ГЛАВА 1

ПОНЯТИЕ НАДЕЖНОСТИ И ПУТИ ЕЕ ОБЕСПЕЧЕНИЯ

Надежность по отношению к техническим объектам и в соответствии со Стандартом (см. ниже) определяется как «свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технологического обслуживания, ремонтов, хранения и транспортировки».

Стиль и качество формулировки, возможно, обусловлены желанием в одном предложении отметить, что надежность – обобщенное свойство, которое в зависимости от назначения объекта и условий его применения является сочетанием частных свойств: безотказности, долговечности, ремонтопригодности и сохраняемости (перечень свойств также заимствован из соответствующего Стандарта). Определение этих свойств сводится к следующему:

безотказность – непрерывное сохранение работоспособности в течение некоторого времени или некоторой наработки;

долговечность – сохранение работоспособности до наступления предельного состояния при установленной системе технического обслуживания и ремонтов.

сохраняемость – непрерывное сохранение исправного и работоспособного состояния во время хранения и транспортировки.

ремонтопригодность – приспособленность к предупреждению и обнаружению причин возникновения отказов, повреждений и устранению их последствий путем проведения ремонтов и технического обслуживания.

При этом под *исправным* понимают состояние, при котором изделие соответствует всем требованиям, установленным технической документацией.

Работоспособность (работоспособное состояние) – это состояние, при котором изделие способно выполнять заданные функции, сохраняя значения параметров в пределах, установленных технической документацией (при имеющемся в практических случаях отождествлении этих понятий необходимо исходить из того, что понятие исправности шире понятия работоспособности).

Наработка – объем работы, выполненной объектом (чаще всего выражается временем, затраченным на ее выполнение.

Отказ – событие, заключающееся в нарушении работоспособности объекта, т.е. переходе в неисправное или неработоспособное состояние.

В свою очередь, отказы могут быть устойчивыми и перемежающимися (перемежающийся отказ называют сбоем). *Сбой* можно определить как кратковременное нарушение работоспособности объекта, которая самовосстанавливается или восстанавливается оператором без проведения ремонта. Кроме того, отказы условно делят на внезапные и постепенные. Внезапные отказы появляются в результате резкого (скачкообразного) изменения основных параметров системы или ее элемента. Отказы постепенные проявляются

в результате медленного изменения параметров системы и их выхода из области допустимых значений. Поскольку отказы в общем случае являются случайными событиями, то они могут быть зависимыми и независимыми.

В СССР существовала система государственных стандартов «Надежность в технике» (ССНТ), описываемая ГОСТ 27.001—81.

Стандарты ССНТ были разделены по группам, обозначаемым цифрой пос-ле точки в номере стандарта: 0 – общие вопросы надежности; 1 – нормирование надежности; 2 – методы расчета надежности; 3 – ме-тоды обеспечения надежности; 4 – испытания и контроль надежно-сти; 5 – сбор и обработка информации о надежности.

В таблице 1.1 приведены важнейшие с точки зрения обеспечения надежности СВТ стандарты, на которые, к сожалению, приходится ссылаться до сих пор, поскольку соответствующие отечественные стандарты пока не разработаны.

Таблица 1.1

Стандарты, нормирующие обеспечение надежности СВТ

Гост ССНТ	Наименование
27.002-83	Термины и определения
27.003-83	Выбор и нормирование показателей надежно-сти. Основные положения.
27.103-83	Критерии отказов и предельных состояний. Ос-новные положения
27.104-84	Признаки классификации отказов и предельных состояний. Общие положения
27.201-81	Оценка показателей надежности при малом чис-ле наблюдений с использованием дополнительной информации. Общие положения
27.301-83	Прогнозирование надежности изделий при про-ектировании. Общие требования
27.410-83	Методы и планы статистического контроля по-казателей надежности по альтернативному приз-наку
27.502-83	Надежность в технике. Система сбора и обра-ботки информации. Планирование наблюдений
ГОСТ	Наименование
23564-79	Техническая диагностика. Показатели диагностирования
19542-83	Совместимость вычислительных машин электромагнитная. Термины и определения.
16325-76	Машины вычислительные электронные цифровые общего назначения. Общие технические требования.

Кроме стандартов ССНТ интерес представляют также стандар-ты, перечисленные во второй части таблицы. В них определено более ста терминов, относящихся к рассматриваемой об-ласти, и смежных вопросов вместе с соответствующими английскими и французскими терминами. Там же приведены некоторые ос-новные теоретические зависимости, рекомендуемые расчетные форму-лы, методы расчета, оценки и испытания на надежность. Перечисленные Стандарты служат основой планирования и обеспечении надежности средств вычислительной техники.

