработка всех изделий за время испытаний по плану типа *В*. Отсюда следует, что точечная оценка (8.15) является несмещённой и эффективной.

План [*N*, *Б*, *T*]. Поскольку испытания проводятся без замены отказавших изделий, число работоспособных изделий после каждого отказа уменьшается на единицу и на λ уменьшается суммарная интенсивность отказов. Согласно плану испытаний, элемент вероятности

$$f(t_1, t_2, ..., t_m, \lambda)\, dt_1 dt_2 ... dt_m = (N\lambda e^{-N\lambda t_1} dt_1)((N-1)\lambda e^{-N\lambda t_2} dt_2)\times ...$$
$$...\times((N-m+1)\lambda e^{-(N-m+1)\lambda t_m} dt_m)\, e^{-(N-m)\lambda(T-t_m)} = \lambda^m A_N^m e^{-\lambda S_Б(T)},$$

где A_N^m – число размещений из *N* элементов по *т*; $S_Б(r)$ – суммарная наработка всех изделий за время испытаний по плану типа *Б*, определяемая по формуле

$$S_Б(t) = \sum_{i=1}^{m}(N-i+1)(t_i - t_{i-1}) + (N-m)(T-t_m), \ \ t_0 = 0.$$

Функция правдоподобия

$$L = \ln A_N^m + m\ln\lambda - \lambda S_Б(T).$$

Уравнение правдоподобия

$$\frac{dL}{d\lambda} = \frac{m}{\lambda} - S_Б(T) = 0.$$

Точечная оценка $\lambda = m / S_Б(T)$. В достаточную статистику здесь входят уже две величины: число отказов m и суммарная наработка $S_Б(T)$. Чтобы определить суммарную наработку, необходимо точно фиксировать моменты всех отказов, т.е. для получения точечной оценки здесь впервые потребовались моменты всех отказов.

План [*N*, *В*, *r*]. Времена между соседними отказами $(Z_1, Z_2, ..., Z_r)$ имеют экспоненциальные распределения с параметром $N\lambda$. Поэтому многомерная плотность распределения вектора $(Z_1, Z_2, ..., Z_r)$ имеет вид

$$f(Z_1, Z_2, ..., Z_r, \lambda) = \prod_{i=1}^{r} N\lambda e^{-N\lambda Z_1} = (N\lambda)^r \exp\left(-N\lambda\sum_{i=1}^{r} Z_i\right).$$

Функция правдоподобия

$$L = \ln f = r(\ln N + \ln\lambda) - N\lambda t_r, \quad t_r = \sum_{i=1}^{r} Z_i .$$

Уравнение правдоподобия

$$\frac{dL}{d\lambda} = \frac{r}{\lambda} - Nt_r = 0 .$$

Отсюда

$$\bar{\lambda}^{\bullet} = r / N t_r \,. \qquad (8.16)$$

Поскольку t_r имеет распределение Эрланга с параметрами $N\lambda$ и r, нетрудно найти математическое ожидание оценки

$$M\bar{\lambda}^{\bullet} = \int_0^{\infty} \frac{r}{Nx} \frac{(N\lambda)^r x^{r-1}}{(r-1)!} e^{-N\lambda x} dx = \frac{r}{r-1}\lambda.$$

Поскольку оценка получается смещённой, необходимо устранить смещение и вместо (8.16) принять

$$\bar{\lambda} = \frac{r-1}{r}\bar{\lambda}^{\bullet} = \frac{r-1}{N t_r}.$$

Чтобы найти дисперсию несмещённой оценки максимального правдоподобия, надо сначала найти второй начальный момент:

$$M\bar{\lambda}^2 = \int_0^{\infty} \left(\frac{r-1}{Nx}\right)^2 \frac{(N\lambda)^r x^{r-1}}{(r-1)!} e^{-N\lambda x} dx = \frac{r-1}{r-2}\lambda^2, \quad r > 2.$$

Дисперсия несмещённой оценки:

$$D\bar{\lambda} = M\bar{\lambda}^2 - \lambda^2 = \lambda^2 / (r-2), \quad r > 2.$$

Чтобы уменьшить дисперсию точечной оценки, надо назначить достаточно большое значение r.

План $[N, Б, r]$. Многомерная плотность распределения вектора $(Z_1, Z_2, \ldots, Z_r)$ имеет вид

$$f(Z_1, Z_2, \ldots, Z_r, \lambda) = N\lambda e^{-N\lambda Z_1} (N-1)\lambda e^{-N\lambda Z_1} \ldots (N-r+1)\lambda e^{-N\lambda Z_r} =$$
$$= A_N^r \lambda^r \exp(-\lambda S_Б(r)), \quad S_Б(r) = \sum_{i=1}^{r} (N-i+1) Z_i.$$

Функция правдоподобия

$$L = r \ln A_N^r + r \ln \lambda - \lambda S_Б(r).$$

Уравнение правдоподобия

$$\frac{dL}{d\lambda} = \frac{r}{\lambda} - S_Б(r) = 0\,.$$

Оценка максимального правдоподобия

$$\bar{\lambda}^{\bullet} = r / S_Б(r)\,.$$

Статистика $S_Б(r)$ имеет распределение Эрланга с параметрами (r, X). Потому эта оценка также смещённая, как и (8.16). Несмещённая оценка $\bar{\lambda} = \frac{r-1}{r}\bar{\lambda}^{\bullet} = \frac{r-1}{S_Б(r)}$.

Заметим, что полученные точечные оценки, как и любые другие точечные оценки, при малом объёме испытаний неустойчивы, обладают большой дисперсией и могут создать неверное представление о действительной интенсивности отказов. Поэтому кроме них используют оценки с помощью доверительных интервалов. Двусторонним доверительным интервалом для параметра λ с коэффициентом доверия δ называют интервал ($\lambda_н$, $\lambda_в$) со случайными границами, зависящими от исхода испытаний и такими, что вероятность покрытия этим интервалом неизвестного значения λ не менее заданной вероятности: $P(\lambda_н < \lambda < \lambda_в) > \delta$. Вероятности

$$\gamma' = P(0 < \lambda < \lambda_н), \quad y'' = P(\lambda_в < \lambda < 1) \qquad (8.17)$$

называются уровнями значимости при определении нижней и верхней границ соответственно. Они связаны с доверительной вероятностью соотношением $\delta + \gamma' + \gamma'' = 1$.

Уравнения (8.17) являются уравнениями, из которых находят доверительные границы $\lambda_в$ и $\lambda_н$. Нижним и верхним односторонними доверительными интервалами называют соответственно интервалы (0, $\lambda_в$) и ($\lambda_н$, ∞) такие, что $P(0 < \lambda$

$< \lambda_{в}) > \delta$; $P(\lambda_{н} < \lambda < \infty) > \delta$. Здесь уровень значимости $y = 1 - \delta$ выражает вероятность того, что параметр λ попадёт в интервал $(\lambda_{в}, \infty)$ или $(0, \lambda_{н})$ соответственно. Рассмотрим теперь некоторые конкретные планы испытаний.

План [*N*, *B*, *T*]. Достаточная статистика *m* распределена по закону Пуассона с параметром $a = N\lambda T$. Если зафиксировать *NT* и построить зависимости от *m* при различных λ, то получим семейство ступенчатых функций, которые после сглаживания имеют вид как на рис. 8.5.

