ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф. Можайского

НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Учебное пособие

Учебное издание «Надежность автоматизированных систем» утверждено в качестве учебного пособия по дисциплине «Надежность автоматизированных систем» и рекомендовано кафедрой информационно-вычислительных систем и сетей Военно-космической академии имени А.Ф. Можайского для обучающихся по основной профессиональной образовательной программе высшего образования – программе специалитета по специальности «Применение и эксплуатация автоматизированных систем специального назначения», протокол № 06 от 27 февраля 2017 г.

Санкт-Петербург
2017

Авторы:
В.В. Тимофеев

Рецензент:
кандидат технических наук, доцент **И.В. Захаров**

Надежность автоматизированных систем [Электронный ресурс]: учебное пособие / В.В. Тимофеев. – Электрон. текстовые дан. (2 МБ). – СПб.: ВКА им. А.Ф. Можайского, 2017. – 1 электрон. опт. диск (CD-ROM).

В электронном учебном пособии рассмотрены вопросы, связанные с оцениванием и обеспечением надежности технических средств, программного обеспечения и оперативного состава автоматизированных систем.

Учебное пособие разработано сотрудниками кафедры информационно-вычислительных систем и сетей в составе кандидата технических наук, доцента В.В. Тимофеева, кандидата технических наук, доцента В.В. Кузнецова, кандидата технических наук К.А. Эсаулова.

Минимальные системные требования: ПК не ниже класса Pentium IV*;* 512 МБ RAM; Windows XP или более поздняя версия; SVGA с разрешением 1024×768; Adobe Acrobat Reader IX или более поздняя версия; CD-ROM дисковод.

Учебное пособие разработано с помощью программного обеспечения Microsoft Office Word, Adobe Acrobat Pro.

Техническая обработка и подготовка материалов для электронного издания: **В.В. Тимофеев.**

Подписано к использованию 28 сентября 2017 г.

Объем издания 4,8 МБ.

Запись на материальный носитель – Военно-космическая академия имени А.Ф. Можайского,

г. Санкт-Петербург, ул. Ждановская, 13;

e-mail: vka@mil.ru

Введение

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [10].

АС представляет собой организационно-техническую систему, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и тому подобное) или их сочетаниях [11].

В зависимости от вида деятельности различают следующие разновидности АС [11]:

— АСУ (автоматизированные системы управления): АСУ технологическими процессами (АСУ ТП), АСУ предприятиями или производством (АСУП) и т. д;

— САП (системы автоматизированного проектирования): САПР (системы автоматизированного проектирования и расчета), САРР ТП системы автоматизированного проектирования технологических процессов) и тому подобное;

— АСНИ (автоматизированные системы научных исследований);

— АС обработки и передачи информации: АИПС (автоматизированная информационно-поисковая система), АСИТО (автоматизированная система информационно-терминологического обслуживания) и тому подобное;

— САМ (АС технологической подготовки производства);

— автоматизированные системы контроля и испытаний;

— АС, объединяющие функции перечисленных выше систем.

Наиболее широкий класс автоматизированных систем представляют АСУ.

В любой автоматизированной системе управления (АСУ) можно выделить комплекс технических средств (средства вычислительной техники, техника каналообразования, каналы связи и другие технические изделия, входящие в состав автоматизированной системы), коллектив людей (операторов, специалистов по техническому обслуживанию, руководителей работ) и программное обеспечение (математические методы, модели и алгоритмы управления, применяемые в АС).

Комплекс технических средств (КТС) АСУ имеет ряд особенностей. К таким комплексам предъявляются высокие требования в отношении достоверности и своевременности обработки больших объемов информации. В ряде случаев отдельные КТС одной АСУ территориально разобщены. Структура отдельных комплексов, как правило, уникальна, хотя они состоят из стандартных элементов. При построении КТС широко применяются иерархические структуры.

Первоначально в теории надежности рассматривались только технические системы. В настоящее время проблема надежности технических систем по-прежнему является актуальной, однако, благодаря развитию АСУ повысился интерес к работам по надежности систем «человек и техника». Такие исследования особенно важны для обеспечения безопасности функционирования систем, в составе которых действующим звеном является человек – оператор.

Исследование надежности системы «человек и техника» сводится к рассмотрению надежности технической системы с учетом деятельности в ее составе операторов или к рассмотрению своевременности и надежности выполнения операторами определенных действий совместно с КТС.

Опыт разработки и применения АСУ свидетельствует также, что важнейшей проблемой является надежность сложных управляющих программ, работающих в реальном масштабе времени. Можно говорить о надежности программ как их свойстве выполнять требования к программе в течение определенного интервала времени в реальных условиях эксплуатации. Из-за наличия скрытых ошибок в программах могут возникать аварийные ситуации и значительно снижаться эффективность АСУ.

Таким образом, при рассмотрении надежности проектируемых АСУ следует оценить: надежность технической системы, надежность деятельности операторов, надежность функционирования программного обеспечения, надежность АСУ как системы, состоящей из первых трех компонентов.

При решении вопросов, связанных с обеспечением требуемого уровня надежности АСУ [ГОСТ 24.701-86] необходимо учитывать следующие их особенности:

— каждая АСУ является многофункциональной системой, функции которой имеют неодинаковую значимость и, соответственно, характеризуются разным уровнем требований к надежности их выполнения;

— во многих АСУ возможно возникновение некоторых исключительных (аварийных, критических) ситуаций, представляющих сочетание отказов или ошибок функционирования системы и способных привести к значительным нарушениям функционирования объекта управления (авариям);

— в функционировании АСУ участвуют различные виды ее обеспечения и персонал АСУ, которые могут в той или иной степени влиять на уровень надежности АСУ;

— в состав каждой АСУ входит большое количество разнородных элементов: технических, программных и др., при этом в выполнении одной функции АСУ обычно участвуют несколько различных элементов, а один и тот же элемент может участвовать в выполнении нескольких функций системы.

При решении вопросов надежности АСУ формальное описание, анализ, оценка и обеспечение надежности проводят по каждой функции АСУ в отдельности. В необходимых случаях используют также анализ возможности возникновения в системе аварийных ситуаций, ведущих к значительным техническим, экономическим или другим потерям вследствие аварии объекта управления (или АСУ в целом).

Функции АСУ подразделяют на простые и составные. Для некоторых АСУ возможно построение составной функции наиболее общего вида, отображающей функционирование АСУ в целом. Перечень функций и видов их отказов, по которым задаются требования к надежности конкретной АСУ, а также критерии этих отказов устанавливает заказчик АСУ по согласованию с разработчиком АСУ и вносит в техническое задание на АСУ.

Для установления критериев отказов составляют перечень признаков или параметров, по которым может быть обнаружен факт возникновения каждого отказа, а при необходимости - количественные (критериальные)значения этих параметров. Если для некоторой функции АСУ определено несколько видов отказов, существенно различающихся по причинам возникновения или по вызываемым ими последствиям, то безотказность и ремонтопригодность по этой функции задают отдельно по каждому виду отказов. При этом критерии отказов устанавливают по каждому виду отказов.

Перечень рассматриваемых аварийных ситуаций, по которым задают требования к надежности, составляет заказчик АСУ по согласованию с разработчиком АСУ и вносит в техническое задание на АСУ с указанием, при каких условиях эксплуатации АСУ рассматривают возникновение каждой из приведенных аварийных ситуаций. Аварийные ситуации в системе могут возникать в условиях нормального ее функционирования и вследствие воздействия на систему внешнего экстремального фактора.

Уровень надежности АСУ зависит от следующих основных факторов:

— состава и уровня надежности используемых технических средств, их взаимосвязи в надежностной структуре комплекса технических средств АСУ;

— состава и уровня надежности используемых программных средств, их содержания (возможностей) и взаимосвязи в структуре программного обеспечения АСУ;

— уровня квалификации персонала, организации работы и уровня надежности действий персонала АСУ;

— рациональности распределения задач, решаемых системой, между техническими средствами, программным обеспечением и персоналом АСУ;

— режимов, параметров и организационных форм технической эксплуатации технических и программных средств АСУ;

— степени использования различных видов резервирования (структурного, информационного, временного, алгоритмического, функционального);

— степени использования методов и средств технической диагностики;

— реальных условий функционирования АСУ.

Свойства информационного, математического, лингвистического, метрологического, организационного, правового обеспечений АСУ влияют на надежность АСУ только косвенно, через функционирование технических и программных средств и персонала АСУ и поэтому при решении вопросов, связанных с надежностью АСУ, отдельно не учитываются.

Совокупность технических, программных и эргатических элементов АСУ (технических и программных средств и части персонала АСУ), выделяемая из всего состава АСУ по признаку участия в выполнении некоторой (*i*-й) функции системы, образует *i*-ю функциональную подсистему АСУ. Если для АСУ сформулирована составная функция наиболее общего вида, то соответствующая ей функциональная подсистема совпадает с системой в целом. Анализ надежности АСУ проводят по каждой функции АСУ в отдельности с учетом уровня надежности и других свойств, входящих в нее технических, программных и эргатических элементов.

При анализе надежности АСУ необходимо учитывать, что элементы, входящие в АСУ, могут решать задачи взаимной компенсации некоторых нарушений нормальной работы, предотвращая переход этих нарушений в отказы АСУ, либо минимизируя их неблагоприятные последствия. Например, персонал может эффективно принимать меры к недопущению отказов АСУ при отказах её технических средств или проявлении сшибок в программном обеспечении, либо к снижению потерь от таких отказов (ошибок).

Выбор состава показателей надежности АСУ производят на основе установленных техническим заданием перечня функций системы, перечня видов их отказов и перечня аварийных ситуаций, по которым регламентируют требования к надежности.

Требуемые численные значения выбранных показателей надежности АСУ (требования к надежности) устанавливают по определенным критериям на основе анализа влияния отказов АСУ в выполнении ее функций и аварийных ситуаций на эффективность функционирования автоматизированного комплекса (АСУ и объект управления) в целом, а также затрат, связанных с обеспечением надежности. Требования к надежности АСУ вносят в техническое задание на АСУ.

Оценку надежности АСУ проводят на различных стадиях создания и эксплуатации АСУ. При разработке АСУ проводят проектную (априорную) оценку надежности системы. При опытной и промышленной эксплуатации АСУ проводят экспериментальную (апостериорную) оценку надежности системы.

1. Надёжность технических средств АС

1.1. Основные положения теории надежности технических объектов

1.1.1. Основные термины и определения теории надежности

Термин – слово или словосочетание являющееся названием некоторого понятия в какой-нибудь области науки, техники, искусства и т.д. Термины служат специализирующими, ограничительными обозначениями, характерными для этой сферы предметов, явлений, их свойств и отношений.

Определение поясняет смысл термина указанием правил выделения его среди прочего.

Термины и определения, используемые в теории надежности, регламентированы ГОСТ 27.002-89 Надежность в технике. Термины и определения.

Надежность – свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях эксплуатации.

Технический объект (объект) – техническое изделие (в том числе элемент и система) определенного целевого назначения, рассматриваемое в периоды проектирования, производства, испытаний и эксплуатации.

Элемент – технический объект (составляющая часть чего-либо), обладающий рядом свойств, внутреннее строение (содержание) которого при расчете показателей надежности значения не имеют.

Система – совокупность связанных между собой элементов, обладающая свойством (назначением, функцией), отличным от свойств отдельных ее элементов.

Структура системы – расположение и связи между составными частями системы, ее устройство.

Процесс – изменение (непрерывное или дискретное) состояния технического объекта, протекающее, как правило во времени.

Надежность технического объекта характеризуется следующими основными состояниями и событиями.

Работоспособным называется такое состояние технического объекта, при котором значения параметров, характеризующих его способность выполнять заданные функции, находятся в пределах, установленных нормативно-технической или конструкторской документацией.

Соответственно, *неработоспособным* называется состояние технического объекта, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не находится в пределах, установленных указанной документацией.

В *исправном* состоянии технический объект соответствует всем требованиям нормативной технической и конструкторской документации.

В *неисправном* состоянии – имеется хотя бы одно несоответствие этим требованиям.

Работоспособный технический объект удовлетворяет только тем требованиям, которые существенны для функционирования, и может не удовлетворять прочим требованиям (напр., по сохранности внешнего вида элементов). Технический объект, находящийся в исправном состоянии, точно работоспособен.

Предельное состояние – состояние технического объекта, при котором его применение по назначению невозможно или нецелесообразно.

Отказ – событие, заключающееся в нарушении работоспособности технического объекта. Т.е. в переходе его из работоспособного состояния в неработоспособное.

Повреждение – событие, заключающееся в переходе технического объекта из исправного состояния в неисправное (но работоспособное).

Восстановление – событие, заключающееся в переходе технического объекта из неработоспособного в работоспособное состояние. *Невосстанавливаемые объекты* – технические объекты, восстановление которых после отказа считается не целесообразным или невозможным. *Восстанавливаемые объекты* – технические объекты, в которых производится восстановление после отказа.

Наработка – продолжительность (без учета хранения, простоя и восстановления) или объем работы технического объекта, измеряемые единицами времени, циклами и т.п. *Наработка до отказа* – наработка технического объекта с начала эксплуатации до возникновения первого отказа. *Наработка между отказами* – наработка технического объекта от окончания восстановления его работоспособного состояния после возникновения отказа до появления следующего отказа.

Технический ресурс – наработка технического объекта от начала эксплуатации (или ее возобновления после ремонта) до перехода в предельное состояние.

Срок службы – календарная продолжительность эксплуатации (с учетом хранения, простоя и восстановления) от ее начала до наступления предельного состояния.

Надежность включает в себя четыре составляющие: безотказность, ремонтопригодность, долговечность и сохраняемость.

Безотказность – способность технического объекта непрерывно сохранять работоспособность в течение некоторого времени или некоторой наработки. Безотказность технического объекта в решающей степени влияет на эффективность их использования и определяется безотказностью элементов, режимом их работы, наличием резервирования, параметрами окружающей среды и др.

Ремонтопригодность – способность технического объекта к восстановлению работоспособного состояния в процессе ремонта. Ремонтопригодность зависит от того, выполнены ли элементы в виде отдельных, легко заменяемых блоков, от использования средств встроенного контроля работоспособности и диагностики, а также от квалификации обслуживающего персонала и организации эксплуатации.

Долговечность – способность технического объекта сохранять работоспособность до наступления предельного состоянии с необходимыми перерывами для технического обслуживания и ремонтов.

Долговечность технического объекта зависит от долговечности технических средств и от подверженности системы моральному старению.

Сохраняемость – способность технического объекта сохранять работоспособность в процессе хранения.

1.1.2. Классификация отказов технических средств

Критерии отказов технических средств АС устанавливаются в соответствии с требованиями, указанными в стандартах, технических условиях или другой технической документации на эти технические средства.

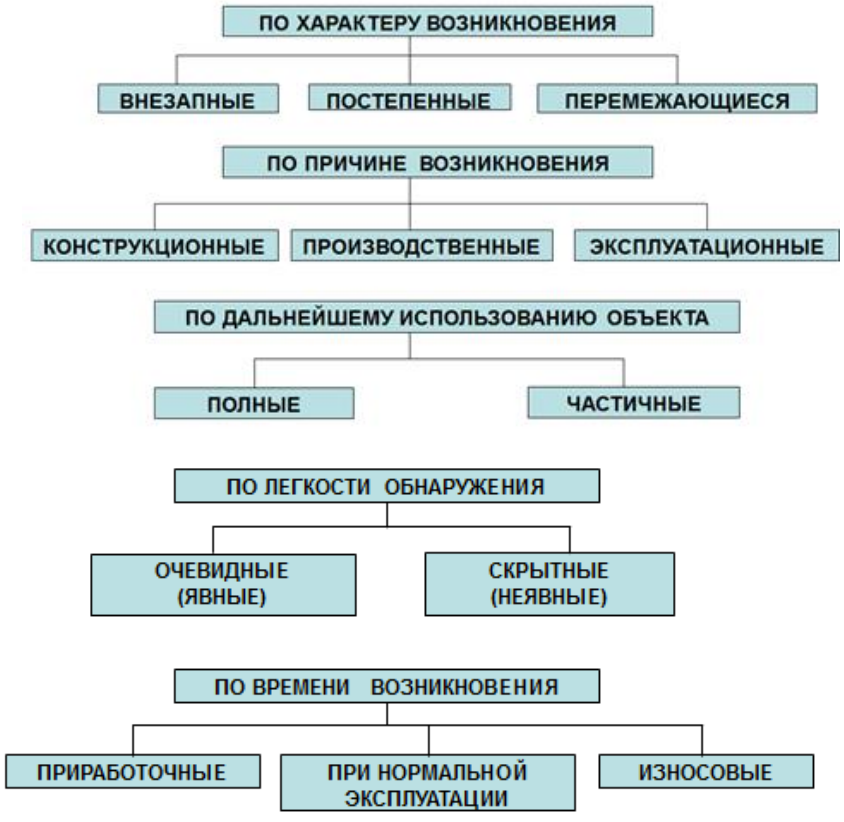


Рис. 1.1. Классификация отказов технических средств

По характеру возникновения различают:

— *внезапный отказ* – отказ, проявляющийся в резком (мгновенном) изменении характеристик технического объекта;

— *постепенный отказ* – отказ, происходящий в результате медленного, постепенного ухудшения характеристик технического объекта из-за износа и старения материалов;

— *перемежающийся отказ* – самоустраняющийся (возникающий и исчезающий) отказ (сбой).

По причине возникновения различают:

— *конструкционный отказ* – появляется в результате недостатков конструкции технического объекта;

— *производственный отказ* – связан с ошибками при изготовлении технического объекта из-за несовершенства технологии или ее нарушений;

— *эксплуатационный отказ* – связан с нарушениями правил эксплуатации технического объекта.

По дальнейшему использованию технического объекта различают:

— *полный отказ* – исключает использование технического объекта до его устранения;

— *частичный отказ* – при возникновении отказа технический объект может частично использоваться.

По лёгкости обнаружения различают:

— *очевидный (явный) отказ* – легко обнаруживается.

— *скрытый (неявный) отказ* – обнаруживается по косвенным признакам.

По времени возникновения различают:

— *приработочный отказ* – возникает в начальный период эксплуатации технического объекта.

— *отказ при нормальной эксплуатации* – отказ, возникший в период нормальной эксплуатации технического объекта.

— *износовый отказ* – вызван необратимыми процессами износа деталей и старением материала.

Предсказать моменты появления отказов в процессе функционирования технических средств АС невозможно, то есть поток отказов имеет случайный характер.

1.1.3. Математический аппарат теории надежности

Так как поток отказов технических средств АС имеет случайный характер, то основным математическим аппаратом теории надежности технических средств являются теория вероятности и теория статистики. Основными случайной величинами, исследуемыми в теории надежности технических объектов, являются время (наработка) до отказа (время безотказной работы) невосстанавливаемого объекта, время между отказами и время восстановления для восстанавливаемого объекта. Данные случайные величины являются непрерывными, то есть их возможные значения непрерывно заполняют некоторый интервал числовой оси, называемый иногда интервалом существования этой случайной величины. Таким образом, на любом конечном интервале существования число возможных значений непрерывной случайной величины бесконечно велико.

Случайная величина считается полностью заданной, если на числовой оси указаны ее возможные значения и установлен закон распределения. Законом распределения случайной величины называется соотношение, устанавливающее связь между возможными значениями случайной величины и соответствующими вероятностями. Про случайную величину говорят,

что она распределена по данному закону, или подчинена данному закону распределения. В качестве законов распределения непрерывной случайной величины используются функция распределения или плотность распределения вероятностей. Закон распределения дает полное вероятное описание случайной величины. По закону распределения можно судить до опыта о том, какие возможные значения случайной величины будут появляться чаще, а какие – реже.

Функцией распределения случайной величины *X* называется функция *F(x),* выражающая для каждого *x* вероятность того, что случайная величина *X* примет значение меньшее *x:*

$$F(x) = P(X < x). \tag{1}$$

Функцию *F(x)* иногда называют интегральной функцией распределения или интегральным законом распределения.

Функции распределения обладает следующими свойствами:

1. Функция распределения случайной величины есть неотрицательная функция, заключенная между нулем и единицей ($0 \le F(x) \le 1$);
2. Функция распределения случайной величины есть неубывающая функция на всей числовой оси;
3. На минус бесконечности функция распределения равна нулю, а на плюс бесконечности равна единице, т.е.

$$F(-\infty) = lim_{x\to-\infty} F(x) = 0, \quad F(+\infty) = lim_{x\to+\infty} F(x) = 1; \tag{2}$$

4. Вероятность попадания случайной величины в интервал $[x_1,x_2)$ равна приращению ее функции распределения на этом интервале, т.е.

$$P(x_1 \le X < x_2) = F(x_2) - F(x_1) \tag{3}$$

Плотность распределения вероятностей *f(x)* часто называют дифференциальным законом распределения случайной величины *X.* Вероятность попадания случайной величины в интервал от x_1 до x_2 при этом задается формулой:

$$P(x_1 \le X < x_2) = \int_{x_1}^{x_2} f(x)dx. \tag{4}$$

А функция распределения случайной величины (интегральный закон распределения) задается через плотность *f(x)* следующим выражением:

$$F(x) = \int_{-\infty}^{x} f(z)dz \tag{5}$$

Закон распределения случайной величины дает исчерпывающую информацию о ней, так как позволяет вычислить вероятности любых событий, связанных со случайной величиной. Однако такой закон распределения бывает трудно обозримым, не всегда удобным для анализа. Иногда бывает удобным оперировать числовыми характеристиками распределения случайной величины, в частности математическое ожидание и отклонениями от него (дисперсия и среднеквадратическое отклонение).

Математическое ожидание или средне значение непрерывной случайной величины определяется выражением

$$M[X] = \int_{-\infty}^{+\infty} f(x)dx. \tag{6}$$

Математическое ожидание случайной величины обладает следующими свойствами:

1. Математическое ожидание константы есть сама константа $M[C] = C$;

2. Математическое ожидание линейно, то есть $M[aX+bY] = aM[X] + bM[Y]$, где X и Y – случайные величины с конечным математическим ожиданием, a и b – произвольные константы;

3. Математическое ожидание сохраняет неравенства, то есть если $0 \le X \le Y$, и Y – случайная величина с конечным математическим ожиданием, то математическое ожидание случайной величиныX также конечно, и более того $0 \le M[X] \le M[Y]$;

4. Если$X = Y$, то $M[X] = M[Y]$;

5. Математическое ожидание произведения двух независимых или некоррелированных случайных величинX и Y равно произведению их математических ожиданий $M[X \cdot Y] = M[X] \cdot M[Y]$.

Дисперсия определяет рассеяние случайной величины около ее математического ожидания

$$D[X] = \int_{-\infty}^{+\infty} xf(x)(x - M[X])^2 dx. \quad (7)$$

Если извлечь квадратный корень из дисперсии, то получится величина, называемая среднеквадратическим отклонением $\sigma = \sqrt{D[X]}$.

В качестве теоретических распределений случайной величины T (времени (наработки) до отказа, времени между отказами и времени восстановления) со значениями t, расположенными в диапазоне $[0,\infty)$, наиболее часто используются следующие непрерывные распределения:

1. *Экспоненциальное распределение:*

$$F(t) = 1 - e^{-\lambda t}; \quad f(t) = \lambda e^{-\lambda t}; \quad M[T] = \frac{1}{\lambda}; \quad D[T] = \frac{1}{\lambda^2}; \quad \sqrt{D[\mathrm{T}]} = \frac{1}{\lambda}; \quad (8)$$

где λ – параметр распределения.

Экспоненциальный закон распределения – единственный из законов распределения, который обладает свойством «отсутствия последействия» (если промежуток времени z уже длился некоторое время τ, то экспоненциальный закон распределения остаётся таким же и для оставшейся части промежутка $t = z - \tau$, то есть $P(z > t + \tau / z > \tau) = P(z > t)$). Свойство отсутствия последействия имеет следующий смысл: каков бы ни был настоящий возраст, оставшееся время жизни не зависит от прошлого и имеет то же самое распределении, что и само время жизни. Широкое использование данного распределения в математических моделях реальных явлений обычно связано именно с этим характерным свойством.

2. *Усеченное нормальное распределение:*

$$F(t) = \frac{c}{\sigma\sqrt{2\pi}} \int_0^t e^{-\frac{(x-m)^2}{2\sigma^2}} dx; \quad f(t) = \frac{c}{\sigma\sqrt{2\pi}} e^{-\frac{(x-m)^2}{2\sigma^2}}; \quad (9)$$

$$M[T] = m + k\sigma; \quad \sqrt{D[\mathrm{T}]} = \sigma\sqrt{1 + k\frac{m}{\sigma} - k^2}; \quad (9а)$$

где c – нормирующий множитель;

σ, m – параметры нормального распределения (m – значение случайной величины, соответствующее максимальному значению $f(t)$ и называемое модой);

$k = \frac{c}{\sqrt{2\pi}} e^{-\frac{m^2}{2\sigma^2}}$.

Коэффициент c определяется из условия нормировки $\int_0^\infty f(t)dt = 1$, откуда

$$c = \frac{1}{0{,}5 + \Phi(\frac{m}{\sigma\sqrt{2}})}. \quad (10)$$

Усеченное нормальное распределение удобно для описания случайных величин, представляющих собой произведение достаточно большого числа случайных величин, подобно тому, как нормальное распределение описывает сумму большого числа случайных величин.

3. Распределение Вейбулла – Гнеденко:

$$F(t) = 1 - e^{-(\frac{t}{\beta})^k};\ \ f(t) = \frac{kt^{k-1}}{\beta^k} e^{-(\frac{t}{\beta})^k};\ \ M[T] = \beta\Gamma(1+\frac{1}{k}); \tag{11}$$

$$\sqrt{D[\mathrm{T}]} = \beta\sqrt{\Gamma(1+\frac{2}{k}) - \Gamma^2(1+\frac{1}{k})}; \tag{11a}$$

где $\Gamma(z) = \int_0^\infty x^{Z-1}e^{-x}\,dx$ – гамма-функция, параметр k определяет вид плотности распределения, параметр β – его масштаб.

Универсальность распределения Вейбулла – Гнеденко объясняется тем, что при $k = 1$ распределение совпадает с экспоненциальным распределением, когда интенсивность отказов постоянна, при $k > 1$ интенсивность отказов монотонно возрастает, а при $k < 1$ монотонно убывает. При $k = 2$ распределение Вейбулла – Гнеденко превращается в распределение Рэлея с плотностью $f(t) = 2\lambda te^{-\lambda t^2}$, где $\lambda = \frac{1}{\beta^2}$. Наряду с логарифмическим нормальным распределением распределение Вейбулла – Гнеденко хорошо описывает наработку технических объектов по усталостным разрушениям.

