УДК 004.052(075)

М.В. Мальков
Институт информатики и математического моделирования Кольского НЦ РАН

О НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ*

Аннотация

В обзоре рассмотрен такой показатель качества информационных систем как надежность. Рассмотрены проблемы обеспечения надежности функционирования информационных систем. Кратко описаны модели и методы расчета надежности. Особое внимание уделено Марковским моделям расчета надежности.

Ключевые слова:

информационная система, надежность, модель, метод, модель Маркова.

M.V. Malkov

ABOUT RELIABILITY OF INFORMATION SYSTEMS

Abstract

This review relates to the reliability of information systems. Different problems concerning provision of the reliability are considered. Models and methods to calculate the reliability are briefly described. Special attention is paid to Markov`s model of reliability calculation.

Keywords:

information system, reliability, model, method, Markov`s model.

Основными показателями качества информационных систем являются надежность, достоверность и безопасность. В этом обзоре мы уделим внимание такому показателю качества как надежность. Надежность - свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения. Надёжность - это более узкая характеристика, чем качество. Надежность - это сложное свойство, включающее в свой состав несколько единичных свойств: безотказность, готовность, сохраняемость, ремонтопригодность, а также безопасность и живучесть [1].

Проблема надежности технических систем существует уже несколько десятилетий, и она особенно обострилась с широким внедрением сложных систем массового обслуживания (СМО). Создание и использование такой техники без специальных мер по обеспечению ее надежности не имеет смысла. Опасность заключается не только в том, что новая сложная техника не будет работать, но главным образом в том, что отказы в ее работе, в том числе и неправильная работа, может привести к катастрофическим последствиям. С учетом этого при проектировании, изготовлении и эксплуатации систем должны предприниматься соответствующие меры, обеспечивающие повышение надежности этих систем.

* Работа выполнена при поддержке РФФИ (грант № 12-07-00138 - Разработка когнитивных моделей и методов формирования интегрированной информационной среды поддержки управления безопасностью Арктических регионов России).

Для решения проблемы надежности потребовалась разработка научных основ нового научного направления - наука о надёжности. Предмет её исследований - изучение причин, вызывающих отказы объектов, определение закономерностей, которым отказы подчиняются, разработка способов количественного измерения надёжности, методов расчёта и испытаний, разработка путей и средств повышения надёжности. Наука о надёжности развивается в тесном взаимодействии с другими науками, такими как:

- математическая логика (позволяет на языке математики представить сложные логические зависимости между состояниями системы и её комплектующих частей);
- теория вероятностей, математическая статистика и теория вероятностных процессов. Эти дисциплины дают возможность учитывать случайный характер возникающих в системе событий и процессов, формировать математические основы теории надёжности;
- теория графов, исследования операций, теория информации, техническая диагностика, теория моделирования, основы проектирования систем и технологических процессов - такие научные дисциплины, без которых невозможно было бы развитие науки о надёжности [9].

Под расчетом надежности понимают определение численных показателей по тем или иным числовым данным.

Все системы в теории надежности классифицируются по ряду признаков. Важными классификационными группами являются: восстанавливаемые; невосстанавливаемые; обслуживаемые; необслуживаемые системы.

Показатели надежности

Показатель надежности - это количественная характеристика одного или нескольких свойств, определяющих надежность системы. В основе большинства показателей надежности лежат оценки наработки системы, то есть продолжительности или объема работы, выполненной системой. Показатель надежности, относящийся к одному из свойств надежности, называется единичным. Комплексный показатель надежности характеризует несколько свойств, определяющих надежность системы.

Обеспечение надежности функционирования информационных систем (ИС)

Информационная система - это сложная человеко-машинная система, включающая в свой состав эргатические звенья, технические средства и программное обеспечение. Все методы обеспечения надежности и достоверности ИС можно отнести к двум классам. Один включает в себя методы, обеспечивающие безошибочность (безотказность) функциональных технических, эргатических и программных звеньев ИС, то есть, в конечном счете, повышающие их надежность. Другой - методы, обеспечивающие обнаружение и исправление ошибок, возникающих в информации, то есть методы контроля достоверности информации и ее коррекции, косвенно также повышающие функциональную надежность систем.