Параметр семейства *a* увеличивается в направлении, указанном стрелкой. Чтобы найти доверительные границы, необходимо, как и при оценке вероятности отказа, найти такие функции семейства, которые проходили бы через точки 1 и 2 пересечения перпендикуляра из точки *m* с горизонтальными прямыми на уровне γ' и $1 - \gamma''$. Составляя соотношения для точек 1 и 2, получаем уравнения Клоппера–Пирсона:

$$\sum_{i=0}^{m} \frac{(N\lambda_{в}T)^i}{i!} e^{-N\lambda_{в}T} = \gamma'; \quad \sum_{i=m}^{\infty} \frac{(N\lambda_{н}T)^i}{i!} e^{-N\lambda_{н}T} = \gamma'', \qquad (8.18)$$

Второе уравнение (8.18) преобразуется к виду

$$\sum_{i=0}^{m-1} \frac{(N\lambda_{н}T)^i}{i!} e^{-N\lambda_{н}T} = 1 - \gamma''.$$

Для решения уравнений можно использовать таблицы распределения Пуассона или χ^2-распределения. При использовании таблиц распределения Пуассона последовательность действий следующая:

$$(\gamma', m) \to a_{в} \to \lambda_{в} = a_{в} / NT; \quad (1-\gamma'', m-1) \to a_{н} \to \lambda_{н} = a_{н} / NT,$$

а при использовании таблиц χ^2-распределения:

$$(\gamma', 2m+2) \to u_{в} \to \lambda_{в} = u_{в} / 2NT, \quad (1-\gamma'', 2m) \to u_{н} \to \lambda_{н} = u_{н} / 2NT.$$

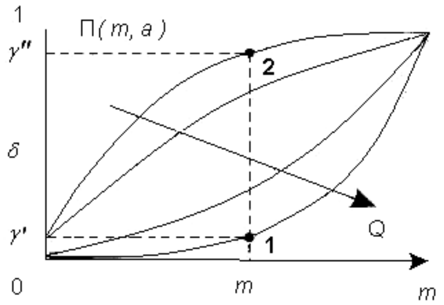


Рис. 8.5. Определение доверительных границ параметра экспоненциального распределения с помощью принципа Клоппера–Пирсона

При *m* = 0 нижняя граница $\lambda_{н} = 0$, а верхнюю находят из уравнения (8.18):

$$\lambda_{в} = -\ln(1-\delta) / \delta = b / \delta, \qquad (8.19)$$

где *b* = 2,3 при $\delta = 0{,}9$, *b* = 3 при $\delta = 0{,}95$ и *b* = 3,68 при $\delta = 0{,}975$.

Из формулы (8.19) следует, что для подтверждения заданного уровня интенсивности отказов даже при безотказной работе всех изделий необходима наработка, приблизительно втрое превышающая среднюю наработку $T_{ср.н} = 1/\lambda_{в}$. Если проанализировать справочные данные о надёжности логических элементов и типовых элементов радиоэлектронной аппаратуры, то можно заметить, что многие из этих элементов имеют интенсивности отказов 10^{-7} ч$^{-1}$ и меньше. Так, резисторы, конденсаторы и трансформаторы имеют $\lambda = 10^{-8} \ldots 10^{-9}$ ч$^{-1}$, соединения паяные и микросхемы – до $10^{-10} \ldots 10^{-11}$ ч$^{-1}$, а сварные электрические соединения – до $10^{-11} \ldots 10^{-12}$ ч$^{-1}$. Из формулы (8.19) видно, насколько трудно экспериментально определить эти значения. При $\lambda_{в} = 10^{-7}$ ч$^{-1}$ необходимо в течение года испытывать 3500 элементов, при $\lambda_{в} = 10^{-8}$ ч$^{-1}$ – 35 000 элементов, при $\lambda_{в} = 10^{-11}$ ч$^{-1}$ – десять миллионов элементов в течение 3,5 лет, или один миллион – в течение 35 лет. Если же столь высокие значения интенсивности отказов задаются для сложных изделий, то практически не удаётся экспериментально подтвердить расчётные значения. Для серии из 1000 изделий практически предельной величиной λ, о подтверждении которой может идти речь, является 10^{-7} ч$^{-1}$, поскольку и в этом случае даже при безотказной работе для сбора сведений потребуется эксплуатация в течение 3,5 лет, что для многих систем близко к периоду морального старения.

Пример 8.6. Из испытаний контрольно-измерительной аппаратуры получена следующая статистика: за 1000 ч в 20 приборах зарегистрированы 22 отказа. Оценить интенсивность отказов с коэффициентом доверия 0,9, если известно, что закон распределения между соседними отказами одного прибора экспоненциальный.

Решение. Согласно (8.15), точечная оценка $X = 22/(2 \cdot 10^4) == 1{,}1 \cdot 10^{-3}$ ч$^{-1}$. Для вычисления доверительного интервала воспользуемся табл. 2.2, *а* из [50]. Для $\delta_1 = 1 - \gamma'' = 95\%$ и *n* = 14 находим $u_{н} = 29{,}787$, а для $\gamma' = 5\%$ и *n* = 46 имеем $u_{в} = 62{,}83$. Отсюда $\lambda_{в} = 29{,}787 / (4 \cdot 10^4) = = 0{,}745 \cdot 10^{-3}$ ч$^{-1}$, $\lambda_{в} = 62{,}83/(4 \cdot 10^4) = 1{,}57 \cdot 10^{-3}$ ч$^{-1}$.

План [N, $Б$, T]. Поскольку именно этот план рассматривался в разделе 8.4 при вычислении доверительных интервалов для вероятности отказа, можно воспользоваться готовыми результатами, учитывая соотношение

$Q(T) = 1 - \exp(-\lambda T)$. (8.20)

Определяя $Q_н$ и $Q_в$ по формулам (8.2) и (8.4), из (8.20) находим:

$$\lambda_н = -\ln(1-Q_н)/T; \quad \lambda_в = -\ln(1-Q_в)/T. \qquad (8.21)$$

Из формул (8.2), (8.4) и (8.21) следует, что для вычисления доверительного интервала достаточно знать лишь количество отказов за время T, тогда как для вычисления точечной оценки максимального правдоподобия необходимо знать также суммарную наработку за время испытаний, что существенно усложняет проведение испытаний.

Пример 8.7. Известно, что за первые 10 000 ч наблюдения за 650 генераторами постоянного тока (ГПТ) отказали 15 из них. Считая ГПТ невосстанавливаемыми изделиями, определить доверительные границы для средней наработки до первого отказа с уровнем значимости 0,05.

Решение. При таком количестве отказов можно использовать нормальное приближение для биномиального распределения. Подставляя в (8.13) и (8.14) $m = 15$ и $z_\delta = 1{,}96$, находим $Q_н = 0{,}0135$; $Q_в = 0{,}0386$ (для сравнения отметим, что при использовании приближения Большева–Смирнова $Q_н = 0{,}01295$, $Q_в = 0{,}0377$). Отсюда $T_{ср.н} = 1/\lambda_в = -T/\ln(1 - Q_в) == 10^4/\ln(1/0{,}9614) = 10^4/0{,}0392 = 2{,}55\cdot10^5$ ч; $T_{ср.в} = 1/\lambda_н = 10^4/0{,}0135 == 7{,}4\cdot10^5$ ч.

План [N, B, r]. Уравнения Клоппера–Пирсона имеют вид

$$F_E(a,\ r) = \gamma'; \quad 1 - F_E(a_в,\ r) = \gamma''; \quad a = N\lambda t_r; \quad F_E(a,\ r) = 1 - \sum_{i=0}^{r-1} \frac{a^i}{i!}\, e^{-a}, \qquad (8.22)$$

где $F_E(a_в,\ r)$ – распределение Эрланга с параметром формы r; a – варианта. Уравнения следует решать с помощью таблиц распределения Эрланга [52, табл. VII], определяя квантиль $a_н$ по значениям (γ', r) и квантиль $a_в$ – по значениям ($1 - \gamma''$, r). Затем находят границы доверительного интервала:

$$\lambda_н = a_н(\gamma',\ r)/Nt_r; \quad \lambda_в = a_в(1-\gamma'',\ r)/Nt_r. \qquad (8.23)$$

Удобнее использовать более распространённые таблицы распределения Пуассона $\Pi(m, a)$ [48], [50], [52], где m – варианта, a – параметр распределения, если учесть, что $F_E(a,\ r) = 1 - \Pi(r - 1,\ a)$. Для этого надо записать уравнения Клоппера–Пирсона в виде

$$\Pi(r-1,\ a_н) = 1 - \gamma'; \quad \Pi(r-1,\ a_в) = \gamma''; \quad a = N\lambda t_r.$$

Задавая вероятность $1 - \gamma'$ и варианту $r - 1$, находят сначала соответствующий параметр $a_н$, а затем по формуле (8.23) – нижнюю границу $\lambda_н$. Аналогично находят и $\lambda_в$. Тогда

$$\lambda_н = a_н(1-\gamma',\ r-1)/Nt_r; \quad \lambda_в = a_в(\gamma'',\ r-1)/Nt_r. \qquad (8.24)$$

В частности, при $r = 1$ имеем

$$\lambda_н = -\ln(1-\gamma')/Nt_r; \quad \lambda_в = -\ln\gamma''/Nt_r.$$

При использовании таблиц χ^2-распределения доверительные границы находят по формулам

$$\lambda_н = u_н(1-\gamma'',\ 2r)/2Nt_r; \quad \lambda_в = u_в(\gamma'',\ 2r)/2Nt,$$

где $u_н(1-\gamma'',\ 2r)$ и $u_в(\gamma'',\ 2r)$ – квантили χ^2-распределения с $k = 2r$ степенями свободы.