4. Распределение Релея:

$$F(t) = 1 - e^{-\frac{t^2}{2M^2}};\ \ f(t) = \frac{t}{M^2} e^{-\frac{t^2}{2M^2}};\ \ M[T] = M\sqrt{\frac{\pi}{2}}; \tag{12}$$

$$\sqrt{D[\mathrm{T}]} = M\sqrt{2 - \frac{\pi}{2}}; \tag{12a}$$

где M – параметр распределения Рэлея.

5. Гамма-распределение:

$$F(t) = \frac{1}{\Gamma(k)}\int_0^{\lambda t} x^{k-1}e^{-x}dx;\ \ f(t) = \frac{\lambda(\lambda t)^{k-1}}{\Gamma(k)} e^{-\lambda t}; \tag{13}$$

$$M[T] = \frac{k}{\lambda};\ \ \sqrt{D[\mathrm{T}]} = \frac{1}{\lambda}\sqrt{k}; \tag{13a}$$

где k и λ – параметры гамма-распределения.

Параметр k, характеризует асимметрию гамма-распределения, при $k > 1$ интенсивность отказа возрастает, при $k < 1$ убывает, а при $k = 1$ становится постоянной, т. е. гамма-распределение превращается в экспоненциальное.

6. Логарифмически нормальное распределение:

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}}\int_0^t \frac{1}{x} e^{-\frac{[ln(x)-\mu]^2}{2\sigma^2}}dx;\ \ f(t) = \frac{1}{t\sigma\sqrt{2\pi}} e^{-\frac{[\ln(t)-\mu]^2}{2\sigma^2}}; \tag{14}$$

$$M[T] = e^{\mu+\frac{1}{2}\sigma^2};\ \ \sqrt{D[\mathrm{T}]} = \sqrt{(e^{\sigma^2} - 1)\, e^{2\mu+\sigma^2}}; \tag{14a}$$

где μ и σ – параметры распределения.

Логарифмически нормальное распределение удобно для описания случайных величин, представляющих собой произведение достаточно большого числа случайных величин, подобно тому, как нормальное распределение описывает сумму большого числа случайных величин.

В теории надёжности часто применяются теоремы и формулы теории вероятностей:

1. Теорема о произведении вероятностей:

Вероятность произведения двух зависимых событий A и B равна произведению вероятности одного из них на условную вероятность другого, найденную в предположении, что первое событие уже наступило:

$$P(A \cdot B) = P(A) \cdot P(B/A). \quad (15)$$

Следствие 1. Вероятность произведения двух независимых событий A и B равна произведению вероятностей событий:

$$P(A \cdot B) = P(A) \cdot P(B). \quad (16)$$

Следствие 2. Вероятность произведения независимых событий $B_1, B_2, \ldots, B_n$ равна произведению вероятностей этих событий:

$$P(B_1, B_2, \ldots, B_n) = P(B_1) \cdot P(B_2) \cdot \ldots \cdot P(B_n). \quad (17)$$

2. Теорема о сумме вероятностей:

Вероятность суммы двух событий A и B равна сумме вероятностей этих событий минус вероятность их произведения:

$$P(A+B) = P(A) + P(B) - P(A \cdot B). \quad (18)$$

Следствие 1. Вероятность суммы несовместных событий A и B равна сумме вероятностей этих событий:

$$P(A+B) = P(A) + P(B). \quad (19)$$

Следствие 2. Вероятность суммы несовместных событий $B_1, B_2, \ldots, B_n$ равна сумме их вероятностей:

$$P(B_1 + B_2 + \ldots + B_n) = P(B_1) + P(B_2) + \ldots + P(B_n). \quad (20)$$

Следствие 3. Если события $B_1, B_2, \ldots, B_n$ образуют полную группу событий, то сумма их вероятностей равна единице, т.е.

$$P(B_1) + P(B_2) + \ldots + P(B_n) = 1. \quad (21)$$

3. Формула полной вероятности:

Если $B_1, B_2, \ldots, B_n$ – несовместные события и в сумме дают достоверное событие A, то вероятность события А можно вычислить, зная вероятности событий $B_1, B_2, \ldots, B_n$, а также условные вероятности этого события в предположении выполнения событий $B_1, B_2, \ldots, B_n$. Выполняется следующая формула:

$$P(A) = P(A/B_1) \cdot P(B_1) + P(A/B_2) \cdot P(B_2) + \ldots + P(A/B_n) \cdot P(B_n).$$

1.2. Показатели надёжности технических средств АС

1.2.1. Показатели надежности невосстанавливаемых объектов

Показатель – это количественная характеристика одного или нескольких свойств объекта, в частности надежности. Для невосстанавливаемых технических объектов ограничиваются показателями безотказности, для чего используют вероятностные характеристики случайной величины $\overline{T}$ – наработки объекта от начала его эксплуатации до первого отказа. Под наработкой понимают продолжительность или объем работы, измеряемые в часах, циклах или в других единицах. Когда наработку до отказа выражают в единицах времени, тогда исполь-

зуют термин «время безотказной работы» или «время до отказа». В этом случае значения *t* случайной величины $\overline{T}$ лежат в диапазоне [0,∞).

К числу показателей технических объектов относятся:

— *P(t)* – вероятность безотказной работы в течение времени *t* (*функция надежности*);
— *F(t)* – функция распределения времени до отказа (*функция ненадежности*);
— *f(t)* – плотность распределения времени до отказа (частота отказов);
— *λ (t)* – интенсивность отказов;
— *T* – среднее время безотказной работы (средняя наработка на отказ).

Вероятность безотказной работы P(t)

Вероятность безотказной работы объекта *P(t)* – это вероятность того, что случайная величина $\overline{T}$ (время безотказной работы) будет не менее некоторого значения *t*, отсчитываемого от начала эксплуатации, то есть вероятность того, что объект за время работы *t* не откажет:

$$P(t) = P(\overline{T} \geq t) = 1 - F(t), \quad (23)$$

где *F(t)* – функция распределения случайной величины $\overline{T}$.

Данное выражение определяется следующими соображениями:

1. Так как $F(t) = P(\overline{T} < t)$, то *F(t)* по сути является вероятностью того, что объект откажет за время *t;*
2. Событие, заключающееся в отказе объекта за время *t*, и событие, заключающееся в том, что объекта за время *t* не откажет, являются несовместными и составляют полную группу событий. Тогда из следствия теоремы о сумме вероятностей сумма вероятностей этих событий равна 1, то есть $P(t) + F(t) = 1$.

Вероятность безотказной работы *P(t)* и функция распределения времени до отказа *F(t)* обладают следующими свойствами (рисунок 1):

1. $P(0) = 1$ и $F(0)=0$, т.е. можно рассматривать безотказную работу лишь тех систем, которые были работоспособны в момент начала работы.
2. *P(t)* и *F(t)* являются монотонными функциями от времени *t*.
3. $P(\infty) = 0$ и $F(\infty) = 1$, т.е. любая система со временем откажет.

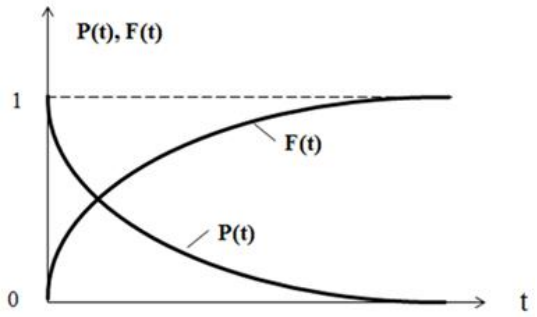


Рис. 1.1. Свойства вероятности безотказной работы P(t) и функции распределения времени до отказа F(t).

Статистические значения вероятности безотказной работы $P^*(t)$ и функции распределения времени до отказа $F^*(t)$ определяются следующими выражениями:

$$P^*(t) = \frac{No - n(t)}{No}; \quad F^*(t) = \frac{n(t)}{No}; \quad (24)$$

где *n(t)* – число отказавших образцов к моменту времени *t*;

No – общее число образцов, поставленных на испытание.

В некоторых задачах надежности приходится определять условную вероятность безотказной работы $P(t,\tau)$ в течение времени τ при условии, что к моменту времени t система была работоспособной.

Рассмотрим два интервала $(0,t)$ и (t,τ). Событие, состоящее в безотказной работе в течение интервала $(0,\tau)$, является совмещением двух зависимых событий:

1) система безотказно проработала на интервале $(0,t)$;
2) работоспособная к моменту t система безотказно проработала на интервале (t,τ).

Поэтому согласно правилу умножения вероятностей:

$$P(t+\tau) = P(t)\,P(t,\tau), \tag{25}$$

следовательно

$$P(t,\tau) = \frac{P(t+\tau)}{P(t)}. \tag{26}$$

Таким образом, условная вероятность безотказной работы на интервале (t,τ) равна отношению значений вероятности безотказной работы в начале и конце интервала.

Плотность распределения времени до отказа (частота отказов) f(t)

$$f(t) = \frac{dF(t)}{dt} = -\frac{dP(t)}{dt}. \tag{27}$$

Плотность распределения времени до отказа $f(t)$ обладает следующими свойствами:

1. $f(t)$ является дифференциальной формой закона распределения времени (наработки) до отказа.
2. $f(t)$ – неотрицательная функция, причем $\int_0^\infty f(t)dt = 1$.

Статистическое значение плотности распределения времени до отказа $f^*(t)$ определяется следующим выражением:

$$f^*(t) = \frac{n(t,t+\Delta t)}{No\Delta t}; \tag{28}$$

где $n(t,t+\Delta t)$ – число отказавших образцов в промежутке времени $(t,t+\Delta t)$;

No – общее число образцов, поставленных на испытание.

Функции $F(t)$ и $P(t)$ безразмерны. Функция $f(t)$ измеряется в единицах обратных наработке (1/ч).

Интенсивность отказов λ(t)

Интенсивность отказов $\lambda(t)$ – условная плотность вероятности возникновения отказа невосстанавливаемой системы, определяемая для рассматриваемого времени (наработки) при условии, что до этого времени (наработки) отказ не возник. Интенсивность отказов можно рассматривать как относительную скорость уменьшения значений вероятности безотказной работы с увеличением интервала $(0,t)$.

Рассмотрим условную вероятность отказа системы $F(t,\Delta t)$ на интервале $(t, t+\Delta t)$

$$F(t,\Delta t) = 1 - P(t, \Delta t) = 1 - \frac{P(t+\Delta t)}{P(t)} = -\frac{P(t+\Delta t)-P(t)}{P(t)}. \tag{29}$$

Разделим $F(t,\Delta t)$ на Δt

$$\frac{F(t,\Delta t)}{\Delta t} = -\frac{P(t+\Delta t)-P(t)}{\Delta t}\cdot\frac{1}{P(t)}. \tag{30}$$

Тогда

$$\lambda(t) = lim_{\Delta t \to 0} \frac{F(t,\Delta t)}{\Delta t} = lim_{\Delta t \to 0} \left[- \frac{P(t+\Delta t) - P(t)}{\Delta t} \cdot \frac{1}{P(t)} \right] =$$

$$= \frac{dF(t)}{dt} \cdot \frac{1}{P(t)} = \frac{f(t)}{P(t)}. \quad (31)$$

Выразим *P(t)* через *λ(t)*

$$\int_0^t \lambda(t)\,dt = - \int_0^t \frac{dP(t)}{P(t)} = - \ln P(t). \quad (32)$$

Отсюда

$$P(t) = e^{-\int_0^t \lambda(t)dt}. \quad (33)$$

Функция $\lambda(t)$ так же как и *f(t)* измеряется в единицах обратных наработке (1/ч).
Для статистического определения интенсивности отказов в выражение

$$\lambda(t) = \frac{f(t)}{P(t)} \quad (34)$$

вместо *f(t)* подставим $f^*(t)$, а вместо *P(t)* подставим $P^*(t)$, тогда

$$\lambda^*(t) = \frac{n(t,t+\Delta t)}{[No - n(t)]\Delta t}, \quad (35)$$

где $No - n(t)$ – число работоспособных образцов к моменту времени *t*.

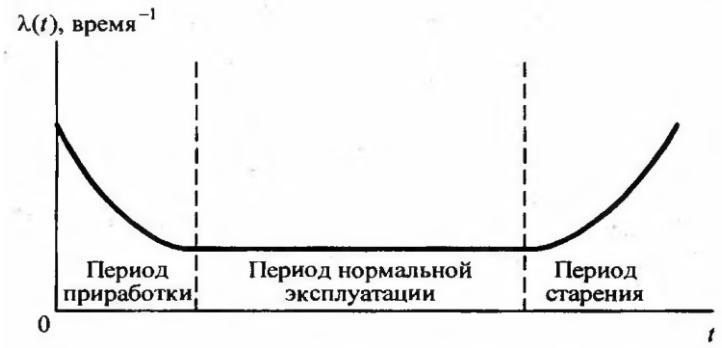


Рис. 1.2. Свойства интенсивности отказов

На первом участке выявляются скрытые дефекты изготовления отдельных элементов системы, недостатки монтажа, наладки, нарушения, произошедшие в результате транспортировки.

На периоде нормальной эксплуатации интенсивность отказов относительно неизменна. Именно этот участок соответствует основному времени эксплуатации систем.

Возрастание кривой $\lambda(t)$ относится к периоду старения системы из-за износа отдельных ее элементов и изменения их характеристик.

Среднее время безотказной работы T

$$T = M(\overline{T}) = \int_0^\infty t f(t) dt = \int_0^\infty P(t) dt, \quad (36)$$

где $M(\overline{T})$ – математическое ожидание случайной величины $\overline{T}$ (времени безотказной работы).

Статистическое значение среднего времени безотказной работы T^* определяется следующим выражением:

$$T^* = \frac{\sum_{i=1}^{r} t_i + (N_0 - r)t_u}{N_0}, \quad (37)$$

где t_u – время испытаний;

t_i – время до отказа i-го объекта, поставленного на испытание;

r – общее число отказавших объектов за время испытаний t_u;

N_0 – общее число объектов, поставленных на испытание.

1.2.2. Показатели надежности восстанавливаемых объектов

В отличие от невосстанавливаемых технических объектов, работающих до первого отказа, восстанавливаемые объекты после отказа ремонтируются, то есть восстанавливают работоспособность, и вновь используются по назначению до очередного отказа, вновь восстанавливаются и опять используются. Этот процесс продолжается до наступления предельного состояния объекта, когда его использование по назначению невозможно или нецелесообразно. Показатели надежности восстанавливаемых объектов должны соответствовать такому режиму их функционирования.

К показателям надежности восстанавливаемых объектов относятся:

1. Показатели безотказности:

   $\omega(t)$ – параметр потока отказов;

   T_0 – среднее время между отказами.
2. Показатели ремонтопригодности:

   $T_В$ – среднее время восстановления.
3. Комплексные показатели надежности:

   $K_Г(t)$ – функция готовности – вероятность того, что объект исправен в момент времени t;

   $K_П(t)$ – функция простоя – вероятность того, что объект в момент времени t неисправен и восстанавливается;

   $K_Г$ – коэффициент готовности – вероятность того, что объект будет исправен при длительной эксплуатации;

   $K_П$ – коэффициент простоя – вероятность того, что объект будет неисправен при длительной эксплуатации.

Для восстанавливаемых систем основным понятием является поток отказов – последовательность отказов, происходящих один за другим в случайные моменты времени. Наиболее часто встречаются модели, которые заключаются в том, что поток отказов является простейшим, а наработка на отказ распределена экспоненциально.

Поток является *простейшим* (однородным, Пуассоновским) при условии его *стационарности, ординарности* и *отсутствия последствия*.

Стационарность потока означает, что количество отказов, возникающих в некотором интервале времени, не зависит от положения этого интервала на временной оси ($\omega(t) = \omega = const$). Т.е. поток не должен иметь тенденции к возрастанию или убыванию.

Ординарность потока означает, что вероятность одновременного наступления двух или более независимых отказов пренебрежимо мала по сравнению с вероятностью наступления одного отказа.

Поток отказов *не имеет последствия*, если количество отказов системы в будущем не зависит от предыстории.

Простейший поток можно ожидать при формировании его из суммы большого числа независимых потоков отказов узлов, время до отказа которых могут быть распределены по любому закону.

Условия применения простейшего потока также следуют из предельной теоремы А.Я. Хинчина. Согласно этой теореме сумма m независимых стационарных и ординарных потоков при весьма общих условиях и при $m \longrightarrow \infty$ стремится к простейшему потоку.

Параметр потока отказов ω(t)

При задании потока отказов как дискретного случайного процесса $\eta(t)$ – числа отказов на интервале $(0,t)$ – показателем безотказности является параметр потока отказов $\omega(t)$, определяемый следующим соотношением:

$$\omega(t) = \frac{dW(t)}{dt}, \tag{38}$$

где $W(t)=M[\eta(t)]$ – ведущая функция потока, определяемая как математическое ожидание числа отказов за время t.

Статистическое значение параметр потока отказов $\omega^*(t)$ определяется следующим выражением:

$$\omega^*(t) = \frac{n(t,t+\Delta t)}{N\Delta t}, \tag{39}$$

где $n(t,t+\Delta t)$ – число отказавших образцов за промежуток времени $(t,t+\Delta t)$ при условии, что отказавшие образцы мгновенно восстанавливаются или заменяются новыми;

N – число образцов, постоянно находящихся на испытании.

Параметр потока отказов $\omega(t)$ имеет следующие свойства:

1. $\omega(t) = \lambda$ при экспоненциальном законе $(F(t) = 1 - e^{-\lambda t})$ времени до отказа объекта и мгновенном его восстановлении;
2. В простейшем потоке средняя наработка на отказ (среднее время между отказами) T и параметр потока связаны соотношением:

$$T = \frac{1}{\omega}; \tag{40}$$

3. $\omega(t) = f(t) + \int_0^t \omega(x) f(t - x)dx$, где $f(t)$ – плотность распределения времени безотказной работы невосстанавливаемого объекта.

Третье свойство устанавливает зависимость между показателями надежности восстанавливаемых и невосстанавливаемых объектов.

Средняя наработка на отказ (среднее время между отказами) T

Статистическое значение среднего времени между отказами T^*определяется следующим выражением:

$$T^* = \sum_{i=1}^{N} \frac{t_i}{N}, \tag{41}$$

где t_i – время между отказами i-го образца, полученное при условии, что отказавшие образцы мгновенно восстанавливаются или заменяются новыми,

N – число образцов, постоянно находящихся на испытании.

Среднее время восстановления T_B

Ранее предполагалось, что продолжительностью восстановления можно пренебречь, так как на практике она значительно меньше времени между отказами. Однако нельзя не учитывать продолжительность восстановления для решения многих задач надежности (например, расчета потерь из-за отказов, количества необходимого ремонтного персонала).

Пусть $\overline{T}_{\text{в}}$ – случайное время восстановления работоспособного состояния системы после отказа, $G(t) = P(\overline{T}_{\text{в}} < t)$ – вероятность восстановления работоспособного состояния системы за заданное время t, тогда среднее время восстановления $T_{\text{В}}$ будет равно

$$T_{\text{В}} = M[\overline{T}_{\text{в}}] = \int_0^{\infty} tg(t)dt, \quad (42)$$

где $g(t) = \frac{dG(t)}{dt}$.

Статистическое значение среднего времени восстановления $T_{\text{В}}^*$ определяется следующим выражением:

$$T_{\text{В}}^* = \sum_{i=1}^{N} \frac{\tau_{\text{i}}}{N}, \quad (43)$$

где τ_{i} – время восстановления i-го образца, полученное при условии, что отказавшие образцы восстанавливаются или заменяются новыми,

N – число образцов, постоянно находящихся на испытании.

Комплексные показатели надежности

Статистические значения функции готовности $K_{\Gamma}^*(t)$ и функции простоя $K_{\Pi}^*(t)$ определяются следующими выражениями:

$$K_{\Gamma}^*(t) = \frac{t_{\Sigma}(t)}{t_{\Sigma}(t) + \tau_{\Sigma}(t)}; \quad K_{\Pi}^*(t) = \frac{\tau_{\Sigma}(t)}{t_{\Sigma}(t) + \tau_{\Sigma}(t)}; \quad (44)$$

где $t_{\Sigma}(t)$ – суммарное время исправной работы к моменту времени t,

$\tau_{\Sigma}(t)$ – суммарное время простоя к моменту времени t.

Коэффициент готовности K_{Γ} и коэффициент простоя K_{Π} являются предельными значениями соответствующих функций $K_{\Gamma}(t)$ и $K_{\Pi}(t)$:

$$lim_{t\to\infty} K_{\Gamma}(t) = K_{\Gamma} = \frac{T}{T+T_{\text{В}}}, \quad lim_{t\to\infty} K_{\Pi}(t) = K_{\Pi} = \frac{T_{\text{В}}}{T+T_{\text{В}}} \quad (45)$$

Функция готовности $K_{\Gamma}(t)$ и функция простоя $K_{\Pi}(t)$, а также коэффициент готовности K_{Γ} и коэффициент простоя K_{Π} обладают следующим свойством:

$$K_{\Gamma}(t) + K_{\Pi}(t) = 1, \quad K_{\Gamma} + K_{\Pi} = 1. \quad (46)$$

1.3. Резервирование как способ обеспечения надежности технических средств АС

Резервирование – это одно из основных средств обеспечения заданного уровня надежности (особенно безотказности) объекта при недостаточно надежных элементах. При резервировании применяются дополнительные средств и возможности (избыточность) с целью сохранения работоспособного состояния системы при отказе одного или нескольких его элементов. Существуют различные виды резервирования: структурное, временное, информационное, функциональное, нагрузочное.

Структурное резервирование (аппаратурное, элементное, схемное), предусматривает применение резервных элементов структуры системы. При структурном резервировании используют такие понятия как основной элемент и резервный элемент. *Основной элемент* — элемент структуры системы, необходимый для выполнения системой требуемых функций при отсутствии отказов её элементов. *Резервный элемент* – элемент системы, предназначенный для выполнения функций основного элемента, в случае отказа последнего.

Временное резервирование связано с использованием резервов времени. Предполагается, что на выполнение системой необходимой работы отводится время больше чем необходимо. Избыточное время используется, например, для двойного или тройного просчёта по программе на ЭВМ и сравнения полученных результатов с целью выбора правильного результата по мажоритарному правилу. Временное резервирование является эффективным средством борьбы со сбоями ЭВМ.

Информационное резервирование — это резервирование с применением избыточности информации. Например, многократная передача одного и того же сообщения по каналу связи. Избыток информации позволяет в той или иной мере компенсировать искажения передаваемой информации или устранять их.

Функциональное резервирование — резервирование, при котором заданная функция может выполняться различными способами и техническими средствами. Например, функция передачи информации в АС может выполняться с использованием радиоканалов, телеграфа, телефона и других средств связи.

Нагрузочное резервирование — это резервирование с применением нагрузочных резервов. Заключается в обеспечении оптимальных запасов способности элементов выдерживать действующие на них нагрузки.

При структурном резервировании возможны различные способы резервирования основных элементов резервными элементами: *общее, раздельное и смешанное резервирование*. При *общем резервировании* вся система резервируется аналогичной системой. При *раздельном резервировании* резервируются отдельные элементы системы. *Смешанное резервирование* предполагает сочетание в одной и той же системе как раздельного так и общего (резервируются отдельные группы элементов) резервирования.

В зависимости от способа подключения резервных элементов к основным различают *постоянное* и *динамическое резервирование*. *Постоянное резервирование* - это резервирование без перестройки структуры системы при возникновении отказа её элементов. *Динамическое резервирование* при возникновении отказов элементов предусматривает перестройку структуры системы. Например, разновидностью динамического резервирования является *резервирование замещением*, когда функции основного элемента передаются резервному только после отказа основного элемента.

Различные способы резервирования и подключения резервных элементов удобно не описывать словесно, а изображать в виде надёжностных схем. Существуют определенные правила изображения таких схем:

1. Отдельные основные элементы, составляющие систему, изображаются в виде последовательной цепочки (основное соединение элементов);

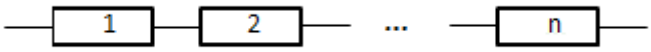


Рис. 1.3. Основное соединение элементов

2. Подключение резервных элементов к основным изображаются в виде параллельного соединения. При этом постоянное резервирование изображается как постоянное подключение (рис. 1.4.а), а динамическое резервирование – в виде стрелок (рис. 1.4.б).

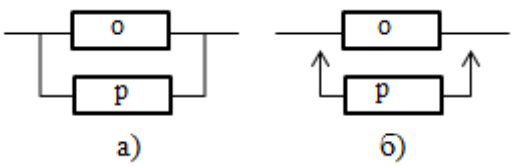


Рис. 1.4. Постоянное резервирование - а), динамическое – б)

На рисунке 1.5 приведены различные способы резервирования и подключения резервных элементов в соответствии с правилами изображения надёжностных схем.

Резервирование замещением имеет ряд преимуществ перед постоянным включением резерва:

— сохраняет надежность резервных элементов, так как при работе основных элементов они находятся в нерабочем состоянии;

— позволяет использовать резервный элемент на несколько основных элементов.