Существуют различные виды обеспечения надежности: экономическое; временное; организационное; структурное; технологическое; эксплуатационное; социальное; эргатическое; алгоритмическое; синтаксическое; семантическое.

Обеспечение можно определить как совокупность факторов (элементов, методов, приемов, процедур, ресурсов и т. п.), способствующих достижению поставленной цели. Экономическое и временное обеспечения, обусловливаемые необходимостью соответственно материальных и временных затрат, используются для реализации процедур обеспечения достоверности. Организационное, эксплуатационное, техническое, социальное и эргатическое обеспечения применяются преимущественно для повышения надежности систем, а структурное и алгоритмическое обеспечения - для обоих классов методов.

При анализе надёжности целесообразно рассматривать три этапа:

1) проектирование;
2) изготовление;
3) эксплуатация.

Факторы, влияющие на надёжность при проектировании:

- количество и качество элементов в системе оказывает влияние на надёжность. Увеличение количества используемых элементов приводит к резкому ухудшению надёжности;
- режим работы элементов. Самые надёжные элементы, работающие в тяжёлом, не предусмотренном для их применения режиме, могут стать источником частых отказов. Для каждого элемента устанавливаются технические условия на режим работы этого элемента;
- применение стандартных и унифицированных элементов резко повышает надёжность системы.

Факторы, влияющие на надёжность в процессе изготовления:

- качество материалов;
- качество хранения материалов и комплектующих изделий;
- соблюдение технологии изготовления и сборки: термообработка, антикоррозийные покрытия и т.п.

Факторы, влияющие на надёжность в процессе эксплуатации:

- квалификация обслуживающего персонала;
- внешние условия: климатические условия, вибрации, перегрузки;
- на надёжность влияет фактор времени. Продолжительность эксплуатации аппаратуры с момента выпуска до капитального ремонта может составлять несколько лет. К концу этого периода повышается опасность возникновения отказов отдельных элементов системы.

Практическая реализация надежных ИС

Обеспечение надежности технических компонентов информационных систем реализуется аппаратным и программным способами. В первом случае ИС использует аппаратную избыточность: все операции выполняются параллельно на одинаковых компонентах системы, а результаты их работы затем сравниваются, что позволяет выявить ошибки; в случае выхода из строя какого-либо компонента его резервные аналоги продолжают работу без остановки, а отказавший компонент заменяется на работоспособный. Программный способ предусматривает: последовательное во времени выполнение одних и тех же информационных процессов и дублирование данных; автоматическое восстановление отказавших операционных систем, приложений и искаженных данных.

Для обеспечения надежности технических средств чаще всего производится: резервирование (дублирование) технических средств; использование стандартных протоколов работы устройств ИС; применение специализированных технических средств защиты информации. Для обеспечения надежности функционирования ИС требуется тщательное тестирование. Например, для компьютеров в качестве наиболее эффективных мер комплексного обеспечения надежности ИС можно назвать кластеризацию компьютеров и использование отказоустойчивых компьютеров [5].

В теории надежности весьма важную роль играет деление элементов и систем на восстанавливаемые и невосстанавливаемые. Содержательный смысл этих понятий очевиден. Они позволяют обоснованно решать задачи надёжности.

При аналитическом методе основными показателями надежности являются: вероятность безотказной работы и средняя наработка на отказ, которые определяются по известным интенсивностям отказов элементов, входящих в данную информационную систему. Однако для АСУ, информационных сетей и вычислительной техники этих понятий для характеристики надёжности недостаточно. В практике создания и использования АСУ применяются дополнительные понятия, без учёта которых нельзя в полной мере представить комплексное понятие “надёжность”. Рассмотрим эти понятия:

1. Живучесть - свойство объекта сохранять работоспособность (полностью или частично) в условиях неблагоприятных воздействий, не предусмотренных нормальными условиями эксплуатации. Главный смысл требования к живучести объекта состоит не только в том, чтобы он длительное время непрерывно без отказа работал в нормальных условиях эксплуатации и, чтобы его можно было быстро отремонтировать, но также и в том, чтобы он в ненормальных условиях эксплуатации сохранял работоспособность, хотя бы и ограниченную.