Как следует из приведенных выше определений, в теории надежности принято различать исправное (работоспособное) и неисправное состояния технической системы (ТС), которые определяют ее статус. Траектория статуса системы в пространстве времени-состояний, собственно, и составляет предмет исследований теории надежности.

Надежность ТС, в первую очередь, характеризуется отрезком времени, в течение которого система находится в исправном состоянии (интервал времени на. рис.1.1). Этот интервал позволяет определить свойство безотказности. Переход из исправного состояния в неисправное является событием отказа, которое характеризуется моментом времени его наступления. Аналогичным образом можно определить отрезок времени, необходимый для устранения отказа, и событие восстановления исправного состояния системы, которые ассоциируются с интервалом и моментом времени соответственно. Свойство системы, обеспечивающее возможность восстановления ее работоспособности после отказа, обычно называют *восстанавливаемостью*, а сами системы восстанавливаемыми.

Рис.1.1.

Для таких систем восстановление исправного или, по крайней мере, работоспособного состояния считается целесообразным и может быть произведено обслуживающим персоналом в ограниченный срок. Это означает, что интервал имеет конечную величину, а процесс нормального функционирования возобновляется начиная с момента времени . Можно говорить о том, что траектория восстанавливаемой системы определяется потоками событий отказов и восстановлений.

Если восстановление объекта после отказа либо невозможно, например для бортовых систем, либо нецелесообразно, то можно полагать, что . При анализе надежности такой системы процесс восстановления не учитывают.

Для характеристики свойства надежности крайне трудно (прак-тически невозможно) не только определить детерминированную зависимость между вызывающими отказ факторами и временем его возникновения, но и конкретизировать само множество таких факторов. Это дает основание полагать, что события отказов и восстановлений в общем случае носят случайный характер, и объясняет правомерность применения аппарата теории вероятности и математической статистики для формулировки соответствующей математической модели.

Основой такой модели в теории надежности является функция надежности, которая по определению равна вероятности того, что в заданном интервале времени или в пределах заданной наработки при заданных режимах и условиях эксплуатации отказов в системе не возникает, т.е.

где – время безотказной работы системы, – заданное время, – вероятность события (в данном случае событие состоит в том, что).

По аналогии с функцией надежности определяется функция ненадежности:

.

Непосредственно из определения этих функций следует, что

,

, ,

, , при . (1.1)

Кроме того предполагается, что система исправна в начальный момент времени, т.е.

, , (1.2)

и время ее исправной работы является конечной величиной, т.е.

, . (1.3)

Функция монотонно возрастает, в силу выполнения условия (1.1), и ограничена в интервале (для нее выполняются условия (1.2) и (1.3)), т.е. она является функцией распределения случайной величины – времени до отказа системы. Поскольку время безотказной работы определяется как интервал , то является также *функцией распределения времени безотказной работы*.

В теории надежности считают, что функция является непрерывной, т.е. существует ее производная:

, (1.4)

которую называют *плотностью распределения времени безотказной работы*.

Часто в качестве функционального показателя надежности рассматривают *интенсивность отказов*, определяемую как условную плотность распределения вероятности времени до

отказа при условии, что до момента времени отказа не было.

Таким образом, вероятность того, что первый отказ произойдет в интервале времени ,

, или

. (1.5)

Для того, чтобы выразить как функцию интенсивности отказов, необходимо преобразовать (1.5) к виду

(1.6)

и решить дифференциальное уравнение (1.6) относительно .

Решением (1.6) является

,

но т.к. для функции надежности должно выполняться условие (1.3), выражение для приобретает окончательный вид:

. (1.7)

Зависимость (1.7) принято называть *основным законом надежности*.

Интенсивность отказа часто используется в качестве расчетного показателя, особенно для систем, состоящих из многих элементов, поскольку обладает свойством аддитивности, проиллюстрировать которое можно следующим примером.

Пусть система состоит из двух элементов, интенсивности отказов которых равны соответственно и . При этом предполагается, что отказы элементов являются независимыми событиями, а отказ системы в целом наступает при отказе хотя бы одного из них.

При выполнении этих условий функция надежности системы имеет вид:

,

где , , – время безотказной работы первого (второго) элемента.

Из независимости случайных величин и следует, что

. (1.8)

Если , где – интенсивность отказа системы в целом, а () – функция надежности первого (второго) элемента, то выражение (1.8) принимает вид:

.