Однако существенным недостатком резервирования замещением является необходимость наличия переключающих устройств. При раздельном резервировании число переключающих устройств равно числу основных элементов, что может сильно понизить надежность всей системы. Поэтому резервировать замещением выгодно крупные узлы или всю систему, а во всех других случаях – при высокой надежности переключающих устройств

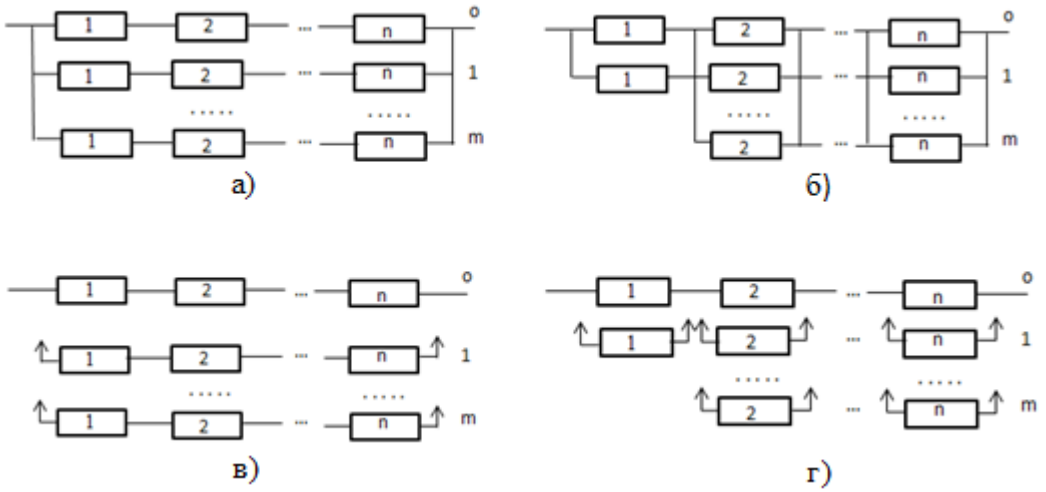


Рис. 1.5. Надёжностные схемы: общего резервирования с постоянно включенным резервом – а), раздельного резервирования с постоянно включенным резервом – б), общего резервирования с включением резерва замещением – в), раздельного резервирования с включением резерва замещением – г)

Скользящее резервирование — это резервирование замещением, при котором группа основных элементов объекта резервируется одним или несколькими резервными элементами, каждый из которых может заменить любой отказавший основной элемент в данной группе (рис. 1.6).

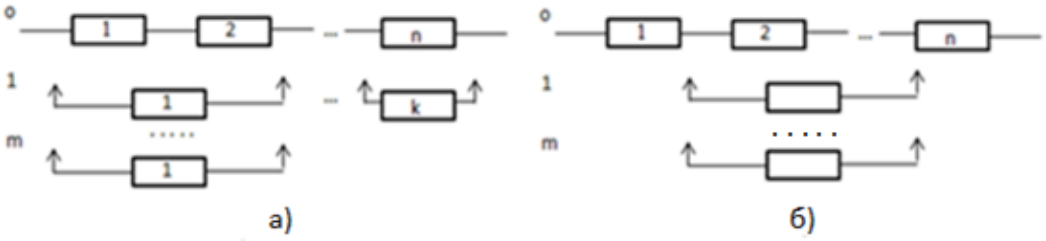


Рис. 1.6. Скользящее резервирование: а) – неоднородными, б) – однородными элементами

Мажоритарное резервирование — способ, основанный на применении мажоритарного элемента, который выполняет операцию «голосования» т.е. принятия окончательного решения по принципу большинства.

При совпадении значений выходных параметров *k-l* устройств, если допустим одновременный отказ *l* устройств, а *k* и *l* связаны между собой формулой $k = 2l + 1$, изделие в целом считают исправным.

На практике наибольшее распространение получил МЭ, для которого $l=1$, а $k = 3$ (рис. 1.7).

1.4. Расчет показателей надежности технических средств АС

1.4.1. Методы расчета надежности технических систем

Рассчитать надежность технической системы – значит определить её показатели надежности по известным показателям надежности элементов. Существует несколько методов расчета надежности технических систем, основанных на различных математических подходах:

- методы, основанные на применении теорем теории вероятностей;
- логико-вероятностные методы;
- топологические методы;
- методы, основанные на теории марковских процессов;
- метод статистического моделирования.

К методам, основанным на применении теорем теории вероятностей, относятся:

- метод перебора гипотез;
- метод, основанный на применении классических теорем теории вероятностей;
- метод минимальных путей и минимальных сечений.

В методе *перебора гипотез* из всех возможных состояний системы выбираются только те состояния (гипотезы), которые соответствуют работоспособности системы, вероятности этих гипотез выражаются через вероятности безотказной работы элементов системы, а их сумма и составляет вероятность безотказной работы системы.

Метод, *основанный на применении классических теорем теории вероятностей*, использует декомпозицию (разбиение) надёжностной схемы системы на узлы, для узлов рассчитываются их вероятности безотказной работы и вероятность безотказной работы всей системы. При расчетах широко используются классические теоремы теории вероятностей (теоремы сложения и умножения вероятностей).

В методе *минимальных путей и минимальных сечений* используются понятия «минимальный путь» и «минимальное сечение». *Минимальный путь* — такой набор элементов в надёжностной схеме, при котором система исправна, если исправны все элементы этого набора; отказ любого из элементов ведет к отказу системы. *Минимальное сечение* — такой набор элементов в схеме, при котором система неисправна, если неисправны все элементы этого набора; исключение любого элемента из набора переводит систему в исправное состояние. У системы может быть несколько минимальных путей и минимальных сечений. Последовательное соединение из *n* элементов имеет один минимальный путь и *n* минимальных сечений, проходящих через каждый элемент. Параллельное соединение из *n* элементов имеет *n* минимальных путей, проходящих через каждый элемент, и одно минимальное сечение. Множество всех минимальных путей определяет множество работоспособных состояний системы, а множество всех минимальных сечений – множество неработоспособных состояний системы. Для работоспособных или неработоспособных состояний (выбирается меньшее количество состояний) определяются их вероятности, а на их основе – вероятность безотказной работы всей системы.

Любой метод расчёта надежности требует описания условий работоспособности системы. Рассмотренные выше методы используют надёжностную схему системы, правила составления схемы приведены в п. 1.3. Для описания условий работоспособности системы также

применяются словесное описание функционирования системы, граф состояний системы и функции алгебры логики.

Логико-вероятностные методы расчёта надежности позволяет формализовать определение и смысл благоприятных гипотез с помощью функций алгебры логики. Неработоспособное состояние каждого элемента кодируется нулем ($\bar{a}_i$), а работоспособное – единицей (a_i). Условие работоспособности системы записывается с помощью функций алгебры логики через работоспособность (состояние) ее элементов ($\bar{a}_i$ и a_i). В полученную двоичную функцию работоспособности системы вместо двоичных переменных $\bar{a}_i$ и a_i подставляются вероятности соответственно вероятности отказа $1–p_i$ и безотказной работы p_i. Знаки конъюнкции и дизъюнкции заменяются алгебраическими умножением и сложением. Полученное выражение и есть вероятность безотказной работы системы.

Топологические методы позволяют определить показатели надежности невосстанавливаемых и восстанавливаемых систем либо по надёжностной схеме, либо по графу состояний системы, не составляя и не решая уравнений.

Методы, основанные на теории марковских процессов, анализируют граф состояний технической системы. Для всех состояний графа по определённым правилам записывается система обыкновенных дифференциальных уравнений Колмогорова. При условии длительной эксплуатации анализируемой технической системы дифференциальные уравнения сводятся к системе линейных алгебраических уравнений, которая должна решаться вместе с условием, что сумма вероятностей всех состояний технической системы равна единице. Решением системы линейных алгебраических уравнений являются вероятности состояний графа, которые позволяют рассчитать показатели надёжности технической системы.

Метод статистического моделирования (Монте-Карло), как правило, используется в случаях, когда выше перечисленными аналитическими методами рассчитать показатели надёжности системы не удаётся. Сущность метода состоит в построении алгоритма, имитирующего «надёжностное» поведение системы, и реализации этого алгоритма на ЭВМ. В результате статистического моделирования системы получается серия частных значений искомых показателей надежности, например, времена до отказа элементов системы. Эти значения обрабатываются методами математической статистики, что позволяет получить сведения о надежности реальной системы в произвольные моменты времени. Если количество реализаций алгоритма достаточно велико, то результаты моделирования системы приобретают статистическую устойчивость и могут быть приняты в качестве оценок искомых показателей надежности.

1.4.2. Расчет показателей надежности невосстанавливаемых систем

Для расчёта показателей надёжности невосстанавливаемых систем воспользуемся методом гипотез.

Пусть:

1. Невосстанавливаемая система с позиции надёжности состоит из n элементов и имеет произвольную надёжностную схему;
2. Каждый элемент может находиться только в одном из двух состояний: состоянии работоспособности и состоянии отказа;
3. Пусть p_i – вероятность работоспособного, а q_i – вероятность отказового состояния i-го элемента, $p_i + q_i = 1$.

Тогда система может находиться в 2^n состояниях, каждому состоянию соответствует своя гипотеза H (событие):

— H_0 – все n элементов работоспособны;

— H_i – отказал i-й элемент, а остальные работоспособны;

— $H_{i,j}$ – отказали i-й и j-й элементы, а остальные работоспособны;

…..

— $H_{1,2\ldots n}$ – отказали все элементы.

Если предположить, что отказы элементов события, то по теореме умножения вероятностей можно найти вероятности всех гипотез:

$$\begin{gathered} P(H_0) = p_1 p_2 \ldots p_n, \\ P(H_i) = p_1 p_2 \ldots q_i \ldots p_n, \\ P(H_{i,j}) = p_1 p_2 \ldots q_i \ldots q_j \ldots p_n, \\ \ldots \\ P(H_{1,2,\ldots,n}) = q_1 q_2 \ldots q_n. \end{gathered} \tag{47}$$

Сумма вероятностей всех гипотез равна единице, так как они составляют полную группу событий.

Вероятность безотказной работы системы по теореме сложения вероятностей будет равна сумме вероятностей тех гипотез, которые соответствуют работоспособному состоянию системы, т.е.

$$P = \sum_{i \in I+} P(H_i). \tag{48}$$

Выражение означает, что суммирование осуществляется по всем гипотезам, которые соответствуют работоспособному состоянию системы.

1.4.2.1. Расчет надежности нерезервированной системы

Постановка задачи:

Дано:

Надёжностная схема невосстанавливаемой системы;

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

$f_i(t)$ – плотность распределения времени до отказа i-го элемента.

Определить:

$P_c(t)$ – вероятность безотказной работы системы;

$f_c(t)$ – плотность распределения времени до отказа системы;

T_c – среднее время безотказной работы системы;

$\lambda_c(t)$ – интенсивность отказа.

Рис. 1.8. Надёжностная схема невосстанавливаемой систем

Пусть:

X_i – время до отказа i-го элемента,

X_c – время до отказа системы.

Тогда:

$$P_c(t) = P(X_c > t) = P(X_1 > t \,\&\, X_2 > t \,\&\, \ldots \,\&\, X_n > t) = \prod_{i=1}^{n} P_i(t); \tag{49}$$

$$f_c(t) = -P_c'(t) = \sum_{i=1}^{n} P_1(t) \ldots f_i(t) \ldots P_n(t); \tag{50}$$

$$T_c = \int_0^\infty t f_c(t) dt = \int_0^\infty P_c(t) dt; \tag{51}$$

$$\lambda_c(t) = \frac{f_c(t)}{P_c(t)} = \sum_{i=1}^{n} \frac{f_i(t)}{P_i(t)}\,. \tag{52}$$

Для этапа нормальной эксплуатации системы, когда $\lambda_i(t) = \lambda_i$ и $P_i(t) = e^{-\lambda_i t}$,

$$P_c(t) = \prod_{i=1}^{n} P_i(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\lambda_c t}, \tag{53}$$

где $\lambda_c = \sum_{i=1}^{n} \lambda_i$.

$$T_c = \int_0^{\infty} P_c(t)dt = \int_0^{\infty} e^{-\lambda_c t} dt = \frac{1}{\lambda_c}. \tag{54}$$

1.4.2.2. Расчет надежности резервированной системы

Система с общим резервированием и постоянно включенным резервом.

Постановка задачи*:*

Дано:

Надёжностная схема системы с общим резервированием и постоянно включенным резервом,

$P_i(t)$ – вероятность безотказной работы i-го элемента,

$f_i(t)$ – плотность распределения времени до отказа i-го элемента.

Определить:

$P_c(t)$ – вероятность безотказной работы системы,

$f_c(t)$ – плотность распределения времени до отказа системы,

T_c – среднее время безотказной работы системы,

$\lambda_c(t)$ – интенсивность отказа.

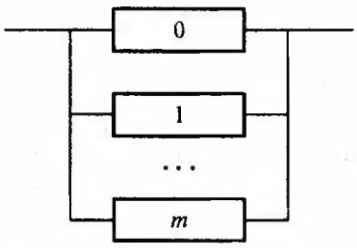


Рис. 1.9. Надёжностная схема системы с общим резервированием и постоянно включенным резервом: 0 – основной элемент, 1…m – резервные элементы

Пусть $Q_c(t)$ – вероятность отказа системы $Q_c(t) = 1 - P_c(t)$, тогда:

$$Q_c(t) = P(X_c \le t) = P(X_0 \le t \,\&\, X_1 \le t \,\&\, \ldots \,\&\, X_m \le t) = \prod_{i=0}^{m} Q_i(t). \tag{55}$$

Так как $Q_i(t) = 1 - P_i(t)$, то

$$P_c(t) = 1 - Q_c(t) = 1 - \prod_{i=0}^{m}(1 - P_i(t)); \tag{56}$$

$$f_c(t) = Q_c'(t) = \sum_{i=0}^{m}(1 - P_0(t)) \ldots f_i(t) \ldots (1 - P_m(t)); \tag{57}$$

$$\lambda_c(t) = \frac{f_c(t)}{P_c(t)} = \frac{\sum_{i=0}^{m}(1-P_0(t)) \ldots f_i(t) \ldots (1-P_m(t))}{1-\prod_{i=0}^{m}(1-P_i(t))}. \tag{58}$$

Для однородных систем и постоянной интенсивности отказов, когда $\lambda_0 = \lambda_1 = \ldots = \lambda_m = \lambda$

$$P_c(t) = 1 - (1 - P(t))^{m+1} = 1 - (1 - e^{-\lambda t})^{m+1}; \quad (59)$$

$$\lambda_c(t) = -\frac{P'_c(t)}{P_c(t)} = \frac{(m+1)\lambda e^{-\lambda t}(1-e^{-\lambda t})^m}{1-(1-e^{-\lambda t})^{m+1}}; \rightarrow \lambda_c(0) = 0; \ lim_{t\to\infty} \lambda_c(t) = \lambda; \quad (60)$$

$$T_c = \int_0^\infty P_c(t)dt = T_0 \sum_{k=1}^{m+1} \frac{1}{k}; \quad (61)$$

где $T_0 = \frac{1}{\lambda}$.

Резервированная система с дробной кратностью и нагруженным резервом

Постановка задачи:

Дано:

Резервированная система с дробной кратностью и нагруженным резервом;

$P(t)$ – вероятность безотказной работы элемента;

$f(t)$ – плотность распределения времени до отказа элемента.

Определить:

$P_c(t)$ – вероятность безотказной работы системы;

$f_c(t)$ – плотность распределения времени до отказа системы;

T_c – среднее время безотказной работы системы;

$\lambda_c(t)$ – интенсивность отказа.

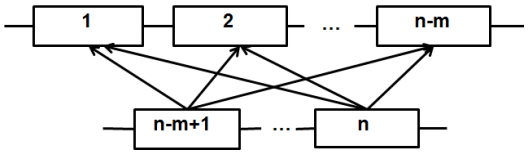


Рис. 1.10. Надёжностная схема резервированной системы с дробной кратностью и нагруженным резервом: m – количество резервных элементов, n – общее количество элементов

Подобные системы часто называют мажоритарными. Система работоспособна при отказе не более чем *m* элементов из *n* (все элементы с позиции надежности однородны и *n* > *m*).

Пусть:

a_i – событие, когда отказывают *i* элементов *(0 ≤ i ≤ m)* из *n*,

A – событие, когда система работоспособна.

Тогда

$$A = \sum_{i=0}^{m} a_i, \ P(A) = \sum_{i=0}^{m} P(a_i), \ \ P(a_i) = C_n^i Q^i(t) P(t)^{n-i}, \quad (62)$$

где

$C_n^i = \frac{n!}{(n-i)!i!}$ – число сочетаний из n по *i*,

Q(t) = 1 – P(t) – вероятность отказа элемента за время *t*,

$$P_c(t) = P(A) = \sum_{i=0}^{m} C_n^i Q(t)^i P(t)^{n-i}, \quad (63)$$

$$f_c(t) = -P'_c(t) = (n-m) C_n^m Q(t)^m P(t)^{n-m-1} f(t), \quad (64)$$

$$\lambda_c(t) = \frac{f_c(t)}{P_c(t)} = \lambda(t) \frac{C_n^m Q^m(t) P(t)^{n-m}(n-m)}{\sum_{i=0}^{m} C_n^i Q^i(t) P(t)^{n-i}}. \quad (65)$$

Система с общим резервированием замещением

Постановка задачи:

Дано:

Система с общим резервированием замещением;

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

$f_i(t)$ – плотность распределения времени до отказа i-го элемента.

Определить:

$P_c(t)$ – вероятность безотказной работы системы;

T_c – среднее время безотказной работы системы.

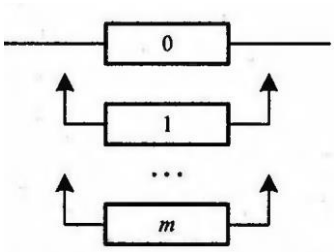


Рис. 1.11. Надёжностная схема системы с общим резервированием замещением: 0 – основной элемент, 1…m – резервные элементы

Поскольку отказ системы наступает при отказе всех m + 1 элементов, то

$$X_c = \sum_{i=0}^{m} x_i, \tag{66}$$

где x_i – время до отказа i-го элемента;

X_c – время до отказа системы.

Плотность суммы независимых случайных величин равна свертке плотностей слагаемых

$$f_\Sigma(t) = f_0^* f_1^* \ldots f_{m-1}^* f_m(t), \tag{67}$$

где $f*f(t) = \int_0^t f(x)f(t-x)dx$; $f*f*f(t) = \int_0^t f(x)\int_0^{t-x} f(y)f(t-x-y)dy\,dx$.

Рассмотрим случай, когда $m = 1$.

Система проработает безотказно в течение времени t при наступлении одного из двух несовместных событий:

1. *А* – элемент 0 проработает безотказно в течение времени t;
2. *Б* – элемент 0 откажет в момент времени x $(x < t)$, а элемент с номером 1 проработает безотказно в течение оставшегося времени $t - x$.

$$P(A) = P_0(t), \tag{68}$$

$$P(Б) = \int_0^t f_0(x)P_1(t-x)dx = f_0 * P_1(t). \tag{69}$$

По теореме сложения вероятностей

$$P_c(t) = P_0(t) + f_0^* P_1(t). \tag{70}$$

Для общего случая

$$P_c(t) = \sum_{i=0}^{m} f_0^* f_1^* \ldots f_{i-1}^* P_i(t). \tag{71}$$

Для однородных систем (основной и резервные элементы равно надежны) и постоянной интенсивности отказов, когда $\lambda_0 = \lambda_1 = \ldots = \lambda_m = \lambda$

$$P_c(t) = e^{-\lambda t} \sum_{i=0}^{m} \frac{(\lambda t)^i}{i!}, \tag{72}$$

$$T_c = \int_0^\infty P_c(t)dt = (m+1)\frac{1}{\lambda} = (m+1)T_0. \tag{73}$$

Система со скользящим резервированием и ненагруженным резервом

Постановка задачи*:*

Дано:

Система со скользящим резервированием и ненагруженным резервом;

$P(t)$ – вероятность безотказной работы элемента;

$f(t)$ – плотность распределения времени до отказа элемента.

Определить:

$P_c(t)$ – вероятность безотказной работы системы.

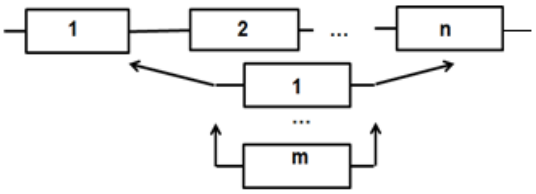


Рис. 1.12. Надёжностная схема системы со скользящим резервированием и ненагруженным резервом: n – количество основных элементов, m – количество резервные элементы

Сначала работают n основных элементов, резервные элементы не работают. При отказе любого элемента из числа основных элементов он заменяется на резервный, который становится основным. При очередном отказе основного элемента он также заменяется на один из оставшихся резервных и т.д. Отказ системы наступает при отказе *(m + 1)*-го элемента *(m < n).*

Рассмотрим случай, когда *m = 2*

$$P_c(t) = P(t)^n + nP(t)^{n-1}\int_0^t f(x)P(t-x)dx + \\ + C_n^2 P(t)^{n-2}\int_0^t f(x)\int_0^{t-x} f(y)P(t-x-y)dy\,dx. \quad (74)$$

Для общего случая

$$P_c(t) = \sum_{i=0}^{m} C_n^i P(t)^{(n-i)} f^{(i)*}P(t), \quad (75)$$

где $f^{(i)*}P(t) = \int_0^t f(x_1)\int_0^{t-x_1} f(x_2)\ldots\int_0^{t-x_1-\cdots-x_i} f(x_i)P(t-x_1-\cdots-x_i)\,dx_i \ldots dx_1.$

Учёт надёжности переключателей

Учет надежности переключателей при расчете показателей надежности резервированных систем рассмотрим на примере мажоритарной системы с постоянно включенным резервом.

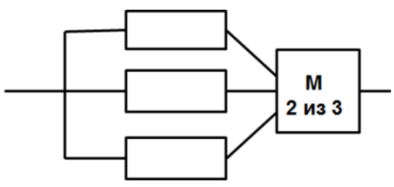


Рис. 1.13. Надёжностная схема мажоритарной системы с постоянно включенным резервом

Пусть

P(t) – вероятность безотказной работы элемента за время *t*,

Q(t) = 1 – P(t) – вероятность отказа элемента за время *t*,

$P_м(t)$ – вероятность безотказной работы мажоритарного элемента за время *t*.

Тогда с учетом того, что в данной системе имеет место резервирование с дробной кратностью

$$P_c(t) = P_м(t) \sum_{i=0}^{1} C_3^i Q(t)^i P(t)^{3-i} = P_м(t)(3P(t)^2 - 2P(t)^3). \quad (76)$$

1.4.3. Расчет показателей надежности восстанавливаемых систем

1.4.3.1. Метод расчёта показателей надёжности восстанавливаемых систем, *основанный на теории марковских процессов*

Инженерные методики расчета показателей надежности восстанавливаемых систем существуют в основном для простейшего потока отказов и экспоненциального закона распределения времени восстановления отказавших элементов, составляющих систему. В случае неэкспоненциальных законов используются численные методы расчета и компьютерные технологии.

Расчёт показателей надёжности восстанавливаемых систем рассмотрим на примере метода, основанного на теории марковских процессов.

Случайный процесс *X(t)* называется марковским или процессом без последействия, если для любых двух моментов времени t_0 и t_1 $(t_0 < t_1)$, распределение вероятностей $X(t_1)$ при условии, что заданы все значения процесса *X(t)* для $t \le t_0$, зависит только от значения процесса $X(t_0)$ в момент времени t_0.

Марковский процесс с непрерывным временем и дискретными состояниями (процесс Пуассона) называется однородным, если для любых значений *i* и *k*, где *i* и *k* – дискретные состояния процесса, и произвольного $\tau \ge 0$ вероятность события $X(t+\tau) = k$ при условии, что $X(t) = i$, не зависит от *t*, т.е. справедливы следующие соотношения:

$$p_{i,k}(\tau) \ge 0;\ \sum_k p_{i,k}(\tau) = 1;\ \ p_{i,k}(\tau_1 + \tau_1) = \sum_j p_{i,j}(\tau_1)\ p_{j,k}(\tau_2), \quad (77)$$

где $p_{i,k}(\tau) = P(X(t+\tau)=k|X(t)=i)$ – условная вероятность перехода из состояния *i* в состояние *k* за время τ.

Однородный марковский процесс определяется постоянными интенсивностями перехода

$$\lambda_{i,j} = lim_{\Delta t \to 0} \frac{P(X(t+\Delta t)=j|X(t)=i)}{\Delta t} \quad (78)$$

и начальным вектором вероятностей состояний $p_i(t)$:

$$p_i(0) = P(X(0)) = i,\ \ i = 0,1,\ldots,m. \quad (79)$$

Вероятности $p_i(t)$ удовлетворяют системе обыкновенных дифференциальных уравнений Колмогорова:

$$p_i'(t) = -\sum_j \lambda_{i,j} p_i(t) + \sum_j \lambda_{i,j} p_j(t),\ \ i = 0,1,\ldots,m. \quad (80)$$

Система уравнений составляется из графа состояний по следующему правилу:

1. Для каждого состояния S_i составляется отдельное уравнение;
2. В левой части уравнения записывается производная от вероятности этого состояния $p_i(t)$;

3. В правой части уравнения записываются со знаком минус произведения $\lambda_{i,j}p_i(t)$, соответствующие выходам из этого состояния во все другие согласно графу состояний, и со знаком плюс – произведения $\lambda_{i,j}p_j(t)$, соответствующие входам в это состояние из всех других опять же согласно графу состояний.

Для условия длительной эксплуатации системы, когда $t \to \infty$, $p_i(t) \to p_i$, $p_i'(t) \to 0$, система дифференциальных уравнений принимает вид системы алгебраических уравнений:

$$0 = -\sum_j \lambda_{i,j}p_i + \sum_j \lambda_{i,j}p_j, \quad i = 0,1,...,m, \tag{81}$$

которая должна решаться вместе с условием: $\sum_{i=0}^{m} p_i = 1$.

1.4.3.2. Расчет надежности нерезервированной системы

Постановка задачи:

Дано:

Нерезервированная восстанавливаемая система;

λ_i – интенсивность отказа i-го элемента;

μ_i – интенсивность восстановления i-го элемента.

Определить:

K_Γ – коэффициент готовности системы,

T_0 – среднее время между отказами системы,

T_B – среднее время восстановления системы.

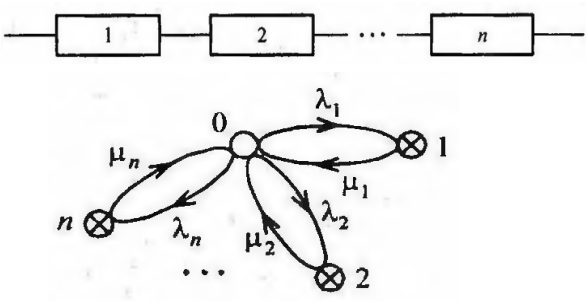


Рис. 1.14. Надёжностная схема и граф состояний нерезервированной восстанавливаемой системы: состояние 0 – исправное состояние системы, состояния 1, 2, ... n – состояния восстановления отказавших элементов.