Пример 8.8. При испытаниях 50 экземпляров процессорной платы до первого отказа получена наработка $t_1 = 1300$ ч. Найти доверительный интервал для средней наработки на отказ платы с коэффициентом доверия 0,8. Если относительная длина интервала δ_1 превысит значение 1,6, то продолжить испытания 50 экземпляров до второго отказа. Если и тогда $\delta_1 >$ 1,6, то продолжить испытания до выполнения указанного условия.

Решение. Согласно условиям задачи, план испытаний относится к типу [N, B, r], $N = 50$, $r = 1$. Согласно (8.23), $\lambda_н = 1{,}62\cdot10^{-6}$ ч$^{-1}$, $= 3{,}54\cdot10^{-5}$ ч$^{-1}$. Доверительные границы для средней наработки на отказ $T_н = 28\ 230$ ч, $T_в = 616\ 930$ ч, относительная длина интервала $\delta_1 = 2(T_в - T_н)\ /\ (T_в + T_н) = 1{,}82$. Продолжение испытаний до второго отказа приводит к суммарной наработке $t_2 = 2400$ ч. Отсюда $T_н = 30\ 770$ ч, $T_в = 226\ 400$ ч, $\delta_1 = 1{,}52 < 1{,}6$. Середина доверительного интервала

T = 128 590 ч.

План [N, $Б$, r]. Поскольку суммарная наработка всех изделий до окончания испытаний $S_Б(r)$ имеет распределение Эрланга с параметрами (r, X), постольку уравнения Клоппера–Пирсона имеют вид (8.22), а границы доверительного интервала

$$\lambda_н = a_н \frac{(1-\gamma',\ r-1)}{S_Б(r)}; \quad \lambda_в = a_в \frac{(\gamma'',\ r-1)}{S_Б(r)};$$

$$S_Б(r) = \sum_{i=1}^{r} (N-i+1)\, Z_i;$$

$$\lambda_н = u_н \frac{(1-\gamma',\ 2r)}{2S_Б(r)}; \quad \lambda_в = u_в \frac{(\gamma'',\ 2r)}{2S_Б(r)}.$$

При $\gamma' = \gamma'' = \gamma/2 = (1-\delta)/2$ длина доверительного интервала минимальна в отличие от других значений, когда $\gamma' \neq \gamma''$.

8.6. ПОСТАНОВКА ЗАДАЧИ КОНТРОЛЯ НАДЁЖНОСТИ

В процессе производства изделия подвергаются различным видам контроля, предусмотренным программой обеспечения качества и надёжности. Так, входному контролю подлежат многие комплектующие изделия. На промежуточных этапах технологического цикла контролируется качество функциональных узлов и блоков. Наиболее полная комплексная проверка качества изделий осуществляется при выходном контроле производства. Каждое изделие проверяется на соответствие техническим условиям (ТУ), испытывается на работоспособность в граничных режимах (проводятся температурные испытания, испытания на вибрацию, при повышенном и пониженном давлении и др.). При массовом производстве, когда нет возможности тщательно проверить каждое изделие, проводится выборочный контроль качества (дефектности), при котором по малой партии (выборке) делают заключение о качестве большой партии (генеральной совокупности) и принимают решение о её приемке или браковке. Выборочный контроль в некоторых специальных режимах может проводиться и при малосерийном производстве.

Перечисленные виды контроля имеют целью установить уровень качества. Изделия, благополучно прошедшие все виды контроля качества, объявляются кондиционными. Однако этого недостаточно для успешной работы изделий на местах эксплуатации. Необходимо установить, насколько устойчиво качество изделий во времени. С этой целью и проводятся контрольные испытания надёжности. Они осуществляются по окончании всех других видов контроля и предназначены для того, чтобы определить, удовлетворяет ли данная партия изделий заданным требованиям к надёжности.

Конечным результатом контроля, как правило, является одно из двух решений: считать партию хорошей, т.е. удовлетворяющей требованиям к надёжности, или забраковать её как ненадёжную. Важная особенность контроля надёжности заключается в том, что решение о приёмке и браковке принимается по отношению не к отдельным изделиям, как при выходном контроле качества, а к целой партии, однородной в смысле начального уровня качества (все изделия в партии кондиционные), причём не только к той партии, которая испытывается, но ко всем партиям большего объёма. В этом его отличие от статистического контроля дефектности, где, строго говоря, решение распространяется на вполне определённую партию большего объёма. Как и в случае определительных испытаний, для проведения контрольных испытаний необходимо составить план, называемый планом контроля [60]. Он представляет собой совокупность условий испытания и правил принятия решения о приёмке или браковке. Состав исходной информации для расчёта параметров плана контроля определяется критерием надёжности. В зависимости от выбора контролируемой характеристики надёжности все планы контроля делятся на две группы: планы контроля вероятности отказа и планы контроля параметров закона распределения. Далее для определённости будем рассматривать планы первого типа, хотя почти все рассуждения справедливы и для планов второго типа.

При контроле вероятности отказа требования к надёжности задаются с помощью двух чисел Q_0 и Q_1, имеющих следующий смысл: партия считается кондиционной ("надёжной"), если вероятность отказа $Q \le Q_0$, и некондиционной ("ненадёжной"), если $Q \ge Q_1$. При контроле надёжности выносится решение о кондиционности или некондиционности партии (в первом случае она принимается, во втором – бракуется). Следует обратить внимание на то, что при проведении определительных испытаний и при теоретических расчётах требования к надёжности часто задаются с помощью одного числа $Q_з$, и изделие считается надёжным, если верхняя оценка $Q_в \le Q_з$, и ненадёжным в противоположном случае. При контроле надёжности принципиально нельзя ограничиться заданием только одного числа, так как в этом случае не удаётся обеспечить равные условия по уровням рисков и принять верное решение для обеих заинтересованных сторон, участвующих в контроле надёжности. Промежуточная зона (Q_0, Q_1), называемая расстоянием между основной и конкурирующей гипотезами, вводится для хорошего различения двух основных уровней (кондиция и брак), и чем она шире, тем проще принять статистическое решение. Контрольные испытания заканчиваются принятием одной из следующих конкурирующих гипотез: H_0 – партия кондиционная ($0 < Q \le Q_0$), H_1 – партия некондиционная ($Q_1 \le Q < 1$). Поскольку статистическое решение принимается на основе неполной информации, существует конечная вероятность совершить ошибку первого (хорошая партия бракуется) или второго (плохая партия принимается) рода.

Вероятность ошибки первого рода называется риском поставщика и представляет собой вероятность того, что будет принята гипотеза H_1 t, хотя на самом деле верна гипотеза H_0 (вероятность отказа $Q < Q_0$). Решение о верности гипотезы H_0 или H_1 принимается на основе критерия u. Если значение критерия, полученного на основании выборки, попадает в область

S_0, то принимается гипотеза H_0. Если же это значение попадает в критическую область S_1, то гипотеза H_0 отвергается и принимается гипотеза H_1. Поэтому ошибку первого рода (риск изготовителя, поставщика) рассчитывают как условную вероятность

$$\tilde{\alpha} = P(u \in S_1 \mid 0 < Q \le Q_0). \qquad (8.25)$$

Вероятность ошибки второго рода называется риском заказчика и представляет собой вероятность того, что будет принята гипотеза H_0, хотя вероятность отказа $Q \ge Q_1$. При использовании критерия *u* ошибку второго рода рассчитывают как условную вероятность того, что значение критерия окажется в области S_0 при условии, что на самом деле верна гипотеза H_1.

$$\tilde{\beta} = P(u \in S_0 \mid Q_1 \le Q < 1). \qquad (8.26)$$

Исследование зависимостей $\bar{\alpha}$ и $\bar{\beta}$ от Q показывает, что они достигают максимума на границе указанного в (8.25) и (8.26) диапазона и планирование контрольных испытаний ведётся в расчёте на максимальные значения риска потребителя и заказчика:

$$\alpha = \max_{(Q)} \tilde{\alpha}(Q) = P(u \in S_1 \mid Q = Q_0); \qquad (8.27)$$

$$\beta = \max_{(Q)} \tilde{\beta}(Q) = P(u \in S_0 \mid Q = Q_1). \qquad (8.28)$$

Значения Q_0, Q_1, α и β являются исходной информацией для расчёта параметров плана контроля. В процессе планирования находят объём контролируемой партии и приёмочные нормативы. Приёмочными нормативами называются некоторые постоянные числа, которые являются границами области S_0 или S_1 и при сравнении которых с числом отказавших изделий *т* принимается одна из конкурирующих гипотез. Правила принятия решения определяются методом контроля.