В общем случае, если система состоит из элементов, для которых выполняется условие независимости отказов, и для системы в целом отказ определяется в том случае, когда откажет хотя бы один из элементов, имеет место соотношение:

.

Кроме перечисленных функциональных характеристик надежности на практике широко используются и числовые показатели.

Важнейшим из них является *наработка до отказа* , которая определяется как ма-тематическое ожидание времени до отказа:

(1.9)

Окончательный вид выражения для получен исходя из того, что равно нулю при , а для встречающихся на практике функций имеет место равенство .

Средняя наработка на отказ является естественным показателем надежности, однако она не характеризует распределение времени до отказа.

Наряду с показателем применяется показатель – *среднеквадратическое отклонение наработки до отказа* или *дисперсия* :

Дисперсия характеризует величину разброса наработ-ки относительно среднего значения.

Описанная вероятностная модель надежности является обобщенной, т.к. любая непрерывная функция, для которой выполнены условия (1.1) – (1.3), может рассматриваться как функция распределения безотказной работы, не отражая при этом реальный процесс функционирования системы. В связи с этим необходима ее дальнейшая конкретизация, связанная с выбором функций, описывающих траекторию статуса системы с подробностью и точностью, соответствующей целям исследования.

Наиболее распространенной вероятностной моделью надежности является *экспоненциальная модель* распреде-ления времени до отказа, по которой вероятность безот-казной работы объекта выражается зависимостью

.

Функция плотности вероятностей распределения вре-мени до отказа при экспоненциальной модели определяется как

.

Функция интенсивности отказов при экспоненциальной модели:

.

Распространенность этой модели объясняется простотой и удобством при расчетах.

Экспоненциальная функция надежности обладает важным свойством, рассматриваемым ниже.

Пусть необходимо определить– надежность системы на интервале времени , если известно, что система работала безотказно до момента .

События и при являются независимыми. Следовательно,

, (1.10)

где – искомая вероятность.

С другой стороны

,т.е.

. (1.11)

Выражения (1.10) и (1.11) позволяют окончательно получить

.

Для экспоненциальной модели (): .

С другой стороны можно показать, что если надежность системы не зависит от того, сколько она уже проработала безотказно, то функция надежности такой системы будет обязательно экспоненциальной, т.е. она является единственной, имеющей указанное свойство.

Таким образом, экспоненциальный закон распределения не учитывает предыстории процесса функционирования, т.е. адекватно описывает надежность только тех систем, которые не подвержены износу в процессе эксплуатации и старению во времени, что не соответствует действительности. Поэтому на практике экспоненциальное распределение применяют в тех случаях, когда процессы старения и износа в системах протекают достаточно медленно и при этом анализируется сравнительно небольшой период "жизни" изделия.

Экспоненциальная модель может быть использована в случае, когда интенсивность отказов есть постоянная величи-на, а также как характери-стика достаточно сложных восстанавливаемых объектов, предполагая, что отдельные части объекта, на-ходясь в разных стадиях износа, характеризуются в среднем постоянной функцией интенсивности потока отказов, т.е. время приработки и интен-сивного старения из рассмотрения в периоде эксплуатации исключается

С экспоненциальной моделью тесно связана *модель Пуассона*, позволяющая выразить вероятность того, что на заданном интервале времени произо-шло ровно событий (отказов), если время между от-дельными событиями (отказами) распределено экспо-ненциально с интенсивностью .

По модели Пуассона

. (1.12)

Эта модель основана на представлении о потоке случайных событий, называемого пуассоновским, для которого выполнены условия стационарности, ординарности и отсутствия последействия.

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

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

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

Эта модель находит свое применение, например, при анализе надежности резервированных систем с ненагруженным резервом [42]. При этом предполагается, что время безотказной работы такой системы, включающей основную подсистему и резервных, определяется как сумма интервалов времени от включения до отказа основного и резервных элементов, т.е.

,

где – время безотказной системы в целом, – время безотказной работы i-ой подсистемы.

Анализ надежности усложняется в том случае, если – случайные величины и необходимо найти функцию надежности системы, т.е. решить задачу нахождения композиции функций надежности ее резервированных элементов. Если предположить,

что надежность этих элементов описывается экспоненциальной моделью, то вероятность того, что за время произойдет отказов можно вычислить по формуле (1.12). Вероятность безотказной работы системы, содержащей резервированных подсистем, определяется как сумма вероятностей событий, состоящих в том, что в системе произошло 0, 1,..., отказ за время , в то время как появление n-ого отказа означает уже отказ системы в целом:

.