Система дифференциальных уравнений, описывающая граф состояний нерезервированной системы с основным соединением элементов:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = -\lambda_c p_0(t) + \sum_{i=1}^{n} \mu_i p_i(t) \\ \dfrac{dp_i(t)}{dt} = \lambda_i p_0(t) - \mu_i p_i(t) \quad i = 1,2,...,n. \end{cases} \tag{82}$$

где $\lambda_c = \sum_{i=1}^{n} \lambda_i$; $p_0(0) = 1$; $p_1(0) = p_2(0) = ... = p_n(0) = 0$.

Для условия длительной эксплуатации (стационарный режим), когда $t \to \infty$, $p_i(t) \to p_i$, $p_i' \to 0$, система дифференциальных уравнений примет вид системы алгебраических уравнений:

$$\begin{cases} -\lambda_c p_0 + \sum_{i=1}^{n} \mu_i p_i = 0 \\ \lambda_i p_0 - \mu_i p_i = 0, \quad i = 1,2,...,n. \end{cases} \tag{83}$$

Решая систему алгебраических уравнений при условии, что $\sum_{i=0}^{n} p_i = 1$, получим выражение для p_0 и $K_Г$:

$$K_Г = p_0 = \frac{1}{1+\sum_{i=1}^{n} p_i}, \quad (84)$$

где $p_i = \frac{\lambda_i}{\mu_i}$.

Среднее время восстановления $T_В$ определяется из выражений для $T_О$ и $K_Г$. Так как $K_Г = \frac{T_О}{T_О + T_В}$ и $K_П = 1 - K_Г$, то $T_В = T_О \frac{K_П}{K_Г}$. Поскольку $K_Г = \frac{1}{1+\sum_{i=1}^{n} p_i}$, то

$$T_В = T_О \sum_{i=1}^{n} p_i. \quad (85)$$

Так как

$$T_О = \frac{1}{\sum_{i=1}^{n} \lambda_i} = \frac{1}{\lambda_с}, \quad (86)$$

то

$$T_В = \frac{1}{\lambda_с} \sum_{i=1}^{n} p_i. \quad (87)$$

1.4.3.3. Расчет надежности резервированной системы

Система с общим резервированием и постоянно включенным резервом

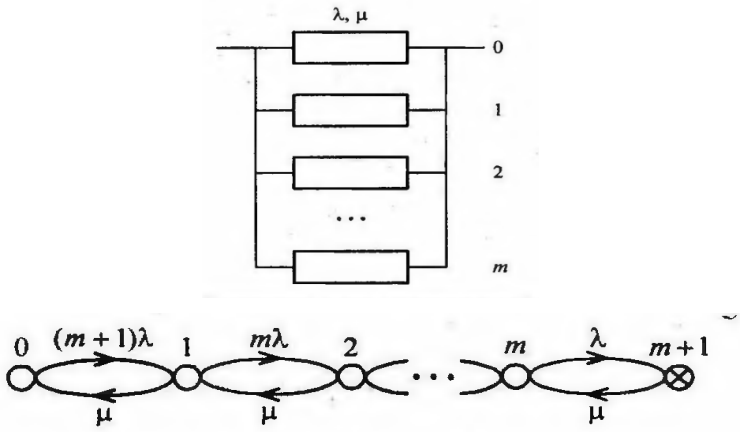


Рис. 1.15. Надежностная схема и граф состояний системы с общим резервированием и постоянно включенным резервом: состояние 0,1,…,m – работоспособные состояния системы, m + 1 – неработоспособное состояние системы

Система алгебраических уравнений, соответствующая графу состояний, для стационарного режима будет иметь следующий вид:

$$\begin{cases} \mu p_1 - (m+1)\lambda p_0 = 0 \\ \sum_{i=1}^{m} (\mu p_{i+1} + (m+2-i)\lambda p_{i-1} - ((m+1-i)\lambda + \mu) p_i) = 0 \\ \lambda p_m - \mu p_{m+1} = 0. \end{cases} \quad (88)$$

Решая систему алгебраических уравнений при условии, что $\sum_{i=0}^{m+1} p_i = 1$, получим выражение для $K_П$ и $K_Г$:

Так как $p_{m+1} = K_П$ *и* $K_Г = 1 - K_П$, то

$$K_{\text{П}} = \frac{1}{1+\frac{\gamma^1}{1!}+\frac{\gamma^2}{2!}+\cdots+\frac{\gamma^{m+1}}{(m+1)!}};\ K_{\text{Г}} = \frac{\sum_{i=1}^{m+1}\gamma^i/i!}{\sum_{i=0}^{m+1}\gamma^i/i!}, \tag{89}$$

где $\gamma = \frac{\mu}{\lambda}$.

Поскольку все элементы системы равно надежны, то в соответствии с графом состояний среднее время восстановления системы будет равно

$$T_{\text{В}} = \frac{1}{\mu}. \tag{90}$$

В силу соотношения $T_0 = T_{\text{В}} \frac{K_{\text{Г}}}{K_{\text{П}}}$ и формул для $K_{\text{П}}$, $K_{\text{Г}}$, и $T_{\text{В}}$ получим

$$T_0 = \frac{1}{\mu}\sum_{i=1}^{m+1}\gamma^i/i!;\ T_0 = T\sum_{i=1}^{m+1}\gamma^{i-1}/i!; \tag{91}$$

где $T = \frac{1}{\lambda}$ – наработка на отказ нерезервированной системы.

Последнее выражение устанавливает зависимость наработки на отказ резервированной системы от кратности резервирования.

Пример 1

Система состоит из двух основных элементов. Средняя интенсивность отказа каждого элемента λ_1 и λ_2, а интенсивность восстановления μ_1 и μ_2. Каждый основной элемент зарезервирован постоянно включенным аналогичным элементом.

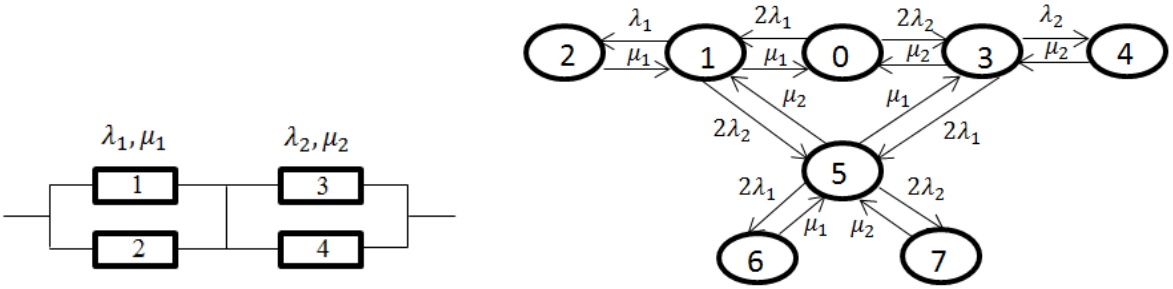


Рис. 1.16. Надёжностная схема и граф состояний системы с раздельным резервированием и постоянно включенным резервом: состояние 0,1,3 – работоспособные состояния системы, состояния 2 и 4 – неработоспособные состояния системы.

$$\begin{cases}
\mu_1 P_1 + \mu_2 P_3 - 2(\lambda_1 + \lambda_2)P_0 = 0 \\
2\lambda_1 P_0 + \mu_1 P_2 + \mu_2 P_5 - (\lambda_1 + 2\lambda_2 + \mu_1)P_1 = 0 \\
\lambda_1 P_1 - \mu_1 P_2 = 0 \\
2\lambda_2 P_0 + \mu_2 P_4 + \mu_1 P_5 - (\lambda_2 + 2\lambda_1 + \mu_2)P_3 = 0 \\
\lambda_2 P_3 - \mu_2 P_4 = 0 \\
2\lambda_2 P_1 + 2\lambda_1 P_3 + \mu_1 P_6 + \mu_2 P_7 - (2\lambda_1 + 2\lambda_2 + \mu_1 + \mu_2) = 0 \\
2\lambda_1 P_5 - \mu_1 P_6 = 0 \\
2\lambda_2 P_5 - \mu_2 P_7 = 0 \\
P_0 + P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_7 = 1.
\end{cases} \tag{92}$$

$$K_{\Г} = P_0 + P_1 + P_3 + P_5 ; \quad K_{\п} = 1 - K_{\Г};$$

При $\mu_1 = \mu_2 = \mu$

$$T_B = \frac{1}{\mu} . \qquad \Theta = \frac{K_{\Г}}{K_{\п}} T_B . \tag{93}$$

Пояснения к графу состояний.

Состояние S_0(работоспособное) – все элементы исправны (событие – $a_1 a_2 a_3 a_4$).

Состояние S_1(работоспособное) – один элемент неисправен (события – $\bar{a}_1 a_2 a_3 a_4$ и $a_1 \bar{a}_2 a_3 a_4$).

Состояние S_2(неработоспособное) – два элемента неисправны (событие – $\bar{a}_1 \bar{a}_2 a_3 a_4$).

Состояние S_3(работоспособное) – один элемент неисправен (события – $a_1 a_2 \bar{a}_3 a_4$ и $a_1 a_2 a_3 \bar{a}_4$).

Состояние S_4(неработоспособное) – два элемента неисправны (событие – $a_1 a_2 \bar{a}_3 \bar{a}$).

Состояние S_5(работоспособное) – два элемента неисправны (события – $\bar{a}_1 a_2 \bar{a}_3 a_4$, $\bar{a}_1 a_2 a_3 \bar{a}_4$, $a_1 \bar{a}_2 \bar{a}_3 a_4$ и $a_1 \bar{a}_2 a_3 \bar{a}_4$).

Состояние S_6(неработоспособное) – три элемента неисправны (события – $\bar{a}_1 \bar{a}_2 \bar{a}_3 a_4$ и $\bar{a}_1 \bar{a}_2 a_3 \bar{a}_4$).

Состояние S_7(неработоспособное) – три элемента неисправны (события – $a_1 \bar{a}_2 \bar{a}_3 \bar{a}_4$ и $\bar{a}_1 a_2 \bar{a}_3 \bar{a}_4$).

Всего событий – $2^4 = 16$. Последнее событие $\bar{a}_1 \bar{a}_2 \bar{a}_3 \bar{a}_4$ не указано в графе состояний, так как оно следует из неработоспособных состояний S_6 и S_7. Предполагается, что в неработоспособном состоянии исправные элементы находятся в выключенном состоянии и потому отказать не могут.

Пример 2

Аппаратура зарезервирована по мажоритарному принципу 2 из 3-х.

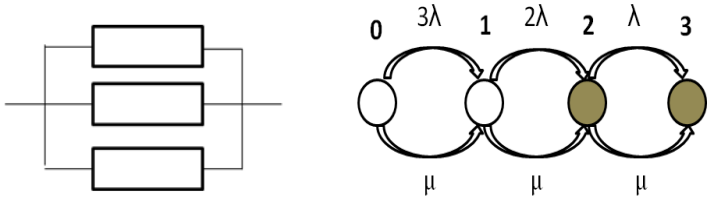


Рис. 1.17. Надёжностная схема и граф состояний мажоритарной системы с постоянно включенным резервом: состояние 0,1 – работоспособные состояния системы, состояния 2 и 3 – неработоспособные состояния системы.

Пояснения к графу состояний.

Состояние S_0(работоспособное) – все элементы исправны (событие – $a_1a_2a_3$).

Состояние S_1(работоспособное) – один элемент неисправен (события – $\bar{a}_1a_2a_3$, $a_1\bar{a}_2a_3$, $a_1a_2\bar{a}_3$).

Состояние S_2(неработоспособное) – два элемента неисправны (события – $\bar{a}_1\bar{a}_2a_3$, $\bar{a}_1a_2\bar{a}_3$, $a_1\bar{a}_2\bar{a}_3$).

Состояние S_3(неработоспособное) – три элемента неисправны (событие – $\bar{a}_1\bar{a}_2\bar{a}_3$).

В данном случае в графе состояний рассмотрены все $2^3 = 8$ событий.

В системе алгебраических уравнений уравнение для состояния S_3 заменено на условие нормировки.

$$\begin{cases} \mu P_1 - 3\lambda P_0 = 0 \\ 3\lambda P_0 + \mu P_2 - (2\lambda + \mu)P_1 = 0 \\ 2\lambda P_1 + \mu P_3 - (\lambda + \mu)P_2 = 0 \\ P_0 + P_1 + P_2 + P_3 = 1, \end{cases} \quad (94)$$

$$K_\Gamma = P_0 + P_1, \; K_\text{п} = 1 - K_\Gamma, \quad \theta = \frac{K_\text{п}}{K_\Gamma} T_B, \quad T_B = \frac{1}{\mu}. \quad (95)$$

1.5. Испытания и контроль надежности АС

1.5.1. Испытания на надежность

Основные понятия и классификация испытаний

Испытания – это экспериментальное определение количественных и (или) качественных характеристик свойств объекта испытаний как результат воздействия на него.

Процессы, свойственные испытаниям:

- воздействие на объекта испытаний;
- измерения;
- выработка оценок характеристик свойств объекта.

Испытания проводятся при широком варьировании условий от минимальных до максимальных значений.

Контроль – это проверка соответствия объекта установленным техническим требованиям.

Контроль проводится при нормальных условиях.

Качество испытаний включает:

- точность, которая характеризует близость полученных при испытаниях характеристик к их истинным значениям;
- воспроизводимость, которая характеризует близость результатов повторных испытаний;
- достоверность, которая характеризует степень доверия к полученным результатам испытаний.

Для оценивания точности используются:

- дисперсия *D*;
- среднее квадратичное отклонение σ.

Для оценивания воспроизводимости используют дисперсию воспроизводимости $D_\text{В}$.

Для оценивания достоверности используют доверительную вероятность β или *доверительный интервал*.

Средства испытаний – любые технические средства, применяемые при испытаниях.

Дисперсией случайной величины называется математическое ожидание квадрата отклонения случайной величины от ее математического ожидания

$$D(X) = M(X - M(X))^2; \;\; D(X) = \sum_{i=1}^{n} (x_i - M(X))^2 p_i. \qquad (96)$$

Дисперсия характеризует рассеяние (разбросанность) значений случайной величины около ее математического ожидания.

Среднеквадратическое отклонение определяется как квадратный корень из дисперсии случайной величины.

Испытания классифицируют по различным критериям:

- по уровню проведения;
- по назначению;
- по этапам разработки изделий;
- по месту и условиям проведения;
- по продолжительности;
- по виду воздействия;
- по определяемым характеристикам объекта;
- по результатам воздействия.

В зависимости от назначения различают:

- исследовательские испытания;
- контрольные испытания;
- определительные испытания;
- сравнительные испытания;
- специальные испытания.

Исследовательские испытания проводятся для изучения свойств объекта.

Контрольные испытания проводятся для контроля качества объекта.

Определительные испытания проводятся для определения значений показателей качества объекта с заданной точностью и достоверностью.

Специальные испытания проводятся с целью проверки устойчивости параметров изделия в специальных условиях эксплуатации.

К специальным испытаниям относятся также испытания стабильности параметров объекта, *надежности и долговечности*.

Сравнительные испытания – это испытания аналогичных по характеристикам и одинаковых образцов техники. Цель этих испытаний – сравнение свойств двух и более образцов техники.

Цель испытаний – выявить ненадежные детали и элементы объекта и определить количественные показатели надежности.

Объем испытаний $V_{\text{исп}}$ определяется по формуле:

$$V_{\text{исп}} = N t_{\text{исп}}, \qquad (97)$$

где N – число испытываемых объектов, $t_{\text{исп}}$ – время испытаний.

Методы испытания надежности

Испытания в зависимости от их организации делятся на следующие основные группы:

NUT – испытания, при которых в течение времени *T* испытываются объектов без их восстановления (*U* означает, что в процессе испытаний отказавшие объекты не восстанавливаются);

NUr – испытания, при которых испытывается *N* объектов без восстановления отказавших до появления r отказов;

NUN – испытания, при которых испытывается *N* объектов без восстановления отказавших в процессе испытаний до отказа всех *N* объектов, поставленных на испытание (дают наиболее полную информацию);

NRT, NRr – испытания, которые проводятся с восстановлением отказавших объектов.

Испытания по плану *NUN* ведутся до отказа всех *N* поставленных на испытания объектов, при этом фиксируется время отказа каждого объекта.

Средняя наработка до отказа определяется как среднее арифметическое

$$T_{\text{ср}} = \frac{\sum_{i=1}^{N} t_i}{N}. \tag{98}$$

Среднеквадратическое отклонение относительно его среднего значения определяется по следующей зависимости

$$\sigma(T_{\text{ср}}) = \sqrt{\frac{\sum_{i=1}^{N}(t_i - T_{\text{ср}})^2}{N}}. \tag{99}$$

Применение восстановления позволяет увеличить информативность испытаний без увеличения числа испытываемых объектов. Для этого используется план *NRT* или *NRr*.

NRT – план испытаний, согласно которому одновременно начинают испытания *N* объектов, отказавшие объекты заменяют новыми, испытания прекращают по истечении времени испытаний или наработки *T* для каждой из *N* позиций (каждый из *N* объектов занимает определенную позицию на испытательном стенде, в отношении которой в дальнейшем отсчитывается продолжительность испытаний *T* независимо от замены объектов).

NRr – план испытаний, согласно которому одновременно начинают испытания *N* объектов, отказавшие объекты заменяют новыми, испытания прекращают, когда суммарное число отказавших объектов по всем позициям достигает *r*.

Средняя наработка до отказа при испытаниях по плану *NRr*

$$T_{\text{ср}} = \frac{t_{p\Sigma}}{r}, \tag{100}$$

где $t_{p\Sigma}$ – суммарная наработка испытываемых объектов.

Если не учитывать время на восстановление, то

$$T_{\text{ср}} = \frac{t_r \cdot N}{r}. \tag{101}$$

где t_r – время фиксации последнего отказа.

Число испытываемых объектов можно определить, используя выражение для определения среднеквадратического значения средней наработки.

Рассмотренные методы испытаний эффективны, но требуют все-таки большого времени испытаний, особенно для испытания объектов с высокой надежностью. С целью уменьшения времени испытаний *применяют ускоренные испытания*, которые проводятся с помощью форсированных режимов.

При ускоренных испытаниях важно, чтобы:

— в условиях форсированных режимов не искажался характер естественного старения и других процессов, протекающих в материалах при нормальной эксплуатации;

— распределение отказов во времени соответствовало распределению отказов при нормальных испытаниях.

Если число зафиксированных отказов при ускоренных испытаниях $k_{\text{уск}}$ равно числу отказов при нормальных испытаниях k_0, то

$$\lambda_{\text{уск}} \approx K_{\text{у}}\,\lambda_0,\ V_{\text{исп.уск}} = V_{\text{исп.0}},\ t_{\text{уск}} = \frac{t_0}{K_{\text{у}}}. \tag{102}$$

где $\lambda_{уск}$, $V_{исп.уск}$, $t_{уск}$ – интенсивность отказов, объем и время испытаний при ускоренных испытаниях;

λ_0, $V_{исп.0}$, t_0 – интенсивность отказов, объем и время испытаний при нормальных испытаниях;

$K_у$ – коэффициент ускорения.

Обработка опытных данных о результатах испытаний

На практике часто требуется иметь интервал оценок, который с достаточно высокой вероятностью «накрывает» возможное значение показателя надежности.

Например, для вероятности безотказной работы достоверным интервалом возможных значений является [0,1], а для средней наработки до отказа соответственно [0,∞). В других случаях указания границ интервалов может быть связано с риском допустить ошибку.

Вероятность α_0 этой ошибки называется уровнем значимости, т.е. α_0 – вероятность того, что истинное значение показателя надежности не попадет в найденный интервал:

$$\alpha_0 = \alpha_1 + \alpha_2, \tag{103}$$

где α_1 – вероятность того, что истинное значение показателя надежности окажется слева от интервала,

α_2 – вероятность того, что истинное значение показателя надежности окажется справа от интервала.

В качестве меры достоверной оценки используется *доверительная вероятность* β:

$$\beta = P(\theta_н \le \theta_0 \le \theta_в); \ \beta = 1 - \alpha_0, \tag{104}$$

где $\theta_н$, $\theta_в$ – нижняя и верхняя границы доверительного интервала,

θ_0 – истинное значение показателя надежности.

Из определения доверительной вероятности следует:

$$\beta = \int_{\theta_н}^{\theta_в} f(\theta) d\theta = 1 - \alpha_1 - \alpha_2, \tag{105}$$

где $f(\theta)$ – плотность распределения оценки θ.

$\alpha_1 = \int_{-\infty}^{\theta_н} f(\theta) d\theta = F(\theta_н)$,

$\alpha_2 = \int_{\theta_в}^{+\infty} f(\theta) d\theta = 1 - \int_{-\infty}^{\theta_в} f(\theta) d\theta = 1 - F(\theta_в)$,

$F(\theta)$ – функция распределения оценки θ показателя надежности.

Отсюда:

$\theta_н$ – квантиль F(θ) по уровню α_1,

$\theta_в$ – квантиль F(θ) по уровню $1 - \alpha_2$.

Квантиль — значение, которое заданная случайная величина не превышает с фиксированной вероятностью.

Если задать $\alpha_1 = \alpha_2 = \alpha$ и β, то можно найти $\theta_н$ и $\theta_в$, выход за которые показателя надежности θ равновероятен.

Знание плотности распределения $f(\theta)$ оценки показателя надежности θ является необходимым условиям нахождения границ доверительного интервала. Вид $f(\theta)$ определяется видом распределения исследуемой случайной величины и функциональными преобразованиями, которые производятся над исходной статистикой при получении оценок.

Пример:

Пусть оценка для математического ожидания случайной величины $\hat{T}$ задается выражением:

$$\hat{T} = \frac{1}{N} \sum_{i=1}^{N} t_i, \tag{106}$$

тогда распределение случайной величины $\hat{T}$ представляет собой распределение суммы N независимых случайных величин с плотностями $f(t_i)$.
Если $f(t_i) = \lambda e^{-\lambda t}$, то распределение оценки $\hat{T}$ соответствует гамма-распределению с N степенями свободы:

$$f(T) = \frac{(N\lambda)^N}{\Gamma(N)} (T)^{N-1} e^{-\lambda TN}, \quad (107)$$

где $\Gamma(N)$ – гамма-функция. Для целых чисел $\Gamma(N) = (N-1)!$.

Для $f(t_i) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-m)^2}{2\sigma^2}}$ – нормальный закон распределения случайной величины со средним значением m и дисперсией σ^2, оценка $\hat{T}$ имеет плотность распределения:

$$f(T) = \frac{\sqrt{N}}{\sigma\sqrt{2\pi}} e^{-\frac{N(T-m)^2}{2\sigma^2}}. \quad (108)$$

Доверительный интервал – это интервал со случайными концами, т.к. длина и положение интервала зависят от результатов испытаний.

Точность оценивания параметра оценки θ зависит от длины интервала, чем уже интервал, тем выше точность. При фиксированной точности (фиксированной длине доверительного интервала) доверительная вероятность будет возрастать по мере увеличения числа испытаний.

Если объем испытаний остается постоянным, то доверительную вероятность невозможно повысить, не уменьшая точность оценивания (не расширяя доверительный интервал), и наоборот, нельзя увеличить точность оценки, не уменьшая доверительную вероятность.

1.5.2. Метод статистических испытаний

Сущность метода статистических испытаний

Сущность метода статистических испытаний (метода Монте-Карло) заключается в построении вероятностной модели системы, реализации ее многократно случайным образом и математической обработке результатов испытаний.

Теоретической основой метода является закон больших чисел, согласно которому частота случайного события стремится к его вероятности, а среднее арифметическое случайной величины – к ее математическому ожиданию при увеличении числа испытаний.

Рассмотрим следующую задачу.

Пусть задана функция $y = f(x)$, причем $0 \le x \le 1$, $|f(x)| < 1$.

Требуется найти площадь S, ограниченную сверху данной функцией на заданном интервале.

Аналитически:

$$S = \int_0^1 f(x)dx. \quad (109)$$

Статистически:

Пусть на координатную плоскость бросили случайную точку (x_1, y_1). Если $y_1 \le f(x_1)$, то есть точка попала на искомую площадь S, то событие считается успешным.

Провели N бросков, из них зафиксировали m успешных, тогда:

$$S \approx \frac{m}{N}, \quad (110)$$

при этом $lim_{N\to\infty} \Delta S(N) \to 0$.

Основные задачи моделирования надежности

Задача 1 – моделирование случайных событий по заданным вероятностям их появлений.

Задача 2 – определение значений случайной величины по заданному закону распределения.

Решение Задачи 1

Пусть есть полная группа событий A_1, A_2, ..., A_n с вероятностями появления P_1, P_2, ..., P_n ($\sum_{i=1}^{n} P_i = 1$) Определить, какое из указанных событий произошло в каждом опыте.

Интервал [0,1] разбивается на *n* непересекающихся отрезков так, чтобы длина i-го отрезка численно была равна P_i. Попадание случайного числа на *i*-й отрезок фиксируется как событие A_i.

В качестве механизма случайного выбора используются программные датчики случайных чисел.

Пример

Пусть:

- отказы ЭВМ обнаруживаются системой контроля с вероятностью 0,9;
- событие 1 – отказ обнаружен, вероятность события 1 равна 0,9;
- событие 2 – отказ не обнаружен, вероятность события 2 равна 0,1.

Разбиваем интервал [0,1] на два отрезка длиной 0,9 и 0,1 соответственно.

Если в i-м опыте случайное число датчика (датчик генерирует случайные числа в интервале [0,1]) меньше либо равно 0,9, т.е. попало в первый отрезок, то имеет место событие 1, если число больше 0,9, то имеет место событие 2.

Решение Задачи 2

Теорема: Если случайная величина *X* имеет плотность распределения *f(x),* то случайная величина *Y = F(x),* где $F(x) = \int_{-\infty}^{x} f(x)dx$, распределена равномерно в интервале [0,1].

Т.е. совокупность чисел $\{y_i = F(x_i)\}$ можно рассматривать как значения случайной величины *Y*, равномерно распределенной на интервале [0,1].