В настоящее время используются три основных метода статистического контроля надёжности: однократной выборки, двукратной выборки и последовательного контроля.

При однократной выборке существует один приёмочный норматив *c*. Если при испытании партии из *N* изделий отказали *т* из них, то решение принимается согласно правилу: $m \le c$ – партия кондиционная (верна гипотеза H_0); $m > c$ – партия некондиционная (верна гипотеза H_1).

Контроль по однократной выборке легче спланировать и осуществить. Однако он наименее экономичен и требует сравнительно большого объёма испытаний, особенно для партий с высокой надёжностью.

При двукратной выборке существуют два этапа. На первом этапе по результатам испытаний n_1 изделий с помощью двух приёмочных нормативов c_1 и c_2 выносится одно из трёх решений: $m_1 \le c_1$ – принять партию (верна гипотеза H_0); $m_1 \ge c_2$ – забраковать партию (верна гипотеза H_1); $c_1 < m_1 < c_2$ – произвести вторую выборку. В последнем случае испытываются ещё N_2 изделий, определяется число отказавших изделий m_2 и выносится решение: $m_2 < c_3$ – принять партию (верна гипотеза H_0); $m_2 > c_3$ – забраковать партию (верна гипотеза H_1).

Метод двукратной выборки более экономичен. Но это его главное преимущество проявляется лишь при контроле больших партий с очень высокой или очень низкой надёжностью. При промежуточном уровне надёжности выигрыша в объёме испытаний почти нет. Расчёты же, связанные с таким контролем, сложнее, чем при однократной выборке. Кроме того, увеличивается время контроля. Поэтому метод двукратной выборки применяется сравнительно редко.

При последовательном контроле приёмочные нормативы рассчитываются не в виде отдельных чисел, а в виде двух функций; $c_1 = c_1(N)$ и $c_2 = c_2(N)$. Для каждого конкретного N определяется число отказавших изделий $m(N)$ и сравнивается с граничными значениями c_1 и c_2. По результатам сравнения выносится решение: $m(N) \le c_1(N)$ – принять партию (верна гипотеза H_0); $m(N) \ge c_2(N)$ – забраковать партию (верна гипотеза H_1); $c_1(N) < m(N) < c_2(N)$ – продолжить испытания.

Объём контролируемой партии *N* изменяется от некоторого минимума до такого назначения, когда будет принята одна из гипотез: H_0 или H_1. Таким образом, объём контролируемой партии и, как следствие, время контроля случайны. Этот метод является самым экономичным. Техническое его осуществление не связано с особыми трудностями. Недостатком метода является возможное, хотя и маловероятное увеличение времени контроля. Однако рациональной организацией испытаний такое увеличение можно свести к минимуму.

8.7. КОНТРОЛЬ НАДЁЖНОСТИ ПО ОДНОКРАТНОЙ ВЫБОРКЕ

Пусть необходимо проконтролировать надёжность некоторой партии изделий. Требования к надёжности каждого изделия заданы в следующем виде: изделие надёжно, если вероятность его отказа Q в течение заданного времени t не превышает $Q_0(t)$ и ненадёжно, если $Q(t) \ge Q_1(t)$. В процессе контроля требуется принять статистическое решение о том, являются изделия данной партии надёжными или нет, и на этом основании принять или забраковать всю партию, обеспечив риск поставщика не более α, а риск заказчика не более β. Так как закон распределения наработки изделия $Q(t)$ неизвестен, то, как и в случае определительных испытаний, выбираем план [*N*, *Б*, *t*], где длительность испытаний *T* совпадает со временем *t* работы изделия в нормальной эксплуатации. Для проведения испытаний и принятия решения кроме Q_0 и Q_1 необходимо знать ещё четыре числа: риски α и β, объём партии *N* и приёмочный норматив *c*. Если два из них задать, то два других можно определить по уравнениям (8.27) и (8.28).

Если задаются *N* и *c*, а определить нужно риски α и β, то получаем прямую задачу планирования контроля. Если же задаются *a* и *p*, а определяются *N* и *c*, то получаем обратную задачу планирования.

Найдём теперь явный вид уравнений (8.27) и (8.28). Поскольку число отказов изделий *m* за время испытаний *t* распределено по биномиальному закону, мы вместо (8.27) и (8.28) можем записать:

$$\alpha = P(m > c \mid Q = Q_0) = \sum_{i=c+1}^{N} C_N^i Q_0^i (1-Q_0)^{N-i} = 1 - \sum_{i=0}^{c} C_N^i Q_0^i (1-Q_0)^{N-i};$$
(8.29)

$$\beta = P(m \le c \mid Q = Q_1) = \sum_{i=0}^{c} C_N^i Q_1^i (1-Q_1)^{N-i}. \qquad (8.30)$$

В частности, при $c = 0$ имеем:

$$\alpha = 1 - (1 - Q_0(t))^N; \quad \beta = (1 - Q_1(t))^N. \qquad (8.31)$$

При $c > 0$ уравнения (8.29) и (8.30) можно решать с помощью таблиц биномиального распределения. Если же *N* велико, а *Q* мало, то можно воспользоваться пуассоновским приближением или приближением Большева–Смирнова для биномиального распределения. При пуассоновском приближении уравнения (8.27) и (8.28) заменяются следующими:

$$\alpha = 1 - \sum_{i=0}^{c} \frac{a_0^i}{i!} e^{-a_0}; \quad a_0 = NQ_0. \qquad (8.32)$$

$$\beta = \sum_{i=0}^{c} \frac{a_1^i}{i!} e^{-a_1}, \; a_1 = NQ_1. \qquad (8.33)$$

При использовании приближения Большева–Смирнова значения a_0 и a_1 вычисляются по формуле

$$a_i = (2N - c)Q_i / (2 - Q_i), \; i = 0, 1. \qquad (8.34)$$

При малом *Q*, большом *N* и достаточно большом *NQ* справедлива формула Муавра–Лапласа, с помощью которой уравнения (8.29) и (8.30) записываются в следующем виде:

$$\alpha = 1 - \Phi\left(\frac{c + 0{,}5 - NQ_0}{\sqrt{NQ_0(1-Q_0)}}\right); \quad \beta = 1 - \Phi\left(\frac{c + 0{,}5 - NQ_1}{\sqrt{NQ_1(1-Q_1)}}\right).$$

где $\Phi(x)$ – функция Лапласа, определяемая по формуле (8.12).

Определяя квантили нормального распределения по уровням 1 – α и β и используя свойство $u_\beta = -u_{1-\beta}$, получаем два уравнения:

$$u_{1-\alpha} = (c + 0{,}5 - NQ_0) \Big/ \sqrt{NQ_0(1-Q_0)};$$

$$u_{1-\beta} = (c + 0{,}5 - NQ_1) \Big/ \sqrt{NQ_1(1-Q_1)}.$$

Пренебрегая здесь под корнем величиной Q_i по сравнению с единицей, имеем:

$$\sqrt{a_0}\, u_{1-\alpha} = c + 0{,}5 - a_0; \quad \sqrt{a_0}\, u_{1-\beta} = c + 0{,}5 - a_1; \quad a_i = NQ_i; \quad i = 0, 1.$$
(8.35)

Складывая эти уравнения и обозначая $\eta = Q_1 / Q_0$, находим:

$$\sqrt{a_0}\,(u_{1-\alpha} + \sqrt{\eta}\, u_{1-\beta}) = a_0(\eta - 1),$$
откуда

$$\sqrt{a_0} = (u_{1-a} + \sqrt{\eta}\, u_{1-\beta}) \big/ (\eta - 1). \qquad (8.36)$$

По известным α, β и η находим сначала N по формуле (8.36), а затем c по формуле (8.35).