2. Достоверность информации, выдаваемой объектом. При работе вычислительной машины или тракта передачи информации могут отсутствовать отказы. Поэтому объект может обладать высокой безотказностью, хорошей долговечностью, сохраняемостью и ремонтопригодностью. Однако в нём могут иметь место сбои, искажающие информацию. “Портится” не аппаратура, а информация. Это не менее опасная “поломка” [9].

При исследовании надёжности часто ставится задача определить причины, приводящие к формированию той или другой стороны надёжности. Без этого невозможно наметить правильную программу работ по повышению надёжности. Это приводит к делению надёжности на:

- аппаратную надёжность, обусловленную состоянием аппаратуры;
- программную надёжность объекта, обусловленную состоянием программ;
- надёжность объекта, обусловленную качеством обслуживания;
- надёжность функциональная [9].

Надёжность функциональная - надёжность выполнения отдельных функций, возлагаемых на систему. Известно, что АСУ, как правило, система многофункциональная, т.е. она предназначается для выполнения ряда функций, различных по своей значимости. Требования к надёжности выполнения

различных функций могут быть различными. Поэтому может оказаться целесообразным задавать различные требования к выполнению различных функций. Примером функциональной надёжности в АСУ может быть надёжность передачи определённой информации в системе передачи данных.

Как правило, методика расчета показателей надежности сводится к следующему:

- составляется система дифференциальных уравнений в соответствии с графом состояний системы;
- выбираются начальные условия решения задачи;
- определяются показатели надежности системы.

Система уравнений составляется согласно правилу: производная вероятности данного состояния равна алгебраической сумме произведений интенсивностей всех возможных переходов этого состояния на вероятность состояний, из которых выходят линии перехода. Знак у слагаемого положительный, если линия перехода входит в данное состояние, и отрицательный, если линия перехода выходит из этого состояния [2].

Модели и методы расчета надежности

На этапе исследования и проектирования систем при построении и реализации машинных моделей (аналитических и имитационных) используются различные методы и модели для расчета надежности.

Метод Монте-Карло

На практике достаточно широко используется метод статистического моделирования Монте-Карло, который базируется на использовании случайных чисел, т.е. возможных значений некоторой случайной величины с заданным распределением вероятностей. Статистическое моделирование представляет собой метод получения с помощью ЭВМ статистических данных о процессах, происходящих в моделируемой системе. Для получения представляющих интерес оценки характеристик моделируемой системы с учетом воздействий внешней среды статистические данные обрабатываются и классифицируются с использованием методов математической статистики.

Сущность метода статистического моделирования сводится к построению для процесса функционирования исследуемой системы некоторого моделирующего алгоритма, имитирующего поведение и взаимодействие элементов системы с учетом случайных входных воздействий и воздействий внешней среды, и реализации этого алгоритма с использованием программно-технических средств ЭВМ.

Различают две области применения метода статистического моделирования:

- для изучения стохастических систем;
- для решения детерминированных задач.

Основной идеей, которая используется для решения детерминированных задач методом статистического моделирования, является замена детерминированной задачи эквивалентной схемой некоторой стохастической системы, выходные характеристики которой совпадают с результатом решения детерминированной задачи. В результате статистического моделирования

системы получается серия частных значений искомых величин или функций, статистическая обработка которых позволяет получить сведения о поведении реального объекта или процесса в произвольные моменты времени. Если количество реализаций достаточно велико, то полученные результаты моделирования системы приобретают статистическую устойчивость и с достаточной точностью могут быть приняты в качестве оценок искомых характеристик процесса функционирования системы [4].

Случайные величины обычно моделируют с помощью преобразований одного или нескольких независимых значений случайной величины, равномерно распределенной в интервале (0,1). Моделирование случайных процессов строится на основе базовых распределений случайных величин. Одним из таких процессов является марковские процессы [4].