Справедливо и обратное утверждение. Если $\{y_i\}$ – совокупность значений равномерно распределенной на интервале [0,1] случайной величины *Y*, то обратным преобразованием $X = F(y)^{-1}$ для каждого y_i можно найти x_i, являющееся значением случайной величины *X*, распределенной по закону *f(x).*

$$F(x) = \begin{cases} 0, & x < \alpha \\ \frac{x-\alpha}{\beta-\alpha}, & \alpha \le x \le \beta \\ 1, & x > \beta \end{cases}$$

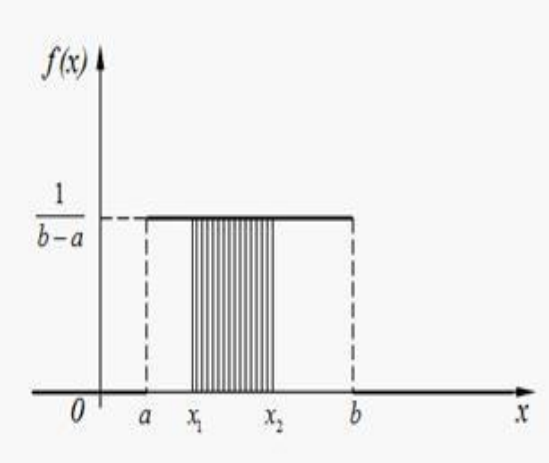


Рис. 1.18. График плотности и функция распределения вероятности равномерно распределенной случайной величины $\hat{X}$

С равномерным законом распределения имеют дело, когда по условиям испытания или опыта изучают случайную величину *X*, которая принимает значения в конечном промежутке и все значения из этого промежутка равно возможны, т.е. ни одно из значений не имеет преимуществ перед другими.

Аналитически задача сводится к решению следующего уравнения:

$$y_i = \int_{-\infty}^{x_i} f(x)dx. \quad (111)$$

Например, для $F(x) = 1 - e^{-\lambda x}$, имеем:

$$y_i = 1 - e^{-\lambda x_i};\ x_i = -\frac{1}{\lambda} ln(1 - y_i); \quad (112)$$

а т.к. для равномерного распределения верно $X = 1 - X$, то

$$x_i = -\frac{1}{\lambda} ln\, y_i. \quad (113)$$

Для других законов не всегда уравнение легко разрешимо.

Определение времени безотказной работы системы

Основной величиной, определяемой в каждом из N опытов при статистическом испытании на надежность, является время безотказной работы системы $T\ (t_1, t_2, \ldots, t_N)$. Все остальные показатели надежности определяются из $(t_1, t_2, \ldots, t_N)$ путем статистической обработки.

Рассмотрим основное соединение элементов без резервирования и восстановления отказавших элементов.

Рис. 1.19. Нерезервированная система

Если известны плотности распределения времени безотказной работы всех элементов: $f_1(t), \ldots, f_n(t)$, то времена безотказной работы элементов $t_1, t_2, \ldots, t_n$ будут определяться выражением:

$$y_i = \int_0^{x_i} f_i(z)dz \ \rightarrow \ x_i = t_i, \quad (114)$$

где y_i – i-е значение случайной величины Y, равномерно распределенной на интервале [0,1].

Например, для экспоненциального закона

$$x_i = t_i = -\frac{1}{\lambda} ln\, y_i. \quad (115)$$

Время безотказной работы системы T определяется как:

$$T = min\ (t_1, t_2, \ldots, t_n). \quad (116)$$

Рассмотрим систему с общим резервированием.

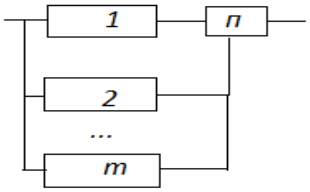


Рис. 1.20. Система с общим резервированием

Пусть: $f_i(t)$ – плотность распределения времени безотказной работы i-го элемента;

$g_i(t)$ – плотность распределения времени восстановления i-го элемента;

$f_п(t)$ – плотность распределения времени безотказной работы переключателя;

R – вероятность обнаружения отказа элемента переключателем.

Рассмотрим резервирование без восстановления отказавших элементов с ненагруженным резервом.

Отказ системы наступает в следующих случаях:

- при отказе всех m элементов,
- резерв не израсходован, но отказал переключатель,
- резерв не израсходован, переключатель не отказал, но отказ неисправного элемента не обнаружен.

Для данных условий последовательность нахождения времени безотказной работы будет следующая:

1. По y_1 и $f_п(t)$ определяется время безотказной работы переключателя $t_п$;
2. По y_2 и $f_1(t)$ определяется время безотказной работы 1-го элемента t_1. Если к моменту отказа 1-го элемента переключатель не оказал и отказ элемента обнаружен ($t_1 \le t_п$ и $y_3 \le R$), то будет подключен резервный элемент. Если не выполняется хотя бы одно условие из ($t_1 \le t_п$ и $y_3 \le R$), то резервный элемент не будет подключен и наступит отказ системы, тогда $T = t_1$.
3. При ($t_1 \le t_п$ и $y_3 \le R$) по y_4 и $f_2(t)$ определяется время безотказной работы 2-го элемента t_2. Проверяются неравенства ($t_1 + t_2 \le t_п$ и $y_5 \le R$). Если хотя бы одно из них не выполняется, то $T = t_1 + t_2$.
4. При ($t_1 + t_2 \le t_п$ и $y_5 \le R$) по y_6 и $f_3(t)$ определяется время безотказной работы 3-го элемента t_3 и проверяются неравенства ($t_1 + t_2 + t_3 \le t_п$ и $y_7 \le R$).

И т.д. Процесс продолжается до тех пор, пока либо не выполнится одно из неравенств, либо будут израсходованы все элементы.

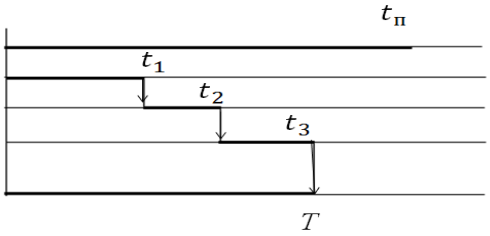


Рис. 1.21. Иллюстрация процесса нахождения времени безотказной работы системы

Рассмотрим ту же систему, но с нагруженным резервом.

В этом случае последовательность нахождения времени безотказной работы будет следующей:

1. По y_1 и $f_п(t)$ определяется время безотказной работы переключателя $t_п$;
2. По y_2 и $f_1(t)$ определяется время безотказной работы 1-го элемента t_1. Если не выполняется хотя бы одно условие из ($t_1 \le t_п$ и $y_3 \le R$), то $T = t_1$.
3. При ($t_1 \le t_п$ и $y_3 \le R$) по y_4 и $f_2(t)$ определяется время безотказной работы 2-го элемента t_2 и проверяется, не отказал ли он раньше первого. Для этого t_2 сравнивается с t_1.
4. При $t_2 < t_1$ по y_5 и $f_3(t)$ определяется время безотказной работы 3-го элемента t_3 и проверяется, не отказал ли он раньше первого. Если и он отказал раньше первого, то анализируется следующий элемент и т.д. до тех пор, пока не будет найден исправный элемент.

Пусть этот элемент имеет номер j. Тогда проверяются неравенства ($t_j \le t_п$ и $y_{j+3} \le R$). Если хотя бы одно из них не выполняется, то $T = t_j$. Если выполняются оба неравенства, то переходят к анализу ($j+1$)-го элемента и т.д.

Процесс продолжается до тех пор, пока либо не выполнится одно из неравенств, либо будут израсходованы все элементы.

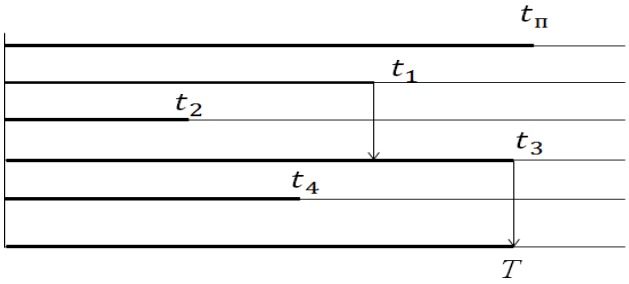


Рис. 1.21. Иллюстрация процесса нахождения времени безотказной работы системы при R = 1

Рассмотрим восстанавливаемую систему с ненагруженным резервом.

После отказа первого элемента в работу включается второй, а первый восстанавливается. По окончании восстановления он становится в резерв. После отказа второго элемента он восстанавливается, а в работу включается следующий исправный резервный элемент. Переключение происходят до тех пор, пока одновременно не окажутся в неисправном состоянии все элементы.

Последовательность нахождения времени безотказной работы системы будем при следующих допущениях:

- отказ элемента обнаруживается с вероятностью *R = 1;*
- восстановление отказавшего элемента осуществляется сразу после переключения;
- переключатель идеальный.

1. По y_1 и $f_1(t)$ определяется время безотказной работы 1-го элемента $t_{р1}^{(1)}$. Подсчитывается суммарная наработка системы $t_\Sigma = t_{р1}^{(1)}$.
2. По y_2 и $g_1(t)$ определяется время восстановления первого элемента $t_{в1}^{(1)}$. Запоминается момент окончания ремонта первого элемента $t_{в1} = t_\Sigma + t_{в1}^{(1)}$.
3. По y_3 и $f_2(t)$ определяется время безотказной работы 2-го элемента $t_{р2}^{(1)}$. Подсчитывается суммарная наработка системы $t_\Sigma = t_{р1}^{(1)} + t_{р2}^{(1)}$.
4. По y_4 и $g_2(t)$ определяется время восстановления второго элемента $t_{в2}^{(1)}$ и запоминается момент окончания его ремонта $t_{в2} = t_\Sigma + t_{в2}^{(1)}$ и т.д.
5. После отказа *m*-го элемента запоминается момент его восстановления $t_{вm} = t_\Sigma + t_{вm}^{(1)}$, где $t_\Sigma = \sum_{i=1}^{m} t_{рi}^{(1)}$, и среди резервных элементов ищется первый исправный элемент (первый среди восстановленных при последовательном просмотре сверху вниз). Пусть номер этого элемента *j*.
6. По y_{2m+1} и $f_j(t)$ определяется время безотказной работы *j*-го элемента $t_{рj}^{(2)}$. Подсчитывается суммарная наработка $t_\Sigma = \sum_{i=1}^{m} t_{рi}^{(1)} + t_{рj}^{(2)}$.
7. По y_{2m+2} и $g_j(t)$ определяется время восстановления *j*-го элемента при втором включении $t_{вj}^{(2)}$ и запоминается момент окончания его ремонта $t_{вj} = t_\Sigma + t_{вj}^{(2)}$.
8. После этого ищется следующий исправный элемент и процесс вычислений продолжается до тех пор, пока все элементы не окажутся в состоянии ремонта. В этом случае наступает отказ системы и $T = t_\Sigma$.

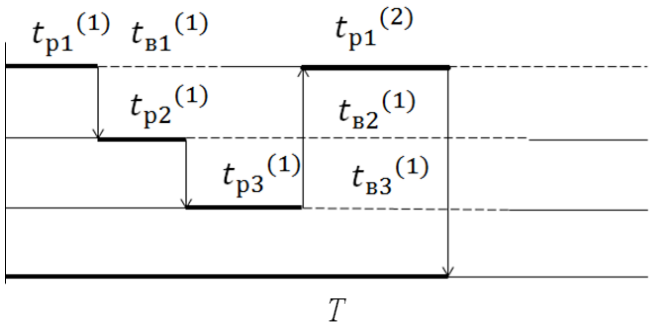


Рис. 1.22. Иллюстрация процесса нахождения времени безотказной работы системы

1.5.3. Контроль уровня надёжности АС

Ошибки первого и второго рода при контроле надёжности АС и их элементов

Цель контроля надежности – проверить гипотезу о том, что надежность не ниже установленного уровня.

Результатом контроля является решение: принять партию аппаратуры или забраковать как ненадежную.

Испытания на надежность серийного производства проводит предприятие-изготовитель не реже двух раз в год в течение первого года выпуска, в дальнейшем – не реже одного раза.

Поскольку решение принимается на основании статистической оценки значения параметра надежности, существует вероятность ошибки при принятии решения:

1. *Ошибка первого рода* – хорошая партия бракуется (вероятность ошибки первого рода α – риск поставщика);
2. *Ошибка второго рода* – плохая партия принимается (вероятность ошибки второго рода β – риск заказчика).

Существует три основных метода контроля надёжности:

- метод однократной выборки;
- метод двукратной выборки;
- метод последовательных испытаний.

Метод однократной выборки

При использовании этого метода в технических условиях записывают объем n выборки, время испытаний $t_{исп}$ и приемочное число c.

Если число d отказавших изделий в выборке за время испытания меньше или равно числу c, то партия принимается, в противном случае – бракуется. В этом и заключается сущность метода однократной выборки.

Объем выборки n для $c = 0$ определяется выражением:

$$n = N(1 - \beta^{\frac{1}{Nq}}), \qquad (117)$$

где N – число изделий в партии;

β – риск заказчика (потребителя);

$q \approx \frac{t_{исп}}{T_0}$;

T_0 – наработка на отказ, заданная в ТУ.

На практике для определения объема выборки и времени испытаний при заданных рисках поставщика и заказчика, а также $c \neq 0$ обычно пользуются специальными таблицами.

Недостатком метода является большой объем выборки, а его достоинством – простота планирования испытаний и небольшое, по сравнению с последовательным методом, время испытаний.

Метод двукратной выборки

1. Из общего числа изделий N выбирается n_1 изделий $(n_1 < N)$;
2. Эта выборка подвергается контролю на надежность и подсчитывается число дефектных изделий $d(n_1)$;
3. Если $d(n_1) \leq c_1$, то партия принимается, если $d(n_1) > c_2$ – партия бракуется;
4. Если $c_1 < d(n_1) \leq c_2$ (зона неопределенности), то берется вторая выборка n_2, такая, что $(n_1 + n_2 < N)$ и подвергается контролю на надежность;
5. Если $d(n_1 + n_2) \leq c_3$ – партия принимается, если $d(n_1 + n_2) > c_3$ – партия бракуется.

Данный метод применим только для больших партий изделий. Возможен вариант, когда $c_2 = c_3$.

Метод последовательного анализа

В основе построения планов испытаний лежит процедура проверки статистических гипотез при последовательном анализе.

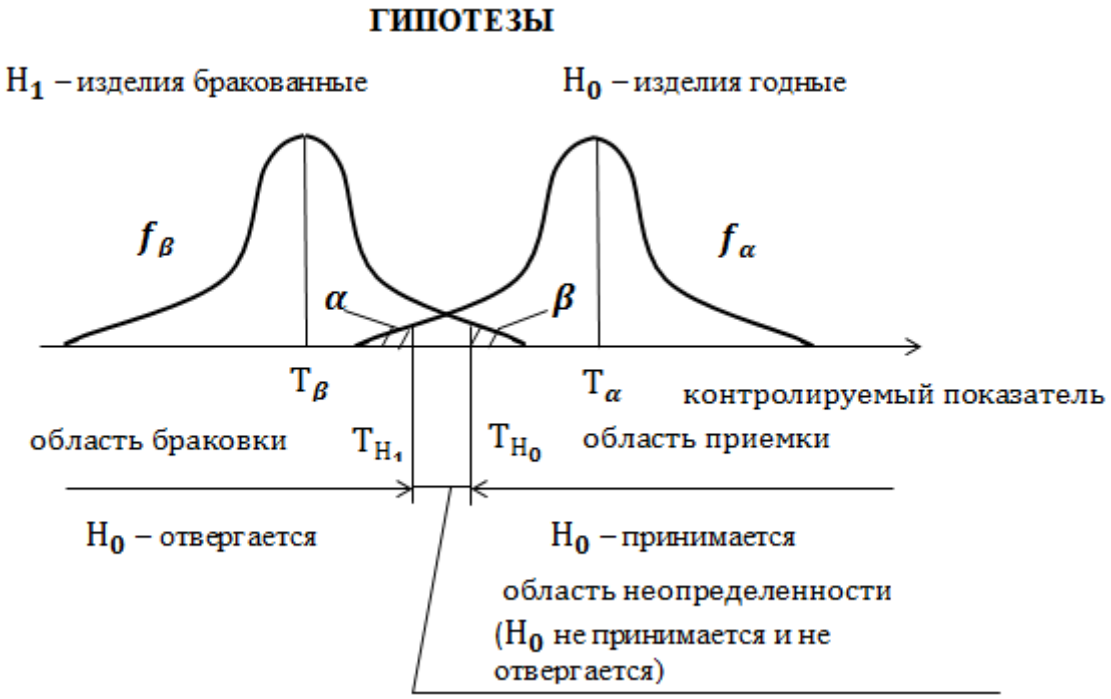


Рис. 1.23. Иллюстрация метода последовательных испытаний

Построение планов последовательного контроля и процедура принятия решений при последовательном анализе основаны на вычислении отношения правдоподобия (статистики Вальда):

$$L = \frac{P_1}{P_0}, \tag{118}$$

где P_1 – вероятность получения выборочных значений при условии, что верна гипотеза H_1 (несоответствие изделий заданным требованиям надежности);

P_0 – вероятность получения выборочных значений при условии, что верна гипотеза H_0 (соответствие изделий заданным требованиям надежности).

Порядок принятия решений при последовательном анализе:

1) если $L \leq \frac{\beta}{1-\alpha}$ – принять гипотезу H_0 (изделия признаются годными);

2) если $L \geq \frac{1-\beta}{\alpha}$ – принять гипотезу H_1 (изделия бракуются);

3) если $\frac{\beta}{1-\alpha} < L < \frac{1-\beta}{\alpha}$ – продолжить испытания.

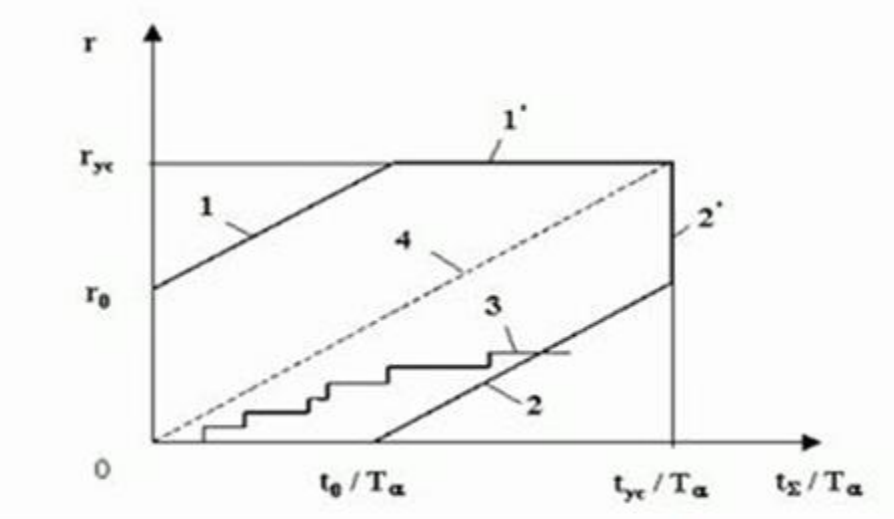
Для случая экспоненциального распределения наработки до отказа функции плотности распределения описываются формулами:

$$f_\alpha(t) = \frac{1}{T_\alpha} e^{-\frac{1}{T_\alpha}} \tag{119}$$

– для группы объектов, соответствующих установленным требованиям по надежности (верна гипотеза H_0);

$$f_\beta(t) = \frac{1}{T_\beta} e^{-\frac{1}{T_\beta}} \tag{120}$$

– для группы и объектов, не соответствующих установленным требованиям по надежности (верна гипотеза H_1).



План последовательного контроля типа Т:
1, 1* - линия несоответствия (браковки); 2, 2* - линия соответствия (приемки); 3 – график испытания; 4 – линия усечения

Рис. 1.24. План последовательного контроля

Вероятность появления r отказов в течение суммарной наработки t_Σ может быть подсчитана по формуле распределения Пуассона:

$$P_r(t_\Sigma) = \left(\frac{t_\Sigma}{T}\right)^r \frac{e^{-\frac{t_\Sigma}{T}}}{r!}, \tag{121}$$

где T – средняя наработка до отказа (на отказ – для восстанавливаемых объектов).

Вероятность получения r отказов при условии, что верна гипотеза H_1 (несоответствие изделий заданным требованиям надежности):

$$P_1 = \left(\frac{t_\Sigma}{T_\beta}\right)^r \frac{e^{-\frac{t_\Sigma}{T_\beta}}}{r!}. \tag{122}$$

Вероятность получения r отказов при условии, что верна гипотеза H_0 (соответствие изделий заданным требованиям надежности):

$$P_0 = \left(\frac{t_\Sigma}{T_\alpha}\right)^r \frac{e^{-\frac{t_\Sigma}{T_\alpha}}}{r!}. \quad (123)$$

Отношение правдоподобия:

$$L = \frac{P_1}{P_0} = \left(\frac{T_\alpha}{T_\beta}\right)^r e^{-\left(\frac{1}{T_\beta}-\frac{1}{T_\alpha}\right)t_\Sigma}. \quad (124)$$

Условие приемки дает:

$$\left(\frac{T_\alpha}{T_\beta}\right)^r e^{-\left(\frac{1}{T_\beta}-\frac{1}{T_\alpha}\right)t_\Sigma} \le \frac{\beta}{1-\alpha}. \quad (125)$$

Логарифмируя последнее выражение, получаем

$$r \cdot ln\left(\frac{T_\alpha}{T_\beta}\right) - \left(\frac{1}{T_\beta}-\frac{1}{T_\alpha}\right)t_\Sigma \le ln\left(\frac{\beta}{1-\alpha}\right), \quad (126)$$

откуда после преобразований получаем условие соответствия:

$$r \le \frac{ln\left(\frac{\beta}{1-\alpha}\right)}{ln\left(\frac{T_\alpha}{T_\beta}\right)} + \frac{T_\alpha - T_\beta}{T_\beta ln\left(\frac{T_\alpha}{T_\beta}\right)}\frac{t_\Sigma}{T_\alpha}. \quad (127)$$

Замена знака « ≤ » на « = » в неравенстве дает уравнение линии соответствия 2 на плане последовательного контроля.

Условие браковки дает:

$$\left(\frac{T_\alpha}{T_\beta}\right)^r e^{-\left(\frac{1}{T_\beta}-\frac{1}{T_\alpha}\right)t_\Sigma} \ge \frac{1-\beta}{\alpha}. \quad (128)$$

Логарифмируя выражение, после преобразований получаем условие несоответствия:

$$r \ge \frac{ln\left(\frac{1-\beta}{\alpha}\right)}{ln\left(\frac{T_\alpha}{T_\beta}\right)} + \frac{T_\alpha - T_\beta}{T_\beta ln\left(\frac{T_\alpha}{T_\beta}\right)}\frac{t_\Sigma}{T_\alpha}. \quad (129)$$

Заменой знака « ≥ » на « = » в последнем неравенстве можно получить уравнение линии несоответствия 1 на плане последовательного контроля.

Усечение плана осуществляется по одноступенчатому методу. Уравнение линии усечения 4 на плане последовательного контроля:

$$r = \frac{T_\alpha - T_\beta}{T_\beta ln\left(\frac{T_\alpha}{T_\beta}\right)}\frac{t_\Sigma}{T_\alpha}. \quad (130)$$

Уравнение дополнительной линии соответствия 2' на плане последовательного контроля:

$$\frac{t_{\text{ус}}}{T_\alpha} = \frac{(1-\alpha)ln\left(\frac{1-\alpha}{\beta}\right) - \alpha ln\left(\frac{1-\beta}{\alpha}\right)}{\frac{T_\alpha}{T_\beta} - 1 - ln\left(\frac{T_\alpha}{T_\beta}\right)}. \quad (131)$$

Уравнение дополнительной линии несоответствия 1' на плане последовательного контроля:

$$r_{\text{ус}} = \frac{T_\alpha - T_\beta}{T_\beta ln\left(\frac{T_\alpha}{T_\beta}\right)}\frac{t_{\text{ус}}}{T_\alpha}. \quad (132)$$

При испытаниях без восстановления или замены отказавших изделий минимальный объем выборки $N_{min} = r_{ус}$.

При испытаниях с восстановлением или заменой объем выборки может быть любым.

При наличии отрицательных исходов графиком последовательных испытаний является ступенчатая линия 3.

Сумма отрезков линии, параллельных оси $\frac{t_\Sigma}{T_\alpha}$, равна отношению суммарной наработки испытываемых образцов в момент времени t испытаний к значению T_α, а сумма отрезков, параллельных оси r, равна числу отрицательных исходов (отказов) к моменту t.

При отсутствии отрицательных исходов графиком последовательных испытаний является прямая линия с началом в начале координат, совпадающая с осью $\frac{t_\Sigma}{T_\alpha}$. При этом суммарная наработка испытываемых образцов в момент времени t испытаний составит $t_\Sigma = Nt$.

При испытаниях с восстановлением или заменой суммарная наработка в момент времени t испытаний составит

$$t_\Sigma = Nt - \sum_{j=1}^{r} \tau_j, \qquad (133)$$

где τ_j – длительность восстановления работоспособности j-го из r отказавших образцов изделия или длительность замены j-го из отказавших образцов.

При испытаниях без восстановления или замены суммарная наработка в момент времени t испытаний может быть подсчитана по формуле:

$$t_\Sigma = (N-r)t - \sum_{j=1}^{r} t_j, \qquad (134)$$

где r – текущее число отказов, соответствующее наработке t каждого работоспособного изделия, отсчитанной от начала испытаний;

t_j – наработка j-го из r отказавших изделий, отсчитанная от начала испытаний.

Результаты испытания положительны, если график испытаний достигает линии соответствия (линия 3), и отрицательны, если график достигает линии несоответствия.

Если конечная точка графика испытаний находится в области неопределенности, то испытания должны быть продолжены (количество полученной при испытаниях информации недостаточно для вынесения решения о соответствии или несоответствии изделий требованиям надежности по контролируемому показателю).