Пример 8.9. Определить объём однократной выборки и риск заказчика в плане контроля надёжности по вероятности с приёмочным нормативом $c = 0$ и риском изготовителя α = 0,15, если известно, что $Q_0 = 0{,}01$, а $Q_1 = 0{,}1$.

Решение. Используя пуассоновское приближение, из формулы (8.32) получаем $\alpha_0 = -\ln(1 - \alpha) = 0{,}162$. Отсюда $N = \alpha_0 / Q_0 \approx 16$. Теперь по формуле (8.34) находим β = 2,202. Уточнение рисков по формулам (8.31) даёт $\alpha = 1 - 0{,}9 \cdot 9^6 = 1 - 10^{-0{,}0704} = 0{,}1496$; $\beta = 0{,}9 \cdot 9^{16} = 1 - 10^{-0{,}7328} = 0{,}185$.

Пример 8.10. Определить объём однократной выборки и приёмочный норматив в плане контроля надёжности партии изделий с риском изготовителя и заказчика, не превышающим 10%, если известно, что вероятность отказа изделий из кондиционной партии за время t = 200 ч не должна превышать 0,01 и что партия признаётся некондиционной, если эта вероятность превышает 0,05.

Решение. Используя таблицу квантилей пуассоновского распределения (табл. 7 в [50]), находим, что квантили для уровней вероятностей 0,9 и 0,1 различаются в 23 раза при $c = 0$, в 7,3 раза при $c = 1$ и в 4,85 раза при $c = 2$. Поскольку здесь $\eta = Q_1 / Q_0 = 5$, выбираем $c = 2$. Тогда $\alpha_0 - 1{,}102$, $\alpha_1 = 5{,}322$, откуда получаем $N = 110$; β = 0,09 < 0,1.

В некоторых планах контроля по ряду причин, не связанных с расчётами, не удается обеспечить приемлемые для обеих сторон риски. Например, такая ситуация возникает, когда объём партии ограничен и не допускается повышенный риск заказчика или, напротив, когда в целях сокращения времени контроля требуется принять $c = 0$ и одновременно не превысить заданное значение риска изготовителя. Тогда контроль планируется в интересах только одной стороны (изготовителя или потребителя), и рассчитываются два норматива: c_0 – приёмочное число, N – браковочное число. При контроле в интересах изготовителя используется число c_0 и решение принимается согласно следующему правилу: $N \le c_0$ – партия кондиционная, $N > c_0$ – партия некондиционная.

8.2. Риски изготовителя и заказчика при изменении объёма партии и приёмочного норматива

N	c	NQ_0	NQ_1	α	β
15	1	0,75	1,50	0,173	0,550
30	2	1,50	3,00	0,191	0,423
75	5	3,75	7,50	0,168	0,241
150	10	7,50	15,0	0,138	0,118
300	20	15,0	30,0	0,083	0,035

При контроле в интересах потребителя решение принимается с помощью c_1 согласно правилу: $m \ge c_1$ – партия некондиционная (брак), $m < c_1$ – партия кондиционная. При $c_0 = c_1 - 1$ оба правила объединяются в одно, сформулированное ранее. В общем же случае может быть $c_0 = c$ и даже $c_0 > c_1$.

Пример 8.11. На заводе изготовлена партия из 100 устройств индикации данных. Необходимо провести контроль надёжности этих устройств в интересах изготовителя и в интересах потребителя, полагая, что вероятность отказа кондиционных изделий в течение 1000 ч не должна превышать 0,01, а некондиционными являются те изделия, вероятность отказа которых за то же время превышает 0,03. Риск изготовителя и риск потребителя не должны превышать 5%.

Решение. Поскольку число контролируемых изделий довольно велико, а Q_0 и Q_1 малы, пользуемся пуассоновским приближением. Выбираем сначала N и c так, чтобы α = 0,05, а $N < 100$. По табл. VII, приведенной в [51], находим, что α < 0,05 обеспечивается при (N, c) = (5; 0), (36; 1), (86; 2) и (136; 3). Выбираем $N = 82$, $c = 2$. По формуле (8.24) вычисляем, что β = 0,583 ? 0,05, т.е. при заданных ограничениях не удаётся удовлетворить одновременно требования изготовителя и потребителя. Поэтому составим два плана. При контроле в интересах изготовителя примем $N = 82$ и $c_0 = c = 2$. Выясним, можно ли при таком объёме партии обеспечить β < 0,05. Полагая $c_1 = 1$, вычислим $p = \exp(-0{,}03 \cdot 82) = \exp(-2{,}46) = 0{,}085 > 0{,}05$, т.е. даже при безотказной работе всех 82 устройств риск потребителя больше заданного. Увеличим число контролируемых изделий до максимально возможного $N = 100$. Тогда при $c_1 = 1$ риск $\beta = \exp(-3) = 0{,}0498 < 0{,}05$. Принимаем $c_1 = 1$. Однако при $N = 100$ и $c_0 = 2$ риска = 0,0803. Поэтому увеличим c_0 на единицу и найдём при $c_0 = 3$, что $c_1 = 0{,}019$. Итак, выбираем $N = 100$, $c_0 = 3$, $c_1 = 1$. При этом риск α = 0,019, риск β = 0,0498.

8.8. ПОСЛЕДОВАТЕЛЬНЫЙ КОНТРОЛЬ НАДЁЖНОСТИ

Информация о надёжности накапливается при последовательно возрастающем объёме испытаний. В зависимости от плана испытаний объём V выражается числом контролируемых изделий N, временем испытаний T, суммарной наработкой $N_{ср} / N_0$ и т.д. При планировании контроля на каждом из последовательных этапов составляется так называемое отношение правдоподобия

$\gamma_m = P(\xi = m | G_1) / P(\xi = m | G_0)$,

где m – число отказов к моменту проверки; G_0 и G_1 – граничные значения контролируемого показателя надёжности для кондиционных и некондиционных изделий соответственно (это могут быть Q_0 и Q_1, λ_0 и λ_1, $T_{\text{ср}0}$ и $T_{\text{ср}1}$ и др.). Число γ_m сравнивается с оценочными нормативами: $A = \alpha / (1 - \alpha)$, $B = (1 - \beta) / \alpha$, где α и β – риски поставщика и заказчика соответственно. Число A есть отношение вероятностей принять плохую и хорошую аппаратуру; B – отношение вероятностей забраковать плохую и хорошую аппаратуру.

На каждом этапе контроля решение может быть вынесено на основании первичного правила: $\gamma_m \le A$ – партия принимается; $\gamma_m \ge B$ – партия бракуется; $A < \gamma_m < B$ – испытания продолжаются. Вместо величин γ_m, A и B можно использовать их логарифмы, и тогда первичные правила приобретают следующий вид: $\ln\gamma_m < \ln A$ – партия принимается; $\ln\gamma_m \ge \ln B$ – партия бракуется; $\ln A < \ln\gamma_m < \ln B$ – испытания продолжаются. Однако это правило не всегда удобно, так как требует для принятия решения не только логической операции сравнения, но и некоторых вычислений. Поэтому из первичного правила выводится вторичное, основанное на сравнении на каждом этапе числа отказавших изделий с приёмочными нормативами c_0 и c_1, являющимися функциями объёма испытаний V. Эти функции $c_0(V)$ и $c_1(V)$ определяют границы между зонами приёмки, продолжения испытаний и браковки и находятся из уравнений:

$$\ln\gamma_{c_0} = \ln A; \quad \ln\gamma_{c_1} = \ln B. \qquad (8.37)$$

Рассмотрим теперь отдельно методику планирования последовательного контроля вероятности отказа и интенсивности отказов.