Разреженный поток – поток событий, где каждое событие осуществляется с вероятностью ; тем самым количество событий уменьшается и поток делается более «редким». Доказано, что разреженный пуассоновский поток является тоже пуассоновским с параметром, т.е. время между событиями последнего потока распределено по экспоненциальному закону.

Модель Вейбулла находит широкое практическое применение благодаря своей простоте и гибкости, так как в зависимости от значений параметров характер модели видоизменяется в широких пределах. Вероятность безотказной работы по модели надежности Вейбулла выражается формулой [30]

,

где и – параметры модели.

Ориентировочно значение для электронных устройств с убывающей функцией интенсивности отказов.

Выбор модели надежности - сложная научно-техни-ческая проблема. Она может быть удовлетворительно решена стандартными методами математической стати-стики, если имеется большой статистический материал об отказах исследуемых объектов. Высокая надежно-сть вычислительных систем и их компонентов обусловливает скудность таких статистических данных. По этой причине при вы-боре модели

руководствуются, в основном, результатами ускоренных испытаний, проводимых в утяжеленных условиях рабо-ты объекта.

В случае приближенных оценок часто выбира-ется экспоненциальная модель как наиболее удобная с точки зрения аналитических преобразований. Ее рекомендуется применять при выпол-нении расчетов надежности в случае отсутствия других исходных данных для расчета, кроме интенсивности от-казов. Если имеются более полные данные, то целесообразно использовать более точную мо-дель, например, модель Вейбулла.

В практической деятельности описанные модели надежности используются для получения численных оценок, которые называют показателями надежности.

Показатели надежности

Как уже упоминалось, при исследовании свойств надежности изделий они могут рассматриваться как невосстанавливаемые и восстанавливаемые объекты. При этом для невосстанавливаемых объектов, согласно рис.1.1, рассматривается только период их функционирования до возникновения первого отказа, следовательно, все показатели надежности для этих систем являются численными оценками длительности этого интервала времени. Для восстанавливаемых систем, в противоположность невосстанавливаемым, для того, чтобы оценить их надежность, необходимо рассматривать траекторию статуса системы на протяжении всего срока «жизни» изделия или на заранее заданном интервале времени. Таким образом, для восстанавливаемых и невосстанавливаемых

объектов используют различные показатели надежности.

Показатели надежности невосстанавливаемых объек-тов

Вероятность безотказной работы выражает вероятность того, что невосстанавливаемый объект не откажет к моменту времени наработки (нара-ботка может быть выражена как календарное время, как время работы, а также как число циклов работы (меха-нических узлов) или в виде другой меры проделанной объектом работы).

Вероятность отказа – вероятность того, что случайное время до отказа меньше заданного времени .

Если задан вид функций или (например, они соответствуют экспоненциальной модели надежности), то вычисление этих параметров может непосредственно проводиться по формуле (1.7), в которой используется заданное время .

В технических условиях обычно задают отдельные ординаты (одну или две) этих функций при значениях , выбираемых из нормированного ряда (ч,) который обычно оговаривается Стандартом.

Наработка на отказ для невосстанавливаемых объектов определяется как ма-тематическое ожидание времени до отказа и вычисляется согласно формулы (1.9).

Среднеквадратическое отклонение наработки до отказа и *дис-персия* характеризуют величину разброса наработ-ки относительно среднего значения и могут быть вычислены по формуле (1.10).

Интенсивность отказов выражает интенсивность процессов возникновения отказов. Задавать этот параметр имеет смысл в случае постоянства во времени этой характеристики, т.е. при

использовании экспоненциальной модели надежности.

Важной характеристикой надежности является *гарантированный технический ресурс* – технический ресурс, которым обладает не менее чем эксплуатируемых изделий (– гарантированная вероятность, а понятия технического ресурса и наработки на отказ для невосстанавливаемых систем совпадают). Этот параметр может быть вычислен исходя из выполнения условия:

. (1.13)

В случае использования экспоненциальной модели (1.13) можно записать в виде:

.

Т.к. значение близко к единице, то имеет место соотношение , используя которое окончательно можно получить выражение:

.

Показатели надежности восстанавливаемых объектов

Как уже упоминалось, при характеристике надежности восстанавливаемых технических систем определяющей является их траектория в пространстве исправного и неисправного состояний. В этом случае меняется смысл понятия наработки на отказ. Теперь этот и другие параметры должны усредняться по “всей траектории” с учетом возможной смены состояний. Кроме того, естественный интерес вызывает ответ на вопрос о наиболее вероятном состоянии системы в некоторый определенный момент времени. В связи с этим, для определения надежности восстанавливаемых систем используются следующие показатели.