Модель Шика - Волвертона

В основе модели Шика - Волвертона лежит предположение, согласно которому частота ошибок пропорциональна не только количеству ошибок в программах, но и времени тестирования, т.е. вероятность обнаружения ошибок с течением времени возрастает. Частота ошибок (интенсивность обнаружения ошибок) предполагается постоянной в течение интервала времени t и пропорциональна числу ошибок, оставшихся в программе по истечении (i-1)-го интервала; но она пропорциональна также и суммарному времени, уже затраченному на тестирование (включая среднее время выполнения программы в текущем интервале). В данной модели наблюдаемым событием является число ошибок, обнаруживаемых в заданном временном интервале, а не время ожидания каждой ошибки. Данная модель относят к группе дискретных динамических моделей.

Модель Муса

Модель Муса относят к динамическим моделям непрерывного времени. Это значит, что в процессе тестирования фиксируется время выполнения программы (тестового прогона) до очередного отказа. Но считается, что не всякая ошибка может вызвать отказ, поэтому допускается обнаружение более одной ошибки при выполнении программы до возникновения очередного отказа.

В модели Муса различают два вида времени:

1) суммарное время функционирования, которое учитывает чистое время тестирования до контрольного момента, когда проводится оценка надежности;

2) оперативное время выполнения программы, планируемое от контрольного момента и далее при условии, что дальнейшего устранения ошибок не будет (время безотказной работы в процессе эксплуатации).

Для суммарного времени функционирования предполагается:

- интенсивность отказов пропорциональна числу неустраненных ошибок;
- скорость изменения числа устраненных ошибок, измеряемая относительно суммарного времени функционирования, пропорциональна интенсивности отказов.

Один из основных показателей надежности, который рассчитывается по модели Муса, - средняя наработка на отказ. Этот показатель определяется, как математическое ожидание временного интервала между последовательными отказами и связан с надежностью.

Модель переходных вероятностей

Эта модель основана на Марковском процессе (см.ниже), протекающем в дискретной системе с непрерывным временем. Процесс, протекающий в системе, называется марковским (или процессом без последствий), если для каждого момента времени вероятность любого состояния системы в будущем зависит только от состояния системы в настоящее время и не зависит от того, каким образом система пришла в это состояние. Процесс тестирования ИС рассматривается как марковский процесс [6].

Марковская модель

В теории массового обслуживания к наиболее изученным и исследованным относятся модели, у которых случайный процесс функционирования относится к классу Марковских процессов, т.е. Марковские модели.

При исследовании ИС аналитическим моделированием наибольшее значение имеют Марковские случайные процессы с дискретными состояниями и непрерывным временем. Процесс называется процессом с дискретными состояниями, если его возможные состояния можно заранее перечислить, т.е. состояния системы принадлежат конечному множеству и переход системы из одного состояния в другое происходит мгновенно. Процесс называется процессом с непрерывным временем, если смена состояний может произойти в любой случайный момент [3].

Процесс возникновения отказов, а также другие характеристики надёжности носят случайный характер. Для исследования случайных явлений используются вероятностные методы. Таким образом, отличительным признаком надежности как свойства технической системы является то, что она характеризуется вероятностными процессами, протекающими во времени.

Марковские случайные процессы названы по имени русского математика А.А. Маркова, впервые начавшего изучение вероятностной связи случайных величин и создавшего теорию, которую можно назвать “динамикой вероятностей”. В дальнейшем основы этой теории явились исходной базой общей теории случайных процессов, а также таких важных прикладных наук, как теория диффузионных процессов, теория надежности, теория массового обслуживания и т.д. В настоящее время теория марковских процессов и ее приложения широко применяются в самых различных областях таких наук, как механика, физика, химия и др.

Марковские случайные процессы относятся к частным случаям случайных процессов. В свою очередь, случайные процессы основаны на понятии случайной функции.

Если случайная последовательность обладает марковским свойством, то она называется цепью Маркова. Если в случайном процессе состояния дискретны, время непрерывно и свойство последействия сохраняется, то такой случайный процесс называется марковским процессом с непрерывным временем [3].

Множество состояний системы марковской цепи, определенным образом классифицируется с учетом дальнейшего поведения системы. Актуальность такого моделирования сохраняется для систем, в которых протекают так называемые процессы без последействия. Процессы без последействия находят место при функционировании многих технических систем. К таковым, в первую очередь, относится широкий класс самых разнообразных объектов, имеющих общее название систем массового обслуживания (СМО).