Контроль вероятности отказа по биномиальному плану. Поскольку вид функции распределения наработки до отказа неизвестен, будем, как и при однократной выборке, использовать план [N, $Б$, t].

$$c_0 \ln\frac{Q_1}{Q_0} + (N - c_0)\ln\frac{1-Q_1}{1-Q_0} = \ln A;$$

$$c_1 \ln\frac{Q_1}{Q_0} + (N - c_1)\ln\frac{1-Q_1}{1-Q_0} = \ln B. \qquad (8.38)$$

Отсюда

$$c_0(N) = h_0 + sN, \quad h_0 = \ln A / D, \quad s = \ln\frac{1-Q_0}{1-Q_1}\Big/ D; \qquad (8.39)$$

$$c_1(N) = h_1 + sN, \quad h_1 = \ln B / D, \quad D = \ln\frac{Q_1}{Q_0} + \ln\frac{1-Q_0}{1-Q_1}. \qquad (8.40)$$

Число h_0 всегда отрицательно, а h_1 и s – положительны. Функции (8.39) и (8.40) являются уравнениями двух параллельных прямых линий, пересекающих координатные оси в точках $(h_0, -h_0/s)$ и $(h_1, -h_1/s)$. Нанося эти прямые на графики, получаем графическую форму плана контроля. Прямые линии разбивают первый квадрант на три зоны: приёмки, продолжения испытаний и браковки (рис. 8.6, *а*).

В процессе испытаний строится реализация случайного процесса $m(N)$ и выясняется её принадлежность одной из зон. Испытания заканчиваются тогда, когда $m(N)$ достигнет одной из границ промежуточной зоны 2 или пересечёт её.

Кроме графической, существует ещё табличная форма плана контроля. В плоскости (m, N) образуются сечения, параллельные оси абсцисс и проходящие через точки $m = 0, 1, 2, ...$, и вычисляются те значения N, при которых пересекаются границы зон. В таблицу заносятся значения $т$ и соответствующие им граничные значения объёма испытаний N_{0m} и N_{1m}, определяемые согласно (8.28) и (8.29) по формулам:

$$N_{0m} = (m - h_0)/s; \quad N_{1m} = (m - h_1)/s; \quad N_{0m} > N_{1m}. \qquad (8.41)$$

Область $N \ge N_{0m}$ является областью приёмки, $N \le N_{1m}$ – областью браковки, а $N_{1m} < N < N_{0m}$ – областью продолжения испытаний.

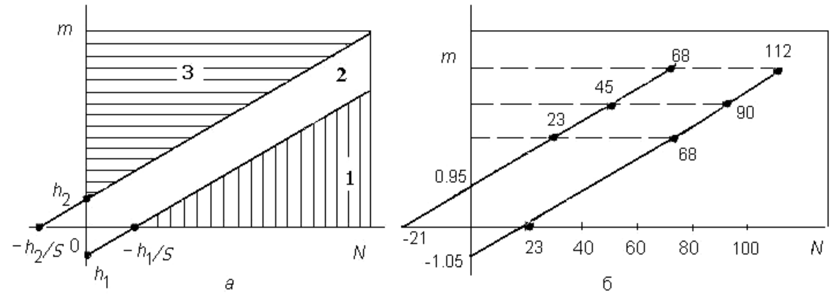


Рис. 8.6. Графическая форма плана последовательного контроля

Пример 8.12. Построить план последовательного контроля вероятности безотказной работы невосстанавливаемых изделий, в котором хорошей считается партия с вероятностью $P(t) > 0{,}99$, а плохой – партия с $P(t) < 0{,}88$. Риск поставщика $\alpha = 0{,}08$, риск заказчика $\beta = 0{,}06$. План представить в графической и табличной формах до $r = 10$ и принять решение для $(m; N) = (1; 46), (4; 60), (5; 100)$.

Решение. Сначала находим $\ln A = \ln(0{,}06/0{,}92) = -2{,}73$; $\ln B = \ln(0{,}94/0{,}08) = 2{,}464$; $\ln(Q_0/Q_1) = 2{,}485$; $\ln[(1 - Q_0)/(1 - Q_1)] = 0{,}1177$; $h_0 = -1{,}049$, $h_1 = 0{,}947$, $s = 0{,}0452$. Отсюда точки пересечения координатных осей $-h_1/s = -21$; $-h_0/s = 23{,}2$, по ним строятся границы зон (рис. 8.6, *б*). Результаты расчётов по формуле (8.41) приведены в табл. 8.3.

8.3. Табличная форма представления плана последовательного контроля вероятности отказа

m	0	1	2	3	4	5	6	7	8	9	10
N_{1m}	23	46	68	90	112	134	156	178	200	222	244
N_{0m}	–	11	23	45	68	90	112	134	156	178	200

На основании составленного плана выносим решение: при $(m; N) = (1; 46)$ принять партию, при (4; 60) забраковать партию, при (5; 100) продолжить испытания.

Контроль интенсивности отказов по суммарной наработке. Пусть контролю подвергается партия изделий с экспоненциальным распределением наработки одного изделия между отказами $F(t) = 1 - \exp(-\lambda t)$. Партия считается хорошей, если $\lambda < \lambda_0$, и плохой, если $\lambda \geq \lambda_1$.

В параграфе 8.5 было показано, что в планах типов *В* и *Б* количество отказов всех изделий контролируемой партии до получения суммарной наработки t_c распределено по закону Пуассона. Поэтому отношение правдоподобия приобретает вид

$$\gamma_m = \frac{(\lambda_1 t)^m e^{-\lambda_1 t_c} \big/ m!}{(\lambda_0 t)^m e^{-\lambda_0 t_c} \big/ m!} = \left(\frac{\lambda_1}{\lambda_0}\right)^m e^{-(\lambda_1 - \lambda_0)\, t_c}. \qquad (8.42)$$

Подставляя (8.42) в (8.37), находим:

$$c_0 \ln\frac{\lambda_1}{\lambda_0} + (\lambda_0 - \lambda_1)\, t_c = \ln A,$$

$$c_1 \ln\frac{\lambda_1}{\lambda_0} + (\lambda_0 - \lambda_1)\, t_c = \ln B.$$

Отсюда

$$c_0(t_c) = \ln A \Big/ \ln\frac{\lambda_1}{\lambda_0} + (\lambda_1 - \lambda_0)\, t_c \Big/ \ln\frac{\lambda_1}{\lambda_0}, \qquad (8.43)$$

$$c_1(t_c) = \ln B \Big/ \ln\frac{\lambda_1}{\lambda_0} + (\lambda_1 - \lambda_0)\, t_c \Big/ \ln\frac{\lambda_1}{\lambda_0}. \qquad (8.44)$$

Как и раньше, партия принимается при $m \leq c_0$, бракуется при $m \geq c_1$ и испытания продолжаются при $c_0 < m < c_1$. Вместо этого правила иногда удобнее пользоваться другим правилом, в котором участвуют граничные значения суммарной наработки t_{c_0} и t_{c_1}, соответствующие точкам пересечения прямых (8.43) и (8.44) с горизонтальными прямыми $m = 0, 1, 2, \ldots$. Принимая в (8.43) и (8.44) $c_0 = m$ и $c_1 = m$, получаем:

$$t_{c_0} = -\ln A/(\lambda_1 - \lambda_0) + m \ln\frac{\lambda_1}{\lambda_0} \Big/ (\lambda_1 - \lambda_0),$$

$$t_{c_1} = -\ln B/(\lambda_1-\lambda_0) + m\ln\frac{\lambda_1}{\lambda_0}\Big/(\lambda_1-\lambda_0).$$

Партия принимается, если $t_c > t_{c_1}$, бракуется, если $t_c < t_{c_1}$, и испытания продолжаются, если $t_{c_1} < t_c < t_{c_0}$.

Пример 8.13. В опытной эксплуатации находятся 100 непрерывно и одновременно работающих восстанавливаемых устройств. Необходимо построить план последовательного контроля их надёжности, обеспечивая риск поставщика не более 10%, риск заказчика не более 3% и полагая, что устройства восстанавливаются практически мгновенно, а закон распределения наработки одного устройства экспоненциальный. Хорошими считаются устройства со средней наработкой $T_{\text{ср}} > 400$ ч, плохими – устройства со средней наработкой $T_{\text{ср}} < 200$ ч.