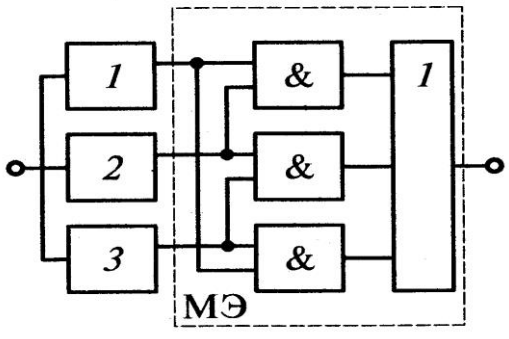


Рис. 1.7. Мажоритарное резервирование по правилу «два из трёх»

Для описания резервирования в структурном резервировании используется термин *«кратность резерва». Кратность резерва* — это отношение числа резервных элементов к числу резервируемых ими основных элементов системы, выраженное несокращенной дробью. *Резервирование с целой кратностью* имеет место, когда один основной элемент резервируется одним или более резервными элементами. *Резервирование с дробной кратностью* — это такое резервирование, когда два и более однотипных основных элементов ре-

зервируются одним и более резервными элементами (например, когда число основных элементов превышает число резервных). Резервирование, кратность которого равна единице, называется *дублированием.*

Резервные элементы в системе могут находиться в режиме основного элемента, в облегченном или ненагруженном режиме. *Нагруженный резерв* — это резерв, который содержит один или несколько резервных элементов, находящихся в режиме основного элемента. При этом принимается, что элементы нагруженного резерва имеют тот же уровень надежности, что и основные элементы объекта. *Облегченный резерв* — это резерв, который содержит один или несколько резервных элементов, находящихся в менее нагруженном режиме, чем основной. Элементы облегченного резерва обладают, как правило, более высоким уровнем надежности, чем основные элементы. *Ненагруженный резерв* — это резерв, который содержит один или несколько резервных элементов, находящихся в ненагруженном режиме до начала выполнения ими функций основного элемента. Для элементов ненагруженного резерва условно полагают, что они до начала выполнения ими функций основного элемента не отказывают и не достигают предельного состояния.

Резервные элементы в системе, также как и основные элементы, могут восстанавливаться после возникновения отказов. *Резервирование с восстановлением* – резервирование, при котором работоспособность любого одного или нескольких резервных элементов в случае возникновения отказов подлежит восстановлению. *Резервирование без восстановления* – резервирование, при котором работоспособность любого одного или нескольких резервных элементов в случае возникновения отказов не подлежит восстановлению. Восстанавливаемость резерва обеспечивается при наличии контроля работоспособности элементов. При наличии резервирования это особенно важно, так как в этом случае число скрытых отказов может быть больше, чем при отсутствии резервирования. В идеальном варианте отказ любого элемента объекта обнаруживается без задержки, а отказавший элемент незамедлительно заменяется или ремонтируется.

2. Оценивание надёжности функционирования программного обеспечения

2.1. Основные понятия надёжности программного обеспечения

Структура программного обеспечения

В иерархии программного обеспечения (ПО) выделяют следующие уровни:

— *программные модули (ПМ)* – законченные компоненты программ. ПМ решают небольшие функциональные задачи и содержат 100-1000 операторов объектного кода;

— *программы, пакеты прикладных программ (П*) – состоят из единиц или десятков ПМ и решают сложную автономную функциональную задачу, содержат до 10^4 операторов объектного кода;

— *комплексы программ (КП)* – завершенный программный продукт определенного целевого назначения, решающий сложные задачи управления и обработки информации.

Архитектура ПО – это:

- набор значимых решений по поводу организации системы программного обеспечения,
- набор структурных элементов (ПМ) и их интерфейсов, при помощи которых компонуется система, вместе с их поведением, определяемым во взаимодействии между этими элементами,
- компоновка элементов в постепенно укрупняющиеся подсистемы (П и ПК),

– стиль архитектуры, который направляет эту организацию – элементы и их интерфейсы, взаимодействия и компоновку.

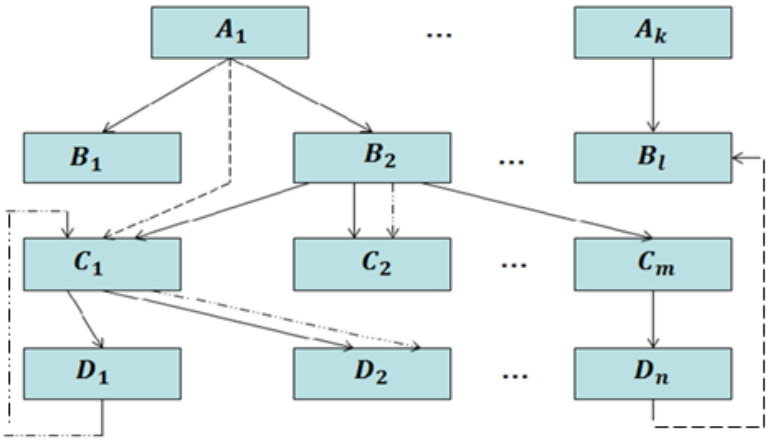


Рис. 2.1. Пример архитектуры ПО, поддерживающего управление физическим объектом

Уровень A – планирующие программы.
Уровень B – программы, обеспечивающие выполнение целевых задач.
Уровень C – программы выполнения типовых режимов работы.
Уровень D – обрабатывающие и управляющие программы.
⟶ – связи по управлению.
–··–> – информационные связи посредством обменных переменных.
– – –> – информационные связи посредством глобальных переменных.

Этапы жизненного цикла ПО

1. Анализ требований, предъявляемых к ПО;
2. Написание спецификаций;
3. Проектирование;
4. Кодирование;
5. Тестирование
6. Эксплуатация и сопровождение.

Требования, предъявляемые к *ПО*, как правило, включают:
– перечень функций, решаемых ПО;
– время обработки информации;
– объем и точность представления выходных данных;
– допустимые ресурсы вычислительной системы;
– допустимая вероятность возникновения ошибки и др.

Спецификации содержат, точное описание поведения ПО с точки зрения пользователя и выполняемые ПО функции, не указывая, каким образом это делается. Спецификации – основополагающий документ в процессе разработки ПО. Данный документ можно использовать для начальных оценок временных затрат, числа специалистов и других ресурсов, необходимых для проведения работ.

На этапе *проектирования* разрабатываются алгоритмы и формируется общая структура ПО. Все ПО разбивается на ПМ, к которым формулируются специфические требования:
– реализуемые функции,
– размеры,
– время выполнения и др.

Основными задачами исследования надежности на данном этапе являются:
– сравнительный анализ эффективности различных способов обеспечения надежности;

– выбор вариантов, обладающих заданной надежностью при учете реально

Итогом этапа является разработка блок-схемы процесса обработки информации существующих ограничений по различного рода ресурсам.

На этапе *кодирования* осуществляется преобразование программных спецификаций в операторы языка кодирования. Завершается этап трансляцией разработанного программного модуля в машинный код. Здесь появляется возможность наблюдения за поведением ПО и проверки выполнения заданных требований по надежности ПО.

На этапе *тестирования* (отладки) осуществляется проверка правильности функционирования разработанного ПО и удовлетворения требованиям его спецификации. В процессе тестирования используются данные, характерные для рабочего режима эксплуатации ПО. Основными методами исследования надежности ПО на этапе являются методы математической статистики.

На этапе *эксплуатации* осуществляется непосредственное взаимодействие пользователя с ПО и сопровождение программ, целью которого является корректировка и совершенствование ПО.

Источники ошибок ПО

На этапе анализа требований, предъявляемых к ПО:

– нечеткое понимание целей функционирования ПО заказчиком;
– неадекватность выражения им своих требований;
– недостаточная полнота их представления.

Их называют организационными ошибками.

На *этапе спецификаций*:

– недостаток знаний об описываемых физических процессах и явлениях;
– использование грубых упрощений;
– искажение или неполное представление структуры входной или выходной информации.

На *этапе проектирования* ошибки связаны:

– с несогласованностью выбранных параметров и преобразований с характеристиками внешних устройств;
– с неполной или некачественной взаимной увязкой отдельных частей ПО;
– с неправильным применением математического аппарата численного анализа и приближенных вычислений;
– нарушением правильной последовательности из-за неполного учета свойств управляемых объектов или условий работы с удаленными объектами;
– неадекватным представлением формализованных условий решения проблемы в виде блок-схем, подлежащих программированию.

Такие ошибки называют алгоритмическими.

На *этапе кодирования* появляются программные ошибки, источниками которых являются:

1) *технологические ошибки* – нарушения, допускаемые при выполнении отдельных технологических операций (искажение документации, ошибки при наборе текста и т.п.);
2) *семантические ошибки* – неправильное применение конструкций входного языка и невыполнение правил взаимосвязи элементов конструкций;
3) *структурные ошибки:*
   – наличие тупиковых и лишних участков,
   – нарушение правил построения схем вычислительного процесса,
   – неправильное использование переменных,
   – ошибки использования и распределения памяти,
   – нарушение правил построения топологической структуры программы;
4) неправильная организация вычислительного процесса;

5) неправильный учет реальных возможностей и ресурсов вычислительных систем, ведущий к нарушениям в обработке информации в реальном масштабе времени.

Из перечисленных источников и причин возникновения ошибок видно, что ненадежность ПО является следствием человеческого фактора. Поэтому надежность функционирования ПО должна обеспечиваться созданием условий и мер, позволяющих:

- снижать количество допущенных ошибок на ранних этапах разработки ПО,
- устранять обнаруженные при тестировании и отладке,
- не допускать новых ошибок в ходе его эксплуатации (сопровождении).

Термины и определения надежности ПО

Ошибка ПО – несоответствие результата функционирования ПО на исправном вычислительном средстве истинному результату.

Отказ ПО – результат проявления такой ошибки, после появления которой точность вычислений вышла за допустимые пределы.

Не все ошибки приводят к отказу функционирования ПО.

Надежность ПО – свойство ПО сохранять точность результата вычислений в допустимых пределах в процессе функционирования при заданных условиях.

Безотказность ПО – свойство ПО сохранять работоспособность в условиях, предусмотренных в его спецификации.

Восстанавливаемость ПО – определяется затратами времени и труда на устранение отказа из-за проявившейся ошибки в ПО и его последствий.

Устойчивость ПО – свойство ПО безотказно функционировать в условиях, не предусмотренных в его спецификации, а также при наличии аппаратных сбоев. Это понятие предполагает, что допустима некоторая потеря качества при функционировании ПО.

Эффективность ПО – свойство ПО в процессе функционирования на вычислительном средстве создавать выходной эффект в соответствии с целевым назначением объекта.

Показатели надежности ПО

Будем рассматривать программные объекты, которые функционируют до первого отказа, т.е. восстановление после отказа не осуществляется.

В условиях, когда *процесс отладки закончен*, показателями надежности функционирования ПО являются:

- вероятность безотказного функционирования ПО в течение требуемого времени;
- плотность распределения времени до отказа;
- интенсивность отказа ПО;
- среднее время безотказной работы функционирования ПО.

В условиях, когда *процесс отладки не закончен*, показателями надежности (степени отлаженности) ПО являются:

- распределение числа оставшихся в ПО ошибок по истечении определенного времени отладки и его числовые характеристики;
- распределение времени отладки ПО при условии обеспечения заданной вероятности его безотказного функционирования в дальнейшем.

Иногда на практике в качестве показателя степени отлаженности используется коэффициент степени отлаженности – вероятность того, что ПО будет функционировать безотказно в соответствии с техническим заданием. Однако чаще всего используется самый простой показатель – время отладки ПО.

2.2. Оценка надежности ПМ на этапе отладки

Классификация методов оценки надежности ПО

По *критерию учета структуры программы* методы оценки надежности ПО можно подразделить:

- на учитывающие структурные взаимосвязи между ее составными элементами;
- рассматривающие программу в виде «черного ящика».

По *критерию учета ошибок:*

- предусматривающие расчет ошибок;
- без расчета ошибок.

ПО *эффективности применения* на различных этапах жизненного цикла ПО:

- для этапов написания спецификаций, проектирования и кодирования программ лучшие оценки позволяют получить методы, основанные на *подходе Холстеда*. Он основывается на свойстве человеческого мозга принимать на ряду с правильными решениями и ошибочные. Поэтому в качестве основных метрических характеристик используются количества операторов и операндов;
- для этапа отладки широкое распространение получил *байесовский подход*. Данный подход позволяет объединить в процессе оценки априорные данные, полученные на ранних этапах жизненного цикла ПО, с данными испытаний. Достоверность оценок при этом не снижается;
- на этапах отладки и эксплуатации ПО хорошие результаты дают детерминистические метод, например, *метод Мусы.*

Достаточно универсальным методом оценки надежности ПО, который можно использовать как при разработке , так и при эксплуатации ПО, является *метод Нельсона.* Он позволяет учитывать эффективность тестов, применяемых для обнаружения ошибок.

Метод оценки надежности ПМ на основе его отладки

Постановка задачи:

Требуется определить вероятностные показатели функционирования ПМ по результатам его отладки, проводимой до использования модуля по его целевому назначению.

Алгоритм отладки:

1. Случайно выбираются значения исходных данных и выполняются вычисления на ЭВМ. Если до окончания вычислений отказа функционирования ПМ не произошло и результат вычислений соответствует эталонному, то случайным образом снова выбираются значения исходных данных, выполняются вычисления, результат проверяется на соответствие эталону и т.д.
2. Если в процессе вычислений фиксируется отказ до их окончания, то запоминается промежуток времени от начала вычислений до момента отказа.
3. Причина отказа определяется, отказ устраняется. Предполагается, что отказа устраняется мгновенно и новые ошибки не вносятся.
4. Затем вновь случайным образом выбираются значения исходных данных и процесс продолжается до тех пор, пока не будет получено достаточно статистических данных для оценки надежности ПМ.

Определение интенсивности и среднего времени между отказами

Пусть:

t_u – длительность одного успешного прогона;

t_i – время от начала i-го прогона до отказа в нем;

n – общее число прогонов;

r – число прогонов из n, в которых имели место отказы.

Тогда:

$$T^* = \frac{\sum_{i=1}^{r} t_i + (n-r)t_u}{n}; \quad \lambda^* = \frac{1}{T^*}; \tag{135}$$

где T^* – статистическое среднее время между отказами ПМ,

λ^*– статистическая интенсивность отказа.

Определение вероятности безотказной работы ПМ

Пусть N – начальное количество ошибок в ПМ, I – число команд в ПМ, тогда

$$\varepsilon_r(t_0) = \frac{N}{I} - \varepsilon_u(t_0); \quad \frac{N}{I} > \varepsilon_u(t_0); \quad \varepsilon_r(t_0) > 0; \tag{136}$$

где $\varepsilon_u(t_0)$ – число исправленных ошибок в ПМ за время отладки t_0,

$\varepsilon_r(t_0)$ – число оставшихся ошибок в ПМ после отладки.

$$F(t, t+\Delta t) = \lambda(t)\cdot\Delta t = k\cdot\varepsilon_r(t_0)\cdot\Delta t, \tag{137}$$

где $F(t, t+\Delta t)$ – условная вероятность отказа ПМ в интервале $[t, t+\Delta t)$, найденная при условии, что до момента t отказа не было;

$\varepsilon_r(t_0)$ – число оставшихся ошибок в ПМ после отладки;

k – некоторая постоянная.

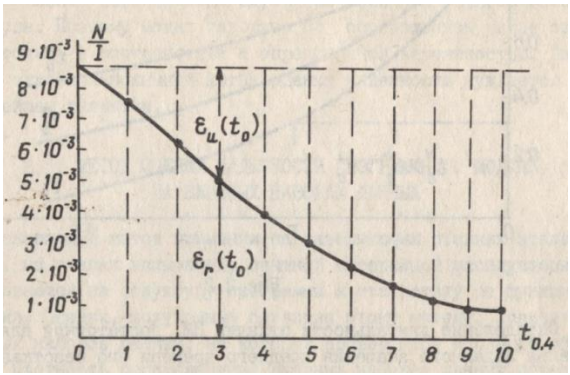


Рис. 2.2. Характерный вид зависимости $\varepsilon_r(t_0)$ от времени отладки

При допущении, что распределение времени до отказа подчинено экспоненциальному закону, вероятность его отсутствия будет равна

$$P(t) = e^{-\lambda t} = e^{-k\varepsilon_r(t_0)t}. \tag{138}$$

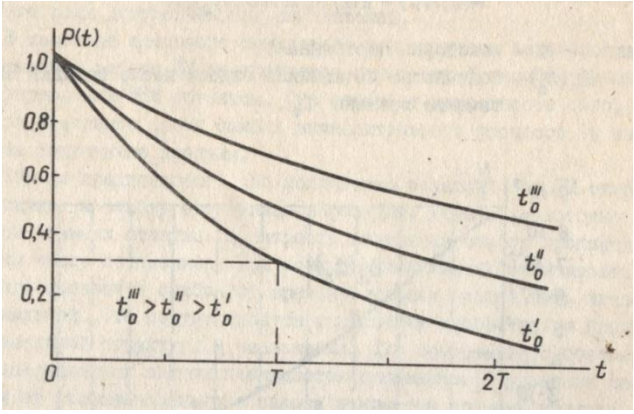


Рис. 2.3. Зависимость вероятности безотказной работы ПМ от времени функционирования для различных времен отладки t_0

Среднее время безотказной работы, определяемое из выражения для *P(t)* будет равно:

$$T = \int_0^\infty P(t)dt = \frac{1}{k \cdot \varepsilon_r(t_0)} = \frac{I}{k[N - I\varepsilon_u(t_0)]}. \quad (139)$$

Определение k и N

Пусть для различных t_0 ' и t_0" определены $\varepsilon_u(t_0')$ и $\varepsilon_u(t_0'')$. Тогда средние времена безотказной работы для каждого периода отладки t_0 ' и t_0" будут равны:

$$T_1 = \frac{1}{\lambda_1} = \frac{I}{k[N - I\varepsilon_u(t_0')]};\ T_2 = \frac{1}{\lambda_2} = \frac{I}{k[N - I\varepsilon_u(t_0'')]}. \quad (140)$$

Тогда

$$N = \frac{I[\eta\varepsilon_u(t_0') - \varepsilon_u(t_0'')]}{\eta - 1};\ \eta = \frac{T_1}{T_2} = \frac{\lambda_2}{\lambda_1};\ K = \frac{\lambda_1}{[\frac{N}{I} - \varepsilon_u(t_0')]} = \frac{\lambda_2}{[\frac{N}{I} - \varepsilon_u(t_0'')]}. \quad (141)$$

Данный метод прост для практического применения и учитывает влияние времени отладки ПМ на показатели его надежности. Однако метод предполагает, что число ошибок в ПМ не случайно. На самом деле оно случайно.

Повышение надежности ПМ на этапе отладки

Надежность ПМ определяется количеством дефектов, заложенных на стадиях ее проектирования и кодирования.

Отладка один из основных этапов создания надежных ПМ.

При выборе тестовых наборов данных учитываются:

– алгоритм ПМ и распределение переменных, являющихся исходными для данного алгоритма;

– характеристики вычислительной (вычислительные средства) и программной (общесистемное и специальное ПО) сред;

– характеристики возможных воздействий, влияющих на программную среду;

– структура ПМ.

Процесс выбора тестовых входных наборов данных осуществляется:

– вручную, когда каждый вариант исходных данных формируется разработчиком ПМ;

– автоматизировано, с использованием специальных имитирующих программ, рассчитывающих тесты непосредственно в ЭВМ, на которой функционируют тестируемые ПМ;

– автоматизировано, с использованием универсальной технологической ЭВМ для генерации тестовых входных наборов данных с последующим их введением в ЭВМ, на которой ведется отладка ПМ;

– автоматизировано, с использованием специальной аналоговой и цифровой аппаратуры для генерации тестовых входных наборов данных.

–

2.3. Проектирование и производство ПО АС

Этапы проектирования и производства программ

Сокращение жизненного цикла ПО и повышение требований к его качеству является характерными особенностями развития сферы информатизации на современном этапе.

Жизненный цикл ПО — период времени, от момента принятия решения о необходимости создания ПО до момента его утилизации. Жизненный цикл делится на множество этапов, включая разработку и использование ПО.

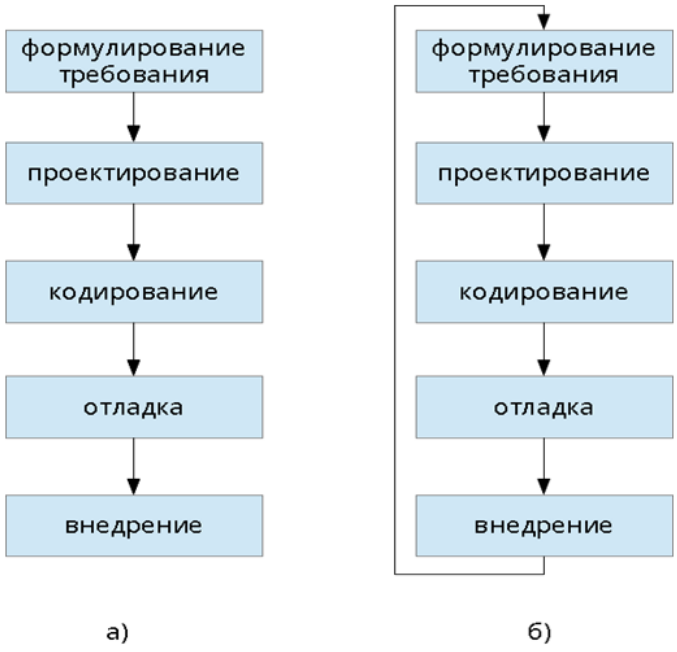


Рис. 2.4. Модели жизненного цикла: а) - каскадная и б) - итерационная модели жизненного цикла.

При использовании *каскадной* модели, дефекты накапливаются по мере реализации проекта. Поиск и устранение дефектов выполняется лишь на этапе отладки, при этом может быть использовано тестирование или верификация ПО.

В *итеративной* модели жизненный цикл делится на итерации, каждая из которых включает все этапы процесса разработки (проектирование — реализация — тестирование — оценка результатов). В результате каждой итерации создаётся работающая модель системы, при этом каждая последующая итерация должна улучшать ПО. В итеративной модели поиск дефектов осуществляется многократно — он обязательно выполняется на каждой итерации.

Управление показателями качества ПО в процессе проектирования и производства

Под управлением качеством понимается совокупность организационной структуры и ответственных лиц, а также процедур, процессов и ресурсов для планирования и управления достижением качества ПО.

В различных источниках терминология и состав характеристик качества ПО отличается. В таблице приведен возможный состав характеристик качества ПО:

Таблица 1. Возможный состав характеристик качества ПО

Характеристика качества	Мера	Требуемое значение
Надежность: наработка на отказ при отсутствии рестарта	час	10
Устойчивость: наработка на отказ при наличии автоматического рестарта	Час	50
Восстанавливаемость: длительность восстановления	минута	5
Доступность-готовность: относительное время работоспособного функционирования	вероятность	0,998
Эффективность: время отклика, получения результатов на типовое задание	секунда	5
пропускная способность, число типовых заданий, исполняемых в единицу времени	число в минуту	20
Используемость ресурсов: относительная величина использования ресурсов ЭВМ при нормальном функционировании ПО	вероятность	0,8

Существует два важнейших стандарта в области качества ПО. Общая система менеджмента качества *ISO* 9001:2000 и представленный в виде специальных рекомендаций стандарт *ISO* 90003:2004.

Управление качеством ПО определяет:

- процессы обеспечения качества;
- процессы управления качеством;
- процессы подтверждения качества.

Процессы *обеспечения качества* служат для подтверждения того, что программные продукты и процессы жизненного цикла проекта соответствуют заданным требованиям. Процессы обеспечения качества включают:

- процесс верификации;
- процесс аттестации;
- процесс совместного анализа;
- процесс аудита.

Процессы *Аттестации* и *Верификации* обеспечивают подтверждение соответствия ПО предъявляемым к нему требованиям.

Верификация – попытка обеспечить правильную разработку продукта, т.е. соответствие спецификациям, заданным в процессе предыдущей деятельности.

Аттестация – попытка обеспечить создание правильного продукта с точки зрения достижения поставленной цели.

Оба процесса – верификация и аттестация – начинаются на ранних стадиях разработки и сопровождения. В настоящее время большее распространение получила Верификация.

Процессы *управления качеством* обеспечивают нахождение дефектов на основе сбора информации на всех стадиях разработки и сопровождения ПО.

Процессы *подтверждения качества*, исследуют и оценивают любой выходной продукт, связанный со спецификацией требований к ПО, на предмет трассируемости *(возможности соотнести элемент проекта с другими элементами, особенно связанными с требованиями),* согласованности, полноты (завершенности), корректности и непосредственно выполнения требований.

Таблица 2. Применение международных стандартов в области создания ПО

Основополагающие международные стандарты	Области применения	Примечание
ISO 9001 ISO 90003 ISO 15504	Система менеджмента качества и оценки зрелости процессов жизненного цикла ПС	Система менеджмента качества организации, рекомендации по совершенствованию процессов, уровни зрелости процессов.
ISO 15288 ISO 12207	Качество процессов жизненного цикла Систем и ПО	Процессы и работы проводимые в рамках создания Систем и ПО охватывающие весь жизненный цикл ПО.
ISO 9126	Качество продукта	Модели качества, способы оценки качества и метрики количественной оценки качества.
ISO 9127	Документирование	Процессы документирования на всех этапах ЖЦ.
ISO 12119	Подтверждение качества ПО	Технология тестирования ПО на различных этапах жизненного цикла.

Обеспечением качества необходимо заниматься на всем протяжении жизненного цикла ПО. Причем это наиболее важно на начальных его этапах.

Накопленный опыт данной сферы заключен во множестве современных международных стандартов, который может быть незаменим при производстве высококачественной конкурентоспособной продукции в сфере информационных технологий.

2.4. Оценивание надёжности функционирования комплексов программ, планирование и организация испытаний ПО

Оценивание надёжности функционирования комплексов программ

Сложные программные комплексы (ПК) можно представить в виде совокупности отдельных программных модулей (ПМ), связанных между собой.

Анализ решаемых целевых задач и спецификаций на ПМ позволяют составить стохастический граф ПК. Основной задачей при анализе стохастического графа является получение функции распределения времени безотказной работы ПК по известным функциям распределения времени безотказной работы отдельных ПМ.

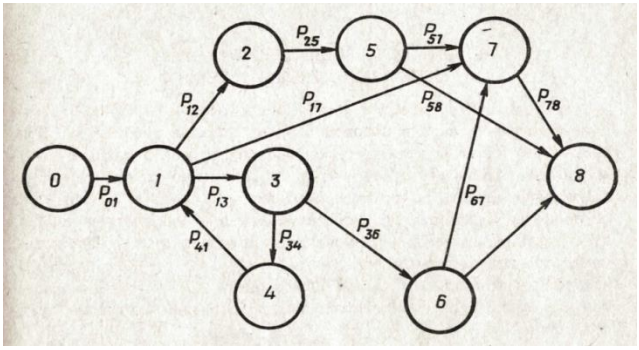


Рис. 2.5. Стохастический граф ПК.