Параметр потока отказов выражает удельное число отказов в единицу времени (на один образец ап-паратуры).

Средняя наработка на отказ определяется как от-ношение наработки восстанавливаемого объекта к мате-матическому ожиданию числа его отказов в течение этой наработки.

При определении этих показателей использованы только параметры потока отказов системы, в то время, как параметры процесса восстановления не учитываются. Если длительностью процесса восстановления нельзя пренебречь, то необходимы показатели, численно оценивающие его длительность.

Показатели надежности, определяющие вероятность безотказной работы, среднюю наработку на отказ и интенсивность потока отказов могут использоваться также как показатели характеризующие процесс восстановления, если вместо момента времени возникновения отказа рассматривать момент времени восстановления работоспособного состояния эксплуатируемого объекта.

Важным параметром надежности, характеризующим время пребывания изделия в работоспособном состоянии, является *коэффициент готовности ,* который опреде-ляется как вероятность того, что в произвольный задан-ный момент времени объект находится в состоянии ра-ботоспособности (кроме планируемых периодов, в тече-ние которых применение объекта по назначению не пре-дусматривается).

Коэффициент готовности вычислительной системы (ВС), сети или их компонент с учетом интенсивностей потоков отказов и восстановления может быть определен следующим образом.

Пусть длительность интервалов времени между моментами возникновения отказов есть случайная величина, распределенная по экспоненциальному закону с параметром , а длительность восстановления – экспоненциально

распределенная случайная величина с параметром . При этом предполагается, что устранение отказа начинается сразу после его наступления, т.е. время поиска неисправности включено во время ремонта.

Таким образом, в процессе эксплуатации объект может находиться в одном из двух состояний – исправном и состоянии отказа, обозначаемым соответственно и .

Пусть также вероятности нахождения ВС в состояниях и обозначены как и и в момент времени имеет место, .

Для определения зависимостей , необходимо вычислить вероятность того, что ВС будет находиться в состоянииив момент времени , где – малый интервал времени.

Тогда, если в момент времени ВС находилась в состоянии , то она останется в этом состоянии в момент с вероятностью . Если же в момент времени ТС находилась в состоянии , то за интервалона перейдет в состояние с вероятностью . Таким образом, можно записать

(1.14).

С учетом того, что при малых имеет место , выражение (1.14) можно представить в виде:

или, после преобразований,

. (1.15)

При можно записать дифференциальное уравнение

,

которое можно преобразовать к виду

, (1.16)

если учесть то, что .

Уравнение (1.16) описывает процесс эксплуатации ТС, на функционирование которой оказывают влияние потоки отказов и восстановлений. Аналитическое решение (1.16) имеет вид:

(1.17)

Вероятность определяет вероятность работоспособного состояния ТС в момент времени , т.е. эквивалентна коэффициенту готовности.

Для определения стационарного коэффициента готовности необходимо вычислить .

Таким образом, стационарный коэффициент готовности будет определяться выражением:

(1.17).

Выражение (1.17) справедливо в том случае, если все отказы, возникающие в объекте обнаруживаются.

В действительности вероятность обнаружения отказа не может быть равна нулю, что связано с ограничением затрат (как временных, так и аппаратных) на проведение контроля технического состояния объекта в процессе функционирования или, вообще, отсутствием такого контроля (применительно к СВТ это приводит к ухудшению достоверности результатов вычислений). Следствием этого является увеличение времени восстановления системы, поскольку на протяжении времени от момента возникновения отказа до момента его обнаружения она функционировала в неработоспособном состоянии, и эта наработка должна быть выполнена заново после восстановления. К аналогичным последствиям приводит также низкая (с вероятностью не равной единице) достоверность локализации неисправности средствами технической диагностики в процессе восстановления системы.

Рис.1.2

При формализации модели процесса эксплуатации СВТ с частичным контролем можно, как и в предыдущем случае, предположить что потоки отказов и восстановления соответствуют экспоненциальной модели. В этом случае процесс эксплуатации рассматривается как марковский процесс.

На рис.1.2 приведен граф состояний объекта с частичным контролем.

В дальнейшем предполагается, что в охваченном контролем оборудовании возникающие отказы обнаруживаются сразу после их возникновения и начинается процесс восстановления работоспособного состояния.

Если в объекте возникает необнаруживаемый средствами контроля отказ, то он переходит в неработоспособное состояние. В этом случае ремонт может начаться только после возникновения в объекте еще одного, обнаруживаемого отказа.