Решение. По исходным данным находим: $\lambda_0 = 2{,}5\cdot10^{-3}$ ч$^{-1}$; $\lambda_1 = 5\cdot10^{-3}$ ч$^{-1}$; $\ln A = 3{,}4$; $\ln B = 4{,}57$; $\ln(\lambda_1/\lambda_0) = 0{,}693$. Поскольку восстановление мгновенное, вместо суммарной наработки t_c можно контролировать время $t = t_c/100$. Тогда $t_0^{\bullet} = t_{c_0}/100 = 13{,}6 + 2{,}772m$; $t_1^{\bullet} = t_{c_1}/100 = -9{,}09 + 2{,}772m$. Результаты расчётов $t_i^{\bullet}$ приведены в табл. 8.4.

8.4. Табличная форма представления плана последовательного контроля средней наработки до отказа

m	0	1	2	3	4	5	6	7	8	9	10
t_0	13,6	16,4	19,14	21,92	24,69	27,46	30,23	33,00	35,78	38,55	41,22
$t_1^{\bullet}$	–	–	–	–	2,00	4,77	7,54	10,32	13,09	15,86	18,63

Экономичность планов оценивают по среднему числу испытываемых изделий. Для метода однократной выборки объём партии – неслучайная величина, определяемая по формуле $N_0 = a_0/Q_0$, где a_0 – параметр распределения Пуассона, вычисленный по уровню вероятности 1 – α при значении варианты $m = c$.

Для последовательного контроля средний объём партии вычисляется по формуле, заимствованной из [52] и приводимой здесь без доказательства:

$$N_{\text{ср}} = \frac{(1-\alpha)\ln A + \alpha\ln B}{Q_0\ln\dfrac{Q_1}{Q_0} + (1-Q_0)\ln\dfrac{1-Q_0}{1-Q_1}}.$$

Расчёты по этой формуле показывают, что последовательный контроль даёт в среднем экономию от 30 до 50% по сравнению с контролем по однократной выборке. Причём отношение $N_{\text{ср}}/N_0$ уменьшается при сближении границ Q_0 и Q_1 и при уменьшении риска поставщика и заказчика. Так, при α = β = 0,1 и η = Q_0/Q_1 = 2,5 отношение $N_{\text{ср}}/N_0$ = 0,64, при α = β = 0,05 и том же η оно уменьшается до 0,59, а при α = β = 0,1 и η = 1,25 – до 0,56.

Выигрыш в среднем вовсе не означает, что выигрыш будет при каждом испытании, так как количество испытываемых изделий до принятия решения о приёмке или браковке не ограничено сверху. Поэтому выигрыш в среднем иногда обращается в большой проигрыш в некоторых испытаниях. Чтобы устранить этот недостаток, применяют усечённый последовательный контроль.

Усечённый последовательный контроль заключается в том, что одновременно составляются два плана: план последовательного контроля и план контроля по однократной выборке. В первом плане определяются параметры прямых линий, являющихся границами зон, во втором плане – объём партии N_0 и приёмочный норматив c. Если представить оба плана графически, то образуется ограниченная со всех сторон зона продолжения испытаний с двумя границами: с зоной приёмки и зоной браковки (рис. 8.7, *а*).

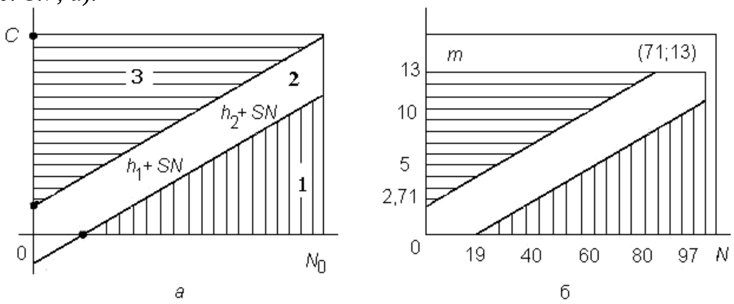


Рис. 8.7. Графическая форма плана усечённого последовательного контроля

Согласно процедуре усечённого последовательного контроля, испытания проходят в соответствии с обычным планом последовательного контроля до тех пор, пока $N < N_0$. Если ко времени достижения значения N_0 испытания ещё не закончены, тогда в силу вступает решающее правило контроля по однократной выборке и партия принимается или бракуется в зависимости от соотношения m и c. Таким образом, объём испытаний становится случайной величиной с известной верхней границей $N_{\max} = N_0$. Следует отметить, что риск поставщика и риск заказчика в усечённом контроле отличаются от вероятностей по которым параметры плана рассчитываются отдельно при последовательном контроле и при контроле по однократной выборке. Однако при изложенном способе усечения такое отличие невелико и им можно пренебречь.

Вопросы для самоконтроля

1. В чём состоит назначение испытаний на надёжность? Приведите пример планов испытаний.
2. В чём заключаются задачи определительных испытаний?
3. Перечислите свойства точечных оценок показателей надёжности.
4. Перечислите точечные оценки средней наработки на отказ и их характеристики.
5. В чём заключается принцип Клоппера–Пирсона интервального оценивания показателей надёжности?
6. В чём состоит постановка задачи контрольных испытаний на надёжность? Прямая и обратная задачи.
7. Как выбирается объём испытаний по рискам заказчика и изготовителя при однократной выборке?
8. Каковы табличная и графическая формы плана последовательного контроля надёжности?
9. Каковы табличная и графическая формы плана усечённого последовательного контроля надёжности?

СПИСОК ЛИТЕРАТУРЫ

1. Липатов, И.Н. Надежность функционирования автоматизированных систем : конспект лекций / И.Н. Липатов. – Пермь : Изд-во Пермского ГТУ, 1996. – 67 с.
2. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. – М. : Изд-во стандартов, 1990.
3. Надежность технических систем и техногенный риск. МЧС России : электронное учебное пособие. – URL : http:// www.obzh.ru/nad/.
4. Ермаков, А.А. Основы надежности информационных систем : учебное пособие / А.А. Ермаков. – Иркутск : ИрГУПС, 2006. – 151 с.
5. Матвеевский, В.Р. Надежность технических систем : учебное пособие / В.Р. Матвеевский. – М. : МГИЭМ, 2002. – 113 с.
6. Масюков, В.А. Надежность информационных систем : учебное пособие / В.А. Масюков. – Тверь, 2002. – 36 с.
7. Острейковский, В.А. Теория надежности / В.А. Острейковский. – М. : Высшая школа, 2003. – 363 с.
8. Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо. – СПб. : Изд-во "Питер", 2004. – 543 с.
9. Гнеденко, Б.В. Математические методы в теории надежности / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М. : Наука, 1965. – 524 с.
10. Дедков, В.К. Основные вопросы эксплуатации сложных систем / В.К. Дедков, Н.А. Северцев. – М. : Высшая школа, 1976. – 406 с.
11. Дружинин, Г.В. Теория надежности радиоэлектронных систем в примерах и задачах / Г.В. Дружинин, С.В. Степанов и др. – М. : Энергия, 1976. – 448 с.
12. Каштанов, В.А. Теория надежности сложных систем / В.А. Каштанов, А.И. Медведев. – М. : Изд-во "Европейский центр по качеству", 2002. – 469 с.
13. Козлов, Б.А. Краткий справочник по расчету надежности радиоэлектронной аппаратуры / Б.А. Козлов, И.Б. Ушаков. – М. : Советское радио, 1966. – 334 с.
14. Липаев, В.В. Надежность программных средств / В.В. Липаев. – М. : Изд-во "Синтез", 1998. – 246 с.
15. Надежность автоматизированных систем управления / под ред. Я.А. Хачатурова. – М. : Высшая школа, 1979. – 271 с.
16. Черкесов, Г.Н. Надежность аппаратно-программных комплексов : учебное пособие / Г.Н. Черкесов. – СПб. : Питер, 2005. – 479 с.
17. Сандлер, Д. Техника надежности систем / Д. Сандлер. – М. : Наука, 1966. – 408 с.
18. Соловьев, А.Д. Оценка надежности восстанавливаемых систем / А.Д. Соловьев. – М. : Знание, 1987. – 271 с.
19. Надежность автоматизированных систем управления / под ред. Я.А. Хетагурова. – М. : Высшая школа, 1979. – 287 с.
20. Половко, А.М. Основы теории надежности / А.М. Половко. – М. : Наука, 1964. – 446 с.
21. Голинкевич, Т.А. Прикладная теория надежности / Т.А. Голинкевич. – М. : Высшая школа, 1985. – 168 с.
22. Рудзит, Я.А. Основы метрологии, точность и надежность в приборостроении / Я.А. Рудзит, В.Н. Плуталов. – М. : Машиностроение, 1991. – 303 с.
23. Садчиков, П.И. Методы оценки надежности и обеспечения устойчивости функционирования программ / П.И. Садчиков, Ю.Г. Приходько. – М. : Знание, 1983. – 102 с.
24. Тейер, Т. Надежность программного обеспечения / Т. Тейер, М. Липов, Э. Нельсон. – М. : Мир, 1981. – 325 с.
25. Майерс, Г. Надежность программного обеспечения / Г. Майерс. – М. : Мир, 1980. – 360 с.
26. Шеннон, Р. Имитационное моделирование систем – искусство и наука / Р. Шеннон. – М. : Мир, 1978. – 244 с.
27. Столлингс, У. Структурная организация и архитектура компьютерных систем / У. Столлингс. – 5-е изд. – М. : Изд-во "Дом Вильямс", 2002. – 892 с.
28. Орлов, И.А. Эксплуатация и ремонт ЭВМ, организация работы вычислительного центра / И.А. Орлов, В.Ф. Корнюшко, В.В. Бурляев. – М. : Энергоатомиздат, 1989. – 400 с.
29. Вентцель, Е.С. Теория вероятностей / Е.С. Вентцель. – М. : Наука, 1964. – 576 с.
30. Холстед, М. Начала науки о программах / М. Холстед ; пер. с англ. – М. : Финансы и статистика, 1981. – 128 с.
31. Шнейдерман, Б. Психология программирования / Б. Шнейдерман. – М. : Радио и связь, 1984. – 304 с.
32. Shooman, M.L. Probabilistic models for software reliability prediction / M.L. Shooman // International Symp. Fault Tolerant Computing. – Newton, Mass.; N. Y., 1972.
33. Shooman, M.L. Operation Testing and Software Reliability Estimation during Program Development / M.L. Shooman // Record of the 1973 IEEE Symp. on Computer Software Reliability. – N. Y., 1973. – P. 51 – 57.