В многоэлементных системах с большим числом состояний аналитическое моделирование на основе теории марковских процессов становится весьма громоздким. В этом случае используется так называемый метод динамики средних, который в основе имеет также марковость процесса. Этот метод существенно упрощает аналитическое моделирование для случаев определения средних характеристик состояний моделируемой системы. В этой теме дано обоснование метода и приводятся примеры его применения. В практике часто возникает задача моделирования процессов случайной смены состояний в исследуемом объекте. Вид очередного состояния может определяться случайным образом, смена состояний может происходить в случайные или не случайные моменты времени.

Практически любой случайный процесс является марковским или может быть сведен к марковскому. В последнем случае достаточно в понятие состояния включить всю предысторию смен состояний системы.

Марковские процессы делятся на два класса:

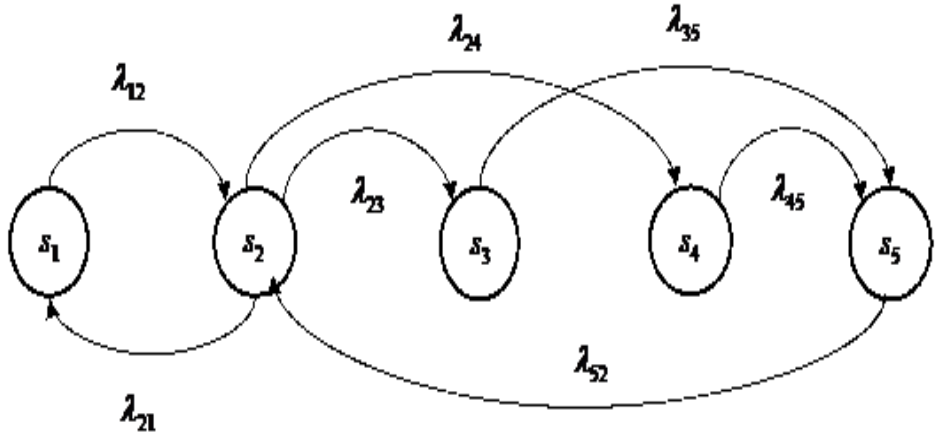
- дискретные марковские процессы (марковские цепи);
- непрерывные марковские процессы.

Марковская цепь может быть представлена графом, вершины которого соответствуют состояниям цепи, а дуги ненулевым вероятностям переходов. Для описания поведения системы в виде марковской модели следует определить понятие состояния системы; выявить все состояния, в которых может находиться система. Указать, в каком состоянии находится система в начальный момент; построить граф (пример графа на рис.) состояний и возможные переходы из состояния в состояние – стрелками, соединяющими состояния (на рисунке вершины графа обозначают состояние $\mathbf{S}_i$, а дуги - переходные вероятности); разметить граф, т.е. для каждого перехода указать интенсивность $\boldsymbol{\lambda}(t)$ потока событий, переводящих систему из состояния $\mathbf{S}_i$ в состояние $\mathbf{S}_j$.

Для стационарных Марковских процессов интенсивности переходов не зависят от времени. Понятие состояния зависит от целей моделирования. В одном случае, например, оно может быть определено по состояниям элементов, каждый из которых может быть «свободен» или «занят»; в другом случае состояние системы определяется числом заявок, находящихся на обслуживании и в очередях.

В классе марковских процессов выделяют процессы с дискретными состояниями, называемые марковскими цепями. Когда множество состояний процесса $\mathbf{S}=\{S_1,\ldots S_2\}$ конечно, марковскую цепь называют конечной.

Конечная марковская цепь может быть определена в непрерывном или дискретном времени. В первом случае переходы процесса из одного состояния в другое связываются с произвольными моментами времени t_0, t_1, t_2 и цепь называют непрерывной; во втором – только в фиксированные моменты времени, обозначаемые порядковыми номерами t=0,1,2… и цепь называется дискретной (рис.).