В стохастическом графе нулевая вершина отражает факт начала использования ПК, восьмая (конечная) – факт окончания его работы, а остальные – ПМ.

Вероятности вызова одного ПМ другим P_{ij} определяются на основе анализа технологии использования ПК и частоты реализации связи между *i*-м и *j*-м ПМ при решении целевых задач и различных исходных данных. Сумма вероятностей P_{ij} равна 1.

Планирование и испытания ПО

Испытания являются важнейшим элементом управления качеством продукции.

В соответствии с ГОСТ 19,004–80 *под испытанием* ПО понимают установление соответствия ПО заданным требованиям и программным документам.

Это определение построено на предположении, что в техническом задании на разработку ПО определены все требования (характеристики), обеспечение которых гарантирует его пригодность к использованию по своему назначению.

Целью испытания является экспериментальное определение фактических (достигнутых) характеристик свойств испытываемого ПО.

Эти характеристики могут быть как количественными, так и качественными. Важно, чтобы на их основе можно было сделать вывод о пригодности данного ПО к использованию по своему назначению. Если вывод отрицательный, то образец ПО возвращается на доработку.

Испытание является завершающим этапом разработки. Ему предшествует этап отладки программ. Цели у отладки и испытания разные. Полностью отлаженная программа может не обладать определенными потребительскими свойствами и тем самым быть непригодной к использованию по своему назначению.

Не может служить альтернативой испытанию и проверка работоспособности программы на контрольном примере, так как программа, работоспособная в условиях контрольного примера, может оказаться неработоспособной в других условиях применения. Попытки охватить контрольным примером все предполагаемые условия функционирования сводятся в конечном счете к тем же испытаниям.

Длительность испытания зависит от типа, конфигурации (сложности) ПО, а также от целей и степени автоматизации рассматриваемого технологического процесса. При испытании операционных систем она колеблется от одного до шести месяцев. Сложные программные комплексы после интеграции могут испытываться и более длительное время.

Основными видами испытания ПО являются:

- предварительные;
- приемочные;
- эксплуатационные испытания, включая опытную эксплуатацию.

В зависимости от места проведения различают:

- стендовые;
- полигонные испытания.

Под *испытательным стендом* понимают совокупность технических устройств и математических моделей, обеспечивающих в автоматическом режиме:

- имитацию среды функционирования;
- поступление входных данных, искажающие воздействия;
- регистрацию информации о функционировании ПО;
- управление процессом испытания и объектом испытания.

Испытательным полигоном называют место, предназначенное для испытаний в условиях, близких к условиям эксплуатации, и обеспеченное необходимыми средствами испытания.

Полигонным испытаниям подвергают системы, работающие в реальном масштабе времени. В полигонных условиях обычно сочетают натурные испытания с использованием реальных объектов автоматизируемых систем.

План проведения испытаний должен быть ориентирован на обеспечение:

a) всесторонней проверки ПО;

b) максимальной (заданной) достоверности полученных результатов при использовании ограниченных ресурсов, выделенных на испытаниях.

Принципиально возможны следующие подходы к решению этой задачи:

1. Анализируют весь диапазон входных данных. На основе анализа заранее готовят такое множество тестовых наборов данных, которое охватывает наиболее характерные подмножества входных данных. Программу рассматривают как черный ящик. Испытания сводятся к последовательному вводу тестовых наборов данных и анализу получаемых результатов;
2. Анализируют множество ситуаций, которые могут возникнуть при функционировании ПО. Выбирают наиболее характерные ситуации. Каждую из них выражают через тестовый набор входных данных. Далее сущность испытания и анализа результатов сводится к подходу (1);
3. Строят граф-схему структуры ПО. Выбирают множество путей, которое полностью покрывает граф-схему ПО, и такую последовательность тестовых наборов исходных данных, выполнение которой будет проходить по выделенным путям. Организация испытаний аналогична подходам (1) и (2);
4. ПО испытывают в реальной среде функционирования;
5. ПО испытывают в статистически моделируемой среде функционирования, адекватной реальной среде.

Ни один из этих подходов не является универсальным. Каждый из них имеет свои преимущества и недостатки, которые в разной степени проявляются в зависимости от специфики испытываемого ПО.

3. Оценка надежности оперативного персонала АС

3.1. Влияние оперативного персонала на надежность АС

Оперативный персонал в составе АС принимает непосредственное участие в реализации ее функций.

Роль оперативного персонала заключается в следующем:

- наблюдение за ходом технологического процесса и правильностью функционирования АС;
- настройка, ввод установок, запуск и коррекция работы технических средств;
- принятие решения по управлению технологическим процессом по не алгоритмизированным правилам;

— непосредственное воздействие на ход технологического процесса включением и отключением регулирующих органов и механизмов в некоторых режимах работы объекта (например, пусковых) или при отказах технических средств.

Оперативный персонал, являясь звеном в структуре АС, может повысить или понизить общую надежность АС. Если оперативный персонал используется в качестве резервного звена в структуре АС, то он повысит общую надежность АС. Если же он используется в качестве основного звена в структуре АС, то он понизит общую надежность АС.

Под *надежностью* оперативного персонала понимается совокупность его свойств, проявляющихся при его участии в функционировании АС и влияющих на ее надежность.

Основными из этих свойств являются:

— безошибочность – способность оперативного персонала выполнять все заданные операции без ошибок;

— своевременность – способность оперативного персонала выполнять заданные операции за заданное время.

В настоящее время сложилось два подхода к учету влияния оперативного персонала на надежность АС.

Первый подход рассматривает оперативный персонал как отдельный элемент системы «человек – техника», аналогичный техническим элементам. При этом рассматриваются показатели надежности оперативного персонала аналогичные показателям надежности технических средств. Например, если оперативный персонал используется в качестве основного звена в структуре АС, то

$$P_{\text{АС}}(t) = P_{\text{Т}}(t)\, P_{\text{О}}(t), \tag{142}$$

где $P_{\text{Т}}(t)$ – вероятность безотказной работы технической системы в течение времени t;

$P_{\text{О}}(t)$ – вероятность безотказной работы оперативного персонала в течение времени t.

Такой подход является довольно грубым, не учитывает активную роль оперативного персонала в системе и другие принципиальные отличия человека.

При *втором подходе* оперативный персонал как элемент АС в задачах надежности имеет ряд существенных особенностей. К ним относятся:

— адаптация к условиям труда;

— существенное отличие характеристик различных операторов друг от друга;

— утомляемость;

— подверженность эмоциональным воздействиям и т.д.

В качестве характеристики безошибочности работы оперативного персонала применяют частоту (вероятность) появления ошибок. Статическое определение частоты ошибок в i-ом опыте:

$$q_i{}^* = \frac{m_i}{n_i}, \tag{143}$$

где n_i – количество предъявленных персоналу тестов в i-ом опыте;

m_i – количество ошибок персонала в i-ом опыте.

В процессе обучения частота ошибок обычно уменьшается и хорошо аппроксимируется экспоненциальной зависимостью

$$q = q_c + (q_0 - q_c)e^{-\frac{n}{N}}, \tag{144}$$

где q_0 – начальное (до обучения) значение частоты ошибок;

q_c – установившееся значение частоты ошибок, при котором оперативный состав считается обученным;

n – накопленная сумма предъявленных персоналу тестов в предыдущих опытах и половина числа тестов в данном опыте;

N – «постоянная обучения», т.е. некоторое среднее характеристическое число опытов.

При $N = n$ разность $(q_0 - q_c)$ уменьшается на 63%. Считается, что значение q_c практически достигается при (4–5) N.

Стабильность обучения оперативного персонала характеризуется средним квадратическим отклонением статистических частот ошибок q_i* от экспоненты q_i:

$$\sigma = \sqrt{\frac{1}{k-1}\sum_{i=1}^{k}(q_i * - q_i)^2}, \quad (145)$$

где k – число опытов.

В качестве показателя *безошибочности* можно рассматривать $P_б$ –вероятность безошибочного выполнения процедуры, т.е. вероятность того, что при выполнении рассматриваемой процедуры будут правильно выполнены именно те операции, которые составляют данную процедуру, и в заданной последовательности.

В качестве показателя *своевременности* чаще всего используют $P_с$ – вероятность своевременного выполнения процедуры, т.е. вероятность того, что совокупность всех операций, составляющих данную процедуру, будет выполнена за время, не превышающее допустимое.

Если же длительность t выполнения процедуры имеет порядок часа и более, то показателем надежности может быть вероятность $P(t)$ безошибочных, своевременных действий оператора за время t.

Основные способы повышения надежности оперативного персонала:

– не допускать условия, вызывающие переутомления в работе: физические, умственные, психические;

– не допускать условия, вызывающие ошибочные действия.

Переутомление в работе возникает:

– вследствие несовершенства рабочего места;

– вследствие нарушение правил охраны труда;

– вследствие внешних информационных воздействий, которые превышают физические возможности человека по восприятию и переработке информации для формирования управленческих решений.

Ошибочные действия человек совершает обычно:

– когда он имеет малый опыт в работе или низкую квалификацию;

– когда он осваивает новое изделие, не имея хороших инструкций;

– когда он отвлекается, спонтанно или вследствие дестабилизирующих внешних воздействий разной природы.

3.2. Модель надежности оперативного персонала АС

Рассматриваемая модель надежности оперативного персонала АС предложена д.т.н. профессором Смагиным В.А. В модели используется первый подход к учету влияния оперативного персонала на надежность АС, т.е. оперативный персонал рассматривается как отдельный элемент системы «человек – техника», аналогичный техническим элементам.

Особенность модели – вероятностный ресурс работоспособности оперативного персонала АС представлен в виде двух противоположно направленных составляющих:

– расходуемый ресурс работоспособности;

– восполняемый ресурс работоспособности.

Восполняемый ресурс работоспособности формируется в процессе обучения персонала и предшествует его расходу в процессе работы.

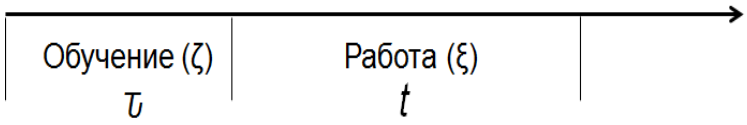


Рис. 3.1. Временная диаграмма модели

Так как *расходуемый ресурс* работоспособности растрачивается персоналом в процессе обучения и в процессе работы, то

$$P_{\text{р}}(t,\tau) = \frac{P(t+x(\tau),\varepsilon)}{P(x(\tau),\varepsilon)}, \tag{146}$$

где $P_{\text{р}}(t,\tau)$ – условная вероятность безошибочной деятельности персонала за время t при условии, что он обучался в течение времени τ в режиме ζ;

$P(y,\varepsilon)$ – безусловная вероятность безошибочной деятельности персонала за время y в режиме ε;

$x(\tau)$ – время работы персонала в режиме ε, эквивалентное по расходу ресурса работоспособности за время τ в режиме ζ.

Тогда условная интенсивность отказа (ошибки) персонала в момент времени t при условии, что он обучался в течение времени τ в режиме ζ будет равна

$$\lambda_{\text{р}}(t,\tau) = \frac{-P_{\text{р}}'(t,\tau)}{P_{\text{р}}(t,\tau)} = \lambda(t + x(\tau), \varepsilon), \tag{147}$$

где $\lambda(y,\varepsilon)$ – интенсивность отказа (ошибки) персонала при отсутствии обучения.

А интенсивность отказа (ошибки) персонала после обучения будет равна

$$\Lambda(t,\varepsilon) = P_y(\tau,\zeta)\,\lambda(t+x(\tau),\varepsilon), \tag{148}$$

где $\text{P}_\text{y}(\tau,\zeta)$ – вероятность неустранения потенциальной ошибки персонала за время обучения τ в режиме ζ, которая может привести к отказу в будущем во время работы в режиме ε.

Данное выражение означает, что потенциальное число ошибок персонала после обучения уменьшается в $P_y(\tau,\zeta)$ раз.

$$P_y(\tau,\zeta) = e^{-\int_0^\tau \nu(y,\zeta)dy}, \tag{149}$$

где $\nu(y,\zeta) = \frac{-P_y'(\tau,\zeta)}{P_y(\tau,\zeta)}$ – интенсивность проявления ошибки в момент времени τ.

Вероятность успешного функционирования персонала после обучения будет равна

$$P_{\text{о}}(t,\tau) = e^{-\int_0^t \Lambda(y,\varepsilon)dy} = e^{-\int_0^t \lambda(t+x(\tau),\varepsilon)dy e^{-\int_0^\tau \nu(z,\zeta)dz}}. \tag{150}$$

Здесь

$e^{-\int_0^t \lambda(t+x(\tau),\varepsilon)dy e^{-\int_0^\tau \nu(z,\zeta)dz}}$ – ресурс работоспособности (надежности) персонала;

$e^{-\int_0^t \lambda(t+x(\tau),\varepsilon)dy}$ – выработанный ресурс работоспособности за время t в условиях ε;

$e^{-\int_0^\tau \nu(z,\zeta)dz}$ – восполненный ресурс работоспособности, полученный персоналом в процессе обучения за время τ в условиях ζ.

При условии полного восстановления расходуемого ресурса персонала после обучения, когда $x(\tau) = 0$, вероятность успешного его функционирования будет равна

$$P_0(t,\tau) = e^{-\int_0^t \lambda(t,\varepsilon)dy \cdot e^{-\int_0^\tau \nu(z,\zeta)dz}}. \quad (151)$$

Для перерасчета времени τ обучения персонала в режиме ζ в эквивалентное время $x(\tau)$ работы персонала в режиме ε можно использовать физический принцип надежности Н.М. Седякина. Суть принципа в том, что надежность объекта в будущем зависит от величины ресурса (запаса) надежности, выработанного в прошлом, и не зависит от того, как вырабатывался этот ресурс.

Под ресурсом надежности $r(t,\varepsilon)$ в условиях ε Н.М. Седякин предложил понимать интеграл

$$r(t,\varepsilon) = \int_0^t \lambda(x,\varepsilon)dx, \quad (152)$$

который входит в «главное» выражение надежности

$$P_\varepsilon(t) = e^{-\int_0^t \lambda(x,\varepsilon)dx}. \quad (153)$$

Тогда, согласно принципу Н.М. Седякина, эквивалентное время $x(\tau)$ работы персонала в режиме ε находится из решения равенства ресурсов затраченных в режимах ζ и ε:

$$\int_0^{x(\tau)} \lambda(y,\varepsilon)dy = \int_0^\tau \lambda(y,\zeta)dy, \quad (154)$$

где $\lambda(y,\varepsilon)$ – интенсивность отказа (ошибки) персонала в режиме ε;

$\lambda(y,\zeta)$ – интенсивность отказа (ошибки) персонала в режиме ζ.

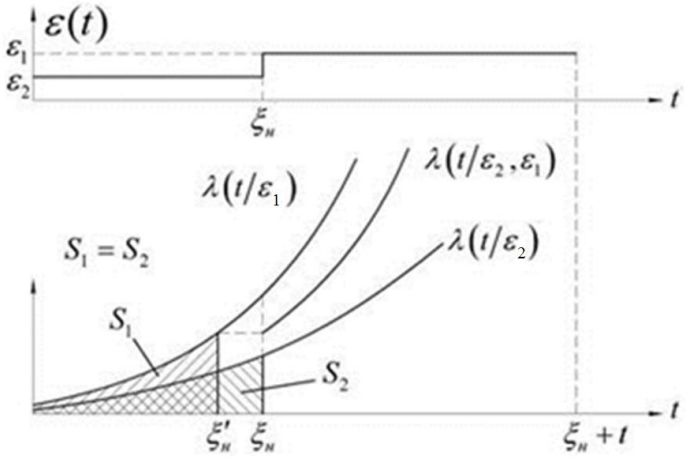


Рис. 3.2. Иллюстрация принципа Н.М. Седякина

4. Примеры решения инженерных задач надежности

4.1. Выбор стратегии использования запасных частей вычислительного комплекса автоматизированной системы

Обеспечению надежности вычислительных комплексов (ВК) автоматизированных систем (АС) наземного автоматизированного комплекса управления (НАКУ) всегда уделяется большое внимание, поскольку ВК являются его основным информационным звеном. Поэтому при поставках в эксплуатирующие организации и вводе в эксплуатацию ВК в обязательном порядке комплектуются запасными частями, инструментом, принадлежностями и рас-

ходным материалом (ЗИП) для поддержания работоспособности и исправности составных частей ВК в процессе эксплуатации, проведении всех видов технического обслуживания, плановых и неплановых ремонтов [3]. Запасные части – это детали, узлы, механизмы, блоки, приборы, пульты, стойки, модули и др.

Запасные части, включенные в состав ЗИП, изготавливают по той же конструкторской и технологической документации, что и соответствующие составные части ВК. Поэтому запасные и соответствующие составные части ВК в плане надежности можно считать однородными.

Как правило, запасные части используются по мере выхода из строя (отказа) соответствующих им составных частей ВК. Это основная стратегия использования ЗИП. Назовем ее *стратегией А*. В теории надежности [1,2] при анализе надежности восстанавливаемых систем подразумевается именно такая стратегия использования резервных элементов (запасных частей). Возможна и другая стратегия, когда запасные части и соответствующие им составные части ВК используются в процессе эксплуатации поочередно. Назовем ее *стратегией В*. Сущность *стратегии В* интуитивно заключается в том, чтобы равномерно расходовать ресурс, как запасных, так и соответствующих им основных частей ВК, и тем самым, увеличивать наработку до отказа, повышать его надежность.

Для сравнения названных стратегий использования запасных частей и определения условий их применения необходимо оценивать надежностные характеристики ~~ВС~~ ВК для обеих стратегий. Если для *стратегии А* математическая модель в теории надежности имеется, например, для общего резервирования элементов замещением с ненагруженным резервом, то для *стратегии В* ее нет. Поэтому является актуальной задача разработки математической модели для оценивания надежностных характеристик ВК для *стратегии В* на примере общего резервирования элементов замещением с ненагруженным резервом. Такой подход позволит провести объективный сравнительный анализа обеих стратегий с целью определения условий, в которых выгодна та или иная стратегия.

Рассмотрим обе стратегии с позиции надежности на примере общего резервирования элементов ВК замещением с ненагруженным резервом [2] (рис. 4.1).

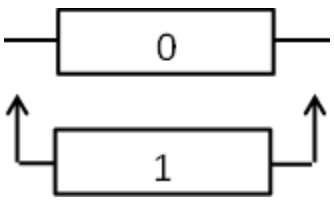


Рис. 4.1. Общее резервирование замещением

Здесь основной элемент 0 – основная часть ВК, а резервный элемент 1 – соответствующая запасная часть ВК. Основной и резервный элементы равно надежны и имеют вероятность безотказной работы *P(t)* и плотность *f(t).*

Для *стратегии А* согласно [1,2] для *m* резервных элементов (запасных частей) вероятность безотказной работы резервированной системы будет определяться выражением (155):

$$P_A\,(t) = \sum_{i=0}^{m} f^{(i)} * P(t), \qquad (155)$$

где $f^{(i)*}\ P(t) = \int_0^t f(x_1)\int_0^{t-x_1} f(x_2)\ldots\int_0^{t-x_1-\cdots-x_{i-1}} f(x_i)P(t-x_1-\ldots-x_i)dx_i\ldots dx_1$ – i-кратная свертка плотностей с $P(t)$.

Диаграмма работы резервной системы при *стратегии В* приведена на рис. 4.2.

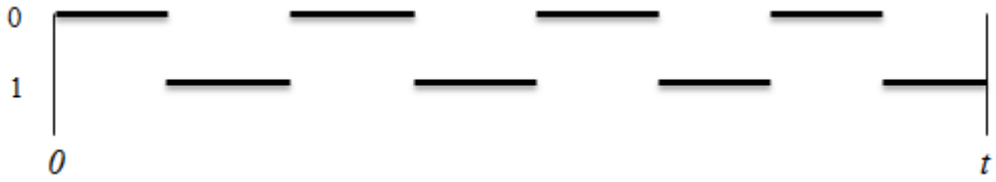


Рис. 4.2. Диаграмма работы резервированной системы при стратегии В.

Резервированная система проработает безотказно в течение времени t при наступлении одного из трех несовместных событий:

— событие B_1 заключается в том, что основной и резервный элементы проработают безотказно в течение времени t, при этом наработка каждого из них составит $\frac{1}{2}t$;

— событие B_2 заключается в том, что основной элемент откажет в момент времени x $(x < \frac{1}{2}t)$, а резервный элемент проработает исправно оставшееся время $t - x$, при условии, что до этого он исправно проработал в течение времени x;

— событие B_3 заключается в том, что резервный элемент откажет в момент времени x $(x < \frac{1}{2}t)$, а основной элемент проработает исправно оставшееся время $t - x$ при условии, что до этого он исправно проработал в течение времени x.

Иллюстрация событий B_1, B_2 и B_3 показана на рис.3, где сплошными линиями показана чистая наработка элементов, т.е. без учета времени нахождения в выключенном состоянии.

Вероятность безотказной работы резервированной системы $P_B(t)$ по теореме сложения вероятностей будет равна сумме вероятностей событий B_1, B_2 и B_3.

$$P_B(t) = Bep(\mathrm{B}_1) + Bep(\mathrm{B}_2) + Bep(\mathrm{B}_3) = P(\tfrac{t}{2})^2 + 2\int_0^{\frac{t}{2}} f(x)P(t-x|x)dx, \qquad (156)$$

где $P(t-x|x)$ – условная вероятность того, что элемент безотказно проработает в течение времени $t - x$ при условии, что до этого исправно проработал в течение времени x.

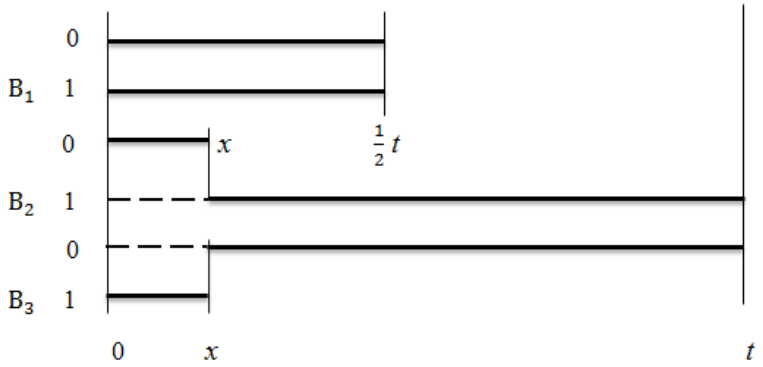


Рис. 4.3. Возможная наработка элементов при стратегии В

По теореме умножения вероятностей $P(t-x|x) = \frac{P(t)}{P(x)}$, тогда

$$P_B\ (t) = P(\frac{t}{2})^{\,2} + 2P(t)\int_0^{\frac{t}{2}} \frac{f(x)}{P(x)}dx. \qquad (157)$$

Для общего случая при количестве резервных элементов равном *m:*

$$P_B\ (t) = \sum_{i=0}^{m} A_{m+1}^{i} \int_0^{\frac{t}{m+1}} f(x_1) \int_0^{\frac{t-x_1}{m}} f(x_2) \ldots$$

$$\ldots \int_0^{\frac{t-x_{i-1}}{2}} f(x_i)\, P(\frac{t-x_1-\cdots-x_i}{m+1-i} | x_1 + \cdots + x_i)^{m+1-i} dx_i \ldots dx_1, \qquad (158)$$

где $A_{m+1}^{i} = \frac{(m+1)!}{(m+1-i)!}$ – число перестановок из $m+1$ по i;

$P(\frac{t-x_1-\cdots-x_i}{m+1-i} | x_1 + \cdots + x_i)$ – условная вероятность того, что элемент проработает безотказно в течение времени $\frac{t-x_1-\cdots-x_i}{m+1-i}$ при условии, что он ранее проработал безотказно в течение времени $x_1 + \cdots + x_i$;

$$P(\frac{t-x_1-\cdots-x_i}{m+1-i} | x_1 + \cdots + x_i) = \frac{P(\frac{t+(m-i)(x_1+\cdots+x_i)}{m+1-i})}{P(x_1+\cdots+x_i)}.$$

На рис. 4.4 приведены зависимости вероятностей безотказной работы резервированной системы $P_A(t)$ и $P_B(t)$. Вероятности $P_A(t)$ и $P_B(t)$ вычислялись по формулам (155) и (158) для $m = 1$. Было принято, что вероятности безотказной работы элементов и плотности, подчиненны закону распределения Вейбулла с параметрами $k = 2$ и $\lambda = 0{,}00011/ч$. Выбор закона Вейбулла обусловлен тем, что он одинаково хорошо описывает надежностные характеристики технических объектов на всех этапах их эксплуатации.

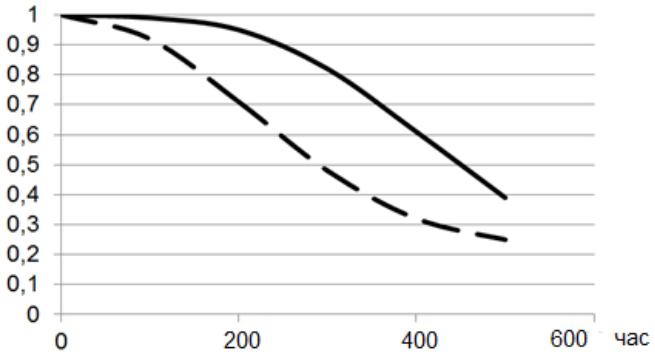


Рис.4.4. Зависимости вероятностей безотказной работы резервированной системы $P_A(t)$ – для стратегии А (пунктирная линия) и $P_B(t)$ – для стратегии В (сплошная линия)

При экспоненциальном распределении времени безотказной работы элементов, который обычно с большими допущениями используется на этапе нормальной эксплуатации и только для нерезервированных систем, данные стратегии не различимы, так как экспоненциальный закон распределения с параметром λ является законом без “памяти”. Покажем это на примере

вычислений по формулам (155) и (158) для $m = 2$, вероятности безотказной работы элементов $P(t) = e^{-\lambda t}$ и плотности $f(t) = \lambda e^{-\lambda t}$.