В силу предположения о экспоненциальных распределениях времени нахождения объекта во всех состояниях, приведенных на рис.1.2, можно записать систему уравнений Колмогорова для стационарных вероятностей:

(1.18)

Решение системы (1.18) имеет вид:

(1.19)

Выражение для определяет стационарный коэффициент готовности объекта с полнотой контроля , – вероятность нахождения объекта в ремонте, а – вероятность его недостоверного функционирования.

Значения численных показателей как для восстанавливаемых, так и для невосстанавливаемых систем, описанные выше, носят приближенный характер (причиной этого является несоответствие применяемых моделей и надежности реальных изделий) и могут быть уточнены, если имеется статистический материал о процессе функционирования либо таких систем, например, полученный в результате натурного эксперимента над опытными образцами, либо подобных анализируемому устройству, например, изделий, состоящих из тех же элементов и содержащих те же структурные решения. В этом случае для уточнения показателей надежности используется аппарат математической статистики.

Формулы для вычисления основных показателей надежности с использованием аппаратов теории вероятности и математической статистики сведены в таблицу 1.2.

Таблица 1.2.

Подход / Показатель надежности	Вероятностный	Статистический
Основной закон надежности		
Вероятность безотказной работы		
Интенсивность отказов		

Средняя наработка на отказ		
Интенсивность восстановления		
Коэффициент готовности		

– вероятность отказа; – момент времени отказа; – текущее время; – общее число образцов; – число образцов, отказавших к моменту t; – число образцов, восстановленных к моменту t; – функция плотности вероятности времени безотказной работы; – функция распределения вероятности времени восстановления; – интенсивность отказов; – интенсивность восстановления; – суммарное время нормального функционирования; – суммарное время восстановления после отказа.

Выбор показателей надежности

В каждом конкрет-ном случае в качестве показателя надеж-ности необходимо выбирать тот, который наилучшим обра-зом характеризуют надежность объекта с точки зрения его целевого назначения. В соответствии с существующими методи-ками краткие рекомендации по такому выбору сводятся к следующему.

Если невосстанавливаемый объект работает одно-кратно в течение небольшого заданного отрезка времени , то в качестве показателя надежности целесооб-разно выбрать вероятность безотказной работы за заданное время. Этот же показатель используется в случае периодиче-ски обслуживаемых ТС и их подсистем, например бортовых.

Если отказ невосстанавливаемого объекта не влечет за собой опасных последствий и объект эксплуатируется, как правило, до наступления отказа, тогда целесообраз-но характеризовать его надежность средней нара-боткой до отказа .

Если невосстанавливаемый объект характеризуется постоянством интенсивности отказов, тогда в качестве показателя надежности целесообразно использовать значение . Применительно к СВТ этот показатель используется для характеристики невос-станавливаемых электронных узлов (ИС и БИС).

Если время восстановления объекта пренебрежимо мало по сравнению со временем безотказной работы, целесообразно использовать показа-тели надежности или , если . Эти же показатели используются в том случае, когда факт отказа влечет за собой тяжелые последствия, не взирая на малое время восстановления.

Если доля полезного времени работы по отношению ко времени восстановления технической системы имеет существенное значение, в качестве показателя надежности целесообразно использовать коэффициент готовности .

Обеспечение надежности технических систем

Описанные параметры могут использоваться исключительно для прогнозирования надежности технической системы. Однако, кроме задачи качественного анализа и количественной оценки

этого свойства существует другая (основная) задача, связанная с *обеспечением* требуемых значений показателей надежности. Применительно к такой задаче следствием анализа модели надежности могут быть только вполне очевидные выводы:
система должна строиться из достаточно надежных элементов, количество которых, по возможности, минимально;
для восстанавливаемых систем необходимо обеспечивать минимизацию времени восстановления (см. [46]).

Если с учетом этих мер требуемые показатели надежности не достигаются, то единственно возможным путем является построение «надежных» систем из «ненадежных» элементов, например, с помощью резервирования [39, 72].

При этом важно отметить, что в общем случае надежность, как и любое другое свойство системы, закладывается на стадии проектирования, реализуется в процессе производства и поддерживается в процессе эксплуатации. Кроме того, меры по обеспечению надежности на каждой из перечисленных стадиях, в основном, не являются прямым следствием описанной выше модели.

Так, на *стадии проектирования* одной из первых решается достаточно сложная технико-экономическая задача формулировки требований к надежности и результаты ее решения могут оказать существенное влияние на затраты, связанные с самим процессом проектирования, а также процессом производства и периодом эксплуатации технического изделия (на период утилизации надежностные характеристики практически не влияют).