34. Moranda, P.B. Final Report of Software Reliability Study / P.B. Moranda, J. Jelinski. – McDonnell Douglas Astronautic Company. MDC Report N 63921. Dec. 1972.
35. Moranda, P.B. Software Reliability Research / P.B. Moranda, J. Jelinski // Statistical Computer – Probability-Based Models for the Failures During Burn – In Phase Joint National Meeting ORSA // Tims. – Las Vegas ; N. Y., Nov., 1975.
36. Shick, C.J. Assessment of Software Reliability / C.J. Shick, R.W. Wolverton // Proc. 11-th Annual Meeting of the German Operation Research Society. – Hamburg, Germany, 6 – 8 Sept., 1972.
37. Shick, C.J. Achieving reliability in large scale software system / C.J. Shick, R.W. Wolverton // Proc. of the Annual Reliability and Maintainability Symp. – Los Angeles, 1974. – P. 302 – 319.
38. Lipov, M. Some variation of a Model for Software Time-to-Failure / M. Lipov // TRW Systems Group. Correspondence ML-74-2260,
19 – 21 Aug., 1974.
39. Hamilton, P.A. Measuring reliability of Computation Center Software / P.A. Hamilton, J.D. Musa // Proc. 3-th Internat. Conf. on Software. Eng. May 10 – 12, 1978. – P. 29 – 36.
40. Sukert, C.A. An investigation of software reliability models / C.A. Sukert // Proc. Annual Reliability and Maintainability Symp. – 1977. – P. 478 – 484.
41. Wall, K. Pragmatic software reliability prediction / K. Wall, P.A. Ferguson // Proc. 1977 Annual Reliability and Maintainability Symp. – 1977. – P. 485 – 488.
42. Nelson, E.C. Software reliability FTC-5 Internat. Symp. Fault Tolerant Computing / E.C. Nelson. – Paris ; N. Y., 1975. – P. 24 – 28.
43. Осима, Ю. Надежность программного обеспечения / Ю. Осима // Дзеко сери. – 1975. – Т. 16, № 10. – С. 887 – 894.
44. Иыуду, К.А. Прогнозирование надежности программ на ранних этапах разработки / К.А. Иыуду, А.И. Касаткин, В.В. Бахтизин // Надежность и контроль качества. – 1982. – № 5. – С. 18 – 30.
45. Ллойд, Д. Надежность / Д. Ллойд, М. Липов. – М. : Сов. радио, 1964. – 686 с.
46. Sukert, C.A. An investigation of software reliability models / C.A. Sukert // Proc. Annual Reliability and Maintainability Symp. – 1977. – P. 478 – 484.
47. Шор, Я.Б. Таблицы для анализа и контроля надежности / Я.Б. Шор, Ф.И. Кузьмин. – М. : Сов. радио, 1968. – 284 с.
48. Большее, Л.Н. Таблицы математической статистики / Л.Н. Большее, Н.В. Смирнов. – М. : Наука, 1965. – 464 с.
49. Гнеденко, Б.В. Математические методы в теории надежности / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М. : Наука, 1965. – 524 с.
50. Справочник по вероятностным расчетам / Г.Г. Абезгауз, А.П. Тронь, Ю.Н. Копенкин, И.А. Коровина. – М. : Воениздат, 1970. – 528 с.
51. Шор, Я.Б. Статистические методы анализа и контроля качества и надежности / Я.Б. Шор. – М. : Сов. радио, 1962. – 564 с.
52. ГОСТ 16504–79. Качество продукции. Контроль и испытания. Основные термины и определения. – М. : Изд-во стандартов, 1979. – 22 с.
53. ГОСТ 17510–79. Надежность изделий машиностроения. Система сбора и обработки информации. Планирование наблюдений. – М. : Изд-во стандартов, 1979. – 23 с.
54. ГОСТ 17509–72. Надежность изделий машиностроения. Система сбора и обработки информации. Методы определения точечных оценок показателей надежности по результатам наблюдений. – М. : Изд-во стандартов, 1972. – 52 с.
55. ГОСТ 18049–72. Надежность в технике. Испытания ограниченной продолжительности с заменой отказавших изделий. – М. : Изд-во стандартов, 1972. – 13 с.
56. ГОСТ 18333–73. Надежность в технике. Испытания ограниченной продолжительности без замены отказавших изделий. – М. : Изд-во стандартов, 1973. – 10 с.
57. ГОСТ 17572–72. Надежность в технике. Испытания с ограниченным числом отказов. – М. : Изд-во стандартов, 1974. – 15 с.
58. ГОСТ 27.504–84. Надежность в технике. Методы оценки показателей надежности по цензурированным выборкам. – М. : Изд-во стандартов, 1984. – 41 с.
59. ГОСТ 27.410–87. Надежность в технике. Методы контроля показателей и планы контрольных испытаний на надежность. – М. : Изд-во стандартов, 1988. – 109 с.
60. ГОСТ 17331–71. Надежность в технике. Метод последовательных испытаний. – М. : Изд-во стандартов, 1971. – 27 с.
61. ГОСТ 20736–75. Качество продукции. Статистический приемочный контроль по количественному признаку при нормальном распределении контролируемого параметра. – М. : Изд-во стандартов, 1975. – 91 с.
62. ГОСТ 11.005–74. Прикладная статистика. Правила определения оценок и доверительных границ для параметров экспоненциального распределения и распределения Пуассона. – М. : Изд-во стандартов, 1974. – 29 с.
63. ГОСТ 11.004–74. Прикладная статистика. Правила определения оценок и доверительных границ для параметров нормального распределения. – М. : Изд-во стандартов, 1974. – 20 с.
64. ГОСТ 27.411–81. Надежность в технике. Одноступенчатые планы контроля по альтернативному признаку при распределении времени безотказной работы по закону Вейбулла. – М. : Изд-во стандартов, 1981. – 20 с.
65. ГОСТ 11.009–79. Прикладная статистика. Правила определения оценок и доверительных границ для параметров логарифмически нормального распределения. – М. : Изд-во стандартов, 1979. – 52 с.
66. Фишер, Р.А. Статистические методы для исследователей / Р.А. Фишер. – М. : Госстатиздат, 1958. – 342 с.

ОГЛАВЛЕНИЕ