Для стратегии А:

$$P(t)_A = e^{-\lambda t} + \int_0^t \lambda e^{-\lambda x_1} e^{-\lambda (t-x_1)}\, dx_1 +$$

$$+ \int_0^t \lambda e^{-\lambda x_1} \int_0^{t-x_1} \lambda e^{-\lambda x_2} e^{-\lambda (t-x_1-x_2)}\, dx_2 dx_1 =$$

$$= e^{-\lambda t}\left(1+\lambda t + \frac{(\lambda t)^2}{2}\right). \qquad (159)$$

Для *стратегии В*:

$$P(t)_B = e^{-3\lambda \frac{t}{3}} + \int_0^{\frac{t}{3}} \lambda e^{-\lambda x_1} \frac{e^{-2\lambda(\frac{t+x_1}{2})}}{e^{-2\lambda(x_1)}}\, dx_1 +$$

$$+ 6\int_0^{\frac{t}{3}} \lambda e^{-\lambda x_1} \int_0^{\frac{t-3x_1}{2}} \lambda e^{-\lambda x_2} \frac{e^{-\lambda t}}{e^{-\lambda(x_1+x_2)}}\, dx_2 dx_1 =$$

$$= e^{-\lambda t}\left(1+\lambda t + \frac{(\lambda t)^2}{2}\right). \qquad (160)$$

В обоих случаях получен одинаковый результат. Это свидетельствует о том, что при экспоненциальном законе распределения времени безотказной работы основных и соответствующих им запасных частей ВК обе стратегии дают одинаковую вероятность безотказной работы. Однако, учитывая тот факт, что экспоненциальный закон в теории надежности имеет в основном теоретическое значение, поскольку позволяет получать конечные выражения для показателей надежности объектов, и описывает время безотказной работы реальных нерезервированных объектов весьма грубо и только на этапе нормальной эксплуатации, можно сделать вывод о предпочтении *стратегии В.* При этом, чем сильнее закон распределения времени безотказной работы объекта отличается от экспоненциального, тем выгода от применения *стратегии В* больше. Применение *стратегии А* может быть оправдано только для законов близких к экспоненциальному и только на этапе нормальной эксплуатации ВК. Обычное же применение на практике *стратегии А* использования запасных частей ВК обусловлено меньшими затратами для ее реализации обслуживающим персоналом.

4.2. Определение периода использования запасных частей вычислительного комплекса

В п.4.1 была рассмотрена стратегия, когда запасные части и соответствующие им составные части ВК используются в процессе эксплуатации поочередно Там же было показано когда данная стратегия имеет преимущество перед обычной стратегией, при которой запасные части используются по мере отказов составных частей ВК. Однако для практического применения данной стратегии необходимо выбрать длительность интервала периодичности использования запасных и составных частей ВК. Для определения длительности интервала периодичности необходима математическая модель, описывающая поведение ВК во времени с

позиции надежности. Целевая функция модели должна позволять находить, как минимум, обоснованную длительность интервала периодичности.

ВК, укомплектованный запасными частями, с позиции надежности эквивалентен резервированной системе, в которой роль резервного элемента выполняет запасная часть, а роль основного элемента соответственно составная часть ВК. Поскольку запасные части, не включенные в состав ВК в конкретный период ее работы, находятся в выключенном состоянии и не теряют надежности, то ВК можно рассматривать как резервированную систему с ненагруженным резервом [1,2].

Если предположить, что отказы одних частей ВК не влияют на отказы других ее частей, то поведение резервированной системы с позиции надежности для определения интервала периодичности достаточно рассмотреть на примере одного основного и одного резервного элемента. При допущении, что запасная часть является идентичной соответствующей составной части ВК, так как изготавливается по одной и той же технологии, их пару можно представить как систему с ненагруженным резервированием замещением (рис.4.5). При этом и основной и резервный элементы работают поочередно в течение некоторого заданного промежутка времени.

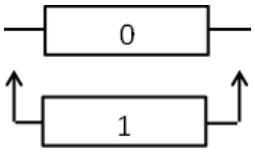


Рис. 4.5. Общее резервирование замещением: 0 – основной элемент, 1 – резервный элемент

Временная диаграмма работы такой системы показана на рис. 4.6.

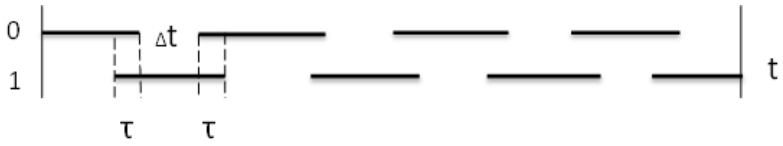


Рис. 4.6. Поочередная работа элементов: Δt – время работы по функциональному назначению, τ – время переключения

Определим вероятность безотказной работы резервированной системы $P_C(t)$ при следующих допущениях:

— основной и резервный элементы равно надежны и имеют вероятность безотказной работы $P(t)$;

— во время нахождения элемента в резерве его надежностный ресурс не расходуется;

— переключение основного элемента на резервный и обратно осуществляется с вероятностью, раной единице;

— $\Delta t >> \tau$ и потому принимаем $\tau = 0$.

Резервированная система проработает безотказно в течение времени t при наступлении одного из трех несовместных событий:

— событие A_1 заключается в том, что основной и резервный элементы проработают безотказно в течение времени t, при этом наработка каждого из них составит $\frac{1}{2}t$;

— событие A_2 заключается в том, что основной элемент откажет в одном из интервалов Δt, а резервный элемент проработает исправно оставшееся время, при условии, что до этого он исправно проработал в предыдущих интервалах;

— событие A_3 заключается в том, что резервный элемент откажет в одном из интервалов Δt, а основной элемент проработает исправно оставшееся время, при условии, что до этого

он исправно проработал в предыдущих интервалах.

Иллюстрация событий показана на рис.4.7.

Вероятность события A_1 в соответствии с принятыми допущениями будет определяться следующим выражением:

$$P(A_1) = P(\frac{t}{2})^2. \quad (161)$$

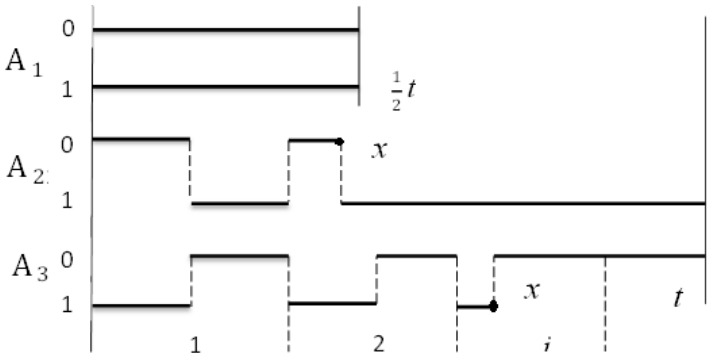


Рис. 4.7. Возможная наработка элементов

Вероятность события A_2 равна вероятности события A_3 и определяется выражением:

$$P(A_2) = P(A_3) = \sum_{i=0}^{\frac{t}{2\Delta t}} \int_0^{\Delta t} f(x + (i-1)\Delta t)\, P(t-(i-1)\Delta t - x \,/\, (i-1)\Delta t + x)\, dx, \quad (162)$$

где условная вероятность $P(t-(i-1)\Delta t - x \,/\, (i-1)\Delta t + x) = \frac{P(t)}{P((i-1)\Delta t + x)}$.

Так как события A_1, A_2 и A_3 независимы друг от друга, то вероятность безотказной работы резервированной системы $P_c(t)$ будет равна сумме вероятностей событий:

$$P_c(t) = P(\frac{t}{2})^2 + 2P(t)\sum_{i=0}^{\frac{t}{2\Delta t}} \int_0^{\Delta t} \frac{f(x+(i-1)\Delta t)}{P((i-1)\Delta t + x)}\, dx \quad (163)$$

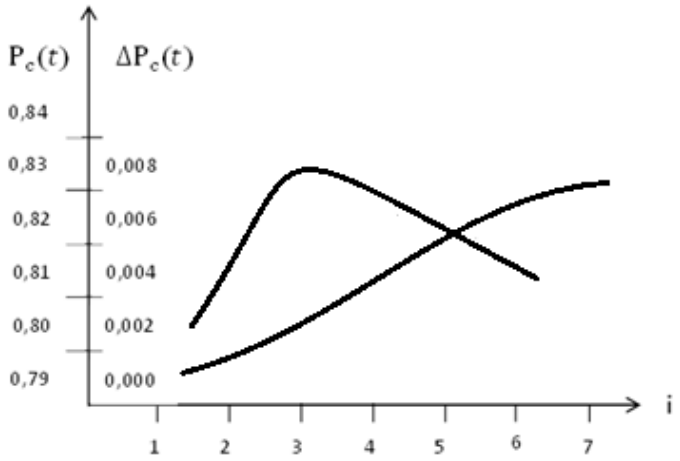


Рис. 4.8. Зависимости вероятности безотказной работы резервированной системы $P_c(t)$ и ее прироста $\Delta P_c(t)$ от числа интервалов i (уменьшения их длительности)

На рис.4.8 приведены зависимости вероятности $P_c(t)$ и ее прироста $\Delta P_c(t)$ от количества интервалов. Из графиков видно, что с ростом числа интервалов или, что одно и то же, с уменьшением длительности интервала, вероятность безотказной работы резервированной системы $P_c(t)$ растет. Однако ее прирост имеет выраженный максимум и с ростом числа интервалов уменьшается, т.е. нет смысла мельчить с длительностью интервалов.

4.3. Оценка надежности бортового вычислительного комплекса с учетом динамики режима функционирования

Бортовой вычислительный комплекс (БВК), относящийся к бортовой радиоэлектронной аппаратуре (БРЭА), является основным управляющим звеном всех систем космического аппарата (КА). От его исправного функционирования в значительной степени зависит эффективное использование КА по своему функциональному назначению в различных условиях. Потому обеспечению требуемой надежности БВК всегда уделяется большое внимание. Под условиями функционирования будем понимать естественные условия космической среды и аномальные условия, характеризующиеся повышенными значениями интенсивностей отказов компонентов БРЭА.

Естественные условия космической среды традиционно учитываются при проектировании БВК, и для оценки его надежности используется большое количество достаточно глубоко проработанных и широко апробированных методов и математических моделей для невосстанавливаемых технических систем [1,2]. В случае аномальных условий космической среды, которые могут возникнуть в результате различных событий деструктивного характера, условия функционирования БРЭА могут резко изменяться, что приведет к существенному росту потока отказов электронных составляющих БВК. В результате следует считать, что БВК КА за время своего существования на орбите может функционировать, по меньшей мере, в двух режимах, характеризующихся различными интенсивностями отказов электронных компонентов БВК. Для оценки надежности такого БВК может быть использован подход, основанный на перерасчете эквивалентного времени функционирования БВК в аномальных условиях космической среды относительно времени работы в естественных условиях.

Вероятность безотказной работы БВК $P_{\text{БВК}}(t)$, за время существования которого на орбите может произойти смена режима функционирования, в общем случае будет равна

$$P_{\text{БВК}}(t) = (1 - P_{\text{су}}(t))\cdot P_{\text{еу}}(t) + P_{\text{су}}(t)\cdot P_{\text{ру}}(t), \qquad (164)$$

где $P_{\text{су}}(t)$ – вероятность того, что за время t существования КА на орбите произойдёт смена режима,

$P_{\text{еу}}(t)$ – вероятность безотказной работы БВК за время t в естественных условиях,

$P_{\text{ру}}(t)$ – вероятность безотказной работы БВК за время t при смене режима функционирования.

Математические модели оценивания вероятности $P_{\text{еу}}(t)$, как отмечено выше, в достаточной степени проработаны, поэтому представляет интерес математическая модель для вычисления вероятности $P_{\text{ру}}(t)$.

Вероятность $P_{\text{ру}}(t)$ будем определять при следующих предположениях:

— за время существования КА на орбите смена режима функционирования БВК обязательно произойдёт;

— время смены режима не зависит от состояний БВК;

— интенсивность отказов БВК при смене режима функционирования изменяется мгновенно, поскольку временем изменения условий функционирования по сравнению со сроком орбитального полета можно пренебречь.

На основании третьего предположения будем считать, что интенсивность отказа БВК в аномальных условиях составляет $\lambda_{ay}(t) = k\lambda_{ey}(t)$, что коррелируется с основными закономерностями работы радиоэлектронной аппаратуры в форсированных режимах [5–7]. Здесь $\lambda_{ey}(t)$ – интенсивность отказа БВК в естественных условиях космической среды, k – повышающий коэффициент ($k > 1$).

Пусть вероятности $P_{py}(t)$ соответствует работа БВК в двух режимах, смена которых происходит в момент времени x (рис. 4.9). Интервалу времени $[0,x]$ соответствует интенсивность отказа БВК $\lambda_{ey}(t)$, а интервалу $[x,t]$ интенсивность $\lambda_{ay}(t)$ (пунктирная кривая на рис. 4.10).

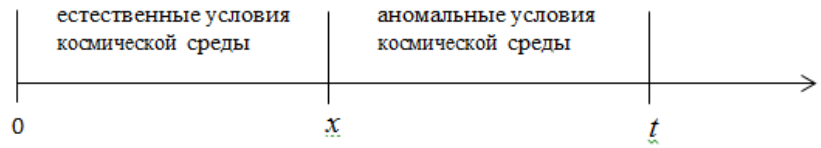


Рис. 4.9. Временная диаграмма работа БВК в двух режимах

Определять вероятность $P_{py}(t)$ будем относительно режима аномальных условий с интенсивностью отказов $\lambda_{ay}(t)$. Для перерасчета эквивалентного времени x работы БВК в режиме естественных условий космической среды с интенсивностью $\lambda_{ey}(t)$ во время $\tau(x)$ работы БВК в режиме аномальных условий космической среды с интенсивностью $\lambda_{ay}(t)$ используем физический принцип надежности Н.М. Седякина [10]. Графическая иллюстрация перерасчета по принципу Н.М. Седякина показана в виде смещения вправо по временной оси точки отсчета и сплошной прямой $\lambda_{ay}(t)$ на рис. 4.10.

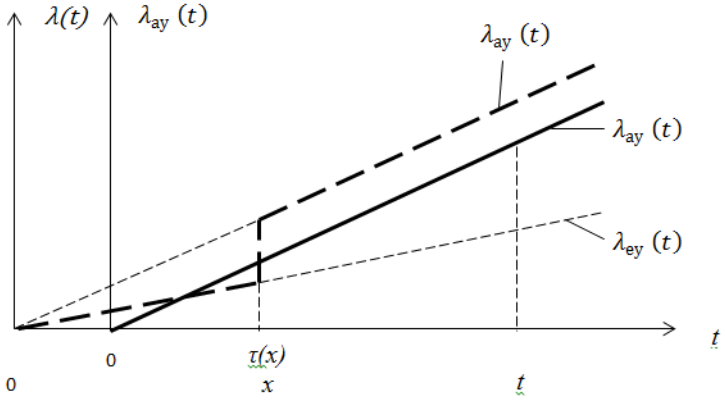


Рис. 4.10. Иллюстрация перерасчета по принципу Н.М. Седякина

Вероятность $P_{py}(t,x)$ безотказной работы БВК за время t при смене условий космической среды в момент времени x согласно рис. 4.10 будет определяться следующим выражением:

$$P_{py}(t,x) = P_{ay}(\tau(x))P_{ay}(t-x|\tau(x)), \qquad (165)$$

где $P_{ay}(\tau(x))$ – вероятность безотказной работы БВК за время $\tau(x)$ в режиме с интенсивностью $\lambda_{ay}(t)$;

$P_{ay}(t-x|\tau(x))$ – условная вероятность безотказной работы БВК в том же режиме за время $t-x$ при условии, что БВК безотказно проработал время $\tau(x)$.

Поскольку условная вероятность $P_{ay}(t-x|\tau(x))$ определяется как

$$P_{\text{ау}}(t-x|\tau(x)) = \frac{P_{\text{ау}}(t-x+\tau(x))}{P_{\text{ау}}(\tau(x))}, \quad (166)$$

то окончательное выражение для $P_{\text{ру}}(t,x)$ примет следующий вид:

$$P_{\text{ру}}(t,x) = P_{\text{ау}}(t-x+\tau(x)). \quad (167)$$

Поскольку момент x смены режима на отрезке времени $[0,t]$ является случайной величиной, то вероятность $P_{\text{ру}}(t)$ можно рассчитать из следующего выражения:

$$P_{\text{ру}}(t) = \int_0^t g(x)P_{\text{ру}}(t,x)\,dx = \int_0^t g(x)P_{\text{ау}}(t-x+\tau(x))\,dx, \quad (168)$$

где $g(x)$ – плотность распределения момента смены режима x на отрезке времени $[0,t]$.

Время $\tau(x)$ согласно принципу Н.М. Седякина будет определяться из интегрального уравнения:

$$\int_0^{\tau(x)} k\lambda_{\text{ey}}(y)dy = \int_0^x \lambda_{\text{ey}}(y)dy. \quad (169)$$

С учетом (168) окончательное выражение для вероятности безотказной работы БВК $P_{\text{БВК}}(t)$ КА, за время существования которого на орбите может произойти смена режима функционирования будет иметь вид:

$$P_{\text{БВК}}(t) = (1-P_{\text{су}}(t))\,P_{\text{ey}}(t) + P_{\text{су}}(t)\int_0^t g(x)P_{\text{ау}}(t-x+\tau(x))\,dx, \quad (170)$$

Повышающий коэффициент k может быть получен из статистических данных о функционировании и испытаниях электронных компонентов в различных условиях, а также с учетом априорной информации по методике, разработка которой может быть предметом отдельного исследования [8−9].

Пусть время безотказной работы БВК за время t в естественных условиях космической среды подчинено экспоненциальному закону распределения, т.е. $P_{\text{ey}}(t) = e^{-\lambda_{\text{ey}}t}$. Данный закон соответствует функционированию нерезервированного БВК на этапе нормальной его эксплуатации и позволяет получить конечные выражения для вероятности его безотказной работы.

Для экспоненциального закона распределения интегральное уравнение (169) примет вид

$$\int_0^{\tau(x)} k\lambda_{\text{ey}}\,dy = \int_0^x \lambda_{\text{ey}}\,dy. \quad (171)$$

Решая данное уравнение относительно $\tau(x)$, получим $\tau(x) = \frac{x}{k}$.

В условиях, когда нет достоверной статистики для определения закона распределения момента смены режима x на заданном отрезке времени, правомерно использовать равномерный закон распределения случайной величины [3]:

$$G(x) = \begin{cases} 1, & x > t \\ \frac{x}{t}, & 0 \le x \le t \\ 0, & x < 0 \end{cases} \quad \text{и} \quad g(x) = \begin{cases} 0, & x > t \\ \frac{1}{t}, & 0 \le x \le t \\ 0, & x < 0. \end{cases}$$

С учётом полученного выражения для $\tau(x)$ и равномерного закона распределения момента x смены режима на интервале времени $[0,t]$ выражение (168) для вероятности $P_{\text{ру}}(t)$ примет вид

$$P_{\text{ру}}(t) = \frac{1}{t}\int_0^t e^{-k\lambda_{\text{ey}}(t-x+\frac{x}{k})}dx = \frac{e^{-\lambda_{\text{ey}}t} - e^{-k\lambda_{\text{ey}}t}}{\lambda_{\text{ey}}\,t(k-1)}. \quad (172)$$

Покажем, что предел $P_{\text{ру}}(t)$ при $t \to 0$ равен 1, а при $t \to \infty$ равен 0, т. е. выражение (172) не противоречит понятию вероятности. Преобразуем его к виду, удобному для анализа:

$$\frac{e^{-\lambda_{\text{ey}} t} - e^{-k\lambda_{\text{ey}} t}}{\lambda_{\text{ey}} t(k-1)} = \frac{e^{-\lambda_{\text{ey}} t}(1-e^{-(k-1)\lambda_{\text{ey}} t})}{\lambda_{\text{ey}} t(k-1)}. \quad (173)$$

Выражение (173) при $t \to 0$ имеет неопределённость типа $\frac{0}{0}$. Согласно правилу Лопиталя подобный предел отношения функций равен пределу их производных. Тогда

$$\lim_{t\to 0} \frac{1-e^{-(k-1)\lambda_{\text{ey}} t}}{\lambda_{\text{ey}} t} = \lim_{t\to 0} \frac{(k-1)\lambda_{\text{ey}} e^{-(k-1)\lambda_{\text{ey}} t}}{\lambda_{\text{ey}}} = k\text{-}1, \quad (174)$$

откуда

$$\lim_{t\to 0} \frac{e^{-\lambda_{\text{ey}} t}(1-e^{-(k-1)\lambda_{\text{ey}} t})}{\lambda_{\text{ey}} t(k-1)} = \lim_{t\to 0} \frac{e^{-\lambda_{\text{ey}} t}(k-1)}{k-1} = 1. \quad (175)$$

Очевидно, $\lim_{t\to\infty} \frac{e^{-\lambda_{\text{ey}} t} - e^{-k\lambda_{\text{ey}} t}}{\lambda_{\text{ey}} t(k-1)} = 0$.

Покажем также, что $\lim_{k\to 1} \frac{e^{-\lambda_{\text{ey}} t}(1-e^{-(k-1)\lambda_{\text{ey}} t})}{\lambda_{\text{ey}} t(k-1)} = e^{-\lambda_{\text{ey}} t}$. Это означает, что смена режима не меняет интенсивность отказов. Ясно, что при $k \to 1$ дробь $\frac{1-e^{-(k-1)\lambda_{\text{ey}} t}}{k-1}$ представляет неопределённость типа $\frac{0}{0}$. Для нахождения этого предела также используем правило Лопиталя:

$$\lim_{k\to 1} \frac{1-e^{-(k-1)\lambda_{\text{ey}} t}}{k-1} = \lim_{k\to 1} \frac{\lambda_{\text{ey}} t e^{-(k-1)\lambda_{\text{ey}} t}}{1} = \lambda_{\text{ey}} t, \quad (176)$$

откуда

$$\lim_{k\to 1} \frac{e^{-\lambda_{\text{ey}} t}(1-e^{-(k-1)\lambda_{\text{ey}} t})}{\lambda_{\text{ey}} t(k-1)} = \lim_{k\to 1} \frac{e^{-\lambda_{\text{ey}} t}\lambda_{\text{ey}} t}{\lambda_{\text{ey}} t} = e^{-\lambda_{\text{ey}} t}. \quad (177)$$

Для определения вероятности безотказной работы БВК $P_{\text{БВК}}(t)$ по формуле (164) необходимо знать вероятность $P_{\text{су}}(t)$, которую на практике получить затруднительно. В этом случае оценим верхнюю и нижнюю границы $P_{\text{БВК}}(t)$. Верхнюю границу $P_{\text{БВК}}(t)$ будет составлять $P_{\text{ey}}(t) = e^{-\lambda_{\text{ey}} t}$, а нижнюю $P_{\text{ру}}(t) = \frac{e^{-\lambda_{\text{ey}} t} - e^{-k\lambda_{\text{ey}} t}}{\lambda_{\text{ey}} t(k-1)}$. На рис. 4.11 приведены зависимости вероятности безотказной работы БВК $P_{\text{БВК}}(t)$ от времени функционирования в естественных условиях ($k = 1$) и в аномальных условиях при $k = 1{,}5$ и $k = 2$.

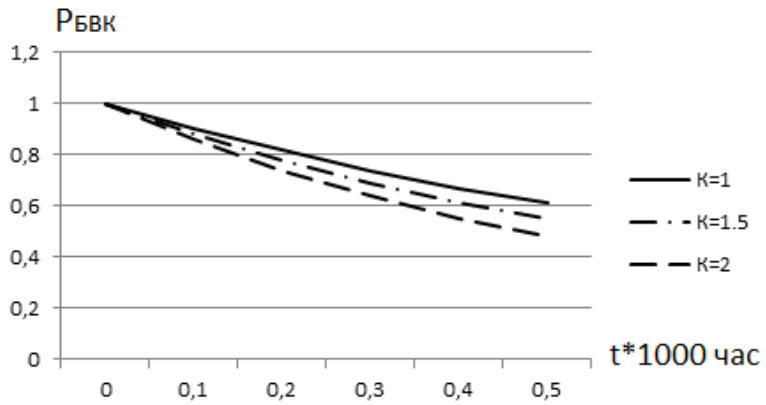


Рис. 4.11. Зависимости $P_{БВК}$ от времени функционирования

Для определения законов распределения отказов БРЭА и их параметров следует использовать результаты исследования влияния космического пространства на показатели надежности радиоэлектронных элементов, изложенные как в руководящих документах и справочной литературе, так и в научных публикациях.

Список используемых источников

1. Долгин В. П., Харченко А. О. Надежность технических систем: учебное пособие/ В.П Долгин., А.О Харченко. - М.: Вузовский учебник, НИЦ ИНФРА–М, 2015. - 167 с.
2. Половко А. М., Гуров С. В. Основы теории надежности. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2006. – 704 с.: ил.
3. Вентцель Е.С. Теория вероятностей: Учеб. для вузов. –5-е изд. –М.: Высш. Шк., 1998. –576 с.: ил.
4. ГОСТ 2.601-2013. Единая система конструкторской документации (ЕСКД). Эксплуатационные документы.
5. ГОСТ Р 27.607-2013. Надежность в технике. Управление надежностью. Условия проведения испытаний на безотказность и статистические критерии и методы оценки их результатов.
6. РД 50-424-83. Методические указания. Надежность в технике. Ускоренные испытания. Основные положения.
7. Майоров А.В., Потюков Н.П. Планирование и проведение ускоренных испытаний на надежность устройств электронной автоматики. –М.: Радио и связь, 1982.
8. Радиационные эффекты в космосе. Часть 3. Влияние ионизирующего излучения на изделия электронной техники / И. П. Безродных, А. П. Тютнев, В. Т. Семёнов. – М.: АО «Корпорация «ВНИИЭМ», 2017. – 64 с.
9. Вологдин Э.Н., Лысенко А.П. Радиационные эффекты в интегральных микросхемах и методы испытаний изделий полупроводниковой электроники на радиационную стойкость. – М.: НОЦ МГИЭМ, 2002. – 46 с.
10. Седякин Н.М. Об одном физическом принципе теории надёжности // СССР. Техническая кибернетика. – 1966. – №3. С.80–87.
11. ГОСТ 34.003-90 «Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».- 1992.
12. РД 50-680-88 "Методические указания. Автоматизированные системы. Основные положения". - М.: -1990.