Например, время наработки на отказ для бортового вычислителя самолета может быть установлено существенно меньшим, чем аналогичный показатель для деталей шасси, поскольку верификация и (при необходимости) восстановление его исправного технического состояния в предполетный период обходятся дешевле. В качестве другого примера можно рассмотреть случай, когда отказ изделия влечет за собой опасность для жизни людей, крупную аварию и т.п. Тогда вероятность отказа должна соответствовать практически невозможному событию

При определении требований к надежности с учетом критерия минимума суммарных затрат необходимо учитывать расходы, связанные:

- с разработкой и реализацией дополнительных средств, обеспечивающих требуемые характеристики надежности, в том числе и дополнительной аппаратуры для проведения контрольно-диагностических мероприятий (см. ниже);
- с оплатой персонала, занятого ремонтом и техническим обслуживанием;
- с устранением (если такое возможно) последствий отказов и простоев;
- с снижением эффективности или производительности системы в связи с применением дополнительных средств;
- с возможным увеличением массы или габаритов системы и др.

К сожалению, модель надежности для решения этой задачи во многих случаях мало конструктивна, поскольку может применяться только при наличии статистических данных, собранных в процессе эксплуатации или испытаний аналогичных или близких по характеристикам систем. Однако также данные могут либо отсутствовать, либо быть недостаточно достоверными.

В дальнейшем, применительно к СВТ, на *системном, операционном, функционально-логическом и техническом* уровнях проектирования (см. главу 4) определяются особенности архитектуры и структурной организации разрабатываемой системы, вы-бирается элементная база и вариант технической реализации системы в целом. Здесь также можно отметить, что конструктивизм модели надежности позволяет оценить соответствующие показатели только после технического проектирования, когда известен полный перечень элементов и способы их соединения. На более ранних уровнях оценить в терминах модели надежность таких структурных компонент, как операционный или управляющий автомат, не представляется возможным. В то же время, необходимость этой оценки очевидна. На ее основе могут быть определены наименее надежные под-системы и приниматься решения о резер-вировании отдельных подсистем, способах и организации технического обслуживания, а также решения о целесообразности и способах реализа-ции методов автоматического восстановления и обеспечения отказо-устойчивости в системе. Ошибка в принятии подобных решений может привести к возврату на предыдущий уровень, вплоть до корректировки технического задания на разработку в целом.

В процессе проектирования эта задача все же решается с помощью формулировки априорных требований к надежности отдельных подсистем (пример с бортовым вычислителем, который может рассматриваться как подсистема по отношению к самолету). Прием используется в связи с отсутствием других, но не исключает возможности ошибок в принятии решения и, кроме того, может повлечь за собой существенное усложнение проектных работ.

При этом особенно важной с точки зрения обеспечения надежности на стадии проектирования можно считать задачу *верификации* проектных решений, которая обусловлена не только необходимостью устранения так называемых тривиальных ошибок в процессе применения проектной методики. Эти ошибки так или иначе будут устранены и поэтому на характеристику надежности, в общем случае, не влияют. Верифицировать принятое решение необходимо на отсутствие семантических (смысловых) ошибок, вызванных несовершенством методик проектирования. Применительно к СВТ последнее выражается в идеализации динамики распространения информационных сигналов (модели не учитывают реальных динамических характеристик цепей передачи информации и конечной длительности переходных процессов при смене состояния элементов, и, как следствие, возможность появления динамических отказов или ошибок, связанных с нарушением синхронизации, возникновением ложных сигналов или помех, их амплитудной и временной фильтрацией и т.п.).

Верификация проектных решений на отсутствие таких ошибок, как правило, осуществляется с помощью различного типа систем имитационного моделирования. На системном уровне это имитация моделей сетей Петри или СМО, на операционном – имитация процессов управления регистровыми передачами и самих регистровых передач, а также системы логического моделирования на функционально-логическом уровне. Принципы построения и реализации таких систем

достаточно широко описаны в литературе, например, в [51, 64, 67], представляют собой самостоятельную предметную область и далее не рассматриваются.

Не менее важной задачей в рамках обеспечения надежности представляется задача проектирования так называемых *контролепригодных* (иначе – *тестопригодных*) объектов, в частности СВТ. Формально свойство контролепригодности СВТ определено в последнем разделе книги, а его неформальный смысл поясняется несколькими абзацами ниже.