Пример графа состояний

Дискретная марковская цепь определяется:

- множеством состояний $\mathbf{S}=\{S_1,\ldots S_K\}$;
- матрицей вероятностей переходов **P**, элементы которой характеризуют вероятности перехода процесса из состояния $\mathbf{S}_i$ в состояние $\mathbf{S}_j$;
- вектором начальных вероятностей $\mathbf{V}_0=\{P_1^{(0)},\ldots, P_k^{(0)}\}$, определяющим вероятности $P_i^{(0)}$ того, что в начальный момент времени t=0 процесс находится в состоянии $\mathbf{S}_i$.

Марковская цепь порождает множество реализаций случайного процесса **f**(t), который представляется последовательностью состояний $\mathbf{f}(t)=\mathbf{S}_i^{(0)}$, $\mathbf{S}_i^{(1)}$, $\mathbf{S}_i^{(2)}$, … соответствующих моментам времени t=1,2,… В зависимости от возможности перехода из одних состояний в другие, марковские цепи делятся на поглощающие и эргодические цепи.

Эргодическая марковская цепь представляет собой множество состояний, связанных матрицей переходных вероятностей таким образом, что из какого бы состояния процесс ни исходил, после некоторого числа шагов он может оказаться в любом состоянии. По этой причине состояния эргодической цепи называются эргодическими (возвратными). Процесс, порождаемый эргодической цепью, начавшись в некотором состоянии, никогда не завершается, а последовательно переходит из одного состояния в другое, попадая в различные состояния с разной частотой, зависящей от переходных вероятностей. Поэтому основная характеристика эргодической цепи – вероятности пребывания процесса в состояниях $\mathbf{S}_j$, j=1,…,k, или относительные частоты попадания процесса в состояния $\mathbf{S}_j$ и доля времени, которую процесс проводит в каждом из состояний. В качестве дополнительных характеристик эргодических цепей используются математическое ожидание, и дисперсия времени (числа шагов) первого попадания в состояние $\mathbf{S}_j$ из состояния $\mathbf{S}_i$, и предельная корреляция числа попаданий в состояния $\mathbf{S}_i$ и $\mathbf{S}_j$. Эти характеристики определяются методами алгебраической теории марковских цепей.

Эргодические цепи широко используются в качестве моделей надежности систем. В этом случае состояния цепи соответствуют состояниям системы различающихся составом исправного и отказавшего оборудования. Переходы между состояниями связаны с отказами и восстановлением устройств и реконфигурацией связей между ними, выполняемой для сохранения работоспособности системы. Оценки характеристик эргодической цепи дают представление о надежности поведения системы в целом. Кроме того, эргодические цепи широко используются в качестве базовых моделей взаимодействия устройств с задачами, поступающими на обработку.

ЛИТЕРАТУРА

1. Оценка качественных и количественных характеристик информационных систем. - Режим доступа: http://daxnow.narod.ru
2. Надёжность информационных систем. – Режим доступа: http://www.metods-rgrtu.ru/index.php
3. Марковские модели. – Режим доступа: http://life-prog.ru/view_modelirovanie.php?id=19
4. Методы и алгоритмы построения элементов систем статистического моделирования. - Режим доступа: http://www.coolreferat.com/
5. Теоретические основы Марковских цепей. - Режим доступа: http://www.sevostyanovpa.ru/uploads/LecMarkovProc0.pdf
6. Динамические модели надежности. - Режим доступа: http://info-tehnologii.ru/kac_sr/Mod_nad/DiN/index.html
7. Базовые сведения о надежности информационных технологий управления. - Режим доступа: http://www.bestreferat.ru/referat-202583.html
8. Модель оценивания работоспособности информационной системы в условиях неопределенности. – Режим доступа: http://sir35.narod.ru/Cmagin/K31122/Part_1_5_31122.htm
9. Надёжность функционирования автоматизированных систем. - Режим доступа: http://gendocs.ru/v4171/

Сведения об авторе

Мальков Михаил Васильевич - к.ф.-м.н., научный сотрудник,
e-mail:malkov@iimm.kolacs.net.ru
Michael V. Malkov - Ph.D. (Phys.&Math. Sci.), researcher