Предусмотренные на стадии проектирования надежностные характеристики технической системы реализуется на стадии *производства* при выполнении следующих условий:
реальные показатели надежности для комплектующих изделий (элементов) соответствуют расчетным;
все технологические операции, связанные с производством, выполнены без ошибок и нарушения технологических режимов из-за воздействия случайных факторов.

Это дает основание утверждать, что задача *определения* технического состояния изделий является одной из основных, решаемых на этой стадии.

Решение задачи определения технического состояния основано на применении средств технического контроля и диагностики, охватывающего все стадии производственного процесса. Иными словами, необходим входной конт-роля качества поступающих материалов и комплектую-щих изделий и, затем, контроль промежуточных технологических стадий и отдельно изготавливаемых компонент (печатных плат, блоков,

устройств, схемных соединений, механических конструк-ций), вплоть до испытаний готовой продукции.

Зависимость показателей надежности (обеспечения надежности в целом) от достоверной верификации производственно-техноло-гического цикла настолько важна, что для ее оценки часто используют отдельный показатель – риск изготовителя. Этот показатель используется в качестве основного многими фирмами-изготовителями за рубежом, но, к сожалению, не предусмотрен отечественными стандартами.

Риск изготовителя определяется как вероятность события, суть которого состоит в ошибочной оценке технического состояния изделия при выходном контроле, точнее, риске принятия в действительности неисправного готового изделия исправным.

При значениях этой вероятности, превышающей 0,02-0,03 выпуск изделия считается убыточным из-за потерь престижа и затрат на гарантийные ремонты.

Пусть известна вероятность того, что будет произведено неисправное изделие, и объем производимой партии составляет величину . Тогда число неисправных изделий, поступающих на стадию выходного контроля можно определить как .

В дальнейшем предполагается, что неисправности, возникшие при этом носят случайный характер, являются независимыми и равновероятными. Используемые средства контроля характеризуются полнотой контроля , которая определяется как отношение числа обнаруживаемых этими средствами неисправностей к числу всех возможных неисправностей контролируемого изделия.

При условии безотказности средств контроля число ошибок, определяющих риск изготовителя, вычисляется следующим образом:

.

Риск изготовителя можно рассчитать в соответствии с классическим определением вероятности события риска, (число всех возможных элементарных исходов определяется числом изделий, признанных годными) :

. (1.20)

По сообщению фирмы TRW [32] при изготовлении СБИС, содержащей активных элементов, с площадью кристалла см^2 и рассеиваемой мощностью 8,5 Вт достигнута величина . При условии, что риск изготовителя составляет величину , полнота выходного контроля должна быть (для –).

Если надежность контролирующей аппаратуры описывается экспоненциальной моделью, а время контроля одного изделия – постоянно, то можно записать выражение для риска изготовителя в виде:

. (1.21)

В выражении (1.21) величина соответствует вычисляемой в соответствии с (1.20), а – интенсивности отказов контролирующего оборудования.

Последнее выражение может использоваться для определения периодичности проведения профилактических мероприятий для контролирующего оборудования с целью обеспечения необходимого риска изготовителя. При этом число изделий проверяемой партии определяется выражением

,

где – средняя наработка на отказ контролирующего оборудования.

На *этапе эксплуатации* для поддержания высоких значений показателей надежности в основном восстанавливаемых систем необходимо минимизировать интервал времени восстановления (при эксплуатации таких технических систем как СВТ устойчивая тенденция к увеличению стоимости времени простоя стала закономерностью). Этот интервал включает время обнаружения неисправности, ее локализации и последующего ремонта, т.е. замены отказавшего элемента, компоненты и т.п. Минимизация первых двух составляющих возможна за счет повышения эффективности и достоверности контрольно-диагностических процедур, последней – с помощью правильно подобранного запасного комплекта, использования квалифицированных профессионалов-ремонтников и, возможно, специального оборудования. Для минимизации времени на последней стадии разработаны специальные методики, например, модель ЗИП и др. [49].

Качество контрольно-диагностических мероприятий на стадиях производства и эксплуатации, а также связанные с ними затраты можно прогнозировать, учитывая при проектировании объектов свойство их контролепригодности. Формально выразить это свойство применительно ко всем методам контроля не представляется возможным. Кроме того, само свойство контролепригодности в настоящее время недостаточно изучено и вызывает у разработчиков технических систем существенно различные ассоциации. В последних разделах книги это свойство исследуется применительно к методам тестового контроля и диагностики СВТ в связи с тем, что весь последующий материал посвящен систематизации этих методов в качестве средств

обеспечения надежности аппаратных (в том числе и программно управляемых) компонент вычислительных систем и сетей.